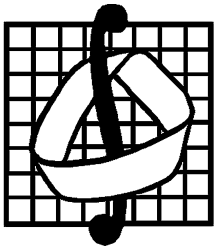
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
им. М. В. ЛОМОНОСОВА



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

МАТЕРИАЛЫ

IX Международного семинара

«ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ»,

посвященного 75-летию со дня рождения академика О. Б. ЛУПАНОВА

(Москва, 18–23 июня 2007 г.)

Издательство механико-математического факультета МГУ

Москва 2007

М34
УДК 519.7

Издание осуществлено при поддержке Российского фонда фундаментальных исследований по проекту 07–01–06057

М34 Материалы IX Международного семинара «Дискретная математика и ее приложения», посвященного 75-летию со дня рождения академика О. Б. Лупанова (Москва, МГУ, 18–23 июня 2007 г.) / Под редакцией О. М. Касим-Заде. — М.: Изд-во механико-математического факультета МГУ, 2007. — 477 с.

Сборник содержит материалы IX Международного семинара «Дискретная математика и ее приложения», посвященного 75-летию со дня рождения академика О. Б. Лупанова, проходившего на механико-математическом факультете МГУ им. М. В. Ломоносова с 18 по 23 июня 2007 г. при поддержке Российского фонда фундаментальных исследований (проект 07–01–06057). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание

МАТЕРИАЛЫ
IX МЕЖДУНАРОДНОГО СЕМИНАРА
«ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ»,
посвященного 75-летию со дня рождения академика О. Б. Лупанова
(Москва, МГУ, 18–23 июня 2007 г.)

Под общей редакцией О. М. КАСИМ-ЗАДЕ

Редакционная группа:
К. А. Зыков, В. В. Кочергин, А. В. Чашкин

Ответственный за выпуск *В. В. Кочергин*

Н/К
ИД № 04059 от 20.02.2001 Подписано к печати 19.07.2007. Формат 60 × 90/16.
Бумага типогр. № 1. Печ. л. 30. Тираж 300 экз.
Издательство механико-математического факультета МГУ. 119992, Москва, Ленинские горы, МГУ.
Отпечатано на оборудовании механико-математического факультета МГУ

ПРЕДИСЛОВИЕ

IX Международный семинар «Дискретная математика и ее приложения», посвященный 75-летию со дня рождения академика О. Б. Лупанова, проходил на механико-математическом факультете МГУ им. М. В. Ломоносова с 18 по 23 июня 2007 г. при поддержке Российского фонда фундаментальных исследований (проект 04–01–06057–г).

Оргкомитетом семинара до начала его работы были разосланы информационные письма в ведущие научные центры и университеты стран СНГ, отобраны наиболее интересные доклады и сообщения для заслушивания на пленарных и секционных заседаниях.

Семинар собрал около 250 участников (в том числе более 60 докторов наук) из 35 научных центров России, Беларуси, Украины, Азербайджана и Польши.

Работа семинара проходила в шести секциях:
— синтез, сложность и надежность управляющих систем,
— теория функциональных систем,
— комбинаторный анализ и теория графов,
подсекции:
— комбинаторный анализ,
— теория графов,
— математическая теория интеллектуальных систем,
— дискретная геометрия,
— теория кодирования и смежные вопросы.

Всего было заслушано 19 пленарных и 178 секционных докладов; содержание большинства из них отражено в настоящем сборнике.

Тексты публикуются в авторской редакции (исправлены замеченные опечатки).

ОЛЕГ БОРИСОВИЧ ЛУПАНОВ (02.06.1932 — 03.05.2006)

Олег Борисович Лупанов родился 2 июня 1932 г. в Ленинграде. Окончив в 1950 г. с золотой медалью среднюю школу, он поступил на механико-математический факультет Московского университета, который закончил с отличием в 1955 г. Еще до окончания университета, в 1954 г. О. Б. Лупанов был принят на работу в Отделение прикладной математики Математического института им. В. А. Стеклова АН СССР (ныне Институт прикладной математики им. М. В. Келдыша РАН). Там же в 1955–1958 гг. проходил аспирантуру. В Ин-

ституте прикладной математики Олег Борисович работал до конца своей жизни, и в последнее время заведовал отделом теоретической кибернетики. В 1958 г. О. Б. Лупанов защитил диссертацию на соискание ученой степени кандидата, в 1963 г. — доктора физико-математических наук. В 1966 г. он вместе с Ю. И. Журавлёвым и С. В. Яблонским был удостоен Ленинской премии за цикл работ по математической теории синтеза управляющих систем. В 1972 г. О. Б. Лупанов был избран членом-корреспондентом АН СССР, в 2003 г. — действительным членом РАН.

Олег Борисович был одним из тех, кто стоял у истоков новой области математической науки — дискретной математики и математической кибернетики, автором основополагающих научных результатов, создателем большой научной школы, крупным организатором отечественной науки и образования.

Научная деятельность О. Б. Лупанова началась в годы учебы в Московском университете под руководством С. В. Яблонского, привлекшего внимание Олега Борисовича к проблемам синтеза и сложности управляющих систем. Пятидесятые годы XX в. были временем становления дискретной математики и математической кибернетики в составе большого цикла новых математических дисциплин, вызванных к жизни быстрым развитием электронной цифровой вычислительной и коммуникационной техники. В проблематике этих дисциплин вопросы сложности занимают одно из центральных мест. В то время исследования только начинались, и отсутствие адекватных средств для решения проблем сложности ощущалось очень остро. Такие средства были предложены О. Б. Лупановым.

Уже в первых работах О. Б. Лупанова проявились его блестящие математические способности. В 1958 г. Олегом Борисовичем были опубликованы две фундаментальные работы, результаты которых стали теперь классическими и вошли во многие учебники. В этих работах им были построены асимптотически оптимальные методы синтеза и получены асимптотически точные оценки сложности для важнейших классов управляющих систем — схем из функциональных элементов и контактных схем. Эти результаты Олега Борисовича принесли ему всемирную известность и заложили основы созданного им нового научного направления — асимптотической теории синтеза и сложности управляющих систем.

В последующих работах О. Б. Лупанова были построены асимптотически оптимальные методы синтеза для основных модельных классов управляющих систем: параллельно-последовательных контактных схем, схем без ветвления выходов элементов (формул) и с ограниченным ветвлением (формул с конечной памятью), формул ограниченной глубины, релейно-контактных схем и других. Главной целью этих работ было изучение влияния на сложность раз-

личных схемных ограничений и установление основных закономерностей синтеза управляющих систем. Получение этих результатов потребовало преодоления значительных трудностей и развития тонкой математической техники оптимального синтеза. Совокупность развитых в этих работах универсальных методов синтеза известна теперь под общим названием "метод Лупанова".

О. Б. Лупановым был сформулирован и обоснован важнейший общий принцип теории синтеза и сложности управляющих систем — принцип локального кодирования, являющийся основным инструментом оптимального синтеза для функций из специальных классов. "Принцип Лупанова" стал крупным вкладом в дискретную математику и математическую кибернетику, существенно углубившим понимание закономерностей синтеза и изменившим прежние представления о феномене сложности. В нем тесно переплелись собственно математика, ее приложения и некоторые проблемы философского характера.

Большинство работ О. Б. Лупанова направлено на решение мотивированных практической деятельностью принципиально важных задач, позволяющих обнаруживать новые явления. Олег Борисович часто говорил, что не следует заниматься простым заполнением "многомерной таблицы" всех возможных результатов, "измерения" которой соответствуют различным классам управляющих систем, различным мерам их сложности, различным классам реализуемых функций и так далее; следует активно искать, находить и решать те задачи ("заполнять те клетки таблицы"), в которых обнаруживаются новые эффекты, ведущие к выявлению общих закономерностей.

Ряд таких новых, часто неожиданных, эффектов был установлен в работах О. Б. Лупанова, посвященных сравнению сложности реализации монотонных булевых функций схемами из замыкающих контактов и контактными схемами общего вида, вопросам сложности реализации симметрических функций контактными схемами, исследованию влияния глубины формул на их сложность, сравнению сложности детерминированных и недетерминированных автоматов, синтезу схем из функциональных элементов с задержками, построению универсальных параллельно-последовательных контактных схем глубины 3 и других.

В большинстве своих работ Олег Борисович опередил время: широкий интерес к разрабатываемым в них вопросам пробудился и стал доминирующим лишь спустя годы, а иногда десятилетия. Многие задачи, поставленные в работах О. Б. Лупанова или сообщенные им ученикам и коллегам, дали начало новым разделам и целым научным направлениям.

Для научного стиля О. Б. Лупанова характерно стремление к получению окончательных результатов. Крупным продвижением стал

созданный Олегом Борисовичем асимптотически оптимальный метод синтеза схем из пороговых элементов. В последних опубликованных работах О. Б. Лупанова решена в асимптотической постановке задача о сложности схем из функциональных элементов, реализующих произвольно задаваемые степени булевых операторов и обратные операторы.

Вклад Олега Борисовича в развитие дискретной математики и математической кибернетики далеко не исчерпывается его научными трудами и результатами его работ. Он уделял большое внимание всем сторонам научной деятельности. В постоянном общении с широким кругом коллег и учеников он обсуждал текущее состояние исследований, выдвигал новые постановки задач, делился идеями их решения. Немалая доля "математического фольклора" в области дискретной математики и математической кибернетики возникла при участии и под влиянием Олега Борисовича. При его прямом участии вырабатывалась система основных понятий дискретной математики и математической кибернетики, формулировались цели и направления исследований, составлялись программные документы и статьи, многие из которых написаны его рукой.

В течение всей своей жизни Олег Борисович не прерывал педагогической деятельности. С 1955 г. он преподавал на механико-математическом факультете Московского университета, а с 1970 г. — кроме того и на только что созданном в МГУ факультете вычислительной математики и кибернетики. Олег Борисович читал обязательные курсы лекций по математической логике, дискретной математике и математической кибернетике, специальные курсы. Им были изданы учебные пособия "Лекции по математической логике", "Асимптотические оценки сложности управляющих систем". Вместе с С. В. Яблонским он возглавил издание научно-методической монографии "Дискретная математика и математические вопросы кибернетики". Олег Борисович руководил несколькими научно-исследовательскими специальными семинарами, работал со студентами, аспирантами и даже со сложившимися математиками. Под его научным руководством было защищено 40 кандидатских диссертаций, более десяти его учеников стали докторами наук, и уже ученики учеников защищают докторские диссертации. Созданная О. Б. Лупановым научная школа объединяет большое число специалистов по дискретной математике и математической кибернетике. Его ученики работают во многих городах нашей страны и за рубежом.

Прирожденный математик, О. Б. Лупанов блестяще проявил себя и как организатор научной и педагогической деятельности. В 1980 г. он стал деканом механико-математического факультета МГУ и бессменно возглавлял факультет в течение 26 лет, до последнего дня

своей жизни. Олег Борисович был мудрым и заботливым руководителем. Работе на посту декана он отдавал большую часть своего времени, вникая во все стороны жизни вверенного ему факультета, и, по отзывам коллег, сумел в эти трудные годы сохранить лучшие традиции мехмата.

В 1981 г. О. Б. Лупанов создал на механико-математическом факультете МГУ кафедру дискретной математики, ставшую одним из ведущих коллективов в области дискретной математики и математической кибернетики, центром притяжения его научной школы.

Большое значение Олег Борисович придавал живому общению математиков. Он принимал участие в Международных конгрессах математиков в Москве (1966 г.) и в Ницце (1970 г.), куда был приглашен для выступления с обзорным докладом. До этого в 1956 г. и 1961 г. участвовал в 3-м и 4-м Всесоюзных математических съездах. Олег Борисович постоянно входил в состав оргкомитета конференции "Проблемы теоретической кибернетики", а с 1998 г. возглавлял его. С 1984 г. он руководил Всесоюзным (впоследствии Международным) семинаром "Дискретная математика и ее приложения", который охватил большинство разделов этой области и всегда собирал большое число участников. Это крупное научное мероприятие проводится раз в три года в Московском университете. О. Б. Лупанов основал школу-семинар "Синтез и сложность управляющих систем", объединившую его учеников и наиболее близких по научным интересам коллег. За небольшим исключением она проводилась ежегодно, начиная с 1988 г. Олег Борисович постоянно участвовал в организации и проведении других международных и российских конференций и семинаров, входил в состав их оргкомитетов и программных комитетов.

Много сил Олег Борисович отдавал редакционно-издательской работе. До конца своих дней он был главным редактором журнала "Вестник Московского университета. Математика. Механика", заместителем главного редактора журнала "Дискретная математика", членом редколлегий журналов "Вестник Московского университета. Вычислительная математика и кибернетика", "Дискретный анализ и исследование операций" (Новосибирск), "Кибернетика и системный анализ" (Киев). В разное время был членом редколлегий журналов "Проблемы передачи информации" и "Fundamenta Informaticae" (Варшава).

Олег Борисович участвовал в составлении и редактировании почти всех выпусков основанного в 1958 г. А. А. Ляпуновым сборника "Проблемы кибернетики" и всех выпусков сборника "Математические вопросы кибернетики", который явился его продолжением. С 1998 г. этот сборник стал выходить под редакцией О. Б. Лупанова.

Вместе с А. А. Ляпуновым он начал в 1960 г. выпускать "Кибернетический сборник" переводов лучших работ зарубежных авторов по дискретной математике и математической кибернетике, с 1974 г. выходивший под редакцией Олега Борисовича. Эти издания сыграли огромную роль в становлении и развитии дискретной математики и математической кибернетики в нашей стране. В последние годы Олег Борисович входил в редколлегию энциклопедии "Дискретная математика".

На протяжении многих лет О. Б. Лупанов был членом экспертного совета ВАК по математике и механике, членом нескольких советов по защитам докторских диссертаций и председателем одного из них на механико-математическом факультете МГУ, председателем Научно-методического совета по математике и механике Учебно-методического объединения университетов России, входил в состав многих других ученых и научных советов.

За выдающиеся заслуги в деле науки и образования О. Б. Лупанов удостоен многих государственных наград, научных премий и почетных званий. Он награжден орденами "Знак почета" (1975 г.), Трудового Красного Знамени (1982), Дружбы Народов (1992), Дружбы (2003). В 1992 г. ему была присуждена премия имени М. В. Ломоносова I степени (МГУ), в 2001 г. присвоено почетное звание "Заслуженный профессор Московского университета".

Олег Борисович был скромным, внимательным и чутким человеком. В то же время он был волевым и твердым в принципиальных вопросах. Яркий талант математика, острый, проницательный ум и большой жизненный опыт в сочетании с неизменной доброжелательностью оставляли при общении с ним незабываемое впечатление. Он был наделен даром находить решения трудных вопросов не только в науке, но и в жизни, многим помог советом и делом.

Кончина Олега Борисовича Лупанова 3 мая 2006 года явилась тяжелой потерей для отечественной науки и образования, для всех, кто работал с ним и близко знал его. Осталась память об этом замечательном математике и человеке, прожившем исполненную глубокого смысла жизнь и успевшем сделать так много, прежде чем она неожиданно и безвременно оборвалась. Остались ученики. Остались его мысли, статьи и книги, задуманные и начатые им дела, всегда имевшие целью благо людей, и благо его любимой науки — математики.

По материалам статьи в сб. "Математические вопросы кибернетики", вып. 15. *М.*: *Физматлит,* 2006. *С.* 3–6.

ПЛЕНАРНЫЕ ДОКЛАДЫ

О МИНИМАЛЬНЫХ И АСИМПТОТИЧЕСКИ МИНИМАЛЬНЫХ СХЕМАХ ДЛЯ НЕКОТОРЫХ ИНДИВИДУАЛЬНЫХ БУЛЕВЫХ ФУНКЦИЙ

Н. П. Редькин (Москва)

Проблема построения минимальных или достаточно близких к минимальным схем для реализации булевых функций является одной из центральных в математической кибернетике. Исторически так сложилось, что первоначально в качестве реализуемых рассматривались совершенно произвольные булевы функции и изобретались такие методы синтеза, которые давали хорошие результаты применительно к наиболее сложно реализуемым (и в этом смысле наиболее «плохим») функциям. В этом направлении основы математической теории были заложены в работах К. Шеннона [1]; мощное развитие и блестящее завершение эта теория получила в работах О. Б. Лупанова [2–4]. Основной итог исследований Шеннона, Лупанова, а также ряда других авторов — это разработанные ими методы синтеза контактных схем и схем из функциональных элементов, которые для «почти всех» булевых функций, а также для наиболее сложных функций из достаточно обширных классов позволяют строить асимптотически минимальные схемы.

Иную картину мы наблюдаем в области построения минимальных (или близких к минимальным) схем для конкретных булевых функций. Здесь продвижения в направлении разработки достаточно общих, универсальных методов синтеза, пригодных для реализации схемами различных конкретных булевых функций, представляются гораздо более скромными. И это несмотря даже на то, что постоянно существовавший интерес к исследованию сложности отдельных булевых функций со временем, пожалуй, только возрастает, особенно с учетом установленного (прежде всего в работах Шеннона и Лупанова) факта сложной реализуемости и в силу этого фактической недоступности «почти всех» булевых функций. Анализ сложившейся совокупности обстоятельств позволяет утверждать, что в этой области ситуация принципиально иная и достаточно общих, универсальных и вместе с тем достаточно хороших методов синтеза схем (типа асимптотически оптимального метода Лупанова для произвольных булевых функций) для конкретных булевых функций, скорее всего, не существует.

Известные к настоящему времени способы получения нижних оценок сложности конкретных булевых функций, как правило, достаточно сильно отличаются друг от друга, используют различные свойства схем из функциональных элементов в тех или иных базисах, свойства реализуемых булевых функций, возможности эквивалентных преобразований схем и т. д. И хотя некоторые подходы к получению нижних оценок сложности схем (например, метод «забивания» переменных на входах схем булевыми константами [5]) и обладают определенной универсальностью, далеко не всегда известные методы позволяют установить необходимую нижнюю оценку при рассмотрении очередной конкретной функции и зачастую приходится изыскивать новые подходы или существенно модифицировать уже известные.

В еще большей степени сказанное относится к верхним оценкам сложности индивидуальных булевых функций. Правда, во многих случаях верхние оценки получаются конструктивно без особых затруднений. Вместе с тем известны и примеры другого рода, когда для построения даже не минимальных, а только асимптотически минимальных схем линейной сложности по числу переменных у реализуемых функций потребовалось изобретение далеко не очевидных конструкций (например, метод Б. И. Финикова [6] для булевых функций с малым числом единиц, метод М. И. Гринчука [7] для монотонных симметрических пороговых функций с порогом 2). В итоге мы наблюдаем достаточно растянутый по времени и далеко еще не завершенный процесс исследования сложности реализации индивидуальных булевых функций.

Здесь уместно сказать о том, что О. Б. Лупанов большое значение придавал научным исследованиям по сложности индивидуальных булевых функций. Он постоянно интересовался всеми продвижениями, новыми подходами и методами в этой области, знал все достигнутые сколь-нибудь значимые результаты, обладал замечательной и зачастую безошибочной научной интуицией и всегда поддерживал, а порой и направлял усилия своих учеников и коллег, связанные с нахождением или оценкой сложности реализации конкретных булевых функций и построением минимальных или в том или ином смысле близких к минимальным схем для таких функций. Ниже приводятся обзор результатов, полученных за последние пять лет на кафедре дискретной математики механико-математического факультета МГУ, а также выпускниками этой кафедры и относящиеся к сложности реализации индивидуальных булевых функций схемами из функциональных элементов; некоторые более ранние работы различных авторов здесь приводятся, чтобы осветить предысторию того или иного вопроса, а также обрисовать общую картину, каса-

ющуюся сложности реализации отдельных булевых функций.

Пусть $B = \{f_1, \ldots, f_k\}$ — некоторое конечное множество булевых функций, а S — схема над B; через $L_B(S)$ будем обозначать число элементов в S, т. е. сложность схемы S. Пусть f — произвольная булева функция, а $L_B(f) = \min L_B(S)$, где минимум берется по всем схемам над B, реализующим f; число $L_B(f)$ будем считать сложностью (реализации) функции f схемами над B. Схему S над B, реализующую функцию f, будем считать минимальной, если $L_B(S) = L_B(f)$.

И. С. Шкребела исследовал сложность реализации линейных булевых функций схемами над базисом $B_1 = \{x \to y, \overline{x}\}$ и доказал [8] следующее утверждение.

Теорема 1. *Для любого натурального n*

$$L_{B_1}(x_1 \oplus x_2 \oplus \ldots \oplus x_n) = 4n - 4,$$
$$4n - 4 \leqslant L_{B_1}(x_1 \oplus x_2 \oplus \ldots \oplus x_n \oplus 1) \leqslant 4n - 3.$$

Нижние оценки получаются методом забивания переменных на входах схем булевыми константами с предварительным использованием, быть может, эквивалентных преобразований схем. Верхняя и нижняя оценки для сложности реализации функции $x_1 \oplus x_2 \oplus \ldots \oplus x_n \oplus 1$ различаются (на единицу!); вопрос о том, какую их этих оценок можно улучшить остается открытым.

М. Н. Сибельдина рассматривала задачу построения минимальных схем для линейных функций в базисе $B_2 = \{\overline{x}\,\&\,y, \overline{x}\}$ и получила следующие результаты [9].

Теорема 2. *При любом натуральном четном n*

$$L_{B_2}(x_1 \oplus x_2 \oplus \ldots \oplus x_n \oplus 1) = 4n - 4,$$
$$4n - 4 \leqslant L_{B_2}(x_1 \oplus x_2 \oplus \ldots \oplus x_n) \leqslant 4n - 3,$$

а при нечетном n

$$L_{B_2}(x_1 \oplus x_2 \oplus \ldots \oplus x_n) = 4n - 4,$$
$$4n - 4 \leqslant L_{B_2}(x_1 \oplus x_2 \oplus \ldots \oplus x_n \oplus 1) \leqslant 4n - 3.$$

Нижние оценки получаются (как и в работе [8]) методом забивания переменных константами с возможным использованием эквивалентных преобразований схем. «Асимметрия» полученных результатов для базисов B_1 и B_2 объясняется тем, что функция $x \oplus y$ реализуется в базисе B_1 со сложностью 4, а в базисе B_2 — со сложностью 5.

Замечание. *Ранее в* [5] *установлено: при любом* $\delta \in \{0,1\}$

$$L_{\{x\,\&\,y,\,x\vee y,\,\overline{x}\}}(x_1 \oplus x_2 \oplus \ldots \oplus x_n \oplus \delta) = 4n-4,$$
$$L_{\{x\,\&\,y,\,\overline{x}\}}(x_1 \oplus x_2 \oplus \ldots \oplus x_n \oplus \delta) =$$
$$= L_{\{x\vee y,\,\overline{x}\}}(x_1 \oplus x_2 \oplus \ldots \oplus x_n \oplus \delta) = 7n-7,$$

В работе [10] *доказано, что*

$$L_{\{x/y\}}(x_1 \oplus x_2 \oplus \ldots \oplus x_n) = 4n-4.$$

Г. А. Кочергина получила ряд новых результатов [11] по сложности реализации элементарных конъюнкций $\mathrm{К}^n_{\tilde{\sigma}} = x_1^{\sigma_1}\ldots x_n^{\sigma_n}$ и элементарных дизъюнкций $\mathrm{Д}^n_{\tilde{\sigma}} = x_1^{\sigma_1} \vee \ldots \vee x_n^{\sigma_n}$ схемами из функциональных элементов в базисах $B^{\vee}_{kl} = \{x_1 \vee \ldots \vee x_k \vee \overline{x}_{k+1} \vee \ldots \vee \overline{x}_{k+l}, \overline{x}\}$, $k+l \geqslant 2$, и в некоторых других полных базисах.

Заметим, что Е. П. Сопруненко [12] и Е. С. Горелик [13] изучали ранее сложность реализации конъюнкций и дизъюнкций схемами в базисе $B^{\vee}_{02} = \{x/y\}$. Сопруненко установила, что

$$L_{\{x/y\}}\left(\mathrm{К}^n_{\tilde{1}}\right) = 2n-2 \quad \text{и} \quad L_{\{x/y\}}\left(\mathrm{Д}^n_{\tilde{1}}\right) = 3n-3;$$

Горелик нашел более простое доказательство этих соотношений и обобщил их на элементарные конъюнкции и дизъюнкции произвольного вида:

$$L_{\{x/y\}}\left(\mathrm{К}^n_{\tilde{\sigma}}\right) = 3n-2-\|\tilde{\sigma}\| \quad \text{и} \quad L_{\{x/y\}}\left(\mathrm{Д}^n_{\tilde{\sigma}}\right) = 2n-3+\|\tilde{\sigma}\|,$$

где $\|\tilde{\sigma}\| = \sum\limits_{i=1}^{n} \sigma_i$.

В работе Кочергиной обобщены результаты Сопруненко и Горелика. Найдены точные значения сложности реализации $\mathrm{К}^n_{\tilde{\sigma}}$ и $\mathrm{Д}^n_{\tilde{\sigma}}$ схемами над произвольным базисом $B^{\vee}_{kl}\left(B^{\&}_{kl}\right)$, при этом в частном случае $k=0$, $l=2$ даны новые доказательства упомянутых фактов, установленных Сопруненко и Гореликом. Предложен некоторый подход к нахождению сложности реализации $\mathrm{К}^n_{\tilde{\sigma}}$ и $\mathrm{Д}^n_{\tilde{\sigma}}$ в произвольном полном базисе, составленном из элементов множества $\{x_1 \vee \ldots \vee x_k \vee \overline{x}_{k+1} \vee \ldots \vee \overline{x}_{k+l},\ x_1\,\&\ldots\&\,x_k\,\&\,\overline{x}_{k+1}\,\&\ldots\&\,\overline{x}_{k+l} : k+l \geqslant 2\} \cup \{\overline{x}\}$. Затем этот подход обобщен на более широкий класс базисов, при этом верхняя и нижняя оценки сложности отличаются не более чем на величину, равную сложности реализации констант в рассматриваемом базисе. Приведем некоторые результаты из [11].

Теорема 3. *При $n \geqslant 2$, $k \geqslant 2$, $l \geqslant 2$ для любой конъюнкции $\mathrm{K}^n_{\tilde{\sigma}}$ справедливы соотношения*

$$L_{B^\vee_{k0}}(\mathrm{K}^n_{\tilde{\sigma}}) = \left\lceil \frac{n-1}{k-1} \right\rceil + \|\tilde{\sigma}\| + 1,$$

$$L_{B^\vee_{0l}}(\mathrm{K}^n_{\tilde{\sigma}}) = n + 2\left\lceil \frac{n-1}{l-1} \right\rceil - \|\tilde{\sigma}\|.$$

Теорема 4. *При $n \geqslant 2$, $k \geqslant 2$, $l \geqslant 2$ для любой дизъюнкции $\mathrm{Д}^n_{\tilde{\sigma}}$ справедливы соотношения*

$$L_{B^\vee_{k0}}(\mathrm{Д}^n_{\tilde{\sigma}}) = \left\lceil \frac{n-1}{k-1} \right\rceil + n - \|\tilde{\sigma}\|,$$

$$L_{B^\vee_{0l}}(\mathrm{Д}^n_{\tilde{\sigma}}) = 2\left\lceil \frac{n-1}{l-1} \right\rceil + \|\tilde{\sigma}\| - 1.$$

Теорема 5. *При $n \geqslant 2$, $l \geqslant 1$ для любой конъюнкции $\mathrm{K}^n_{\tilde{\sigma}}$ справедливо соотношение*

$$L_{B^\vee_{1l}}(\mathrm{K}^n_{\tilde{\sigma}}) = \left\lceil \frac{n-1}{l} \right\rceil + \left|n - 1 - \|\tilde{\sigma}\|\right| + 1.$$

Теорема 6. *При $n \geqslant 2$, $l \geqslant 1$ для любой дизъюнкции $\mathrm{Д}^n_{\tilde{\sigma}}$ справедливо соотношение*

$$L_{B^\vee_{1l}}(\mathrm{Д}^n_{\tilde{\sigma}}) = \left\lceil \frac{n-1}{l} \right\rceil + \left|\|\tilde{\sigma}\| - 1\right| + 1.$$

Далее, найдены значения $L_{B^\vee_{kl}}(\mathrm{K}^n_{\tilde{\sigma}})$ и $L_{B^\vee_{kl}}(\mathrm{Д}^n_{\tilde{\sigma}})$ при $n \geqslant 2$, $k \geqslant 2$, $l \geqslant 1$, т. е. при более общих предположениях относительно рассматриваемых базисов (соответствующие формулы достаточно громоздки и поэтому здесь не воспроизводятся). Представленный в [11] подход оказалось возможным применить при нахождении минимальных схем для $\mathrm{K}^n_{\tilde{\sigma}}$ и $\mathrm{Д}^n_{\tilde{\sigma}}$ над базисами $\left\{x^\alpha y^\beta, x^\gamma \vee y^\delta, \overline{x}\right\}$, где $\alpha, \beta, \gamma, \delta \in \{0, 1\}$, а также при нахождении асимптотик для сложности реализации конъюнкции и дизъюнкции схемами над некоторыми другими базисами, составленными из элементарных дизъюнкций и элементарных конъюнкций.

Важными моментами в работе [11] являются, во-первых, выделение так называемых «правильных» схем, которые имеют естественную, «правильную» структуру и обладают рядом полезных свойств,

позволяющих обосновывать нужные нижние оценки сложности рассматриваемых схем, и, во-вторых, обоснование возможности эквивалентных преобразований произвольных минимальных схем (над рассматриваемыми базисами) для конъюнкций и дизъюнкций в правильные.

В работе автора [14] рассматривалась задача оценки сложности реализации булевых функций из класса $F_{n,k}$, состоящего из всех тех функций от n переменных, каждая из которых обращается в единицу ровно на k наборах значений переменных.

Пусть $f(x_1,\ldots,x_n)$ — произвольная булева функция из $F_{n,k}$, обращающаяся в единицу на наборах $\tilde{\sigma}_1,\ldots,\tilde{\sigma}_k$, где $\tilde{\sigma}_i = (\sigma_{i,1},\ldots,\sigma_{i,n})$, $i=1,\ldots,k$. Функции f сопоставим $(k\times n)$-матрицу M_f, строками которой являются наборы $\tilde{\sigma}_1,\ldots,\tilde{\sigma}_k$; j-й столбец данной матрицы отвечает переменной x_j, $j=1,\ldots,n$. Столбцы матрицы M_f разобьем на группы одинаковых между собой столбцов. Для произвольного набора $\tilde{\tau}$ длины (а точнее, высоты) k через $M_{\tilde{\tau}}$ обозначим подматрицу матрицы M_f, составленную из всех столбцов матрицы M_f, равных $\tilde{\tau}$; для каких-то $\tilde{\tau}$ подматрицы $M_{\tilde{\tau}}$ могут оказаться пустыми. Непустую подматрицу $M_{\tilde{\tau}}$ будем считать сильной, если она содержит не менее двух столбцов $\tilde{\tau}$ и в этих столбцах имеются как нули, так и единицы; переменные, отвечающие столбцам из сильной подматрицы, также будем считать сильными. Все остальные подматрицы и переменные, не относящиеся к сильным, будем считать слабыми.

Пусть $B = P_2^{(2)}\backslash\{x_1\oplus x_2, x_1\oplus x_2\oplus 1\}$, где $P_2^{(2)}$ — все 16 булевых функций от переменных x_1, x_2; символ log означает логарифм по основанию 2.

Теорема 7. *Пусть у булевой функции $f(x_1,\ldots,x_n)$ из класса F_{n,k_n} имеется m_n сильных переменных, а для параметра k_n выполняется условие*

$$1 \leqslant k_n \leqslant \log n - c\log\log n,$$

где c — произвольная константа, бóльшая единицы. Тогда

$$L_B(f) \sim n + m_n.$$

При доказательстве последней теоремы верхняя оценка получается с использованием метода Финикова [6] или, точнее, некоторой простой модификации этого метода. Нижняя оценка получается в [14] методом забивания переменных константами с использованием эквивалентных преобразований рассматриваемых схем. Эти преобразования переводят (при необходимости) всякую схему, реализующую функцию f из F_{n,k_n}, в другую схему, в которой каждая силь-

ная переменная подается на входы не менее чем двух элементов; последнее свойство получающихся схем позволяет доказать требуемую нижнюю оценку. Полученные оценки показали, что для некоторых конечных базисов метод Финикова является асимптотически оптимальным при небольших k. Принципиальное явление, обнаруженное в данном случае, заключается в том, что при небольших значениях k, скажем, при $k \leqslant \log n - c \log\log n$, где c — любая бóльшая единицы константа, метод Финикова (или незначительная почти очевидная модификация этого метода) позволяет строить асимптотически минимальные схемы для всех булевых функций из $F_{n,k}$.

При получении нижних оценок для схем над базисом $B = P_2^{(2)} \setminus \{x_1 \oplus x_2, x_1 \oplus x_2 \oplus 1\}$ установлена

Теорема 8. *Если булева функция f имеет n существенных переменных и m из них являются сильными, то любая схема над B, построенная из элементов с одним и с двумя входами и реализующая f, содержит не менее $n + m - 1$ элементов с двумя входами.*

Этой оценки в некоторых случаях может оказаться достаточно даже для доказательства минимальности рассматриваемых схем. Нетрудно установить, например, что минимальная схема над B для функции $f(x_1, \ldots, x_n) = (x_1^{\sigma_1} \ldots x_m^{\sigma_m} \vee x_1^{\overline{\sigma}_1} \ldots x_m^{\overline{\sigma}_m}) \,\&\, x_{m+1}^{\sigma_{m+1}} \ldots x_n^{\sigma_n}$ содержит $n + m - 1$ элементов, а минимальная схема над базисом $\{x \,\&\, y,\ x \vee y, \overline{x}\}$ для функции $f(x_1, \ldots, x_n) = (x_1 \ldots x_m \vee \overline{x}_1 \ldots \overline{x}_m) \,\&\, x_{m+1} \ldots x_n$ содержит $n + m$ элементов.

В заключение приведем открытую проблему, решение которой (точное, асимптотическое или хотя бы даже приближенное — «по порядку») было бы, на наш взгляд, существенным продвижением в изучении сложности индивидуальных булевых функций. Требуется указать конкретную последовательность $F = \{f_n\}$, где f_n — булева функция, существенно зависящая от n переменных, $n = 1, 2, \ldots$, и эффективный («неперебóрный») метод синтеза схем для функций из F такие, что для любого полного конечного базиса B данный метод позволяет строить для функций из F либо минимальные схемы (точное решение), либо асимптотически минимальные схемы (асимптотически оптимальное решение), либо минимальные по порядку схемы (приближенное решение). В последнем случае (приближенное решение) требуется указать две абсолютные константы c_1 и c_2, определяемые последовательностью F и не зависящие от базиса B, для которых выполняется соотношение

$$c_1 L_B(f_n) \leqslant L_B(S_n) \leqslant c_2 L_B(f_n),$$

где $L_B(S_n)$ — сложность построения указанным методом схемы S_n

для функции f_n, $n = 1, 2, \ldots$

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 05-01-00994) и Программы поддержки ведущих научных школ РФ (проект НШ-5400.2006.1).

Список литературы

1. Шеннон К. Работы по теории информации и кибернетике. — М.: ИЛ, 1963.

2. Лупанов О. Б. Об одном методе синтеза схем // Известия Вузов. Сер. Радиофизика. — 1958. — Т. 1, № 1. — С. 120–140.

3. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. Вып. 14. — М.: Наука, 1965. — С. 31–110.

4. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

5. Редькин Н. П. Доказательство минимальности некоторых схем из функциональных элементов // Проблемы кибернетики. Вып. 23. — М.: Наука, 1970. — С. 83–101.

6. Фиников Б. И. Об одном семействе классов функций алгебры логики и их реализации в классе П-схем // Докл. АН СССР. — 1957. — Т. 115, № 2. — С. 247–248.

7. Гринчук М. И. О монотонной сложности пороговых функций // Методы дискретного анализа в теории графов и сложности. Вып. 52. — Новосибирск, Ин-т математики СО РАН, 1992. — С. 41–48.

8. Шкребела И. С. О сложности реализации линейных булевых функций схемами из функциональных элементов в базисе $\{x \to y, \overline{x}\}$ // Дискретная математика. —2003. — Т. 1, № 4 — С. 101–112.

9. Сибельдина М. Н. О сложности реализации линейных булевых функций схемами из функциональных элементов // Дипломная работа. — М.: Механико-математический факультет МГУ, 2005.

10. Редькин Н. П. О минимальной реализации линейной функции схемой из функциональных элементов // Кибернетика. — 1971, № 6. — С. 31–38.

11. Кочергина Г. А. О сложности реализации элементарных конъюнкций и дизъюнкций схемами в некоторых полных базисах // Математические вопросы кибернетики. Вып. 11. — М.: Физматлит, 2002. — С. 219–246.

12. Сопруненко Е. П. О минимальной реализации некоторых функций схемами из функциональных элементов // Проблемы кибернетики. Вып. 15. — М.: Наука, 1965. — С. 117–134.

13. Горелик Е. С. О сложности реализации элементарных конъюнкций и дизъюнкций в базисе $\{x/y\}$ // Проблемы кибернетики.

Вып. 26. — М.: Наука, 1973. — С. 117–134.

14. Редькин Н. П. О сложности булевых функций с данным числом единиц // Дискретная математика. — 2004. — Т. 3, № 4. — С. 20–31.

ФОРМУЛА ВКЛЮЧЕНИЯ-ИСКЛЮЧЕНИЯ И ОЦЕНКИ ДЛЯ ВЕРОЯТНОСТИ ОБЪЕДИНЕНИЯ СОБЫТИЙ

А. М. Зубков (Москва)

В классической постановке принцип включения-исключения формулируется следующим образом (см. [1]). Пусть V — множество из $|V|$ различных элементов, каждый из которых может обладать свойствами $A_1, \ldots, A_n$, пусть V_i — совокупность элементов, обладающих свойством A_i, $i = 1, \ldots, r$, и $V^* = V \setminus \bigcup_{i=1}^{r} V_i$ — множество элементов $v \in V$, не обладающих ни одним из этих свойств. Тогда

$$|V^*| = |V| + \sum_{k=1}^{r} (-1)^k \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant r} |V_{i_1} \cap V_{i_2} \cap \ldots \cap V_{i_k}|.$$

В более общей вероятностной интерпретации множества $V_1, \ldots, V_r \subset V$ рассматриваются как события, и тогда

$$\mathbf{P}\{V^*\} = 1 + \sum_{k=1}^{r} (-1)^k S_k, \;\; S_k = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant r} \mathbf{P}\{V_{i_1} \cap V_{i_2} \cap \ldots \cap V_{i_k}\}.$$

Частичные суммы $\Sigma_m = \sum_{k=1}^{m} (-1)^{k-1} S_k$, $m = 1, \ldots, r$, образуют обвертывающую последовательность; неравенства

$$1 + \sum_{k=1}^{2m+1} (-1)^k S_k \leqslant \mathbf{P}\{V^*\} \leqslant 1 + \sum_{k=1}^{2m} (-1)^k S_k, \quad 1 \leqslant m \leqslant \tfrac{r}{2}\,, \qquad (1)$$

принято называть неравенствами Бонферрони.

Если ξ есть случайная величина, которая в каждой точке $v \in V$ равна числу событий, содержащих точку v, то событие V^* совпадает с событием $\xi = 0$ и $\mathbf{P}\{\xi = 0\} = f_\xi(0)$, где $f_\xi(z) = \mathbf{M} z^\xi$ — производящая функция распределения ξ. Если $x^{[k]} = x(x-1)\ldots(x-k+1)$, то $S_k = \frac{1}{k!}\,\mathbf{M}\xi^{[k]} = \frac{1}{k!}\,f_\xi^{(k)}(1)$ при любом $k = 1, 2, \ldots$

Неравенства, получающиеся после замены S_k в (1) на $\frac{1}{k!}\,f_\xi^{(k)}(1)$:

$$1+\sum_{k=1}^{2m+1}(-1)^k\frac{f_\xi^{(k)}(1)}{k!}\leqslant\mathbf{P}\{\xi=0\}=f_\xi(0)\leqslant 1+\sum_{k=1}^{2m}(-1)^k\frac{f_\xi^{(k)}(1)}{k!},\quad(2)$$

легко следуют из разложения $f_\xi(z)$ на отрезке $[0,1]$ по формуле Тейлора в точке $z=1$ с остаточным членом в форме Лагранжа.

Во многих задачах факториальные моменты $\mathbf{M}\xi^{[k]}$ (и суммы S_k) быстро растут с ростом k, и в неравенствах (1) и (2) при начальных значениях m левые части оказываются отрицательными, а правые превышают 1. Для исправления этого недостатка в ряде статей предлагались различные уточнения неравенств Бонферрони; обычно они сводились либо к добавлению к левым и правым частям дополнительных слагаемых, либо к замене сумм S_k другими аналогичными выражениями. Подробный обзор большого числа подобных неравенств можно найти в книге [2].

В [3] изучались границы точности оценок для мощности объединения r множеств в терминах мощностей пересечений не более k множеств. Доказано, что для любых наборов конечных множеств $A_1,\ldots,A_r$ и $B_1,\ldots,B_r$, удовлетворяющих условиям

$$\left|\bigcap_{i\in S}A_i\right|=\left|\bigcap_{i\in S}B_i\right|\quad\text{для всех}\quad S\subset\{1,\ldots,r\},\ |S|\leqslant k,$$

то при $r\to\infty$

$$\frac{|\cup_{i\in S}A_i|}{|\cup_{i\in S}B_i|}=\begin{cases}1+O(\exp\{-\frac{2k}{\sqrt{r}}\}), & \frac{k}{\sqrt{r}}\to\infty,\\ O\left(\frac{r}{k^2}\right), & k=O(\sqrt{r}),\end{cases}$$

и, главное, — что последняя оценка неулучшаема по порядку.

Задачу уточнения неравенств Бонферрони (2) можно рассматривать как задачу поиска экстремальных значений $\mathbf{P}\{\xi>0\}$ при условии, что фиксировано несколько первых моментов ξ. Она сводится к задаче линейного программирования на симплексе вероятностных распределений на множестве $\{0,1,\ldots\}$. Ее решение, полученное в [4], имеет рецептурный характер: указаны условия, определяющие грань политопа, на которой достигается экстремум.

Небольшое изменение постановки экстремальной задачи позволяет найти решение в явном виде. Вместо случайных величин, принимающих значения в $\{0,1,2,\ldots\}$, рассмотрим более широкое множество случайных величин ξ, принимающих значения в $\{0\}\cup[1,\infty)$,

и будем искать экстремальные по этому множеству значения $\mathbf{P}\{\xi \geqslant 1\} = 1 - \mathbf{P}\{\xi = 0\}$ при фиксированных значениях нескольких первых степенных моментов $\mathbf{M}\xi^k = m_k$, $k = 1, 2, \ldots$

Положим $D(a_0, a_1, \ldots, a_{2r}) = \det\|a_{i+j}\|_{i,j=0}^{r}$.

Теорема [5]. *Если* $\mathbf{P}\{\xi \geq 0\} = 1$, $\mathbf{M}\xi^j = m_j < \infty$, $j = 1, \ldots, 2r$, *то при* $D(m_2, m_3, \ldots, m_{2r}) \neq 0$

$$\mathbf{P}\{\xi > 0\} \geqslant -\frac{D(0, m_1, m_2, \ldots, m_{2r})}{D(m_2, \ldots, m_{2r})} \geq 0. \tag{3}$$

Если, кроме того, $\mathbf{M}\xi^{2r+1} = m_{2r+1} < \infty$, $\mathbf{P}\{0 < \xi < 1\} = 0$ *и* $\Delta m_j = m_j - m_{j-1}$, *то при* $D(\Delta m_3, \ldots, \Delta m_{2r+1}) \neq 0$

$$\mathbf{P}\{\xi \geqslant 1\} \leqslant m_1 + \frac{D(0, \Delta m_2, \ldots, \Delta m_{2r+1})}{D(\Delta m_3, \ldots, \Delta m_{2r+1})}. \tag{4}$$

Короткое доказательство этой теоремы использует свойства положительно определенных квадратичных форм.

Неравенства (3), (4) неулучшаемы в следующем смысле: если $m_1, m_2, \ldots$ являются моментами какой-нибудь случайной величины со значениями в $\{0\} \cup [1, \infty)$, то существуют случайные величины со значениями в том же множестве, которые имеют такие же моменты и для которых (3), (4) превращаются в равенства. Исключение составляют случаи, когда правая часть (4) больше 1: тогда существуют случайные величины с такими же моментами, удовлетворяющие условию $\mathbf{P}\{\xi \geqslant 1\} = 1$ (см. [6]).

Список литературы

1. Холл М. Комбинаторика. — М.: Мир, 1970.

2. Galambos J., Simonelli I. Bonferroni-type inequalities with applications. — Berlin e.a.: Springer-Verlag, 1996.

3. Linial N., Nisan N. Approximate inclusion-exclusion // Combinatorica. — 1990. — V. 10. — P. 349–365.

4. Kwerel S. M. Most stringent bounds on the probability of the union and intersection of m events for system partially specified by $S_1, S_2, \ldots, S_k$, $2 \leqslant k \leqslant m$ // Journal of Applied Probability. — 1975. — V. 12, № 3. — P. 612–619.

5. Зубков А. М. Неравенства для распределения числа одновременно происходящих событий // Обозрение прикладной и промышленной математики. — 1994. — Т. 1, вып. 4. — С. 638–666.

6. Макрушин А. В. Неулучшаемость моментных оценок // Теория вероятностей и ее применения. — 2002. — Т. 47, вып. 1. — С. 159–166.

РАСПРЕДЕЛЕНИЕ ЗНАЧЕНИЙ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В. Н. Чубариков (Москва)

§1. Введение

Натуральные числа $1, 2, 3, 4, 5, 6, 7, \ldots$ составляют предмет арифметики. Операция сложения на множестве этих чисел задает аддитивную структуру абелевой полугруппы и определяет на нем понятие порядка, т. е. отношение больше, равно и меньше. Для сложения одинаковых чисел с целью упрощения записи вводят новую операцию над натуральными числами — операцию умножения. Можно рассматривать эту операцию как самостоятельную, отдельно от сложения. Тогда она задает мультипликативную структуру на множестве натуральных чисел. Если аддитивная структура этого множества достаточна проста: любое число можно получить сложением определенного количества единиц, то мультипликативная структура получается достаточно сложной, поскольку основных "базисных элементов" — простых чисел — имеется бесконечно много. Изучение аддитивной и мультипликативной структур натуральных чисел и их взаимосвязей приводит к теории функций натурального аргумента (в несколько более общем контексте говорят о теории последовательностей или теории теоретико-числовых (арифметических) функций). Сначала скажем о некоторых методах исследования в теории функций натурального аргумента.

А. Формулы суммирования значений теоретико-числовых функций [1–3].

Теорема 1. (Формула Эйлера суммирования значений функции в целых точках.) *Пусть функция $f(t)$ является непрерывно дифференцируемой на отрезке $[a, b]$ и $\rho(x) = 1/2 - \{x\}$, где символ $\{x\}$ обозначает дробную часть числа x. Тогда для любого $x \in [a, b]$ справедлива формула*

$$\sum_{a<n\le x} f(n) - \rho(x)f(x) = \int_a^b f(t)\,dt - \int_a^b \rho(t)f'(t)\,dt - \rho(a)f(a).$$

Теорема 2. (Формула Абеля суммирования по частям значений функции в целых точках.) *Пусть функция $f(t)$ является непрерывно дифференцируемой на отрезке $[a, b]$ и $C(x) = \sum\limits_{a<n\le x} c_n$, где символ $\{c_n\}$ обозначает произвольную последовательность комплекс-*

ных чисел. Тогда для любого $x \in [a,b]$ справедлива формула

$$\sum_{a<n\le x} c_n f(n) - C(x)f(x) = -\int_a^b C(t)f'(t)\,dt.$$

Теорема 3. (Формула Пуассона суммирования значений функции в целых точках.) *Пусть функция $f(t)$ является непрерывно дифференцируемой на отрезке $[a,b]$ и a и b — полуцелые числа. Тогда справедлива формула*

$$\sum_{a<n\le b} f(n) = \lim_{N\to+\infty} \sum_{n=-N}^{n=N} \int_a^b f(t)e^{2\pi int}\,dt.$$

Более точно, имеет место формула

$$\sum_{a<n\le b} f(n) = \sum_{n=-N}^{n=N} \int_a^b f(t)e^{2\pi int}\,dt + R_N,$$

где

$$R_N \le \frac{8M\ln N}{N}, \quad M = \max_{x\in[a,b]} |f'(x)|.$$

Б. Метод включения-исключения. Методы решета в теории чисел [4–6]. Пусть задано конечное множество S и конечное семейство свойств $\alpha_1,\dots,\alpha_n$. Обозначим через $N(i_1,\dots,i_r)$ количество элементов из S, обладающих всеми свойствами α_i с индексами $i_1,\dots,i_r$; через N — количество элементов из S, для которых $(i_1,\dots,i_r)$ — пустое множество; через $N_{j_1,\dots,j_s}$ — количество элементов из S, не имеющих ни одного из свойств α_j с индексами $j_1,\dots,j_s$; наконец, пусть $M(i_1,\dots,i_r)$ обозначает количество элементов из S, которые не обладают хотя бы одним из свойств α_i с индексами $i_1,\dots,i_r$.

Формула включения исключения-исключения является фундаментальным соотношением теории решета. Она имеет вид

$$N_{1,\dots,n} = \sum_{s=0}^{n} (-1)^s \sum_{(i_1,\dots,i_s)} N(i_1,\dots,i_s).$$

В основе решета В. Бруна [5] лежат неравенства Бонферрони. Их можно представить в следующем виде

$$N_{1,\dots,n} = \sum_{s=0}^{k-1}(-1)^s \sum_{(i_1,\dots,i_s)} N(i_1,\dots,i_s) + O\left(\sum_{(i_1,\dots,i_k)} N(i_1,\dots,i_k)\right),$$

где $k \le n$.

Приведем еще одну полезную формулу, лежащую в основе простого асимптотического решета. При $r < n$ имеем

$$N_{1,\dots,n} = N_{1,\dots,r} + O(M(r+1,\dots,n)).$$

Это соотношение обычно применяют, когда величины $N(i)$ малы при $i > r$.

В 1947 г. А. Сельберг [6] предложил новый мощный метод получения верхних оценок величины $N_{1,\dots,n}$. Он состоит в следующем. Каждому элементу $a \in S$ ставится в соответствие выражение $\left(\sum_{(i_1,\dots,i_r)} \lambda_{i_1,\dots,i_r}\right)^2$, где сумма берется по всем подмножествам $(i_1,\dots,i_r)$ множества всех индексов, которые имеет элемент a. Число λ, отвечающее пустому множеству, полагается равным 1, а все остальные значения символа $\lambda_{i_1,\dots,i_r}$ выбираются произвольным образом. Отсюда имеем

$$N_{1,\dots,n} \le \sum_{a\in S}\left(\sum_{(i_1,\dots,i_r)} \lambda_{i_1,\dots,i_r}\right)^2 = \sum_{\substack{(i_1,\dots,i_r)\\(k_1,\dots,k_s)}} N(m_1,\dots,m_t),$$

где набор $(m_1,\dots,m_t)$ является объединением наборов $(i_1,\dots,i_r)$ и $(k_1,\dots,k_s)$. Условный минимум по наборам λ последней квадратичной формы часто позволяет получить достаточно точные оценки.

В. Метод производящих рядов [7]. Метод производящих степенных рядов в основном применяется в аддитивной теории чисел, метод производящих рядов Дирихле — в мультипликативной теории чисел, метод характеристических функций и рядов Фурье является незаменимым инструментом исследования в теории распределения значений функций. Существенным элементом метода производящих рядов являются формулы обращения или более общо, процесс обращения, позволяющий выразить коэффициенты этих рядов через значения самих рядов или значения функций, которые эти ряды

представляют. В случае степенных рядов указанную роль выполняет интеграл Коши, для рядов Дирихле — формулы Перрона и для рядов Фурье — формулы Эйлера — Фурье.

Часто весьма полезными в исследованиях являются абелевы и тауберовы теоремы. Как правило теоремы абелева типа постулируют некоторые свойства коэффициентов ряда и выводят свойства функций, являющейся значением суммы ряда. Обращение подобного рода теорем, т. е. вывод из свойств функций, представляющих производящий ряд, свойства коэффициентов ряда, называют тауберовыми теоремами.

Круговой метод Харди — Литтлвуда — Рамануджана — Виноградова представляет собой весьма важный случай исследования производящих степенных рядов, для которых единичный круг является естественной областью аналитичности, т. е. не существует аналитического продолжения производящей функции за пределы этого единичного круга. Впервые этот метод найден Харди и Рамануджаном [8] для исследования функции количества разбиений натурального числа на натуральные слагаемые. Весьма изящные и плодотворные применения данного метода в форме конечных тригонометрических сумм дал И. М. Виноградов [9].

Г. Метод тригонометрических сумм. Многие задачи теории распределения значений функций вещественной переменной сводятся к изучению тригонометрических сумм вида

$$S_t = \sum_{(x_1,\ldots,x_r)\in\Omega} f(x_1,\ldots,x_r) = \sum_{(x_1,\ldots,x_r)\in\Omega} e^{2\pi i t F(x_1,\ldots,x_r)},$$

где наборы $(x_1,\ldots,x_r)$ пробегают значения из дискретного множества Ω, t — вещественный параметр и $F(x_1,\ldots,x_r)$ — вещественнозначная функция. Постановка задачи распределения значений функций с помощью тригонометрических сумм принадлежит И. М. Виноградову [9]. Он писал: “Из весьма разнообразных более частных видов этой в столь общей формулировке поставленной проблемы (проблемы распределения значений функций), получаемых при тех или иных ограничениях, налагаемых как на функцию $f(x_1,\ldots,x_r)$, так и на совокупность Ω, мы выделим три достаточно большие и весьма важные для теории чисел проблемы...

1. Весьма важной является проблема распределения значений показательной функции

$$f(x_1,\ldots,x_r) = e^{2\pi i F(x_1,\ldots,x_r)},$$

где $F(x_1, \ldots, x_r)$ — вещественная функция; наиболее существенным в этой проблеме является установление верхней границы модуля суммы

$$S = \sum_{\Omega} f(x_1, \ldots, x_r) = \sum_{\Omega} e^{2\pi i F(x_1, \ldots, x_r)}$$

всех значений $f(x_1, \ldots, x_r)$ в том случае, когда число T точек совокупности Ω конечно.

2. С рассмотренной проблемой 1 самым тесным образом связана проблема распределения значений дробной части

$$f(x_1, \ldots, x_r) = \{F(x_1, \ldots, x_r)\}$$

вещественной функции $F(x_1, \ldots, x_r)$.

3. Особый интерес представляют законы распределения значений функции $f(x_1, \ldots, x_r)$, принимающей для точек $(x_1, \ldots, x_r)$ совокупности Ω целочисленные значения. Здесь в отношении каждого данного целого N возникает вопрос: для скольких точек совокупности Ω это N будет служить значением функции $f(x_1, \ldots, x_r)$; иными словами: каково будет число $I(N)$ решений неопределенного уравнения

$$f(x_1, \ldots, x_r) = N. \tag{1}$$

В некоторых случаях здесь речь идет только об установлении неравенства $I(N) > 0$, показывающего, что уравнение (1) разрешимо; в других случаях оказывается возможным установить для $I(N)$ асимптотическую формулу; наконец иногда вопрос сводится о разыскании точного выражения для $I(N)$, и т. д."

Следует отметить, что вообще говоря, сформулированные И. М. Виноградовым проблемы 1–3 представляют интерес в том случае, когда $f(x_1, \ldots, x_r)$ и область Ω несут в себе те или иные арифметические свойства. Выбирая соответствующим образом функцию $f(x_1, \ldots, x_r)$ и область Ω, мы приходим к таким классическим задачам, как проблемы Гольдбаха, Варинга, Гольдбаха — Варинга, Гильберта — Камке, оценки сумм Г. Вейля и т. д.

Д. "Плотностные" методы [10]. Пусть A — подмножество множества неотрицательных целых чисел. Символом $A(n)$ обозначим количество натуральных чисел множества A, не превосходящих n. Тогда плотностью по Шнирельману множества A называется неотрицательное число

$$\sigma(A) = \inf_n \frac{A(n)}{n}.$$

Справедливы следующие простые свойства плотности по Шнирельману:

1. Для любого натурального числа n имеем $A(n) \geq n\sigma(A)$.

2. Величина $\sigma(A) = 1$ тогда и только тогда, когда A совпадает с множеством всех неотрицательных целых чисел.

3. Если $1 \notin A$, то $\sigma(a) = 0$.

Л. Г. Шнирельман [10] доказал следующие утверждения. Пусть $0, 1 \in A$. Тогда:

α) $\sigma(A + B) \geq \sigma(A) + \sigma(B) - \sigma(A)\sigma(B)$.

β) Если $\sigma(A) + \sigma(B) \geq 1$, то $A + B$ совпадает с множеством всех неотрицательных целых чисел.

γ) Пусть P — множество, состоящее из всех простых чисел, 0 и 1. Тогда $\sigma(P + P) > 0$.

Н. П. Романов [11] получил следующий результат.

δ) $\sigma(P + A) > 0$, где $A = \{a^m\}, m = 1, \ldots,$ и a — фиксированное натуральное число.

Г. Б. Манн [12] доказал следующую фундаментальную теорему о плотности суммы двух множеств.

ε) $\sigma(A + B) \geq \min(1, \sigma(A) + \sigma(B))$.

§2. Простые числа

Ограничимся несколькими замечаниями о простых числах. Бесконечность множества простых чисел доказал Евклид. Расходимость ряда $\sum\limits_p \frac{1}{p}$ установил Л. Эйлер. Теоремы об оценках снизу и сверху для количества простых чисел, не превосходящих любой наперед заданной границы, доказал П. Л. Чебышёв. Он же получил, что при любом $x \geq 2$ на отрезке $[x, 2x]$ есть простое число. Два простых числа называются простыми близнецами, если разность между ними равна 2. Нерешенная пока проблема состоит в том, что простых близнецов бесконечно много. Джин-рун Чен доказал, что существует бесконечно много пар (p, q), для котрых $p - q = 2$, причем p — простое и число q имеет не более двух простых делителей.

Символом $\psi(x)$ обозначим функцию Чебышёва

$$\psi(x) = \sum_{n \leq x} \Lambda(n), \quad \Lambda(n) = \begin{cases} \ln p, & n = p^m, \\ 0, & n \neq p^m. \end{cases}$$

Следствием гипотезы Римана является утверждение

$$\psi(x) - x = O(x^{1/2} \ln x).$$

Е. Шмидт (1903) установил по существу неулучшаемость приведенной выше оценки:

$$\psi(x) - x = \Omega_{\pm}(x^{1/2}).$$

Для функции $\pi(x)$ — количества простых чисел, Д. Е. Литтлвуд (1914) доказал, что

$$\pi(x) - \mathrm{li}(x) = \Omega_{\pm}\left(\frac{x^{1/2}\ln\ln(\ln x)}{\ln x}\right)$$

Первое существенное улучшение теоремы Чебышёва получил Г. Хохайзель. Современный результат здесь таков:

$$p_{n+1} - p_n = O(p_n^{\alpha}), \quad \alpha = \frac{38}{61}.$$

Наилучший результат в противоположном направлении принадлежит Р. А. Ранкину: существует бесконечная последовательность простых чисел p_n таких, что имеет место неравенство

$$p_{n+1} - p_n > c\ln p_n \frac{\ln\ln p_n \ln\ln\ln\ln p_n}{(\ln\ln\ln p_n)^2}.$$

Весьма интересными являются результаты о простых числах в редких последовательностях (например, теорема А. Мильуоло о количестве простых чисел в последовательности $p2^p-1$, $p \le x, x \to \infty$).

§3. Мультипликативные функции

Комплекснозначная функция $f(n)$ натурального аргумента n называется теоретико-числовой (или арифметической). Если для любых взаимно простых чисел m и n справедливо равенство

$$f(m)f(n) = f(mn), \tag{2}$$

то функция $f(n)$ называется мультипликативной (м.ф.). Если же равенство (2) выполняется всегда, то функция называется вполне мультипликативной.

Например, м.ф. является функция $\tau(n)$ — количество делителей числа n. Для любого натурального числа n имеем $\tau(n) \ge 2$. С другой стороны, справедливо предельное соотношение

$$\overline{\lim_{n\to\infty}} \frac{\ln\tau(n)\ln\ln n}{\ln n} = \ln 2.$$

Кроме того, для среднего значения функции $\tau(n)$ при $x \to \infty$ имеем

$$\frac{1}{x}\sum_{n\le x}\tau(n) \sim \ln x + 2\gamma - 1,$$

где $\gamma = 0,577215664901532\ldots$ — постоянная Эйлера.

Функция $\sigma(n)$ — сумма всех делителей числа n, также является м.ф. Имеем

$$\sigma(n) \ge n+1, \quad \overline{\lim_{n\to\infty}}\frac{\sigma(n)}{n\ln\ln n} = e^{\gamma}, \quad \frac{1}{x}\sum_{n\le x}\sigma(n) \sim \frac{\pi^2}{12}x.$$

Функция Эйлера $\varphi(n)$, представляющая собой количество натуральных чисел, взаимно простых с n и не превосходящих n, является м.ф. Она имеет вид

$$\varphi(n) = \prod_{p|n}\left(1-\frac{1}{p}\right).$$

Кроме того, справедливы соотношения

$$\varphi(n) \le n-1, \quad \underline{\lim_{n\to\infty}}\frac{\varphi(n)\ln\ln n}{n} = e^{-\gamma}, \quad \frac{1}{x}\sum_{n\le x}\varphi(x) \sim \frac{3}{\pi^2}x.$$

§4. Аддитивные функции

Арифметическая функция $f(n)$ называется аддитивной (а.ф.), если для любых взаимно простых чисел m и n выполняется равенство

$$f(m)+f(n) = f(mn). \tag{3}$$

Если равенство (3) выполняется всегда, то функция $f(n)$ называется вполне аддитивной.

Функция $\omega(n)$ — количество различных простых делителей числа n, является а.ф. Имеем

$$\omega(n) \ge 1, \quad \overline{\lim_{n\to\infty}}\frac{\omega(n)\ln\ln n}{\ln n} = 1, \quad \frac{1}{x}\sum_{n\le x}\omega(x) \sim \ln\ln x.$$

Более того, в 1917 г. Г. Харди и С. Рамануджан доказали, что для любой положительной неограниченно возрастающей при $n\to\infty$ функции $\psi(n)$ частота

$$\nu_n\{m \le n : |\omega(m) - \ln\ln n| \le \psi(n)\sqrt{\ln\ln n}\}$$

стремится к единице при $n \to \infty$. Тем самым для функции $\omega(n)$ справедлив "закон больших чисел".

Далее, для любого фиксированного натурального числа k имеем

$$\nu_n\{m \le n : \omega(m) = k\} \sim \frac{(\ln\ln n)^{k-1}}{(k-1)!\ln n}.$$

Это показывает, что функция $\omega(n)$ распределена приблизительно по закону Пуассона с параметром $\ln\ln n$.

Кроме того, для функции $\omega(n)$ имеет место "центральная предельная теорема". Для любого фиксированного x при $n \to \infty$ справедливо предельное соотношение

$$\nu_n\left\{m \le n : \frac{\omega(m) - \ln\ln n}{\sqrt{\ln\ln n}} < x\right\} \to G(x) = \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{x} e^{-u^2/2}\, du.$$

В 1947 г. В. Левек получил "центральную предельную теорему" для распределения значений разностей $\omega(m) - \omega(m+1)$. Он нашел, что при фиксированном значении x и при $n \to \infty$ имеет место соотношение

$$\nu_n\left\{m \le n : \frac{\omega(m) - \omega(m+1)}{\sqrt{2\ln\ln n}} < x\right\} \to G(x).$$

Список литературы

1. Виноградов И. М. Основы теории чисел. — М.: Наука, 1981.

2. Карацуба А. А. Основы аналитической теории чисел. — М.: Наука, 1983.

3. Архипов Г. И., Садовничий В. А., Чубариков В. Н. Лекции по математическому анализу. — М.: Дрофа, 2005.

4. Хооли К. Применения методов решета в теории чисел. — М.: Наука, 1983.

5. Brun V. Le crible d'Eratosthene et le theoreme de Goldbach. — Videnskaps-selskapets Skrifter, Mat. naturv. klasse, Kristiania, 1920, № 3.

6. Selberg A. On an elementary method in the theory of primes // Det Kongelige Norske Videnskabers Selskab Forhandlinger. — 1947. — V. 19, № 18. — P. 64–67.

7. Постников А. Г. Введение в аналитическую теорию чисел. — М.: Наука, 1971.

8. Hardy G. H., Ramanujan S. Asymptotic formulae in combinatory analysis // Proc. London Math. Soc. (2). — 1918. — V. 17. — P. 75–115.

9. Виноградов И. М. Метод тригонометрических сумм в теории чисел // Труды МИАН СССР. — 1947. — Т. XXIII. — С. 109.

10. Шнирельман Л. Г. Об аддитивных свойствах чисел // Изв. Донского политехн. ин-та. — 1930. — Т. 14, № 2–3. — С. 3–28.

11. Romanoff N. P. Über einige Satze der additiven Zahlentheorie // Math. Ann. — 1934. — V. 109. — P. 668–678.

12. Mann H. B. A proof of the fundamental theorem on the density of sums of sets of positive integers // Ann. of Math. (2). — 1942. — V. 43. — P. 67–78.

13. Гашков С. Б., Чубариков В. Н. Арифметика. Алгоритмы. Сложность вычислений. — М.: Дрофа, 2005.

ОБ ИССЛЕДОВАНИИ МИНОРОВ МАТРИЦЫ ПРИ ПОМОЩИ ЕЁ СИНГУЛЯРНОГО МНОГОЧЛЕНА

В. Н. Шевченко (Нижний Новгород)

Обозначим $(p \times q)$-матрицу, каждый элемент которой равен 1, через $\mathbf{1}^{p\times q}$, нулевой вектор (подходящей размерности) через $\mathbf{0}$, единичную матрицу n-го порядка — через E_n.

Для исследования миноров m-го порядка целочисленной $(m \times n)$-матрицы A $(m \le n)$ используется формула Бине — Коши (см., например, [1]), утверждающая, в частности, что $\det AA^\top = s_m(A)$ есть сумма квадратов всех миноров m-го порядка матрицы A (где $A^\top$ — матрица, транспонированная к A). Если $s_m(A)$ удаётся вычислить (или хотя бы оценить), то этот приём позволяет оценить величину $\sigma_m(A) = s_m(A) \,/\, \binom{n}{m}$ — среднее значение квадрата минора матрицы A. Например, в [2] это сделано для матрицы $B_{n,k}$, столбцами которой являются всевозможные векторы, содержащие k единиц и $n-k$ нулей, и некоторых других матриц, а в [3] для матриц T_{ks} многоиндексных транспортных задач (МТЗ).

Использование характеристического многочлена матрицы $AA^\top$

$$\det(\lambda E_m - AA^\top) = \sum_{i=0}^{m} (-1)^i s_i(A) \lambda^{m-i}, \tag{1}$$

предложенное в [4], позволяет распространить этот подход на миноры $\det A(I,J)$ i-го порядка для любого $i \le r$, где $|I| = |J| = i$, а

r — ранг матрицы A, так как $s_i(A) = \sum \det^2 A(I,J)$, где суммирование идёт по всем i-элементным подмножествам $I \subseteq \{1,\ldots,m\}$ и $J \subseteq \{1,\ldots,n\}$, а $A(I,J)$ — подматрица матрицы A, номера строк которой принадлежат подмножеству $I \subseteq \{1,\ldots,m\}$, а номера столбцов — подмножеству $J \subseteq \{1,\ldots,n\}$.

Из курса линейной алгебры известна

Теорема. *Если* $\det(\lambda E_m - AA^\top) = \prod_{i=1}^{l}(\lambda - \lambda_i)^{m_i}$, *где* $\lambda_{i_1} \neq \lambda_{i_2}$ *при* $i_1 \neq i_2$, *и* $L_i = \{x | AA^\top x = \lambda_i x\}$, *то линейное пространство* $\mathbf{R}^m$ *является ортогональной суммой* m_i*-мерных подпространств* L_i $(i = 1,\ldots,l)$:

$$\mathbf{R}^m = L_1 \oplus \ldots \oplus L_l.$$

Если ранг матрицы A равен r, то

$$\det(\lambda E_m - AA^\top) = \lambda^{m-r} \sum_{i=0}^{r} (-1)^i s_i(A) \lambda^{r-i}.$$

В этом случае многочлен $\varphi(\lambda, A) = \sum_{i=0}^{r}(-1)^i s_i(A)\lambda^{r-i}$ назовем сингулярным многочленом матрицы A, а его корни — сингулярными числами. Как отмечалось в [4], сингулярные многочлены матриц A и $A^\top$ совпадают, чем удалось воспользоваться при исследовании МТЗ.

Если сингулярный многочлен матрицы A известен, то можно получить существенную дополнительную информацию о минорах матрицы A. В противном случае можно воспользоваться теоремой Куранта — Фишера [1] для получения соответствующих неравенств.

Для иллюстрации рассмотрим $A = B_{n,k}$. Исправляя опечатки в [2], заметим, что матрица $B_{n,k}B_{n,k}^\top$ имеет на главной диагонали число $\binom{n-1}{k-1}$, а остальные ее элементы равны $\binom{n-2}{k-2}$. Тогда

$$s_n(B_{n,k}) = k\binom{n-1}{k-1}\binom{n-2}{k-1}^{n-1}.$$

Так как число миноров n-го порядка в матрице $B_{n,k}$ не превосходит $\binom{n}{k}^n / n!$, то

$$\sigma_n(B_{n,k}) \geq k\binom{n-1}{k-1}\binom{n-2}{k-1}^{n-1} n! / \binom{n}{k}^n,$$

откуда следует, что

$$\sigma_{2d-1}(B_{2d-1,d}) \geq (2d)!/4^d.$$

Положим $\mathbb{A}_d = \{0,1\}^{d\times d}$ и поставим вопрос о поведении величины $\Delta_d = \max\{|\det A|, A \in \mathbb{A}_d\}$ при изменении d.

Следствие 1. *Справедливы неравенства*

$$cd^{1/4}(d/e)^d < \sqrt{\sigma_{2d-1}(B_{2d-1,d})} \leq \Delta_{2d-1} \leq 2d^{\ d},$$

где $c = (8e^2/5)^{1/4}$.

Здесь верхняя оценка — известное (см., напр., [5]) следствие из неравенства Адамара для матриц с неотрицательными элементами, а нижняя — уточнение соответствующего неравенства [2, 6].

В частности, в [4] (см. также [7]) вычислены многочлены (1) для МТЗ с различными параметрами, что позволило получить ряд результатов о росте квадратов миноров матрицы МТЗ [7, 8].

Дальнейшее распространение предлагаемого подхода связано с таким окаймлением матрицы A, при котором сингулярный многочлен окаймленной матрицы можно вычислить. Один из способов это сделать основан на следующем результате.

Следствие 2. *Если* $AA^\top g = \alpha g$, $aA^\top g = 0$, $B = \left(\frac{a}{A}\right)$, $C = \left(\frac{1}{\boldsymbol{0}}\middle|\frac{a}{A}\right)$, *то* $(0|g^\top)BB^\top = \alpha(0|g^\top)$, $(0|g^\top)CC^\top = \alpha(0|g^\top)$.

Пример. При $A = B_{n,k}$ и $a = \mathbf{1}^{1\times\binom{n}{k}}$

$$\varphi(\lambda, A) = \left[\lambda - \binom{n-2}{k-1}\right]^{n-1} \cdot \left[\lambda - k\binom{n-1}{k-1}\right],$$

$$\varphi(\lambda, B) = \left[\lambda - \binom{n}{k} - \binom{n-1}{k-1} - (n-1)\binom{n-2}{k-2}\right] \cdot \left[\lambda - \binom{n-2}{k-1}\right]^{n-1},$$

$$\det(\lambda E_{n+1} - BB^\top) = \lambda\varphi(\lambda, B),$$

$$\varphi(\lambda, C) = \det(\lambda E_{n+1} - CC^\top) =$$

$$= \left[\lambda - \binom{n-2}{k-1}\right]^{n-1} \cdot \left[\lambda^2 - \left[\binom{n}{k} + k\binom{n-1}{k-1} + 1\right]\lambda + k\binom{n-1}{k-1}\right].$$

Работа выполнена при частичной финансовой поддержке РФФИ, код проекта 05-01-00552-а.

Список литературы

1. Воеводин В. В., Кузнецов Ю. А. СМБ. Матрицы и вычисления. — М.: Наука, 1984.

2. Шевченко В. Н. Качественные вопросы целочисленного программирования. — М.: Наука, 1995.

3. Ильичёв А. П. Исследование многогранников многоиндексных транспортных задач: Автореферат дис.... канд. физ.-мат. наук. — Горький, 1988.

4. Шевченко В. Н. Характеристические многочлены многоиндексных транспортных задач // Дискретная математика. — 2003. — Т. 15, вып. 2. — С. 83–88.

5. Мишина А. П., Проскуряков И. В. Высшая алгебра. Линейная алгебра, многочлены, общая алгебра. — М.: Наука, 1965.

6. Шевченко В. Н., Чумаков В. В. О некоторых количественных характеристиках целочисленных матриц // Вестник ННГУ им. Н. И. Лобачевского. — 2005. — С. 209–215.

7. Шевченко В. Н. Многогранники многоиндексных транспортных задач: алгебраический подход // Материалы конференции "Дискретный анализ и исследование операций" (28 июня – 2 июля 2004). — Новосибирск: Изд-во ИМ СО РАН, 2004. — С. 64–70.

8. Титова Е. Б., Шевченко В. Н. Среднее значение квадрата минора матрицы ограничений аксиальной транспортной задачи // Автоматика и телемеханика. —2004. — № 2. — С. 113–117.

ЗАДАЧА ДЕЛЬСАРТА ДЛЯ РАЗЛОЖЕНИЙ ПО МНОГОЧЛЕНАМ ЧЕБЫШЕВА

В. И. Иванов (Тула)

При решении многих задач дискретной геометрии по экстремальному расположению точек в сильно однородном пространстве большую роль играют экстремальные задачи теории функций. Одной из таких задач является задача Дельсарта.

Пусть $\alpha \geq -1/2$, $\{P_n^{(\alpha,\alpha)}(t)\}$ — ортогональная система ультрасферических многочленов Якоби на отрезке $[-1,1]$ с весом $(1-t^2)^\alpha$ и условием $P_n^{(\alpha,\alpha)}(1)=1$, $-1 \leq s < 1$, $K_D(s,\alpha)$ — класс непрерывных функций $f(t)=\sum_{k=0}^{\infty} \hat{f}_k P_k^{\alpha,\alpha}(t)$, для которых

1) $\hat{f}_k \geq 0$, $k=0,1,\ldots$,

2) $f(1)=\sum_{k=0}^{\infty} \hat{f}_k = 1$,

3) $f(t) \le 0,\ -1 \le t \le s$.

Задача Дельсарта для разложений по многочленам Якоби состоит в вычислении величины

$$A_D(s,\alpha) = \sup\left\{\hat{f}_0 : f \in K_D(s,\alpha)\right\}. \tag{1}$$

Обычно в задаче Дельсарта ищут величину $1/A_D(s,\alpha)$, равную $\inf 1/\hat{f}_0$ или $\inf f(1)/\hat{f}_0$.

Задача Дельсарта (1) позволяет при $\alpha = \frac{n-3}{2}$, $n \in \mathbb{N}$, $n \ge 2$, оценивать сверху максимальную мощность сферических кодов и контактного числа сферы S^{n-1}, плотность упаковки пространства $\mathbb{R}^n$.

Решению задачи (1) или нахождению функций (многочленов) из класса $K_D(s,\alpha)$ с большим нулевым коэффициентом посвящено много работ. Отметим работы Г. А. Кабатянского, В. И. Левенштейна, В. М. Сидельникова, В. В. Арестова, А. Г. Бабенко, Н. Н. Андреева, В. А. Юдина, Н. Слоэна, А. М. Одлыжко и многих других авторов. Как правило, точные результаты получались для отдельных значений α и s. Нам удалось решить задачу Дельсарта (1) при $\alpha = -1/2$ для всех s. В этом случае многочлены $P_n^{(-1/2,-1/2)}(t) = \cos(n \arccos t)$ — известные многочлены Чебышева первого рода, и задачу Дельсарта после замены $t = \cos 2\pi x$ удобно рассматривать для четных 1-периодических функций.

Пусть $0 < h \le 1/2$, $K_D(h)$ — класс непрерывных четных 1-периодических положительно определенных функций $f(x)$, для которых

$$f(0) = 1,\ f(x) \le 0\ (h \le |x| \le 1/2).$$

Задача Дельсарта: вычислить величину

$$A_D(h) = \sup\left\{\int_{-1/2}^{1/2} f(x)\,dx : f \in K_D(h)\right\}. \tag{2}$$

Отметим, что для $-1 \le s < 1$

$$A_D(s,-1/2) = A_D\left(\frac{\arccos s}{2\pi}\right).$$

Наряду с задачей Дельсарта рассмотрим и задачу Турана. Пусть $K_T(h)$ — класс непрерывных четных 1-периодических положительно определенных функций $f(x)$, для которых

$$f(0) = 1,\ f(x) = 0\ (h \le |x| \le 1/2).$$

Задача Турана: вычислить величину

$$A_T(h) = \sup\left\{\int_{-h}^{h} f(x)\,dx : f \in K_T(h)\right\}. \tag{3}$$

Очевидно, что $A_T(h) \le A_D(h)$. Задача (3) была поставлена П. Тураном в 1970 году в частной беседе С. Б. Стечкину. Она имеет приложения в аналитической теории чисел, цифровой обработке сигналов. Ею занимались С. Б. Стечкин, А. Ю. Попов, Д. В. Горбачев, А. С. Маношина. В 2004 году автор и Ю. Д. Рудомазина вычислили [1] величины (2), (3) для рациональных чисел h. Оказалось, что для всех рациональных h верно равенство $A_D(h) = A_T(h)$. В 2006 году автору [2] удалось, следуя методу В. С. Балаганского, доказать непрерывность функции $A_D(h)$. Значит, равенство $A_D(h) = A_T(h)$ выполняется для всех h. При вычислении величины (3) для иррациональных h оказалость удобно перейти к эквивалентной задаче для целых функций экспоненциального типа [2].

Пусть $\langle x\rangle$ — расстояние от x до ближайшего целого, $0 < h < 1/2$,

$$S_0(h) = \{\nu \in \mathbb{N} : \langle \nu h\rangle = 0\},\ S_1(h) = \{\nu \in \mathbb{N} : \langle \nu h\rangle \in (0,h)\},$$

$$S_2(h) = \{\nu \in \mathbb{N} : \langle \nu h\rangle \ge h\}$$

— разбиение множества натуральных чисел.

Рассмотрим следующие функции

$$G_h(z) = \Lambda_h \prod_{k\in S_0(h)} \left(1 - \left(\frac{z}{k}\right)^2\right)^2 \prod_{k\in S_1(h)} \left(1 - \left(\frac{z}{k}\right)^2\right),\ \sum_{\nu\in\mathbb{Z}} G_h(\nu) = 1,$$

$$\varphi_h(x) = G_h(0) + 2\sum_{\nu=1}^{\infty} G_h(\nu)\cos 2\pi\nu x.$$

Отметим, что $G_h(z)$ — целая четная функция экспоненциального типа $2\pi h$, для которой $G_h(\nu) \ge 0$ $(\nu \in \mathbb{Z})$, $\varphi_h(x) \in K_T(h)$ и $\varphi_h(x)$ неотрицательна при $|x| \le h$.

Теорема 1. *Для любой функции* $f(x) = \hat{f}_0 + 2\sum_{k=1}^{\infty} \hat{f}_k \cos(2\pi kx)$, $\sum_{k=1}^{\infty} |\hat{f}_k| < \infty$ *справедлива квадратурная формула*

$$G_h(0)f(0) + 2\sum_{k\in S_2(h)} G_h(k) f(\langle kh\rangle) = \hat{f}_0 + 2\sum_{k\in S_0(h)} \hat{f}_k + 2\sum_{k\in S_1(h)} \hat{f}_k \varphi_h(\langle kh\rangle).$$

Теорема 2. *Для всех* $0 < h < 1/2$

$$A_D(\cos 2\pi h, -1/2) = A_D(h) = A_T(h) = \Lambda_h = G_h(0).$$

Оценки сверху величин (2), (3) получаются с помощью квадратурной формулы в теореме 1. Их точность проверяется на функции $\varphi_h(x)$. Экстремальная функция в (3) единственна при иррациональных h и нет при рациональных h.

При $\alpha > -1/2$ задачи Дельсарта и Турана, по-видимому, будут различаться, так как экстремальные функции в задаче Дельсарта в некоторых случаях будут только многочленами.

Работа выполнена при финансовой поддержке РФФИ (проекты №05-01-39005, №06-01-00372).

Список литературы

1. Иванов В. И., Горбачев Д. В., Рудомазина Ю. Д. Некоторые экстремальные задачи для периодических функций с условиями на их значения и коэффициенты Фурье // Труды ИММ УрО РАН. — 2005. — Т. 11. — С. 92–111.

2. Иванов В. И. О задачах Турана и Дельсарта для периодических положительно определенных функций // Математические заметки. — 2006. — Т. 80, № 6. — С. 934–939.

ОБ АСИМПТОТИКАХ ЛОГАРИФМА ЧИСЛА ДИСКРЕТНЫХ ФУНКЦИЙ

В. Б. Алексеев (Москва)

При изучении дискретных функций с заданными свойствами обычно имеется некоторый параметр n (чаще всего — число переменных у функций) такой, что множество F_n функций с фиксированным параметром n конечно. При этом важной является проблема оценки мощности $|F_n|$. В большинстве случаев удается установить лишь асимптотику для $\log_2 |F_n|$. Иногда и верхняя и нижняя асимптотические оценки для $\log_2 |F_n|$ получаются сложно. Такая ситуация была, например, с числом пороговых булевых функций, где основной проблемой оказалась нижняя оценка [1]. Однако обычно несложно построить довольно много функций из F_n, что дает хорошую нижнюю оценку, и основная проблема состоит в получении верхней оценки.

Пусть функции из F_n отображают множество A_n в B_n. Если A_n удается разбить на некоторое количество m групп так, что число вариантов задания функций из F_n на каждой группе не превосходит d, то, очевидно, $|F_n| \leq d^m$ и $\log_2 |F_n| \leq m \log_2 d$. При этом можно задавать функции на группах по порядку и учесть, что задание функции на предыдущих группах дополнительно ограничивает число вариантов на очередной группе. Однако, в большинстве случаев таким приемом d не удается понизить до необходимой величины.

Для решения этой задачи автором был разработан метод искусственных ограничений [2], идеи которого восходят к работе Д. Клейтмена [3], в которой была установлена асимптотика логарифма числа монотонных булевых функций. Идея состоит в том, чтобы, учитывая задание функции на предыдущих группах, вводить искусственные ограничения на очередной группе так, чтобы число вариантов задания функций из F_n на очередной группе не превосходило желаемого d. При этом можно рассматривать некоторое количество p разбиений на группы и некоторое количество q упорядочений. Можно также выбрать параметр t и разрешить, чтобы наше искусственное ограничение нарушалось, но не более, чем на t группах, где число вариантов может вырасти до h. Тогда число функций, которые можно построить при таких ограничениях не будет превосходить $C_m^t d^{m-t} h^t pq$. Если параметры выбраны так, что при этом все функции из F_n будут построены, то

$$\log_2 |F_n| \leq m \log_2 d + \log_2 C_m^t + t \log_2 (h/d) + \log_2 p + \log_2 q.$$

Если при этом

$$\log_2 C_m^t + t \log_2 (h/d) + \log_2 p + \log_2 q = o(m \log_2 d),$$

то $\log_2 |F_n| \leq (1 + o(1)) m \log_2 d$.

Трудность использования данного подхода состоит обычно в подборе параметра t так, чтобы выполнялись указанные соотношения и при этом порождались все функции из F_n. Эта проблема сводится обычно к комбинаторным проблемам оценки сверху мощности произвольного независимого (в некотором смысле) подмножества в A_n. Так, например, при установлении асимптотики логарифма числа монотонных функций в k-значных логиках основной оказалась проблема оценки сверху мощности независимых подмножеств в декартовых степенях заданного частично упорядоченного множества [4].

Многие важные классы в k-значных логиках P_k и частичных k-значных логиках P_k^* определяются как классы $U(R)$ всех функций, сохраняющих некоторый предикат $R(y_1, \ldots, y_h)$ на множестве

$E_k = \{0, 1, \ldots, k-1\}$. Так, например, определяются все предполные классы в P_k и P_k^*. Интересно было бы найти алгоритм, который по заданному предикату R определял бы параметры асимптотики логарифма числа функций от n переменных в $U(R)$. Однако пока этого сделать не удается. Асимптотику логарифма числа функций удалось найти для всех предполных классов в P_k и P_2^*, а также для всех предполных классов в P_k^*, задаваемых двухместными предикатами [4–6].

Даже для двухместных предикатов $R(y_1, y_2)$ задача установления асимптотики логарифма числа функций в $U(R)$ оказывается сложной. Например, в P_3 имеется всего 74 типа двухместных предикатов и для 6 из них пока не удается решить эту задачу.

Ряд новых методов для оценки числа дискретных функций предложил А. А. Вороненко, в частности, метод жирных точек, идея которого состоит в следующем. Пусть H_n — некоторая последовательность множеств и ϕ_n — всюду определенное отображение, действующее из F_n в H_n. Тогда $|F_n| \leq |H_n| \max_{a \in H_n} |\phi_n^{-1}(a)|$ и

$$\log_2 |F_n| \leq \log_2 |H_n| + \log_2 \max_{a \in H_n} |\phi_n^{-1}(a)|.$$

Если при этом оказывается, что $\log_2 |H_n| = o(\log_2 |F_n|)$, то $\log_2 |F_n| \sim \log_2 \max_{a \in H_n} |\phi_n^{-1}(a)|$. Главная проблема в этом методе — подобрать подходящие H_n и ϕ_n. С помощью этого метода А. А. Вороненко, в частности, установил асимптотику логарифма числа функций, сохраняющих заданный предикат, для многих семейств двухместных предикатов в P_k, а также для классов функций, отображающих "близкие" значения аргументов в "близкие" значения функции [7].

Д. В. Ховратович для оценки числа функций применил следующий метод. Каждой функции из F_n ставится в соответствие элемент декартова произведения $G_1 \times G_2 \times \ldots \times G_l$, где G_i — некоторые множества функций, так, что разным функциям соответствуют разные элементы. Тогда $\log_2 |F_n| \leq \log_2 |G_1| + \log_2 |G_2| + \ldots + \log_2 |G_l|$. Этот метод дает хорошие верхние оценки, если одно из слагаемых в правой части асимптотически забивает сумму остальных. Таким методом Д. В. Ховратович установил асимптотику логарифма числа функций для классов, являющихся пересечением класса монотонных функций с другими предполными классами в P_3 [8].

Сведением к дискретным функциям удается получать асимптотику логарифма и для других объектов. Отображение $\phi : S \to S$, где S — частично упорядоченное множество (ч.у.м.), называется замы-

канием, если для любых элементов $a, b \in S$ выполняются условия:

$$1)\ \phi(a) \geq a; \quad 2)\ (a \leq b) \Longrightarrow (\phi(a) \leq \phi(b)); \quad 3)\ \phi(\phi(a)) = \phi(a).$$

С помощью метода искусственных ограничений удается получить асимптотику логарифма числа замыканий как на семействе всех подмножеств n-элементного множества [9], так и на декартовых степенях произвольного ч.у.м. [10]. В ряде работ А. А. Вороненко установил асимптотику логарифма числа отображений на декартовых степенях ч.у.м., удовлетворяющих произвольному подмножеству из указанных 3 условий (см. [7]).

Задача о замыканиях на семействе всех подмножеств n-элементного множества эквивалентна задаче о семействах подмножеств n-элементного множества, замкнутых относительно пересечений. Для числа $\alpha(n)$ таких семейств подмножеств n-элементного множества в [9] получено асимптотическое равенство $\log_2 \alpha(n) \sim C_n^{\lfloor n/2 \rfloor}$.

Ниже мы рассмотрим, как изменяется число семейств подмножеств, замкнутых относительно пересечений, если ослабить требования на замкнутость. Пусть $A \triangle B$ обозначает симметрическую разность двух множеств.

Определение. Пусть p — натуральное число. Тогда через $\alpha_p(n)$ будем обозначать количество семейств N подмножеств n-элементного множества, удовлетворяющих условию:

$$\text{если} \quad A \in N, B \in N \quad \text{и} \quad |A \triangle B| \leq p, \quad \text{то} \quad A \cap B \in N, \qquad (1)$$

а через $\beta_p(n)$ — количество семейств, удовлетворяющих условию:

$$\text{если} \quad A \in N, B \in N \quad \text{и} \quad |A \triangle B| = p, \quad \text{то} \quad A \cap B \in N. \qquad (2)$$

Очевидно, что $\alpha_1(n) = \beta_1(n) = 2^{2^n}$. Также нетрудно видеть, что $\alpha_2(n) = \beta_2(n)$ и $\alpha_p(n) \geq \alpha_q(n)$ при $p \leq q$.

Утверждение 1. *Пусть $\psi(n)$ — число монотонных булевых функций от n переменных. Тогда для любого p выполняются неравенства $\alpha_p(n) \geq \psi(n)$ и $\beta_p(n) \geq \psi(n)$.*

Доказательство. Для произвольной монотонной булевой функции множество наборов, на которых она равна 0, удовлетворяет условиям (1) и (2), если рассматривать наборы как подмножества n-элементного множества. Отсюда и вытекает утверждение 1.

Теорема 1. *Если $p = p(n) \geq 2$ для всех n, то при $n \to \infty$ выполняется асимптотическое равенство*

$$\log_2 \alpha_p(n) \sim C_n^{\lfloor n/2 \rfloor}.$$

Доказательство. Нижняя оценка вытекает из утверждения 1. Для доказательства верхней оценки достаточно рассмотреть $\alpha_2(n)$, поскольку $\alpha_p(n) \le \alpha_2(n)$ при всех $p \ge 2$. Характеристическими функциями семейств подмножеств, удовлетворяющих условию (1) при $p = 2$, будут булевы функции, удовлетворяющие условию: если функция равна 1 на двух наборах, непосредственно больших набора $\tilde{\gamma}$, то и $f(\tilde{\gamma}) = 1$. Для множества G_2 таких функций в [9, теорема 2] получена верхняя оценка

$$\log_2 |G_2| = C_n^{\lfloor n/2 \rfloor}(1 + O(n^{-1/4} \log_2 n)).$$

Отсюда и вытекает утверждение теоремы 1.

Рассмотрим теперь количество $\beta_p(n)$ семейств N подмножеств n-элементного множества, удовлетворяющих условию (2). Оказывается, что эта величина существенно зависит от четности p.

Теорема 2. *Если $p = 2k$ — любое фиксированное четное натуральное число, то при $n \to \infty$ выполняется асимптотическое равенство*

$$\log_2 \beta_p(n) \sim kC_n^{\lfloor n/2 \rfloor}.$$

Доказательство. 1°. Нижняя оценка. Пусть Q — семейство всех подмножеств n-элементного множества мощности от $\lfloor n/2 \rfloor$ до $\lfloor n/2 \rfloor + k - 1$ включительно. Так как $k = const$, то $|Q| \sim kC_n^{\lfloor n/2 \rfloor}$. Пусть в семейство N входят все подмножества n-элементного множества мощности строго меньше, чем $\lfloor n/2 \rfloor$, и не входят все подмножества мощности строго больше, чем $\lfloor n/2 \rfloor + k - 1$. Легко видеть, что каждое такое семейство удовлетворяет (2). Таким образом, $\beta_p(n) \ge 2^Q$, и получаем нижнюю оценку.

2°. Верхняя оценка. Обозначим через $\gamma_p(n)$ количество семейств N подмножеств n-элементного множества, удовлетворяющих условию:

$$\text{если} \quad A, B \in N, |A| = |B|, |A \triangle B| = p, \quad \text{то} \quad A \cap B \in N. \qquad (3)$$

Так как условие (3) слабее, чем (2), то $\beta_p(n) \le \gamma_p(n)$. Поэтому верхнюю оценку достаточно получить для $\gamma_p(n)$. Пусть Q_r^k — семейство всех подмножеств A n-элементного множества таких, что $|A| \equiv r \pmod{k}$. Если $p = 2k$, то условие (3) связывает между собой только подмножества из одного Q_r^k. Поэтому если $\gamma_{p,r}(n)$ — число семейств подмножеств в Q_r^k, удовлетворяющих (3), то $\gamma_{2k}(n) = \prod_{r=0}^{k-1} \gamma_{2k,r}(n)$.

Верхняя оценка в теореме следует теперь из оценки $\log_2 \gamma_{2k,r}(n) \sim C_n^{\lfloor n/2 \rfloor}$, которую удается доказать с использованием варианта метода искусственных ограничений [2], обобщающего конструкцию из [9].

Теорема 3. *Если $p = 2k - 1$ — любое фиксированное нечетное натуральное число, то $\log_2 \beta_p(n) \geq 2^{n-1}$ и $\beta_p(n)/2^{2^{n-1}} \to \infty$ при $n \to \infty$.*

Доказательство. Если семейство N содержит только подмножества четной мощности, то оно тривиально удовлетворяет (2) при $p = 2k - 1$. Отсюда следует первая часть теоремы. Для доказательства второй части достаточно рассмотреть все семейства подмножеств, содержащие пустое подмножество, произвольные подмножества четной мощности и произвольные подмножества мощности 1.

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проекты 06-01-00438 и 07-01-00154).

Список литературы

1. Зуев Ю. А. Пороговые функции и пороговые представления булевых функций // Математические вопросы кибернетики, вып. 5. — М.: Физматлит, 1994. — С. 5–62.

2. Алексеев В. Б. Метод искусственных ограничений для оценки числа дискретных функций // Математические вопросы кибернетики, вып. 8. — М.: Наука, 1999. — С. 123–134.

3. Клейтмен Д. О проблеме Дедекинда: число монотонных булевых функций // Кибернетический сборник. Новая серия, вып. 7. — М.: Мир, 1970. — С. 43–52.

4. Алексеев В. Б. О числе монотонных k-значных функций // Проблемы кибернетики, вып. 28. — М.: Наука, 1974. — С. 5–24.

5. Алексеев В. Б. О числе функций в классах, задаваемых центральными предикатами // Математические заметки. — 1985. — Т. 38, вып. 1. — С. 148–156.

6. Алексеев В. Б. О числе функций в некоторых замкнутых классах частичной k-значной логики // Дискретная математика. — 1989. — Т. 1, вып. 1. — С. 32–42.

7. Вороненко А. А. Оценки количества дискретных функций. Учебное пособие по спецкурсу. — М.: Издательский отдел факультета ВМиК МГУ им. М. В. Ломоносова, 2006.

8. Ховратович Д. В. О мощности некоторых подклассов монотонных функций // Дискретная математика. — 2005. — Т. 17, вып. 4. — С. 81–97.

9. Алексеев В. Б. О числе семейств подмножеств, замкнутых относительно пересечения // Дискретная математика. — 1989. — Т. 1,

вып. 2. — С. 129–136.
10. Алексеев В. Б. О числе отображений типа замыкания // Дискретная математика. — 2004. — Т. 16, вып. 2. — С. 85–97.

ТЕОРЕМЫ МИНКОВСКОГО О ВЫПУКЛЫХ МНОГОГРАННИКАХ И ПАРАЛЛЕЛОЭДРАХ

Н. П. Долбилин (Москва)

Обсуждаются новые результаты в классической проблематике, заложенной Е. С. Федоровым, Г. Минковским, Г. Ф. Вороным.

Пусть $P \subset \mathbf{E}^d$ — компактный выпуклый d-многогранник с k гипергранями ($(d-1)$-гранями). Семейство $\mathcal{F} = \{\mathbf{F}_1, \mathbf{F}_2, \ldots, \mathbf{F}_k\}$ векторов, перпендикулярных к гиперграням, направленных вовне многранника и по длине равным $(d-1)$-объемам гиперграней, назовем *ежом многогранника* P. Нетрудно показать, что:

1) аффинная оболочка ежа есть все пространство: $\mathrm{aff}(\mathcal{P}) = \mathbf{E}^d$;

2) $\sum_{i=1}^{k} \mathbf{F}_i = 0$.

Теорема 1 (Минковский [1]). *Пусть семейство векторов $\mathcal{F}$ удовлетворяет условиям* (1) *и* (2). *Тогда существует выпуклый многогранник P, для которого $\mathcal{F}$ является ежом. Более того, многогранник P определяется ежом однозначно с точностью до параллельного переноса.*

При доказательстве существования используется принцип множителей Лагранжа. Вопрос о единственности опирается на неравенство Брунна — Минковского. Теорема Минковского имеет много приложений; нам понадобятся два из них.

Предложение 1 (А. Д. Александров, Дж. Шефард). *Выпуклый многогранник, все гиперграни которого центрально симметричны, центрально симметричен.*

Предложение 2. *Выпуклый многогранник, являющийся объединением попарно неперекрывающихся центрально симметричных многогранников, также центрально симметричен.*

Прежде всего заметим, что полная информация о еже является избыточной. В действительности, нам нет необходимости знать направления и объемы (или площади, если $d = 3$) всех k гиперграней, где $k \geq d+1$. Достаточно знать направления и объемы $k-d$ гиперграней, а для остальных d гиперграней достаточно знать их направления.

Предложение 3. *Пусть заданы* $k-d$ *векторов* $\mathbf{F}_1, \ldots \mathbf{F}_{k-d}$ *с ненулевой суммой* $\mathbf{F}$ *и* d *линейно независимых осей* $l_1, \ldots, l_d$, *таких что* $\mathbf{F}$ *не лежит ни в каком координатном подпространстве, натянутом на* l_j. *Тогда существует единственный выпуклый многогранник* P *с* k *гипергранями, причем*:

1) *указанные* $k-d$ *векторов* $\mathbf{F}_i$ *входят в еж многогранника* P;

2) *остальные* d *гиперграней перпендикулярны направлениям* l_j.

Действительно, разложим сумму $\mathbf{F} = \sum_{i=1}^{k-d} \mathbf{F}_i$ по d заданным направлениям: $\mathbf{F} = \sum_{j=1}^{d} \mathbf{G}_j$. В силу предположения, все $\mathbf{G}_j$ ненулевые. Совокупность векторов $\{\mathbf{F}_1, \ldots, \mathbf{F}_{k-d}, -\mathbf{G}_1, \ldots, -\mathbf{G}_d\}$ удовлетворяет условиям (1) и (2) теоремы Минковского и, следовательно, является ежом единственного выпуклого многогранника.

Параллелоэдр определяется как выпуклый d-мерный многогранник, *нормально* (т. е. грань-в-грань) разбивающий евклидово пространство $\mathbf{E}^d$ параллельными копиями. Понятие и термин *параллелоэдр* были введены Е. С. Федоровым.

Теорема 2 (Минковский). *Пусть* P — d*-мерный параллелоэдр. Тогда*:

1) P *центрально симметричен*;

2) *все гиперграни многогранника* P *центрально симметричны*;

3) *проекция* P *вдоль любой его* $(d-2)$*-грани на дополнительную* 2*-плоскость есть либо параллелограмм, либо центрально симметричный шестиугольник.*

В доказательстве теоремы 2 решающим является доказательство п. 1. Действительно, так как разбиение нормально, то каждая гиперграни параллелоэдра имеет равную и параллельную гиперграни. Поэтому в еже параллелоэдра наряду с вектором $\mathbf{F}$ содержится противоположный вектор $-\mathbf{F}$. Таким образом, еж параллелоэдра центрально симметричен. В силу теоремы 1 многогранник P также центрально симметричен.

Теорема 2 особенно важна потому, что свойства 1–3 параллелоэдра являются характеристическими:

Теорема 3 (Венков, [2–4]). *Выпуклый многогранник со свойствами* 1–3 *из теоремы* 2 *является параллелоэдром.*

Теорема 3 легко выводится также из более общей *теоремы о продолжении* [5, 6].

Теорема 4 (Минковский). *Число* f_{d-1} *гиперграней у* d*-параллелоэдра* P *не превышает* $2(2^d-1)$, *причем существует параллелоэдр* P *с* $f_{d-1} = 2(2^d-1)$.

В этой статье показывается, что обе теоремы верны также и для "ненормальных" параллелоэдров, т. е. для выпуклых многогранни-

ков, разбивающих пространство параллельными копиями без требования "грань-в-грань" (теорема 5). Уточняется п. 2 теоремы 2 и усиливается теорема 4 (теорема 6).

Теорема 5. *Если P — выпуклый многогранник, который разбивает (не обязательно нормально) пространство $\mathbf{E}^d$ параллельными копиями, то для него выполняются свойства*:

1) *P центрально симметричен*;

2) *все гиперграни многогранника P центрально симметричны*;

3) *проекция P вдоль любой его $(d-2)$-грани на дополнительную 2-плоскость есть либо параллелограмм, либо центрально симметричный шестиугольник.*

Из теорем 2, 3 и 5 вытекает

Следствие. *Всякий "ненормальный" параллелоэдр является нормальным.*

Доказательство (теоремы 5). Пусть T — разбиение пространства параллельными копиями многогранника P. Каждая гипергрань F разбивается на выпуклые $(d-1)$-многогранники F_i, каждый из которых является пересечением многогранника с теми многогранниками P_i, которые смежны с P по гиперграни F: $F_i = P \cap P_i$. Так как P_i является частью гиперграни многогранника P_i, конгруэнтного и параллельного многограннику P, то в многограннике каждая гипергрань F имеет параллельную гипергрань F'. Решающее обстоятельство: все попарно противоположные гиперграни имеют равные $(d-1)$-объемы. Отсюда следует, что еж, а значит и сам многогранник центрально симметричны.

Предположим, что гиперграни F и F' имеют неравные объемы $s(F)$ и $s(F')$: $\Delta = s(F) - s(F') > 0$. Возьмем совокупность $T' \subset T$ из N параллелоэдров. Гиперграни F_i параллелоэдров из T', конгруэнтные и параллельные гиперграни $F \subset P$, частично покрываются гипергранями F'_j, которые принадлежат смежным параллелоэдрам и конгруэнтны и параллельны гиперграни $F' \subset P$. Пусть S — суммарная площадь частей гиперграней F, не покрытых гипергранями F'_j и, обратно, S' — суммарная площадь частей гиперграней F'_j, не покрытых гипергранями F_i. Очевидно, что $S - S' = N\Delta$. Пусть R — минимальный радиус шара, содержащего параллелоэдр P. Обозначим через B_ρ шар радиуса ρ, через T_ρ минимальную совокупность параллелоэдров Q разбиения T, которые покрывают шар B_ρ, а через T'_ρ совокупность многогранников $Q' \in T \setminus T_\rho$, таких что $Q \cap Q' \neq \emptyset$. В силу определения радиуса R очевидно, что

$$B_\rho \subset \cup_{Q \in T_\rho} Q \subset \cup_{Q \in T_\rho \cup T'_\rho} Q \subset B_{\rho+4R}.$$

Поэтому, если через N_ρ обозначить число параллелоэдров в $T_\rho \cup T'_\rho$, а через N'_ρ — число параллелоэдров в T'_ρ, то для некоторых положительных $c = c(R,d)$, $C = C(R,d)$, $c_1 = c_1(R,d)$, $C_1 = C_1(R,d)$

$$c\rho^d < N_\rho < C\rho^d, \qquad c_1\rho^{d-1} < N'_\rho < C_1\rho^{d-1}. \tag{2}$$

Если $s - s' = \Delta > 0$, то для суммарной площади непокрытых участков граней, параллельных паре граней F и F', у параллелоэдров из T_ρ верно

$$N_\rho\Delta = O(\rho^d). \tag{3}$$

С другой стороны, в силу определения T'_ρ, эти участки, не покрытые параллелоэдрами из T_ρ, покрываются соответствующими гранями параллелоэдров из T'_ρ. Поэтому

$$N_\rho\Delta < N'_\rho(s + s') = O(\rho^{d-1}). \tag{4}$$

Но (4) невозможно, если верно (3). Противоречие доказывает, что $\Delta = 0$. Итак, пункт 1 теоремы 5 доказан.

Далее, каждая гиперграань F параллелоэдра P распадается в объединение попарно неперекрывающихся $(d-1)$-многогранников $F_j = P \cap P_j$. Каждый F_j, как пересечение двух центрально симметричных многогранников, которые параллельны друг другу, является центрально симметричным. На основании предложения 2 гиперграань F центрально симметрична. Пункт 2 теоремы 5 установлен.

Теперь для каждой $(d-2)$-грани $Q \subset P$ можно построить *пояс* $B(Q)$ следующим образом. Грань Q является смежной для двух гиперграней, скажем F_0 и F_1. В гиперграни F_1 имеется центрально-симметричная для Q $(d-2)$-грань Q_1, которая отделяет гиперграань F_1 от следующей гиперграни, F_2. Применяя к Q_1 симметрию гиперграни F_2, получаем следующую $(d-2)$-грань, и т. д. Получается циклически замкнутая последовательность $(d-2)$-граней $Q, Q_1, Q_2, \ldots, Q_k = Q$. Параллелоэдр P, а также $P_1, \ldots, P_k$, смежные с P по граням пояса, проектируются вдоль грани Q в центрально симметричные, параллельные друг другу многоугольники, которые попарно не перекрываются. Отсюда легко выводится, что этот многоугольник может быть либо параллелограммом, либо центрально симметричным шестиугольником.

Пусть T — нормальное разбиение на параллелоэдры и $P, P' \in T$ — такие параллелоэдры, что $P \cap P' \neq \emptyset$. Пересечение $P \cap P'$ является гранью F^i некоторой размерности i. Грань F^i, являющуюся

пересечением $P \cap P'$ двух параллелоэдров, будем называть *максимальной общей* гранью (м.о.г.) для P и P'. Не всякая грань параллелоэдра является м.о.г. Так, в разбиении плоскости на правильные шестиугольные соты, никакая вершина не является м.о.г., но каждая сторона шестиугольника является м.о.г. В разбиении плоскости на параллелограммы и вершина, и сторона являются м.о.г.

1) У d-мерного параллелепипеда все грани любой размерности — м.о.г.

2) У шестиугольной призмы, все грани и 12 ребер, лежащих в основаниях, — м.о.г. Боковые ребра и все 12 вершин не являются м.о.г.

Примитивный d-параллелоэдр — это параллелоэдр, такой что в каждой вершине соответствующего разбиения сходится минимально возможное число (а именно $d+1$) параллелоэдров. Поэтому каждый параллелоэдр P', имеющий с P непустое пересечение, имеет с P м.о.г. размерности $d-1$. В примитивном параллелоэдре никакая грань размерности меньше $d-1$ не является м.о.г.

Из симметричности параллелоэдра (теорема 2, п. 1) следует

Лемма 1. *Каждая м.о.г. параллелоэдра является центрально симметричной гранью. Более того, центр симметрии м.о.г. является центром симметрии всего разбиения.*

Из леммы 1 следует п. 2 теоремы 2. Множество всех параллелоэдров разбиения, сходящихся в грани F, образует *звезду* $St(F)$ грани F.

Лемма 2. *Если F — м.о.г., то для $P \in St(F)$ существует единственный параллелоэдр $P' \in St(F)$, такой что $F = P \cap P'$.*

Лемма 3. *Если F не является м.о.г. и P, $P' \in St(F)$, то пересечение $P \cap P'$ содержит F как собственную грань.*

Валентностью $n(F)$ грани F параллелоэдра назовем число параллелоэдров в $St(F)$. Из лемм 2 и 3 немедленно следует

Лемма 4. *Валентность $(d-2)$-грани F^{d-2} параллелоэдра либо* 3, *либо* 4. *Равенство $n(F^{d-2}) = 4$ верно тогда и только тогда, когда F^{d-2} — м.о.г.*

Из леммы 4 непосредственно вытекает п. 3 теоремы 2.

Индексом грани F назовем число $\nu(F) := \frac{1}{n(F)}$. Обозначим через $\mathcal{D}$ множество всех м.о.г. в параллелоэдре P.

Теорема 6 [7]. *Для параллелоэдра выполняется*

$$\sum_{F \in \mathcal{D}} \nu(F) = 2^d - 1. \tag{5}$$

Отсюда следует оценка Минковского для f_{d-1}. Так как каждая $(d-1)$-грань F^{d-1} — м.о.г., ее индекс $\nu(F^{d-1}) = 1/2$, то из (5) имеем:

$$2^d - 1 = \sum_{F\in\mathcal{D}} \nu(F) = \sum_{F\in\mathcal{D}_{d-1}} \nu(F) + \sum_{F\in\mathcal{D}'} \nu(F) = \frac{1}{2} f_{d-1} + \sum_{F\in\mathcal{D}'} \nu(F). \quad (6)$$

В (6) $\mathcal{D}_{d-1}$ и $\mathcal{D}'$ обозначают множество гиперграней и множество всех м.о.г. размерностей не более $d-2$, соответственно. Из (6) видно, что $f_{d-1} \leq 2(2^d - 1)$ и число f_{n-1} у непримитивных параллелоэдров уменьшается из-за появления м.о.г. меньших размерностей.

Работа выполнена при поддержке грантов РФФИ 05-01-00170 и 06-01-72551.

Список литературы

1. Minkowski H. Allgemeine Leherzätze über konvexe Polyeder // Nach. Ges. Wiss. Göttingen. —1897. — P. 198–219.

2. Венков Б. А. О некотором классе эвклидовых многогранников // Вестник Ленинградского университета. Сер. матем., физ., хим. — 1954. — Т. 9. — С. 11–31.

3. Александров А. Д. О заполнении пространства многогранниками // Вестник Ленинградского университета. Сер. матем, физ., хим. — 1954. — Т. 9. — С. 33–43.

4. McMullen P. Convex bodies which tile space by translation // Mathematika. — 1980. — V. 27. — С. 113–121.

5. Dolbilin N. P. The extension theorem // Discrete mathematics. — 2000. — V. 221, № 1–3. — С. 43–60.

6. Долбилин Н. П., Макаров В. С. Теорема о продолжении в теории правильных разбиений и ее приложения // Труды МИАН. — 2002. — Т. 239. — С. 136–159.

7. Долбилин Н. П. Теоремы Минковского о параллелоэдрах и их обобщения // Успехи матем. наук. — 2007. — Т. 62, № 4.

О ЧИСЛЕ ПЕРИОДИЧЕСКИХ СТРУКТУР В КОНЕЧНЫХ СЛОВАХ (обзор)

Р. М. Колпаков (Москва)

Данная работа представляет обзор научных результатов, связанных с максимальным возможным числом периодичностей в формальных символьных словах. Наличие периодичностей в словах имеет

фундаментальное значение для комбинаторных свойств этих слов и активно используется в различных алгоритмах, работающих с формальными словами, в частности, в алгоритмах поиска образцов в слове, алгоритмах сжатия слов, алгоритмах анализа биологических последовательностей и т. д. Простейшим примером периодичности является *квадрат*, т. е. подслово вида uu, где u — произвольное непустое слово, которое называется *корнем* данного квадрата. Другими словами, под квадратом понимается подслово, состоящее из двух идущих подряд одинаковых непустых подслов. Подслово вида uuu, где u — произвольное непустое слово, называется *кубом*. В общем случае, для любого целого $n \geq 2$ подслово вида $u^n = \underbrace{uu\ldots u}_{n}$, где u — произвольное непустое слово, называется *n-ой целой степенью* с корнем u. Слово называется *примитивным*, если оно не является целой степенью с меньшим корнем. Длину слова u будем обозначать через $|u|$.

Нетрудно заметить, что максимальное возможное число квадратов содержится в слове, все буквы которого совпадают. В таком слове, очевидно, квадратом является любое подслово четной длины. Поэтому в таком слове содержится $\Theta(n^2)$ квадратов, где n — длина слова, но все эти квадраты являются на самом деле четными целыми степенями с однобуквенным корнем. Чтобы исключить из рассмотрения данный тривиальный случай, можно ввести понятие *примитивного квадрата*, т. е. квадрата с примитивным корнем, и рассматривать в слове только примитивные квадраты. Аналогичным образом вводятся также понятия *примитивного куба* и *примитивной целой степени*.

Максимальное возможное число квадратов в конечных словах изучалось в работах [1, 4]. В частности, в [4] установлен следующий интересный факт.

Лемма (о трех квадратах). *Пусть три примитивных квадрата u_1u_1, u_2u_2 и u_3u_3 такие, что $|u_1| < |u_2| < |u_3|$, являются префиксами одного и того же слова. Тогда $|u_1| + |u_2| \leq |u_3|$.*

Из леммы о трех квадратах непосредственнон вытекает, что с одного и того же символа конечного слова может начинаться не более чем $\log_\varphi n$ примитивных квадратов, где n — длина слова и $\varphi = (1 + \sqrt{5})/2$ — "золотое сечение". Таким образом, общее число содержащихся в слове примитивных квадратов не превосходит $n \log_\varphi n$. С другой стороны, в [1] был приведен пример слов, содержащих $\Theta(n \log n)$ примитивных квадратов. Это широко известные в теории формальных языков слова Фибоначчи над бинарным алфавитом $\{a, b\}$, которые определяются следующим образом: $f_0 = b$,

$f_1 = a$ и $f_k = f_{k-1} f_{k-2}$ для $k \geq 2$. Длина слова f_k обозначается через F_k и является, очевидно, k-м числом Фибоначчи. В [1] показано, что f_k содержит не менее $\frac{1}{6} F_k \log_2 F_k$ примитивных квадратов. Позднее в [6] было установлено, что при $k \geq 3$ в f_k содержится в точности $\frac{4}{5} k F_k - \frac{2}{5}(k+6) F_{k-1} - F_{k-2} + k + 1 = \frac{2(3-\varphi)}{5 \log_2 \varphi} F_k \log_2 F_k + O(F_k) \approx 0.7962 F_k \log_2 F_k + O(F_k)$ примитивных квадратов. Таким образом, если обозначить через $S(n)$ максимальное возможное число примитивных квадратов в словах длины n, на сегодняшний день известно, что $0.7962 n \log_2 n \leq S(n) \leq n \log_\varphi n \approx 1.441 n \log_2 n$.

Как было ранее отмечено, примитивные квадраты являются частным случаем примитивных целых степеней. Примитивная целая степень называется *максимальной*, если она не является частью большей целой степени с тем же примитивным корнем. Другими словами, примитивная целая степень u^n является максимальной, если в слове нет еще одного вхождения примитивного корня u этой степени непосредственно перед ней или непосредственно после нее. Например, слово *abcabcabcababa* содержит пять максмальных целых степеней: *abcabcabc*, *bcabcabca*, *cabcabcab*, *abab* и *baba*. Отметим, что любой примитивный квадрат в слове является частью некоторой максимальной целой степени с тем же примитивным корнем, поэтому, исходя из содержащихся в слове максимальных целых степеней, можно определить в нем все примитивные квадраты. Пусть $M(n)$ — максимальное возможное число максимальных целых степеней в словах длины n. Очевидно, что в любом слове число максимальных целых степеней не превосходит числа примитивных квадратов, поэтому $M(n) \leq S(n) = \Theta(n \log n)$. С другой стороны, известно (см., например, [13]), что слова Фибоначчи не содержат четвертых целых степеней, т. е. в слове f_k частями одной и той же максимальной целой степени могут быть не более двух примитивных квадратов. Следовательно, f_k содержит $\Theta(F_k \log F_k)$ максимальных целых степеней. Таким образом, $M(n) = \Theta(n \log n)$.

Наряду с целыми степенями можно также рассмотреть "дробные" степени. Для этого введем понятие периодичности в общем виде. Напомним, что натуральное число p называется *периодом* слова $w = w_1 \ldots w_n$, если $w_i = w_{i+p}$ для $1 \leq i \leq n - p$. *Порядком* слова называется отношение длины слова к его минимальному периоду. Слово является *периодичностью*, если его порядок не меньше, чем 2. Для периодичностей в слове мы также можем ввести понятие максимальной периодичности: периодичность $w_i \ldots w_j$ с минимальным периодом p является *максимальной* в слове $w = w_1 \ldots w_n$, если $w_{i-1} \neq w_{i-1+p}$ при $i > 1$ и $w_{j+1-p} \neq w_{j+1}$ при $j < n$. Дру-

гими словами, периодичность в слове является максимальной, если она не является частью большей периодичности с тем же минимальным периодом. Например, в слове *abcabcabcababa* содержится только две максимальных периодичности: *abcabcabcab* и *ababa*. Очевидно, что любая периодичность в слове является частью некоторой максимальной периодичности, т. е. максимальные периодичности задают в слове все остальные периодичности любого другого типа: квадраты, кубы, целые степени и т. д., полностью определяя таким образом периодическую структуру слова. В [9] было показано, что слово Фибоначчи содержит линейное относительно длины слова число максимальных периодичностей (позднее в [11] было установлено, что при $k \geq 4$ слово f_k содержит ровно $2F_{k-2}-3$ максимальных периодичностей). Таким образом, возникла гипотеза о том, что в любом слове число максимальных периодичностей линейно ограничено длиной слова. Эта гипотеза была доказана в [12]. Точнее говоря, было установлено, что $R(n) = O(n)$, гле $R(n)$ — максимальное возможное число максимальных периодичностей в слове длины n. Была также высказана основанная на компьютерных экспериментах гипотеза о том, что в действительности $R(n) < n$.

Отметим, что предложенное в [12] доказательство линейности $R(n)$ является достаточно громоздким и не позволяет получить разумной верхней оценки для коэффициента линейного роста $R(n)$. Поэтому дальнейшие исследования в данной области были связаны с упрощением доказательства линейности $R(n)$ и получением конкретных линейных оценок для $R(n)$. Более простое доказательство линейности $R(n)$ было дано в [2]. В [10] был предложен принципиально новый подход для оценки $R(n)$ сверху. Используя этот подход, в [15] доказано, что $R(n) \leq 6.3n$. Данное доказательство было независимо усовершенствовано в работах [14] и [16], в которых получены оценки $R(n) \leq 3.48n$ и $R(n) \leq 3.44n$ соответственно. В [3] предложен еще один метод оценки $R(n)$ сверху, с помощью которого получено $R(n) \leq 1.6n$. Что касается нижних оценок для $R(n)$, в [7] построено бесконечное семейство слов, в которых число максимальных периодичностей асимптотически равно $\frac{3}{2\varphi}n \approx 0.927n$, где n — длина слова, и тем самым показано, что $R(n) \gtrsim \frac{3}{2\varphi}n$. Более того, выдвинута гипотеза, что данные слова являются наиболее богатыми периодичностями, т. е. $R(n) \sim \frac{3}{2\varphi}n$.

Отметим, что, строго говоря, в [12] был установлен более сильный факт, из которого очевидным образом вытекает линейность $R(n)$. Именно, было доказано, что $E(n) = O(n)$, гле $E(n)$ — макси-

мальная возможная сумма порядков всех максимальных периодичностей в слове длины n. Альтернативное доказательство этого факта приведено в [15], однако ни в [12], ни в [15] не было получено конкретных верхних оценок для коэффициента линейного роста $E(n)$. Первая конкретная верхняя оценка $E(n) \leq 5.6n$ представлена в [3]. Исходя из компьтерных экспериментов, предполагается, что $E(n) < 2n$. С другой стороны, в [11] показано, что сумма порядков всех максимальных периодичностей в слове f_k асимптотически не меньше, чем $1.922F_k$, т. е. $E(n) \gtrsim 1.922n$.

Необходимо отметить, что под числом периодичностей в слове понимается число, в котором различные вхождения одной и той же периодичности в слово учитываются по отдельности. Вместе с тем, при подсчете числа периодичностей в слове мы также можем учитывать все вхождения одной и той же периодичности в слово как одно вхождение ровно один раз. В этом случае мы говорим о числе *различных* периодичностей в слове. В [6] установлено, что при $k \geq 5$ число различных квадратов в f_k равно $2F_{k-2} - 2 = 2(2-\varphi)F_k + o(1)$ ($2(2-\varphi) \approx 0.7639$). При этом, поскольку f_k не содержит периодичностей порядка 4, все эти квадраты являются примитивными. Пусть $D(n)$ — максимальное возможное число различных квадратов в слове длины n, и $P(n)$ — максимальное возможное число различных примитивных квадратов в слове длины n. Очевидно, что $P(n) \leq D(n)$. Под *крайне правым* вхождением периодичности в слово будем понимать вхождение, правее которого в слове нет других вхождений той же самой периодичности. Из леммы о трех квадратах вытекает, что если три примитивных квадрата u_1u_1, u_2u_2 и u_3u_3, где $|u_1| < |u_2| < |u_3|$, начинаются в слове с одного и того же символа, то $|u_1| < |u_3|/2$, поэтому в слове существует еще одно вхождение квадрата u_1u_1, находящееся на $|u_3|$ символов правее рассматриваемого квадрата u_1u_1. Таким образом, с одного и того же символа в слове может начинаться не более двух крайне правых вхождений примитивных квадратов в слово, поэтому $P(n) \leq 2n$. В [5] показано, что на самом деле с одного и того же символа в слове может начинаться не более двух крайне правых вхождений не только примитивных, но и любых квадратов, и с помощью этого факта доказано, что $D(n) \leq 2n - 8$ при $n \geq 5$. С другой стороны, в [5] построено бесконечное семейство слов, в которых число различных примитивных квадратов асимптотически не меньше их длины. Верхняя оценка для $D(n)$ была несколько усилена в [8], где получено, что $D(n) \leq 2n - \Theta(\log n)$. Таким образом, к настоящему времени установлено, что $n \lesssim P(n) \leq D(n) \leq 2n - \Theta(\log n)$.

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994) и программы поддержки ведущих научных школ РФ (проект НШ–5400.2006.1).

Список литературы

1. Crochemore M. An optimal algorithm for computing the repetitions in a word // Information Processing Letters. — 1981. — V. 12. — P. 244–250.

2. Crochemore M., Ilie L. A simple proof that the number of runs in a word is linear (manuscript). — 2006. — (To appear.)

3. Crochemore M., Ilie L. Analysis of maximal repetitions in strings // Proceedings of 32nd International Symposium on Mathematical Foundations of Computer Science (MFCS'07). — (To appear.)

4. Crochemore M., Rytter W. Squares, cubes, and time-space efficient string searching // Algorithmica. — 1995. — V. 13. — P. 405–425.

5. Fraenkel A. S., Simpson J. How many squares can a string contain? // Journal of Combinatorial Theory (Ser. A). — 1998. — V. 82. — P. 112–120.

6. Fraenkel A. S., Simpson J. The exact number of squares in Fibonacci words // Theoretical Computer Science. — 1999. — V. 218, № 1. — P. 83–94.

7. Franek F., Simpson R.J., Smyth W. The maximum number of runs in a string // Proceedings of 14th Australasian Workshop on Combinatorial Algorithms. — 2003. — P. 26–35.

8. Ilie L. A note on the number of squares in a word // Theoretical Computer Science. — (To appear.)

9. Iliopoulos C. S., Moore D., Smyth W. A characterization of the squares in a Fibonacci string // Theoretical Computer Science. — 1997. — V. 172. — P. 281–291.

10. Kangmin Fan, Puglisi S. J., Smyth W., Turpin A. A new periodicity lemma // SIAM Journal on Discrete Mathematics. — 2006. — V. 20, № 3. — P. 656–668.

11. Kolpakov R., Kucherov G. On maximal repetitions in words // Lecture Notes in Computer Science. — 1999. — V. 1684. — P. 374–385.

12. Kolpakov R., Kucherov G. On maximal repetitions in words // Journal of Discrete Algorithms. — 2000. — V. 1, № 1. — P. 159–186.

13. Mignosi F., Pirillo G. Repetitions in the Fibonacci infinite word // Theoretical Informatics and Applications. — 1992. — V. 26, № 3. — P. 199–204.

14. Puglisi S. J., Simpson J., Smyth W. How many runs can a string contain? // Theoretical Computer Science. — (To appear.)

15. Rytter W. The number of runs in a string: improved analysis of the linear upper bound // Lecture Notes in Computer Science. — 2006. — V. 3884. — P. 184–195.

16. Rytter W. The number of runs in a string // Information and Computation. — (To appear.)

Секция «Синтез, сложность и надежность управляющих систем»

О НАДЕЖНОСТИ СХЕМ В ШИРОКОМ КЛАССЕ ПОЛНЫХ БАЗИСОВ

С. И. Аксенов (Пенза)

Рассматривается задача реализации булевых функций схемами из ненадежных функциональных элементов в произвольном полном базисе *Б*. Введем необходимые понятия. Предполагается, что все элементы схемы независимо друг от друга с вероятностью ε подвержены *инверсным неисправностям* на выходах элементов, когда функциональный элемент с приписанной ему функцией φ в неисправном состоянии реализует функцию $\bar{\varphi}$. Пусть схема S реализует функцию $f(\tilde{x})$ ($\tilde{x} = (x_1, x_2, \ldots, x_n)$) при отсутствии неисправностей в схеме. Обозначим $P_{\overline{f(\tilde{a})}}(S, \tilde{a})$ — вероятность того, что схема S при $\tilde{x} = \tilde{a}$ выдает значение $\bar{f}(\tilde{a})$. Будем считать, что схема S реализует функцию $f(\tilde{x})$ с *ненадежностью* $P(S)$, если $P(S) = \max\limits_{\tilde{a}} P_{\overline{f(\tilde{a})}}(S, \tilde{a})$, где максимум берется по всем входным наборам $\tilde{a}$. *Надежность* схемы S равна $1 - P(S)$.

Пусть $P_\varepsilon(f) = \inf_S P(S)$, где S — схема из ненадежных элементов, реализующая $f(\tilde{x})$. Схему A, реализующую f, назовем *асимптотически оптимальной* по надежности, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \to 0$.

Впервые эту задачу рассмотрел Дж. фон Нейман [1]. Для произвольной булевой функции он построил асимптотически оптимальные по надежности схемы над базисами, в которых содержится медиана $m(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$.

В этой статье мы рассматриваем полные базисы, которые могут не содержать медиану.

Сформулируем ранее доказанную автором теорему.

Теорема 1 [2]. *Пусть Б — полный в* $\mathbf{P}_2$ *базис, тогда существуют такие константы* ε_0 *и* c, *что при* $\varepsilon \le \varepsilon_0$ *любую булеву функцию* f *можно реализовать схемой* S *из функциональных элементов над Б, для которой* $P(S) \le 5\varepsilon + c\varepsilon^2$.

Из теоремы 1 следует, что над произвольным полным базисом любую булеву функцию можно реализовать схемой, ненадежность

которой асимптотически не более 5ε. Ниже в теореме 2 приведено достаточное условие на базис $Б$, в случае выполнения которого оценку для ненадежности схем можно снизить до 4ε.

Введем множества функций Ψ_i, $i = 1, 2, 3, 4$:

$$\Psi_1 = \{\bar{x}, 0, 1\} \cup \bigcup_{k=1}^{\infty} \left\{ \mathop{\&}_{i=1}^{k} x_i \right\},$$

$$\Psi_2 = \{0, 1\} \cup \bigcup_{k=1}^{\infty} \left\{ \mathop{\&}_{i=1}^{k} x_i \right\} \cup \bigcup_{k=2}^{\infty} \left\{ \bar{x}_1 \cdot \mathop{\&}_{i=2}^{k} x_i \right\},$$

$$\Psi_3 = \Psi_1^*, \quad \Psi_4 = \Psi_2^*,$$

где Ψ_3, Ψ_4 — множества, содержащие функции, двойственные к функциям из множеств Ψ_1, Ψ_2.

Справедлива следующая теорема.

Теорема 2. *Пусть $Б$ — полный в $\mathbf{P}_2$ базис, и пусть при этом $Б$ не является подмножеством ни одного из множеств Ψ_i, $i = 1, 2, 3, 4$, тогда существуют такие константы ε_0 и c, что при $\varepsilon \le \varepsilon_0$ любую функцию f можно реализовать схемой S над $Б$, для которой $P(S) \le 4\varepsilon + c\varepsilon^2$.*

Список литературы

1. Нейман Дж. Вероятностная логика и синтез надежных организмов из ненадежных компонент // Автоматы. — М.: ИЛ, 1956. — С. 68–139.

2. Аксенов С. И. О надежности схем над произвольной полной системой функций при инверсных неисправностях на выходах элементов // Известия высших учебных заведений. Поволжский регион. Естественные науки. — 2005. — № 6. — С. 42–55.

О СЛОЖНОСТИ НАДЕЖНЫХ СХЕМ ПРИ ИНВЕРСНЫХ НЕИСПРАВНОСТЯХ НА ВЫХОДАХ ЭЛЕМЕНТОВ

М. А. Алехина, С. И. Аксенов (Пенза)

Рассматривается реализация булевых функций схемами из ненадежных элементов в произвольном конечном базисе $Б$ =

$\{e_1, e_2, \ldots, e_s\}$. Каждому элементу E_i базиса приписано положительное число $v(E_i)$ — вес данного элемента. *Сложность* схемы S определяется как сумма весов всех входящих в нее элементов и обозначается $L(S)$. Пусть $\rho = \min v(E_i)/(n(E_i) - 1)$, где минимум берется по всем элементам E_i базиса, для которых $n(E_i) > 1$, а $n(E_i)$ — число существенных переменных функции e_i, реализуемой элементом E_i, $i = 1, 2, \ldots, s$.

Предполагается, что все элементы схемы независимо друг от друга с вероятностью ε ($\varepsilon \in (0, 1/2)$) подвержены инверсным неисправностям на выходах элементов, когда функциональный элемент с приписанной ему булевой функцией $e(\tilde{x})$ в неисправном состоянии реализует функцию $\bar{e}(\tilde{x})$). Пусть $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ — вероятность появления значения $\bar{f}(\tilde{a})$ на выходе схемы S, реализующей булеву функцию $f(\tilde{x})$, при входном наборе $\tilde{a}$. *Ненадежность* $P(S)$ схемы S определяется как максимальное из чисел $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ при всевозможных входных наборах $\tilde{a}$ схемы S. *Надежность* схемы S равна $1 - P(S)$.

Инверсные неисправности на выходах элементов исследовались в работах Дж. фон Неймана, С. И. Ортюкова, Д. Улига [1] и некоторых других авторов.

Введем функцию Шеннона $L_{p,\varepsilon}(n) = \max_f \min_S L(S)$, где минимум берется по всем схемам S из ненадежных элементов, реализующим функцию $f(x_1, x_2, \ldots, x_n)$ с ненадежностью $P(S) \le p$, а максимум — по всем булевым функциям f от n переменных.

Обозначим через N_f минимальное число надежных элементов, необходимое для реализации функции f в базисе $Б$.

Теорема 1 [1]. *Для любых $c, b > 0$ существует такое $\varepsilon_1 \in (0, 1/2)$, что при любых $\varepsilon \in (0, \varepsilon_1)$, и $p \ge (1 + c)\varepsilon N_g$ (точнее при любом $p \ge q(\varepsilon)N_g$, где $q(\varepsilon) = \varepsilon + 3\varepsilon^2 + o(\varepsilon^2)$ при $\varepsilon \to 0$, а $g(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$), верно соотношение $L_{p,\varepsilon}(n) \lesssim (1 + b)\rho \cdot 2^n/n$.*

С. И. Ортюков и Д. Улиг для инверсных неисправностей на выходах элементов нашли методы синтеза оптимальных по сложности схем, функционирующих с некоторым уровнем надежности $1 - p$.

Пусть булева функция $m(x_1, x_2, \ldots, x_k)$ существенно зависит от $k \ge 3$ переменных и обладает свойством: найдется такой набор $(b_1, b_2, \ldots, b_k)$, что на нем и всех соседних с ним наборах функция m принимает значение 0, а на наборе $(\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_k)$ и всех соседних с ним наборах — значение 1. Пусть M — множество всех булевых функций с названым свойством [2]. Обозначим $N_Б(M) = \min N_f$, где минимум берется по всем функциям $f \in M$.

С. И. Аксенов [3] доказал, что в произвольном полном базисе

$Б$ существуют константы ε_2 и c_2 такие, что при $\varepsilon \in (0, \varepsilon_2)$ любую булеву функцию можно реализовать схемой S, для которой $P(S) \le \varepsilon N_Б(G) + c_2\varepsilon^2$, где константа $N_Б(G) \le 5$, $N_Б(G) = \min N_h$, здесь минимум берется по всем функциям $h \in G$, $G = \{(x_1^{a_1}x_2^{a_2} \vee x_3^{a_3}x_4^{a_4})^a, x_1^{a_1}x_2^{a_2} \vee x_1^{a_1}x_3^{a_3} \vee x_2^{a_2}x_3^{a_3}\}$, $a, a_i \in \{0,1\}$, $i = 1,2,3,4$.

Очевидно, что $G \subset M$ и $N_Б(G) \ge N_Б(M)$. Ясно также, что в некоторых базисах константу 5 в оценке $N_Б(G)$ можно уменьшить до 1 [2], 2 [4], 3 и 4 [5]. В действительности, приведенный результат С. И. Аксенова можно улучшить, заменив константу $N_Б(G)$ константой $N_Б(M)$, т. е. верна теорема 2.

Теорема 2. *В произвольном полном базисе $Б$ существуют константы ε_2 и c_2 такие, что при $\varepsilon \in (0, \varepsilon_2)$ любую булеву функцию можно реализовать схемой S, для которой $P(S) \le \varepsilon N_Б(M) + c_2\varepsilon^2$.*

Лемма [2]. *Пусть схема S_1 реализует булеву функцию f с ненадежностью $P(S_1)$. Пусть схема A реализует медиану $g(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$ с ненадежностью $P(A)$. Тогда функцию f можно реализовать такой схемой S_2, что $P(S_2) \le P(A) + 3P^2(S_1)$.*

Докажем основной результат этой статьи.

Теорема 3. *Для любого $b > 0$ существуют константы $\varepsilon_3 \in (0, 1/2)$ и d такие, что при любых $\varepsilon \in (0, \varepsilon_3)$, любую булеву функцию $f(x_1, x_2, \ldots, x_n)$ можно реализовать схемой S, для которой $P(S) \le \varepsilon N_Б(M) + d\varepsilon^2$, $L(S) \lesssim 3(1+b)\rho \cdot 2^n/n$.*

Доказательство. Пусть $f(x_1, x_2, \ldots, x_n)$ — произвольная булева функция. Воспользуемся теоремой 1, полагая $c = 1$. Тогда существует ε_1 такое, что при любом $\varepsilon \in (0, \varepsilon_1)$ и $p = 2\varepsilon N_g$ функцию f можно реализовать схемой S_1, для которой $P(S_1) \le 2\varepsilon N_g$ и $L(S_1) \lesssim (1+b)\rho \cdot 2^n/n$. По теореме 2 существуют константы ε_2 и c_2 такие, что при $\varepsilon \in (0, \varepsilon_2)$ медиану $g(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$ можно реализовать схемой A, для которой $P(A) \le \varepsilon N_Б(M) + c_2\varepsilon^2$. Возьмем три экземпляра схемы S_1 и соединим их выходы со входами схемы A. Построенную схему обозначим через S. По лемме при $\varepsilon \in (0, \varepsilon_3)$ ($\varepsilon_3 = \min\{\varepsilon_1, \varepsilon_2\}$) получаем $P(S) \le P(A) + 3P^2(S_1) \le \varepsilon N_Б(M) + c_2\varepsilon^2 + 3(2\varepsilon N_g)^2 = \varepsilon N_Б(M) + d\varepsilon^2$, где $d = c_2 + 12(N_g)^2$. Очевидно, $L(S) = 3L(S_1) + L(A) \lesssim 3L(S_1) \lesssim 3(1+b)\rho \cdot 2^n/n$. Теорема 3 доказана.

Из теоремы 3 следует, что при инверсных неисправностях на выходах элементов схемы с ненадежностью, "близкой" к оптимальной (точнее, превышающую оптимальную ненадежность не больше чем

в пять раз), можно строить для почти всех булевых функций с увеличением оптимальной сложности не более чем в три раза.

Замечание. Если $N_B(M) = 1$, то схемы, построенные при доказательстве теоремы 3, являются асиптотически оптимальными по надежности и функционируют с ненадежностью, асимптотически равной ε при $\varepsilon \to 0$.

Список литературы

1. Uhlig D. Reliable networks from unreliable gates with almost minimal comlexity // Fundamentals of Computation Theory. Intern. conf. FCT'87 (Kazan, June 1987). — Proc. Berlin: Springer-Verl., 1987. — P. 462–469. (Lecture Notes in Comput. Sci.; V. 278).

2. Алехина М. А. Синтез асимптотически оптимальных по надежности схем. Монография. — Пенза: ИИЦ ПГУ, 2006.

3. Аксенов С. И. О надежности схем над произвольной полной системой функций при инверсных неисправностях на выходах элементов // Известия высших учебных заведений. Поволжский регион. Естественные науки. N 6, 2005. — С. 42–55.

4. Аксенов С. И. О надежности схем над некоторыми полными системами при инверсных неисправностях на выходах элементов // Труды Международного симпозиума "Надежность и качество" (г. Пенза, 25–31 мая 2006 г.). Пенза: Изд-во Пенз. гос. ун-та, 2006. Т. 1. — С. 220–221.

5. Аксенов С. И. О надежности схем над частными классами полных систем при инверсных неисправностях на выходах элементов // Труды VII международной конференции "Дискретные модели в теории управляющих систем" (Покровское, 4–6 марта 2006 г.). М.: МАКС Пресс, 2006. — С. 10–16.

О НАДЕЖНОСТИ СХЕМ ПРИ ОДНОТИПНЫХ КОНСТАНТНЫХ НЕИСПРАВНОСТЯХ

М. А. Алехина, Д. М. Клянчина (Пенза)

Рассматривается реализация булевых функций схемами из ненадежных функциональных элементов в некотором базисе B. Схема реализует булеву функцию $f(x_1, ..., x_n)$, если при поступлении на входы схемы двоичного набора $\tilde{a} = (a_1, ..., a_n)$ при отсутствии неисправностей на выходе схемы появляется значение $f(\tilde{a})$ [1]. Входы

всех элементов схемы независимо друг от друга переходят в неисправные состояния типа 0 (1). *Неисправности типа* 0 *на входах элементов* характеризуются тем, что поступающий на вход элемента нуль не искажается, а единица — с вероятностью γ ($\gamma < 1/2$) может превратится в нуль. *Неисправности типа* 1 *на входах* элементов определяются аналогично. Далее считаем, что базисные элементы подвержены неисправностям типа 0 на входах.

Пусть $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ — вероятность появления значения $\bar{f}(\tilde{a})$ на выходе схемы S, реализующей функцию $f(\tilde{x})$ при входном наборе $\tilde{a}$. *Ненадежность* $P(S)$ схемы S определяется как $\max\{P_{\bar{f}(\tilde{a})}(S, \tilde{a})\}$, где максимум берется по всем входным наборам $\tilde{a}$ схемы S. *Надежность* схемы S равна $1 - P(S)$.

Пусть $P_\gamma(f) = \inf P(S)$, где S — схема, реализующая $f(\tilde{x})$. Схему A, реализующую f, назовем *асимптотически оптимальной по надежности*, если $P(A) \sim P_\gamma(f)$ при $\gamma \to 0$.

Очевидно, функции $x_i,\ i \in \mathbf{N}$ можно реализовать абсолютно надежно (не используя при этом функциональных элементов).

Известно [2, 3], что асимптотически оптимальные по надежности схемы для почти всех булевых функций функционируют с ненадежностью, асимптотически (при $\gamma \to 0$) равной γ в базисах $\{\bar{x}\&y, x \sim y\}, \{\bar{x}\&y, \bar{x}\}$, 2γ — в базисах $\{\bar{x} \vee \bar{y}\}, \{\bar{x} \vee y, \bar{x}\}, \{\bar{x}\&y, 1\}$, γ^2 — в базисах $\{x \oplus y, x \vee y, \bar{x}\}, \{x\&y, x \vee y, \bar{x}\}$, $2\gamma^2$ — в базисе $\{\bar{x}\&\bar{y}\}$, γ^3 — в базисе $\{x\&y\&z, x \vee y \vee z, \bar{x}\}$.

Интересным представляется ответ на вопрос, может ли в некотором базисе ненадежность асиптотически оптимальных схем быть равной $\gamma^k,\ k \geq 4$? Ответ положительный, следует из теорем 1 и 2.

Теорема 1. *Существуют такие положительные константы* c_1, c_2, *что если* $\gamma \leq c_1$, *то любую булеву функцию* f *в базисе* $\{\bigvee_{i=1}^k x_i, \bigwedge_{i=1}^k x_i,\ \bar{x}\}$ *можно реализовать схемой* S, *ненадежность которой* $P(S) \leq \gamma^k + c_2\gamma^{k+1}$.

Из теоремы 1 следует, что в базисе $\{\bigvee_{i=1}^k x_i,\ \bigwedge_{i=1}^k x_i,\ \bar{x}\}$ любую булеву функцию можно реализовать схемой, ненадежность которой асимптотически не больше γ^k, если $\gamma \to 0$.

Пример 1. Пусть базис $B = \{\bigvee_{i=1}^k x_i,\ \bigwedge_{i=1}^k x_i,\ \bar{x}\}$. При $\gamma \leq 1/k^2$ константы 0 и 1 можно реализовать схемами с ненадежностью не больше $(1/k)^{k^m}$, где m — любое натуральное число (число итераций), т. е. константы 0 и 1 можно реализовать схемами сколь угодно высокой надежности.

Теорема 2. *Пусть* $\gamma \leq 1/(2k)$, $f(x_1, ..., x_n)$ — *функция*, $f \neq$

0, 1, x_i, *а* S — *любая схема, реализующая* f *в базисе* $\{\bigvee_{i=1}^{k} x_i, \bigwedge_{i=1}^{k} x_i,\ \bar{x}\}$. *Тогда* $P(S) \geq \gamma^k$.

Из теоремы 2 следует, что при неисправностях типа 0 на входах элементов в базисе $\{\bigvee_{i=1}^{k} x_i,\ \bigwedge_{i=1}^{k} x_i,\ \bar{x}\}$ схемы из теоремы 1 для функций $f(x_1, ..., x_n)$, отличных от x_i и констант, являются асимптотически оптимальными по надежности и функционируют с ненадежностью, асимптотически равной γ^k при $\gamma \to 0$.

Поскольку ненадежности двойственных схем равны [1], а рассматриваемый базис двойственнен себе, теоремы 1, 2 и пример 1 справедливы при неисправностях типа 1 на входах элементов в базисе $\{\bigvee_{i=1}^{k} x_i,\ \bigwedge_{i=1}^{k} x_i,\ \bar{x}\}$.

Список литературы

1. Редькин Н. П. Надежность и диагностика схем. — М.: Изд-во МГУ, 1992.

2. Алехина М. А. Синтез асимптотически оптимальных по надежности схем. Монография. — Пенза: ИИЦ ПГУ, 2006.

3. Алехина М. А. О надежности схем в базисе $\{x \vee y \vee z, x\&y\&z, \bar{x}\}$ при однотипных константных неисправностях на входах элементов // Дискретная математика. — 2006. — Т. 18, вып. 1. — С. 116–125.

ОБ ОЦЕНКАХ СЛОЖНОСТИ РЕШЕНИЯ ОПЕРАТОРНЫХ УРАВНЕНИЙ

И. В. Бойков (Пенза)

В работе [1] исследован вопрос о числе арифметических действий необходимых при решении интегральных уравнений с гладкими ядрами. Результаты работы [1] распространены в [2,3] на многомерные интегральные уравнения Фредгольма второго рода с ядрами принадлежащими классам $Q_{r,\gamma}(\Omega, M), B_{r,\gamma}(\Omega, M)$ и на слабосингулярные интегральные уравнения.

В данной работе предложен способ оценки сложности решения операторных уравнений второго рода, основанный на исследовании поперечников множеств, к которым принадлежат компактные операторы и правые части уравнений.

Определение оптимальных по сложности алгоритмов приведем, следуя работе [1], на примере уравнения

$$Kx \equiv x + Hx = f, \tag{1}$$

где оператор K действует из банахова пространства X в банахово пространство X, H — компактный оператор.

Пусть $\Xi(n)-$ множество всех приближенных методов решения уравнения (1.1), при которых производится не больше чем n простейших операций. Введем, следуя [1], величину $E(n, \Psi_1, \Psi_2, d) = \inf_{\Xi(n)} \sup_{H\in\Psi_1, f\in\Psi_2} \|x^* - x_n^*\|_X$, где Ψ_1 — множество операторов, действующих из X в X, Ψ_2- множество правых частей, x^*- точное решение уравнения (1.1), x_n^* — приближенное решение уравнения (1), требующее n простейших операций, минимальное расстояние от 1 до множества собственных значений больше $d(d > 0)$. Введем функционал $\zeta_n(\xi(n)) = \sup_{H\in\Psi_1, f\in\Psi_2} \|x^* - \overline{x}_n^*\|_C$, где $\overline{x}_n^*-$ приближенное решение уравнения (1) по алгоритму $\xi(n)$, требующему не более n простейших операций.

Приближенный метод $\xi(n) \in \Xi(n)$ назовем оптимальным, асимптотически оптимальным, оптимальным по порядку по сложности на классах Ψ_1, Ψ_2, если $E(n, \Psi_1, \Psi_2, d)/\zeta_n(\xi(n)) = 1, \sim 1, \asymp 1$, соответственно.

В работах [1–3] в качестве простейших операций взят набор P={арифметические действия; вычисление значений функций}. Более общей является постановка задачи, при которой в качестве простейших операций взят набор Ф={арифметические действия; вычисление функционалов}.

Ниже нам понадобится определение поперечников в банаховых пространствах.

Пусть X и Y — B-пространства, $B[X, Y]$ — множество линейных операторов, отображающих X и Y. Обозначим через $\Psi[X, Y]$ множество компактных линейных операторов, отображающих X в Y.

Пусть $\Psi_N[X, Y]$ — множество N-мерных линейных ограниченных операторов, отображающих X в Y.

Введем, по аналогии с определением поперечника Колмогорова в функциональных пространствах, определение N-поперечника в банаховых пространствах.

Определение 1. N-поперечником множества компактных операторов $\Psi[X, Y]$ назовем число

$$d_N(\Psi[X, Y]; B[X, Y]) = \inf_{\Psi_N[X,Y]} \sup_{H\in\Psi[X,Y]} \inf_{H_N\in\Psi_N[X,Y]} \|H - H_N\|,$$

где последний inf берется по всем N-мерным линейным ограниченным операторам, действующим из X и Y.

Изложим общий метод на примере операторного уравнения

$$K_H x \equiv x + Hx = f, \tag{2}$$

действующего из пространства X в X.

Операторы H принадлежат множеству $\Psi_1[X, X]$, а правые части f принадлежат Ψ_2.

Будем считать, что операторы $K_H \in [X, X]$ непрерывно обратимы при всех $H \in \Psi_1$ и нормы обратных операторов K_H^{-1}, $H \in \Psi_1$, ограничены одними и теми же константами: $B_* \le \|K_H^{-1}\| \le B^*$ при всех $H \in \Psi_1$. Кроме того, будем считать, что нормы операторов K_H при всех $H \in \Psi_1$ ограничены одними и теми же константами D^* и $D_* : D_* \le \|K_H\| \le D^*$.

Оценим снизу число функционалов, необходимых для решения уравнения (2) с точностью ϵ.

При сделанных выше предположениях для решения уравнения (2.1) с точностью ε необходимо проделать $n = n_1 + n_2$ базисных операций, где n_1 и n_2 определяются из неравенств $d_{n_1}(\Psi_1, X) \ge \epsilon/2$, $\quad d_{N_2}(\Psi_2, X) \ge \varepsilon/2$.

На интегральные уравнения Фредгольма второго рода это утверждение распространяется следующим образом. Рассмотрим уравнение

$$K_h x \equiv x + H_h x \equiv x(t) + \int\limits_{\Omega} h(t, \tau) x(\tau) d\tau = f(t), \tag{3}$$

действующее из пространства C в C (здесь $\Omega = [-1, 1]^l$, $l = 1, 2, \ldots$), $t = (t_1, \ldots, t_l)$, $\tau = (\tau_1, \ldots, \tau_l)$).

Функции $h(t, \tau)$ и $f(t)$ принадлежат функциональным множествам Ψ_1 и Ψ_2.

Теорема. *Пусть уравнение (3) с оператором $K_h \in [C, C]$ однозначно разрешимо при $h \in \Psi_1$ и $f \in \Psi_2, 0 < D_* \le \|K_h\| \le D^* < \infty$ и нормы обратных операторов ограничены в совокупности: $0 < B_* = \|K_h^{-1}\| \le B^* < \infty$. Пусть классы функций Ψ_1 и Ψ_2 таковы, что операторы K_h отображают множество $x = \{x : x \in C(\Omega), \|x\| = 1\}$ в Ψ_2. Тогда число арифметических действий, необходимых для решения уравнения (3) с точностью $O(\epsilon)$ определяется формулой $n = n_1 + n_2$, где n_1 и n_2 — решения уравнений $d_n(\Psi_2, C) = \epsilon$ и $d_n(\Psi_1, L_1) = \epsilon$, соответственно.*

Список литературы

1. Емельянов К. В., Ильин А. М. // ЖВМ и МФ. — 1967. — Т. 7, № 4. — С. 905–910.

2. Бойков И. В. // Дифференциальные уравнения. — 1998. — Т. 34, № 9. — С. 1240–1245.

3. Бойков И. В. // Дифференциальные уравнения. — 1999. — Т. 35, № 9. — С. 1240–1245. С. 1199–1206.

О СИНТЕЗЕ ЛЕГКОТЕСТИРУЕМЫХ СХЕМ В СЛУЧАЕ ОДНОТИПНЫХ КОНСТАНТНЫХ НЕИСПРАВНОСТЕЙ НА ВЫХОДАХ ЭЛЕМЕНТОВ

Ю. В. Бородина (Москва)

Будем рассматривать схемы из функциональных элементов [1, 2]. Пусть S — некоторая схема из функциональных элементов, реализующая булеву функцию $f(\tilde{x})$, $\tilde{x} = (x_1, x_2, \ldots, x_n)$.

Функция, реализуемая на выходе схемы при наличии в схеме неисправных элементов, называется функцией неисправности. Всякое множество T входных наборов схемы S называется полным проверяющим тестом для этой схемы, если для любой функции неисправностей $g(\tilde{x})$, не равной тождественно $f(\tilde{x})$, в T найдется хотя бы один такой набор $\tilde{\sigma}$, что $f(\tilde{\sigma}) \neq g(\tilde{\sigma})$ [3, 4]. Число наборов, составляющих этот тест, называется длиной теста. В качестве тривиального теста всегда можно взять тест, содержащий все 2^n наборов значений переменных булевой функции от n переменных.

Введем обозначения: $D(T)$ — длина теста T; $D(S) = \min D(T)$, где минимум берется по всем полным проверяющим тестам T для схемы S; $D(f) = \min D(S)$, где минимум берется по всем схемам S, реализующим функцию f; $D(n) = \max D(f)$, где максимум берется по всем булевым функциям f от n переменных.

В работе рассматривается задача построения легкотестируемых схем из функциональных элементов для произвольных булевых функций. В качестве базиса возьмем $\{\&, \vee, \bar{}\}$. В качестве неисправностей предполагаются константные неисправности типа "1" на выходах элементов.

Для произвольной булевой функции $f(\tilde{x})$, $\tilde{x} = (x_1, x_2, \ldots, x_n)$ известен [5] способ построения реализующей ее схемы, допускающей полный проверяющий тест длины не больше n.

Нулевой набор функции $f(\tilde{x})$, где $\tilde{x} = (x_1, x_2, \ldots, x_n)$, — это набор значений переменных $x_1, x_2, \ldots, x_n$, на котором функция принимает значение 0.

Обозначим через $\|\tilde{\sigma}\|$ количество единиц в наборе $\tilde{\sigma} = (\sigma_1, \ldots, \sigma_n)$, и положим $m(f) = \max\{\|\tilde{\sigma}\| : f(\tilde{\sigma}) = 0\}$, т. е. $m(f)$ — максимальное количество единиц в нулевых наборах функции f.

Теорема 1. *Пусть для функции f от n переменных, отличной от константы, найдутся такой нулевой набор $\tilde{\sigma}$ и такая тупиковая дизъюнктивная нормальная форма F, что*

1) $\|\tilde{\sigma}\| = m(f) \neq 0$,

2) *если для какого-то $j \in \{1, \ldots, n\}$ значение $\sigma_j = 0$, то соответствующая переменная x_j входит в F без отрицания.*

Тогда функцию f можно реализовать схемой из функциональных элементов, допускающей полный проверяющий тест длины 1.

Замечание. Исключенные в теореме 1 константные функции также реализуются схемами, допускающими полный проверяющий тест длины 1 — см. [5, с. 149].

Теорема 2. *Для любого $n \geq 2$ выполняется равенство $D(n) = 2$.*

Автор глубоко благодарен профессору Н. П. Редькину за внимание к работе и ценные замечания.

Работа выполнена при финансовой поддержке РФФИ (проект 05-01-00994), Программы поддержки ведущих научных школ РФ (проект НШ-5400.2006.1) и Программы фундаментальных исследований Отделения математических наук РАН "Алгебраические и комбинаторные методы математической кибернетики" (проект "Синтез и сложность управляющих систем").

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: изд-во МГУ, 1984.

2. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 2002.

3. Яблонский С. В. Некоторые вопросы надежности и контроля управляющих систем // Математические вопросы кибернетики. Вып. 1. — 1988. — С. 5–25.

4. Редькин Н. П. Надежность и диагностика схем —М., 1992.

5. Редькин Н. П. О схемах, допускающих короткие тесты // Вестн. Моск. ун-та. Сер. 1. Матем. Мех. — 1988. — № 2. — С. 17–21.

О БУЛЕВЫХ СХЕМАХ ДЛЯ АРИФМЕТИКИ В ПСЕВДОМЕРСЕННОВСКИХ ПОЛЯХ

А. А. Бурцев (Москва)

В связи с возможными применениями в криптографии на эллиптических кривых [1] появился интерес к эффективной реализации арифметики в конечных полях большой характеристики. С этой целью в [2] предложено использовать поля с характеристикой, относительно мало отличающейся от степени двойки (такие простые числа в [2] названы псевдомерсенновскими), в которых существуют полиномиальные базисы, соответствующие неприводимым двучленам (такие представления этих полей в [2] названы оптимальными расширениями простых полей).

Для случаев когда характеристика поля является числом Мерсенна в настоящей работе предлагается лучшая, чем в [2, 3] реализация арифметики в башнях полей некоторых типов. Основная идея состоит в использовании на каждом этаже башни для умножения подходящего варианта из методов Карацубы, Тоома, дискретного преобразования Фурье [4–7], их композиций и модификаций. В отличие от [2, 3] предлагается не программная, а схемная реализация. Определение схемы, ее сложности и глубины, можно найти в [8]. В качестве базиса выбирается множество всех двуместных булевых операций.

Используем следующие обозначения: $GF(s)$ — конечное поле порядка s, $M(s)$ — сложность умножения в $GF(s)$, $A(s)$ — сложность сложения в $GF(s)$, $M(C,s)$ — сложность умножения на константу C в $GF(s)$, w_k — примитивный корень k-й степени из единицы в $GF(q)$, $\varepsilon = w_3$; n, k_i — неотрицательные целые, p — простое.

Теорема 1. *Умножение в башне полей $GF(q^3)$, $q = p^n$, имеет оценку сложности*

$$M(q^3) \le 5M(q) + 21A(q) + 6M(2,q) + 2(M(4,q) + M(1/2,q) +$$

$$+M(1/6,q)) + 2M(\alpha_0,p)$$

в предположении, что $q-1$ кратно 3, двучлен $x^n - \alpha_0$ неприводим над $GF(p)$ и двучлен $x^{3n} - \alpha_0$ тоже неприводим над $GF(p)$.

Теорема 2. *Умножение в башне полей $GF(q^4)$, $q = p^n$, имеет оценку сложности*

$$M(q^4) \le 7M(q) + 6M(\varepsilon,q) + 54A(q) + 6M(1/6,q) + 3M(\alpha_0,p)$$

в предположении, что $q-1$ *кратно* 12, $x^n-\alpha_0$ *неприводим над* $GF(p)$ *и* $x^{4n}-\alpha_0$ *неприводим над* $GF(p)$.

Теорема 3. *Умножение в башне полей* $GF(q^6)$, $q=p^n$, *имеет оценку сложности*

$$M(q^6) \le 12M(q)+121A(q)+6M(\alpha_0,p)+M(1/12,q)+$$

$$+2(M(-3/2,q)+M(\frac{\varepsilon-\varepsilon^2}{2},q)+M(-1/8,q)+M(\frac{\varepsilon-\varepsilon^2}{24},q))+$$

$$+2(M(\omega_4,q)+M(-3\omega_4/2,q)+M(\omega_4\frac{\varepsilon-\varepsilon^2}{2},q))+$$

$$+M(\frac{\omega_4}{12},q)+M(-\omega_4/8,q)+M(\omega_4\frac{\varepsilon-\varepsilon^2}{24},q)$$

в предположении, что $q-1$ *кратно* 12, $x^n-\alpha_0$ *неприводим над* $GF(p)$ *и* $x^{6n}-\alpha_0$ *тоже неприводим над* $GF(p)$.

Теорема 4. *Для* $q=p^n$, $p=2^{13}-1$, $n=2^{k_0}\cdot 3^{k_1}\cdot 5^{k_2}\cdot 7^{k_3}\cdot 13^{k_4}$, $k_0=0,1$, *умножение в поле* $GF(q^5)$ *имеет оценку сложности*

$$M(q^5) \le 77A(q)+11M(q),$$

умножение в поле $GF(q^7)$ *имеет оценку сложности*

$$M(q^7) \le 13M(q)+344A(q)+6A(p),$$

умножение в поле $GF(q^{13})$ *имеет оценку сложности*

$$M(q^{13}) \le 26M(q)+1026A(q)+12A(p),$$

умножение в поле $GF(q^{14})$ *имеет оценку сложности*

$$M(q^{14}) \le 26M(q)+1032A(q)+13A(p).$$

Теорема 5. *Для* $q=p^n$, $p=2^{17}-1$, $n=2^{k_0}\cdot 3^{k_1}\cdot 5^{k_2}\cdot 17^{k_3}$, $k_0=0,1$, *умножение в поле* $GF(q^9)$ *имеет оценку сложности*

$$M(q^9) \le 17M(q)+578A(q)+6A(p),$$

умножение в поле $GF(q^{18})$ *имеет оценку сложности*

$$M(q^{18}) \le 35M(q)+1825A(q)+17A(p).$$

Автор благодарит профессора Гашкова С. Б. за постановку задачи и ценные советы.

Работа выполнена при финансовой поддержке РФФИ (проект 05-01-00994), Программы поддержки ведущих научных школ РФ (проект НШ-5400.2006.1) и Программы фундаментальных исследований Отделения математических наук РАН "Алгебраические и комбинаторные методы математической кибернетики" (проект "Синтез и сложность управляющих систем").

Список литературы

1. Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А. Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы и протоколы криптографии на эллиптических кривых. — М.: КомКнига, 2006.

2. Bailey D. V., Paar C. Efficient arithmetic in finite field extensions with application in elliptic curve cryptography // J. of Cryptology. — 2001. — V. 14, № 3. — P. 156–173.

3. Baktir S., Sunar B. Optimal tower fields // IEEE Trans. Comp. — 2004. — V. 53, № 10. — 1231–1243.

4. Кнут Д. Искусство программирования. Т. 2, — 2000.

5. Карацуба А. А., Офман Ю. П. Умножение многозначных чисел на автоматах // ДАН СССР. — 1962. — Т. 145, № 2. — С. 293–294.

6. Тоом А. Л. О сложности схемы из функциональных элементов, реализующей умножение целых чисел // ДАН СССР. — 1963. — Т. 150. — С. 496–498.

7. Ноден П., Китте К. Алгебраическая алгоритмика. — М.: Мир, 1999.

8. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

СООТНОШЕНИЕ КЛАССОВ NC^1 И $poly(n)$-OBDD$_5$

А. В. Васильев (Казань)

Известный результат Д. Баррингтона [1] устанавливает совпадение класса функций, реализуемых схемами полиномиальной сложности и логарифмической глубины из функциональных элементов с ограниченным числом входов (NC^1), с классом функций, представимых ветвящимися программами константной ширины и полиномиальной длины ($BWBP$).

В данной работе уточняется структура ветвящихся программ, получаемых предложенным Баррингтоном методом. А именно, доказывается, что с помощью k-OBDD ширины 5 при $k = n^{O(1)}$ можно реализовать все функции из класса NC^1 и только их.

Для доказательства данного утверждения потребуется понятие перестановочных ветвящихся программ, а также их связь со стандартными (на основе изложения в монографии Вегенера [2]).

Пусть S_n — это группа подстановок n-й степени с композицией подстановок в качестве групповой операции.

Определение. *Перестановочную ветвящуюся программу* (ПВП) ширины k и длины (или глубины) l будем задавать последовательностью инструкций вида $\langle x_{j(i)}, g_i, h_i \rangle$, где $x_{j(i)}$ — одна из переменных $\{x_1, \ldots, x_n\}$, $g_i, h_i \in S_k$ для всех $1 \leq i \leq l$. Такая ПВП содержит на уровнях $1 \leq i \leq l+1$ по k вершин $v_{i,1}, \ldots, v_{i,k}$. На уровне $i = 1, \ldots, l$ реализуется подстановка $\sigma_i(x) = g_i$, если $x_{j(i)} = 0$, в противном случае $\sigma_i(x) = h_i$, т.е. для всех $1 \leq m \leq k$ два ребра, помеченные 0 и 1, ведут из вершины $v_{i,m}$ к вершинам $v_{i+1,g_i(m)}$ и $v_{i+1,h_i(m)}$ соответственно. ПВП на входном наборе x вычисляет композицию подстановок $\sigma(x) = \sigma_1(x)\sigma_2(x)\ldots\sigma_l(x) \in S_k$.

Обозначим через id тождественную подстановку.

Определение. Говорят, что *ПВП вычисляет функцию* $f_n \in B_n$ *посредством подстановки* τ, если $\sigma(x) = id$ для $x \in f_n^{-1}(0)$ и $\sigma(x) = \tau \neq id$ для $x \in f_n^{-1}(1)$.

Следующая лемма устанавливает связь перестановочных и стандартных ветвящихся программ (определенных в [2, 3]).

Лемма. *Пусть G — перестановочная ветвящаяся программа ширины k и длины l, вычисляющая некоторую функцию f. Тогда существует стандартная ветвящаяся программа ширины k и длины $k \cdot l$, вычисляющая ту же самую функцию.*

Доказательство. Для каждой из k вершин на первом уровне ПВП построим ветвящуюся программу ширины k и длины l: все вершины на уровне i помечаются переменной $x_{j(i)}$, а ребра на следующий уровень соответствуют подстановкам g_i и h_i, т.е. ведут из вершины $v_{i,m}$ к вершинам $v_{i+1,g_i(m)}$ и $v_{i+1,h_i(m)}$ соответственно. Вершины на последнем уровне заменяются конечными, а именно: в r-ой ветвящейся программе $\tau(r)$-ая вершина последнего уровня заменяется на 1, остальные на 0. Полученная ветвящаяся программа вычисляет 1 тогда и только тогда, когда $\sigma(x)(r) = \tau(r)$. Таким образом, $f(x) = 1$ тогда и только тогда, когда все построенные ветвящиеся программы вычисляют 1, т. е. $\sigma(x) = \tau$. Для получения конечного результата достаточно соединить ветвящиеся программы следующим

образом: единичная конечная вершина r-ой программы заменяется на начальную вершину $(r+1)$-ой программы и так далее. Итоговая ветвящаяся программа сохраняет ширину k, а длина увеличивается до $k \cdot l$. Лемма доказана.

Согласно предложенному Баррингтоном [1, 2] методу по схеме из функциональных элементов глубины d можно получить перестановочную ветвящуюся программу ширины 5 и глубины 4^d, по которой, в свою очередь, можно построить стандартную ветвящуюся программу той же ширины и глубины $5 \cdot (4^d)$. Возникает вопрос, а сколько раз и в каком порядке читаются переменные в результирующей ветвящейся программе?

Ответ на данный вопрос содержится в следующей теореме.

Пусть $poly(n)$-OBDD_5 — это класс функций, представимых k-OBDD ширины 5, где $k = poly(n) = n^{O(1)}$ есть некоторый полином от n.

Теорема. *$poly(n)$-$OBDD_5 = NC^1$.*

Доказательство. Из определения следует, что любая перестановочная ветвящаяся программа является забывающей, т.е. на каждом вычислительном пути порядок считывания переменных один и тот же. Кроме того, эквивалентная ей стандартная ветвящаяся программа, согласно построениям леммы, также сохраняет это свойство. Поэтому порядок считывания переменных s является общим для всех путей программы, а метод Баррингтона позволяет определить его рекурсивным образом: s соответствует последнему элементу AND схемы (на глубине d) и представляет собой конкатенацию $s_1 \circ s_2 \circ s_1 \circ s_2$, где s_1 и s_2 точно так же соответствуют последним элементам подсхем глубины $d-1$.

Коммутативность функционального элемента AND, который и моделируется в построениях теоремы Баррингтона, дает альтернативное представление порядка считывания $s = s_2 \circ s_1 \circ s_2 \circ s_1$. Таким образом, на глубине 1, где задаются порядки считывания пар переменных, можно переставить их так, чтобы эти элементарные порядки на парах переменных подчинялись бы одному фиксированному порядку на n переменных, задаваемому некоторой подстановкой π. Действительно, если некоторая упорядоченная пара переменных (x_{i_1}, x_{i_2}) нарушает этот порядок, т.е. $\pi(i_2) < \pi(i_1)$, то ничто не мешает заменить эту пару на (x_{i_2}, x_{i_1}) — результат конъюнкции будет тот же.

Получаемая ПВП глубины 4^d содержит $4^d/2$ пар переменных, которые, как было показано, подчиняются одному и тому же порядку считывания. Моделируя ее стандартной ветвящейся программой, имеем $k(d)$-OBDD ширины 5, где $k(d) \leq 5 \cdot 2^{-1} \cdot 4^d$.

В частности, для класса функций, реализуемых схемами логарифмической глубины из элементов с ограниченным числом входов (NC^1), $d = O(\log(n))$, т.е. результирующая ветвящаяся программа находится в классе $poly(n)$-OBDD$_5$. Значит, $NC^1 \subseteq poly(n)$-OBDD$_5$.

Обратная теорема Баррингтона (см. [2]) демонстрирует включение класса функций, представимых ветвящимися программами константной ширины и полиномиальной сложности ($BWBP$), в класс NC^1, т. е. $BWBP \subseteq NC^1$.

Таким образом, предшествующие рассуждения, а также тот факт, что $poly(n)$-OBDD$_5 \subseteq BWBP$, доказывают утверждение теоремы.

Список литературы

1. Barrington D. Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1 // Proceedings of the 18th Annual ACM Symposium on Theory of Computing, 1986. — P. 1–5.

2. Wegener I. The complexity of boolean functions. — Stuttgart: John Wiley & Sons Ltd, and B. G. Teubner, 1987.

3. Wegener I. Branching programs and binary decision diagrams. — Philadelphia: SIAM, 2000.

О ФУНКЦИЯХ, ИСПОЛЬЗУЕМЫХ ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ СХЕМ

А. В. Васин (Пенза)

Впервые задачу синтеза надежных схем из ненадежных элеметов рассматривал Дж. фон Нейман [1]. Он предполагал, что все элементы схемы независимо друг от друга с вероятностью ε ($\varepsilon < 1/2$) подвержены инверсным неисправностям на выходах, когда функциональный элемент с приписанной ему булевой функцией $f(\widetilde{x})$ в неисправном состоянии реализует $\bar{f}(\widetilde{x})$. Для повышения надежности схем Дж. фон Нейман использовал схему, реализующую функцию голосования (медиану) $g_1(x_1, x_2, x_3) = x_1x_2 \vee x_2x_3 \vee x_1x_3$. Позднее задача реализации булевых функций надежными схемами при однотипных константных неисправностях элементов решалась Алехиной [2], а для повышения надежности применялись схемы, реализующие как медиану $g_1(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$, так и функции $g_2(x_1, x_2, x_3, x_4) = x_1x_2 \vee x_3x_4$ и $g_3(x_1, x_2, x_3) = (x_1 \vee$

$x_2)\&(x_3 \vee x_4)$. С. И. Аксенов [3] расширил множество функций повышающих надежность схем. Он ввел следующие множества функций $G_1 = \{x_1^{a_1}x_2^{a_2} \vee x_2^{a_2}x_3^{a_3} \vee x_1^{a_1}x_3^{a_3}\}$ и $G_2 = \{(x_1^{a_1}x_2^{a_2} \vee x_3^{a_3}x_4^{a_4})^{a_5}\}$, где $a_i \in \{0,1\}, i = \overline{1,5}$, показал, что наличие любой из функций данных множеств в произвольном полном базисе B гарантирует реализацию произвольной булевой функции схемой, функционирующей с вероятностью ошибки не больше $\varepsilon + c\varepsilon^2$, где $\varepsilon < d$, c, d — некоторые положительные константы. Оказалось, что наличие и некоторых других функций в базисе дает такой же результат. Класс M таких функций был введен Алехиной [2]. Она задавала функции из M при помощи описания их свойств. Реализуем функции из этого класса при помощи ДНФ и оценим сложность ДНФ.

Пусть булева функция $m(x_1, x_2, \ldots, x_k)$ $(k \geq 3)$ обладает свойством: найдется такой набор $(\sigma_1, \sigma_2, \ldots, \sigma_k)$, что на нем и всех соседних с ним наборах функция m принимает значение 1, а на наборе $(\bar{\sigma}_1, \bar{\sigma}_2, \ldots, \bar{\sigma}_k)$ и всех соседних с ним наборах — значение 0. Наборы $(\sigma_1, \sigma_2, \ldots, \sigma_k)$ и $(\bar{\sigma}_1, \bar{\sigma}_2, \ldots, \bar{\sigma}_k)$ будем называть *характеристическими наборами* функции $m(x_1, x_2, \ldots, x_k)$. Обозначим через M множество всех функций $m(x_1, x_2, \ldots, x_k)$ с названным свойством.

Пусть частично определенная функция $f_{\tilde{\sigma}}(x_1, x_2, \ldots, x_k) \in M$, а набор $\tilde{\sigma} = (\sigma_1, \sigma_2, \ldots, \sigma_k)$ — характеристический для данной функции и $f_{\tilde{\sigma}}(\tilde{\sigma}) = 1$. Таким образом, функция $f_\sigma(x_1, x_2, \ldots, x_k)$ определена на $2k + 2$ наборах.

Утверждение 1. *В ДНФ функции $f_{\tilde{\sigma}}(x_1, x_2, \ldots, x_k)$ не содержится конъюнкций ранга* 1.

Доказательство. Сопоставим функции $f_{\tilde{\sigma}}(x_1, x_2, \ldots, x_k)$ подмножество N_{f_σ} вершин куба E^k так, что вершина $(a_1, a_2, \ldots, a_k) \in N_{f_\sigma}$ тогда и только тогда, когда $f_{\tilde{\sigma}}(a_1, a_2, \ldots, a_k) = 1$. Допустим, что в ДНФ функции $f_{\tilde{\sigma}}(x_1, x_2, \ldots, x_k)$ присутствует элементарная конъюнкция x_i^τ ранга 1, $i = \overline{1,k}$, $\tau \in \{0,1\}$. Наборы $\widetilde{\alpha}^0 = (\sigma_1, \sigma_2, \ldots, \sigma_k)$, $\widetilde{\alpha}^1 = (\bar{\sigma}_1, \sigma_2, \ldots, \sigma_k)$, $\widetilde{\alpha}^2 = (\sigma_1, \bar{\sigma}_2, \ldots, \sigma_k), \ldots,$ $\widetilde{\alpha}^k = (\sigma_1, \sigma_2, \ldots, \bar{\sigma}_k) \in N_{f_{\tilde{\sigma}}}$, функция $f_{\tilde{\sigma}}$ обращается на них в 1. Пусть $\tau = 1$. Тогда набор $\widetilde{\beta}_1 = (\bar{\sigma}_1, \bar{\sigma}_2, \ldots, \bar{\sigma}_{i-1}, \sigma_i, \bar{\sigma}_{i+1}, \ldots, \bar{\sigma}_k) \in N_{f_{\tilde{\sigma}}}$, что противоречит условию $f_{\tilde{\sigma}} \in M$. Аналогично в случае $\tau = 0$ имеем единичный набор $\widetilde{\beta}_2 = (\bar{\sigma}_1, \bar{\sigma}_2, \ldots, \bar{\sigma}_{i-1}, \bar{\sigma}_i, \bar{\sigma}_{i+1}, \ldots, \bar{\sigma}_k)$, что противоречит условию $f_{\tilde{\sigma}} \in M$.

Утверждение 2. *Функцию $f_{\tilde{\sigma}}(x_1, x_2, \ldots, x_k)$ можно представить в виде ДНФ $x_{i_1}^{\sigma_1}\&x_{i_2}^{\sigma_2}\&\ldots\&x_{i_r}^{\sigma_r} \vee x_{i_{r+1}}^{\sigma_{r+1}}\&x_{i_{r+2}}^{\sigma_{r+2}}\&\ldots\&x_{i_k}^{\sigma_k}$, $r = 2, \ldots, k-2$ $(k \geq 4)$.*

Доказательство следует из определения функции $f_{\widetilde{\sigma}}$ и утверждения 1.

Утверждение 3. *Пусть* $k \geq 4$, *набор* $\widetilde{\sigma} = (\sigma_1, \sigma_2, \ldots, \sigma_k)$ — *характеристический для функции* $f_{\widetilde{\sigma}}(x_1, x_2, \ldots, x_k) \in M$ *и* $f_{\widetilde{\sigma}}(\widetilde{\sigma}) = 1$. *Возьмем произвольное разбиение множества* $\{x_1^{\sigma_1}, x_2^{\sigma_2}, \ldots, x_k^{\sigma_k}\} = \bigcup_{i=1}^{l} S_i$, *где* $|S_i| \geq 2$, $\sum |S_i| = k, S_j \bigcap S_i = \emptyset (j \neq i)$, $i, j = \overline{1,l}$ $(2 \leq l \leq \lfloor k/2 \rfloor)$. *Сопоставим каждому* S_i, $i = \overline{1,l}$, *элементарную конъюнкцию* K_i, *состоящую из всех элементов* S_i. *Из конъюнкций* $K_1, K_2, \ldots, K_l$ *составляем ДНФ:*

$$D(x_1, x_2, \ldots, x_k) = \bigvee_{i=1}^{l} K_i.$$

Тогда ДНФ D *есть ДНФ функции* $f_\sigma(x_1, x_2, \ldots, x_k)$.

Доказательство. Очевидно, что на наборе $\widetilde{\sigma} = (\sigma_1, \sigma_2, \ldots, \sigma_k)$ все K_i, $i = \overline{1,l}$, равны 1. Так как переменные в конъюнкциях K_i не повторяются, то на любом наборе, соседнем с $\widetilde{\sigma}$, хотя бы одна K_i равна 1. На наборе $(\bar{\sigma}_1, \bar{\sigma}_2, \ldots, \bar{\sigma}_k)$ все K_i обращаются в 0. Так как в каждую конъюнкцию K_i входит не менее двух переменных, то на всех соседних наборах с $(\bar{\sigma}_1, \bar{\sigma}_2, \ldots, \bar{\sigma}_k)$ все K_i равны 0. Таким образом, $D(x_1, x_2, \ldots, x_k)$ реализует частично определенную функцию $f_{\widetilde{\sigma}}(x_1, x_2, \ldots, x_k) \in M$.

Теперь число букв в записи ДНФ, реализующей булеву функцию f, будем называть *сложностью* ДНФ и обозначать $L(f)$.

Из утверждений 2 и 3 следует, что $L(f_{\widetilde{\sigma}}) = k$ для любой функции $f_{\widetilde{\sigma}}(x_1, x_2, \ldots, x_k) \in M$.

Список литературы

1. фон Нейман Дж. Вероятностная логика и синтез надежных организмов из ненадежных компонент // Автоматы. М.: ИЛ, 1956. — С. 68–139.

2. Алехина М. А. Синтез асимптотически оптимальных по надежности схем. — Пенза: ИИЦ ПГУ, 2006.

3. Аксенов С. И. О надежности схем над произвольной полной системой функций при инверсных неисправностях на выходах элементов // Известия высших учебных заведений. Поволжский регион. Естественные науки. — 2005. — № 6. — С. 42–55.

ДОСТИЖИМОСТЬ НИЖНЕЙ ОЦЕНКИ СЛОЖНОСТИ ПРИ РЕАЛИЗАЦИИ ЛИПШИЦЕВЫХ ФУНКЦИЙ

Я. В. Вегнер (Москва)

Рассмотрим класс $W[a,b]$ вещественных функций одного аргумента, определённых на отрезке $[a,b]$, не превосходящих по модулю 1 и удовлетворяющих условию Липшица с константой 1. Рассматривается задача приближённой реализации произвольной функции $f \in W[0,1]$ с погрешностью ε схемой из функциональных элементов; базис состоит из конечного числа липшицевых функций и произвольного ограниченного множества вещественных констант. Такие базисы называются липшицевыми. Под сложностью понимаем количество функциональных элементов в схеме без учёта констант.

В статье [1] доказана нижняя оценка сложности приближённой реализации функций в липшицевых базисах, для класса $W[0,1]$ равная $C/\sqrt{\varepsilon}$, но не доказано, что она достижима. В этой работе доказывается достижимость оценки по порядку для базиса $\{x+y, x-y, x*y, |x|\} \cup [0,1]$, где $x*y = \min(\max(x,0),1)\min(\max(y,0),1)$.

Теорема 1. *Любую функцию $f \in W[0,1]$ можно приблизить с заданной погрешностью ε схемой из функциональных элементов сложности $O(1/\sqrt{\varepsilon})$ в почти конечном базисе $\{x+y, x-y, x*y, |x|\} \cup [0,1]$.*

Доказательство. Пусть задана погрешность ε, далее считаем, что $\varepsilon < 1/4$. Определим параметры $s = \lceil 1/\sqrt{\varepsilon} \rceil \geq 3$, $u = 1/s^2$, $v = 1/s$. Тогда

$$1/u = 1/\varepsilon + O(1/\sqrt{\varepsilon}), \quad 1/v = 1/\sqrt{\varepsilon} + O(1), \quad u \leq \varepsilon, \quad v \leq \sqrt{\varepsilon}.$$

Разобьём отрезок $[0,1]$ на отрезки $[kv,(k+1)v]$, $k = 0,\ldots,s-1$.

Лемма 1. *Пусть заданы функция $f \in W[a,b]$, $f(a) = 0$, $f(b) = 0$, и величина δ, такая что $b-a = n\delta$, $n \in \mathbf{N}$. Тогда найдётся кусочно-линейная функция $\tilde{f}(x)$ с угловыми коэффициентами ± 1, $\tilde{f}(a) = 0$, $\tilde{f}(b) = 0$, которая может менять поведение только в точках $\{a + i\delta/2 : i = 0,1,\ldots,2n-1\}$, приближающая функцию f на отрезке $[a,b]$ с погрешностью δ.*

Зафиксируем произвольную функцию $f \in W[0,1]$. Представим её в виде суммы двух функций:

$$f(x) = f_1(x) + f_1'(x),$$

где $f_1(x)$ — функция, равная $f(x)$ в точках kv, $k = 0, \ldots, s$, в остальных точках продолженная по линейности; $f'_1(x)$ — липшицева функция с константой 2. Рассмотрим набор функций $f'_{1,k}(x)$, $k = 0, \ldots, s-1$; функция $f'_{1,k}(x)$ является сужением функции $f'_1(x)$ на отрезок $[kv, (k+1)v]$. Она липшицева с константой 2, обращающаяся в ноль на концах отрезка. Применяя к функции $f'_{1,k}/2$ лемму 1, где $\delta = u/4$, найдём кусочно-линейную функцию $f_{2,k}(x)$ с угловыми коэффициентами ± 1, меняющую поведение только в точках $kv + i\delta/2$, равную нулю в концах отрезка, и приближающую функцию $f'_{1,k}/2$ с погрешностью $\delta \leq \varepsilon/4$, так что $\|f'_{1,k} - 2f_{2,k}\| \leq \varepsilon/2$.

Далее, рассмотрим функции $f_{3,k}(x)$, $k = 0, \ldots, s-1$; каждая функция $f_{3,k}(x)$ определена на отрезке $[kv, (k+1)v]$, совпадает с $f_{2,k}(x)$ на отрезках $[kv, kv+u]$ и $[(k+1)v-u, (k+1)v]$ и доопределена по линейности на отрезке $\Delta_k = [kv+u, (k+1)v-u]$. Представим функцию $f_{2,k}(x)$ в виде суммы

$$f_{2,k}(x) = f_{3,k}(x) + f'_{3,k}(x),$$

где $f'_{3,k}(x)$ — липшицева функция с константой 2, равная нулю на концах отрезка Δ_k и вне него. Применяя к функции $f'_{3,k}/2$ лемму 1 при $\delta = u/8$, находим функцию $f_{4,k}(x)$ с угловыми коэффициентами ± 1, меняющую поведение только в точках $kv + u + i\delta/2$, и приближающую функцию $f'_{3,k}/2$ с погрешностью $\delta \leq \varepsilon/8$, так что $\|f'_{3,k} - 2f_{4,k}\| \leq \varepsilon/4$.

Определим функции $f_3(x) = f_{3,k}(x)$ при $x \in [kv, (k+1)v]$, и

$$f_4(x) = \begin{cases} f_{4,k}(x), & \text{если } x \in \Delta_k, \\ 0 & \text{иначе.} \end{cases}$$

Схема, вычисляющая $f_1(x) + 2\left(f_3(x) + 2f_4(x)\right)$, приближает функцию $f(x)$ с погрешностью ε. Верны следующие леммы.

Лемма 2. *Функцию $f_1(x)$ можно реализовать схемой сложности $O(1/\sqrt{\varepsilon})$.*

Лемма 3. *Функцию $f_3(x)$ можно реализовать схемой сложности $O(1/\sqrt{\varepsilon})$.*

Лемма 4. *Функцию $f_4(x)$ можно реализовать схемой сложности $O(1/\sqrt{\varepsilon})$.*

Используя леммы 2, 3, 4, построим схемы, вычисляющие $f_1(x)$, $f_3(x)$ и $f_4(x)$, и соединим их по формуле $f_1(x) + 2\left(f_3(x) + 2f_4(x)\right)$, где

в качестве умножения на 2 используется функция $2x = x + x$. Как было доказано ранее, такая схема приближает значение функции $f(x)$ с погрешностью ε. Сложность схемы составляет $O(1/\sqrt{\varepsilon})$.

Работа выполнена при финансовой поддержке РФФИ (проект 05-01-00994), Программы поддержки ведущих научных школ РФ (проект НШ-5400.2006.1) и Программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики» (проект «Синтез и сложность управляющих систем»).

Список литературы

1. Гашков С. Б. О сложности приближенной реализации непрерывных функций схемами и формулами в полиномиальных и некоторых других базисах // Математические вопросы кибернетики. Вып. 5. — М.: Наука, 1995. — С. 144–207.

2. Turán G., Vatan F. On the computation of Boolean functions by analog circuit of bounded fan-in // Journal of Computer and System Sciences. — 1997. — V. 54, № 1. — P. 199–212.

ОБ АБСОЛЮТНО НЕУСТОЙЧИВЫХ КОНТАКТНЫХ СХЕМАХ

А. А. Вороненко, Д. С. Романов (Москва)

Контактная схема (КС) называется *приведенной*, если всякий ее контакт лежит на какой-нибудь простой проводящей (на каком-либо наборе входных переменных) цепи, соединяющей полюса схемы. Операция приведения состоит в последовательном удалении из схемы контактов, не удовлетворяющих этому условию, и двухполюсных подсхем, представляющих собой цепочки с тождественно нулевой проводимостью, — до тех пор, пока схема не станет приведенной. Пусть S — двухполюсная КС. Через $Y(S)$ обозначим множество ее контактов. Пусть $Y' \cup Y'' \subseteq Y(S)$, $Y' \cap Y'' = \varnothing$. Будем говорить, что в контактной схеме S *имеется неисправность* $J(Y', Y'')$ тогда и только тогда, когда всякий контакт схемы S из множества Y' разомкнут (т. е. его ребро удалено из схемы), а всякий контакт схемы S из множества Y'' замкнут (т. е. концы его

ребра отождествлены в схеме и его ребро удалено из схемы). Если $Y' \cup Y'' \neq \varnothing$, неисправность $J(Y', Y'')$ будем называть *нетривиальной*. Контактную схему, полученную в результате приведения схемы S с неисправностью $J(Y', Y'')$ в ней, будем обозначать так: $S[J(Y', Y'')]$. При этом мы будем допускать в качестве схем $S[J(Y', Y'')]$ *пустые* схемы, в которых нет контактов, а входной и выходной полюсы могут быть либо отождествлены, либо нет (таковы, например, схемы $S[J(\varnothing, Y(S))]$ и $S[J(Y(S), \varnothing)]$). Заметим, что если S — π-схема, то всякая ее схема $S[J(Y', Y'')]$ — тоже π-схема (при этом пустые схемы будем относить к π-схемам). Двухполюсная контактная схема S, реализующая булеву функцию f, называется *абсолютно неустойчивой контактной схемой (АНКС)* тогда и только тогда, когда для любой нетривиальной неисправности $J(Y', Y'')$ схема $S[J(Y', Y'')]$ реализует булеву функцию, не равную f (пустые схемы также будем считать АНКС). Сложность схемы S (число контактов в ней $|Y(S)|$) будем обозначать через $L(S)$. Через $P_2(n)$ обозначим множество всех функций алгебры логики, зависящих от переменных $\tilde{x}^n = (x_1, x_2, \ldots, x_n)$. Далее будем рассматривать схемы от этих n переменных. Пусть $X_n = \{x_1, x_2, \ldots, x_n\}$, $X' \subseteq X_n$. Через $Y_{X'}(S)$ будем обозначать множество всех контактов схемы S, управляемых переменными из X'. Пусть $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n) \in \{0, 1, 2\}^n$, $f = f(x_1, x_2, \ldots, x_n)$ — булева функция. Через $f|^\gamma$ будем обозначать подфункцию функции f, полученную из f подстановкой константы γ_i, отличной от 2, вместо переменной x_i для всех $i \in \{1, 2, ..., n\}$, для которых $\gamma_i \neq 2$. Пусть теперь S — контактная схема от переменных $(x_1, x_2, \ldots, x_n)$, реализующая функцию f. Определим приведенную контактную схему $S|^\gamma$, полученную из S в результате подстановки набора γ, следующим образом. Если в наборе γ значение $\gamma_i = 2$, то все контакты переменной x_i в схеме сохраняются. Если же $\gamma_i = \alpha_i$, $\alpha_i \in \{0, 1\}$, то в схеме вместо x_i подставляется константа α_i, то есть все контакты вида $x_i^{\alpha_i}$ в схеме стягиваются (отождествляются концы таких контактов с последующим удалением самих контактов), а все контакты вида $x_i^{\bar{\alpha}_i}$ в схеме удаляются. Затем к схеме применяется операция приведения. Результатом таких преобразований является схема $S|^\gamma$. Ясно, что схема $S|^\gamma$ реализует булеву функцию $f|^\gamma$. Отметим, что каждый контакт схемы $S|^\gamma$ мы будем считать также контактом схемы S, из которого он получен. Дадим теперь определение *наследственной АНКС*. Пустые схемы $S[J(\varnothing, Y(S))]$ и $S[J(Y(S), \varnothing)]$ будем считать наследственными АНКС. Далее, будем говорить, что контактная схема S

является *наследственной АНКС*, если она является АНКС и для любого $i \in \{1, 2, \ldots, n\}$ схемы $S|^{(2,\ldots,2,0,2,\ldots,2)}$ и $S|^{(2,\ldots,2,1,2,\ldots,2)}$ (в наборах отличный от двойки элемент стоит в i-й позиции) являются наследственными АНКС. Обозначим через Ω^π (соответственно через Ω^H) класс всех АН π-КС (соответственно класс всех наследственных АНКС). Пусть $\xi \in \{\pi, H\}$. Введем функцию $V^\xi : N \to \{0, 1, 2, \ldots, \aleph_0\}$ следующим образом: $V^\xi(n) = \max\limits_{f(\tilde{x}^n) \in P_2(n)} \max\limits_{S \in \Omega^\xi \text{ реал. } f} L(S)$.

Теорема 1. *Для всякого натурального n значение функции $V^\pi(n)$ конечное, а именно, $V^\pi(n) \leq 2^{2^n \cdot 2^{2^n}}$.*

Следствие 1. *Для всякой булевой функции существует лишь конечное число реализующих ее абсолютно неустойчивых π-схем.*

Теорема 2. *Для любого $n \in N$ справедливо равенство $V^H(n) = n2^{n-1}$.*

Рангом ДНФ W называется число $R(W)$ букв в ней. *Функцией максимума ранга тупиковой ДНФ* называется функция $Q(n) = \max\limits_{f(\tilde{x}^n) \in P_2(n)} \max\limits_{\substack{\text{тупиковая ДНФ } W \\ \text{реализует } f}} R(W)$.

Утверждение (см., например, [3]). *Имеет место асимптотика $Q(n) = n2^n(1 + o(1))$.*

Следствие 2. *Всякая КС, моделирующая тупиковую ДНФ, является АНКС, но не всякая такая КС является наследственной АНКС.*

Работа выполнена при поддержке РФФИ, проекты 06-01-00745 и 07-01-00444.

Список литературы

1. Вороненко А. А. Абсолютно неустойчивые схемы // Тезисы докладов XIII Международной конференции «Проблемы теоретической кибернетики» (Казань, 2002). Часть I. — М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2002. — С. 39.

2. Ложкин С. А. Лекции по основам кибернетики. — М.: Издательский отдел ф-та ВМиК МГУ, 2004.

3. Дискретная математика и математические вопросы кибернетики / Под ред. С. В. Яблонского и О. Б. Лупанова. — Т. 1. — М.: Наука, 1974.

НЕУЛУЧШАЕМОСТЬ НИЖНИХ ОЦЕНОК ФОРМУЛЬНОЙ РЕАЛИЗАЦИИИ БУЛЕВЫХ ФУНКЦИЙ ВЕЩЕСТВЕННЫМИ ФОРМУЛАМИ

С. Б. Гашков, Я. В. Вегнер (Москва)

Рассматривается поставленная О. Б. Лупановым задача реализации булевых функций с помощью формул в базисах, состоящих из конечного числа непрерывных действительных функций и континуума констант. Базис называется *липшицевым*, если он состоит из конечного числа липшицевых функций и произвольного ограниченного множества действительных констант. Под сложностью понимается число символов функций в формуле, без учёта констант. Недостающие определения можно найти в [1].

В статье [1] доказаны нижние оценки вида $\Omega(2^{n/2})$ для формульной реализации булевых функций в липшицевых базисах и базисах, состоящих из липшицевых и мультилинейных функций. В этой работе доказывается, что такие оценки по порядку неулучшаемы. Основные результаты представлены в теоремах 2 и 4 и замечаниях после них.

Лемма 1. *Для произвольного булевого набора* $\alpha = (\alpha_1, \ldots, \alpha_{2^n})$ *число* $a = a_\alpha = \sum\limits_{i=1}^{2^n} 2^{-2i}\alpha_i$, $0 \le a < 1/3$, *удовлетворяет условиям:*

$$\alpha_j = 0 \Leftrightarrow \cos 2^{2j} a\pi > 1/2; \qquad \alpha_j = 1 \Leftrightarrow \cos 2^{2j} a\pi < -1/2.$$

Лемма 2. *Для кусочно-линейной функции* $l(x) = \min(1, \max(0, \frac{1}{2} - x))$ *справедливо тождество* $l(\cos 2^{2j} a\pi) = \alpha_j$, $j = 1, \ldots, 2^n$. *Функцию* $l(x)$ *можно реализовать в базисах* $\{x+y, x-y, xy, |x|\} \cup [0,\, 1]$ *и* $\{x+y, \cos x, xy, |x|\} \cup [0,\, 1]$ *формулами, куда переменная* x *входит по* 2 *раза.*

Лемма 3. *В базисе* $\{x+y, xy\} \cup [0,\, 1]$ *можно построить формулу* $F_n(X)$ *сложности* $O(n)$, *реализующую функцию* $2^{2+2|X|-2^{n+1}}$, *где* $|X| = \sum\limits_{k=1}^{n} 2^{k-1}x_k$. *Эту формулу можно реализовать с линейной сложностью в базисах* $\{x+y, x*y\} \cup [0,\, 1]$ *и* $\{\min(x+y, 1), x*y\} \cup [0,\, 1]$, *где* $x*y = \max(-1, \min(1, x)) \max(-1, \min(1, y))$. *Эти базисы удовлетворяют условию Липшица с константой* 1 *относительно нормы* $\|(x_1, \ldots, x_n)\| = \sum |x_i|$.

Теорема 1. *Для любого натурального* n *в базисе* $\{x + y, xy, \cos x, |x|\} \cup [0,\, 1]$ *существует формула* Φ_n *сложности* $O(2^n)$,

зависящая от одного параметра c_f и переменных $(x_1, \ldots, x_n) = X$, такая что:

1) *каждой булевой функции $f(X)$ можно сопоставить константу $c_f \in [0, 1]$, такую что формула $\Phi_n(c_f, X)$ будет реализовывать f;*

2) *константа c_f входит в формулу Φ_n два раза.*

Теорема 2. *Любую булеву функцию $f(x_1, \ldots, x_n)$ можно реализовать формулой в базисе $\{x+y, xy, \cos x, |x|\} \cup [0, 1]$ со сложностью $O(2^{n/2})$.*

Замечание 1. *Формулу $C(x_1, \ldots, x_m)$ можно реализовать в полиномиальном базисе $\{x + y, xy, 1 - x\}$ и в кусочно-полиномиальных базисах $\{x + y, x * y, 1 - x\}$, $\{\min(x + y, 1), x * y, 1 - x\}$.*

Замечание 2. *Из теоремы 2 следует, что для базиса $\{x + y, xy, \cos x, |x|\} \cup [0, 1]$ нижняя оценка теоремы 12 из [1] по порядку неулучшаема.*

Замечание 3. *Добавление в базис функции x^2 приводит к базису, не удовлетворяющему условию теоремы 12 из [1]. Для нового базиса утверждение теоремы 12 из [1] перестает быть верным.*

Лемма 4. *Существует кусочно-линейная 4-периодичная функция $u(x)$, $u(4k) = 1$, $u(4k+2) = -1$, $u(2k+1) = 0$, $k \in \mathbf{Z}$, такая что для числа a_α из леммы 1 выполнены равенства:*

$$\alpha_j = 0 \Leftrightarrow u(2^{2j+1}a) > 1/3; \qquad \alpha_j = 1 \Leftrightarrow u(2^{2j+1}a) < -1/3.$$

Следствие 1. *Пусть $l(x) = \min(1, \max(0, \frac{1}{2} - \frac{3}{2}x))$. Справедливо тождество $l(u(2^{2j+1}a)) = \alpha_j$.*

Лемма 5. *Функцию $l(x)$ можно реализовать формулой в следующих базисах с конечной сложностью и двумя вхождениями переменной:*

$$\{x+y, x-y, xy, |x|\} \cup [0,1]; \{x-y, xy, |x|\} \cup [0,1]; \{x-y, x*y, |x|\} \cup [0,1].$$

Лемма 6. *В конечном базисе $\{x - y, 2x, |x|, 1\}$ можно реализовать функцию $u(2^{2^{n+1}+1}x), x \in [0, \frac{1}{2}]$, формулой сложности $O(2^n)$ с одним вхождением переменной.*

Лемма 7. *Функцию $u(x)$ можно реализовать на отрезке $[0, 2^{2^{n+1}}]$ формулой сложности $O(2^n)$ с одним вхождением переменной в бесконечном базисе $\{|x|\} \cup \{x - c : c > 0\}$, имеющем липшицеву норму 1.*

Теорема 3. *Для любого натурального числа n в каждом из базисов $\{x + y, x - y, xy, |x|\} \cup [0, +\infty)$, $\{x - y, xy, 2x, |x|\} \cup [0, 1]$,*

$\{x-y, x*y, 2x, |x|\}\cup[0,1]$ *существует формула* $\Phi_n(c_f, X)$ *сложности* $O(2^n)$, *такая что:*

1) *каждой булевой функции* f *можно сопоставить такую константу* $c_f \in [0, 1]$, *что формула* $\Phi_n(c_f, X)$ *будет реализовывать* f;

2) *константа* c_f *входит в формулу* 2 *раза.*

Теорема 4. *В кусочно-полиномиальных базисах* $\{x + y, x - y, xy, |x|\}\cup[0, +\infty)$, $\{x-y, xy, 2x, |x|\}\cup[0,1]$, $\{x-y, x*y, 2x, |x|\}\cup[0,1]$ *любую булеву функцию* $f(X)$ *можно реализовать формулой сложности* $O(2^{n/2})$.

Замечание 4. *Во втором базисе нельзя обойтись без модуля, что видно из теоремы* 11 *из* [1]. *В третьем базисе нельзя обойтись без функции* $2x$, *так как тогда в нем сложность формул была по порядку не меньше* $2^n/n$ *согласно теореме* 9 *в* [1]. *В этом базисе достигается по порядку оценка теоремы* 12 *из* [1].

Работа выполнена при финансовой поддержке РФФИ (проект 05-01-00994), Программы поддержки ведущих научных школ РФ (проект НШ-5400.2006.1) и Программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики» (проект «Синтез и сложность управляющих систем»).

Список литературы

1. Гашков С. Б. Сложность реализации булевых функций схемами из функциональных элементов и формулами в базисах, элементы которых реализуют непрерывные функции // Проблемы кибернетики. Вып. 37. — 1980. — С. 57—118.

АЛГОРИТМ РАСПОЗНАВАНИЯ ФУНКЦИЙ АЛГЕБРЫ ЛОГИКИ, ПРЕДСТАВИМЫХ БЕСПОВТОРНЫМИ КОНТАКТНЫМИ СХЕМАМИ

А. Н. Готманов (Москва)

Задача синтеза оптимальных представлений для индивидуальных функций алгебры логики слабо поддается математическому анализу. Многообразие форм, получающихся объединением конечного числа простейших логических операций, оказывается значительным, что затрудняет поиск и обоснование утверждений общего характера.

Ситуация существенно упрощается при введении дополнительных требований на множество схем или функций. Например, для линейной функции алгебры логики может быть установлено точное значений сложности и перечислены все оптимальные представления; существуют практически значимые средства синтеза дизъюнктивных нормальных форм — формул с строгими структурными ограничениями. Правильное сужение задачи позволяет сконцентрировать усилия в области функций "умеренной сложности".

В большинстве случаев уменьшение сложности функций возникает косвенно, как следствие тех или иных структурных требований. Однако, возможен и обратный подход, основанный на явном ограничении сложности. Так, можно выделить функции алгебры логики, представимые контактными схемами из не более, чем $2n$ контактов, где n — число существенных переменных функции. При этом оказывается разумным потребовать, чтобы аналогичная оценка сложности выполнялась не только для самой функции, но и для всех ее производных (производной называется функция алгебры логики, получающаяся из данной подстановкой констант $0, 1$ вместо некоторых ее переменных). Тогда выделенное множество образует инвариантный класс. Определив таким образом набор рассматриваемых функций, можно перейти к анализу их свойств. Автор не знаком с какими-либо нетривиальными общими свойствами функций с ограничением сложности порядка αn, $\alpha > 1$. Ситуация несколько улучшается в случае $\alpha = 1$.

Рассматривается множество функций алгебры логики, представимых контактными схемами сложности равной числу существенных переменных функции. Из очевидных соображений следует, что такая схема содержит ровно один контакт каждой существенной переменной определяемой функции. Указанные схемы и функции называют *бесповторными*. Их основные свойства рассмотрены в [2, 3]. Класс бесповторных функций — простейший из нетривиальных классов функций с ограничением сложности. Используя метод декомпозиции, описанный в [1], удается построить алгоритм распознавания бесповторных функций, заданных векторно или в форме двоичной ветвящейся программы (BDD) [4].

Теорема 1. *В любом полном базисе существует последовательность схем из функциональных элементов* $\{\Sigma_n\}_{n=0}^{+\infty}$, *с* 2^n *входами* $x_0, \ldots, x_{2^n-1}$ *и одним выходом* y, *таких что* $y = 1$ *тогда и только тогда, когда функция алгебры логики, заданная столбцом значений* $(x_0, \ldots, x_{2^n-1})$, *является бесповторной. Сложность схем* Σ_n *ограничена величиной* $O(2^n)$.

Теорема 2. *Существует машина Тьюринга* M *с двумя финаль-*

ными состояниями q_+ и q_-, принимающая на вход код произвольной двоичной ветвящейся программы (BDD). M переходит в состояние q_+ тогда и только тогда, когда двоичная ветвящаяся программа на входе задает бесповторную функцию. Время работы машины M на любом входе ограничено величиной $O(m^k)$, где m — размер входа, а k — некоторое натуральное число.

Построение алгоритмов существенно опирается на возможность быстрого решения проблемы эквивалентности бесповторных контактных схем (теорема 4) и на свойства устойчивости представлений бесповторных функций алгебры логики (теорема 3).

Теорема 3 [2, 3]. *В классе бесповторных контактных схем существует полная система эквивалентных преобразований, состоящая из единственного тождества переворачивания двухполюсной подсхемы:*

$$\underbrace{\Sigma(\widehat{\Sigma}_{a,b})}_{\Sigma_1} \equiv \underbrace{\Sigma(\widehat{\Sigma}_{b,a})}_{\Sigma_2},$$

где схема Σ_2 получается из схемы Σ_1, содержащей двухполюсную подсхему $\widehat{\Sigma}$, путем переименования полюсов a, b в подсхеме $\widehat{\Sigma}$. Схема Σ, дополнительная к подсхеме $\widehat{\Sigma}$ остается неизменной.

Теорема 4 [2, 3]. *Существует машина Тьюринга M с двумя финальными состояниями q_+ и q_-, принимающая на вход коды двух бесповторных контактных схем Σ_1 и Σ_2 такая, что M переходит в состояние q_+ тогда и только тогда, когда схемы Σ_1 и Σ_2 определяют одну и ту же функцию алгебры логики. Время работы машины M на любом входе ограничено величиной $O(m^k)$, где m — размер входа, а k — некоторое натуральное число.*

Теорема 4 может быть легко распространена на случай схем, близких к бесповторным, а именно схем с не более, чем $n+c$ контактами, где n — число существенных переменных соответствующей функции алгебры логики, а c — натуральное число. Для каждого значения c может быть построена своя машина Тьюринга M_c, решающая проблему эквивалентности за полиномиальное время.

Теоремы 1 и 2 также допускают обобщения на случай функций алгебры логики, представимых схемами сложности $n + c$. Однако, при этом возникают специфические трудности, связанные с нарушением теоремы 3. На данный момент обобщенные варианты теорем 1 и 2 полностью обоснованы автором для случая $c = 1$.

Работа выполнена при финансовой поддержке РФФИ, проект 06-01-00745.

Список литературы

1. Вороненко А. А. О методе разложения для распознавания принадлежности инвариантным классам // Дискретная математика. — 2002. — Т. 14, № 4. — С. 110–116.

2. Кузнецов А. В. О бесповторных контактных схемах и бесповторных суперпозициях функций алгебры логики // Труды МИАН СССР. — 1958. — Т. 51. — С. 186–225.

3. Трахтенброт Б. А. Синтез бесповторных схем // Докл. АН СССР. — 1955. — Т. 103, № 6. — С. 973–976.

4. Wegener I. Branching programs and binary decision diagrams // Philadelphia: SIAM, 2000.

О ГЛУБИНЕ ФОРМУЛ, РЕАЛИЗУЮЩИХ ФУНКЦИИ ИЗ НЕКОТОРЫХ КЛАССОВ ТРЕХЗНАЧНОЙ ЛОГИКИ

Д. А. Дагаев (Москва)

Известно [1], что для любой конечной системы Ψ булевых функций всякая функция $f(x_1, ..., x_n)$ из замыкания $[\Psi]$ реализуется формулой над Ψ, глубина которой имеет линейный порядок роста по числу переменных. Для $k \geq 4$ построены примеры последовательностей функций k-значной логики, глубина которых в классе формул над некоторой конечной неполной системой имеет экспоненциальный порядок роста по числу переменных [2].

В настоящей работе рассматривается задача о реализации функций из $P_{3,2}$ — множества всех функций трехзначной логики, принимающих значения 0 или 1, — формулами над конечными неполными системами. Для некоторых семейств замкнутых классов из $P_{3,2}$ получены асимптотически точные оценки соответствующих функций Шеннона по глубине.

Описание всех замкнутых классов булевых функций было получено Э. Постом [3, 4]. Обозначим через P_2 множество всех булевых функций. Введем следующие обозначения для некоторых подмножеств P_2: L — множество всех линейных функций, M — множество всех монотонных функций, T_i — класс всех функций, сохраняющих константу i ($i \in \{0, 1\}$), S — класс всех самодвойственных функций. Множества M, S, L, T_0, T_1 являются предполными замкнутыми классами в P_2. Для конечной системы функций

Ψ и функции $f(x_1, ..., x_n) \in [\Psi]$ обозначим через $D_\Psi(f)$ глубину функции $f(x_1, ..., x_n)$ в классе формул над Ψ. Функцией Шеннона по глубине для класса $[\Psi]$ называется функция $D_\Psi(n) = \max\limits_{f(x_1,...,x_n)\in[\Psi]} D_\Psi(f(x_1, ..., x_n))$. Результаты данной работы сформулированы в терминах введенного в [5] отображения *проекция* из $P_{3,2}$ в P_2. *Проекцией* функции $f(x_1, ..., x_n) \in P_{3,2}$ называется такая функция $prf(x_1, ..., x_n) \in P_2$, значение которой на наборе $(\alpha_1, ..., \alpha_n)$, где $\alpha_1, ..., \alpha_n \in \{0, 1\}$, определяется равенством $prf(\alpha_1, ..., \alpha_n) = f(\alpha_1, ..., \alpha_n)$. Проекцией prF множества функций $F \subseteq P_{3,2}$ называется множество $\bigcup\limits_{f\in F}\{prf\}$. Нетрудно проверить, что для любого замкнутого класса $F \in P_{3,2}$ множество prF является замкнутым классом булевых функций. Все необходимые определения и обозначения, используемые в данной работе, можно также найти в [6].

Теорема 1. *Пусть $Q \in \{P_2, M, S, T_0, T_1\}$, а H — замкнутый класс из $P_{3,2}$, причем $prH = Q$. Тогда существует конечный базис G класса H и константа c (зависящая от G) такая, что $D_G(n) \sim cn$.*

Приведем описание замкнутых классов из $P_{3,2}$, проекция которых совпадает с L (см. [5]). Пусть $f(x_1, ..., x_n)$ — произвольная функция, для которой $prf(x_1, ..., x_n) \in L$, а $\sigma = (\sigma_1, ..., \sigma_n)$ — такой набор, что $f(\sigma) = 1$. Без ограничения общности будем считать, что $\sigma_1 = ... = \sigma_k = 2$, $\sigma_{k+1} = ... = \sigma_l = 1$, $\sigma_{l+1} = ... = \sigma_n = 0$. Обозначим через $j_i(x)$ $(i = 0, 1, 2)$ функцию из $P_{3,2}$, равную 1 при $x = i$ и 0 в остальных случаях. Для любых двуместных функций $\oplus$ и $\wedge$ из $P_{3,2}$, проекции которых являются соответственно булевым сложением по модулю 2 и булевой конъюнкцией, верно равенство

$$f(x_1, ..., x_n) = \bigoplus_{\sigma: f(\sigma)=1} j_2(x_1) \wedge ... \wedge j_2(x_k) \wedge \\ \wedge j_1(x_{k+1}) \wedge ... \wedge j_1(x_l) \wedge j_0(x_{l+1}) \wedge ... \wedge j_0(x_n).$$

Заменим каждое вхождение функции j_0 в правой части равенства на равную ей функцию $1 \oplus j_1 \oplus j_2$ и раскроем скобки. Получим представление функции $f(x_1, ..., x_n)$:

$$f(x_1, ..., x_n) = a \oplus (\bigoplus_{i=1}^{n} a_i j_1(x_i)) \oplus (\bigoplus_{\substack{I,J \\ I\cup J\subseteq\{1,...,n\} \\ I\cap J=\emptyset \\ J\neq\emptyset}} a_{I,J} k_{I,J}(x_1, ..., x_n)),$$

где $a, a_i, a_{I,J} \in \{0,1\}$. Функции $k_{I,J}(x_1,...,x_n) = (\bigwedge\limits_{i\in I} j_1(x_i)) \wedge (\bigwedge\limits_{j\in J} j_2(x_j))$ называют *компонентами* функции $f(x_1,...,x_n)$. Множество всех компонент функции f будем обозначать через K_f. Положим $pr^{-1}(L) = \{f | prf \in L\}$, $K = \bigcup\limits_{f\in pr^{-1}(L)} K_f$. Через $Z_{2,a}$ $(a \in \{0,1\})$ обозначим замкнутый класс функций $f(x_1,...,x_n) \in P_{3,2}$, обладающих следующим свойством: если набор α получен из набора β заменой всех двоек на a, то $f(\alpha) = f(\beta)$. Перечислим множество всех замкнутых классов из $P_{3,2}$, проекция которых совпадает с L:

$$pr^{-1}(L),$$

$$L_2 = \{f \in pr^{-1}(L) | K_f \subseteq \{k_{I,J} \in K |\ |I| \le 1\}\},$$

$$L_{2,r} = \{f \in pr^{-1}(L) | K_f \subseteq \{k_{I,J} \in K |\ I = \emptyset, |J| \le r\}\} \quad (1 \le r < \infty),$$

$$L_{2,\infty} = \{f \in pr^{-1}(L) | K_f \subseteq \{k_{I,J} \in K |\ I = \emptyset\}\},$$

$$Z_{2,a} \cap pr^{-1}(L) \quad (a \in \{0,1\}).$$

Отметим, что каждый из перечисленных замкнутых классов, кроме $L_{2,\infty}$, обладает конечным базисом.

Теорема 2. *Пусть H — замкнутый класс из $P_{3,2}$, причем $prH = L$ и $H \neq L_{2,\infty}$. Тогда существует конечный базис G класса H и константа c (зависящая от G) такая, что: $D_G(n) \sim cn$ в случае $H \in \{pr^{-1}(L), L_2\}$ и $D_G(n) \sim c\log n$ в случае $H \in \{L_{2,r}, Z_{2,a} \cap pr^{-1}(L)\}$.*

Таким образом, из теорем 1 и 2 следует, что для замкнутого класса $H \subseteq P_{3,2}$, проекция которого совпадает с P_2 или является предполным классом в P_2, и любого конечного базиса G класса H величина $D_G(n)$ имеет либо логарифмический, либо линейный порядок роста по числу переменных.

Автор выражает благодарность А. Б. Угольникову за постановку задачи и внимание к работе.

Список литературы

1. Угольников А. Б. О глубине формул в неполных базисах // Математические вопросы кибернетики. Вып. 1. — М.: Наука, 1988. — С. 242–245.

2. Угольников А. Б. О сложности реализации формулами одной последовательности функций 4-значной логики // Вестник Московского Университета. Сер. 1, Математика. Механика. — 2004. — № 3. — С. 52–55.

3. Post E. L. Introduction to a general theory of elementary propositions // American Journ. Mathem. — 1921. — V. 43. — C. 163–185.

4. Post E. L. Two-valued iterative system of mathematical logic // Annals of Math Studies. — London: Princeton Univ. Press, 1941. — № 5.

5. Lau D. Funktionenalgebren über endlichen Mengen. — Berlin: Springer, 2004.

6. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2003.

ОБ ОДНОМ ПОДХОДЕ К СИНТЕЗУ КЛЕТОЧНЫХ СХЕМ

Т. Н. Евдокимова (Москва)

Широко известны такие модели вычисления дискретных функций, как схемы из функциональных элементов (СФЭ) и контактные схемы (КС). Их сложность (число функциональных элементов и контактов) исследовалась во многих работах. Однако, в ряде случаев необходимо учитывать то, что реальные схемы располагаются в пространстве, их элементы и соединения занимают определенный объем, имеют конкретные геометрические размеры. В частности, при реализации дискретных функций интегральными схемами одним из важнейших параметров схемы является ее площадь.

В работе [1] рассматриваются СФЭ, размещенные на плоскости, в которой критерием сложности схемы являлась занимаемая ею площадь. Для данной модели схем найдены точные по порядку значения функции Шеннона, а также сложности реализации некоторых конкретных булевых функций и систем булевых функций. Для этой же модели, а также более общей модели в работе [2] найдена асимптотика сложности реализации некоторых систем булевых функций.

В работах [3, 4] рассмотрены две модели вложения в прямоугольную решетку контактных схем, причем в первой из этих моделей отсутствуют проводники, по которым передаются управляющие воздействия (значения переменных) к каждому контакту схемы, а во второй модели эти проводники составляют отдельный слой схемы. В [3] установлено асимптотическое поведение функции Шеннона в первой из указанных моделей, а в [4] получены совпадающие по порядку нижняя и верхняя оценка для функции Шеннона во второй модели.

В [5] рассмотрена модель вложения контактных схем в прямоугольную решетку, которая близка к модели клеточных схем из функциональных элементов и наиболее удобна для теоретических исследований. В данной модели проводники, по которым передаются управляющие воздействия к каждому контакту схемы и осуществляются соединения контактов, представлены обычными коммутационными элементами. Под сложностью (длиной, высотой) клеточной КС Σ понимается площадь (соответственно длина, высота) минимального по включению содержащего ее прямоугольника рассматриваемой решетки и обозначается эта величина через $A(\Sigma)$ (соответственно $\lambda(\Sigma)$ и $h(\Sigma)$). Сложностью $A(F)$ системы функций алгебры логики F называется минимальная сложность реализующих ее клеточных КС. В этой модели получена асимптотика сложности реализации системы всех элементарных конъюнкций ранга n от n булевых переменных и системы всех функций от n переменных.

В настоящей работе обобщается и уточняется [2, 5] один подход к синтезу клеточных схем, позволяющий получать асимптотически точные верхние оценки для сложности некоторых систем функций алгебры логики (ФАЛ).

Предполагается, что исходная система ФАЛ допускает разложение на две системы ФАЛ, которые реализуются отдельными схемами. При этом схема, соответствующая первой подсистеме ФАЛ строится с оптимальной высотой и "приемлемой" длиной, а схема, соответствующая второй подсистеме ФАЛ — с оптимальной длиной и "приемлемой" высотой. После синтеза указанных схем искомая схема получается в результате соответствующей операции суперпозиции.

Введем некоторые обозначения, которые используются при формулировке результатов. Положим $B = \{0,1\}$, $x = (x_1, \ldots, x_n)$, $P_2(x) = \{f(x) : B^n \to B\}$, а $P_2^m(x)$ — множество наборов длины m из ФАЛ множества $P_2(x)$ и обозначим через $\overrightarrow{P_2}(x)$ — систему всех ФАЛ, зависящих от x, а через $\overrightarrow{T_1}(x)$ ($\overrightarrow{T_0}(x)$) — систему всех ФАЛ, зависящих от x, и сохраняющих единицу(соответственно ноль).

Теорема 1. *Пусть система* $F = (f_1, \ldots, f_m) \in P_2^m(x)$, $x' = (x_1, \ldots, x_k)$, $x'' = (x_{k+1}, \ldots, x_n)$ *и пусть выполняются следующие условия:*

1) *существует система* $F' = (f'_1, \ldots, f'_{m'}) \in P_2^{m'}(x')$ *и система* $F'' = (f''_1, \ldots, f''_{m''}) \in P_2^{m''}(x'')$, *такие, что для любого* $i \in [1, m]$, *существует* $j \in [1, m']$ *и существует* $\ell \in [1, m'']$ *для которых* $f_i(x', x'') = f''_j(x'', f_\ell(x'))$;

2) *существует схема* Σ', *реализующая систему* F' *и такая, что* $h(\Sigma') = k + O(1)$, $\lambda(\Sigma') \le Cm'$;

3) *существует схема* Σ'', *реализующая систему* F'' *и такая, что* $h(\Sigma'') \le C_1(n-k)$, $\lambda(\Sigma'') \le m'' + C_2$.

Тогда существует схема Σ, *реализующая систему* F *и для которой* $A(\Sigma) \le (\frac{1}{2} + o(1))nm$

Заметим, что для систем всех элементарных конъюнкций и всех элементарных дизъюнкций ранга n от n булевых переменных выполняются условия указанной теоремы, и для сложности реализации любой из данных систем функций получается асимптотическая верхняя оценка вида $\frac{1}{2}n2^n$.

Теорема 2. *Пусть множество* $M = \{\alpha_1, \ldots, \alpha_\ell\} \subseteq B^n$, *набор* $\gamma = (\gamma_1, \ldots, \gamma_\ell) \in B^\ell$ *и система* $F = (f_1, \ldots, f_m) \in P_2^m(x_1, \ldots, x_n)$, *где* $m = 2^{2^n - \ell}$, *удовлетворяют следующим условиям:*

1) *для каждого* $i \in [1, \ell]$ *и каждого* $j \in [1, m]$ $f_j(\alpha_i) = \gamma_i$;

2) *на наборах множества* $B^n \backslash M$ *функции из системы* F *принимают произвольные значения.*

Тогда при $\ell \in [0, 2^n - C\sqrt{n}\log n]$, *существует схема* Σ, *реализующая систему* F *и для которой* $A(\Sigma) \le (\frac{1}{2} + o(1))nm$.

Следствие. *Для сложностей* $A(\overrightarrow{P_2}(x))$, $A(\overrightarrow{T_0}(x))$ *и* $A(\overrightarrow{T_1}(x))$ *имеют место неравенства*

$A(\overrightarrow{P_2}(x)) \le (\frac{1}{2} + o(1))n2^{2^n}$, $A(\overrightarrow{T_0}(x)) \le (\frac{1}{2} + o(1))n2^{2^n-1}$ *и* $A(\overrightarrow{T_1}(x)) \le (\frac{1}{2} + o(1))n2^{2^n-1}$.

Теорема 3. *Если* F — *система всех самодвойственных функций, то* $A(F) \le (\frac{1}{2} + o(1))n2^{2^n-1}$.

Работа выполнена при финансовой поддержке РФФИ (проект 06-01-00745).

Список литературы

1. Шкаликова Н. А., О реализации булевых функций схемами из клеточных элементов // Математические вопросы кибернетики. Вып. 2. — 1989. — С. 177–197.

2. Ложкин С. А., Пашковский А. М. О сложности реализации некоторых систем функций алгебры логики клеточными и планарными схемами // Проблемы теоретической кибернетики. Тезисы докладов IX Всесоюзн. конф. 1990. Часть I. — 1991. — С. 28.

3. Задорожнюк О. А., Рыбко А. И. Об одной модели плоских контактных схем // Дискретная математика. — 1995. — Вып. 4, № 7. — С. 40–50.

4. Задорожнюк О. А., О контактных схемах из клеточных элементах // Математические вопросы кибернетики. Вып. 6. — 1996. — С. 257–280.

5. Ложкин С. А., Евдокимова Т. Н. Об асимптотике сложности универсального клеточного контактного многополюсника // Вестник МГУ. Сер. 15. Вычислительная математика и кибернетика. — 2005. — № 4. — С. 30–38.

АЛГОРИТМ ПОСТРОЕНИЯ МИНИМАЛЬНОГО РАЗРЕШАЮЩЕГО МНОЖЕСТВА ПОРОГОВОЙ ФУНКЦИИ МНОГОЗНАЧНОЙ ЛОГИКИ

Н. Ю. Золотых, М. А. Илюшина (Нижний Новгород)

Пусть $E_k = \{0, 1, \ldots, k-1\}$. Функция $f : E_k^n \to \{0, 1\}$ называется *пороговой*, если существуют числа $a_0, a_1, \ldots, a_n$, такие, что

$$\{x \in E_k^n : f(x) = 0\} = \{x \in E_k^n : \sum_{j=1}^{n} a_j x_j \le a_0\}.$$

Множество всех пороговых функций, заданных на гиперкубе E_k^n, обозначим $F(n, k)$.

Разрешающим множеством функции $f \in F(n, k)$ называется такое $T \subseteq E_k^n$, что для произвольной функции $g \in F(n, k) \setminus \{f\}$ найдется точка $z \in T$, такая, что $f(z) \ne g(z)$. Разрешающее множество функции f называется *минимальным*, если никакое его собственное подмножество не является разрешающим для функции f. Известно, что для любой пороговой функции f минимальное разрешающее множество единственно. Минимальное разрешающее множество функции f обозначим $T(f)$. *Длиной обучения* называется величина

$$\sigma(n, k) = \max_{f \in F(n,k)} |T(f)|.$$

В [3] на основе [4] и [5] установлено, что если n фиксировано и $k \to \infty$, то $\sigma(n, k) = O(\log^{n-1} k)$. В [1, 2] доказано, что если n фиксировано и $k \to \infty$, то $\sigma(n, k) = \Omega(\log^{n-2} k)$. В [1, 6] доказано, что $\sigma(2, k) = 4$ при $k \ge 2$. В [7] установлено, что $\sigma(3, k) = \Theta(\log k)$ при $k \to \infty$.

Авторами настоящей заметки на основе [4] построен полиномиальный при фиксированном n алгоритм, который по заданным числам $a_0, a_1, \ldots, a_n$ строит минимальное разрешающее множество $T(f)$ для функции f. Трудоемкость алгоритма — $O(\log^{n+1} k)$ арифметических операций при $k \to \infty$.

Работа поддержана грантом РФФИ 05-01-00552-а.

Список литературы

1. Шевченко В. Н., Золотых Н. Ю. О сложности расшифровки пороговых функций k-значной логики // Доклады РАН. — 1998. — Т. 362, № 5. — С. 606–608.

2. Золотых Н. Ю., Шевченко В. Н. О нижней оценке расшифровки пороговых функций k-значной логики // Журнал вычислительной математики и математической физики. — 1999. — Т. 39, № 2. — С. 346–352.

3. Hegedüs T. Geometrical concept learning and convex polytopes // Proceedings of the 7th Annual ACM Conference on Computational Learning Theory (COLT'94). — New York: ACM Press, 1994. — P. 228–236.

4. Шевченко В. Н. О расшифровке пороговых функций многозначной логики // Комбинаторно-алгебраические методы в прикладной математике. — Горький: Горьковский гос. ун-т, 1987. — С. 155–163.

5. Cook W., Hartmann M., Kannan R., McDiarmid C. On integer points in polyhedra // Combinatorica. — 1992. — V. 12, № 1. — P. 27–37.

6. Золотых Н. Ю. О сложности расшифровки пороговых функций, зависящих от двух переменных // Материалы XI Межгосударственной школы-семинара "Синтез и сложность управляющих систем". Часть I. — М.: Изд-во Центра прикладных исследований при механико-математическом ф-те МГУ, 2001. — С. 74–79.

7. Вировлянская М. А., Золотых Н. Ю. О мощности разрешающего множества пороговой функции многозначной логики // Материалы XIV Международной школы-семинара "Синтез и сложность управляющих систем". — Нижний Новгород: Издательство Нижегородского государственного педагогического университета, 2003. — С. 20–21.

О СЛОЖНОСТИ РЕАЛИЗАЦИИ СИСТЕМ ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ, СООТВЕТСТВУЮЩИХ НЕКОТОРЫМ ЦИКЛИЧЕСКИМ МАТРИЦАМ

К. А. Зыков (Москва)

Рассматривается реализация систем функций k-значной логики схемами из функциональных элементов в базисе из элементов, имеющих не более двух входов. Элементы с одним входом реализуют перестановки. Элементы с двумя входами реализуют перестановки при любой фиксации любых входных переменных (т. е. базис содержит такие функции $h(x,y)$, что для всех x_0, y_0 каждая из функций $h(x_0,y)$, $h(x,y_0)$ принимает все k своих значений). Отметим, что данный базис является полным при $k>3$ и не является полным при $k=3$.

Мы будем рассматривать реализацию систем функций, удовлетворяющих специальному ограничению на взаимное расположение существенных переменных. Оно задается циклической матрицей $M_{r,n}$ с элементами

$$m_{1,1}=\cdots=m_{1,r}=1,\quad m_{1,r+1}=\cdots=m_{1,n}=0,$$

$$m_{i,1}=m_{i-1,n},\quad m_{i,j}=m_{i-1,j-1}\text{ при }i,j=2,\ldots,n.$$

Приведем пример матрицы $M_{r,n}$ при $n=5$, $r=3$:

$$\begin{pmatrix}1&1&1&0&0\\0&1&1&1&0\\0&0&1&1&1\\1&0&0&1&1\\1&1&0&0&1\end{pmatrix}.$$

Через $M_{r,n}^{i_1,\ldots,i_d}$ обозначим матрицу размера $n\times d$, которая получается из матрицы $M_{r,n}$ вычеркиванием всех столбцов, кроме столбцов с номерами $i_1,\ldots,i_d$.

Пусть $\tilde{x}=x_1,\ldots,x_l$. Будем говорить, что структура существенных переменных системы функций $f_1(\tilde{x}),\ldots,f_n(\tilde{x})$ задается матрицей $M=(a_{i,j})$, если функция f_j $(j=1,\ldots,n)$ зависит от переменной x_i $(i=1,\ldots,l)$ тогда и только тогда, когда $a_{i,j}=1$. Далее номера функций и переменных будем брать по модулю n, т. е. будем считать $f_n=f_0$ и т. д.

Пусть структура существенных переменных системы $f_1(\tilde{x}),\ldots,f_n(\tilde{x})$ задается матрицей $M_{\frac{n}{2},n}$. Будем говорить, что для подсистемы $f_{i_1}(\tilde{x}),\ldots,f_{i_d}(\tilde{x})$ *выполняется условие* $(*)$, если для некоторого

j система функций $f_{i_1}, \ldots, f_{i_d}$ содержит функции f_j и f_{j+r} и не содержит ни одной из функций $f_{j+1}, \ldots, f_{j+r-1}$, либо $d = 4$ и система $f_{i_1}, \ldots, f_{i_d}$ совпадает с системой f_j, f_{j+a}, f_{j+r}, f_{j+a+r} для некоторых j и a.

Теорема. *Пусть $f_1(\tilde{x}), \ldots, f_n(\tilde{x})$ — произвольная система функций k-значной логики, структура существенных переменных которой задается матрицей $M_{r,n}$. Пусть, кроме того, $f_{i_1}(\tilde{x}), \ldots, f_{i_d}(\tilde{x})$ — подсистема системы $f_1(\tilde{x}), \ldots, f_n(\tilde{x})$, структура существенных переменных которой задается матрицей $M_{r,n}^{i_1,\ldots,i_d}$. Тогда при $r > 2$, $n - 1 \geq r \geq n/2$ и $d > 1$ имеет место соотношение $L(f_{i_1}, \ldots, f_{i_d}) \geq b + d + c$, где b — число ненулевых строк матрицы $M_r^{i_1,\ldots,i_d}$, а константа c определяется равенством*

$$c = \begin{cases} 2, & \text{если } r = n - 1 \text{ и } d > 2; \\ 4, & \text{если выполняется условие } (*); \\ 3, & \text{в остальных случаях.} \end{cases}$$

Легко видеть, что число b совпадает с числом переменных, от которых зависит хотя бы одна функция подсистемы $f_{i_1}(\tilde{x}), \ldots, f_{i_d}(\tilde{x})$.

Замечание 1. *Для $k = 3$ дополнительно требуется чтобы система $f_{i_1}(\tilde{x}), \ldots, f_{i_d}(\tilde{x})$ реализовывалась в рассматриваемом базисе.*

Замечание 2. *В случае $k = 2$ результат может быть распространен на базис из всех двувходовых элементов* [1, 2].

Замечание 3. *Утверждение теоремы остается верным, если при подсчете сложности не учитывать одновходовые элементы.*

Полученная в теореме нижняя оценка является в некотором смысле неулучшаемой, так как при $r = n/2$, $r = n/3$ и $r = n - 1$ для любых удовлетворяющих условию n, k и d найдутся системы линейных функций, для которых данная оценка является точной.

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994), программы поддержки ведущих научных школ РФ (проект НШ–5400.2006.1) и Франко-русского центра по прикладной математике и информатике им. А. М. Ляпунова при МГУ.

Список литературы

1. Зыков К. А. Реализация некоторых систем булевых функций схемами из двувходовых элементов // Дискретная математика. — Т. 5, вып. 3. — 1993. — С. 125–149.

2. Зыков К. А. О линейной нижней оценке сложности реализации некоторых систем булевых функций схемами из двувходовых элементов // Теоретические и прикладные аспекты математических исследований (сборник трудов конференции молодых ученых

механико-математического факультета МГУ). —М.: Из-во МГУ. — 1994. — С. 18–22.

ОЦЕНКИ ЧИСЛА ШАГОВ РЕШЕНИЯ НЕКОТОРЫХ ЗАДАЧ РАСПОЗНАВАНИЯ ОБРАЗОВ С ЛОГИЧЕСКИМИ ОПИСАНИЯМИ

Т. М. Косовская (Санкт-Петербург)

В работе [1] предложен логико-аксиоматический подход к решению задач распознавания образов. Пусть имеется множество Ω конечных множеств $\omega = \{\omega_1, \ldots, \omega_t\}$, которые в дальнейшем будем называть распознаваемыми объектами. Пусть также на элементах ω задан набор предикатов $p_1, \ldots, p_n$. Пусть задано разбиение множества Ω на M (возможно пересекающихся) классов $\Omega = \bigcup_{k=1}^{M} \Omega_k$.

Логическим описанием $S(\omega)$ объекта ω называется набор всех истинных постоянных формул вида $p_i(\overline{\tau})$ или $\neg p_i(\overline{\tau})$, выписанных для всех возможных частей τ объекта ω. Здесь и далее посредством $\overline{x}$ будем обозначать некоторое упорядочение конечного множества x.

Логическим описанием класса (ОК) Ω_k называется такая формула $A_k(\overline{x})$, что $A_k(\overline{x})$ содержит в качестве атомарных только формулы вида $p_i(\overline{y})$, где $y \subseteq x$; $A_k(\overline{x})$ не содержит кванторов; если истинна формула $A_k(\overline{\omega})$, то $\omega \in \Omega_k$. ОК всегда может быть записано в виде дизъюнкции простых конъюнкций атомарных формул.

С помощью построенных описаний предлагается решать следующие задачи распознавания образов.

Задача идентификации. *Проверить, принадлежит ли объект ω или его часть классу Ω_k.* Эта задача в [1] сведена к доказательству выводимости формулы $\exists\overline{y}(y \subseteq \omega \;\&\; A_k(\overline{y}))$ из описания распознаваемого объекта $S(\omega)$.

Задача классификации. *Найти все такие номера классов k, что $\omega \in \Omega_k$.* Эта задача в [1] сведена к доказательству выводимости формулы $\bigvee_{k=1}^{M} A_k(\overline{\omega})$ из описания распознаваемого объекта $S(\omega)$ с указанием всех таких номеров k, для которых соответствующий дизъюнктивный член истинен на ω.

Задача анализа сложного объекта. *Найти и классифицировать все части τ объекта ω, для которых $\tau \in \Omega$.* Эта задача в [1] сведена к доказательству выводимости формулы $\bigvee_{k=1}^{M} \exists\overline{y}(y \subseteq$

ω & $A_k(\overline{y})$) из описания распознаваемого объекта $S(\omega)$ с указанием всех частей объекта ω, поддающихся классификации, и идентифицировать их.

В случае, если исходные признаки характеризуют весь объект целиком, а не его части, предикаты $p_1, \ldots, p_n$ можно рассматривать как пропозициональные (или булевы) переменные. Тогда описанием класса является формула A_k в ДНФ с пропозициональными переменными $p_1, \ldots, p_n$.

Теорема 1. *Для всякого целого положительного числа n можно построить машину Тьюринга, которая по набору логических констант $(\alpha_1, \ldots, \alpha_n)$ и формуле в ДНФ A_k проверит, истинна ли эта формула при подстановке заданных констант вместо соответствующих пропозициональных переменных. При этом число шагов такой машины Тьюринга не превосходит длины записи исходных данных.*

Следствие теоремы 1. *Если заданы описания классов в терминах признаков, глобально характеризующих распознаваемые объекты, то задачи идентификации и классификации принадлежат классу LIN-TIME.*

В более общем случае, когда число n не зафиксировано и описания классов являются исходными данными, можно доказать, что задача принадлежит классу **P** (причем полином имеет небольшую, равную 4, степень).

Оценка временно́й сложности работы алгоритма в терминах числа шагов работы машины Тьюринга общепринята в алгоритмической теории сложности алгоритмов, но это не выглядит естественным при решении задач, предназначенных для практического программирования.

Теорема 2. *Количество применений как правила резолюций при использовании линейной стратегии метода резолюций так и правил вывода при построении вывода в секвенциальном исчислении высказываний для решения задачи классификации в случае, когда исходные признаки характеризуют весь объект, не превосходит суммарного количества вхождений пропозициональных переменных в формулы, задающие описания классов.*

В случае, если исходные признаки являются локальными, то есть характеризуют не весь объект целиком, а его части, предикаты $p_1, \ldots, p_n$ являются многоместными и задают свойства и отношения между частями объекта. В общей постановке задачи не представляется возможным существенно избавиться от экспоненциального числа шагов ее решения, если P$\neq$NP [2], так как можно доказать NP-трудность рассматриваемых задач.

Выполнимость в конечной интерпретации.

Дано: Множество объектов $\omega = \{\omega_1, \ldots, \omega_t\}$ и набор истинных постоянных формул вида $p_i^{\alpha_{i,\overline{\tau}}}(\overline{\tau})$, где $i = 1, \ldots, n$, $\tau \subseteq \omega$, $\alpha_{i,\overline{\tau}}$ — логические константы. Бескванторная формула $A(\overline{y})$, представленная в виде дизъюнкции простых конъюнкций атомарных формул.

Вопрос: $\exists\overline{y}(y \subseteq \omega \ \& \ A(\overline{y}))$?

Теорема 3. *Задача «выполнимость в конечной интерпретации» NP-полна.*

Следствие теоремы 3. *Задача идентификации NP-трудна.*

Выполнимость на заданном множестве.

Дано: Множество объектов $\omega = \{\omega_1, \ldots, \omega_t\}$, набор истинных постоянных формул вида $p_i^{\alpha_{i,\overline{\tau}}}(\overline{\tau})$, где $i = 1, \ldots, n$, $\tau \subseteq \omega$, $\alpha_{i,\overline{\tau}}$ — логические константы. Бескванторная формула $A(\overline{y})$, представленная в виде дизъюнкции простых конъюнкций атомарных формул.

Вопрос: $\exists y_{i_1}, \ldots, y_{i_t}(\{y_{i_1}, \ldots, y_{i_t}\} = \omega \ \& \ A(y_{i_1}, \ldots, y_{i_t}))$?

Теорема 4. *Задача «выполнимость на заданном множестве» NP-полна.*

Следствие теоремы 4. *Задача классификации NP-трудна.*

Теорема 5. *Задача анализа сложного объекта NP-трудна.*

При решении конкретных задач распознавания описания классов не являются исходными данными для алгоритма и количество предметных переменных, входящих в формулы $A_k(\overline{y_k})$ фиксировано. В такой постановке задача идентификации может быть решена за полином от длины записи идентифицируемого объекта ω шагов, причем степень полинома равна количеству предметных переменных в $A_k(\overline{y})$. Задача классификации может быть решена за число шагов, равное достаточно большой константе $t!$. Задача анализа сложного объекта может быть решена за полином от длины записи распознаваемого объекта ω шагов, причем степень полинома не превосходит максимума от количества предметных переменных в описаниях классов.

Список литературы

1. Косовская Т. М., Тимофеев А. В. Об одном новом подходе к формированию логических решающих правил в задачах распознавания // Вестник ЛГУ. — 1985. — № 8. — С. 22–29.

2. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

ОБ ЭФФЕКТИВНОСТИ ПОЛУЧЕНИЯ БУЛЕВОГО РЕШЕНИЯ У ПОЛИНОМИАЛЬНЫХ СРАВНЕНИЙ И У СИСТЕМ ИЗ НИХ

Н. К. Косовский, Т. М. Косовская (Санкт-Петербург)

Приводятся пары похожих по формулировке задач, одна из которых полиномиальна по времени, а другая обобщает ее в NP-полную, причем последняя сводится традиционными математическими символьными преобразованиями к первой (по существу путем раскрытия скобок и приведения подобных членов).

Демонстрируется важность и необходимость аккуратной формулировки задачи, отделяющей NP-полные задачи от полиномиальных (в том числе отделяющей параметры серии задач от аргументов задачи (предиката), являющихся исходными данными для алгоритма, решающего эту задачу). Решаются частные случаи NP-полных задач, связанных с проверкой существования булевого решения у арифметических сравнений и несравнений (индивидуальные задачи), в краткой формулировке малого размера. Последнее, так же как и полиномиальные алгоритмы, предложенные здесь, весьма полезны при практическом программировании (см., также [1]).

Задача 1. Несравнимость с нулем полинома.

Пусть P — полином с целыми коэффициентами и, возможно, несколькими переменными, задаваемый суммой одночленов с ненулевыми коэффициентами, записанными в позиционной системе счисления. При этом в каждом одночлене присутствуют только те переменные, которые имеют ненулевые показатели степени, записанные в позиционной системе счисления. Пусть также m — целое число, записанное в позиционной системе счисления ($m \geq 2$).

Верно ли, что

$$\exists \overline{x}_{\in\{0,1\}^*}(P(\overline{x}) \not\equiv 0(mod\ m))?$$

Теорема. *Алгоритм решения задачи 1 может быть реализован на детерминированной машине Тьюринга за число шагов, не превосходящее полинома от длины записи P и m.*

Замечание. Аналогичный полиномиальный по времени алгоритм позволяет решать задачу о неравенстве нулю полинома: $\exists \overline{x}_{\in\{0,1\}^*}(P(\overline{x}) \neq 0)$.

Серия задач 2. Несравнимость с нулем системы двучленов по фиксированному модулю.

Параметром этой серии задач является число m ($m \geq 2$).

Пусть $B_1, \ldots, B_k$ — система двучленов, возможно, с несколькими переменными, состоящих из суммы или разности двух одночленов с целыми положительными коэффициентами. При этом в каждом двучлене присутствуют только те переменные, которые имеют ненулевые показатели степени, записанные в позиционной системе счисления.

Верно ли, что

$$\exists \overline{x}_{\in\{0,1\}^*}(B_1(\overline{x}) \not\equiv 0(mod\ m)\& \ldots \& B_k(\overline{x}) \not\equiv 0(mod\ m))?$$

При каждом фиксированном k ($k \geq 1$) эта задача имеет полиномиальный алгоритм решения, если m — простое число.

Замечание. Является NP-полной задача

$$\exists \overline{x}_{\in\{0,1\}^*}(B_1(\overline{x}) \neq 0 \ldots B_k(\overline{x}) \neq 0),$$

где $B_1, \ldots, B_k$ — система двучленов, состоящих из суммы или разности двух одночленов и число k входит в исходные данные для задачи.

Однако при каждом фиксированном k эта задача может быть решена с помощью полиномиального по времени алгоритма. Для этого достаточно перемножить полиномы $P_1, \ldots, P_k$ с последующим приведением подобных членов (что можно сделать за полином шагов, степень которого растет с ростом k) и воспользоваться замечанием к теореме.

Серия задач 3. Несравнимость с нулем арифметического выражения по фиксированному простому модулю.

Параметром этой серии задач является число m ($m \geq 2$).

Пусть A — арифметическое выражение (терм), возможно, с несколькими переменными, содержащее функции $+$, $-$, $\cdot$ и числа, записанные в позиционной системе счисления.

Верно ли,что

$$\exists \overline{x}_{\in\{0,1\}^*}(A(\overline{x}) \not\equiv 0\ (mod\ m))?$$

Утверждение 1. *При любом простом m ($m \geq 2$) каждая задача из серии задач 3 NP-полна.*

Замечание. Задача $\exists \overline{x}_{\in\{0,1\}^*}(A(\overline{x}) \neq 0)$ является NP-полной.

Серия задач 4. Сравнимость с нулем полинома по фиксированному простому модулю.

Каждая задача серии определяется параметром серии, который является простым числом p.

Пусть P — полином с целыми коэффициентами и, возможно, несколькими переменными, задаваемый суммой одночленов с ненулевыми коэффициентами, записанными в позиционной системе счисления. При этом в каждом одночлене присутствуют только те переменные, которые имеют ненулевые показатели степени, записанные в позиционной системе счисления.

Верно ли, что

$$\exists \overline{x}_{\in\{0,1\}^*}(P(\overline{x}) \equiv 0 \ (mod\ p))?$$

Иначе говоря, по полиному P с несколькими переменными и с приведенными подобными членами определить, сравнимо ли по модулю p с нулем значение полинома на некотором наборе значений аргументов из $\{0,1\}^*$.

Следствие теоремы. *Для решения каждой задачи из серии задач* 4 *имеется полиномиальный по времени алгоритм.*

Отметим, что при большом значении простого числа p число шагов полиномиального алгоритма ограничено сверху полиномом большой степени.

Замечание. Задача $\exists \overline{x}_{\in\{0,1\}^*}(P(\overline{x}) = 0)$ является NP-полной.

Задача 5. Сравнимость с нулем полинома.

Задача 5 отличается от задач из серии 4 внесением параметра p в исходные данные для задачи 5.

Утверждение 2. *Задача* 5 *NP-полна.*

Список литературы

1. Arvind V., Vijayarughavan T. C. The complexity of solving linear equations over a finite ring // STACS 2005. — LNCS 3404. — Berlin: Springer, 2005.

ОБ АДДИТИВНОЙ СЛОЖНОСТИ ЦЕЛОЧИСЛЕННЫХ МАТРИЦ РАЗМЕРА 3×2

В. В. Кочергин (Москва)

Для произвольной целочисленной матрицы $A = (a_{ij})$ размера $p \times q$ определим величину $l_F(A)$ — *аддитивную сложность* (F-*сложность*) матрицы A, используя язык аддитивных цепочек (см, например, [1]). Назовем *аддитивной F-цепочкой* для матрицы A последовательность q-мерных векторов (наборов) вида

$$\mathbf{v}_1 = (1, 0, \ldots, 0),\ \mathbf{v}_2 = (0, 1, \ldots, 0),\ \ldots, \mathbf{v}_q = (0, 0, \ldots, 1),$$

$$\mathbf{v}_{q+1} = (-1, 0, \ldots, 0),\ \mathbf{v}_{q+2} = (0, -1, \ldots, 0),\ \ \ldots, \mathbf{v}_{2q} = (0, 0, \ldots, -1),$$
$$\mathbf{v}_{2q+1}, \mathbf{v}_{2q+2}, \ldots, \mathbf{v}_{2q+r},$$

начинающуюся с $2q$ единичных и обратных к ним векторов и удовлетворяющую условиям:

1) для каждого k, $2q+1 \le k \le 2q+r$, найдется два натуральных числа (не обязательно различных) i и j, $1 \le i \le k-1$, $1 \le j \le k-1$, таких, что $\mathbf{v}_k = \mathbf{v}_i + \mathbf{v}_j$ (сложение векторов покомпонентное);

2) $\{(a_{11}, a_{12}, \ldots a_{1q}), \ldots, (a_{p1}, a_{p2}, \ldots a_{pq})\} \subseteq \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2q+r}\}$.

Число r называется длиной этой цепочки. Величина $l_F(A)$ определяется как минимальная длина аддитивных F-цепочек для матрицы A.

Отметим, что величина $l_F(A)$ численно равна наименьшему числу операций умножения в свободной («free» — отсюда символ «F» в обозначении) абелевой группе с образующими $g_1, g_2, \ldots, g_q$, достаточному для вычисления по самим образующим и обратным к ним элементам системы элементов $g_1^{a_{11}} g_2^{a_{12}} \ldots g_q^{a_{1q}}$, $g_1^{a_{21}} g_2^{a_{22}} \ldots g_q^{a_{2q}}, \ldots, g_1^{a_{p1}} g_2^{a_{p2}} \ldots g_q^{a_{pq}}$. Величину $l_F(A)$ можно также интерпретировать как минимально возможную сложность схемы из функциональных элементов [2], на входы которой подаются функции $\{x_1, x_2, \ldots, x_q, x_1^{-1}, x_2^{-1}, \ldots, x_q^{-1}\}$, на выходах схемы вычисляются функции $x_1^{a_{11}} x_2^{a_{12}} \ldots x_q^{a_{1q}}$, $x_1^{a_{21}} x_2^{a_{22}} \ldots x_q^{a_{2q}}, \ldots,$ $x_1^{a_{p1}} x_2^{a_{p2}} \ldots x_q^{a_{pq}}$, а сама схема состоит из двухвходовых элементов, реализующих произведение функций, подаваемых на входы элемента.

Введенная мера l_F сложности целочисленных матриц близка мерам сложности l и l_2, рассматривавшимся в работах [3, 4], но имеет и принципиальные отличия от них, в частности, не обладает свойством двойственности [4]. В общем виде задача нахождения асимптотики роста величины $l_F(A)$ (с ростом, например, максимума абсолютных значений элементов матрицы) представляется довольно сложной. В данной работе она решена для случая $p = 3$, $q = 2$.

Пусть число k удовлетворяет неравенствам $1 \le k \le \min(p, q)$. Для наборов индексов $(i_1, i_2, \ldots, i_k)$ и $(j_1, j_2, \ldots, j_k)$, таких что $1 \le i_1 < i_2 < \ldots < i_k \le p$, $1 \le j_1 < j_2 < \ldots < j_k \le q$, обозначим через $A(i_1, i_2, \ldots, i_k;\, j_1, j_2, \ldots, j_k)$ квадратную матрицу порядка k, состоящую из элементов, находящихся на пересечении k строк с номерами $i_1, i_2, \ldots, i_k$ и k столбцов с номерами $j_1, j_2, \ldots, j_k$. Положим

$$D(A) = \max_k \left\{ \max_{(i_1, \ldots, i_k;\, j_1, \ldots, j_k)} |\det A(i_1, \ldots, i_k;\, j_1, \ldots, j_k)| \right\},$$

$$T(A) = \max_{j:\ 1 \le j \le q} \left\{ \max\{a_{1j}, a_{2j}, \ldots, a_{pj}, 0\}\, |\min\{a_{1j}, a_{2j}, \ldots, a_{pj}, 0\}| \right\}.$$

Таким образом, $D(A)$ — это максимум абсолютных величин миноров матрицы A, где максимум берется по всем минорам, а $T(A)$ — это максимум абсолютных величин попарных произведений элементов матрицы A, где максимум берется по всем парам элементов, удовлетворяющих двум условиям — эти элементы должны находиться в одном столбце и иметь разные знаки.

Из результатов работы [5] следует справедливость для матриц размера $2 \times q$ сотношений (здесь и далее $\log x$ означает $\log_2 x$)

$$\log \max\{D(A), T(A)\} \le l_F(A) \le \log \max\{D(A), T(A)\} + O\left(\frac{q \log \max |a_{ij}|}{\log \log \max |a_{ij}|}\right).$$

В случае $p = 3$ даже при $q = 2$ ситуация принципиально меняется. Далее считаем, что целочисленная матрица A имеет размер 3×2.

Для удобства под записью a_{st} при $s > 3$ и/или $t > 2$ будем понимать элемент a_{ij}, где i и j определяются из условий $1 \le i \le 3$, $i \equiv s \pmod 3$; $1 \le j \le 2$, $j \equiv t \pmod 2$. Обозначим через $A(s,t)$ матрицу размера 2×2, в которой первой строкой является строка матрицы A, содержащая элемент a_{s1}, а второй — строка матрицы A, содержащая элемент a_{t1}.

Элемент a_{ij} матрицы A размера 3×2 назовем *особым*, если выполняются следующие условия: $a_{ij} \ne 0$, $a_{ij}a_{i+1,j} \le 0$, $a_{ij}a_{i+2,j} \le 0$, $|a_{i+1,j}| + |a_{i+2,j}| \ne 0$. Для особого элемента a_{ij} матрицы A размера 3×2 определим величину $r(a_{ij})$ таким образом:

1) если выполняются неравенства $\det A(i+1, i+2) \det A(i+2, i) \ge 0$ и $\det A(i+1, i+2) \det A(i, i+1) \ge 0$, то полагаем

$$r(a_{ij}) = |a_{ij} \det A(i+1, i+2)|;$$

2) если выполняется неравенство $\det A(i+1, i+2) \det A(i+2, i) < 0$, то полагаем

$$r(a_{ij}) = |a_{ij} \det A(i+1, i+2)| \frac{\max\{|a_{i1}|, |a_{i2}|, |a_{i+2,1}|, |a_{i+2,2}|\}}{D(A(i+2, i))};$$

3) если выполняется неравенство $\det A(i+1, i+2) \det A(i, i+1) < 0$, то полагаем

$$r(a_{ij}) = |a_{ij} \det A(i+1, i+2)| \frac{\max\{|a_{i1}|, |a_{i2}|, |a_{i+1,1}|, |a_{i+1,2}|\}}{D(A(i, i+1))}.$$

Для элементов a_{ij}, не являющихся особыми в целочисленной матрице A размера 3×2, положим $r(a_{ij}) = 0$. Теперь для матрицы A определим величину $R(A)$ равенством

$$R(A) = \max_{a_{ij} \in A} r(a_{ij}).$$

Теорема. *Пусть последовательность* $A(n) = (a_{ij}(n))$ *ненулевых целочисленных матриц размера* 3×2 *удовлетворяет условию*

$$\max_{a_{ij} \in A(n)} |a_{ij}| \to \infty \quad \textit{при} \quad n \to \infty.$$

Тогда справедливы соотношения:

$$\log \max\{D(A_n), T(A_n), R(A_n)\} \le l_F(A_n) \le$$
$$\le (1 + o(1)) \log \max\{D(A_n), T(A_n), R(A_n)\}.$$

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994) и программы поддержки ведущих научных школ РФ (проект НШ–5400.2006.1).

Список литературы

1. Кнут Д. Е. Искусство программирования для ЭВМ, т. 2 — М.: Мир, 1977.

2. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики, вып. 14. — М.: Наука, 1965. — С 31–110.

3. Кочергин В. В. Об асимптотике сложности аддитивных вычислений систем целочисленных линейных форм // Дискретный анализ и исследование операций. Серия 1. — 2006. — Т. 13, № 2. — С. 38–58.

4. Кочергин В. В. О сложности совместного вычисления трех одночленов от трех переменных // Математические вопросы кибернетики, вып. 15. — М.: Физматлит, 2006. — С. 79–155.

5. Кочергин В. В. О сложности совместного вычисления двух элементов свободной абелевой группы // Материалы XVI Международной школы-семинара «Синтез и сложность управляющих систем» (Санкт-Петербург, 26–30 июня 2006 г.). — М.: Изд-во механико-математического факультета МГУ, 2006. — С. 54–59.

О ГЛУБИНЕ МУЛЬТИПЛЕКСОРНОЙ ФУНКЦИИ

С. А. Ложкин, Н. В. Власов (Москва)

Рассматривается задача оптимальной по глубине реализации мультиплексорной функции алгебры логики (ФАЛ) в классе формул и схем из функциональных элементов (СФЭ) (понятия, которые

в данной работе не определяются, могут быть найдены, например, в [1, 2]).

Мультиплексорной ФАЛ (мультиплексором) μ_n порядка n называется ФАЛ от $n + 2^n$ булевых переменных (БП), где первые n переменных называются "адресными", оставшиеся 2^n — "информационными", а значение функции равно значению той его информационной БП, номер которой задаётся значениями адресных БП.

Задача синтеза решается в классе формул или СФЭ с поднятыми отрицаниями в стандартном базисе $Б_0 = \{x\&y, x \vee y, \bar{x}\}$, причём в качестве меры сложности используется глубина формул или СФЭ, а глубина базисных функциональных элементов (ФЭ) "&" и "$\vee$" считается равной 1, а ФЭ "$\neg$" — равной 0.

Сложность мультиплексорной функции изучалась в ряде работ, например, в [3, 4], где, в частности, была установлена асимптотика сложности ФАЛ μ_n в классе СФЭ как в базисе $Б_0$, так и в базисе $\{x\&y, x \oplus y, \bar{x}\}$. Кроме того, для указанной сложности в базисе $Б_0$ в [5] были получены оценки достаточно высокой степени точности. Что касается глубины, то в работе [6] было доказано, что глубина ФАЛ μ_n в базисе $Б_0$ не превосходит величины $n+4$ для случая единичной глубины всех ФЭ и не превосходит $n+3$ в рассматриваемой модели.

В связи с тем, что в результате применения тождества ветвления и тождеств де Моргана [2, гл. 3, §1], всякую СФЭ в базисе $Б_0$ можно преобразовать в формулу той же глубины, достаточно рассмотреть только формулы в базисе $Б_0$, причём только формулы с поднятыми отрицаниями. Через $D(f)$ будем обозначать минимальную глубину формул указанного вида, реализующих ФАЛ f.

Теорема.

$$D(\mu_n) = \begin{cases} 2, & \textit{если} \;\; n = 1; \\ n+2, & \textit{если} \;\; 1 < n \leqslant 5, \;\; n \geqslant 25. \end{cases}$$

Доказательство верхней оценки проводится непосредственным построением формулы. Для случаев $n = 1, ..., 5$ формулы требуемой глубины получаются с использованием стандартных тождеств. Для случая $n \geqslant 25$ набор адресных БП $x = (x_1, ..., x_n)$ делится на поднаборы $x' = (x_1, ..., x_q)$, где $q < n$, и $x'' = (x_{q+1}, ..., x_n)$. При этом для единичного куба B^q от БП x' строится его специальное m-регулярное [2] разбиение $\Delta = (\delta_1, ...\delta_{2^{q-m}})$ такое, что для любого натурального i, $i \in [1, 2^{q-m}]$, и любого набора $\sigma' = (\sigma_1, ..., \sigma_q)$ из δ_i элементарная конъюнкция $K_{\sigma'}(x') = x_1^{\sigma_1} ... x_q^{\sigma_q}$ совпадает на δ_i с ФАЛ

вида $x_{j_{i,\sigma'}}^{\alpha_{i,\sigma'}}$, где $m+1 \leqslant j_{i,\sigma'} \leqslant q$ и $\alpha_{i,\sigma'} \in \{0,1\}$. На базе указанного разбиения мультиплексорная ФАЛ μ_n представляется в виде:

$$\mu_n(x,y) = \bigvee_{i=1}^{2^{q-m}} \chi_{\delta_i}(x') \left(\mathop{\&}_{\sigma'' \in B^{n-q}} \left(J_{\sigma''}(x'') \bigvee \mathop{\vee}_{\sigma' \in \delta_i} y_{\nu(\sigma',\sigma'')} \cdot x_{j_{i,\sigma'}}^{\alpha_{i,\sigma'}} \right) \right), \quad (1)$$

где $y = (y_0, ..., y_{2^n-1})$ — набор информационных БП, $\chi_{\delta_i}(x')$ — характеристическая ФАЛ δ_i, $J_{(\sigma_{q+1},\ldots,\sigma_n)}(x'') = x_{q+1}^{\overline{\sigma}_{q+1}} \vee ... \vee x_n^{\overline{\sigma}_n}$ и $\nu(\sigma', \sigma'')$ — номер набора (σ', σ''), то есть целое число из отрезка $[0, 2^n-1]$, двоичная запись которого совпадает с этим набором.

Для оптимальной по глубине реализации представления (1) используются приёмы [7], связанные с исключением из этого представления части слагаемых (сомножителей), связанных с некоторыми наборами σ' (соответственно, σ''), для получения подформул оптимальной глубины. При этом строится специальная формула, реализующая "часть" ФАЛ μ_n, связанную с "исключёнными" наборами, которая затем дизъюнктируется с формулой, соответствующей оставшейся части представления (1).

Нижняя оценка основана на технике незабиваемых переменных ФАЛ (для мультиплексорной ФАЛ информационные переменные образуют незабиваемое множество переменных) и соответствующих оценках сложности и глубины (см., например, [2, 3]).

Работа выполнена при финансовой поддержке РФФИ — проект 06-01-00745.

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: изд-во МГУ, 1984.

2. Ложкин С. А. Лекции по основам кибернетики. — М.: Издательский отдел ф-та ВМиК МГУ, 2004.

3. Алексеев В. Б., Ложкин С. А. Элементы теории графов, схем и автоматов. — М.: Издательский отдел ф-та ВМиК МГУ, 2000.

4. Коровин В. В. О сложности реализации универсальной функции схемами из функциональных элементов // Дискретная математика. — 1995. — Т. 7, вып. 2. — С. 95–102.

5. Румянцев П. В. О сложности реализации мультиплексорной функции схемами из функциональных элементов. // Проблемы теоретической кибернетики. Тезисы докладов XIV международной конференции (Пенза, 23–28 мая 2005 г.). М.: Изд-во механико-математического факультета МГУ, 2005. — С. 133.

6. Ложкин С. А. О синтезе формул, сложность и глубина которых не превосходят асимптотически наилучших оценок высокой степени точности // Вестн. Моск. ун-та. Сер. 1. Математика. Механика. — 2007. — № 3. — С. 20–26.

7. Ложкин С. А. О глубине функций алгебры логики в некоторых базисах // Annal. Univ. Sci. Budapest. — 1983. — Sectio Computatorica, Tomus IV. — P. 113–125.

УСЛОВИЯ ОПТИМАЛЬНОСТИ ДЛЯ ДИСКРЕТНЫХ УПРАВЛЯЕМЫХ СИСТЕМ С НЕЛОКАЛЬНЫМИ УСЛОВИЯМИ

Г. Ю. Мехтиева, Я. А. Шарифов (Баку)

Задачи перспективного и оперативного планирования, составление программ различных систем, расчет многоступенчатых комплексов и т. д. обычно описываются рекуррентными соотношениями. Они естественно возникают при дискретизации "непрерывных" задач когда операция дифференцирования и интегрирования заменяются конечно-разностными и квадратурными формулами. Интерес к проблемам управления и оптимизация рекуррентных соотношений, вызванный запросами практики, привел к созданию теории оптимальных дискретных систем [1].

В настоящей работе выводится необходимые и достаточные условия оптимальности для общих дискретных систем задач оптимального уравнения с нелокальными условиями.

Пусть некоторый управляемый процесс описывается системой разностных уравнений

$$x_{i+1} - x_i = f_i(x_i, u_i) \quad i = 0, 1, ...N-1, \tag{1}$$

с нелокальными условиями

$$Ax_0 = a\,, \tag{2}$$

$$\sum_{i=0}^{N-1} B_i x_i = b. \tag{3}$$

Критерием качества управления является минимизации функционала

$$I([u]) = \Phi(x_N)\,, \tag{4}$$

где

$$[u] = (u_0, u_1, ..., u_{N-1}) : u_i \in V_i,\ i = 0, 1, ...N-1. \tag{5}$$

В оптимальной задаче (1)–(5) $x_i = \left(x_i^1, x_i^2, ..., x_i^n\right)$, $u_i = \left(u_i^1, u_i^2, ..., u_i^r\right)$; функции $f_i = \left(f_i^1, ..., f_i^n\right)$, Φ предполагается известными, A — постоянная прямоугольная матрица порядка $m \times n$, B_i, $i = 0, 1, ...N-1$ матрицы порядка $(n-m) \times n$, причем

$$\det \begin{pmatrix} A \\ \sum\limits_{i=0}^{N-1} B_i \end{pmatrix} \neq 0.$$

Через $L_2^r[0,N]$ обозначим гильбертово пространство вектор-функций дискретной переменной $[u] = (u_0, u_1, ..., u_{N-1})$ со скалярным произведением $< [u_i], [v_i] >= \sum\limits_{i=0}^{N-1} < u_i, v_i >_{E^r}$ и с нормой $\|[u]\| = \left(\sum\limits_{i=0}^{N-1} |u_i|_{E^r}^2\right)^{1/2}$. Пусть U — множество всех управлений, удовлетворяющих условию (5).

Теорема 1. *Пусть функции f_i, Φ непрерывны по совокупности своих аргументов вместе со своими частными производными по переменным (x,u) при $x \in E^n, u \in V_i$, $i = 0, 1, ..., N-1$. Кроме того,*

$$|f_i(x+\overline{x}, u+\overline{u}) - f_i(x,u)|_{E^n} \leq K_i \left(|\overline{x}|_{E^n} + |\overline{u}|_{E^r}\right)$$

при всех $x, x+\overline{x} \in E^n$ и всех $u, u+\overline{u} \in V_i$, $i = 0, 1, ...N-1$, и $KN\left[\|L\| \, \|B\|_{(N)} \dfrac{N}{2} + 1\right] < 1$, где через L обозначена обратная матрица к матрице $\begin{pmatrix} A \\ \sum\limits_{i=0}^{N-1} B_i \end{pmatrix}$, $k = max\{k_0, k_1, ..., k_{N-1}\}$. Тогда краевая задача при каждом фиксированном $[u] \in U$ имеет единственное решение.

Теорема 2. *Пусть выполняются все условия теоремы 1. Тогда функционал (4) при ограничениях (1)–(3) непрерывен и дифференцируем в норме $L_2^r[0,N]$, причем его градиент $I'([u])$ в точке $[u_i] \in U$ представим в виде*

$$I'([u_i]) = \{H_{iu}(x_i, \psi_i, u_i),\ i = 0, 1, ..., N-1\} \in L_2^r[0,N],$$

где

$$H_i(x, \psi, u) =< \psi, f_i(x,u) >, \quad H_{iu} = \left(H_{iu^1}, ..., H_{iu^r}\right),$$

$[x_i] = (x_0, x_1, ..., x_{N-1})$ — *дискретная траектория задачи* (1)–(3), *соответствующая выбранному управлению* $[u_i] \in U$, *а* $[\psi_i] = (\psi_0, \psi_1, ..., \psi_{N-1})$ *определяется из условий*

$$A^T\lambda + \sum_{i=0}^{N-1} B_i^T\mu + \sum_{i=0}^{N-1} H_{ix_i}\left(x_i, \psi_i, u_i\right) + \Phi_{x_N}\left(x_N\right) = 0,$$

$$\psi_i = \sum_{k=0}^{i} B_k^T\mu + \sum_{k=0}^{i} H_{kx_k}\left(x_k, \psi_k, u_k\right) + A^T\lambda,\ i = 0, 1, ..., N-1, \quad (6)$$

где λ — m-мерный, а μ — $(n-m)$-мерный постоянный вектор, T означает транспонирование.

Теорема 3. *Пусть выполняются все условия теоремы* 1 *и $[u_{i*}]$ — оптимальное уравнение, $[x_{i*}]$ — соответствующая ему траектория системы* (1)–(3)*, а $[\psi_{i*}]$ — решение системы* (6)*, соответствующее управлению $[u_{i*}]$. Тогда выполняются неравенства*

$$< H_{ix_i}\left(x_{i*}, \psi_{i*}, u_{i*}\right), u_i - u_* >\geq 0,\ i = 0, 1, ..., N-1 \quad (7)$$

при всех $u_i \in V_i$, для которых направление $e = u_i - u_*$ является возможным для множества V_i в точке u_{i*}.

Следствие. *Пусть в системе* (1) $f_i(x_i, u_i) = A_i x_i + B_i u_i + f_i$, $i = 0, 1, ..., N-1$ *и выполняются все условия теоремы 1. Кроме того, функция $\Phi(x)$ выпукла по x на E^n и множества V_i, $i = 0, 1, ..., N-1$ выпуклы. Тогда условия* (7) *является необходимым и достаточным условием для оптимальности.*

Работа выполнена при частичной финансовой поддержки INTAS (проект 06-1000017-8909).

Список литературы

1. Васильев Ф. П. Методы оптимизации. — М.: Факториал Пресс, 2002.

О РАНГЕ НЕЯВНЫХ ПРЕДСТАВЛЕНИЙ НАД ОДНИМ КЛАССОМ ФУНКЦИЙ ТРЕХЗНАЧНОЙ ЛОГИКИ

Е. В. Михайлец (Москва)

Понятие неявной выразимости функций k-значной логики введено А. В. Кузнецовым как одно из обобщений понятия выразимости функций суперпозициями [2].

Пусть A — произвольная система функций k-значной логики, $A \subseteq P_k$. *Системой неявных уравнений* над системой функций A будем называть всякую систему уравнений вида

$$\begin{cases} \Phi_1(x_1, \ldots, x_n, y) = \Psi_1(x_1, \ldots, x_n, y), \\ \ldots \\ \Phi_q(x_1, \ldots, x_n, y) = \Psi_q(x_1, \ldots, x_n, y), \end{cases} \tag{1}$$

где $\Phi_1, \ldots, \Phi_q$, $\Psi_1, \ldots, \Psi_q$ — некоторые формулы над системой функций A.

Говорят, что функция $f(x_1, \ldots, x_n)$ k-значной логики *неявно выразима* над системой функций A, если существует система неявных уравнений над A вида (1), имеющая при любых фиксированных значениях $x_1, \ldots, x_n$ единственное решение $y = f(x_1, \ldots, x_n)$. При этом соответствующую систему уравнений называют *неявным представлением* функции $f(x_1, \ldots, x_n)$ над A.

Множество всех функций f, $f \in P_k$, неявно выразимых над системой функций A, называется *неявным расширением* системы A и обозначается через $I(A)$ [1]. Благодаря очевидному соотношению $I(A) = I([A])$, при исследовании неявных расширений можно ограничиться рассмотрением только замкнутых относительно суперпозиции классов функций k-значной логики.

Если любая функция k-значной логики неявно выразима над A, т. е. $I(A) = P_k$, то систему функций A называют *неявно полной* в P_k.

Помимо неявных расширений, большой интерес для исследования представляют метрические характеристики неявных представлений.

Рассмотрим произвольную функцию f из неявного расширения некоторой системы A функций k-значной логики, $f \in I(A)$. Назовем *рангом* функции f над системой A и будем обозначать через $m_A^k(f)$ наименьшее число уравнений, достаточное для построения неявного представления f над A.

Как обычно, вводится функция Шеннона $m_A^k(n) = \max m_A^k(f)$, называемая *ранговой функцией* системы A (максимум берется по всем функциям k-значной логики, принадлежащим неявному расширению системы A и существенно зависящим не более чем от n переменных).

О. М. Касим-Заде в работе [1] исследовал поведение ранговой функции $m_A^2(n)$ для всех замкнутых классов булевых функций. Из результатов работы [1] следует, что максимальный порядок роста величины $m_A^2(n)$ достигается на классах D_2 и F_i^μ, где $i = 2, 3, 6, 7$ и

$\mu = 2, 3, \ldots, \infty$, и составляет $\Theta(n \log n)$. Для всех нетривиальных неявно полных замкнутых классов в P_2 порядок роста ранговой функции составляет $\Theta(n)$.

Автором было исследовано поведение ранговых функций для некоторых неявно полных классов функций в P_k. Выяснилось, что для широкого диапазона неявно полных систем функций k-значной логики ранговые функции имеют линейный порядок роста $\Theta(n)$. В частности, для классов функций, монотонных относительно произвольного нетривиального частичного порядка на множестве E_k, $E_k = \{0, 1, \ldots, k-1\}$, выражение для ранговой функции определяется следующей теоремой.

Теорема 1 [3]. *Пусть $k \geq 2$ и на множестве E_k задан частичный порядок $\mathfrak{M}$, содержащий хотя бы одну пару сравнимых элементов. Пусть A — класс всех функций в P_k, монотонных относительно частичного порядка $\mathfrak{M}$. Тогда система функций A неявно полна в P_k и при всех натуральных n для ранговой функции $m_A^k(n)$ имеет место равенство*

$$m_A^k(n) = \left\lceil \frac{n+2}{2} \right\rceil .$$

В связи с полученными результатами возник вопрос, существует ли неявно полная система функций в P_k, у которой порядок роста ранговой функции выше линейного. В данной работе описан неявно полный класс функций в P_3, ранговая функция которого имеет экспоненциальный порядок роста.

Для задания функций одной и двух переменных в P_3 будем использовать таблицы значений [4]. Рассмотрим следующую систему функций:

$\max(x,y)$	$\min_{01}(x,y)$	$l(x)$	0	1
0 1 2	0 0 2	0	0	1
1 1 2	0 1 2	0	0	1
2 2 2	2 2 2	1	0	1

Обозначим ее через W. В работе [4] Е. А. Ореховой показано, что система функций W неявно полна в P_3. Сформулируем основной результат.

Теорема 2. *Для ранговой функции системы функций W при всех натуральных n справедливы следующие оценки:*

$$2^{(n+1)/2} \leq m_W^3(n) \leq 2^{n+1}.$$

Автор выражает благодарность своему научному руководителю О. М. Касим-Заде за всестороннее внимание к данной работе.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 05-01-00994), Программы поддержки ведущих научных школ РФ (проект НШ-5400.2006.1) и Программы фундаментальных исследований Отделения математических наук РАН "Алгебраические и комбинаторные методы математической кибернетики" (проект "Синтез и сложность управляющих систем").

Список литературы

1. Касим-Заде О. М. Об одной метрической характеристике неявных и параметрических представлений булевых функций // Математические вопросы кибернетики. Вып. 6. — М.: Наука. Физматлит, 1996. — С. 133–188.

2. Кузнецов А. В. О средствах для обнаружения невыводимости или невыразимости // Логический вывод. — М.: Наука, 1979. — С. 5–33.

3. Михайлец Е. В. О ранге неявных представлений над классами монотонных функций k-значной логики // Материалы VI молодежной научной школы по дискретной математике и ее приложениям. Ч. II.—Москва, 2007. —С. 26–29.

4. Орехова Е. А. Об одном критерии неявной полноты в трехзначной логике // Математические вопросы кибернетики. Вып. 12. — М.: Наука. Физматлит, 2003. — С. 27–74.

ГРАДИЕНТНЫЙ АЛГОРИТМ С ВЕСАМИ ДЛЯ ПОСТРОЕНИЯ УСЛОВНЫХ ТЕСТОВ

М. Ю. Мошков (Сосновец, Польша)

В работе рассматривается приближенный (градиентный) алгоритм для минимизации взвешенной глубины условных тестов [1]. Получена оценка точности этого алгоритма, которая в общем случае не может быть улучшена. При некоторых естественных предположениях о классе NP рассматриваемый алгоритм близок (с точки зрения точности) к наилучшим полиномиальным приближенным алгоритмам для минимизации взвешенной глубины условных тестов. Заметим, что имеются аналогии между этим алгоритмом и градиентным алгоритмом с весами для задачи о покрытии [2].

Тестовая таблица (*с весами*) T — таблица с n столбцами, которым приписаны пары $(f_1, w_1), \ldots, (f_n, w_n)$, где f_i — *проверка* и w_i — положительное действительное число, называемое *весом* проверки f_i. Таблица T заполнена целыми числами (значениями проверок). Строки T попарно различны, и каждой строке приписано целое число (*решение*). Вес проверки можно интерпретировать как стоимость или временную сложность, или риск (в случае проблем медицинской или технической диагностики) вычисления значения проверки. Таблица T называется *вырожденной*, если либо в ней нет ни одной строки, либо всем строкам T приписано одно и то же решение.

Условный тест над $\{f_1, \ldots, f_n\}$ — конечное дерево с корнем, в котором каждой концевой вершине приписано целое число (решение), каждой вершине, не являющейся концевой, приписана проверка из множества $\{f_1, \ldots, f_n\}$, и для каждой вершины, не являющейся концевой, дугам, выходящим из этой вершины, приписаны попарно различные целые числа.

Пусть Γ — условный тест над $\{f_1, \ldots, f_n\}$. Опишем работу Γ на строке $\bar{\delta} = (\delta_1, \ldots, \delta_n)$ таблицы T. Работа начинается в корне v дерева Γ. Если v — концевая вершина, которой приписано решение d, то результатом работы Γ является число d. Пусть вершина v не является концевой, и ей приписана проверка f_i. Если существует дуга, которая выходит из вершины v и которой приписано число δ_i, то переходим по этой дуге в новую вершину, которая будет обрабатываться так же, как и вершина v. В противном случае результат работы Γ не определен.

Будем говорить, что Γ является *условным тестом для* T, если для каждой строки $\bar{\delta}$ таблицы T результат работы Γ на $\bar{\delta}$ определен и совпадает с решением, приписанным строке $\bar{\delta}$.

Вес пути в Γ — сумма весов проверок, приписанных вершинам этого пути. *Взвешенная глубина* Γ — максимальный вес пути, начинающегося в корне и заканчивающегося в некоторой концевой вершине Γ. Обозначим $D_{\min}(T)$ минимальную взвешенную глубину условного теста для T. Заметим, что проблема построения для заданной таблицы условного теста, имеющего минимальную взвешенную глубину, является NP-трудной.

Пусть $f_i \in \{f_1, \ldots, f_n\}$ и σ — целое число. Обозначим $T(f_i, \sigma)$ тестовую таблицу, полученную из T удалением всех строк, которые на пересечении со столбцом f_i содержат числа, отличные от σ. Обозначим $P(T)$ число неупорядоченных пар строк таблицы T, которым приписаны различные решения. Для любого $f_i \in \{f_1, \ldots, f_n\}$

обозначим через $E(T, f_i)$ множество чисел, содержащихся в столбце f_i таблицы T.

Градиентный алгоритм.

1-*й шаг.* Построим дерево, содержащее ровно одну вершину. Припишем этой вершине таблицу T и перейдем ко второму шагу.

Предположим, что уже выполнено $t \geq 1$ шагов. Дерево, построенное на шаге t, обозначим G.

$(t+1)$-*й шаг.* Если ни одной вершине дерева G не приписана тестовая таблица, то дерево $G(T) = G$ является результатом работы алгоритма. В противном случае выберем некоторую вершину v дерева G, которой приписана тестовая таблица T'.

Если T' — вырожденная таблица, то вместо T' припишем вершине v решение, которое приписано всем строкам таблицы T', и перейдем к $(t+2)$-му шагу. Пусть T' — невырожденная таблица. Для каждого $f_i \in \{f_1, \ldots, f_n\}$ пусть

$$d(f_i) = \frac{P(T') - \max\{P(T'(f_i, \sigma)) : \sigma \in E(T', f_i)\}}{w_i}.$$

Пусть p — минимальное число из $\{1, \ldots, n\}$ такое, что $|E(T', f_p)| \geq 2$ и $d(f_p) = \max\{d(f_i) : f_i \in \{f_1, \ldots, f_n\}, |E(T', f_i)| \geq 2\}$. Вместо T' припишем вершине v проверку f_p. Для каждого $\delta \in E(T', f_i)$ добавим к дереву G вершину $v(\delta)$ и дугу, выходящую из вершины v и входящую в вершину $v(\delta)$. Припишем этой дуге число δ, а вершине $v(\delta)$ припишем таблицу $T'(f_p, \delta)$. Перейдем к $(t+2)$-му шагу.

Обозначим $D_{\mathrm{greedy}}(T)$ взвешенную глубину условного теста $G(T)$, построенного градиентным алгоритмом для таблицы T. Для произвольного натурального m обозначим $H(m) = 1 + \frac{1}{2} + \ldots + \frac{1}{m}$. Известно, что $\ln m \leq H(m) \leq \ln m + 1$.

Теорема. *Для любой невырожденной тестовой таблицы T выполняется неравенство $D_{\mathrm{greedy}}(T) \leq D_{\min}(T) H(P(T))$.*

В общем случае полученная оценка не может быть улучшена.

Предложение 1. *Для любого действительного $a > 0$ и для любого натурального m существует тестовая таблица T такая, что $D_{\min}(T) = a$, $P(T) = m$ и $D_{\mathrm{greedy}}(T) = aH(m)$.*

Оценим число шагов градиентного алгоритма и число вершин в построенном условном тесте. Обозначим $N(T)$ число строк в таблице T и $L(G(T))$ — число вершин в условном тесте $G(T)$.

Предложение 2. *Пусть T — невырожденная тестовая таблица. Тогда $L(G(T)) \leq 2N(T)$, и при построении условного теста $G(T)$ градиентный алгоритм выполняет не более $2N(T)+2$ шагов.*

Используя предложение 2, получаем, что для таблиц с натуральными весами градиентный алгоритм является полиномиальным.

Из теоремы 1 следует, что $D_{\text{greedy}}(T) \leq D_{\min}(T)(\ln P(T) + 1)$ для любой невырожденной таблицы T. Покажем, что при некоторых предположениях о классе NP эта оценка не может быть существенно улучшена в классе полиномиальных алгоритмов.

Предложение 3. *Если* $\text{NP} \not\subseteq \text{DTIME}(n^{O(\log_2 \log_2 n)})$, *то для любого* ε, $0 < \varepsilon < 1$, *не существует полиномиального алгоритма, строящего по заданной невырожденной тестовой таблице* T *с натуральными весами условный тест для* T, *взвешенная глубина которого не превосходит* $(1 - \varepsilon) D_{\min}(T) \ln P(T)$.

Список литературы

1. Чегис И. А., Яблонский С. В. Логические способы контроля электрических схем // Труды МИ АН СССР. — 1958. — Т. 51. — С. 270–360.

2. Chvátal V. A greedy heuristic for the set-covering problem // Mathematics of Operations Research. — 1979. — V. 4, № 3. — P. 233–235.

НЕЛИНЕЙНОЕ ПРЕОБРАЗОВАНИЕ ДИАГРАММ РЕШЕНИЙ

Р. Г. Мубаракзянов (Казань)

Упорядоченные диаграммы решений (*OBDD* [1]) являются на сегодняшний день одним из средств верификации и исследования интегральных схем. Главный параметр представления *OBDD* — ее размер — зависит от порядка чтения переменных. Некоторые важные функции, например, "УМНОЖЕНИЕ" ([2]), имеют очень большой размер представления этой функции в виде *OBDD* для любого порядка чтения переменных. Способ расширения возможностей представления функций (схем) основан на преобразовании переменных [3–5]. После подобного преобразования (которое должно быть биективным и "просто моделируемым"), функция должна иметь более компактное *OBDD*-представление.

Одно из таких преобразований, активно исследованное в последнее время, — это линейное преобразование ("linear sifting") [6, 7] вида

$$x_i \mapsto (x_i \equiv x_j).$$

В работе представляется новый нелинейный тип преобразований, основанный на следующей операции

$$x_i \mapsto (x_i \equiv (x_j x_k)),$$

то есть переменная x_i заменяется на значение, равное эквивалентности x_i и конъюнкции x_j и x_k.

Определим функцию f на множестве V от n переменных, $n = k^2 + 2k$,

$$CON_k(x_1, \ldots, x_k, y_1, \ldots, y_k, z_{11}, \ldots, z_{kk}) := \bigwedge_{i,j=1,1}^{k,k} (z_{ij} \equiv x_i y_j).$$

Эта функция представляется в виде $OBDD$ размера $k^2 < n$, если сначала выполняются преобразования $z_{ij} \mapsto (z_{ij} \equiv (x_i y_j))$, для всех $i, j = 1, \ldots, k$.

Теорема. *OBDD, вычисляющая функцию CON, имеет сложность не менее* 2^k .

При внедрении нашего алгоритма в пакет "cudd" [8] удалось показать, что он позволяет представить большинство функций более экономно.

Результаты были получены на компьютере Intel Pentium III 500 MHz, базированном на операционой системе Linux. Алгоритм был внедрен в программу "nanotrav" пакета *CUDD* [8] (версия 2.3.0) и протестирован на схемах LGSynth'93 [4].

Кроме того, в работе показано, что пакет [8], тестирующий схемы, имеет ряд ошибок.

Список литературы

1. Bern J., Meinel Ch., Slobodova A. OBDD-based Boolean manipulation in CAD beyond current limits // Proc. 32nd ACM/IEEE Design Automaton Conference, San Francisco, CA. — 1995. — P. 408–413.

2. Bryant R. E. On the complexity of VLSI implementations and graph representations of Boolean functions with application to integer multiplication // IEEE Trans. on Comput. — 1991. — V. 40. — P. 205–213.

3. Kerntopf P. Nonlinear transformation of decision diagrams // Proc. 10th IEEE/ACC Int. Workshop on Logic Synthesis, Granlibakken, CA. — 2001. — P. 173–178.

4. LGSynth'93 Benchmarks. (`http://www.cbl.ncsu.edu/CBL_Docs/lgs93.html`)

5. Meinel Ch., Theobald T. Algorithms and Data Structures in VLSI Design. — Springer, 1998.

6. Meinel Ch., Somenzi F., Theobald T. Linear sifting of decision diagrams and its application in synthesis // IEEE Trans. on Computer-Aided Design. — 2000. — V. 19, № 5. — P. 521–533.

7. Meinel Ch., Theobald T. Local encoding transformations for optimizing OBDD-representations of finite state machines // Formal Methods in System Design. — 2001. — V. 18. — P. 285–301.

8. Somenzi F. CUDD: CU decision diagram package. (`ftp://vlsi.colorado.edu/pub/`)

ОЦЕНКИ СЛОЖНОСТИ РЕАЛИЗАЦИИ ЭЛЕМЕНТАРНЫХ СИММЕТРИЧЕСКИХ ФУНКЦИЙ В КЛАССЕ САМОКОРРЕКТИРУЮЩИХСЯ КОНТАКТНЫХ СХЕМ

Е. А. Попов (Москва)

В настоящей работе рассматривается задача синтеза контактных схем, реализующих элементарные симметрические функции. С точностью до аддитивной константы найдены значения сложности реализации элементарных симметрических функций в классе контактных схем, корректирующих фиксированное число обрывов.

В дальнейшем будем использовать классические понятия булева куба B^n, функции алгебры логики, проводящей цепи, контактной схемы и самокорректирующейся контактной схемы (см., например, [1]).

Под *сложностью* функции алгебры логики $L(f)$ будем понимать минимальную из сложностей контактных схем, реализующих f. Через $L^{r,t}(f)$ обозначим сложность реализации функции f контактными схемами корректирующими r обрывов и t замыканий.

Напомним, что *симметрической функцией* называется функция алгебры логики не изменяющая свое значение при любой перестановке аргументов. *Элементарной симметрической функцией* с рабочим числом w от n переменных называется функция алгебры логики s_n^w равная 1 на всех наборах с w единицами и 0 на всех остальных наборах.

Под *цепным блоком* ширины w будем понимать контактную схему с $(w+1)$ входом и $(w+1)$ выходом. Множество входных и выходных вершин будем называть концевыми вершинами блока. Для всех $i \in [1, w+1]$, i-й вход схемы соединен с i-м выходом схемы цепью вида $\overline{x}_1 \ldots \overline{x}_1 \overline{x}_2 \ldots \overline{x}_2 \ldots \overline{x}_n \ldots \overline{x}_n$, называемой в дальнейшем i-цепью.

Каждая i-цепь соединена с $(i+1)$-цепью $(n-1)$ цепью из замыкающих контактов следующего вида. Цепь, идущая из вершины инцидентной размыкающим контактам типа $\overline{x}_j$ и $\overline{x}_{j+1}$ i-й цепи в вершину инцидентную размыкающим контактам типа $\overline{x}_{j+1}$ и $\overline{x}_{j+2}$ $(i+1)$-й цепи, где $j \in [1, n-2]$, состоит из замыкающих контактов типа x_{i+1}; цепь, идущая из вершины инцидентной размыкающим контактам только типа $\overline{x}_1$ i-й цепи в вершину инцидентную размыкающим контактам типа $\overline{x}_1$ и $\overline{x}_2$ $(i+1)$-й цепи, состоит из замыкающих контактов типа x_1; цепь, идущая из вершины инцидентной размыкающим контактам типа $\overline{x}_{n-1}$ и $\overline{x}_n$ i-й цепи в вершину инцидентную размыкающим контактам только типа $\overline{x}_n$ $(i+1)$-й цепи, состоит из замыкающих контактов типа x_n.

Цепной блок содержит только перечисленные выше контакты. Таким образом, цепной блок реализует между i-м входом и j-м выходом, где $1 \leqslant i < j \leqslant w+1$, элементарную симметрическую функциую с порогом $(j-i)$.

Обобщая результаты [2, 3], удалось найти структуру минимальных, с точностью до аддитивной константы, контактных схем реализующих элементарные симметрические функции с коррекцией фиксированного числа обрывов.

Установлено, что минимальные контактные схемы, реализующие элементарные симметрические функции, могут быть построены из цепных блоков, соединенных между собой концевыми вершинами, причем вход и выход контактной схемы находятся в множестве концевых вершин блоков.

Опираясь на описанную структуру минимальных схем доказана следующая теорема.

Теорема. *При достаточно больших n справедливо равенство*

$$L^{r,0}(s_n^w) = (2w+1)(r+1)n - B_w^{r,0},$$

где $B_w^{r,0}$ некоторая неотрицательная константа.

Для доказательства этой теоремы рассматриваются наборы с w единицами и соответствующие им различные проводящие цепи в схеме, реализующей элементарную симметрическую функцию и корректирующую r обрывов. В ходе доказательства используются две леммы.

Лемма 1. *Пусть контактная схема Σ с входом a и выходом b, реализующая некоторую функцию $f(x_1, \ldots, x_n)$, корректирует r обрывов. Обозначим через $\nu_{\Sigma,\widetilde{\alpha}}(a,b)$ максимальное число проводящих цепей от входа a схемы Σ к её выходу b на наборе $\widetilde{\alpha} \in \boldsymbol{B}^n$ не пересекающихся по контактам. Тогда для любого набора $\widetilde{\alpha} \in \boldsymbol{B}^n$ такого, что $f(\widetilde{\alpha}) = 1$ выполняется $\nu_{\Sigma,\widetilde{\alpha}}(a,b) \geqslant r+1$.*

Лемма 2. *Пусть схема Σ, состоящая из цепных блоков, реализует элементарную симметрическую функцию s_n^w. Тогда для всех наборов $\widetilde{\alpha} \in \boldsymbol{B}$ с w единицами все проводящие на наборе $\widetilde{\alpha}$ цепи из входа в выход схемы, проходят через одни и те же концевые вершины блоков.*

Работа выполнена при финансовой поддержке РФФИ, проект 06-01-00745.

Список литературы

1. Ложкин С. А. Лекции по основам кибернетики. – М.: Издательский отдел факультета ВМиК МГУ им. М. В. Ломоносова, 2004.

2. Валентинов Е. В. О сложности и структуре минимальных самокорректирующихся контактных схем из некоторых классов. — Диссертация на соискание ученой степени кандидата физико-математических наук. — Москва, 2001.

3. Гринчук М. И. О сложности реализации симметрических булевых функций контактными схемами // Математические вопросы кибернетики. Вып. 3. — М.: Наука, 1991. — С. 77–104.

О МОДЕЛИРУЕМОСТИ ДИСКРЕТНЫХ ДИНАМИЧЕСКИХ СИСТЕМ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

Е. Я. Ройтенберг (Москва)

Рассмотрим дискретную динамическую систему, представленную в пространстве $\mathbf{R}^s$ нелинейным разностным уравнением

$$\begin{aligned} &x(n+1) = A(n)x(n) + \varphi(x(n), n), \\ &x(0) = x_0 \in S_\rho(\zeta_0); \quad x : \mathbf{N}_0 \to \mathbf{R}^s, \quad \mathbf{N}_0 = \{0, 1, \ldots\}. \end{aligned} \tag{1}$$

Здесь $(s \times s)$-матрица $A(n), n \in \mathbf{N}_0$, $||A(n)|| < a$, $n \in \mathbf{N}_0$; $\varphi(x(n), n)$ нелинейный оператор, определенный на $\mathbf{R}^s \times \mathbf{N}_0$ со значениями из $\mathbf{R}^s$, удовлетворяющий для всех $x, \zeta \in \mathbf{R}^s$ условию

$$||\varphi(\zeta, n) - \varphi(x, n)|| \le q||\zeta - x||, \text{ где постоянная } q > 0;$$

$S_\rho(\zeta(0)) \subseteq \mathbf{R}^s$ — шар допустимых начальных состояний радиуса ρ с центром в ζ_0. Вектор начального состояния x_0 неизвестен, но известна l-векторная последовательность

$$y(n) = C(n)x(n), \quad n \in \mathbf{N}_0, \tag{2}$$

которую будем называть следом решения задачи (1). Здесь $C(n)$, $(l \times s)$-матрица $(l < s)$, $||C(n)|| < c$, $n \in \mathbf{N}_0$, постоянные величины a и c известны.

Рассмотрим вспомогательную управляемую систему

$$\zeta(n+1) = A(n)\zeta(n) + \varphi(\zeta(n), n) + u(n),\ \zeta(0) = \zeta_0 \in \mathbf{R}^s,\ n \in \mathbf{N}_0. \quad (3)$$

Здесь $\zeta(n) \in \mathbf{R}^s$ — вектор состояния системы (3) в момент времени n, $n \in \mathbf{N}_0$; $u(\cdot) = \{u(n)\}$, $n \in \mathbf{N}_0$, s-векторная последовательность управлений $u(n) \in \mathbf{R}^s, n \in \mathbf{N}_0$; s-вектор начального состояния $\zeta_0 \in \mathbf{R}^s$ известен. Требуется получить оценку $\widetilde{x}(n), n \in \mathbf{N}_0$, состояния $x(n)$, $n \in \mathbf{N}_0$, системы (1), (2). Систему (3), которая будет определять $\widetilde{x}(n)$, $n \in \mathbf{N}_0$, назовем *моделью*. Принимаем, что $\widetilde{x}(n) = \zeta(n)$, $n \in \mathbf{N}_0$. Тогда ошибка оценки $z(n) = \widetilde{x}(n) - x(n)$ имеет вид $z(n) = z(n) - x(n)$, $n \in \mathbf{N}_0$. Вектор-функцию $z(n)$, $n \in \mathbf{N}_0$, будем называть *ошибкой модели*.

Определение. Пусть по известному следу $y(n)$, $n \in \mathbf{N}_0$, можно найти s-вектор-функцию $\zeta(n)$, $n \in \mathbf{N}_0$, такую, что для заданной постоянной величины ε будет

$$||z(n)|| \le \varepsilon, \quad n \ge n_\varepsilon > 0, \quad \varepsilon > 0, \quad \text{где } n, n_\varepsilon \in \mathbf{N}_0. \quad (4)$$

Тогда будем говорить, что система (1), (2) *асимптотически моделируема*.

Образуем $\eta(n) = C(n)\zeta(n)$, $n \in \mathbf{N}_0$, след решения задачи (3). Векторную последовательность управлений $u(n)$, $n \in \mathbf{N}_0$, берем в виде $u(n) = B(n)(\eta(n) - y(n))$, $n \in \mathbf{N}_0$, где $(s \times l)$-матрица $B(n)$, $n \in \mathbf{N}_0$, равномерно ограничена $||B(n)|| < b$, $n \in \mathbf{N}_0$, постоянная b известна. Матрицу $B(n)$ необходимо определить так, чтобы обеспечить выполнение неравенства (4). Обозначим $\varphi(\zeta(n), n) - \varphi(x(n), n) = F(z(n), n)$, $n \in \mathbf{N}_0$. Ошибка модели $z(n)$ удовлетворяет разностному уравнению

$$\begin{aligned} &z(n+1) = (A(n) + B(n)C(n))z(n) + F(z(n), n), \\ &z_0 \in \mathbf{R}^s, \quad n \in \mathbf{N}_0, \quad ||z_0|| < \rho. \end{aligned} \quad (5)$$

Теорема 1. *Для асимптотической моделируемости системы* (1), (2) *достаточно* $(s \times l)$*-матрицу* $B(n) = B_V(n)$, $n \in \mathbf{N}_0$, *выбрать таким образом, чтобы решение уравнения* $z(n+1) = \mathfrak{A}(n)z(n)$, $n \in \mathbf{N}_0$, *удовлетворяло свойству* $\mathcal{L}(\lambda, L, q)$, *а именно* $||z(n)|| \le L\lambda^{n-k}||z(k)||$, $n > k$, $n, k \in \mathbf{N}_0$, $0 < \lambda < 1$, $L > 0$, $q < \frac{1-\lambda}{L}$. *Здесь* $\mathfrak{A}(n) = A(n) + + B_V(n)C(n)$, $n \in \mathbf{N}_0$.

Доказательство. Для нормы решения (5) верна [1] оценка

$$||z(n)|| \le T(\lambda + Lq)^n ||z(0)||, n > 0, n \in \mathbf{N}_0, \text{ где } T = \frac{L(\lambda+q)}{\lambda+qL}.$$

Поэтому с момента $n_\varepsilon = \dfrac{\ln\varepsilon - \ln\rho - \ln T}{\ln(\lambda+Lq)}$ для всех $n \ge 0$ выполнено (4).

Очевидно, имеет место

Теорема 2. *Уравнение модели, осуществляющей асимптотическое моделирование системы* (1), (2), *имеет вид*

$$\zeta(n+1) = A(n)\zeta(n) + \varphi(\zeta(n), n) + B_V(n)(\eta(n) - y(n)), \zeta(0) = \zeta_0, n \in \mathbf{N}_0.$$

В качестве $(s \times l)$-матрицы $B_V(n)$, $n \in \mathbf{N}_0$, берем матрицу

$$B_V(n) = -A(n)P(n)C^*(n)[C(n)P(n)C^*(n) + R(n)]^{-1}.$$

Здесь $P(n)$, $n \in \mathbf{N}_0$, — симметрическая, равномерно ограниченная, положительно определенная $(s \times s)$-матрица, являющаяся решением разностного матричного уравнения

$$P(n+1) = A(n)P(n)A^*(n) - A(n)P(n)C^*(n)[C(n)P(n)C^*(n) + \\ + R(n)]^{-1} \times C(n)P(n)A^*(n) + \Gamma(n)Q(n+1)\Gamma^*(n),\ P(0) = P_0,\ n \in \mathbf{N}_0,$$

где $(r \times r)$-матрица $Q(i)$, $(l \times l)$-матрица $R(i)$, $(s \times l)$-матрица $\Gamma(i)$ суть свободные параметры, $i \in \mathbf{N}_0$.

Следствие 1. *Если задача* (1), (2) *имеет вид*

$$x(n+1) = A(n)x(n) + \varphi(x(n), n) + p(n), \\ x(0) = x_0 \in S_\rho(\zeta_0),\ n \in \mathbf{N}_0, \qquad (6)$$

$$y(n) = C(n)x(n), \quad n \in \mathbf{N}_0, \qquad (7)$$

где $p(n), n \in \mathbf{N}_0$, *s-мерная векторная последовательность неизвестных возмущений из* $\mathbf{R}^s$ *таких, что* $||p(n)|| < p_0$, $n \in \mathbf{N}_0$, p_0 *— известная постоянная, то уравнение* (5) *для ошибки оценки принимает вид* $z(n+1) = \mathfrak{A}(n)z(n) + F(z(n), n) - p(n)$, $z_0 \in \mathbf{R}^s$, $n \in \mathbf{N}_0$. *Для его решения очевидно верна оценка* $||z(n)|| \le T(\lambda + Lq)^n ||z_0|| + Lp_0 \frac{1-(\lambda+Lq)^n}{1-(\lambda+Lq)}$, $n > 0$, $n \in \mathbf{N}_0$, *из которой следует, что*

можно решить задачу асимптотической моделируемости для системы (6), (7).

Следствие 2. *Пусть решение уравнения* (6) *при* $p(n) \equiv 0$, $n \in \mathbf{N}_0$, *равномерно ограничено* $||x(n)|| < \varkappa$, $\varkappa > 0$ — *известная постоянная. Рассмотрим систему*

$$x(n+1) = (A(n) + \Xi(n))x(n) + \varphi(x(n), n) + p_2(n), \quad x_0 \in S_\rho(\zeta_0), \quad n \in \mathbf{N}_0, \tag{8}$$

$$y(n) = (C(n) + G(n))x(n) + p_3(n), n \in \mathbf{N}_0, \tag{9}$$

где $\Xi(n)$ — *неизвестная* $(s \times s)$-*матрица,* $||\Xi(n)|| < \xi$; $G(n)$ — *неизвестная* $(l \times s)$-*матрица,* $||G(n)|| < g$, $p_2(n)$ *и* $p_3(n)$ *соответственно* s *и* l-*векторные последовательности неизвестных возмущений таких, что* $||p_2(n)|| < p_2$, $||p_3(n)|| < p_3$, $n \in \mathbf{N}_0$; ξ, g, p_2, p_3 — *известные положительные постоянные. Тогда система* (8), (9) *асимптотически моделируема.*

Список литературы

1. Халанай А., Векслер Д. Качественная теория импульсных систем. — М.: Мир, 1971.

О РЕАЛИЗАЦИИ ФУНКЦИЙ АЛГЕБРЫ ЛОГИКИ СХЕМАМИ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ, ВЛОЖЕННЫМИ В ЕДИНИЧНЫЙ КУБ

О. Б. Седелев (Москва)

В настоящее время достаточно распространенной моделью реализации функций алгебры логики (ФАЛ), являются схемы из функциональных элементов (СФЭ) [1, 2]. Известно [1], что функция Шеннона для сложности самой "сложной" ФАЛ от n булевских переменных (БП) при их реализации в классе СФЭ в базисе $Б$, асимптотически равна $\rho_Б \frac{2^n}{n}$, где $\rho_Б$ — константа, зависящая от базиса.

Во многих случаях для дальнейшего использования построенной схемы необходима ее геометрическая реализация, т. е. вложение определенного вида в ту или иную заданную геометрическую структуру. В качестве такой структуры в последнее время часто выступает единичный n-мерный куб. При этом рассматриваются различные типы вложений и, в частности, гомеоморфные [3] вложения.

В данной работе рассматривается геометрическая реализация СФЭ, связанная с их квазигомеоморфными вложениями в единичные кубы при которых вершины СФЭ переходят в вершины единичного куба, а пучки дуг — в аналогичные пучки или так называемые транзитные деревья единичного куба, не имеющие общих внутренних вершин.

Пусть $Б$ — конечный полный базис из функциональных элементов (ФЭ), а $R_Б(n)$ — минимальная размерность единичного куба, допускающего для любой ФАЛ $f(x_1,\ldots,x_n)$ квазигомеоморфное вложение некоторой СФЭ в базисе $Б$, реализующей $f(x_1,\ldots,x_n)$. Основной результат работы заключается в установлении следующих оценок (эти оценки дополняют аналогичные оценки для BDD из [3]; все логарифмы в данной работе берутся по основанию 2):

$$n - \log\log(n) - c_Б \le R_Б(n) \le n - \log\log(n) + c'_Б, \qquad (1)$$

где $c_Б$ и $c'_Б$ — некоторые константы, зависящие от базиса.

Доказательство нижней оценки в (1), проводится на основе мощностных соображений. Пусть $A_Б(n,r)$ — число различных СФЭ в базисе $Б$ от n БП $x_1,\ldots,x_n$, которые можно вложить в единичный куб B^r размерности r, где $B = 0,1$. Докажем верхнюю оценку вида:

$$A_Б(n,r) \le (n + r + 1 + tr(r-1)(r-2)...(r-k+1))^{2^r}, \qquad (2)$$

где t — число ФЭ базиса $Б$, а k — максимальное число входов у ФЭ базиса $Б$.

Действительно, при вложении СФЭ в базисе $Б$ от БП $x_1,\ldots,x_n$ в B^r каждой вершине куба может соответствовать либо одна из этих n БП, либо один из t ФЭ базиса $Б$, либо вершина может оказаться внутренней вершиной транзитного квазидерева, либо остаться не использованной вершиной единичного куба. При этом для любой вершины, которой сопоставлена вершина СФЭ, существует не более чем $r(r-1)(r-2)...(r-k+1)$ вариантов выбора ее входных ребер, а для транзитной вершины — не более r таких вариантов, после чего вложение становится полностью определенным. Требуемая нижняя оценка (1) получается из решения мощностного неравенства:

$$A_Б(n, R_Б(n)) \ge 2^{2^n}.$$

Перейдем к доказательству верхней оценки неравенства (1). Сначала рассмотрим СФЭ в так называемом мультиплексорном базисе $Б_\mu$, т. е. базисе $\{\mu(x,y_0,y_1) = \bar{x}y \vee xy, 0, 1\}$, который тесно связан с

понятием BDD [3]. Установим для E_μ верхнюю оценку:

$$R_{E_\mu}(n) \leq n - \log\log n + 11, \qquad (2)$$

которая получается с использованием аналогичной оценки из [3] для BDD.

Построим для любой BDD Σ от БП $x_1, \ldots, x_n$ моделирующую ее СФЭ Σ' в мультиплексорном базисе с входами $x_1, \ldots, x_n$ следующим образом:

1) каждой вершине BDD Σ с пометкой σ, $\sigma = 0, 1$, сопоставим ФЭ типа σ, присоединенный к входу x_1;

2) каждой вершине v BDD Σ с пометкой x_i, из которой выходят ребра (v, v_0) и (v, v_1) с пометками 0 и 1 соответственно, сопоставим вершину v' СФЭ Σ' с расположенным в ней ФЭ $\mu(x_i, y_0, y_1)$ и входящими в нее ребрами (x_i, v), (v'_0, v'), (v'_1, v'), где v'_0 и v'_1 — вершины СФЭ Σ', сопоставленные вершинам v_0 и v_1 BDD Σ, а порядок ребер соответствует порядку БП x_i, y_0, y_1 данного ФЭ.

Заметим, что СФЭ Σ' реализует ту же самую ФАЛ, что и BDD Σ.

Доказательство верхней оценки (3) состоит из трех этапов.

На первом этапе осуществляется реализация заданной (произвольной) ФАЛ $f(x_1, ..., x_n)$ в виде специальным образом построенной BDD Σ_f, которая, далее, вкладывается в единичный куб размерности $R = n - \lfloor \log\log n \rfloor + 5$ так, как это сделано в работе [3]. На втором этапе BDD Σ_f заменяется вышеуказанным способом на моделирующую ее СФЭ Σ'_f в мультиплексорном базисе. При этом вложение BDD Σ_f в единичный куб B^R переходит в соответствующее вложение СФЭ Σ'_f в B^R без системы из n транзитных деревьев, осуществляющих "подвод" БП $x_1, \ldots, x_n$ к ФЭ типа μ и БП x_1 к элементам типа σ.

На третьем этапе полученное вложение СФЭ Σ'_f в единичный куб B^R преобразуется в аналогичное вложение СФЭ Σ'_f в единичный куб B^{R+6}, снабженное необходимой системой "подвода" БП $x_1, \ldots, x_n$.

Остановимся, подробнее, на третьем этапе описанного выше построения. Построение системы "подвода" БП $x_1, \ldots, x_n$ основывается на следующей теореме.

Теорема. *Если в подкубе B^n, единичного куба B^{n+6} каждой вершине присвоен один из n типов (цветов), то в B^{n+6} найдутся n деревьев, не имеющих общих вершин, каждое из которых, содержит все вершины одного типа (цвета).*

На основе теоремы может быть построена система "подвода" БП $x_1, \ldots, x_n$ и получена искомая верхняя оценка (3).

Для получения верхней оценки из (1) заметим, что в вышеуказанном вложении ФЭ $\mu(x, y_0, y_1)$ и константы 0, 1 могут быть заменены их реализациями в произвольном базисе $Б$, что потребует увеличения верхней оценки (3) на константу.

Работа выполнена при финансовой поддержке РФФИ (проект 06-01-00745).

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

2. Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. Вып. 6. — М.: Наука, 1996. — С. 189–214.

3. Ложкин С. А., Седелев О. Б. О реализации функций алгебры логики BDD, вложенными в единичный куб // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. — 2006. — № 4. — С.29–35.

БЫСТРЫЕ АЛГОРИТМЫ ДЛЯ ЭЛЕМЕНТАРНЫХ ОПЕРАЦИЙ СО СТЕПЕННЫМИ РЯДАМИ

И. С. Сергеев (Москва)

В настоящей работе рассматривается реализация некоторых элементарных операций с комплексными степенными рядами, сложность измеряется количеством бинарных арифметических операций с комплексными или вещественными числами.

Пусть $F(n) = \min_{m \geq n} \Phi(m)$, где $\Phi(n)$ — сложность дискретного преобразования Фурье (ДПФ) порядка n. Для $F(n)$ известны асимптотические верхние оценки: $1,5n \log_2 n$ операций над $\mathbf{C}$ или $(34/9)n \log_2 n$ операций над $\mathbf{R}$ (см. [1, 6]).

Выражение оценок сложности рассматриваемых ниже операций через $F(n)$ корректно, например, в следующих предположениях:

$$n \log^2 \log n = O(F(n)), \quad F(an) \sim aF(n), \text{ где } 1 \leq a = O(\log n). \quad (1)$$

В случае невыполнения условий (1) следует $F(n)$ в оценках сложности заменить функцией $F'(n) \geq F(n)$, удовлетворяющей (1).

Стандартный метод умножения двух степенных рядов $f, g \in \mathbf{C}[[\mathbf{x}]]$ по модулю x^n требует асимптотически $6F(n)$ операций. Эффективная реализация других элементарных операций (инвертирования, деления, логарифма, экспоненты) основана на методе последовательных приближений — дискретном аналоге классического «метода касательных» Ньютона—Рафсона (см. [4, гл. 9], а также [2, 3]).

Для произвольного ряда g введем обозначение $g_m = g \bmod x^m$.

Инвертирование степенного ряда f, $f_1 = 1$, т. е. вычисление r_n, где $r = 1/f$, выполняется последовательностью итераций вида

$$r_{2m} = r_m(2 - r_m f_{2m}) \bmod x^{2m}. \qquad (2)$$

Шёнхаге [7] и Бернштейн [2] независимо получили асимптотическую оценку сложности инвертирования $9F(n)$. В методе Шёнхаге для реализации (2) используются ДПФ порядка $3m$, а в методе Бернштейна ряды разбиваются на блоки длины k, для умножения рядов используются ДПФ порядка $2k$ (такой способ вычислений будем называть методом A или A-$2k$, в соответствии с порядком ДПФ). Комбинированный метод A-$3k$, в котором используется разбиение на блоки и применяются ДПФ порядка $3k$ для вычисления тройных произведений, позволяет реализовать инвертирование со сложностью $7,5F(n)$.

Еще один подход к построению быстрых алгоритмов со степенными рядами был предложен ван дер Хувеном [5]. В методе ван дер Хувена также используется разбиение ряда на блоки длины k, но на каждой итерации вычисляются коэффициенты только одного очередного блока (такой способ назовем методом $Б$). В работе [5], как и в [2], использовались только ДПФ порядка $2k$.

Рассмотрим задачу извлечения квадратного корня из степенного ряда: требуется вычислить f_n, где $f = \sqrt{h}$, $h_1 = 1$. Обозначим $r = 1/f$. Итерация метода $Б$ записывается как

$$f_{m+k} = f_m + (h_{m+k} - f_m^2) r_k/2 \bmod x^{m+k}.$$

Для сложности квадратного корня в [2] указана оценка $11F(n)$. Метод $Б$-$2k$ позволяет улучшить ее до $8F(n)$. К дальнейшему улучшению оценки, до $7,5F(n)$, приводит $3k$-вариант метода $Б$.

Одна из возможностей ускорения реализации некоторых операций заключается в использовании двойных ДПФ. Двойное ДПФ порядка (n, m) (применяемое к набору коэффициентов многочлена переменной x) определяется следующим образом: первые n компонент

являются значениями ДПФ порядка n, а другие m компонент — композиции преобразования $x \to \zeta x$ и ДПФ порядка m, где ζ — подходящее комплексное число.

Применение ДПФ порядка $(2k, k)$ в методах A, $Б$ является эффективным для алгоритмов, использующих как обычные, так и тройные умножения рядов. Так, для вычисления экспоненты степенного ряда методом $Б$-$2k$ в работе [5] получена оценка $14F(n)$. Метод A-$(2k, k)$ позволяет улучшить ее до $13F(n)$.

Возведение ряда в произвольную степень обычно [3, 1] выполняется посредством логарифмирования, умножения на необходимую константу и вычисления экспоненты — это приводит к асимптотической оценке сложности $23F(n)$, если логарифмирование свести к делению (см. [3]), которое, как показано в [5], выполняется со сложностью $10F(n)$. Организуя итерационный процесс непосредственно для операции возведения в степень, можно построить алгоритм сложности $20,5F(n)$ методом $Б$-$(2k, k)$.

В таблице приводятся сведения о сложности обсуждавшихся операций, выделены результаты, которые, по-видимому, являются новыми. Аналогичные оценки имеют место для рядов с коэффициентами из алгебраически замкнутого поля, из $\mathbf{R}$, а также из произвольного кольца (при переопределении $F(n)$ в последнем случае, см. [1]).

Операция	$F(n)$	метод
Умножение	6	—
Инвертирование	**7,5**	A-$3k$
Деление и логарифм	10	$Б$-$2k$
Деление с остатком	12	$Б$-$2k$
Квадратный корень	**7,5**	$Б$-$3k$
Экспонента	**13**	A-$(2k, k)$
Возведение в степень	**20,5**	$Б$-$(2k, k)$

Автор благодарен научному руководителю С. Б. Гашкову за внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект 05-01-00994), Программы поддержки ведущих научных школ РФ (проект НШ-5400.2006.1) и Программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики» (проект «Синтез и сложность управляющих систем»).

Список литературы

1. Bernstein D. J. Fast multiplication and its applications. — 2004. — `http://cr.yp.to/papers.html#multapps`.

2. Bernstein D. J. Removing redundancy in high-precision Newton iteration. — 2004. — http://cr.yp.to/papers.html#fastnewton.

3. Brent R. Multiple-precision zero-finding methods and the complexity of elementary function evaluation // Analytic computational complexity. — NY: Academic Press, 1975. — P. 151–176.

4. von zur Gathen J., Gerhard J. Modern computer algebra. — Cambridge University Press, 1999.

5. van der Hoeven J. Newton's method and FFT trading. Tech. report. — Univ. Paris-Sud, Orsay, France, 2006.

6. Johnson F., Frigo M. A modified split-radix FFT with fewer arithmetic operations // IEEE Trans. Sign. Proc. — 2007. — V. 55, № 1. — P. 111-119.

7. Schönhage A. Variations on computing reciprocals of power series. // Inform. Proc. Letters. — 2000. — V. 74. — P. 41–46.

ПРЕОБРАЗОВАНИЕ ФУНКЦИОНАЛЬНЫХ УРАВНЕНИЙ И ПОКАЗАТЕЛИ СЛОЖНОСТИ БУЛЕВЫХ ФУНКЦИЙ

И. Ф. Чебурахин (Москва)

Рассмотрено развитие работы [1] по совершенствованию методов представления произвольной булевой функции $f^{(n)}$ над множеством переменных $X = \{x_1, ..., x_n\}$ в классе формул F в некотором базисе $G = \{g_1, ..., g_k\}$ (точнее $G_1 = \{\&, \vee, \neg\}$ или $G_2 = \{\&, \oplus, 1\}$) и/или в классе схем S из соответствующих базису G функциональных элементов (ФЭ) g_i (сохраняя для них обозначения функций). При этом целью изучения различных представлений функции является минимизация ее основных показателей сложности. В первом случае получаем суперпозиционную формулу F в базисе G, во втором случае — схему (с ветвлением и без) S из ФЭ, и соответствующие значения показателей сложности (качества) этого представления. Напомним их сокращенные обозначения: $L_{\text{Б}}$ — число букв и L_F — число подформул в формуле F, Dep_F — глубина F и, соответственно, L_S — число ФЭ в схеме S, Dep_S — глубина S. Если метод функциональных уравнений (ФУ)[2] в [1] применен к представлению функций формулами и схемами в разных базисах с получением оценок показателей сложности, то в этой работе они улучшаются на основе преобразования ФУ.

1. *Сложность n-местной дизъюнкции в разных базисах.* В [1] применено ФУ типа 1 и 2 (вариант 1), которые обозначаем ниже как — типов 1-1 и 2-1, к решению задачи: разработка методов рационального представления определенной булевой функции и получения соответствующих оценок для его различных показателей сложности. Этапы решения задачи: для класса булевых функций, начальных условий (функций g и h) и соответствующего базиса составляется основное ФУ, из которого выводится семейство ФУ для вышеуказанных показателей сложности; из основного ФУ выводим формулу F (схему S), реализующую заданную функцию, а из семейства ФУ — оценки показателей сложности (качества) представления.

В [1] получены оценки показателей сложности n-местной дизъюнкции

$$f^{(n)} = x_1 \vee x_2 \vee ... \vee x_n \tag{1}$$

в базисе G_2 на основе ФУ типа 1-1, т.е.

$$f^{(n)} = h(f^{(n-1)}, x_n) = (f^{(n-1)} \cdot x_n \oplus f^{(n-1)} \oplus x_n), \tag{2}$$

и типа 2-1 для случая $n = 2^s, s = 1, 2, ..., f_i = f(X_i), i = 1, 2,$

$$f^{(n)} = h^{(2)}(f_1^{(n/2)}, f_2^{(n/2)}) = (f_1^{(n/2)} \cdot f_2^{(n/2)} \oplus f_1^{(n/2)} \oplus f_2^{(n/2)}). \tag{3}$$

Ниже рассматривается вариант 2 начальных условий: $f^{(2)}(x_1, x_2) = g^{(2)}(x_1, x_2) = (x_1(x_2 \oplus 1) \oplus x_2)$ и $h^{(2)}(t_1, t_2) = (t_1(t_2 \oplus 1) \oplus t_2)$,
$L_{\text{Б}}(f^{(2)}, G_2) = L_{\text{Б}}(h^{(2)}, G_2) = 4, L_F(f^{(2)}, G_2) = L_F(h^{(2)}, G_2) = 3,$
$Dep_F(f^{(2)}, G_2) = Dep_F(h^{(2)}, G_2) = 3, L_S(f^{(2)}, G_2) = L_S(h^{(2)}, G_2) = 3,$
$Dep_S(f^{(2)}, G_2) = Dep_S(f^{(2)}, G_2) = 3.$ (4)

2. *Сложность на основе ФУ типа* 1. Преобразуя (2) к виду

$$f^{(n)} = h(f^{(n-1)}, x_n) = (f^{(n-1)} \cdot (x_n \oplus 1) \oplus x_n), \tag{5}$$

Для (5) устанавливаем рекуррентные соотношения
$L_{\text{Б}}(f^{(n)}, G_2) = L_{\text{Б}}(f^{(n-1)}, G_2) + 3$, $L_F(f^{(n)}, G_2) = L_F(f^{(n-1)}, G_2) + 3$,
$Dep_F(f^{(n)}, G_2) = Dep_F(f^{(n-1)}, G_2)+3, L_S(f^{(n)}, G_2) = L_S(f^{(n-1)}, G_2)+$
$+3$, $Dep_S(f^{(n)}, G_3) = Dep_S(f^{(n-1)}, G_2) + 3$,
откуда на основе (4) и (5) индукцией по n получаем

$$L_{\text{Б}}(f^{(n)}, G_2) = 3n - 2, \tag{6}$$

$$L_F(f^{(n)}, G_2) = L_S(f^{(n)}, G_2) = 3 \cdot (n - 1), \tag{7}$$

$$Dep_F(f^{(n)}, G_3) = Dep_S(f^{(n)}, G_2) = 3 \cdot (n-1). \qquad (8)$$

3. *Сложность на основе ФУ типа* 2. Преобразуем ФУ (3)

$$f^{(n)} = h(f_1^{(n/2)}, f_2^{(n/2)}) = (f_2^{(n/2)} \cdot (f_1^{(n/2)} \oplus 1) \oplus f_1^{(n/2)}). \qquad (9)$$

На основе ФУ (9) — типа 2-2 устанавливаем рекуррентные соотношения

$L_{\text{Б}}(f^{(n)}, G_2) = L_{\text{Б}}(f_1^{(n/2)}, G_2) + 2 \cdot L_{\text{Б}}(f_2^{(n/2)}, G_2) + 1,$
$L_F(f^{(n)}, G_2) = L_F(f_1^{(n/2)}, G_2) + 2 \cdot L_F(f_2^{(n/2)}, G_2) + 3,$
$L_S(f^{(n)}, G_2) = L_S(f_1^{(n/2)}, G_2) + L_S(f_2^{(n/2)}, G_2) + 3,$
$Dep_F(f^{(n)}, G_2) = Dep_F(f_1^{(n/2)}, G_2) + 3,$
$Dep_S(f^{(n)}, G_2) = Dep_S(f_1^{(n/2)}, G_2) + 3,$
откуда на основе (4) и (9) индукцией по s ($n = 2^s, s = 1, 2, \ldots$)

$$L_{\text{Б}}(f^{(n)}, G_2) = (3^{\log_2 n+1} - 1)/2, \qquad (10)$$

$$L_F(f^{(n)}, G_2) = 3(3^{\log_2 n} - 1)/2, \qquad (11)$$

$$L_S(f^{(n)}, G_2) = 3(n-1), \text{(применялись схемы с ветвлением)} \qquad (12)$$

$$Dep_F(f^{(n)}, G_2) = Dep_S(f^{(n)}, G_2) = 3 \cdot \log_2 n \qquad (13)$$

4. *Сравнение показателей сложности на основе ФУ типов* 1-2 *и* 2-2. Из сравнения результатов (6)-(8) и (10)-(13) представления функции (1) в базисе G_2 следует: уменьшение значений показателей $L_{\text{Б}}$ и L_F для ФУ типа 1-2, и - Dep_F и Dep_S для ФУ типа 2-2, сохранение - L_S для ФУ типа 1-2 и 2-2.

5. *Сложность n-местной линейной функции: случай* $n = 2^s, s = 1, 2, \ldots$. Аналогично получим показатели сложности представления линейной функции $f^{(n)} = x_1 \oplus x_2 \oplus \ldots \oplus x_n$ в базисе $G_1 = \{\&, \vee, \neg\}$ на основе ФУ типа 2 (для ФУ типа 1 см. [1]), точнее типа 2-1:

$L_{\text{Б}}(f^{(n)}, G_1) = n^2;$
$L_F(f^{(n)}, G_1) = 5(n^2-1)/3; L_S(f^{(n)}, G_1) = 5(n-1); Dep_F(f^{(n)}, G_1) = Dep_S(f^{(n)}, G_1) = 3\log_2 n$ (схемы с ветвлением), и типа 2-2:

$L_{\text{Б}}(f^{(n)}, G_1) = n^2;$
$L_F(f^{(n)}, G_1) = 4(n^2-1)/3; \qquad L_S(f^{(n)}, G_1) = 4(n-1);$

$Dep_F(f^{(n)}, G_1) = Dep_S(f^{(n)}, G_1) = 3\log_2 n$ (схемы с ветвлением), для которых ФУ соответственно имеют вид

$f^{(n)} = h^{(2)}(f_1^{(n/2)}, f_2^{(n/2)}) = ((\neg f_1^{(n/2)}) \cdot f_2^{(n/2)} \vee f_1^{(n/2)} \cdot (\neg f_2^{(n/2)}))$, $f^{(n)} = h^{(2)}(f_1^{(n/2)}, f_2^{(n/2)}) = (\neg(f_1^{(n/2)} \cdot f_2^{(n/2)}) \cdot (f_1^{(n/2)} \vee f_2^{(n/2)})$.

Список литературы

1. Чебурахин И. Ф. Функциональные уравнения и сложность булевых функций в разных базисах // Труды VII Межд.конф. "Дискретные модели в теории управляющих систем". — М.: МАКС Пресс, 2006.

2. Успенский В. А. Лекции о вычислимых функциях. — М., 1960.

3. Редькин Н. П. Доказательство минимальности некоторых схем из функциональных элементов // Проблемы кибернетики. Вып. 23. — 1970.

4. Ложкин С. А. О структуре минимальных схем из функциональных элементов, реализующих линейную функцию // Труды V Межд. конф. "Дискретные модели в теории управляющих систем". — М., 2003.

ТЕОРЕТИКО-ИНФОРМАЦИОННЫЙ ПОДХОД К ПОЛУЧЕНИЮ НИЖНИХ ОЦЕНОК СЛОЖНОСТИ

Д. Ю. Черухин (Москов)

В работе предложена аксиоматическая теория, описывающая количественные свойства информации. Показана возможность применения этой теории к получению эффективных нижних оценок сложности схем из функциональных элементов (СФЭ, [1]).

Информационным пространством (*ИП*) назовём систему $\mathrm{IS} = (M, \circ, |\cdot|)$, где M — множество объектов, называемых *сообщениями*, $\circ\colon M^2 \to M$ — операция *объединения* сообщений, $|\cdot|\colon M \to \mathbb{R}$ — функционал *нормы* сообщения, причём выполнены следующие аксиомы (для любых $x, y, z \in M$):

I. $x \circ x = x$	(идемпотентность)
II. $x \circ y = y \circ x$	(коммутативность)
III. $(x \circ y) \circ z = x \circ (y \circ z)$	(ассоциативность)
IV. $\exists \Lambda\ (\lvert\Lambda\rvert = 0\ \&\ \forall t\ \Lambda \circ t = t)$	(существование нуля)
V. $\lvert x \circ y\rvert + \lvert x \circ z\rvert \geqslant \lvert x \circ y \circ z\rvert + \lvert x\rvert$	(сильная субаддитивность)

Отметим, что под сообщением мы понимаем не конкретный текст, а нечто общее, присущее некоторым текстам, несущим одну и ту же информацию; норма сообщения есть количество информации. Отметим также, что теория ИП тесно связана с такими известными структурами, как субмодулярные решётки и матроиды.

Приведём три примера ИП.

1. M — алгебра измеримых множеств, $\circ$ — объединение множеств, $|\cdot|$ — мера множества.

2. M — множество подпространств данного линейного пространства, $\circ$ — сумма подпространств, $|\cdot|$ — размерность.

3. M — множество систем булевых функций, зависящих от переменных $x_1, \ldots, x_n$, $\circ$ — объединение систем, норму определим ниже. Для системы $S = \{f_1, \ldots, f_m\}$ введём отношение эквивалентности ρ_S на множестве $\{0,1\}^n$:

$$\tilde{x}\ \rho_S\ \tilde{y} \Longleftrightarrow \forall f \in S\ f(\tilde{x}) = f(\tilde{y}).$$

Пусть $K_1, \ldots, K_t$ — все классы эквивалентности отношения ρ_S. Положим

$$|S| = -\sum_{i=1}^{t} p_i \log_2 p_i, \quad \text{где } p_i = \frac{|K_i|}{2^n},\ i = 1, \ldots, t. \tag{1}$$

Например, если $1 \leqslant i_1 < \ldots < i_k \leqslant n$, то $|\{x_{i_1}, \ldots, x_{i_k}\}| = k$.

В трёх приведённых примерах наибольшую сложность вызывает доказательство сильной субаддитивности энтропии Шеннона (1). Далее мы будем работать только с примером 3.

Назовём *n-сетью* ациклический ориентированный граф с n входами и n выходами, в котором входная степень каждого входа равна 0, а входная степень любой вершины, отличной от входов, равна 2; входы и выходы упорядочены. Сложность сети есть число вершин, отличных от входов. Скажем, что СФЭ C *вписана* в сеть S, если C можно получить из S приписыванием всем вершинам, отличным от входов, двуместных булевых функций (считаем, что входам соответствуют переменные $x_1, \ldots, x_n$).

Рассмотрим оператор циклического сдвига [2] F_n с n информационными входами. Пусть $F_n^0, \ldots, F_n^{n-1}$ — его подоператоры, причём F_n^i получен из F_n подстановкой вместо управляющих переменных констант, образующих двоичную запись числа i. Тогда F_n^i — перестановочный оператор, полученный из тождественного циклическим сдвигом выходов на i позиций. В [2] показано, что сложность F_n в классе СФЭ нелинейна тогда и только тогда, когда нелинейна

минимальная сложность сети, в которую можно вписать СФЭ для каждого из операторов $F_n^0, \ldots, F_n^{n-1}$.

Пусть S — сеть, в которую вписаны СФЭ $C^0, \ldots, C^{n-1}$, где C^i реализует оператор F_n^i. Зафиксируем i. Каждой вершине v сети S припишем функцию $f_v^i(x_1, \ldots, x_n)$, вычисляемую в вершине v схемы C^i. Рассмотрим эту функцию, как сообщение ИП из примера 3 (функцию f мы отождествляем с системой $\{f\}$). Тогда, если вершина v непосредственно предшествует вершинам v' и v'', то

$$f_v^i \subseteq f_{v'}^i \circ f_{v''}^i, \tag{2}$$

где под вложением в ИП понимается следующее отношение:

$$x \subseteq y \iff |x \circ y| = |y|.$$

Прямой суммой ИП $(M_1, \circ_1, |\cdot|_1)$ и $(M_2, \circ_2, |\cdot|_2)$ называется ИП $(M_1 \times M_2, \circ, |\cdot|)$, где объединение $\circ$ выполняется покоординатно, а $|(x, y)| = |x|_1 + |y|_2$. Рассмотрим ИП IS_n, являющееся прямой суммой n экземпляров ИП из примера 3. Каждой вершине v сети S сопоставим сообщение $f_v = (f_v^0, \ldots, f_v^{n-1})$ ИП IS_n. Тогда вложение (2) сохранится, а именно,

$$f_v \subseteq f_{v'} \circ f_{v''}. \tag{3}$$

Отметим также, что норма одной булевой функции не больше единицы, а значит,

$$|f_v| \leqslant n. \tag{4}$$

Введём функцию $\rho(x, y)$, характеризующую меру зависимости сообщений:

$$\rho(x, y) = |x| + |y| - |x \circ y|.$$

В частности, если $\rho(x, y) = 0$, то можно сказать, что сообщения x и y *независимы*. Пусть $X = \{v_1, \ldots, v_k\}$ — множество некоторых входов сети S, а $Y = \{w_1, \ldots, w_l\}$ — множество некоторых её выходов, $|X| = k$, $|Y| = l$. Обозначим $f_X = f_{v_1} \circ \ldots \circ f_{v_k}$, $f_Y = f_{w_1} \circ \ldots \circ f_{w_l}$. Тогда

$$|f_X| = kn, \quad |f_Y| = ln, \quad \rho(f_X, f_Y) = kl. \tag{5}$$

Идея применения теории ИП к получению нижней оценки сложности СФЭ для оператора сдвига состоит в том, чтобы попробовать доказать нижнюю оценку для сложности сети S, в которой каждой вершине сопоставлено сообщение некоторого ИП, причём выполнены соотношения (3)–(5). На этом пути удалось получить нижнюю оценку $2,5n(1 - o(1))$.

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994), программы поддержки ведущих научных школ РФ (проект НШ–5400.2006.01) и программы "Университеты России" (проект УР.04.02.528).

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

2. Черухин Д. Ю. Об информационной составляющей в сложности оператора сдвига // Дискрет. анализ и исслед. операций. — 2005. — Т. 12, № 2. — с. 73–77.

О СЛОЖНОСТИ ОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ «ПОЧТИ СИММЕТРИЧЕСКИХ» ФУНКЦИЙ В КЛАССЕ &ДНФ

С. Е. Черухина (Москва)

В [1, 2] рассматривался класс монотонных булевых функций $\mathcal{F}_n$, определяемый следующим образом: $f(x_1, \ldots, x_n) \in \mathcal{F}_n$, если $S_n^2 \geqslant f \geqslant S_n^3$ (S_n^i — монотонная симметрическая функция с порогом i). Изучалась $L(f)$ — сложность реализации функций из этого класса формулами вида &∨& над базисом $\{\&, \vee\}$.

В частности, была получена нижняя оценка сложности $L(f)$ для функции, построенной на основе матрицы Нечипорука.

В данной работе рассматриваются функции, построенные на основе матриц, связанных с решениями определенных систем уравнений над полем Галуа [3], и для них доказываются нижние оценки сложности.

Используется следующая комбинаторная

Лемма. *Максимальное число единиц в матрице T размера $k \times k$, не имеющей подматриц размера $s \times s$, целиком состоящих из единиц (элементами T являются $\{0, 1\}$), не превышает*

$$(s-1)^{\frac{1}{s}} k^{2-\frac{1}{s}} + (s-1)k.$$

Из нее и результатов [1] следует

Теорема. *Существует некоторая* $f \in \mathcal{F}_n$ *такая, что* $L(f) = \Omega(n^{2-\varepsilon})$, *где* ε — *любое положительное число.*

Эта теорема усиливает нижнюю оценку $L(f) \geqslant 2M(f) - 7n$, (где $M(f)$ — количество наборов, содержащих ровно 2 единицы, на которых функция f обращается в 0), полученную в [1], до вида $L(f) = \Omega(2M(f)n^c)$, (c — константа, зависящая от $M(f)$).

Для сравнения с другими классами формул, отметим, что реализация "самой сложной" из рассматриваемых функций формулами без ограничений требует по порядку $\frac{n^2}{\log n}$ вхождений переменных, и для этого достаточно воспользоваться формулами вида $\vee$КНФ.

Список литературы

1. Черухина С. Е. О сложности реализации одного класса "почти симметрических" функций &$\vee$&-формулами // Материалы VIII Международного семинара "Дискретная математика и ее приложения" (Москва, 2–6 февраля 2004 г.). — М.: Изд-во механико-математического ф-та МГУ, 2004. — С. 109–111.

2. Черухина С. Е. О реализации "почти симметрических" функций // Тезисы докладов XIV Международной конференции "Проблемы теоретической кибернетики" (Пенза, 23–28 мая 2005 г.). — М.: Изд-во механико-математического ф-та МГУ, 2005. — С. 171.

3. Андреев А. Е. Об одном семействе булевых матриц // Вестник МГУ. Сер. 1. Матем. Мех. — 1986. — № 2. — С. 97–100.

О НАДЕЖНОСТИ СХЕМ В НЕКОТОРЫХ ПРИВОДИМЫХ ПОЛНЫХ БАЗИСАХ

В. В. Чугунова (Пенза)

Рассмотрим реализацию булевых функций схемами из ненадежных двухвходовых функциональных элементов. Схема реализует функцию $f(x_1, x_2, ..., x_n)$, если при поступлении на входы схемы набора $\tilde{a} = (a_1, a_2, ..., a_n)$ при отсутствии неисправностей на выходе схемы появляется значение $f(\tilde{a})$. Предполагается, что все входы элементов схемы независимо друг от друга с вероятностью ε $(0 < \varepsilon < 1/2)$ подвержены инверсным неисправностям. Эти неисправности характеризуются тем, что поступающее на вход элемента значение a, $(a \in \{0, 1\})$ с вероятностью ε может превратиться в значение $\bar{a}$.

Пусть $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ — вероятность появления значения $\bar{f}(\tilde{a})$ на выходе схемы S, реализующей булеву функцию $f(\tilde{x})$ при входном наборе $\tilde{a}$. Ненадежность $P(S)$ схемы S определяется как максимальное из чисел $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ при всевозможных входных наборах $\tilde{a}$. Надежность схемы S равна $1 - P(S)$.

Обозначим $P_\varepsilon(f) = \inf P(S)$, где S — схема из ненадежных элементов, реализующая булеву функцию f. Схему A из ненадежных элементов, реализующую булеву функцию f, назовем асимптотически оптимальной (наилучшей) по надежности, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \to 0$.

Пусть B' — это множество всех булевых функций, зависящих не более чем от двух переменных. Тогда множество попарно неконгруэнтных булевых функций, зависящих (возможно, фиктивно) от двух переменных, есть $M = \{\&, \vee, |, \downarrow, \to, \not\to, \sim, \oplus, \bar{}, 0, 1\}$.

Множество $B \subset M$ назовем неприводимым полным базисом (в P_2), если множество B полно и никакое его собственное подмножество полным не является.

Известно, что в P_2 существует 17 (с точностью до переименования переменных) неприводимых полных базисов, содержащих функции не более чем двух переменных: $B_1 = \{|\}$, $B_2 = \{\downarrow\}$, $B_3 = \{\to, \not\to\}$, $B_4 = \{\to, \oplus\}$, $B_5 = \{\not\to, \sim\}$, $B_6 = \{\oplus, \&, 1\}$, $B_7 = \{\sim, \vee, 0\}$, $B_8 = \{\sim, \&, \oplus\}$, $B_9 = \{\sim, \vee, \oplus\}$, $B_{10} = \{\sim, \&, 0\}$, $B_{11} = \{\oplus, \vee, 1\}$, $B_{12} = \{\not\to, \bar{}\}$, $B_{13} = \{\to, \bar{}\}$, $B_{14} = \{\not\to, 1\}$, $B_{15} = \{\to, 0\}$, $B_{16} = \{\&, \bar{}\}$, $B_{17} = \{\vee, \bar{}\}$. Любой другой базис, отличный от базисов $B_1 - B_{17}$ (например, $B_{18} = \{\&, \vee, \bar{}\}$), можно получить переименованием переменных без отождествления, а также добавлением одной или нескольких функций из множества M к некоторому базису из указанного списка.

Пусть базис B — один из базисов $B_1 - B_{18}$, тогда для него справедливы теоремы 1 и 2 [1].

Теорема 1. *Пусть константы a, b, c, d (см. табл.) соответствуют базису B и $\varepsilon \in (0; d\,]$. Тогда любую булеву функцию $f(\tilde{x})$ в базисе B можно реализовать такой схемой S, что $P(S) \le a\varepsilon + b\varepsilon^2$.*

Теорема 2. *Пусть константы $a, \hat{b}, \hat{d}$ и класс булевых функций $K(n)$ (см. табл.) соответствуют базису B. Тогда для любой булевой функции $f(\tilde{x})$, $f \notin K(n)$, и любой схемы S, реализующей f в базисе B, при $\varepsilon \in (0; \hat{d}\,]$ верно неравенство $P(S) \ge a\varepsilon + \hat{b}\varepsilon^2$, причем a — та же константа, что и в теореме* 1.

B	a	b	d	$\hat{b}$	$\hat{d}$	$K(n)$
$B_1 = \{\mid\}$	2	19	1/100	-1	1/4	$x_i, 1$
$B_2 = \{\downarrow\}$	2	19	1/100	-1	1/4	$x_i, 0$
$B_3 = \{\rightarrow, \not\rightarrow\}$	2	51	1/300	-1	1/4	$x_i, 0, 1$
$B_4 = \{\rightarrow, \oplus\}$	2	66	1/200	-2	1/4	$x_i, 1$
$B_5 = \{\not\rightarrow, \sim\}$	2	66	1/200	-2	1/4	$x_i, 0$
$B_6 = \{\oplus, \&, 1\}$	2	67	1/200	-2	1/4	$x_i, 0, 1$
$B_7 = \{\sim, \vee, 0\}$	2	67	1/200	-2	1/4	$x_i, 0, 1$
$B_8 = \{\sim, \&, \oplus\}$	2	62	1/300	-2	1/4	$x_i, 0$
$B_9 = \{\sim, \vee, \oplus\}$	2	62	1/300	-2	1/4	$x_i, 1$
$B_{10} = \{\sim, \&, 0\}$	2	66	1/200	-2	1/4	$x_i, 0$
$B_{11} = \{\oplus, \vee, 1\}$	2	66	1/200	-2	1/4	$x_i, 1$
$B_{12} = \{\not\rightarrow, ^-\}$	3	41	1/150	-6	1/6	$x_i^\delta \& h(\tilde{x}), 1$
$B_{13} = \{\rightarrow, ^-\}$	3	41	1/150	-6	1/6	$x_i^\delta \vee h(\tilde{x}), 0$
$B_{14} = \{\not\rightarrow, 1\}$	4	59	1/200	-8	1/11	$(x_i^\delta \& h(\tilde{x}))^\mu$
$B_{15} = \{\rightarrow, 0\}$	4	59	1/200	-8	1/11	$(x_i^\delta \& h(\tilde{x}))^\mu$
$B_{16} = \{\&, ^-\}$	4	83	1/200	-12	1/10	$(x_i^\delta \& h(\tilde{x}))^\mu$
$B_{17} = \{\vee, ^-\}$	4	83	1/200	-12	1/10	$(x_i^\delta \& h(\tilde{x}))^\mu$
$B_{18} = \{\&, \vee, ^-\})$	2	19	1/150	-2	1/6	$x_i, 0, 1$

Используемые в таблице обозначения: $i = \overline{1,n}$, $\delta, \mu \in \{0,1\}$, $h(\tilde{x})$ — произвольная булева функция от n переменных.

Из теоремы 2 следует, что схемы, построенные при доказательстве теоремы 1, являются асимптотически оптимальными по надежности для почти всех функций.

Заметим, что если к базису $\{\&, ^-\}$ добавить дизъюнкцию $\vee$, то оценка ненадежности значительно улучшается с 4ε до 2ε. Какой же будет эта оценка, если базис B' содержит все функции, зависящие не более чем от двух переменных? Справедливы теоремы 3 и 4.

Теорема 3. *Пусть в базисе B' $\varepsilon \leq 1/300$, а $f(\tilde{x})$ — произвольная функция. Тогда функцию f в базисе B' можно реализовать схемой S, ненадежность которой $P(S) \leq 2\varepsilon + 19\varepsilon^2$.*

Доказательство следует из того, что $B' \supset \{\mid\}$.

Пусть $\hat{K}(n)$ — множество функций $f(x_1, x_2, ..., x_n)$, отличных от функций x_i, $\bar{x}_i$ и $0, 1 (i = 1, 2, ..., n)$. Очевидно, $|\hat{K}(n)| = 2n + 2$.

Теорема 4. *Пусть $\varepsilon \leq 1/6$, $f(\tilde{x})$ — булева функция, $f \notin \hat{K}(n)$, и S — любая схема в базисе B', реализующая f. Тогда $P(S) \geq 2\varepsilon - 2\varepsilon^2$.*

Для доказательства достаточно выделить связную подсхему, содержащую выход схемы S и состоящую не более чем из двух элементов.

Из теоремы 4 следует, что схемы, построенные при доказательстве теоремы 3, являются асимптотически оптимальными по надежности для почти всех функций в базисе B'.

Рассмотрим менее "богатые" полные базисы. Пусть $Б$ один из базисов $\{\&, \vee, \bar{}\}$, $\{\&, \bar{}, |\}$, $\{\&, \bar{}, \downarrow\}$, $\{\&, \bar{}, \sim\}$, $\{\&, \bar{}, \oplus\}$, $\{\&, \bar{}, \to\}$, $\{\vee, \bar{}, \downarrow\}$, $\{\vee, \bar{}, \not\to\}$, $\{\vee, \bar{}, |\}$, $\{\vee, \bar{}, \oplus\}$, $\{\vee, \bar{}, \sim\}$ или получен из одиннадцати названных базисов добавлением любых других функций двух переменных. Тогда в базисе $Б$ справедливы теоремы 5 и 6.

Теорема 5. *При $\varepsilon \leq 1/300$ любую булеву функцию $f(\tilde{x})$ в базисе $Б$ можно реализовать такой схемой S, ненадежность которой $P(S) \leq 2\varepsilon + 70\varepsilon^2$.*

Теорема 6. *Пусть $\varepsilon \leq 1/6$, $f(\tilde{x})$ — булева функция, $f \notin \hat{K}(n)$, и S — любая схема, реализующая f в базисе $Б$. Тогда $P(S) \geq 2\varepsilon - 2\varepsilon^2$.*

Из теоремы 6 следует, что схемы, построенные при доказательстве теоремы 5, являются асимптотически оптимальными по надежности для почти всех функций в базисе $Б$.

Список литературы

1. Чугунова В. В. Синтез асимптотически оптимальных по надежности схем при инверсных неисправностях на входах элементов // Автореферат канд. дис. Пенза: Изд-во Пенз. гос. ун-та, 2007.

ОПЕРАЦИЯ УМНОЖЕНИЯ ЭЛЕМЕНТОВ ПОЛЕЙ ГАЛУА $GF((2^k)^l)$

С. В. Шалагин (Казань)

Операция умножения элементов поля Галуа является базовой при реализации широкого класса устройств [1–7]. В частности, операция умножения над элементами расширений полей Галуа вида $GF((2^k)^l)$ позволяет осуществить распараллеливание процесса вычислений и потоковую обработку данных. Выполнение умножения сводится к операциям над элементами $GF(2^k)$ [8]. Существует возможность организовать конвейерную обработку данных путем сохранения промежуточных результатов. Это способствует уменьшению времени задержки функционирования для устройств, реализующих данную

операцию — схем умножения (СУ). Проведены исследования реализации СУ элементов $GF(2^k)$ (СУ/$GF(2^k)$) на ПЛИС класса (семейства, серии) FPGA [9]. Теоретические исследования операций над частными случаями $GF((2^k)^l)$ и их приложения описаны в [4, 7]. Вышеизложенное позволяет ставить вопрос об актуальности исследования реализации СУ/$GF((2^k)^l)$. Для СУ/$GF(2^k)$ имеет место

Теорема 1. *Вычисление произведения элементов вида* $\alpha = (\alpha_0\ \alpha_1\ ...\ \alpha_{k-1})^T$ *и* $\beta = (\beta_0\ \beta_1\ ...\ \beta_{k-1})^T$ *поля Галуа* $GF(2^k)$ *производится по формуле вида*

$$\begin{pmatrix} c_0 \\ c_1 \\ ... \\ c_{k-1} \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 + \alpha_1\beta_0 \\ ... \\ \alpha_0\beta_{k-1} + ... + \alpha_{k-1}\beta_0 \end{pmatrix} + \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ ... \\ \alpha_{k-1} \end{pmatrix}^T \begin{pmatrix} \beta_{k-1} \\ ... \\ \beta_2 \\ \beta_1 \end{pmatrix} \xi^k +$$

$$+ \begin{pmatrix} \alpha_2 \\ ... \\ \alpha_{k-1} \end{pmatrix}^T \begin{pmatrix} \beta_{k-1} \\ ... \\ \beta_2 \end{pmatrix} \xi^{k+1} + ... + \alpha_{k-1}\beta_{k-1}\xi^{2k-2}, \qquad (1)$$

где $\alpha_i,\ \beta_i,\ c_i \in GF(2),\ i = \overline{0,\ k-1},\ \xi^m,\ m = \overline{k,\ (2k-2)},$ *— степени примитивного элемента* $\xi \in GF(2^k)$, *постоянные величины* [10].

Для СУ/$GF(2^k)$ значения разрядов произведения вычисляются параллельно и независимо, что способствует снижению оценок временной сложности. Оценки временной и емкостной сложности СУ/$GF(2^k)$, представленной в виде (1) — $T_{GF(2^k)}$ и $Q_{GF(2^k)}$, получены на основе частного случая равнодоступной адресной машины — "битовые вычисления":

$$T_{GF(2^k)} =]\log_2 2k] = 1 +]\log_2 k]; \qquad (2)$$

$$Q_{GF(2^k)} = \sum_{i=0}^{k-1} (2k-1) = k(2k-1). \qquad (3)$$

В общем случае, для расширения поля Галуа вида $GF((2^k)^l)$ справедлива

Теорема 2. *Вычисление произведения элементов вида* $\alpha = (\alpha_0\ \alpha_1\ ...\ \alpha_{l-1})^T$ *и* $\beta = (\beta_0\ \beta_1\ ...\ \beta_{l-1})^T$ *расширения поля Галуа* $GF((2^k)^l)$ *производится по формуле*

$$\begin{pmatrix} c_0 \\ c_1 \\ ... \\ c_{l-1} \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 + \alpha_1\beta_0 \\ ... \\ \alpha_0\beta_{l-1} + ... + \alpha_{l-1}\beta_0 \end{pmatrix} + \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ ... \\ \alpha_{l-1} \end{pmatrix}^T \begin{pmatrix} \beta_{l-1} \\ ... \\ \beta_2 \\ \beta_1 \end{pmatrix} \xi^l +$$

$$+\begin{pmatrix}\alpha_2\\ \dots\\ \alpha_{l-1}\end{pmatrix}^T\begin{pmatrix}\beta_{l-1}\\ \dots\\ \beta_2\end{pmatrix}\xi^{l+1}+\dots+\alpha_{l-1}\beta_{l-1}\xi^{2l-2}, \qquad (4)$$

где $\alpha_i,\ \beta_i,\ c_i \in GF(2^k),\ i=\overline{0,\ l-1},\ \xi^m \in GF((2^k)^l),\ m=\overline{l,\ (2l-2)}$, — *степени примитивного элемента* $\xi \in GF((2^k)^l)$, *постоянные величины.*

На базе теоремы 2 согласно (4) получены сложностные оценки для СУ/$GF((2^k)^l)$ при заданных l. Оценки временной сложности для них будут меньше, чем для СУ/$GF(2^n)$, где $n=k\cdot l$, в силу особенностей их архитектуры, адекватной базису ПЛИС/FPGA. Операция умножения элементов $GF((2^k)^l)$ сводится к операциям над элементами $GF(2^k)$. На основе (2) и (3) получены оценки временной и емкостной сложности реализации СУ/$GF((2^k)^l)$, равные $T_{G_{kl}}=\max\left(T_{GF(2^k)},\ \max\limits_{i=\overline{0,l-1}} T_i\right)$, и

$$T_i=\left\rceil \log_2\left(1+i+k\sum_{j=l}^{2l-2}(2l-1-j)(\xi_i^j\neq 0)\right)\right\rceil,$$

$$Q_{G_{kl}}=l^2Q_{GF(2^k)}+k\sum_{i=0}^{l-1}\left(i+k\sum_{j=l}^{2l-2}(2l-1-j)\left(\xi_i^j\neq 0\right)\right),$$

где $\xi^m=\left(\xi_0^m\ \dots\ \xi_{l-1}^m\right)\in GF((2^k)^l)$, $\xi_{l-1}^m\in GF(2^k)$, $i=\overline{0,\ l-1}$, $m=\overline{f,\ (2f-2)}$.

Список литературы

1. Захаров В. М., Нурутдинов Ш. Р., Шалагин С. В. Полиномиальное представление цепей Маркова над полем Галуа // Вестник КГТУ им. А. Н. Туполева. — 2001. — № 3. — С. 27 –31.

2. Захаров В. М., Нурутдинов Ш. Р. Шалагин С. В. Реализация полиномиальных моделей над полем GF(2^n) неоднородных цепей Маркова и их функций в базисе ПЛИС/FPGA // Тез. докл. 4-й ежегодной Межд. науч.-пр. конф. "Инфокоммуникац. технологии глобальн. информационного общества". — Казань: ЦИТ, 2006. — С. 62–66.

3. Шалагин С. В. Синтез генераторов дискретной случайной величины над полем GF(2^n) // Матер. пятого Всерос. семинара "Сеточные методы для краевых задач и приложения". — Казань: Изд-во КГУ, 2004. — С. 236–240.

4. Paar C., Fleischmann P., Roelse P. Efficient multiplier architectures for Galois fields GF($(2^4)^n$) // IEEE Trans. on Computers. — 1998. — V. 47, № 2. — P. 162–170.

5. Orlando G., Paar C. A high-performance reconfigurable elliptic curve processor for GF(2^m) // Workshop on Cryptographic Hardware and Embedded Systems (CHES). — Springer-Verlag, 2000.

6. Paar C., Fleischmann P., Soria-Rodriguez P. Fast arithmetic for public-key algorithms in Galois fields with composite exponents // IEEE Trans. on Computers. — 1999. — V. 48, № 10. — P. 1025–1034.

7. Нурутдинов Ш. Р. Основы теории полиномиальных моделей автоматных преобразований над полем Галуа. — Казань: Изд-во КГУ, 2005.

8. Лидл Р., Нидеррайтер Г. Конечные поля. — М.: Мир, 1988.

9. Шалагин С. В. Экспериментальное исследование методики синтеза комбинационных схем на программируемых микросхемах класса FPGA // Микроэлектроника. — 2004. — Т. 33, № 1. — С.56–67.

10. Шалагин С. В. Оценка сложности для операций умножения элементов поля Галуа // Материалы всерос. научн. конф. молодых ученых. Ч. 1. — Новосибирск: Изд-во НГТУ. — С. 76–78.

О СЛОЖНОСТИ ДИАГНОСТИКИ НЕКОТОРЫХ НЕИСПРАВНОСТЕЙ В СХЕМАХ

В. И. Шевченко (Нижний Новгород)

Рассматриваются схемы из функциональных элементов формульного типа, то есть схемы, в которых разветвления могут быть только на входах схемы [1]. В каждой такой схеме в результате воздействия "источника неисправностей" некоторые входы элементов и выходы некоторых элементов могут находиться в неисправном состоянии. Пусть B — произвольное конечное множество функциональных элементов (схемный базис), S — схема в базисе B, в которой n входов ($n \geq 1$), один выход, l функциональных элементов ($l \geq 1$), и пусть $f(x_1, \ldots, x_n)$ — булева функция, реализуемая S. Входы схемы S и выходы ее элементов иногда будем называть *вершинами*. Занумеруем вершины S от 1 до $N = n + l$ по порядку следующим образом: сначала нумеруем входы S (вершины нулевого уровня), затем выходы элементов, входы которых присоединены только к входам S

(вершины первого уровня), далее нумеруем выходы элементов, входы которых присоединены только к вершинам нулевого и первого уровней, и так далее. Через e_i обозначим элемент S, выход которого имеет номер $n+i$, через $\phi_i(x_1,\ldots,x_p)$ — функцию, приписанную e_i, через $j_1,\ldots,j_p$ — номера вершин S, к которым присоединены входы e_i, а через $A_1,\ldots,A_N$ — функции, которые схема S реализует в вершинах $1,2,\ldots,N$ соответственно. В качестве возможных неисправностей рассматриваются "1" или "И" ("0" или "ИЛИ") замыкания на некоторых входах элементов и выходах некоторых элементов S. В дальнейшем будем говорить только об "1" или "И" замыканиях, для "0" или "ИЛИ" замыканий все определяется и формулируется аналогичным образом. Если произошло "1" замыкание выхода (j_s входа) элемента e_i, то на выходе e_i получаем константу 1 (на j_s вход e_i поступает константа 1). Если произошло "И" замыкание выхода (j_s входа) элемента e_i с вершинами $r_1,\ldots r_k$ предыдущих уровней, то на выходе e_i получаем значение конъюнкции $A_i\cdot A_{r_1}\ldots\cdot A_{r_k}$ (на j_s вход e_i поступает значение конъюнкции $A_{j_s}\cdot A_{r_1}\ldots\cdot A_{r_k}$).

Задача диагностики схемы S, которая, возможно, содержит неисправности состоит в том, чтобы определить функцию, которую она реализует. Для решения этой задачи используются деревья решений (условные тесты) [2–3].

Дерево решений Y для решения этой задачи представляет собой конечное ориентированное корневое дерево, в котором каждой вершине, не являющейся концевой, приписан двоичный набор из $\{0,1\}^n$, каждой концевой вершине — некоторое число из множества $1,\ldots,m$. Из каждой вершины, не являющейся концевой, исходят ровно две дуги, которым приписаны числа 0 и 1. Далее, для любой функции $f_i\in F(S)$ найдется полный путь (от корня до концевой вершины) $\gamma=v_1,u_1,\ldots,u_r,v_{r+1}$ такой, что вершине v_{r+1} приписано число i и, если при $q=1,\ldots,r$ вершине v_q приписан набор $\alpha_q\in\{0,1\}^n$, а дуге u_q — число $\delta_q\in\{0,1\}$, то функция f_i — единственная функция в $F(S)$, которая на наборах $\alpha_1,\ldots,\alpha_r$ принимает значения $\delta_1,\ldots,\delta_r$ соответственно. Максимальную длину полного пути дерева решений Y обозначим через $h(Y)$. Пусть $d(S)=\min h(Y)$, где минимум берется по всем деревьям решений для диагностики S (*минимальная глубина деревьев решений* для диагностики S), а $d_B(N)=\max d(S)$, где максимум берется по всем схемам в базисе B, число вершин в которых не превосходит N. В работе для всевозможных конечных схемных базисов исследуются верхние и нижние оценки функции $d_B(N)$ — минимальной глубины деревьев решений для схем в базисе B, число вершин в которых не превосходит N, в худшем случае.

Справедлива

Теорема. 1) *Если все элементы базиса B реализуют только конъюнкции или константы, то для $N \geq 2$ справедливы неравенства*

$$N - 1 \leq d_B(N) \leq N;$$

2) *если все элементы базиса B реализуют только монотонные булевы функции и при этом B содержит хотя бы один элемент, реализующий функцию, отличную от конъюнкции и константы, то для $N \geq 2$ имеют место неравенства*

$$2^{\lfloor (N-1)/3 \rfloor} \leq d_B(N) \leq \binom{N}{\lfloor N/2 \rfloor + 1};$$

3) *если хотя бы один элемент базиса B реализует немонотонную булеву функцию, то для $N \geq 2$ справедливы неравенства*

$$2^{\lfloor (N-1)/2 \rfloor} - 1 \leq d_B(N) \leq 2^{N-1}.$$

Вспомогательные утверждения

Лемма 1. *Если ϕ — монотонная булева функция и не является ни конъюнкцией и не константой, то из нее путем отождествления переменных и подстановки константы 1 можно получить функцию $x \vee y$.*

Лемма 2. *Если ϕ — немонотонная булева функция, то из нее путем подстановки константы 1 и функций вида x, $x \cdot y$ можно получить одну из функций вида $\bar{x}$, $x + y + 1$, $x \vee \bar{y}$.*

Лемма 3. *Пусть булевы функции $\alpha(x_1, \ldots, x_p)$ и $\beta(x_1, \ldots, x_q)$ такие, что $\beta(x_1, \ldots, x_q)$ может быть получена из $\alpha(x_1, \ldots, x_p)$ подстановкой константы 1 и функций вида x, $x \cdot y$, а базисы $B_1 = \{E_1\}$ и $B_2 = \{E_2\}$ такие, что элемент E_1 реализует функцию $\alpha(x_1, \ldots, x_p)$, элемент E_2 реализует функцию $\beta(x_1, \ldots, x_q)$. Тогда $d_{B_1}(N) \geq d_{B_2}(N)$ при любом $N \geq 2$.*

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

2. Мошков М. Ю. Деревья решений. Теория и приложения. — Нижний Новгород: Изд-во ННГУ, 1994.

3. Чегис И. А., Яблонский С. В. Логические способы контроля работы электрических схем // Тр. Матем. ин-та АН СССР. — 1958. — Т. 51. — С. 270–360.

ВЕРХНИЕ ОЦЕНКИ НЕНАДЕЖНОСТИ СХЕМ В НЕКОТОРЫХ ПОЛНЫХ НЕПРИВОДИМЫХ БАЗИСАХ

А. В. Шилов (Пенза)

Рассматривается реализация булевых функций схемами из ненадежных функциональных элементов. Предполагается, что все элементы схемы ненадежны и подвержены инверсным неисправностям на выходах. Во всех полных неприводимых базисах, содержащих функции не более чем двух переменных, получены верхние оценки ненадежности схем, реализующих произвольные булевы функции.

Впервые задачу синтеза надежных схем из ненадежных элементов рассматривал Дж. Нейман [1]. Он предполагал, что элементы подвержены инверсным неисправностям на выходах, когда функциональный элемент с приписанной ему булевой функцией $\varphi(\tilde{x})$ в неисправном состоянии, в которое переходит с вероятностью $\varepsilon \in (0, 1/2)$, реализует функцию $\bar{\varphi}(\tilde{x})$. С помощью итерационного метода Дж. Нейман установил, что при $\varepsilon \in (0, 1/6)$ произвольную булеву функцию можно реализовать схемой, вероятность ошибки на выходе которой при любом входном наборе значений переменных не превосходит $c\varepsilon$, где c — некоторая абсолютная константа, зависящая от базиса. С. И. Аксенов уточнил значение константы c. Он показал [2], что над произвольным полным базисом при $\varepsilon \leq \varepsilon_0$ любую булеву функцию можно реализовать схемой, вероятность ошибки на выходе которой при любом входном наборе значений переменных асимптотически не больше 5ε. Для некоторых полных базисов константу 5 в последнем неравенстве можно уменьшить [3]. В этой работе приведены верхние оценки для вероятностей ошибок во всех полных неприводимых базисах, содержащих функции не более чем двух от переменных.

Введем базисы: $B_1 = \{\not\to, \sim\}$, $B_2 = \{\to, \oplus\}$, $B_3 = \{\oplus, \&, 1\}$, $B_4 = \{\sim, \&, 0\}$, $B_5 = \{\sim, \&, \oplus\}$, $B_6 = \{\sim, \vee, 0\}$, $B_7 = \{\sim, \vee, \oplus\}$, $B_8 = \{\oplus, \vee, 1\}$, $B_9 = \{|\}$, $B_{10} = \{\downarrow\}$, $B_{11} = \{\to, \not\to\}$, $B_{12} = \{\not\to, \bar{}\}$, $B_{13} = \{\to, \bar{}\}$, $B_{14} = \{\to, 0\}$, $B_{15} = \{\not\to, 1\}$, $B_{16} = \{\&, \bar{}\}$, $B_{17} = \{\vee, \bar{}\}$.

Использованы следующие обозначения: $x|y = \bar{x} \vee \bar{y}$, $x \downarrow y = \bar{x}\&\bar{y}$, $x \sim y = x\&y \vee \bar{x}\&\bar{y}$, $x \oplus y = x\&\bar{y} \vee \bar{x}\&y$, $x \to y = \bar{x} \vee y$, $x \not\to y = x\&\bar{y}$.

Известно, что любой полный базис в P_2, содержащий функции двух переменных, отличный от приведенных базисов, получается переименованием переменных без отождествления, а также добавлением одной или нескольких функций к некоторому базису из этого списка.

Пусть $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ — вероятность появления значения $\bar{f}(\tilde{a})$ на вы-

ходе схемы S, реализующей функцию $f(\tilde{x})$ при входном наборе $\tilde{a}$. *Ненадежность* схемы S равна $P(S) = \max\{P_{\overline{f(\tilde{a})}}(S, \tilde{a})\}$, где максимум берется по всем всем входным наборам $\tilde{a}$ схемы S. *Надежность* схемы S равна $1 - P(S)$.

Замечание. Нетрудно проверить, что ненадежность любой схемы, содержащей хотя бы один функциональный элемент, не меньше ε, т. е. $P(S) \geq \varepsilon$.

Теорема. *Каждому из базисов B_1–B_{17} можно сопоставить константы a, b, d (см. табл.) такие, что при $\varepsilon \in (0, d]$ произвольную булеву функцию можно реализовать схемой S, ненадежность которой $P(S) \leq a\varepsilon + b\varepsilon^2$.*

Таблица

B	a	b	d
$B_1 = \{\not\rightarrow, \sim\}$	2	29	1/160
$B_2 = \{\rightarrow, \oplus\}$	2	29	1/160
$B_3 = \{\oplus, \&, 1\}$	2	27	1/240
$B_4 = \{\sim, \&, 0\}$	2	27	1/240
$B_5 = \{\sim, \&, \oplus\}$	2	27	1/240
$B_6 = \{\sim, \vee, 0\}$	2	27	1/240
$B_7 = \{\sim, \vee, \oplus\}$	2	27	1/240
$B_8 = \{\oplus, \vee, 1\}$	2	27	1/240
$B_9 = \{\mid\}$	3	126	1/600
$B_{10} = \{\downarrow\}$	3	126	1/600
$B_{11} = \{\rightarrow, \not\rightarrow\}$	3	72	1/160
$B_{12} = \{\not\rightarrow, \bar{}\}$	4	64	1/160
$B_{13} = \{\rightarrow, \bar{}\}$	4	64	1/160
$B_{14} = \{\rightarrow, 0\}$	5	91	1/160
$B_{15} = \{\not\rightarrow, 1\}$	5	91	1/160
$B_{16} = \{\&, \bar{}\}$	5	99	1/240
$B_{17} = \{\vee, \bar{}\}$	5	99	1/240

Доказательство этой теоремы опубликовано в статье [4].

Список литературы

1. фон Нейман Дж. Вероятностная логика и синтез надежных организмов из ненадежных компонент // Автоматы. — М.: ИЛ, 1956. — С. 68–139.

2. Аксенов С. И. О надежности схем над произвольной полной системой функций при инверсных неисправностях на выходах элементов // Известия высших учебных заведений. Поволжский регион. Естественные науки. — 2005. — № 6. — С. 42–55.

3. Аксенов С. И. О надежности схем над частными классами полных систем при инверсных неисправностях на выходах элементов // Труды VII международной конференции "Дискретные модели в теории управляющих систем" (Покровское, 4–6 марта 2006 г.). — М.: МАКС Пресс, 2006. — С. 10–16.

4. Алехина М. А., Шилов А. В. Верхние оценки ненадежности схем в некоторых базисах при инверсных неисправностях на выходах элементов // Известия вузов. Поволжский регион. Естественные науки. — 2006. — № 5 (26). — С. 116–125.

КАЧЕСТВЕННЫЕ УСЛОВИЯ ОПТИМАЛЬНОСТИ МЕТОДА ПОСЛЕДОВАТЕЛЬНОЙ РЕАЛИЗАЦИИ

Л. А. Шоломов (Москва)

Рассматривается реализация частичных булевых функций схемами из функциональных элементов в произвольном конечном базисе. Определения схемы, сложности $L(S)$ схемы S и сложности $L(F)$ системы функций F см. в [1]. Запись S_F будем применять для обозначения некоторой схемы, реализующей систему F, а $S \subseteq S'$ будет означать, что схема S является подсхемой схемы S'.

Пусть (f, g) — система двух частичных функций. Будем рассматривать последовательную реализацию этой системы, когда вначале строится схема S_f, которая затем достраивается до $S_{f,g}$. *Сложностью последовательной реализации* пары (f, g) при ограничении t, $t \geq L(f)$, на сложность реализации функции f назовем величину

$$L_t(f, g) = \min\{s \mid \exists S_f \exists S_{f,g}(S_f \subseteq S_{f,g},\ L(S_f) \leq t,\ L(S_{f,g}) \leq s)\}.$$

Для пары $(f(\tilde{x}), g(\tilde{x}))$, $\tilde{x} = (x_1, \ldots, x_n)$, обозначим через $l_{\alpha\beta}(f, g)$, $\alpha, \beta \in \{0, 1, *\}$, число наборов $\tilde{x}$, на которых $f(\tilde{x}) = \alpha$, $g(\tilde{x}) = \beta$ (символ $*$ соответствует неопределенному значению). Пару (f, g) будем характеризовать набором $\mathbf{l}(f, g) = (l_{\alpha\beta}(f, g),\ \alpha, \beta \in \{0, 1, *\})$. Введем класс $\mathcal{K}_n(f, g) = \{(f', g') \mid \mathbf{l}(f', g') = \mathbf{l}(f, g)\}$ и функцию Шеннона

$$L(n, f, g) = \max\{L(f', g') \mid (f', g') \in \mathcal{K}_n(f, g)\}.$$

Аналогично для функции f могут быть определены параметры $l_\alpha(f)$, введены набор $\mathbf{l}(f)$, класс $\mathcal{K}_n(f)$ и функция Шеннона $L(n, f)$.

Задавшись функцией $t(n)$, $t(n) \geq L(n, f)$, введем *функцию Шеннона для последовательной реализации* при ограничении $t(n)$

$$L_{t(n)}(n, f, g) = \max\{L_{t(n)}(f', g') \mid (f', g') \in \mathcal{K}_n(f, g)\}.$$

Будем рассматривать асимптотическое поведение функций Шеннона, считая пару (f, g) членом последовательности пар $(f^{(n)}, g^{(n)})$ от n аргументов. В работе изучаются условия одновременной достижимости при последовательной реализации асимптотик для $L(n, f)$ и $L(n, f, g)$, т. е. соотношения $L_{t(n)}(n, f, g) \sim L(n, f, g)$ при некотором $t(n) \sim L(n, f)$. В случае достижимости будем говорить, что метод последовательной реализации *асимптотически оптимален* для класса $\mathcal{K}_n(f, g)$ при упорядочении (f, g). Если он асимптотически оптимален при каком-либо из упорядочений (f, g) и (g, f) будем говорить о его асимптотической оптимальности для $\mathcal{K}_n(f, g)$.

Пары функций (f, g) и (f', g') будем называть *сходными*, если они принимают одинаковое множество значений (α, β), т. е. для них $l_{\alpha\beta}(f, g) > 0 \Leftrightarrow l_{\alpha\beta}(f', g') > 0$, $\alpha, \beta \in \{0, 1, *\}$. Условие на пары (f, g) назовем *качественным*, если им обладают все пары, сходные с (f, g). Будем говорить, что качественное условие на пары (f, g) *обеспечивает асимптотическую оптимальность* метода последовательной реализации при заданном ограничении на функцию Шеннона $L(n, f, g)$, если для любой пары (f, g), удовлетворяющей этому условию и такой, что для $L(n, f, g)$ выполнено заданное ограничение, метод последовательной реализации асимптотически оптимален для класса $\mathcal{K}_n(f, g)$. Если ограничение имеет вид $L(n, f, g) \geq c2^n/n$ для некоторой константы c, зависящей от последовательности $(f^{(n)}, g^{(n)})$, будем говорить о *слабой* асимптотической оптимальности метода, а при ограничении $L(n, f, g)/n \to \infty$ — о его *сильной* асимптотической оптимальности.

Примером качественного условия может служить $D(f) \supseteq D(g)$, где $D(f) = \{\tilde{x} \mid f(\tilde{x}) \neq *\}$ — область определения функции f. В [2] доказано, что оно обеспечивает сильную асимптотическую оптимальность метода последовательной реализации. Следующая теорема содержит описание всех качественных условий асимптотической оптимальности.

Теорема 1. *Качественные условия сильной и слабой асимптотической оптимальности метода последовательной реализации совпадают и исчерпываются следующими:*

(а) *функция f либо g доопределима до константы,*

(б) *области определения $D(f)$ и $D(g)$ сравнимы по включению,*

(в) *области определения $D(f)$ и $D(g)$ не пересекаются.*

Существенную роль при доказательстве теоремы играют найденные в работе качественные условия совместимости пар (f, g). Введем соответствующие понятия. Будем рассматривать нетривиальный случай $D(f) \neq \emptyset$.

Для $\alpha \in \{0, 1, *\}$, $\mu \in \{0, 1\}$ запись $\alpha \succeq \mu$ будет означать, что μ является доопределением α. Для пары (f, g) и набора неотрцательных чисел $Q^{(2)} = (q_{\mu\nu},\ \mu, \nu \in \{0, 1\})$, $\sum_{\mu\nu} q_{\mu\nu} = 1$, определим функцию

$$h_{f,g}(Q^{(2)}) = - \sum_{\alpha,\beta\in\{0,1,*\}} l_{\alpha\beta}(f, g) \log \sum_{\mu\preceq\alpha,\nu\preceq\beta} q_{\mu\nu}.$$

Будем говорить, что *набор $Q^{(2)}$ совместим с $Q^{(1)} = (q_0, q_1)$*, если $q_{00} + q_{01} = q_0$, $q_{10} + q_{11} = q_1$. Скажем, что *пара функций (f, g) совместима*, если существует точка минимума $Q(f, g)$ функции $h_{f,g}(Q^{(2)})$, совместимая с $Q(f) = \left(\dfrac{l_0(f)}{l_0(f) + l_1(f)}, \dfrac{l_1(f)}{l_0(f) + l_1(f)}\right)$.

Всякое качественное условие на пары (f, g) может быть задано множеством $W \subseteq \{0, 1, *\}^2$: пара (f, g) *удовлетворяет условию W*, если $\{(\alpha, \beta) \mid l_{\alpha\beta}(f, g) > 0\} = W$. Считаем, что условие W *обеспечивает совместимость* пар, если всякая пара (f, g), удовлетворяющая этому условию, совместима.

Лемма. *Если условие W обеспечивает совместимость пар, то условие W', $W' \subseteq W$, также обеспечивает совместимость.*

В связи с этим достаточно указать лишь максимальные (по включению) условия W.

Теорема 2. *Имеется 8 максимальных качественных условий совместимости пар. Они описываются множествами*

(a) $W^a = \{0, 1, *\}^2 \setminus \{(*, 0), (*, 1)\}$,

(b) $W^b_\alpha = \{(0, \alpha), (1, \alpha), (*, 0), (*, 1), (*, *)\}$, $\alpha \in \{0, 1, *\}$,

(c) $W^c_\mu = \{(\mu, \alpha), (*, \alpha), \alpha \in \{0, 1, *\}\}$, $\mu \in \{0, 1\}$,

(d) $W^d_\mu = \{(\alpha, \mu), (\alpha, *), \alpha \in \{0, 1, *\}\}$, $\mu \in \{0, 1\}$.

Этот факт и результаты из [2] приводят к теореме 1.

Работа выполнена при финансовой поддержке ОИТВС РАН (проект 1-1) и РФФИ (проекты 06-01-00577 и 06-07-89293).

Список литературы

1. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. Вып. 14. — М.: Наука, 1965. — С. 31–110.

2. Шоломов Л. А. О сложности последовательной реализации частичных булевых функций схемами // Дискретный анализ и исследование операций. Сер 1. — 2007. — Т. 14, № 1. — С. 110–139.

О РЕАЛИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ ИНФОРМАЦИОННЫМИ ГРАФАМИ

Ю. С. Шуткин (Москва)

Рассматривается задача реализации булевых функций с помощью информационных графов. Такая реализация дает возможность базируясь на свойствах вероятностного пространства запросов строить различные информационные графы и минимизировать тем самым количество действий, затраченных на вычисление функции. В нашей задаче эти действия есть ни что иное, как вычисление предикатов на ребрах графа, а суммарно затраченные усилия — сложность этого графа. Такой функционал сложности соответствует среднему нагреванию чипа, реализующего какую-либо булеву функцию.

Реализация функций с помощью информационных графов может также пригодиться, например, когда мы эмулируем контактную схему и ее функционирование на компьютере. В этом случае функционал сложности для простейших информационных графов как раз отвечает затратам на вычисление предикатов на контактах схемы.

Получены основные оценки сложности реализации, такие как оценка функции Шеннона сложности реализации функции в классе информационных графов и информационных деревьев. Также для почти всех булевых функций получен порядок сложности реализации их информационными графами, а для деревьев установлена асимптотика сложности. Результаты данной работы анонсированы в [1].

Дадим некоторые необходимые определения. Сложность информационного графа [2] (в данной статье мы рассматриваем информационные графы без ориентированных циклов, с базовым множеством предикат $F = \{f_1, \ldots, f_m\}$) на запросе α

$$L(G, \alpha) = \sum_{v \in \theta_{v_0}(\alpha)} \psi(v),$$

где $\psi(v)$ — количество ребер, выходящих из v, а $\theta_{v_0}(\alpha)$ — множество вершин, достижимых из начальной на запросе α.

Сложность информационного графа

$$L(G) = \sum_{\alpha \in \{0,1\}^n} L(G, \alpha) P(\alpha) = E_\alpha \big(L(G, \alpha) \big),$$

где $P(\alpha)$ — вероятность запроса α в вероятностном пространстве.

Сложность функции

$$L(f, F) = \inf_{G \in U(f,F)} L(G),$$

$U(f, F)$ — множество информационных графов, реализующих функцию f.

Далее в качестве базового множества будем подразумевать $F_0 = \{x_1, \bar{x}_1, \ldots, x_n, \bar{x}_n\}$ и второй аргумент в обозначении сложности опускать $L(f, F_0) \to L(f)$.

Функция Шеннона сложности функций n переменных.

$$L^{Sh}(n) = \max_{f \in P_2^{(n)}} L(f).$$

Аналогичные определения вводятся для древовидных информационных графов. Мы будем обозначать их индексом D внизу.

Итак, ставится задача построения информационного графа с минимальной сложностью.

Получена верхняя оценка сложности реализации функции n переменных в классе информационных графов. А именно, для любой функции f из $P_2^{(n)}$ выполнено

$$L(f) \leq 2n - 1.$$

В классе информационных деревьев эта оценка совпадает с нижней оценкой функции Шеннона, т.е.

$$L_D^{Sh}(n) = 2n - 1.$$

В классе информационных графов получена более слабая нижняя оценка функции Шеннона

$$L^{Sh}(n) \geq \frac{3n - 1}{2}.$$

Найден порядок сложности для почти всех функций $f \in P_2^{(n)}$ их реализации с помощью информационных графов

$$L(f) \asymp n.$$

И асимптотика сложности реализации информационными деревьями для почти всех функций $f \in P_2^{(n)}$

$$L_D(f) \sim 2n.$$

Также рассмотрен случай обобщенного базового множества, когда в качестве F берется некоторое модифицированное множество, а не F_0. Приведены некоторые методы синтеза информационных графов с такими множествами.

Получена верхняя оценка сложности реализации информационными графами и деревьями для почти всех $f \in M_2^{(n)}$

$$L(f, F) \lesssim 2\sqrt{n}$$

при $n \to \infty$, для некоторого базового множества F, не сильно отличающегося от простого F_0.

Автор выражает благодарность Гасанову Э. Э. за постановку задачи и помощь в исследовании.

Список литературы

1. Шуткин Ю. С. Реализация булевых функций с помощью информационных графов // Материалы IX международной конференции "Интеллектуальные системы и компьютерные науки". — Изд-во мех-мат ф-та МГУ, 2006.

2. Гасанов Э. Э., Кудрявцев В. Б. Теория хранения и поиска информации. — М.: Физматлит, 2002.

3. Лупанов О.Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

ВЫЧИСЛЕНИЕ ЛОГАРИФМИЧЕСКОЙ ФУНКЦИИ В ПРЕДЕЛАХ LINSPACE ДЛЯ КОНСТРУКТИВНЫХ ВЕЩЕСТВЕННЫХ ЧИСЕЛ

С. В. Яхонтов (Санкт-Петербург)

Пусть $M(n)$ — количество битовых операций, необходимых для умножения n-битных целых чисел. В [1] показано, что значения элементарных функций с точностью 2^{-n} можно вычислять с временной сложностью $O(M(n)\log(n))$. В [1] также указывается, что для этого достаточно знать $n + O(\log(n))$ битов аргумента, хотя собственно

оценок объема промежуточной памяти, необходимой для вычислений, не приводится.

Вместе с тем, для практических приложений важно уметь вычислять элементарные функции с помощью алгоритмов из некоторого емкостного класса сложности. В [2] предлагается алгоритм класса $FLINSPACE$ (емкостная сложность ограничена функцией $C \cdot n$) для вычисления элементарных функций на основе разложений в ряд Тейлора. В данной работе схема из [2] используется для вычисления в пределах $LINSPACE$ логарифмической функции на всей области определения.

Основные сведения по $LINSPACE$ вычислимым вещественным числам и функциям и классам вычислительной сложности можно найти в [2–4].

Рассмотрим ряд Тейлора логарифмической функции:

$$\ln(1+x) = \sum_{i=1}^{\infty} (-1)^{(i-1)} \frac{x^i}{i}. \tag{1}$$

Этот ряд сходится для значений x в промежутке $(-1, 1]$. С помощью редукции интервала вычисление логарифма для аргумента $u = 1+x$ можно свести к вычислению логарифма для аргумента $\frac{u}{2^k}$:

$$\ln(u) = \ln\left(\frac{u}{2^k} 2^k\right) = \ln\left(\frac{u}{2^k}\right) + k \cdot \ln(2) = \ln\left(\frac{u}{2^k}\right) - k \cdot \ln\left(\frac{1}{2}\right)$$

(здесь k может быть отрицательным). Приближенные значения аргументов конструктивных вещественных функций берутся из множества двоично-рациональных чисел [4]. Так как двоично-рациональные числа имеют конечное двоичное представление, то для редукции интервала можно, например, сдвигать битовое представление аргумента u так, чтобы старший значащий бит оказался сразу после двоичной точки. В этом случае $u' = \frac{u}{2^k}$ будет принадлежать интервалу $\left[\frac{1}{2}, 1\right)$, а $x' = u' - 1$ будет находиться в интервале $\left[-\frac{1}{2}, 0\right)$. Остаточный член ряда (1) для $x' < 0$ в форме Коши [5] имеет вид:

$$|r_n(x')| \le \frac{|x'|^{n+1}}{1-|x'|} \cdot \left(\frac{1-\theta}{1+\theta x'}\right)^n, \quad (0 < \theta < 1).$$

При $x' > -1$ будет $1 + \theta x' > 1 - \theta$, и последний множитель меньше единицы. Поэтому для $|x'| \le \frac{1}{2}$ остаточный член будет удовлетво-

рять неравенству:

$$|r_n(x')| < \frac{1}{1-|x'|} \cdot \frac{1}{2^{n+1}} \leq \frac{2}{1} \cdot \frac{1}{2^{n+1}} = 2^{-n}.$$

Далее, коэффициенты ряда (1) ограничены по модулю единицей и $LINSPACE$ вычислимы. Воспользуемся теоремой 1 из [2] для вычисления в пределах $LINSPACE$ ряда (1) на интервале $\left[-\frac{1}{2}, 0\right)$, в частности для вычисления $\ln(2^{-1}) = \ln(1 - 2^{-1})$. Это дает возможность сделать вывод об емкостной вычислительной сложности логарифмической функции.

Теорема. *Логарифмическая функция является $LINSPACE$ конструктивной на всей области определения.*

Список литературы

1. Brent R. P. Fast multiple-precision evaluation of elementary functions // Journal of the ACM. — 1976. — V. 23, № 2. — P. 242–251.

2. Яхонтов С. В. Вычисление степенных рядов в пределах LINSPACE // Материалы VIII Международного семинара "Дискретная математика и ее приложения" (Москва, 2–6 февраля 2004 г.). — М.:Изд-во механико-математического факультета МГУ, 2004.

3. Du D., Ko K. Theory of computational complexity. — John Wiley & Sons, 2000.

4. Ko K. Complexity theory of real functions. — Birkhauser, 1991.

5. Фихтенгольц Г. М. Курс дифференциального и интегрального исчисления. Т. 2. — М.: Физматлит, 2003.

Секция «Функциональные системы»

О ПОЛНОТЕ S-МНОЖЕСТВ ДЕТЕРМИНИРОВАННЫХ ФУНКЦИЙ

В. А. Буевич, М. А. Подколзина (Москва)

Пусть $k \geq 2$, $\tau \geq 1$, $E_k = \{0, 1, \ldots, k-1\}$, E_k^τ — множество всех слов длины τ, составленных из элементов E_k. Через P_k^τ обозначим множество детерминированных функций (д.функций), зависящих от переменных, принимающих значения из множества E_k^τ. Заметим, что любая д.функция для заданного $\tau \geq 1$ может быть вычислена некоторым конечным автоматом за первые τ тактов его работы. На множестве P_k^τ обычным образом вводится операция суперпозиции.

Определение. Пусть $k \geq 2$, $\tau \geq 1$, $\mathfrak{M} \subseteq P_k^\tau$. Множество $\mathfrak{M}$ называется полным в P_k^τ, если $[\mathfrak{M}] = P_k^\tau$.

Известно [1–3], что критерий полноты в P_k^τ может быть сформулирован в терминах предполных в P_k^τ классов. В [3] с использованием аппарата сохранения отношений для любого $k \geq 2$ описаны все предполные классы в P_k^τ при $\tau = 1$, т. е. в P_k, а в [1] с ипользованием того же аппарата описаны все предполные в P_k^τ классы для любых $k \geq 2$, $\tau \geq 1$.

Определение. Пусть $k \geq 2$, $\tau \geq 1$. Пусть $f(x_1, \ldots, x_n) \in P_k^\tau$. Д.функцию $f(x_1, \ldots, x_n)$ назовем S-функцией, если в любом состоянии вычисляющего ее автомата реализуется функция k-значной логики, не выпускающая ни одного значения из множества E_k.

Пусть $\mathfrak{M} \subseteq P_k^\tau$. Множество $\mathfrak{M}$ назовем S-множеством, если любая д.функция из $\mathfrak{M}$ является S-функцией.

Определение. Пусть $k \geq 2$, $\tau \geq 1$. S-множество $\mathfrak{N} \subset P_k^\tau$ называется S-предполным классом в P_k^τ, если $\mathfrak{N}$ не является полным в P_k^τ, но для любой S-функции $f \notin \mathfrak{N}$ замыкание множества $\mathfrak{N} \cup \{f\}$ совпадает с P_k^τ [2].

Определение. Пусть $k \geq 2$, $\tau \geq 1$. Пусть $t \in \{1, \ldots, \tau\}$, $h \geq 1$, $E_k^t(h) = \underbrace{E_k^t \times \ldots \times E_k^t}_{h}$. Произвольное непустое подмножество $R \subseteq E_k^t(h)$ называется отношением, заданным на E_k^t, а число h — арностью этого отношения.

Определение. Пусть $k \geq 2$, $\tau \geq 1$, $t \in \{1, \ldots, \tau\}$, $h \geq 1$. Д.функция $f(x_1, \ldots, x_n)$ из P_k^τ сохраняет отношение $R \subset E_k^t(h)$, если для любой совокупности $(a_1^1, \ldots, a_h^1), \ldots, (a_1^n, \ldots, a_h^n)$ элементов из R набор $(f(a_1^1, \ldots, a_1^n), \ldots, f(a_h^1, \ldots, a_h^n))$ также принадлежит R. Множество $\mathfrak{M} \subseteq P_k^\tau$ сохраняет отношение R, если каждая д.функция из $\mathfrak{M}$ сохраняет это отношение.

Множество всех д.функций, сохраняющих некоторое отношение R, обозначим через $U(R)$. Рассмотрим шесть семейств отношений — семейства $Z(k,\tau)$, $D(k,\tau)$, $N(k,\tau)$, $I(k,\tau)$, $L(k,\tau)$ и $V(k,\tau)$.

Семейство $Z(k,\tau)$**.** ($Z(k,\tau) \neq \emptyset$ для любых $k \geq 2, \tau \geq 1$. Унарное отношение R принадлежит семейству $Z(k,\tau)$ тогда и только тогда, когда для некоторого t, $(t \leq \tau)$ $R \subset E_k^t$, причем при $\tau \geq 2, t \geq 2$ имеет место следующее: для любого $a \in E_k^{t-1}, a = (a(1), \ldots, a(t-1))$ существуют $a(t) \in E_k, a'(t) \in E_k$ такие, что $a(t) \neq a'(t), (a(1), \ldots, a(t-1), a(t))$ принадлежит, а $(a(1), \ldots, a(t-1), a'(t))$ не принадлежит R.

Семейство $D(k,\tau)$**.** $D(k,\tau) \neq \emptyset$ для любых $k \geq 3, \tau \geq 1$. Бинарное отношение R принадлежит семейству $D(k,\tau)$ тогда и только тогда, когда для некоторого t $(1 \leq t \leq \tau)$ $R \subset E_k^t(2)$; R является определенным на E_k^t отношением эквивалентности, причем имеет место следующее. Существует принадлежащий R набор (a_1, a_2) такой, что $a_1(1) = a_2(1), \ldots, a_1(t-1) = a_2(t-1)$. Кроме того, для любого $a \in E_k^t$ существует $a' \in E_k^t$ такое, что $a(t) \neq a'(t)$, набор (a, a') не принадлежит R и при $\tau \geq 2, t \geq 2$ $a(1) = a'(1), \ldots, a(t-1) = a'(t-1)$.

Семейство $N(k,\tau)$**.** $N(k,\tau) \neq \emptyset$ для любых $k \geq 2, \tau \geq 1$. Бинарное отношение R принадлежит семейству $N(k,\tau)$ тогда и только тогда, когда для некоторого $1 \leq t \leq \tau$ $R \subset E_k^t(2)$, существует определенная на E_k^t подстановка σ_R, разлагающаяся в произведение циклов одинаковой простой длины $p \geq 2$, график которой совпадает с R, причем, если $\tau \geq 2$, $t \geq 2$ и набор (a_1, a_2) принадлежит R, то $a_1(1) = a_2(1), \ldots, a_1(t-1) = a_2(t-1)$.

Пусть $k \geq 2$, $\tau \geq 1$. Пусть Σ — множество всех подстановок (перестановок), определенных на E_k. Пусть $t \in \{1, \ldots, \tau\}$ и Φ_t — совокупность отображений множества E_k^t в Σ такая, что при $t = 1$ для любых $\varphi \in \Phi_t$, $a \in E_k$, $a' \in E_k$ $\varphi(a) = \varphi(a')$, а при $\tau \geq 2$, $t \geq 2$ для любых $\varphi \in \Phi_t, a \in E_k^t, a' \in E_k^t$ если $a(1) = a'(1), \ldots, a(t-1) = a'(t-1)$, то $\varphi(a) = \varphi(a')$. Подстановку, которую отображение $\varphi \in \Phi_t$ ставит в соответствие элементу $a \in E_k^t$, обозначим через $\sigma_{\varphi(a)}$.

Семейство $I(k,\tau)$**.** $I(k,\tau) \neq \emptyset$ для любых $k \geq 5, \tau \geq 1$. Пусть

$h \geq 5, m \geq 1, k = h^m$. Бинарное отношение R принадлежит подсемейству $I_h(k,\tau)$ семейства отношений $I(k,\tau)$, если для некоторых $1 \leq t \leq \tau$, $\varphi \in \Phi_t$ имеет место следующее: $R \subset E_k^t(2)$, набор (a_1, a_2) принадлежит R тогда и только тогда, когда для любого i $(1 \leq i \leq m)$ i-е компоненты чисел $\sigma_{\varphi(a_1)}(a_1(t)), \sigma_{\varphi(a_1)}(a_2(t))$ при разложении их по степеням числа h различны, причем при $\tau \geq 2$, $t \geq 2$, $a_1(1) = a_2(1), \ldots, a_1(t-1) = a_2(t-1)$. Семейство отношений $I(k,\tau)$ есть объединение семейств $I_h(k,\tau)$, взятое по всем $h \geq 5$, таким, что $h^m = k, m \geq 1$.

Пусть $k = p^m$, где p — простое число, $p \geq 2, m \geq 1$. Пусть $G = \langle E_k, \oplus \rangle$ — произвольная элементарная абелева p-группа.

Семейство $L(k,\tau)$**.** $D(k,\tau) \neq \emptyset$ для любого $\tau \geq 1$, если $k = p^m$, где p — простое число, $p \geq 2, m \geq 1$. Отношение R, арность которого равна четырем, принадлежит семейству $L(k,\tau)$, если для некоторых t $(1 \leq t \leq \tau)$, $\varphi \in \Phi_t$ имеет место следующее: $R \subset E_k^t(4)$, набор (a_1, a_2, a_3, a_4) принадлежит R тогда и только тогда, когда $\sigma_{\varphi(a_1)}(a_1(t)) \oplus \sigma_{\varphi(a_1)}(a_2(t)) = \sigma_{\varphi(a_1)}(a_3(t)) \oplus \sigma_{\varphi(a_1)}(a_4(t))$, причем при $\tau \geq 2$, $t \geq 2$, $a_1(1) = a_2(1) = a_3(1) = a_4(1), \ldots, a_1(t-1) = a_2(t-1) = a_3(t-1) = a_4(t-1)$.

Семейство $V(k,\tau)$**.** $V(k,\tau) \neq \emptyset$ для любых $k \geq 2, \tau \geq 2$. Бинарное отношение R принадлежит семейству $V(k,\tau)$, если для некоторых $t \leq \tau$, $\varphi \in \Phi_t$ имеет место следующее: $R \subset E_k^t(2)$, набор (a_1, a_2) принадлежит R тогда и только тогда, когда либо $a_1(t-1) = a_2(t-1), a_1(t) = a_2(t)$, либо $a_1(t-1) \neq a_2(t-1)$ и существует $\alpha \in E_k$ такое, что $a_1(t) = \sigma_{\varphi(a_1)}(\alpha), a_2(t) = \sigma_{\varphi(a_2)}(\alpha)$, причем при $\tau \geq 3$, $t \geq 3$, $a_1(1) = a_2(1), \ldots, a_1(t-2) = a_2(t-2)$.

Пусть $k \geq 2$, $\tau \geq 1$; $W(k,\tau)$ — объединение семейств $Z(k,\tau)$, $D(k,\tau)$, $N(k,\tau)$, $I(k,\tau)$, $L(k,\tau)$ и $V(k,\tau)$.

Имеет место следующее

Утверждение. *Пусть $k \geq 2, \tau \geq 1$. Пусть $\mathfrak{N}$ — произвольный S-предполный класс в P_k^τ. Существует $R \in W(k,\tau)$ такое, что $\mathfrak{N} = S(U(R))$. Вместе с тем, для любого $R' \in W(k,\tau)$ множество $S(U(R'))$ — S-предполный класс в P_k^τ.*

Список литературы:

1. Буевич В. А. О τ-полноте в классе детерминированных функций // Докл. РАН. — 1992. — Т. 326, № 3. — С. 399–403.

2. Кудрявцев В. Б. О свойствах S-систем функций k-значной логики // Elektronische Informationsverarbeitung und Kybernetik. — 1973. — 9, 1/2. — С. 8–105.

3. Rosenberg Y. La structure des fonctions de plusieure variables sur un ensemble fini-Compes Rendus // Acad. Sci. Paris. — 1965. — P. 3817–3819.

СИНТАКСИЧЕСКАЯ КЛАССИФИКАЦИЯ ФУНКЦИЙ, ВЫЧИСЛИМЫХ ЗА ЛИНЕЙНОЕ ВРЕМЯ

М. А. Герасимов (Санкт-Петербург)

В рассматриваемой работе применяется подход, впервые описанный в работе А. Гжегорчика [1]. В соответствии с этим подходом применяется синтаксическое описание классов функций, вычислимых на сублинейной зоне машины Тьюринга [2]. Применяя определенные ограничения на структуру порождаемых термов, можно добиться расслоения исходного класса на множества функций, вычислимых за линейное время. Рассматриваемый подход позволяет создавать профайлеры для оценки временной сложности программ, записанных на структурированных языках программирования.

Для определения исходных классов функций применяется подход, описанный в уже упомянутой работе А. Гжегорчика [1] и заключающийся в определении множества всех вычислимых функций на основе базового множества (сигнатуры) и конечного множества порождающих операций. В исходной работе рассматривались базисы вида:

$$\{\mathrm{I}_n^m,\ 0,\ \dot{-},\ f_i\}_{i=0}^{\infty},$$
$$B_i = \{\mathrm{I}_n^m,\ 0,\ f_i\},$$

где

$$f_0(x,y) = y+1,$$
$$f_1(x,y) = x+y,$$
$$f_2(x,y) = (x+1)(y+1).$$

Для $n \geq 2$

$$f_{n+1}(0,y) = f_n(y+1, y+1),$$
$$f_{n+1} = (x+1,y) = f_{n+1}(x, f_{n+1}(x,y)).$$

Основные операции, порождающие классы функций включали операцию подстановки и ограниченной рекурсии

$$f(u,0) = g(u),$$
$$f(x,u+1) = h(u,x,f(u,x)),$$
$$f(u,x) \leq j(u,x),$$
$$f = R(g,h,j).$$

Если ограничивающая функция j берется из того же класса, то получаем стандартную классификацию А. Гжегорчика [1]

$$\varepsilon^0 \subseteq \varepsilon^1 \subseteq \varepsilon^3 \subset \mathrm{K}.$$

Однако, возможно выбрать ограничивающую функцию j из другого класса или подкласса данного класса функций, т.е. независимо от исходного базиса. В этом случае получаем операцию F, отличную от исходной ограниченной рекурсии.

Нетрудно заметить, что при $F = R \circ \mathrm{I}_n^m$ результирующая функция может быть получена с помощью ограниченной рекурсии и подстановки [3], что не выводит за пределы исходного класса функций, т. е. F совпадает с операцией ограниченной рекурсии.

Наиболее интересный случай $F = R \circ M$, где $M(\bar{x}) = [\log Max(\bar{x})]$ для произвольного исходного класса. В дальнейшем такая рекурсия будет называться M-ограниченной. Если дополнительно взять в качестве базиса

$$B_0 = \{\mathrm{I}_n^m,\ 0,\ x+1\},$$

то получаем все функции, вычислимые за полиномиальное время на линейной зоне:

$$P_{Lin} \leq P_{time},$$
$$P_{Lin} \leq L_{space}.$$

Добавляя понятие рекурсивной глубины терма и ограничиваясь только теми, которые имеют глубину «1», получаем P_{time^2} (множество алгоритмов, вычислимых за квадратичное время на линейной зоне одноленточной, одноголовочной МТ [4]).

В частности, этот класс содержит универсальную функцию для всех предикатов, вычислимых конечными автоматами [2] или неветвящимися программами [2]. На самом деле этот класс функций совпадает с классом, вычислимым RAM в смысле [3] со сложением за линейное время. Но поскольку сведение RAM к МТ квадратично, этот подход не позволяет получить описания множества алгоритмов, вычислимых за линейное время.

Рассмотрим следующий базис функций:

$$B = \{\mathrm{I}_n^m,\ 0,\ *2,\ /2,\ \psi,\ \delta\},$$

где

$$\delta(x) = \begin{cases} 0, & \text{если младший бит равен 0,} \\ 1, & \text{если младший бит равен 1,} \end{cases}$$

$\psi(x)$ — число, получаемое инверсией младшего бита в «X», $*2$ — унарная операция умножения на два, $/2$ — унарная операция деления на два нацело.

В этом случае замыкание этого класса с помощью операций подстановки и M-ограниченной рекурсии $F \circ M$ дает все функции, вычислимые за линейное время на одноленточной, одноголовочной машине Тьюринга [2].

Следствие. *Для любой рекурсивной функции, вычислимой за линейное время на одноленточной, одноголовочной машине Тьюринга за линейное время, линейный коэффициент может быть получен не более чем за* $4n + C_0$ *шагов машины Тьюринга.*

Список литературы

1. Гжегорчик А. Некоторые классы рекурсивных функций // Проблемы математической логики. Сложность алгоритмов и классы вычислимых функций: сб. пер. — И., 1970.

2. Минский М. Вычисления и автоматы. — М., 1971.

3. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. — М., 1979.

4. Бельтюков А. П. Малые классы, обоснованные на ограниченной рекурсии // Вычислительная техника и вопросы кибернетики. — Л., 1979.

О РАСПОЗНАВАНИИ НЕДЕТЕРМИНИРОВАННОГО АВТОМАТА В ЗАДАННОМ КЛАССЕ

М. Л. Громов, Н. В. Шабалдина (Томск)

Задача распознавания автомата в заданном классе, в случае, если под автоматом подразумевается детерминированный автомат, хорошо известна [1]. Также известно, что исключительным классом для детерминированных автоматов является такой класс автоматов, в котором любая пара автоматов различима (т. е. класс попарно неэквивалентных автоматов). В данной работе рассматривается задача распознавания недетерминированного автомата в заданном классе недетерминированных автоматов. Кроме того, определяется исключительный класс для недетерминированных автоматов в зависимости от типа эксперимента.

Недетерминированным (*нд-*) *автоматом* A называется пятерка (S,I,O,h,s_1), где S — множество состояний с выделенным начальным состоянием s_1, I и O — соответственно входной и выходной алфавиты, $h \subseteq S \times I \times S \times O$ — отношение переходов-выходов. Элементами

множества h являются четверки вида (s,i,s',o), называемые *переходами*; при этом говорят, что автомат может перейти из состояния $s\in S$ под действием входного символа $i\in I$ в состояние $s'\in S$ с выдачей выходного символа $o\in O$, если четверка (s,i,s',o) содержится в h. Если для любых $(s,i,o)\in S\times I\times O$ в нд-автомате существует не более одного перехода из состояния s под действием входного символа i с выходным символом o, то говорят, что нд-автомат является *наблюдаемым*. Если для каждой пары $(s,i)\in S\times I$ существует хотя бы одна пара $(s',o)\in S\times O$, такая что $(s,i,s',o)\in h$, то нд-автомат называется *полностью определенным*. В данной работе рассматриваются только полностью определенные автоматы. Обычным образом отношение переходов-выходов h нд-автомата A распространяется на множество вход-выходных последовательностей. Пара α/β называется *входо-выходной последовательностью* автомата в состоянии s, если существует состояние s' такое, что четверка $(s,\alpha,s',\beta)\in h$. Обозначим $out(s,\alpha)=\{\beta\colon \exists\ s'\in S\ [(s,\alpha,s',\beta)\in h]\}$, т.е. $out(s,\alpha)$ есть множество выходных реакций автомата в состоянии s на входную последовательность α.

Пусть $A=(S,I,O,h,s_1)$, $B=(T,I,O,g,t_1)$, $s\in S$, $t\in T$, — полностью определенные автоматы. Состояние s автомата A и состояние t автомата B *различимы*, если $\exists\alpha\in I^*[out(s,\alpha)\neq out(t,\alpha)]$. Если $\forall\in I^*$ $[out(s,\alpha)=out(t,\alpha)]$, то состояние s автомата A и состояние t автомата B называются *эквивалентными*. Автоматы A и B *различимы*, если различимы их начальные состояния s_1 и t_1. В противном случае автоматы A и B *эквивалентны*. Состояние s наблюдаемого автомата A и состояние t наблюдаемого автомата B 1-*r-различимы*, если $\exists i\in I[out(s,i)\cap out(t,i)=\emptyset]$. Состояние s автомата A и состояние t автомата B k-*r-различимы*, если они являются $(k$-1$)$-r-различимыми, или существует $i\in I$, такой, что для любых $s'\in S$, $t'\in T$ и $o\in O$, таких, что $(s,i,s',o)\in h$ и $(t,i,t',o)\in g$ состояния s' и t' являются $(k$-1$)$-r-различимыми. Состояние s автомата A и состояние t автомата B r-*различимы*, если они являются k-r-различимыми для некоторого $k>0$. Наблюдаемые автоматы A и B r-*различимы*, если r-различимы их начальные состояния s_1 и t_1. Если автоматы A и B не являются r-различимыми, то они называются r-*совместимыми*. Состояние s автомата A и состояние t автомата B *неразделимы*, если $\forall\alpha\in I^*[out(s,\alpha)\cap out(t,\alpha)\neq\emptyset]$. Если $\exists\alpha\in I^*$ $[out(s,\alpha)\cap out(t,\alpha)=\emptyset]$, то состояния s и t *разделимы по* α, или просто *разделимы*. Автоматы A и B *неразделимы*, если неразделимы их начальные состояния s_1 и t_1. Если начальные состояния автоматов A и B разделимы по α, то автоматы A и B *разделимы по* α, или просто *разделимы*. Для детерминированных автоматов отношения эквивалентности, r-сов-

местимости, неразделимости совпадают.

При экспериментах с детерминированными автоматами различают безусловные и условные эксперименты. Распознать детерминированный автомат в классе можно как при помощи безусловного, так и при помощи условного эксперимента. При этом условный эксперимент может быть короче безусловного. При экспериментах с недетерминированными автоматами отношение, которое можно проверить, существенно зависит от типа эксперимента. При экспериментах с недетерминированными автоматами часто используется так называемое предположение "о всех погодных условиях". В этом случае предполагается, что, если каждая последовательность подается на автомат несколько раз, то недетерминированный автомат в процессе распознавания "покажет" все возможные выходные реакции на эту последовательность. В этом случае можно использовать отношение различимости между недетерминированными автоматами, и исключительным классом будет класс попарно различимых автоматов (как и при распознавании автомата в заданном классе детерминированных автоматов). Известно, что различающая последовательность для пары автоматов полиномиально зависит от произведения числа состояний автоматов. Предположение "о всех погодных условиях" перестает быть реалистичным, если при тестировании нет возможности полностью контролировать распознаваемый автомат. Отношение, которое может быть проверено в этом случае, зависит от того, какой тип эксперимента используется: безусловный или условный. В случае безусловного эксперимента проверяемым отношением будет отношение разделимости. Исключительным классом при использовании безусловного эксперимента является класс попарно разделимых автоматов. В работе [2] показано, что длина кратчайшей разделяющей последовательности для пары автоматов в худшем случае экспоненциально зависит от произведения числа состояний автоматов. В случае условного эксперимента проверяемым отношением будет отношение r-различимости, а исключительный класс автоматов — класс попарно r-различимых автоматов. Хотя известно [3], что число последовательностей в r-различающем множестве для пары автоматов экспоненциально зависит от произведения числа состояний автоматов, однако, для проведения условного эксперимента достаточно одной последовательности. Длина последовательности r-различающего множества полиномиально зависит от произведения числа состояний различаемых автоматов, кроме того, полиномиальным является алгоритм построения этой последовательности для пары автоматов в процессе проведения условного эксперимента по распознаванию автомата в заданном классе.

Список литературы

1. Гилл А. Введение в теорию конечных автоматов. — М:

Наука, 1966.

2. Евтушенко Н. В., Спицына Н. В. О верхней оценке длины разделяющей последовательности // Вестник ТГУ. Приложение. — 2006. — № 18. — С. 54–59.

3. Евтушенко Н. В., Спицына Н. В. О верхней оценке R-различающих и разделяющих последовательностей для наблюдаемых автоматов // Материалы IX Международной конференции "Интеллектуальные системы и компьютерные науки", 1, 1. — М.: ММФ МГУ, 2006. — С. 124–126.

О КЛАССАХ ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ, МОНОТОННЫХ ОТНОСИТЕЛЬНО ЧАСТИЧНО УПОРЯДОЧЕННЫХ МНОЖЕСТВ

О. С. Дудакова (Москва)

Рассматривается задача о конечной порожденности предполных классов монотонных функций k-значной логики. Известно [1], что любой предполный класс в P_k из семейств $\mathcal{Z}$, $\mathcal{L}$, $\mathcal{U}$, $\mathcal{C}$ и $\mathcal{B}$ порождается конечным числом функций (описание семейств предполных классов см. в [2, 3]). Для предполных классов всех функций, монотонных относительно частично упорядоченных множеств с наименьшим и наибольшим элементами (классов из семейства $\mathcal{M}$) этот результат верен, вообще говоря, лишь при $k \leq 7$ [1]. В ряде работ (см., например, [5–7]) приводятся достаточные условия конечной порожденности для классов из семейства $\mathcal{M}$. В то же время, при $k \geq 8$ в P_k существуют предполные классы монотонных функций, не имеющие конечного базиса [4]; полное описание конечно-порожденных классов из семейства $\mathcal{M}$ к настоящему времени отсутствует. В данной работе для некоторого семейства частично упорядоченных множеств получен критерий конечной порожденности соответствующих предполных классов монотонных функций. Все необходимые определения можно найти в работах [9–11].

Пусть $\mathcal{P}$ — некоторое частично упорядоченное множество с отношением порядка $\leq$. Через $\mathcal{M}_\mathcal{P}$ будем обозначать замкнутый класс всех функций, монотонных относительно $\mathcal{P}$; через $w_\mathcal{P}$ будем обозначать ширину множества $\mathcal{P}$. Обозначим через $\mathbb{A}$ семейство всех частично упорядоченных множеств с наименьшим и наибольшим элементами. Следует отметить, что класс $\mathcal{M}_\mathcal{P}$ является предполным тогда и только тогда, когда $\mathcal{P} \in \mathbb{A}$ (см. [2, 3]).

Пусть $\mathcal{P} \in \mathbb{A}$, пусть $a_1, a_2 \in \mathcal{P}$, элементы a_1 и a_2 несравнимы, b_1 и b_2 — две минимальные верхние грани этих элементов, и существует $c = \sup(b_1, b_2)$. В этом случае будем говорить, что c — *точная верхняя грань второго порядка* элементов a_1 и a_2 (обозначение $\sup^2(a_1, a_2)$).

Обозначим через $\mathbb{A}_2$ семейство всех множеств $\mathcal{P} \in \mathbb{A}$, для которых выполняются неравенства $|\mathcal{P}| \geq 2$ и $w_{\mathcal{P}} \leq 2$. Определим семейство $\mathbb{B}_2$ частично упорядоченных множеств следующим образом: $\mathbb{A}_2 \subset \mathbb{B}_2$; далее, если $\mathcal{R}_1, \mathcal{R}_2 \in \mathbb{B}_2$, и если множество $\mathcal{R}$ получено в результате применения операций последовательного или параллельного соединения к множествам $\mathcal{R}_1$ и $\mathcal{R}_2$ (см. [8, 11]), то $\mathcal{R} \in \mathbb{B}_2$. Обозначим через $\mathbb{A}_2^{(1)}$ (соответственно, через $\mathbb{B}_2^{(1)}$) семейство всех множеств $\mathcal{P} \in \mathbb{A}_2$ (соответственно, $\mathcal{P} \in \mathbb{B}_2$), таких, что для любой пары несравнимых элементов x_1, x_2 в $\mathcal{P}$ существует либо $\sup(x_1, x_2)$, либо $\sup^2(x_1, x_2)$. Отметим, что множество, приведенное в работе [4], принадлежит семейству $\mathbb{B}_2 \setminus \mathbb{B}_2^{(1)}$.

Функция $\mu : \mathcal{P}^n \to \mathcal{P}$, где $n \geq 3$, называется *мажоритарной* [7], если для любых $a, b \in \mathcal{P}$ выполняются равенства

$$\mu(a, b, \ldots, b) = \mu(b, a, b, \ldots, b) = \ldots = \mu(b, \ldots, b, a) = b.$$

Лемма. *Пусть $\mathcal{A}, \mathcal{B} \in \mathbb{A}$, а множество $\mathcal{C}$ получено либо в результате последовательного соединения, либо в результате параллельного соединения множеств $\mathcal{A}$ и $\mathcal{B}$. Пусть в классах $\mathcal{M}_{\mathcal{A}}$ и $\mathcal{M}_{\mathcal{B}}$ существуют мажоритарные функции. Тогда в классе $\mathcal{M}_{\mathcal{C}}$ также существует мажоритарная функция.*

Теорема 1 [9, 10]. *Пусть $\mathcal{P} \in \mathbb{A}_2 \setminus \mathbb{A}_2^{(1)}$. Тогда класс $\mathcal{M}_{\mathcal{P}}$ не имеет конечного базиса.*

Этот результат обобщается на множества из семейства $\mathbb{B}_2$:

Следствие. *Пусть $\mathcal{P} \in \mathbb{B}_2 \setminus \mathbb{B}_2^{(1)}$. Тогда класс $\mathcal{M}_{\mathcal{P}}$ не имеет конечного базиса.*

Теорема 2 [10]**.** *Пусть $\mathcal{P} \in \mathbb{A}_2^{(1)}$. Тогда в классе $\mathcal{M}_{\mathcal{P}}$ содержится некоторая мажоритарная функция.*

Из леммы, теорем 1 и 2, а также интерполяционной теоремы из работы [7] извлекается следующий основной результат.

Теорема 3. *Пусть $\mathcal{P} \in \mathbb{B}_2$. Тогда следующие условия эквивалентны:*

(1) *класс $\mathcal{M}_{\mathcal{P}}$ является конечно-порожденным;*

(2) $\mathcal{P} \in \mathbb{B}_2^{(1)}$;

(3) *в классе $\mathcal{M}_\mathcal{P}$ существует некоторая мажоритарная функция.*

Автор выражает благодарность профессору А. Б. Угольникову за постановку задачи и постоянное внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект 05-01-00994), программы поддержки ведущих научных школ РФ (проект НШ-5400.2006.1) и программы фундаментальных исследований Отделения математических наук РАН "Алгебраические и комбинаторные методы математической кибернетики" (проект "Синтез и сложность управляющих систем").

Список литературы

1. Lau D. Bestimmung der Ordnung maximaler Klassen von Funktionen der k-wertigen Logik // Z. math Log. und Grundl. Math. — 1978. — 24. — P. 79–96.

2. Rosenberg I. G. Über die funktionale Vollständigkeit in den mehrwertigen Logiken // Rozpr. ČSAV. MPV. — 1970. — 80. — P. 3–93.

3. Яблонский С. В., Гаврилов Г. П., Набебин А. А. Предполные классы в многозначных логиках — М.: изд-во МЭИ, 1997. 142 с.

4. Tardos G. A not finitely generated maximal clone of monotone operations // Order. — 1986. — 3. — P. 211–218.

5. Demetrovics J., Hannák L., Rónyai L. Near unanimity functions and partial orderings // Proc. 14 ISMVL, Manitoba. — 1984. — P. 52–56.

6. Demetrovics J., Hannák L., Rónyai L. On algebraic properties of monotone clones // Order. — 1986. — 3. — P. 219–225.

7. Baker K., Pixley A. Polynomial interpolation and the Chinese remainder theorem for algebraic systems // Math. Z. — 1975. — 143. — P. 165–174.

8. Яблонский С. В. Введение в дискретную математику — М.: Высшая школа, 2001.

9. Дудакова О. С. Об одном семействе предполных классов функций k-значной логики, не имеющих конечного базиса // Вестн. Моск. ун-та. Серия 1. Математика. Механика. — 2006. — № 2. — С. 29–33.

10. Дудакова О. С. О свойствах предполных классов монотонных функций k-значной логики // Труды VII Международной конференции "Дискретные модели в теории управляющих систем" (Покровское, 4–6 марта 2006 г.). —М.: МАКС Пресс. — 2006. — С. 107–113.

11. Дудакова О. С. О конечной порожденности некоторых семейств предполных классов монотонных функций k-значной логики // Материалы XVI Международной школы-семинара "Синтез

и сложность управляющих систем" (Санкт-Петербург, 26–30 июня 2006 г.). — М.: Изд-во механико-математического ф-та МГУ. — 2006. — С. 35–37.

О СЛОЖНОСТИ ВЫЧИСЛИМЫХ СЕМЕЙСТВ МОНОТОННЫХ ОБЩЕРЕКУРСИВНЫХ ФУНКЦИЙ

Ю. Д. Корольков (Иркутск)

Целью работы является поиск достаточно простых семейств общерекурсивных функций, и в то же время представляющих структуру индексных множеств всех вычислимых семейств общерекурсивных функций. Здесь мы их ищем среди семейств неубывающих конечнозначных функций.

Одним из подходов к классификации семейств общерекурсивных функций (о.р.ф.) является исследование индексных множеств этих семейств относительно клиниевской (главной вычислимой) нумерации κ: $N \to R$ семейства всех одноместных частично-рекурсивных функций (ч.р.ф.). На классе R также рассматривается стандартная топология, базис открытых множеств которой порождается конечными функциями.

Оценка сложности множеств будет даваться в арифметической иерархии Клини — Мостовского. Принадлежность множества к классу $\Sigma_n(\Pi_n)$ этой иерархии означает возможность выделения его формулой с n переменами кванторов и рекурсивным предикатом в качестве бескванторной части формулы, причем первый квантор есть $\exists(\forall)$. Класс Δ_n определяется как $\Sigma_n \cap \Pi_n$. Отношение частичного порядка задается m-сводимостью множеств.

Ю. Л. Ершов [1, 2] рассматривает исследования индексных множеств вычислимых семейств как важные в теории нумераций.

Вычислимое семейство A называется дискретным, если существует такая вычислимая последовательность конечных множеств $T_0, T_1, ...$, что:

а) для всякого $X \in A$ найдется $T_i \subseteq X$;

б) $T_i \subseteq T_j \Rightarrow T_i = T_j$;

в) если $T_i \subseteq X_j \in A$ и $T_i \subseteq X_k \in A$, то $X_j = X_k$.

Теорема 1. *Для каждого вычислимого семейства общерекурсивных функций существует вычислимое дискретное семейство неубывающих конечнозначных общерекурсивных функций такое, что их индексные множества изоморфны.*

Эта теорема служит основой для поиска дальнейших упрощений. Введем новые семейства. Обозначим через C множество всех функций-констант c_i, где $c_i(x) = i$ при всех $x \in N$. Через S обозначим множество следующих функций $s_{ij}(x) = s(i,j)(x)$ при всех $i,j \in N$. Значение $s(i,j)(x)$ при $x \in [0,...,i]$ равно j, а при остальных x равно $j+1$. Такие функции можно назвать полуконстантами.

Обозначим через $B(A)$ множество всех внешних предельных общерекурсивных точек семейства A.

Пусть $K \subseteq N$. Назовем семейство M общерекурсивных функций K-семейством, если выполнены условия:

а) $M \subseteq C \cup S$;

б) $M \cap C = C(K) = \{c_i | i \in K\}$;

в) $B(M) = C(N \backslash K)$.

Другими словами, семейство M состоит из констант $C(K)$ и еще достаточного количества функций из S, чтобы остальные константы оказались внешними предельными точками для M. Для каждого нетривиального K таких семейств бесконечно много. Обозначим $F(K) = C(K) \cup S$ — полное (наибольшее) K-семейство. Заметим, что при всех K семейства $F(K)$ недискретны.

Теорема 2. *Для каждого $K \subseteq N$ следующие условия эквивалентны*:

а) $K \in \Sigma_2$;

б) имеются вычислимые K-семейства;

в) имеются дискретные вычислимые K-семейства;

г) $F(K)$ вычислимо.

Далее будем считать порождающие множества K принадлежащими классу Σ_2.

Теорема 3. *Для каждого фиксированного $K \subseteq N$ все вычислимые K-семейства имеют изоморфные индексные множества.*

Ввиду последнего результата можно ввести обозначение $I(K)$ для индексного множества одного из вычислимых K-семейств, например, $F(K)$. Введенные K-семейства удобны тем, что свойства их индексных множеств $I(K)$ часто выражаются через свойства "обычных" множеств K.

Теорема 4. *Если $K \leq L$, то $I(K) \leq I(L)$.*

Как будет видно из теоремы 6, простое обращение этой теоремы неверно.

В [3] замечено, что класс всех индексных множеств вычислимых семейств о.р.ф. имеет наименьший по сводимости элемент, полный в классе Π_2, и наибольший элемент, расположенный в классе

$\Delta_3 \setminus (\Sigma_2 \cup \Pi_2)$. Там же предложены некоторые критерии принадлежности индексного множества классу Π_2.

Теорема 5. *Существуют такие $K, L \in \Sigma_2$, что $I(K)$ является наименьшим элементом, а $I(L)$ — наибольшим элементом в классе индексных множеств всех вычислимых семейств общерекурсивных функций.*

В завершение дадим простой критерий минимальности $I(K)$.

Теорема 6. *Для $K \in \Sigma_2$ имеем $I(K) \in \Pi_2$ ($I(K)$ является наименьшим элементом) тогда и только тогда, когда $K \in \Pi_2$.*

Из теоремы 6 и результатов [3] следует, что все K-семейства при $K \in \Sigma_2 \cap \Pi_2$ имеют изоморфные индексные множества. В то же время, среди таких K встречаются, например, несравнимые. Тем самым получаем контрпримеры для обращения теоремы 4. Остается надежда найти ослабленный вариант обращения теоремы 4, что позволит построить промежуточные индексные множества.

Работа выполнена при финансовой поддержке Института динамики систем и теории управления СО РАН.

Список литературы

1. Ершов Ю. Л. Теория нумераций. — М.: Наука, 1977.

2. Ershov Yu. L. Theory of numberings. — Preprint № 18. — Novosibirsk, 1996.

3. Корольков Ю. Д. Оценка сложности индексных множеств семейств общерекурсивных функций в арифметической иерархии // Алгебра и логика. — 2002. — Т. 41, № 2. — С. 155–165.

О НЕКОТОРЫХ СВОЙСТВАХ СИММЕТРИЧЕСКИХ ФУНКЦИЙ ТРЁХЗНАЧНОЙ ЛОГИКИ

А. В. Михайлович (Москва)

В работе изучаются свойства функций трёхзначной логики. Рассматривается задача о существовании базисов замкнутых классов из некоторых семейств в P_3.

Э. Пост [1, 2] описал структуру всех замкнутых (относительно операции суперпозиции) классов булевых функций. При этом он показал, что все эти классы имеют конечный базис. В k-значных логиках ($k \geq 3$) сохраняются многие результаты, имеющие место в двухзначной логике (см. [3]). Вместе с тем, имеются существенные различия между булевыми функциями и функциями многозначной логики. К ним относятся примеры Янова и Мучника [4] в P_k при

$k \geq 3$ о существовании замкнутых классов со счётным базисом и без базиса (P_k — множество фукнций k-значной логики). Следует отметить, что функции из этих примеров являются симметрическими, принимают значения из множества $\{0,1\}$, причём ненулевые значения могут приниматься на наборах, состоящих только из единиц и двоек. В данной работе изучаются классы из P_3, порождённые функциями, которые обладают вышеперечисленными свойствами. Все необходимые определения можно найти в [3].

Пусть $E_k = \{0,1,\ldots,k-1\}$, $k \geq 2$. Через E_k^n обозначим множество наборов $\{(\alpha_1,\alpha_2,\ldots,\alpha_n)\}$, где $\alpha_1,\alpha_2,\ldots,\alpha_n \in E_k$. Положим $D_n = \{1,2\}^n \backslash \{\{1\}^n \cup \{2\}^n\} \subset E_3^n$, $n > 1$. В работе рассматриваются функции $f(x_1,\ldots,x_n)$, которые равны единице на некоторых наборах из множества D_n, а на всех остальных наборах равны нулю. *Слоем* будем называть множество всех наборов из E_3^n, которые получаются друг из друга перестановкой компонент. Будем обозначать слой из D_n, содержащий e единиц и d двоек, через $\mathcal{L} < e,d >$, $1 \leq e,d < n$, $e+d=n$. *Типом слоя* $\mathcal{L} < e,d >$ ($e \geq 1$, $d \geq 1$) будем называть рациональное число $\frac{e}{d}$. Функцию $f(x_1,\ldots,x_n)$ из P_3 будем называть *однослойной симметрической функцией*, если для некоторых чисел e,d, $1 \leq e,d < n$, $e+d=n$, функция $f(x_1,\ldots,x_n)$ равна единице на слое $\mathcal{L} < e,d >$, а на остальных наборах из E_3^n равна нулю. Множество всех таких функций будем обозначать через Sym_1. *Типом однослойной симметрической функции* будем называть тип слоя, на котором эта функция равна единице.

Определим отношение частичного порядка $\succeq$ на множестве Sym_1 следующим образом: $f_1 \succeq f_2$, тогда и только тогда, когда f_1 и f_2 — функции одного типа и число переменных функции f_1 кратно числу переменных функции f_2 ($f_1, f_2 \in Sym_1$). Отметим следующее свойство функций, сравнимых относительно введённого отношения порядка. Пусть $f \succeq g$, а $\mathcal{L} < e^1,d^1 >$ и $\mathcal{L} < e^2,d^2 >$ — слои, на которых функции f и g соответственно принимают значение 1. Тогда для некоторого $m \in \mathbb{N}$ выполняются равенства $e^1 = me^2$, $d^1 = md^2$. Множество $H \subset Sym_1$ будем называть *цепью*, если любые два элемента множества H сравнимы относительно порядка $\succeq$. Цепь H будем называть *максимальной цепью множества* G, если для любой цепи $H_1 \subset Sym_1$ такой, что $H \subset H_1$, $H \neq H_1$, H_1 не является подможноеством множества G.

Пусть $f,g \in P_3$. Функции $f(x_1,\ldots,x_n)$ и $g(y_1,\ldots,y_n)$ называются *конгруэнтными*, если одна из них получается из другой переименованием переменных без отождествления.

Теорема. *Пусть* $G \subseteq Sym_1$, $F = [G]$. *Тогда справедливы сле-*

дующие утверждения. 1. *Класс F имеет конечный базис тогда и только тогда, когда множество G содержит конечное число неконгруэнтных функций.*

2. *Класс F имеет счётный базис тогда и только тогда, когда множество G содержит бесконечное число неконгруэнтных функций и каждая функция $g \in G$ содержится в некоторой конечной максимальной цепи множества G.*

3. *Класс F не имеет базиса тогда и только тогда, когда множество G содержит бесконечное число неконгруэнтных функций и существует функция $g \in G$, которая не содержится ни в какой конечной максимальной цепи множества G.*

Данные результаты можно обобщить на функции, равные единице на фиксированном числе слоёв.

Работа выполнена при финансовой поддержке РФФИ (проект 05-01-00994), программы поддержки ведущих научных школ РФ (проект НШ-5400.2006.1) и программы фундаментальных исследований Отделения математических наук РАН "Алгебраические и комбинаторные методы математической кибернетики" (проект "Синтез и сложность управляющих систем").

Список литературы

1. Post E. L. Introduction to a general theory of elementary propositions // Amer. J. Math. — 1921. — V. 43, № 3. — P. 163–185.

2. Post E. L. The two-valued iterative system of mathematical logic // Annals of Math. Studies. — V. 5 — Princeton Univ. Press, 1941.

3. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2001.

4. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // ДАН СССР. — 1959. — Т. 127, № 1. — С. 44–46.

ПОЛИНОМИАЛЬНОЕ МОДЕЛИРОВАНИЕ КОНЕЧНОГО ДЕТЕРМИНИРОВАННОГО АВТОМАТА НА ОСНОВЕ ИЗБЫТОЧНОСТИ ПРЕДСТАВЛЕНИЯ В ПОЛЕ $GF(2^p)$

А. Г. Николаев, Ш. Р. Нурутдинов (Казань)

В работе предложены критерии построения для КДА полиномиальной модели с заданными свойствами в поле $GF(2^p)$.

Теорема 1. *Пусть $A_Q = (X, Q, \delta)$ — конечный детерминированный автомат без выхода, где множество входных элементов*

$X \subset GF(2^k) = G$, множество состояний $Q \subset GF(2^m) = F$, отображение $\delta : G \times F \to F$ или $\delta(x, q) = q'$, где $x \in G$, $q, q' \in F$. Если для δ построить эквивалентное отображение $\delta' : G \times F \to G \times F$ или $\delta'(x, q) = (x', q')$, где $x, x' \in G$, $q, q' \in F$, то критерием создания полиномиальной модели с заданными свойствами для δ' в виде многочлена от одной переменной является совместность системы из $p \cdot 2^p$ уравнений с $m \cdot 2^p$ неизвестными над $GF(2)$, $p = m + k$.

Предлагаемый критерий основан на том, что в значении отображения δ' содержится избыточность: компонента x', может принимать произвольные значения из $GF(2^k)$ [1].

Теорема 2. *Пусть f — отображение, моделирующее функцию перехода КДА, s — наибольшее натуральное число, которое удовлетворяет неравенству*

$$\frac{m}{k} \geq 2^s - 1,$$

где m, k — значения, как в теореме 1. Тогда существует отображение $\widehat{f}$, которое моделируется многочленом степени, не превышающей $2^{p-s}-1$. При этом, исходное отображение f однозначно восстанавливается по отображению $\widehat{f}$.

Пусть s — наибольшее натуральное число, для которого выполняется неравенство теоремы. Тогда элемент x можно представить в виде:

$$x = (x_{2^s}, x_{2^s-1}, \ldots, x_1),$$

где x_i, $i = \overline{1, 2^s - 1}$ — векторы размерности k, x_{2^s} — есть вектор размерности $m - (2^s - 1)k$. Пусть отображение задано при помощи таблицы 1, где (i) двоичное представление числа i. Тогда отображение $\widehat{f}$ зададим таблицей 2. Отображение $\widehat{f}$ представимо многочленом степени не большей $2^{p-s} - 1$.

y	$x = (x_{2^s}, x_{2^s-1}, ..., x_1)$	$x_0 = q$
(0)	$*$	q_0
(1)	$*$	q_1
(2)	$*$	q_2
...	...	...
$(2^p - 2)$	$*$	q_{2^p-2}
$(2^p - 1)$	$*$	q_{2^p-1}

Таблица 1.

y	$x = (x_{2^s}, x_{2^s-1}, ..., x_1)$	$x_0 = q$
(0)	$(*, q_{2^{p-1}}, q_{2^p-2}, ..., q_{2^{p-s+1}}, q_{2^{p-s}})$	q_0
(1)	$(*, q_{2^{p-1}+1}, q_{2^p-2+1}, ..., q_{2^{p-s+1}+1}, q_{2^{p-s}+1})$	q_1
(2)	$(*, q_{2^{p-1}+2}, q_{2^p-2+2}, ..., q_{2^{p-s+1}+2}, q_{2^{p-s}+2})$	q_2
...	...	...
$(2^{p-s}-2)$	$(*, q_{2^p-2}, q_{2^{p-1}-2}, ..., q_{2^{p-s+2}-2}, q_{2^{p-s+1}-2})$	$q_{2^{p-s}-2}$
$(2^{p-s}-1)$	$(*, q_{2^p-1}, q_{2^{p-1}-1}, ..., q_{2^{p-s+2}-1}, q_{2^{p-s+1}-1})$	$q_{2^{p-s}-1}$

Таблица 2.

На рис. блок $\hat{f}$ вычисляет значения отображения $\hat{f}(x)$. На вход блоку подаётся вектор длины p: $(0, 0, ..., 0, u_{p-s-1}, u_{p-s-2}, ..., u_0)$.

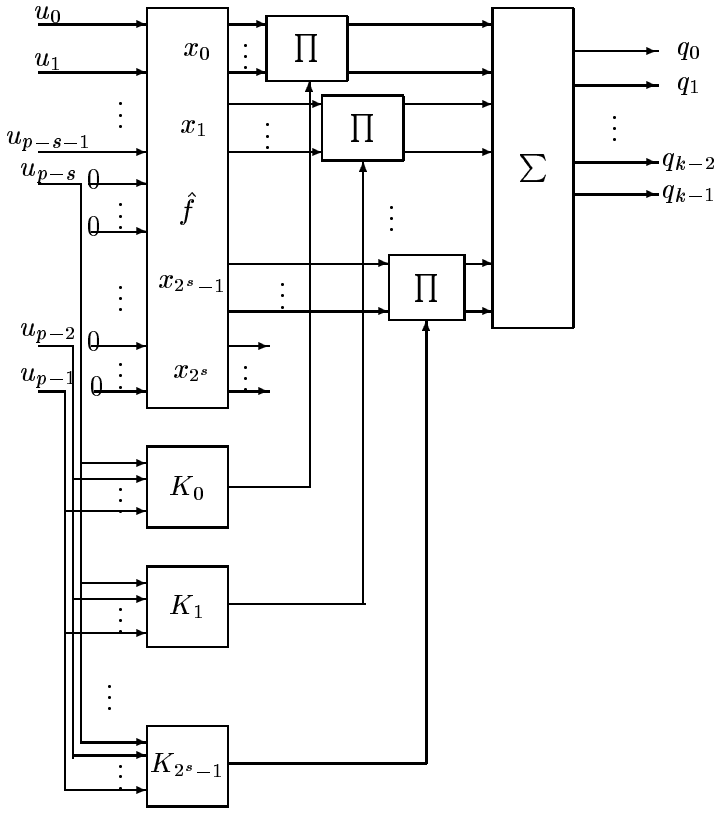


Рис.

Выходные значения блока можно представить в виде $u' = (x_{2^s}, x_{2^s-1}, ..., x_0)$, где x_i, $i \neq 2^s$ — двоичные векторы длины k, а

двоичный вектор x_{2^s} имеет длину $m-(2^s-1)k$. Из таблицы 2 следует, что один из векторов $x_i,\ i \neq 2^s$, а именно вектор с номером, двоичная запись которого равна $(u_{p-1}, u_{p-2}, ..., u_{p-s})$, будет содержать значение нового состояния. Блоки $K_i,\ i = 0, 1, ..., 2^s - 1$ вычисляют значение функции:

$$u_{p-1}^{i_{s-1}} \cdot u_{p-2}^{i_{s-2}} \cdot ... \cdot u_{p-s}^{i_0},$$

где $(i_{s-1}, i_{s-2}, ..., i_0)$ — двоичное представление числа i. Данные блоки при помощи блоков П обнуляют те вектора $x_i,\ i \neq 2^s$, номера которых в двоичной записи не равны $(u_{p-1}, u_{p-2}, ..., u_{p-s})$. Блоки П умножают входной вектор на константу, подаваемую одним из блоков $K_i,\ i \neq 2^s$. Блок $\sum$ суммирует векторы, подаваемые на вход.

Список литературы

1. Николаев А. Г., Нурутдинов Ш. Р. Полиномиальные модели конечных детерминированных автоматов на полем $GF(2^p)$ // Вестник Удмуртского Университета. — 2007. — № 1.

О ФОРМАХ ПРЕДСТАВЛЕНИЯ МОНОТОННЫХ ФУНКЦИЙ НА ТРЁХЭЛЕМЕНТНОЙ ПОЛУРЕШЁТКЕ

Н. Г. Парватов (Томск)

1. *Функции на полурешётке.* Будем обозначать через $E_{\tilde{2}}$ трёхэлементную верхнюю полурешетку, с двумя минимальными элементами 0 и 1 и наибольшим элементом $\top$. В ней и её декартовых степенях отношение порядка обозначется через $\leq$, а операция взятия точной верхней грани обозначается сложением. Будем рассматривать функции, принимающие значения вместе с аргументами в множестве $E_{\tilde{2}}$. Считаются известными понятия суперпозиции, замыкания, замкнутого класса, сохраняемого отношения, схемы (из функциональных элементов) и формулы. Замыкание множества функций A обозначается через $[A]$. Класс сохранения отношений $\alpha_1, \ldots, \alpha_n$ обозначается через $Pol(\alpha_1, \ldots, \alpha_n)$. Функции, сохраняющие отношение $\leq$, называются *монотонными*; их множество обозначается через $M_{\tilde{2}}$. Монотонная функция $f : E_{\tilde{2}}^n \to E_{\tilde{2}}$ называется *точечной*, если для любого $a \in E_{\tilde{2}}^n$ выполняется равенство $f(a) = \sum f(a')$, где сумма вычисляется в полурешетке $E_{\tilde{2}}$ по всевозможным минимальным элементам a' полурешетки $E_{\tilde{2}}^n$ таким, что $a' \leq a$. Если же эта функция ещё сохраняет множество $E_{\tilde{2}}$, то она называется *минимальной*

точечной. Множество всех минимальных точечных функций обозначается через $T_{\tilde{2}}$. Всякую булеву функцию f можно доопределить, причём единственным образом, до минимальной точечной функции f', которую называют *точечным расширением* функции f. В дальнейшем булева функция f и её точечное расширение f' обозначаются и называются одинаково. В частности, через $\vee, \wedge$ и $\neg$ обозначаются точечные расширения соответствующих булевых функций: конъюнкции, дизъюнкции и отрицания.

Монотонные функции на полурешетке $E_{\tilde{2}}$ описывается динамическое поведение комбинационных переключательных и функциональных схем с двузначными сигналами [1]. В [2] для таких функций рассматривались проблемы полноты и выразимости. В данном сообщении рассматриваются некоторые вопросы, связанные с представлением полурешеточных функций формулами и схемами, построенными из элементов $0, 1, \vee, \wedge, \neg$. В частности, в явном виде описывается класс функций, вычисляемых (реализуемых) такими формулами.

2. *Формулы в базисе* $\{0, 1, \vee, \wedge, \neg\}$. Рассмотрим задачу описания в явном виде класса $[0, 1, \vee, \wedge, \neg]$ функций, вычисляемых схемами (формулами) в базисе $\{0, 1, \vee, \wedge, \neg\}$. Заметим, во-первых, что множество $\{0, 1, \top\}$, линейно упорядоченное отношением $\preceq$ так, что $0 \preceq \top \preceq 1$, является (дистрибутивной) решеткой с нулем 0 и единицей 1, со сложением $\vee$ и умножением $\wedge$. Операция $\neg$ является, очевидно, инверсным автоморфизмом этой решетки. В связи с этим операции $\vee$ и $\wedge$ ассоциативны, коммутативны, идемпотентны, дистрибутивны одна по другой, для них выполняются законы поглащения, а с операцией $\neg$ они удовлетворяют законам де Моргана. Вместо закона исключенного третьего в трехзначном случае выполняются неравенства $x \vee \neg x \geq 1$ и $x \wedge \neg x \geq 0$, являющиеся строгими при $x = \top$. Сделанные наблюдения позволяют любую формулу в базисе $\{0, 1, \vee, \wedge, \neg\}$ привести эквивалентными преобразованиями либо к константам 0 или 1, либо к виду "днф" $K_1 \vee \ldots \vee K_r$, где K_i — конъюнкции, составленные из переменных и отрицаний; причем в некоторые конъюнкции некоторые переменные могут входить дважды — с отрицанием и без него.

3. *ДНФ для монотонной функции.* Рассмотрим днф, в которых каждая переменная в любую конъюнкцию входит не более одного раза. Сделаем некоторые обозначения. Для любого набора переменных $x = (x_1, \ldots, x_n)$ и набора $a = (a_1, \ldots, a_n)$ из $E_{\tilde{2}}^n$ через x^a обозначим конъюнкцию $x_1^{a_1} \wedge \ldots \wedge x_n^{a_n}$, где $x_i^0 = \neg x$, $x_i^1 = x$, $x_i^\top = 1$. Для функции f через $f^{-1}(b)$ обозначим полный прообраз элемента b, состоящий из всевозможных таких наборов a, что $f(a) = b$. В частично упорядоченном множестве A через $\max(A)$ обозначим

множество максимальных элементов. Это обозначение имеет смысл и для подмножеств $A \subseteq E_{\tilde{2}}$, упорядоченных отношением $\leq$. В полурешётке $E_{\tilde{2}}^n$ наборы a и b, не имеющие общей нижней грани, назовем *ортогональными* и будем писать $a \perp b$ в этом случае. Для подмножества $B \subseteq E_{\tilde{2}}^n$ через $\perp B$ обозначим множество всех наборов в $E_{\tilde{2}}^n$, ортогональных всем наборам из B. Имеет место

Теорема 1. *Для непустого множества $A \subseteq E_{\tilde{2}}^n$ и набора переменных $x = (x_1, \ldots, x_n)$ формула $\bigvee_{a \in A} x^a$ тогда и только тогда вычисляет функцию $f(x_1, \ldots, x_n)$ из $M_{\tilde{2}}$, когда $f^{-1}(0) = \perp A$ и $\max(f^{-1}(1)) \subseteq A \subseteq f^{-1}(1)$.*

В качестве следствия этой теоремы можно получить, что минимальная точечная функция f вычисляется "сокращенной днф" $\bigvee_{a \in A} x^a$, где $A = \max(f^{-1}(1))$, дальнейшая минимизация которой невозможна. Следовательно, $T_{\tilde{2}} \subseteq [0, 1, \vee, \wedge, \neg]$. В действительности, имеет место

Теорема 2. *Имеет место равенство классов:* $[0, 1, \vee, \wedge, \neg] = M_{\tilde{2}} \cap Pol(E_2)$, *где* $E_2 = \{0, 1\}$.

4. *Разложение Шеннона.* Аналог разложения Шеннона для минимальной точечной функции f имеет вид:

$$f(x_1, \ldots, x_n) = \neg x_1 f_0 \vee x_1 f_1 \vee f_0 f_1,$$

где $f_a = f(a, x_2, \ldots, x_n)$. В отличие от двузначного случая, последним слагаемым здесь нельзя пренебречь. Данное разложение позволяет получить верхнюю оценку $O(2^n/n)$ сложности схем для минимальных точечных функций от n аргументов в базисе $\{0, 1, \vee, \wedge, \neg\}$. Отметим, что нижняя оценка сложности здесь такая же, как для булевых функций, то есть $2^n/n(1 - o(1))$. Вопрос о формульной сложности минимальных точечных функций остаётся открытым.

5. *Точечные продолжения монотонных булевых функций.* Известные методы синтеза схем и формул для булевых функций вообще говоря не применимы к синтезу схем и формул для минимальных точечных функций. Это происходит потому, что последние образуют класс, не замкнутый относительно суперпозиции. В связи с этим вызывают интерес всевозможные случаи, когда суперпозиция точечных функций сама оказывается точечной. В частности, вызывают интерес замкнутые классы минимальных точечных функций. Одним из таких замкнутых классов является класс M_2' всех точечных продолжений монотонных булевых функций (сохраняющих отношение порядка $\preccurlyeq$ на множестве $E_2 = \{0, 1\}$ такое, что $0 \preccurlyeq 1$). Это следует из теоремы 3.

Теорема 3. *Имеет место равенство классов:* $M_2^! = Pol(E_2, \leq, \preceq) = [0, 1, \vee, \wedge]$, *где* $E_2 = \{0, 1\}$.

Список литературы

1. Агибалов Г. П. Дискретные автоматы на полурешетках. — Томск: Изд-во Томского ун-та, 1993.

2. Парватов Н. Г. Функциональная полнота в замкнутых классах квазимонотонных и монотонных трёхзначных функций на полурешетке // Дискретный анализ и исследование операций. Сер. 1. — 2003. — Т. 10, № 1. — С. 61–78.

ФУНКЦИОНАЛЬНЫЕ СИСТЕМЫ НЕДООПРЕДЕЛЕННЫХ ЧАСТИЧНЫХ ФУНКЦИЙ

Н. А. Перязев (Иркутск)

Функциональные системы возникают в различных разделах математики как при теоретических исследованиях, так и в приложениях [1, 2]. Причем в приложениях особую роль играют функциональные системы не всюду определенных функций. При этом не определенность понимается по разному. Ниже вводятся алгебры над множеством функций с двумя типами неопределенности: частичностью и недоопределенностью.

Отображение из A^n в $B(A)$ — можество всех подмножеств A, назовем n-местной недоопределенной частичной функцией (н.ч.ф.) над A. Обозначим через F_A множество всех недоопределенных частичных функций над A. Функции из A^n в $\{0, 1\}$ будем называть квазибулевыми функциями над A, а функции из $\{0, 1\}^n$ в $B(A)$ — псевдобулевыми функциями над A.

Определить в F_A следующие операции: циклической перестановки аргументов (ζ), транспозиции аргументов (τ), отождествления аргументов (Δ), подстановки ($*$), которые введены в [1] для тотальных и частичных функций, а также операцию установки ($\div$):

$(\zeta f)(a_1) = f(a_1)$ и $(\zeta f)(a_1, a_2, ..., a_n) = f(a_2, ..., a_n, a_1)$ при $n > 1$;

$(\tau f)(a_1) = f(a_1)$ и $(\tau f)(a_1, a_2, ..., a_n) = f(a_2, a_1, ..., a_n)$ при $n > 1$;

$(\Delta f)(a_1) = f(a_1)$ и $(\Delta f)(a_1, a_2, ..., a_{n-1}) = f(a_1, a_1, a_2, ..., a_{n-1})$ при $n > 1$;

$(f * g)(a_1, a_2, ..., a_{n+m-1}) = \{a | a \in f(a_0, a_{m+1}, ..., a_{m+n-1})$ для некоторого $a_0 \in g(a_1, ..., a_m)\}$;

$(g \div f)(a_1, ..., a_{n+m-1}) = \{a | f(a, a_1, ..., a_{n-1}) = g(a_n, ..., a_{n+m-1})\}$.

Применяя операции ζ, τ, Δ, можно получать новые функции с перестановкой и отождествлением любых аргументов функций. Для простоты задания таких функций будем именовать аргументы переменными.

Теорема. *Тождественно выполняются следующие включения:*

$$(f(y, y_1, ..., y_n) * (g(x_1, ..., x_m) \div f(y, y_1, ..., y_n))) \subseteq g(x_1, ..., x_m);$$

$$g(x_1, ..., x_m) \subseteq ((f(y, y_1, ..., y_n) * g(x_1, ..., x_m)) \div f(y, y_1, ..., y_n)).$$

Алгебру $\Im_A =< F_A; \zeta, \tau, \Delta, *, \div >$ назовем алгеброй н.ч.ф. над A. Мощность A называется рангом $\Im_A$.

Если алгебра $\Im_A$ конечного ранга k, т.е. $A = \{a_0, ..., a_{k-1}\}$, то она изоморфна следующей алгебре $\Im_k =< F_k; \zeta, \tau, \Delta, *, \div >$, где F_k множество функций из $\{2^0, 2^1, ..., 2^{k-1}\}$ в $\{0, 1, ..., 2^k - 1\}$, получаемых из $f \in F_A$ при кодировке $a_i \to 2^i; \{a_{i_1}, ..., a_{i_s}\} \to 2^{i_1} + ... + 2^{i_s}$.

Алгебру $\Im_k$ назовем алгеброй недоопределенных частичных конечных функций (н.ч.к.ф.), а $\Im_2$ есть алгебра недоопределенных частичных булевых функций (н.ч.б.ф.), которые рассматривались в [3].

Определим сопутствующие функции $f_0, ..., f_{k-1}$ для $f \in F_k$ следующим образом: $f_i(a_1, ..., a_n) = \alpha_i$, где $(\alpha_0, ..., \alpha_{k-1})_2 = f(a_1, ..., a_n)$ и $\alpha_i \in \{0, 1\}$. Через t_k обозначим функцию $t_k(\alpha_0, ..., \alpha_{k-1}) = (\alpha_0, ..., \alpha_{k-1})_2$.

Тогда любая н.ч.к.ф. f представима в виде суперпозиции псевдобулевой и квазибулевых функций

$$f = t_k(f_0, ..., f_{k-1}).$$

Работа выполнена при финансовой поддержке РФФИ, проект 07-01-00240.

Список литературы

1. Мальцев А. И. Итеративные алгебры Поста. — Новосибирск: Новосибирский государственный университет, 1976.

2. Кудрявцев В. Б. О функциональных системах. — М.: Вычислительный центр АН СССР, 1981.

3. Пантелеев В. И., Перязев Н. А. Недоопределенные частичные булевы функции и булевы уравнения // Материалы VII Международной конференции "Дискретные модели в теории управляющих систем". — М.: МАКС Пресс, 2006. — С. 262–265.

ОБ ОДНОЙ СИСТЕМЕ КОНЕЧНЫХ МНОЖЕСТВ АВТОМАТНЫХ ОТОБРАЖЕНИЙ, ДЛЯ КОТОРОЙ ЗАДАЧА ОБ А-ПОЛНОТЕ АЛГОРИТМИЧЕСКИ РАЗРЕШИМА

М. А. Подколзина (Москва)

Пусть P — функциональная система, элементами которой являются ограниченно-детерминированные функции (о.-д.функции), а операциями — операции суперпозиции и обратной связи; при этом предполагается, что переменные о.-д.функций, принадлежащих P, принимают значения из E_2^∞ — множества всех бесконечных последовательностей, составленных из нулей и единиц. Заметим, что любая о.-д.функция может быть "вычислена" некоторым конечным автоматом, если считать, что этот автомат способен "работать" бесконечно долго.

Определение. Пусть $\tau \geq 1$, $\mathfrak{M} \subset P$. Множество $\mathfrak{M}$ называется τ-полным, если для любой о.-д.функции $f \in P$ о.-д.функций множества $\mathfrak{M}$ с помощью операций суперпозиции и обратной связи можно получить о.-д.функцию $g \in P$, совпадающую с f на всех наборах, составленных из слов длины τ.

Определение. Пусть $\mathfrak{M} \subset P$. Множество $\mathfrak{M}$ называется А-полным (аппроксимационно полным), если для любого $\tau \geq 1$ это множество является τ-полным.

Известно [1], что в общем случае задача об А-полноте конечных систем о.-д.функций алгоритмически неразрешима. Вместе с тем, представляет интерес отыскание примеров содержательных подклассов множества конечных систем о.-д.функций, для которых задача об А-полноте была бы разрешима. Приведем один из таких примеров.

Определение. О.-д.функция называется S-о.-д.функцией, если в каждом состоянии "вычисляющего" ее автомата реализуется функция алгебры логики, отличная от тождественной константы.

Пусть $\mathfrak{M} \subseteq P$. Множество $\mathfrak{M}$ называется S-множеством, если $\mathfrak{M}$ состоит только из S-о.-д.функций.

Исходя из [2], нетрудно убедиться в том, что произвольное S-множество $\mathfrak{M}$ является А-полным тогда и только тогда, когда для любого $\tau \geq 1$ множество отображений, осуществляемых о.-д.функциями на словах длины τ, не принадлежит ни одному из S-предполных классов в функциональной системе P_2^τ [3].

Определение. Пусть $T = (t_1, t_2, \ldots)$ — произвольная бесконечная периодическая последовательность. Пусть $n \geq 2$, $f(x_1, \ldots, x_n)$ — S-о.-д.функция из P и λ — разбиение множества $\{1, \ldots, n\}$ на два подмножества — N_1 и N_2. S-о.-д.функцию $f(x_1, \ldots, x_n)$ назовем

(λ, T)-функцией, если для любого $t \in \{t_1, t_2, \ldots\}$ в любом состоянии "вычисляющего" $f(x_1, \ldots, x_n)$ конечного автомата, достижимого из начального с помощью набора слов длины $t-1$, реализуется функция алгебры логики, существенно зависящая от переменных $x_i(t)$ и $x_j(t)$, таких, что $i \in N_1$, $j \in N_2$.

Пусть $\mathfrak{N}$ — множество, состоящее из всех (λ, T)-функций, где разбиение λ и последовательность T могут быть любыми.

Пусть Ω — система конечных S-множеств такая, что для любого $\mathfrak{M} \in \Omega$ $\mathfrak{N} \cap \mathfrak{M} \neq \emptyset$.

Теорема. *Существует алгоритм для распознавания A-полноты S-множеств, принадлежащих системе* Ω.

Список литературы

1. Буевич В. А. Об алгоритмической неразрешимости распознавания А-полноты для ограниченно-детерминированных функций. — Математические заметки. — 1972. — Вып. 6. — С. 687–697.

2. Буевич В. А. Критерий А-полноты для автоматов в терминах А-предполных классов. — PWN. — Warsaw: Banach center publications, 1982. — S. 53–63.

3. Буевич В. А., Подколзина М. А. О полноте S-множеств детерминированных функций // (см. настоящий сборник).

О СЛОЖНОСТИ ОБОБЩЕННЫХ ПОЛИНОМОВ k-ЗНАЧНЫХ ФУНКЦИЙ

С. Н. Селезнева, А. Б. Дайняк (Москва)

Одной из канонических форм задания булевых и k-значных функций являются полиномы. Расширением понятия полинома являются обобщенные полиномы.

Пусть $k \geq 2$, $E_k = \{0, 1, \ldots, k-1\}$. Назовем k-значной функцией отображение $f^n : E_k^n \to E_k$, $n = 0, 1, \ldots$. Множество всех k-значных функций обозначим через P_k, множество всех k-значных функций, зависящих от переменных $x_1, \ldots, x_n$, обозначим через P_k^n.

Определим обобщенные полиномы. Будем рассматривать сложение и умножение по $\bmod k$.

Под *поляризованной переменной* x_i будем понимать выражение вида $x_i + d$, где $d \in E_k \setminus \{0\}$. Произведение вида $y_{i_1}^{m_1} \cdot \ldots \cdot y_{i_r}^{m_r}$, где y_{i_j} есть либо переменная x_{i_j} либо поляризованная переменная x_{i_j}, $y_{i_s} \neq y_{i_t}$ при $s \neq t$, $1 \leq m_1, \ldots, m_r \leq k-1$, назовем *обобщенным мономом.*

Обобщенный моном, в котором нет поляризованных переменных, есть просто *моном*. *Рангом* обобщенного монома называется число r. Будем считать константу 1 вырожденным мономом ранга 0.

Сумму вида $\sum_{i=1}^{l} c_i \cdot X_i$, где $c_i \in E_k \setminus \{0\}$ — коэффициенты, X_i — различные обобщенные мономы, $i = 1, \ldots, l$, назовем *обобщенным полиномом*. *Длиной* обобщенного полинома называется число l. Мы будем полагать константу 0 вырожденным обобщенным полиномом с длиной, равной 0.

Обобщенный полином, в котором не встречаются поляризованные переменные, является просто *полиномом* по $\bmod k$. Если k — простое число, то для каждой функции k-значной логики существует единственный полином по модулю k, ее задающий [1].

Если рассматривать обобщенные полиномы, то однозначность задания каждой функции k-значной логики теряется. Назовем сложностью функции f в классе обобщенных полиномов величину $l(f)$, равную минимальной длине обобщенного полинома, задающего функцию f. Пусть $l_k^{\text{о.п.}}(n) = \max l(f)$, где максимум берется по всем функциям $f \in P_k^n$.

В работе [2] была исследована сложность обобщенных полиномов для булевых функций и получена оценка

$$l_2^{\text{о.п.}}(n) \leq 2 \cdot \frac{2^n}{n}(\log_2 n + 1).$$

Эта оценка была получена методом построения обобщенного полинома на основе затеняющего множества на E_2^n.

Нами был обобщен этот метод на случай k-значных функций (при простых k) и была получена оценка сложности обобщенных полиномов для k-значных функций.

Теорема 1. *Пусть k — простое число. Тогда*

$$l_k^{\text{о. п.}}(n) \lesssim 2 \cdot \frac{k^n}{n} \cdot \ln n$$

при $n \to \infty$.

В работе [3] для булевых функций была получена нижняя мощностная оценка

$$l_2^{\text{о.п.}}(n) \geq \frac{2^n}{n \log_2 3}.$$

Нами была получена нижняя мощностная оценка сложности полиномов для k-значных функций.

Теорема 2. *Пусть k — простое число. Тогда*

$$l_k^{o.n.}(n) \geq \frac{k^n}{n \log_k(k(k-1)+1)}.$$

Работа поддержана РФФИ, проект 07-01-00444 и частично — проект 06-01-00438-а.

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 2001.

2. Кириченко К. Д. Верхняя оценка сложности полиномиальных нормальных форм булевых функций // Дискретная математика. — 2005. — Т. 17, вып. 3. — С. 80–88.

3. Even S., Kohavi I., Paz A. On minimal modulo 2 sums of products for switching functions // IEEE Trans. Elect. Comput. — 1967. — P. 671–674.

ПЕРЕЧИСЛЕНИЕ ЛИНЕЙНЫХ АВТОМАТОВ НАД КОНЕЧНЫМ КОЛЬЦОМ

В. В. Скобелев (Донецк)

В последнее время резко возрос интерес к исследованию дискретных преобразователей информации, построенных на основе конечно-автоматных моделей, представленных системами уравнений над конечными алгебраическими системами. Автоматы над конечным кольцом — важный специальный случай таких преобразователей. При выполнении условия "быть БПИ-автоматом" [1] они являются основой для построения высокоскоростных поточных шифров. Поэтому анализ классов автоматов над конечным кольцом актуален как с теоретической, так и прикладной точки зрения. В настоящей работе решены задачи перечисления [2, 3] линейных автоматов над кольцом $\mathcal{Z}_{p^k} = (\mathbf{Z}_{p^k}, \oplus, \circ)$. С учетом сказанного выше основной упор делается на исследовании тех или иных подклассов БПИ-автоматов.

Выберем в качестве основных моделей автомат Мили M_1

$$\mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus B \circ \mathbf{x}_{t+1},$$

$$\mathbf{y}_{t+1} = C \circ \mathbf{q}_t \oplus D \circ \mathbf{x}_{t+1}$$

и автомат Мура M_2

$$\mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus B \circ \mathbf{x}_{t+1},$$

$$\mathbf{y}_{t+1} = C \circ \mathbf{q}_{t+1},$$

где $A, B, C, D \in \mathsf{M}_n$ – $(n \times n)$-матрицы над кольцом $\mathcal{Z}_{p^k}$, а векторы-столбцы $\mathbf{q}_t, \mathbf{x}_t, \mathbf{y}_t \in \mathbf{Z}_{p^k}^n$ представляют, соответственно, состояние, входной и выходной символы в момент t. Обозначим через $\mathcal{A}_{n,1}$ и $\mathcal{A}_{n,2}$ множество всех рассматриваемых автоматов, соответственно, Мили и Мура, а через $\mathcal{A}_{n,i}^{inv}$ $(i = 1, 2)$ – множество всех БПИ-автоматов $M \in \mathcal{A}_{n,i}$.

На основе оценки числа обратимых матриц

$$n! \cdot (p-1)^n \cdot p^{-n^2} \cdot |\mathsf{M}_n| \le |\mathsf{M}_n^{inv}| \le (1 - p^{-n})^n \cdot |\mathsf{M}_n|,$$

установленной в [4], доказана

Теорема 1. *Для всех $n \in \mathbf{N}$ истинны неравенства*

$$(n! \cdot (p-1)^n \cdot p^{-n^2})^i \cdot |\mathcal{A}_{n,i}| \le |\mathcal{A}_{n,i}^{inv}| \le (1 - p^{-n})^{n \cdot i} \cdot |\mathcal{A}_{n,i}| \quad (i = 1, 2).$$

Исследуем теперь конечно-автоматные характеристики подклассов автоматов $M \in \mathcal{A}_{n,i}^{inv}$ $(i = 1, 2)$. Обозначим через $\mathsf{D}_n^{(1)}$ и $\mathsf{D}_n^{(2)}$ множество диагональных $(n \times n)$-матриц, на главной диагонали которых расположены, соответственно, обратимые и необратимые элементы кольца $\mathcal{Z}_{p^k}$.

Пусть $\mathcal{B}_{n,1}^{inv}$ — множество всех таких автоматов $M_1 \in \mathcal{A}_{n,1}^{inv}$, что $D \in \mathsf{D}_n^{(1)}$, а $\mathcal{B}_{n,2}^{inv}$ — множество всех таких автоматов $M_2 \in \mathcal{A}_{n,2}^{inv}$, что $B, C \in \mathsf{D}_n^{(1)}$. На основе оценки

$$|\mathsf{D}_n^{(1)}| = (p-1)^n \cdot p^{(k-1)\cdot n - k \cdot n^2} \cdot |\mathsf{M}_n|,$$

установленной в [5], доказана

Теорема 2. *Для любого простого числа p при всех $k, n \in \mathbf{N}$*

$$|\mathcal{B}_{n,i}^{inv}| = ((p-1)^n \cdot p^{(k-1-k\cdot n)\cdot n})^i \cdot |\mathcal{A}_{n,i}| \ \ (i = 1, 2).$$

Обозначим через $\mathcal{G}_{n,i}$ $(i = 1, 2)$ множество всех автоматов $M \in \mathcal{A}_{n,i}$, у которых граф переходов — полный граф с петлями. Положим $\mathcal{G}_{n,i}^{inv} = \mathcal{G}_{n,i} \bigcap \mathcal{A}_{n,i}^{inv}$ $(i = 1, 2)$.

Теорема 3. *Для любого простого числа p при всех $k, n \in \mathbf{N}$ истинны равенство $\mathcal{G}_{n,2}^{inv} = \mathcal{A}_{n,2}^{inv}$ и неравенства*

$$((n!) \cdot (p-1)^n \cdot p^{-n^2})^2 \cdot |\mathcal{A}_{n,1}| \leq |\mathcal{G}_{n,1}^{inv}| \leq (1-p^{-n})^{2 \cdot n} \cdot |\mathcal{A}_{n,1}|.$$

Пусть $\mathcal{C}_{n,i}^{inv}$ $(i = 1, 2)$ — множество всех перестановочных автоматов $M \in \mathcal{A}_{n,i}^{inv}$.

Теорема 4. *Для любого простого числа p при всех $k, n \in \mathbf{N}$*

$$|\mathcal{C}_{n,i}^{inv}| \geq (n! \cdot (p-1)^n \cdot p^{-n^2})^{i+1} \cdot |\mathcal{A}_{n,i}| \ \ (i = 1, 2).$$

Пусть $\mathcal{D}_{n,i}^{inv}$ $(i = 1, 2)$ — множество всех приведенных автоматов $M \in \mathcal{A}_{n,i}^{inv}$.

Теорема 5. *Для любого простого числа p при всех $k, n \in \mathbf{N}$*

$$|\mathcal{D}_{n,i}^{inv}| \geq (n! \cdot (p-1)^n \cdot p^{-n^2})^{i+1} \cdot |\mathcal{A}_{n,i}| \ \ (i = 1, 2).$$

Пусть $\mathcal{E}_{n,i}^{inv}$ $(i = 1, 2)$ — множество всех автоматов $M \in \mathcal{A}_{n,i}^{inv}$, имеющих состояния-близнецы.

Теорема 6. *Для любого простого числа p при всех $k, n \in \mathbf{N}$*

$$|\mathcal{E}_{n,1}^{inv}| \geq n! \cdot (p-1)^n \cdot p^{-n^2} \cdot (1-(1-p^{-n})^n)^2 \cdot |\mathcal{A}_{n,1}|,$$

$$|\mathcal{E}_{n,2}^{inv}| \geq (1-(1-p^{-n})^n) \cdot (n! \cdot (p-1)^n \cdot p^{-n^2})^2 \cdot |\mathcal{A}_{n,2}|.$$

Пусть $\mathcal{F}_{n,1}^{inv}$ — множество всех таких автоматов $M \in \mathcal{E}_{n,1}^{inv}$, что $A, C \in \mathsf{D}_n^{(2)}$, а $\mathcal{F}_{n,2}^{inv}$ — множество всех таких автоматов $M \in \mathcal{E}_{n,2}^{inv}$, что $A \in \mathsf{D}_n^{(2)}$. На основе оценки

$$|\mathsf{D}_n^{(2)}| = p^{(k-1) \cdot n - k \cdot n^2} \cdot |\mathsf{M}_n|,$$

установленной в [5], доказана

Теорема 7. *Для любого простого числа p при всех $k, n \in \mathbf{N}$*

$$|\mathcal{F}_{n,1}^{inv}| \geq n! \cdot (p-1)^n \cdot p^{-n^2} \cdot p^{2 \cdot n \cdot (k-1-k \cdot n)} \cdot |\mathcal{A}_{n,1}|,$$

$$|\mathcal{F}_{n,2}^{inv}| \geq p^{n \cdot (k-1-k \cdot n)} \cdot (n! \cdot (p-1)^n \cdot p^{-n^2})^2 \cdot |\mathcal{A}_{n,2}|.$$

Список литературы

1. Even S. On information-lossless automata of finite order // IEEE Trans. on Elect. Comput. — 1965. — V. C-14. — № 4. — P. 561–569.

2. Трахтенброт Б. А., Барздинь Я. М. Конечные автоматы (поведение и синтез). — М.: Наука, 1970.

3. Коршунов А. Д. О перечислении конечных автоматов // Пробемы кибернетики. Вып. 34. — М.: Наука, 1978. — С. 5–82.

4. Скобелев В. В. Об обратимых матрицах над кольцом $\mathcal{Z}_{p^k}$ // Труды ИПММ НАН Украины. — 2006. — Т. 13. — С. 185–192.

5. Скобелев В. В. Анализ структуры класса линейных автоматов над кольцом $\mathcal{Z}_{p^k}$ // Кибернетика и системный анализ (в печати).

ПОСТРОЕНИЕ НИЖНИХ ЭКСПОНЕНЦИАЛЬНЫХ ОЦЕНОК НА ОСНОВЕ ПЕРЕСТАНОВОК

В. Г. Скобелев (Донецк)

Пусть $f \in S(n)$ и

$$f = D_{r_1} \dots D_{r_l} \ \ (r_1 + \dots + r_l = n), \tag{1}$$

где D_{r_i} $(i = 1, \dots, l)$ — цикл длины r_i. Тогда

$$|f| = \text{НОК}\ (r_1, \dots, r_l), \tag{2}$$

где НОК — наименьшее общее кратное. Можно показать, что для функции Шеннона

$$L(n) = \max\{|f| \ | f \in S(n)\}$$

истинно неравенство

$$L(n) \geq e^{O(\sqrt{n})} \ \ (n \to \infty), \tag{3}$$

причем, как это вытекает из [1, 2], оценка из правой части неравенства (3) достигается для перестановок вида

$$f = D_{r+1} \dots D_{2r}, \tag{4}$$

где

$$r = \left\lfloor \frac{1}{6}(\sqrt{24n+1} - 1) \right\rfloor. \tag{5}$$

Вначале покажем, что перестановки вида (4) дают возможность получать экспоненциальные нижние оценки в теории экспериментов с конечными автоматами.

Пусть $\mathcal{A}_{kmn}$ $(r \geq 2)$ — множество всех автоматов $A = (Q, X, Y, \delta, \lambda)$, имеющих фиксированные k-элементное множество состояний Q, m-элементный входной и n-элементный выходной алфавиты. Рассмотрим множество слабоинициальных автоматов

$$\mathcal{A}_{kmn,r} = \{(A, Q_0) | A \in \mathcal{A}_{kmn}, Q_0 \subseteq Q\} \ (2 \leq r \leq k).$$

Обозначим через $L^{diag}_{kmn,r}$ и $L^{sync}_{kmn,r}$ функцию Шеннона для длины минимального, соответственно, диагностического и синхронизирующего слова для слабоинициальных автоматов, принадлежащих множеству $\mathcal{A}_{kmn,r}$. Применение перестановки (4) при определении функции переходов автомата $(A, Q_0) \in \mathcal{A}_{k22,r}$ для фиксированного входного символа дает возможность доказать следующие теоремы.

Теорема 1. *Пусть* $r = \lfloor \frac{1}{6}(\sqrt{24k - 23} + 1) \rfloor$. *Тогда*

$$L^{diag}_{k22,r} \geq e^{O(\sqrt{k})} \ (k \to \infty).$$

Теорема 2. *Пусть* $r = \lfloor \frac{1}{6}(\sqrt{24k - 47} + 1) \rfloor$. *Тогда для всех* $n \in \mathbf{N}$

$$L^{sync}_{k2n,r} \geq e^{O(\sqrt{k})} \ (k \to \infty).$$

Отметим, что из теорем 1 и 2 вытекает, что имеет экспоненциальную временную сложность любой алгоритм построения диагностических или синхронизирующих слов для слабоинициальных конечных автоматов, обладающий следующим свойством: за единицу времени алгоритм строит фрагмент слова, длина которого ограничена полиномом от "площади" автоматной таблицы.

Покажем теперь, что перестановки (4) дают возможность устанавливать экспоненциальные нижние оценки для сложности "взлома" нестационарного секретного замка, в котором "ключ" реализован композицией автономных конечных автоматов, построенных на основе перестановки (4), а "сердцевина" замка — общерекурсивной функцией, вычисляющей "открывающее" на данном промежутке времени замок состояние композиции автоматов.

Назовем автомат без выхода $C_r = (\mathbf{Z}_r, \{x\}, \delta_r)$ счетчиком, если $\delta_r(z, x) = z + 1 (mod\ r)$. Положим

$$\zeta(C_{r_1}, \ldots, C_{r_l}) = (\mathbf{Z}_{r_1} \times \cdots \times \mathbf{Z}_{r_l}, \{x\}, \delta),$$

где

$$\delta((z_1,\ldots,z_l),x)=(\delta_{r_1}(z_1,x),\ldots,\delta_{r_l}(z_l,x)).$$

Из (2) вытекает (НОД — наибольший общий делитель)

Теорема 3. *Автомат* $\zeta(C_{r_1},\ldots,C_{r_l})$ *состоит из* НОД $(r_1,\ldots,r_l)$ *компонент сильной связанности, каждая из которых содержит* НОК $(r_1,\ldots,r_l)$ *состояний.*

Из теоремы 3 и (1)–(5) вытекает

Теорема 4. *Пусть* $r=\lfloor\frac{1}{6}(\sqrt{24n+1}-1)\rfloor$. *Тогда:*

1) *при любой инициализации автомат* $\zeta(C_{r+1},\ldots,C_{2r})$ *генерирует двоичную последовательность периода*

$$L=\sum_{i=1}^{r}\lceil\log(r+i)\rceil\cdot e^{O(\sqrt{n})}\ \ (n\to\infty);$$

2) *при инициализациях, принадлежащих различным компонентам сильной связанности, двоичные последовательности, генерируемые автоматом* $\zeta(C_{r+1},\ldots,C_{2r})$ *— существенно различные.*

Из теоремы 4 вытекает, что "взлом" секретного замка, у которого "ключом" является композиция автоматов $\zeta(C_{r_1},\ldots,C_{r_l})$, сводится к выбору единственного входного слова из экспоненциального множества входных слов. Таким образом, сложность взлома этого секретного замка является экспоненциальной вне зависимости от того, известно или нет число r (или число n) "взломщику".

Список литературы

1. Прахар К. Распределение простых чисел. — М.: Мир, 1967.

2. Скобелев В. Г. Анализ дискретных систем. — Донецк: ИПММ НАНУ, 2002.

О СООТНОШЕНИИ ЗАДАЧИ СИНТЕЗА ИГРОВЫХ ПРОГРАММ И РАСПОЗНАВАНИЯ ВЫПОЛНИМОСТИ ФОРМУЛ ЛОГИКИ ВЕТВЯЩЕГОСЯ ВРЕМЕНИ

Р. В. Хелемендик (Москва)

Игровая программа (ИП) представляет собой специальный граф, который описывает выигрышную стратегию при взаимодействии двух сторон. Рассматривается задача синтеза ИП для заданных условий: начальных значений переменных, набора функций ("ходов"), типа взаимодействия и цели, записываемой формулой логики

ветвящегося времени. При этом стратегия, описываемая получаемой в случае существования ИП, считается выигрышной, если для этой ИП выполнены все компоненты зафиксированного условия $\mathcal{U}$.

Определения игровых правил, игрового взаимодействия, игровой программы и цели приведены в работе [1] и библиографии к ней. В этих работах одна из взаимодействующих сторон считалась "нашей" (например, программа), а другая — внешней (партнёром — пользователем, роботом, другой программой). В настоящей работе взаимодействующие стороны рассматриваются равноправно как "белые" и "чёрные" с сохранением в частных случаях прежней интерпретации. В работе [1] введены переменные, используемые для управления очерёдностью ходов и сотрудничеством ("доверием") или противоборством ("просчитыванием"), после чего стало возможным рассмотрение новых типов взаимодействия, в частности, управляемых ходами сторон.

В связи с этим возник вопрос о выразительных возможностях языка ИП по сравнению с логикой ветвящегося времени (см. [2]). Для всякой ли выполнимой формулы Θ, являющейся целью в условии взаимодействия $\mathcal{U}$, можно подобрать начальные значения переменных, игровое взаимодействие и ходы сторон, чтобы существовала ИП $\mathcal{P}_{\mathcal{U}}$, удовлетворяющая этому условию? И каковы необходимые и достаточные расширения языка игровых программ для достижения требуемой выразительности в случае отрицательного ответа на данный вопрос?

Рассмотрим следующую формулу Θ_1 логики ветвящегося времени.

$$\psi_1 = (\neg z \wedge \neg s \wedge \neg u \wedge \neg p) \tag{1}$$

$$\begin{aligned}\psi_2 = \forall\Box((\neg z \wedge \neg s \wedge \neg u \wedge \neg p \wedge \exists\bigcirc p \wedge \exists\bigcirc\neg p \\ \wedge\forall\bigcirc((z \wedge \neg s \wedge \neg u) \vee (s \wedge \neg z \wedge \neg u) \vee (u \wedge \neg s \wedge \neg z))) \\ \vee((u \vee s \vee z) \wedge \forall\bigcirc(\neg z \wedge \neg s \wedge \neg u \wedge \neg p)))\end{aligned} \tag{2}$$

$$\psi_3 = \forall\Box\forall\Diamond s \wedge \forall\Box\forall\Diamond z \wedge \forall\Box\forall\Diamond u \tag{3}$$

$$\Theta_1 = \psi_1 \wedge \psi_2 \wedge \psi_3 \tag{4}$$

Формула Θ_1 выполнима и имеет модель в форме дорожки из ромбов. Эта модель состоит из вершин u_0, u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8, дуг (u_0, u_1), (u_0, u_2), (u_1, u_3), (u_2, u_3), (u_3, u_4), (u_3, u_5), (u_4, u_6), (u_5, u_6), (u_6, u_7), (u_6, u_8), (u_7, u_0), (u_8, u_0) и функции означивания L: $L(u_0) = L(u_3) = L(u_6) = \emptyset$, $L(u_1) = \{z, p\}$, $L(u_2) = \{z\}$, $L(u_4) = \{s, p\}$, $L(u_5) = \{s\}$, $L(u_7) = \{u, p\}$, $L(u_8) = \{u\}$. Однако для

неё нет подходящего условия $\mathcal{U}$ с целью Θ_1, для которого бы существовала ИП $\mathcal{P}_\mathcal{U}$, так как ходы сторон в "позиции" $\neg z \wedge \neg\, s \wedge \neg u \wedge \neg p$ фиксированы, а сторон две, и поэтому хотя бы одна из формул-обещаний, являющихся членами конъюнкции (3) остается неподтверждённой.

В связи с этим, наряду с имеющимися игровыми взаимодействиями "доверия" (выбор одного хода из всех возможных) и "просчитывания" (предусмотрение каждого из возможных ходов), введём взаимодействие "выбора", при котором рассматриваются любые подмножества возможных ходов. В то же время следуемая ниже формула Θ_2 показывает, что одного такого расширения недостаточно.

$$\Theta_2 = p \wedge \exists\bigcirc(p \wedge \exists\bigcirc p) \wedge \exists\bigcirc(p \wedge \forall\bigcirc(p \wedge \neg p)) \qquad (5)$$

Эта формула выполнима и имеет модель, состоящую из вершин u_0, u_1, u_2, u_3, дуг (u_0, u_1), (u_0, u_2), (u_1, u_3) и функции означивания L: $L(u_0) = L(u_1) = L(u_2) = L(u_3) = \{p\}$. Однако для неё также нет подходящего условия $\mathcal{U}$ с целью Θ_2, так как в ИП одинаковый ход в позиции делается в единственном экземпляре. Поэтому дополним указанное выше расширение игрового взаимодействия до "максимального выбора", при котором допускается рассмотрение любого подмножества возможных ходов белых (чёрных), причём каждый ход из этого подмножества может быть продублирован конечное число раз.

Для ИП с расширенными типами взаимодействия, которые детально описаны в работе [3], имеют место следующие теоремы.

Теорема 1. *Если формула Θ выполнима, то возможно такое доопределение условия $\mathcal{U}$ с целью Θ, что существует ИП $\mathcal{P}_\mathcal{U}$, которая удовлетворяет этому условию.*

Теорема 2. *Если существует ИП $\mathcal{P}_\mathcal{U}$, удовлетворяющая условию $\mathcal{U}$ с целью Θ, то формула Θ выполнима.*

Таким образом, любая проблема, решаемая путём распознавания выполнимости формулы логики ветвящегося времени с построением модели в случае выполнимости, может быть записана и решена в языке игровых программ.

Работа выполнена при финансовой поддержке программы фундаментальных исследований Отделения математических наук РАН "Алгебраические и комбинаторные методы математической кибернетики" (проект "Оптимальный синтез управляющих систем").

Список литературы

1. Хелемендик Р. В. О расширении логического языка игровых программ и решении задачи синтеза // Синтаксис и семантика логических систем: Материалы российской школы-семинара. — Ир-

кутск: издательство ГОУ ВПО “Иркутский государственный педагогический университет”, 2006. — С. 108–112.

2. Хелемендик Р. В. Алгоритм распознавания формул логики ветвящегося времени и эффективный алгоритм построения выводов общезначимых формул из аксиом // Математические вопросы кибернетики. Вып. 15. — М.: Физматлит, 2006. — С. 217–266.

3. Хелемендик Р. В. О расширении типов игрового взаимодействия в языке игровых программ // Материалы VI молодежной научной школы по дискретной математике и ее приложениям (Москва, 16–21 апреля 2007 г.). Часть III. — С. 30–35.

О КОНЕЧНО-ПОРОЖДЁННЫХ ИМПЛИКАТИВНЫХ СТРУКТУРАХ И ПОЛУСТРУКТУРАХ

В. И. Хомич, А. И. Федосеев (Москва)

Настоящее сообщение посвящено изучению конечно-порождённых импликативных структур и полуструктур.

Известно [1, 2], что псевдобулевы алгебры, импликатуры, импликативные полуструктуры и импликативные структуры являются моделями для интуиционистской пропозициональной логики и её фрагментов. В работе [3] эти алгебры называются ν-алгебрами, где ν — набор логических пропозициональных знаков, содержащий знак импликации и определяющий вид алгебры. Очевидно, что конечная алгебра является конечно-порождённой. Известно [4], что существует бесконечная псевдобулева алгебра с одним образующим элементом. Возникает вопрос: при каких условиях конечно-порождённая алгебра будет конечной?

В работах [5, 6] получены критерии конечности конечно-порождённых псевдобулевых алгебр. Согласно теореме Попеля-Диего [7, 8] конечно-порождённая ν-алгебра, где ν не содержит знака дизъюнкции, является конечной. В данном сообщении изложим результаты, доказанные в [9] и касающиеся конечно-порождённых импликативных полуструктур. Основной результат — это критерий конечности для кончено-порождённых импликативных полуструктур с нулём (т.е. $\supset\vee\neg$-алгебр). Он является аналогом критерия конечности, полученного в работах [5, 6] для конечно-порождённых псевдобулевых алгебр.

Элементы $\xi_1, \ldots, \xi_n$ ν-алгебры Ξ называются её образующими элементами, если для любого элемента η из Ξ существует терм $T(\xi_1, \ldots, \xi_n)$, построенный из $\xi_1, \ldots, \xi_n$ с помощью операций ν-алгебры Ξ и удовлетворяющий в Ξ равенству $\eta = T(\xi_1, \ldots, \xi_n)$. Если в ν-алгебре Ξ существует конечное число образующих (не более, чем n образующих) элементов, то Ξ называется конечно-порождённой (n-порождённой) ν-алгеброй.

Пусть Θ — какая-либо ν-алгебра, $\xi, \eta, \zeta_1, \ldots, \zeta_n$ — какие-нибудь её элементы и Φ — её подмножество. Выделенный элемент ν-алгебры Θ будем обозначать через $\mathbf{1}$, а её наименьший элемент (если он имеется) — через $\mathbf{0}$. На Θ можно задать отношение частичного порядка, положив $\xi \leqslant \eta$ в том и только в том случае, когда $\xi \supset \eta = \mathbf{1}$. Элемент σ множества Φ назовём минимальным элементом, если в Θ из соотношений $\tau \in \Phi$ и $\tau \leqslant \sigma$ следует, что $\tau = \sigma$. Множество всех минимальных элементов множества Φ будем обозначать через $\mathfrak{M}(\Phi)$, терм $\zeta_n \supset (\cdots \supset (\zeta_1 \supset \xi) \ldots)$ — через $\{\zeta_1, \ldots, \zeta_n\} \supset \xi$ и число элементов конечного множества Ψ — через $|\Psi|$.

Лемма 1. *В любой конечно-порождённой импликативной полуструктуре (т.е. $\supset\vee$-алгебре) Θ для любых её образующих элементов $\xi_1, \ldots, \xi_n$ верно соотношение $\mathfrak{M}(\Theta) \subseteq \{\xi_1, \ldots, \xi_n\}$.*

В $\supset\vee\neg$-алгебре её наименьший элемент может не содержаться среди её образующих элементов. Поэтому для конечно-порождённых $\supset\vee\neg$-алгебр аналог леммы 1, вообще говоря, не верен. Однако, если конечно-порождённую $\supset\vee\neg$-алгебру рассматривать как $\supset\vee$-алгебру, то для неё лемма 1 верна и, тем самым, её наименьший элемент содержится среди образующих элементов этой $\supset\vee$-алгебры.

Пусть Θ — конечно-порождённая $\supset\vee$-алгебра, а $\xi_1, \ldots, \xi_n$ — её образующие элементы. Положим $\mathfrak{F}_\Theta = \{\xi_i \vee (\xi_i \supset \xi_j) | 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n\}$, а $\mathfrak{E}_\Theta = \{\zeta | \mathfrak{F}_\Theta \supset \zeta = \mathbf{1}\}$. Нетрудно проверить, что $\mathfrak{F}_\Theta \subseteq \mathfrak{E}_\Theta$.

Пусть Φ — конечно-порождённая $\supset\vee\neg$-алгебра, а $\xi_1, \ldots, \xi_n$ — её образующие. Положим $\mathfrak{F}_\Phi = \{\xi_i \vee \neg\xi_i | 1 \leqslant i \leqslant n\}$, а $\mathfrak{E}_\Phi = \{\zeta | \mathfrak{F}_\Phi \supset \zeta = \mathbf{1}\}$. Нетрудно проверить, что $\mathfrak{F}_\Phi \subseteq \mathfrak{E}_\Phi$. Следующие леммы устанавливают некоторые свойства множества $\mathfrak{E}_\Phi$.

Лемма 2. *Пусть ν — один из наборов логических знаков $\supset\vee$ или $\supset\vee\neg$, а Θ — конечно-порождённая ν-алгебра. Тогда имеют место следующие утверждения:*

1) *подмножество $\mathfrak{E}_\Theta$ ν-алгебры Θ вместе с её операциями $\supset$ и $\vee$ является $\supset\vee$-подалгеброй ν-алгебры Θ;*

2) *если $\sigma \in \mathfrak{E}_\Theta$, $\tau \in \Theta$ и $\sigma \supset \tau \in \mathfrak{E}_\Theta$, то $\tau \in \mathfrak{E}_\Theta$;*

3) *если $\sigma \in \mathfrak{E}_\Theta$, $\tau \in \Theta$ и $\sigma \leqslant \tau$, то $\tau \in \mathfrak{E}_\Theta$.*

Лемма 3. *В любой конечно-порождённой $\supset\vee$-алгебре Ψ для любых её элементов η и φ имеет место соотношение $\eta \vee (\eta \supset \varphi) \in \mathfrak{E}_\Psi$.*

Лемма 4. *В любой конечно-порождённой $\supset\vee\neg$-алгебре Ψ для любого её элемента η имеет место соотношение $\eta \vee \neg\eta \in \mathfrak{E}_\Psi$.*

Пусть ν — один из наборов логических знаков $\supset\vee$ или $\supset\vee\neg$. Построим ν-формулу Q_ν, положив Q_ν равной формуле $p \vee (p \supset q)$ или $p \vee \neg p$, где p и q — пропозициональные переменные, в зависимости от того, равен ν набору $\supset\vee$ или набору $\supset\vee\neg$.

Лемма 5. *Пусть ν — один из наборов логических знаков $\supset\vee$ или $\supset\vee\neg$, а Ψ — n-порождённая ν-алгебра. Тогда если ν-формула Q_ν общезначима в Ψ, то $|\Psi| \leqslant 2^{2^n}$.*

Пусть ν — один из наборов логических знаков $\supset\vee$ или $\supset\vee\neg$, а Θ — конечно-порождённая ν-алгебра. Согласно пункту 1) леммы 2 подмножество $\mathfrak{E}_\Theta$ является $\supset\vee$-подалгеброй ν-алгебры Θ. На ν-алгебре Θ зададим бинарное отношение $\sim$. Отношение $\xi \sim \eta (\xi, \eta \in \Theta)$ верно на Θ, если $\xi \supset \eta \in \mathfrak{E}_\Theta$ и $\eta \supset \xi \in \mathfrak{E}_\Theta$. Оно является отношением эквивалентности на Θ и задаёт конечно-порождённую ν-алгебру классов эквивалентности [2], которую обозначим через $\Theta/\mathfrak{E}_\Theta$. Следующая теорема показывает, что ν-алгебра $\Theta/\mathfrak{E}_\Theta$ имеет конечное число элементов.

Теорема 1. *Пусть ν — один из наборов логических знаков $\supset\vee$ или $\supset\vee\neg$, а Θ — конечно-порождённая ν-алгебра. Тогда конечно-порождённая ν-алгебра $\Theta/\mathfrak{E}_\Theta$ — конечна.*

Следующая теорема, даёт критерий конечности для конечно-порождённых $\supset\vee\neg$-алгебр.

Теорема 2. *Конечно-порождённая $\supset\vee\neg$-алгебра Ψ конечна в том и только том случае, когда конечна её $\supset\vee$-подалгебра $\mathfrak{E}_\Psi$.*

Список литературы

1. Карри Х. Б. Основы математической логики. — М.: Мир, 1969.

2. Расева Е., Сикорский Р. Математика метаматематики. — М.: Наука, 1972.

3. Хомич В. И. Об отделимых суперинтуиционистских пропозициональных исчислениях и о конъюнктивно неразложимых элементах в импликативных полуструктурах // Zeitschrift für mathematische Logik und Grundlagen der Mathematik. — 1986. — Bd. 3,. № 2. — S. 149–180.

4. Nishimura I. On formulas of one veriable in intuitionistic propositional calculus // Journal of Symbolic Logic. — 1960. — V. 25, №4. — P. 327–331.

5. Кузнецов А. В. О конечно-порожденных псевдобулевых алгебрах и финитно аппроксимируемых многообразиях // XII Всесоюзный алгебраический коллоквиум. Тезисы сообщений. — Свердловск, 1973. — С. 255–256.

6. Циткин А. И. Структурально полные суперинтуиционистские логики и примитивные многообразия псевдобулевых алгебр // Математические исследования. Неклассические логики. — 1987. — Вып. 98. — С. 134–151.

7. Diego A. Sur les algebrès de Hilbert // Trand. de léspangnol. — Paris, 1966.

8. Янков В. А. Конъюнктивно неразложимые формулы в пропозициональных исчислениях // Известия АН СССР. Серия математическая. — 1969. — Т. 33, № 1. — С. 18–38.

9. Хомич В. И., Федосеев А. И. К вопросу о конечности конечнопорождённых импликативных полуструктур // Логические исследования. Вып. 13. — М.: Наука, 2006. — С. 199–214.

КЛАССЫ НЕДЕТЕРМИНИРОВАННЫХ ФУНКЦИЙ

А. Н. Черепов (Смоленск)

Рассмотрим множество всех бесконечных двоичных последовательностей E. Множество всех функций вида $f : E^n \to E$ обозначим P. Пусть $a_1, a_2, \ldots, a_n$ последовательности из E, $\widetilde{a} = (a_1, a_2, \ldots, a_n)$ — набор таких последовательностей длины n. Пусть $a_1 \mid k, a_2 \mid k, \ldots, a_n \mid k$ первые k членов последовательностей $a_1, a_2, \ldots, a_n$ соответственно, тогда $\widetilde{a}k = (a_1 \mid k, a_2 \mid k, \ldots, a_n \mid k)$.

Назовем функцию f детерминированной, если для всех $k = 1, 2, \ldots$ выполнено:

$$\forall \tilde{a}, \tilde{b} : \tilde{a} \mid k = \tilde{b} \mid k \to f(\tilde{a}) \mid k = f(\tilde{b}) \mid k.$$

Класс всех детерминированных функций обозначим $P_Д$. Обычным образом введем понятия суперпозиции функций, замкнутого класса и полной системы. На множестве функций P определим отношение эквивалентности следующим образом: функции f и g эквивалентны, если $f \in [g \bigcup P_Д], g \in [f \bigcup P_Д]$. Будем считать, что эквивалентные функции имеют один тип недетерминированности. На фактор-множестве по введенному отношению эквивалентности можно ввести частичный порядок: говорим, что $g \preceq f$, если $g \in [f \cup P_Д]$.

Основная цель работы — исследование некоторых из типов недетерминированности функций.

Пусть $\tilde{r} = (r_1, r_2, \ldots)$ — произвольная неубывающая последовательность натуральных чисел, такая, что $\forall i : r_i \geq i$. В множество $P(\tilde{r})$ включим все функции, удовлетворяющие свойству: для любого i и любых $\tilde{a}, \tilde{b}$ выполнено:

$$\tilde{a} \mid r_i = \tilde{b} \mid r_i \to f(\tilde{a}) \mid i = f(\tilde{b} \mid i)$$

В устройствах, реализующих такие функции, i-е значение на выходе появляется после получения r_i-го значения на входе.

Определение. Будем говорить, что функция f принадлежит замкнутому классу m-детерминированных функций $P(m)$, если $\forall k \geq m$ и $\forall \tilde{a}, \tilde{b}$ из того, что $\tilde{a} \mid k = b\tilde{b} \mid k$ следует, что $f(\tilde{a}) \mid k = f(\tilde{b} \mid k$.

Исследуем структуру замкнутых подмножеств класса $P(m)$, содержащих класс P_∂.

Определение. Пусть набор натуральных чисел $\tilde{r} = (r_1, r_2, \ldots, r_n)$ таков, что: $1)\forall i(i \leq r_i \leq m); 2) r_1 \leq r_2 \leq \ldots r_m; 3) если r_i = juj > i, mo r_i = r_i + 1 = = r_j$. В замкнутый класс $P_{\tilde{r}}$ включим все функции $P(m)$, для которых выполнено: $\forall i \forall \tilde{a}, \tilde{b} \in E^n : \tilde{a} \mid r_i = \tilde{b} \mid r_i \to f(\tilde{a}) \mid i = f(\tilde{b}) \mid i$.

Теорема. *В решетку подклассов класса $P(m)$, содержащих все функции класса P_∂, входят классы $P_{\tilde{r}}$ и только они. Эта решетка антиизоморфна решетке по включению всех подмножеств множества $1, 2, \ldots, m-1$. В этом антиизоморфизме классу P_∂ соответствует множество $1, 2, \ldots m-1$, а классу $P(m)$ — пустое множество.*

Следствие 1. *Если функция F принадлежит классу $P_{\tilde{r}}$ и не принадлежит ни одному подклассу этого класса того же типа, то $P_{\tilde{r}} = [f \bigcup P_Д]$.*

Следствие 2. *Количество типов функций, принадлежащих классам $P(m)$, счетно.*

Список литературы

1. Черепов А. Н., Черепов И. А. О классификации недетерминированных функций // Материалы VIII Международного семинара "Дискретная математика и ее приложения" (2–6 февраля 2004 г.). — М.: Изд-во механико-математического факультета МГУ, 2004. — С. 160–163.

ОБ ЭКВИВАЛЕНТНОСТИ ПРОГРАММ С ОПЕРАТОРАМИ, ОБЛАДАЮЩИМИ СВОЙСТВАМИ КОММУТАТИВНОСТИ И ПОДАВЛЕНИЯ

В. Л. Щербина, В. А. Захаров (Москва)

Проблема эквивалентности программ состоит в том, чтобы для пары программ выяснить, имеют ли эти программы одинаковое поведение. Для разработки эффективно проверяемых достаточных условий функциональной эквивалентности программ применяется метод аппроксимации операционных семантик программ алгебраическими моделями программ. В серии работ [1, 2] были выделены классы алгебраических моделей программ, пригодные для аппроксимации последовательных императивных программ. Также в работах [3, 4] были описаны условия, гарантирующие разрешимость проблемы эквивалентности в некоторых классах алгебраических моделей программ. В настоящей работе представлен еще один пример применения этого подхода для решения проблемы эквивалентности программ.

Алгебраические модели программ призваны описывать характерные особенности взаимодействия операторов программ. К таковым относятся свойства коммутативности и подавления операторов. Операторы a и b считаются *коммутативными*, если результат последовательного выполнения этих операторов не зависит от того порядка, в котором они выполняются. Считается, что оператор b *подавляет* оператор a, если выполнение оператора b приводит к такому же результату, что и последовательное выполнение операторов a и b. Эти две особенности программных операторов легко обнаруживаются средствами синтаксического анализа и могут быть адекватно представлены в алгебраических моделях программ.

Пусть заданы конечные алфавиты операторов $\mathcal{A}$ и логических условий $\mathcal{C}$. *Программа* представляется помеченной системой переходов $\langle V, \mathbf{start}, \mathbf{stop}, B, T\rangle$, где V — множество *точек* программы, включающее *точку входа* **start** и *точку выхода* **stop**, $B\colon V \to \mathcal{A}$ — *функция привязки*, сопоставляющая каждой точке программы оператор из $\mathcal{A}$, и $T\colon (V \setminus \{\mathbf{stop}\}) \times \mathcal{C} \to V$ — *функция переходов*, определяющая порядок прохождения точек программы в зависимости от значений логических условий. *Размер* $|\pi|$ программы π — это количество точек в множестве V.

Алгебраические модели задают интерпретацию операторов и логических условий. Рассматриваемые нами модели определяются парой $M = \langle S, \xi\rangle$, состоящей из полугруппы S с множеством образующих $\mathcal{A}$ и *оценки* $\xi : S \to \mathcal{C}$, задающей интерпретацию логических условий программы. *Вычислением* $comp(\pi, M)$ программы π в моде-

ли M называется последовательность пар

$$(v_0, s_0), (v_1, s_1), \ldots, (v_m, s_m), \ldots \ ,$$

удовлетворяющая следующим требованиям:

1) компонентами каждой пары (v_i, s_i) служат точка программы v_i и элемент s_i из S;

2) $v_0 = \mathbf{start}$, s_0 — нейтральный элемент S;

3) $v_i = T(v_{i-1}, \xi(s_{i-1}))$, $s_i = s_{i-1}B(v_{i-1})$ для каждого i, $i \geq 1$;

4) вычисление оканчивается парой (v_m, s_m) тогда и только тогда, когда $v_m = \mathbf{stop}$.

Если $comp(\pi, M)$ оканчивается парой $(\mathbf{stop}, s_m)$, то элемент s_m называется его *результатом* и обозначается $[comp(\pi, M)]$. В противном случае результат $[comp(\pi, M)]$ полагается неопределенным. Программы π' и π'' назовем *эквивалентными на полугруппе* S, если для любой модели $M = \langle S, \xi \rangle$ выполняется равенство $[comp(\pi', M)] = [comp(\pi'', M)]$.

Далее мы будем полагать, что задано разбиение T алфавита операторов $\mathcal{A}$ на два непересекающихся конечных множества $\mathcal{A}_1$ и $\mathcal{A}_2$. В качестве полугруппы S_T выбирается полугруппа с множеством образующих $\mathcal{A}$ и множеством определяющих соотношений $\{ab = b \ : \ a \in \mathcal{A}_1, b \in \mathcal{A}_2\}$. Таким образом задается свойство подавления операторов множества $\mathcal{A}_1$ операторами множества $\mathcal{A}_2$. Полугруппа S_T позволяет описывать некоторые эффекты, связанные с обработкой прерываний, рассмотренные в работе [5]. Подавление $ab = b$ означает, что всякий раз, когда оператор обработки прерываний a успешно завершает работу, и после этого основной оператор b продолжает регулярное вычисление, действия оператора обработки прерываний не оказывает никакого видимого влияния на промежуточное состояние данных. Однако в том случае, если выполнение обработки прерывания приводит к завершению вычисления программы, то результат вычисления зависит как от основных операторов, так и от тех операторов обработки прерывания, которые привели к завершению вычисления.

Наряду со свойствами подавления операторы программы могут обладать свойствами коммутативности. Рассмотрим два симметричных отношения C_1 и C_2 на множестве операторов $\mathcal{A}_1$ и $\mathcal{A}_2$ соответственно. В качестве полугруппы S_{T,C_1,C_2} выбирается полугруппа с множеством образующих $\mathcal{A}$ и множеством определяющих соотношений $\{ab = b \ : \ a \in \mathcal{A}_1, b \in \mathcal{A}_2\} \cup \{ab = ba \ : \ (a, b) \in C_1 \cup C_2\}$. Соотношения последнего вида указывают на то, что пары операторов, находящиеся в отношении $C_1 \cup C_2$, коммутативны.

Теорема 1. *Проблема эквивалентности программ* π_1 *и* π_2 *на полугруппе* S_T *разрешима за время* $O(n^2 \log n)$, *где* $n = \max(|\pi_1|, |\pi_2|)$.

Теорема 1 уточняет предварительную оценку сложности проверки эквивалентности программ с операторами, обладающими свойством подавления, установленную ранее в работе [5]. Этот результат обобщен в следующей теореме.

Теорема 2. *Задача проверки эквивалентности программ* π_1 *и* π_2 *на полугруппе* S_{T,C_1,C_2} *разрешима за время* $O(n^4 \log n)$, *где* $n = \max(|\pi_1|, |\pi_2|)$.

Работа выполнена при финансовой поддержке гранта РФФИ (проект 06-01-00106).

Список литературы

1. Подловченко Р. И. Иерархия моделей программ // Программирование. — 1981. — № 2. — С. 3–14.

2. Подловченко Р. И. Полугрупповые модели программ // Программирование. — 1981. — № 4. — С. 3–13.

3. Захаров В. А. Быстрые алгоритмы разрешения эквивалентности операторных программ на уравновешенных шкалах // Математические вопросы кибернетики. Вып. 7. — М.: Физматлит, 1998. — С. 303–324.

4. Захаров В. А. Быстрые алгоритмы разрешения эквивалентности пропозициональных операторных программ на упорядоченных полугрупповых шкалах // Вестник Московского ун-та. Сер. 15. Вычислит. матем-ка и кибернет. — 1999. — № 3. — С. 29–35.

5. Захаров В. А. Об одной алгебраической модели программ, связанной с обработкой прерываний // Материалы VIII Международного семинара "Дискретная математика и ее приложения" (2–6 февраля 2004 года), 2004. — М.: Изд-во механико-математического факультета МГУ, 2004. — С. 129–131.

Секция «Комбинаторный анализ и теория графов»

Подсекция «Комбинаторный анализ»

ПАМЯТИ ПРОФЕССОРА К. А. РЫБНИКОВА (18.08.1913 – 20.08.2004)

А. Я. Петренюк (Кировоград), А. М. Ревякин (Москва), Е. Е. Маренич (Мурманск)

Начало современной истории развития комбинаторного анализа в России тесно связано с именем **Константина Алексеевича Рыбникова** — доктора физико-математических наук, профессора механико-математического факультета Московского государственного университета имени М. В. Ломоносова.

Рыбников Константин Алексеевич родился 18 августа 1913 г. в станице Луганская Области Войска Донского (по современному административному делению — Луганская область Украины).

Окончил механико-математический факультет МГУ в 1936 г. Математик. Кандидат физико-математических наук (1941). Доктор физико-математических наук (1954). Участник Великой Отечественной войны. С 1945 г. — преподаватель МГУ, с 1956 г. — профессор. Заведующий кабинетом истории и методологии математики и механики механико-математического факультета МГУ (с 1954 по 2004 гг.) с перерывом (1966–1969), когда работал в ЮНЕСКО директором высшего образования (таково официальное название должности). Член ученого совета факультета. В Московском университете читал курсы лекций по истории и методологии математики, комбинаторному анализу студентам механико-математического факультета.

Заслуженный деятель науки РСФСР (1974), Заслуженный профессор МГУ (1994).

Награды: орден «Отечественной войны II степени», два ордена

«Знак Почета», 11 государственных медалей («За оборону Москвы», «За победу над Германией в Великой Отечественной войне», «За трудовую доблесть», «Ветеран труда» и др.), бронзовая медаль ВДНХ, почетный знак Минвуза СССР «За отличные успехи в работе», 5 знаков «Победитель социалистического соревнования», памятные и юбилейные знаки.

Вся жизнь Константина Алексеевича неразрывно связана с Московским университетом. Закончив его в 1936 г., он с 1936 г. по 1938 г. работал в МГУ на заочном отделении заведующим учебной частью, а позднее — заместителем ректора по заочному обучению. В 1938 г. поступил в аспирантуру механико-математического факультета. Кандидатскую диссертацию «К истории вариационного исчисления» защитил 25 июня 1941 г. (на третий день после начала Великой Отечественной войны). Через несколько дней после защиты диссертации приступил к работе на строительстве оборонительных рубежей. С ноября 1941 г. по сентябрь 1945 г. служил в Красной Армии. Был курсантом, затем преподавателем Ленинградского высшего военно-инженерного училища. С мая по октябрь 1944 г. находился на фронте. Был командиром взвода саперов (минеров). Принимал участие в наступлении войск 1-го Белорусского фронта (Белорусская операция 1944 г.). Первый бой — форсирование Березины и освобождение Бобруйска. Работая на минных полях и постоянно подвергаясь смертельной опасности, прошел боевой путь от Бобруйска до Бреста и далее, освобождая Польшу, через Люблин, Пулавы до расположенного на восточном берегу Вислы предместья Варшавы — Праги. После демобилизации в 1945 г. Константин Алексеевич — доцент кафедры математики физического факультета МГУ, с мая 1953 г. — доцент механико-математического факультета. Ровно через 13 лет после защиты кандидатской диссертации, день в день, 25 июня 1954 г. защитил докторскую диссертацию «Исследование математических рукописей Маркса» (А. Н. Колмогоров оценил ее весьма положительно). В 1956 г. стал профессором.

Двумя основными направлениями научной работы К. А. Рыбникова стали: 1) история и методология математики; 2) комбинаторный анализ. Более 40 лет он читал основной курс истории математики на механико-математическом факультете МГУ. Главной задачей исследований в области истории математики Константин Алексеевич считал создание научно обоснованной цельной системы знаний о путях развития математической науки вплоть до времен, как можно более близких к современности. Реализуя этот замысел, он издал учебник «История математики» для студентов математических специальностей университетов и педагогических институтов, а так-

же для широких кругов математиков-специалистов. Первое издание вышло в двух томах: т. 1 (1960 г.), т. 2 (1963 г.). При последующих изданиях (1974 г. и 1994 г.) оба тома были сведены в один. Учебник был переведен на венгерский (1968 г.), испанский (1987 г. и 1988 г.) и японский языки. Это первый фундаментальный учебник, посвященный данной дисциплине (и пока единственный). Он стал классическим руководством, на котором было воспитано не одно поколение математиков. При каждом переиздании текст в ряде мест подвергался переработке и в книгу добавлялись новые главы.

Решению аналогичных задач в области методологии математики посвящена вышедшая в 1979 г. книга К. А. Рыбникова «Введение в методологию математики». Позднее, в 1995 г., она была существенным образом переработана и издана под названием «Введение в методологию математики (тезисы лекций)» (в 1986 г. появился ее перевод на греческий язык). Вместе с учебником «История математики» эти тезисы образуют единое учебное пособие к курсу лекций по истории и методологии математики на механико-математическом факультете МГУ. В последние годы К. А. Рыбниковым была издана серия учебных пособий, дополняющих основной учебник по курсу истории и методологии математики:

1. Комбинаторный анализ. Очерки истории. 1996.
2. Математическое образование и наука в Соединенных Штатах Америки. 1997.
3. Математические модели конфликтных ситуаций. 1998.
4. Вычислительная математика и вычислительная техника; очерки истории (совместно с проф. Л. Н. Королевым). 1999.
5. Математические модели конфликтов. Очерк истории. 2000.
6. Математические модели конфликтов. Очерк истории 2. 2001.
7. Математические интерпретации. 2002.
8. Математические инварианты. 2003.
9. Математика в СССР; образование и наука. Очерк истории. 2004.

Другим важнейшим направлением научной и педагогической деятельности Константина Алексеевича явился комбинаторный анализ. Роль комбинаторного анализа в 20-м столетии чрезвычайно возросла. Поразительно много областей математики содержит задачи или группы задач комбинаторного характера. При этом, несмотря на заманчивую простоту постановки, комбинаторные задачи в большинстве очень трудны; многие из них не поддаются решению до сих пор. Для этой совокупности разнообразных задач к середине прошлого столетия все еще не существовало единой теории или единого метода. Вместе с тем существование целой сети взаимных интерпретаций приводило к мысли о наличии их общей теоретической

основы. Работу по построению общей теории комбинаторного анализа Константин Алексеевич начал в 1960-е годы. Длительная научная командировка в США (1963–1964 гг.) способствовала накоплению информации и возникновению научных контактов со многими известными комбинаториками (Джан-Карло Рота, Генри Крапо и др.). Константину Алексеевичу довелось стать свидетелем «комбинаторного взрыва», начавшегося в 50-х годах прошлого века. В предисловии к своему переводу книги Г. Дж. Риордана «Комбинаторная математика» (М.: Мир, 1966) Константин Алексеевич связывал развитие комбинаторики с бурным развитием вычислительной техники, которое, по его мнению, привело не только к расширению ее приложений, но и к перестройке содержания.

Регулярной учебной и научной работе Константина Алексеевича в области комбинаторного анализа предшествовал период, когда он с июня 1966 г. по август 1969 г. работал в ЮНЕСКО директором высшего образования. После его возвращения, на механико-математическом факультете началось чтение учебных курсов, начали работать учебный и научный семинары, появились аспиранты, специализирующиеся по комбинаторному анализу. Константин Алексеевич отмечал, что штатных должностей для этой работы не было ни тогда, ни потом. Но К. А. Рыбников был хорошим организатором, поэтому быстро подросли молодые энтузиасты, добровольные помощники. Все виды учебной работы до середины 90-х годов сохраняли регулярность, привлекали значительное число студентов.

В 1972 г. был издан учебник К. А. Рыбникова «Введение в комбинаторный анализ» (изд-во МГУ). Впоследствии этот учебник «оброс» дополнениями, и, когда в 1985 г. появилось его второе издание, оно приобрело вид научной монографии (в 1988 г. появился перевод на испанский язык). В период времени между этими изданиями появился задачник: «Комбинаторный анализ: задачи и упражнения»; в 1979 г. ротапринтным изданием, а в 1982 г. — в издательстве «Наука». Его составителями, кроме К. А. Рыбникова, были М. В. Меньшиков, А. М. Ревякин, А. Н. Копылова, Ю. Н. Макаров, Б. С. Стечкин. Все 879 задач в этой книге снабжены не только ответами, но и пояснениями, указаниями, даже решениями (в 1988 г. появился перевод на польский язык, а в 1989 г. — на испанский).

Быстро возник научный семинар по комбинаторному анализу, бессменным руководителем которого долгие годы был Константин Алексеевич. Этот семинар пользовался огромной популярностью. В его работе принимали участие исследователи из всех регионов СССР. Научные контакты Константина Алексеевича давали ему возможность привлекать к участию в работе семинара и иностранных участников, что делало работу семинара еще интереснее. На-

учные результаты семинара публиковались в сборниках под общим названием «Комбинаторный анализ» под редакцией К. А. Рыбникова, ко всем сборникам было написано предисловие редактора с кратким анализом опубликованных результатов. Всего было 8 выпусков сборника: в 1971, 1972, 1974, 1976, 1980, 1983, 1986, 1989 гг.

Усилиями Константина Алексеевича и участников семинара на механико-математическом факультете были проведены Всесоюзные семинары по комбинаторному анализу в 1971, 1973, 1975, 1978, 1981 гг., которые привлекали большое число участников.

Начиная с 1984 г., на механико-математическом факультете регулярно проходят семинары по дискретной математике и ее приложениям под руководством академика О. Б. Лупанова (1932–2006) и его сотрудников. В программах этого семинара одна из самых многочисленных секций — секция комбинаторного анализа.

Многие ученики К. А. Рыбникова под его руководством защитили кандидатские и докторские диссертации по комбинаторному анализу или близкой тематике. Приведем их список:

1. Кутлумуратов Джамурат (23.02.1965, мех-мат, МГУ) 07.00.10. «История комбинаторного анализа».

2. Петренюк Анатолий Яковлевич (7.04.1972, мех-мат, МГУ) 01.01.06. «Исследования в теории конечных систем инцидентностей».

3. Ревякин Александр Михайлович (24.12.1976, мех-мат, МГУ) 01.01.06. «Комбинаторные конструкции общих алгебраических систем (матроидов)».

4. Пермяков Петр Петрович (14.12.1978, ИИЕиТ) 07.00.10. «Из истории комбинаторного анализа (Кэли, Сильвестр, современники)».

5. Большаков Владимир Иванович (12.02.1982, мех-мат МГУ) 01.01.06. «Коалгебры и алгебры инцидентности с весом над предкатегориями и их приложения».

6. Сидоренко Александр Феликсович (26.11.1982, мех-мат МГУ) 01.01.05. «Экстремальные константы и неравенства для распределения сумм случайных векторов».

7. Малых Алла Ефимовна (25.03.1983, мех-мат, МГУ) 07.00.10. «Возникновение и развитие конечных геометрий»; Докторская диссертация: «Комбинаторный анализ в его развитии». (19.11.92, ИИЕиТ РАН)

8. Яковлев Николай Николаевич (10.02.1984, мех-мат, МГУ) 01.01.04. «Экстремальные задачи геометрий чисел».

9. Лузгин Владимир Николаевич (12.04.1985, мех-мат, МГУ) 01.01.05. «Последовательные статические и случайные планы для линейной модели планирования отсеивающих экспериментов».

10. Бурый Кирилл Евгеньевич (20.12.1985, мех-мат, МГУ) 01.01.05. «Асимптотические задачи в теории планирования отсеивающих экспериментов».

11. Сальников Сергей Георгиевич (13.10.1989, ВМК, МГУ) 01.01.09. «Локально рамсеевские свойства дискретных структур».

12. Иванов Олег Валентинович (15.10.1992, ИИЕиТ) 07.00.10. «Из истории симметрических функций (начиная с теории П. А. Мак Магона)».

13. Шматков Вадим Дмитриевич (12.05.1995, мех-мат, МГУ) 01.01.06. «Изоморфизмы и автоморфизмы колец и алгебр инцидентности».

Кроме того, один из авторов этой статьи Маренич Евгений Евгеньевич, будучи докторантом и работая в возглавляемом Константином Алексеевичем коллективе комбинаториков, защитил (14.02.1997, мех-мат, МГУ) докторскую диссертацию: «Алгебры бинарных функций на упорядоченных множествах» (01.01.09).

Тематика диссертаций столь разнообразна потому, что общий объект исследования — комбинаторная теория — допускает большое число интерпретаций, в том числе и таких, которые уже вошли в состав сопредельных научных дисциплин.

Много внимания Константин Алексеевич уделял вопросам преподавания математики в средней школе. Им написан ряд статей для журнала «Математика в школе», книги для школьников «Профессия — математик» (1983) и для учителей «Возникновение и развитие математической науки» (1987).

К. А. Рыбников внес значительный вклад в дело подготовки научных кадров высшей квалификации. Под его руководством защищено 32 кандидатских и 7 докторских диссертаций по пяти специальностям ВАК. Он был членом нескольких ученых советов в МГУ и РАН.

Константин Алексеевич вел также большую редакционно-издательскую работу. Он был членом редколлегий журналов «Вестник Московского университета. Серия 1. Математика. Механика», «Дискретная математика», а также издаваемого в Институте истории естествознания и техники (ИИЕиТ) РАН периодического издания «Историко-математические исследования». Он был одним из основателей, а затем бессменным членом редколлегии систематически выходившего в МГУ сборника «История и методология естественных наук».

Два сына К. А. Рыбникова — Алексей Константинович и Константин Константинович и внуки Татьяна Алексеевна и Константин Алексеевич (младший) — дети А. К. Рыбникова — также стали математиками. Научные интересы К. К. Рыбникова и

К. А. Рыбникова-младшего оказались в значительной степени близки к комбинаторному анализу.

К. К. Рыбников занимался проблемами решения систем булевых уравнений, включая вопросы прикладного характера, связанные с анализом узлов нейросетей. Совместно с Т. А. Ласковой (дочерью А. К. Рыбникова) он опубликовал ряд работ, в которых, в частности, решается вопрос оценки числа решений системы булевых уравнений для некоторых частных случаев (журналы «Обозрение прикладной и промышленной математики» и «Вестник МГУ леса. Лесной вестник», 2002–2007 гг.).

К. А. Рыбников-младший является специалистом в области дискретной математики. Он — ученик Сергея Сергеевича Рышкова. Две его работы посвящены комбинаторике (обе написаны совместно с Томасом Заславским). В одной из них изучаются циклические свойства графов с «усилениями» (gain graphs) и их приложения к геометрии кусочно-линейных поверхностей. Граф с усилениями — это ориентированный граф, в котором каждому ребру предписан элемент группы; обращение ориентации соответствует замене элемента группы на обратный. Граф с усилениями называется сбалансированным, если произведение усилений вдоль любого замкнутого пути равно 1. Сбалансированный граф с усилениями также известен в литературе как граф напряжений (voltage graph). В статье выведено несколько тестов для проверки сбалансированности графа с абелевыми усилениями. Применимость этих тестов, вообще говоря, зависит от свойств группы. Оказывается, что для каждого теста класс графов, для которых тест может быть применен с любой абелевой группой усилений, замкнут относительно операции взятия миноров. В другой работе приводятся характеризации этих классов в терминах запрещенных миноров.

Заметим, что А. К. Рыбников (старший сын Константина Алексеевича), работы которого посвящены дифференциальной геометрии, тоже отдал дань комбинаторному анализу, написав совместно с супругой Наталией Михайловной Рыбниковой статью «Новое доказательство несуществования проективной плоскости порядка 6» («Вестник Московского университета». — 1966. — № 6.).

НЕКОТОРЫЕ ЗАДАЧИ УПРАВЛЕНИЯ ДИНАМИЧЕСКИМИ СТРУКТУРАМИ ДАННЫХ

Е. А. Аксёнова (Петрозаводск)

Во многих приложениях требуется обработка записей с упорядоченными определенным образом ключами. Часто мы накапливаем некоторый набор записей, после чего обрабатываем запись с максимальным значением ключа, затем, возможно, накопление записей продолжается, затем обрабатывается запись с наибольшим текущим ключом и т. д. Соответствующая структура данных, поддерживающая операции вставки нового элемента и удаления элемента наибольшим приоритетом, называется очередью по приоритетам.

Пусть в памяти размера m единиц мы хотим работать с двухприоритетной очередью, представленной в виде двух последовательных FIFO-очередей. Первой очереди присвоим приоритет 1, второй — приоритет 2. Наивысший приоритет — 2. Пусть заданы вероятностные характеристики очередей: p_1, p_2 — вероятности включения элемента в первую и вторую очереди соответственно, q — вероятность исключения элемента из очередей, r — вероятность операции, не изменяющей длины очереди (например, чтение). Исключение элемента из очереди происходит по наивысшему приоритету, т. е. пока вторая очередь не пуста, с вероятностью q исключение элементов происходит из этой очереди. Как только вторая очередь станет пустой, с вероятностью q исключение элементов будет происходить из первой очереди.

Пусть первой очереди выделено s единиц памяти, где $0 \le s \le m$. Обозначим x_1 и x_2 — текущие длины очередей в каждый момент времени. В качестве математической модели будем иметь случайное блуждание по целочисленной решетке в двухмерном пространстве, где $0 \le x_1 < s+1$, $0 \le x_2 < m-s+1$, а $x_1 = s+1$, $x_2 = m-s+1$ — поглощающие экраны. Блуждание начинается из состояния $x_1 = 0, x_2 = 0$.

Задача состоит в том, чтобы определить параметр s так, чтобы время блуждания до попадания на поглощающие экраны было максимальным, т. е. сколько единиц памяти выделить первой очереди в зависимости от вероятностных характеристик так, чтобы время работы до переполнения какой-либо очереди было максимальным.

Пронумеровав состояния области блуждания, получим конечную однородную поглощающую цепь Маркова. Для полученной цепи рассмотрим матрицу Q — матрицу переходных вероятностей из невозвратных состояний в невозвратные. Она будет иметь блочную структуру. Вычислим фундаментальную матрицу $N = (I-Q)^{-1}$ [1]. Элемент N_{ij} имеет смысл количества единиц времени, которое процесс находился в состоянии j, если блуждание началось из состо-

яния i. Чтобы найти математическое ожидание $M(t)$ числа шагов до поглощения, нужно найти сумму элементов строки матрицы N, соответствующей началу процесса.

Теперь рассмотрим способ управления очередями, когда при переполнении какой-либо из очередей работа не завершается, а если очередь занимает всю предоставленную ей память, то все последующие элементы, поступающие в нее, отбрасываются до тех пор, пока не появится свободная память (т. е. до тех пор, пока не произойдет исключение элемента из очереди).

В [2] рассмотрена задача управления двумя последовательными циклическими FIFO-очередями на бесконечном времени, в [3] рассмотрена задача управления тремя FIFO-очередями для последовательного, связного и страничного способов представления, в [4] рассмотрена задача управления тремя последовательными циклическими FIFO-очередями на бесконечном времени.

Пусть в памяти размера m единиц мы работаем с тремя FIFO-очередями, представленными в виде трех связных списков. Для связного представления очередей $\frac{m}{2}$ единиц памяти тратится на хранение связей, $\frac{m}{2}$ — на хранение данных. Мы здесь предполагаем, что поле связи и информационное поле имеют одинаковый размер. Пусть известны некоторые вероятностные характеристики операций, производимых с очередями. Пусть p_1, p_2, p_3 — вероятности включения информации в в первую, вторую и третью очереди, соответственно, q_1, q_2, q_3 — вероятности исключения информации из первой, второй и третьей очереди соответственно, r — вероятность операции, не изменяющей длины очереди, где $p_1 + p_2 + p_3 + q_1 + q_2 + q_3 + r = 1$. Предполагается, что в очередях хранятся данные фиксированного размера.

Обозначим x_1, x_2, x_3 — текущие длины очередей в каждый момент времени. В качестве математической модели рассмотрим случайное блуждание в трехмерном пространстве по целочисленной решетке в области $0 \le x_1 \le \frac{m}{2} + 1$, $0 \le x_2 \le \frac{m}{2} + 1$, $0 \le x_3 \le \frac{m}{2} + 1$. Попадание на плоскость $x_1 + x_2 + x_3 = \frac{m}{2} + 1$ соответствует ситуациям потери элементов.

Для данного способа представления необходимо вычислить время, проведенное в состояниях потери элементов, и сравнить с временем в случае последовательного представления.

Случайное блуждание будем рассматривать в виде регулярной конечной цепи Маркова с матрицей переходных вероятностей P. Зададим нумерацию состояний цепи. При введеной нумерации матрица P в данной задаче имеет определенную структуру. Далее, необходимо решить уравнение $\alpha \cdot P = \alpha$ [1], где α — предельный вектор для полученной марковской цепи. По закону больших чисел

для регулярной цепи элемент вектора α_i — это доля времени, которое процесс проводит в состоянии i. Для вычисления времени, проведенного в состояниях потери элементов, нужно просуммировать соответствующие элементы вектора α.

Для решения представленных задач доказаны теоремы, определяющие вид необходимых матриц, разработаны алгоритмы и программы, вычисляющие среднее время работы.

Работа выполнена при финансовой поддержке РФФИ (проект №06-01-00303).

Список литературы

1. Кемени Дж., Снелл Дж. Конечные цепи Маркова. — М.: Наука, 1970.

2. Соколов А. В., Тарасюк А. В. Об оптимальном управлении циклическими FIFO-очередями // Системы управления и информационные технологии. — 2005. — № 3 (20). — С. 29–33.

3. Аксенова Е. А. Исследование методов представления трех очередей в памяти одного уровня // Труды ИПМИ КарНЦ. Методы математического моделирования и информационные технологии. — Петрозаводск, 2006. — Вып. 4. — С. 163–186.

4. Аксенова Е. А. Оптимальное управление FIFO-очередями на бесконечном времени // Межвуз. сб. "Стохастическая оптимизация в информатике". — Изд-во С.-Петербургского университета. — Вып. 2. — С. 71–76.

ОПТИМАЛЬНОЕ УПРАВЛЕНИЕ ПАРАЛЛЕЛЬНОЙ ДВУХПРИОРИТЕТНОЙ ОЧЕРЕДЬЮ

Т. В. Афанасьева, А. В. Соколов (Петрозаводск)

Пусть в памяти размера m требуется работать с приоритетной очередью с двумя приоритетами [1–3], реализованной в виде двух FIFO очередей [3–5], операции с которыми могут выполняться параллельно. Пусть первая очередь имеет высший приоритет. Заданы вероятностные характеристики очередей, причем исключение из второй очереди возможно, только, когда очередь с высшим приоритетом пуста.

Обозначим через y текущую длину первой очереди, а через x — длину второй. Пусть для первой очереди мы выделили s-единиц памяти, а для второй — $m - s$.

Тогда в качестве математической модели процесса мы будем иметь случайное блуждание по целочисленной решетке в области

$0 \le x \le s+1$, $0 \le y \le m-s+1$. Находясь в точке (x,y), где $0 \le x < s+1$, $0 < y < m-s+1$, мы с вероятностью p_1 перейдем в точку $(x, y+1)$, с вероятностью p_1p_2 — в точку $(x+1, y+1)$, с вероятностью p_2 — в точку $(x+1, y)$, с вероятностью p_2q — в точку $(x+1, y-1)$, с вероятностью q — в точку $(x, y-1)$, с вероятностью r — в точку (x, y).

Если же $0 \le x < s+1$, $y = 0$, то мы с вероятностью p_1 перейдем в точку $(x, y+1)$, с вероятностью p_1p_2 — в точку $(x+1, y+1)$, с вероятностью p_2 — в точку $(x+1, y)$, с вероятностью p_1q — в точку $(x-1, y+1)$, с вероятностью q — в точку $(x-1, y)$, с вероятностью r — в точку (x, y), где $p_1 + p_2 + q + r + p_1p_2 + p_1q = 1$.

Отметим, что $p_1q = p_2q$, так как p_1q появляется на границе области, а p_2q в середине области блуждания.

Блуждание начинается в точке $(0, 0)$, а поглощение на границах происходит на прямых $x = s+1$, $y = m-s+1$. Нашей задачей является выбор такого значения s, чтобы среднее время до поглощения было максимальным.

Пронумеровав точки области блуждания начиная с нуля с правого верхнего угла вниз справа налево, получим однородную цепь Маркова с $(m-s+1)(s+1)$ состояниями.

Геометрически блуждание по решетке можно представить так: добавление элемента в первую очередь — сдвиг вверх по оси Y, удаление элемента из первой очереди — сдвиг вниз по оси Y, добавление элемента во вторую очередь — сдвиг вправо по оси X, удаление элемента из второй очереди (при условии, что нет элементов в первой) — сдвиг влево по оси X, добавление элемента в две очереди одновременно — сдвиг вправо и вверх по диагонали, удаление элемента из первой очереди и одновременно добавление элемента во вторую — сдвиг вправо и вниз по диагонали, добавление в первую, исключение из второй одновременно — сдвиг влево и вверх по диагонали.

Теперь рассмотрим матрицу Q — матрицу переходных вероятностей из невозвратных состояний в невозвратные. Если размер памяти равен m, а для второй очереди — s, то размерность матрицы Q будет $(m-s+1)(s+1)$. Введем обозначение $diag(a, b, c)$ — диагональная матрица размерности $(m-s+1)(m-s+1)$, в которой значения элементов на главной диагонали равны a, ниже — b, выше — c, а остальные — нули.

Теорема. *Матрица Q размерности $(m-s+1)(s+1)$ при за-*

данной нумерации и при данных размерах памяти m и s имеет вид:

$$Q = \begin{pmatrix} A & C & 0 & 0 & 0 & & & 0 \\ B & A & C & 0 & 0 & & & 0 \\ 0 & B & A & C & 0 & & & 0 \\ \vdots & \vdots & \ddots & \vdots & & & & \\ 0 & & & & & B & A & C \\ 0 & & & & & & B & D \end{pmatrix},$$

где A=$diag(r, p_1, q)$, B=$diag(p_2, p_1p_2, p_1q)$, подматрица C является матрицей размерности $(m-s+1)(m-s+1)$, все элементы которой равны 0, кроме $c_{m-s+1,m-s}$ и $c_{m-s+1,m-s+1}$, которые имеют значение p_1q и q соответственно, а подматрица D аналогична матрице A, кроме элемента $d_{m-s+1,m-s+1}$, который равен $r+q$.

Для решения необходимо найти фундаментальную матрицу $N = (I-Q)^{-1}$, где I — единичная матрица.

Элемент N_{ij} имеет смысл количества единиц времени, которое процесс находился в состоянии j, если блуждание началось из состояния i. Значит, чтобы найти математическое ожидание $E(t)$ числа шагов до перераспределения, надо найти сумму элементов строки фундаментальной матрицы, соответствующей начальному состоянию, и добавить 1, так как чтобы произошло перераспределение нужен еще один шаг для переполнения или опустошения. Разработаны алгоритм и программа решения задачи. Приводятся результаты численных экспериментов.

Работа выполнена при финансовой поддержке РФФИ (грант 06-01-00303).

Список литературы

1. Боллапрагада В., Мэрфи К., Уайт Р. Структура операционной системы Cisco IOS. — Вильямс, 2002.

2. Седжвик Р. Фундаментальные алгоритмы на C++. Анализ, структуры данных, сортировка, поиск. — ДиаСофт, 2001.

3. Аксенова Е. А., Соколов А. В. Некоторые задачи оптимального управления FIFO очередями // Труды Второй Всероссийской научной конференции "Методы и средства обработки информации". — М.: Изд. отдел ВМК МГУ, 2005. — С. 318–322.

4. Кнут Д. Искусство программирования для ЭВМ. Т. 1. — М.: Мир, 1976.

5. Соколов А. В. Математические модели и алгоритмы оптимального управления динамическими структурами данных. — Изд. ПГУ, 2002.

6. Кемени Дж., Снелл Дж. Конечные цепи Маркова. — М: Наука, 1970.

О СТАТИСТИКАХ ЭЙЛЕРА НА ГРУППЕ ПЕРЕСТАНОВОК

Л. Н. Бондаренко (Пенза)

В [1] рассмотрен ряд свойств распределения Эйлера на группе перестановок S_n. В данной работе приводятся некоторые дополнительные результаты о статистиках Эйлера.

Определим многочлены Эйлера $A_n(t)=\sum_{k=1}^{n} A_{n,k}t^k$ выражением $A_n(t)=(1-t)^{n+1}(tD)^n(1-t)^{-1},\ n\in\{0\}\bigcup\mathbf{N}$, где $D=d/dt$. Тогда числа Эйлера $A_{n,k}$ вычисляются по рекуррентной формуле

$$A_{0,k}=\delta_{0,|k|},\ A_{n,k}=kA_{n-1,k}+(n-k+1)A_{n-1,k-1},\ n\in\mathbf{N},k\in\mathbf{Z}, \quad (1)$$

где $\delta_{i,j}$ — символ Кронекера, $A_n(1)=n!$ и последовательность $\{A_{n,k}/n!\}$ задает вероятностное распределение Эйлера, асимптотически сходящееся к нормальному с параметрами $(n/2,\sqrt{n/12})$ [1, 2].

Определение. *Отображение* $\mathrm{E}: S_n\to\mathbf{N}$ *называется эйлеровой статистикой или* E*-статистикой, если выполнено соотношение* $A_n(t)=\sum_{\sigma\in S_n} t^{\mathrm{E}(\sigma)}$, *где* $\sigma=\sigma(1)\ldots\sigma(n)\in S_n$.

Для перестановки $\sigma\in S_n$ через $\mathrm{RISE}(\sigma)$ обозначается число подъемов, т. е. число всех номеров $0\le i\le n-1$, для которых $\sigma(i)<\sigma(i+1)$, $(\sigma(0)=0)$, а $\mathrm{IRISE}(\sigma)=\mathrm{RISE}(\sigma^{-1})$. Через $\mathrm{IMAL}(\sigma)$ обозначается число различных целых чисел последовательности $\{x_i\}$, где x_i — число значений $\sigma(j)$, стоящих слева от $\sigma(i)$ и таких, что $\sigma(j)<\sigma(i)$. Отображения RISE, IRISE, IMAL являются E-статистиками [1].

Определим $\mathrm{IVP}(\sigma)$ (индекс вектора перестановки $\sigma\in S_n$) при фиксированном ключе $\kappa\in S_n$ как вес $|\tau|$, т. е. сумму компонент τ, где $\tau\equiv\sigma\oplus\kappa(\mathrm{mod}\ n)$, деленный на n. Знак "$\oplus$" по mod n означает покоординатное сложение векторов перестановок σ и κ по mod n, причем в результате записываются наименьшие положительные вычеты.

Имеет место следующая

Теорема 1. *Статистика* IVP: а) *не зависит от выбора ключа* κ; б) *является эйлеровой, т. е.* $A_n(t)=\sum_{\sigma\in S_n} t^{\mathrm{IVP}(\sigma)}$.

Доказательство. Переставим элементы ключа $\kappa\in S_n$ так, чтобы получить единичную перестановку $\varepsilon\in S_n$. Отображение $\Phi:\kappa\mapsto\varepsilon$ применимо ко всем перестановкам $\sigma\in S_n$. Биекция $\Phi: S_n\to S_n$ показывает, что статистика IVP при любом ключе κ будет такой же, как и для ключа ε. Для доказательства пункта б) применяется метод математической индукции, использующий формулу (1) и простое неравенство $0<\mathrm{IVP}(\sigma)<(|\sigma|+|\varepsilon|)/n=n+1$.

При фиксированном ключе $\kappa \in S_n$ остается открытым вопрос о построении на S_n биекции Ψ такой, что $\mathrm{RISE}(\sigma)=\mathrm{IVP}(\Psi(\sigma))$, $\forall \sigma \in S_n$.

Если циклическая матрица (циркулянт) $C=C(t^{1/n}, t^{2/n}, \ldots, t)$ образована вектором $(t^{1/n}, t^{2/n}, \ldots, t)$, то элементы циркулянта $\{c_{ij}\}_{i,j=1}^{n}$ имеют вид $c_{ij}=t^{\tau_{ij}/n}$, где числа $\tau_{ij} \equiv n-i+1+j \pmod n$ — наименьшие положительные вычеты. Из теоремы 1 при ключе $\kappa=\kappa(1)\ldots\kappa(n)$, где $\kappa(i)=n-i+1$, вытекает

Теорема 2. *Многочлен Эйлера $A_n(t)$ имеет следующее представление $A_n(t)=\mathrm{per}\, C(t^{1/n}, t^{2/n}, \ldots, t)$, где перманент циркулянта определяется выражением* $\mathrm{per}\, C=\sum_{\sigma \in S_n} c_{1\sigma(1)} \cdots c_{1\sigma(n)}$.

С помощью теоремы 2 находим $\sum_{\sigma \in S_n} \mathrm{sgn}\,\sigma\, t^{\mathrm{IVP}(\sigma)}=\det C$, где $\mathrm{sgn}\,\sigma$ обозначает знак перестановки $\sigma \in S_n$. Поэтому справедлива

Теорема 3. *При фиксированном ключе $\kappa \in S_n$ имеем*

$$\sum_{\sigma \in S_n} \mathrm{sgn}\,\sigma\, t^{\mathrm{IVP}(\sigma)}=\mathrm{sgn}\,\kappa \cdot (-1)^{[(n-1)/2]} \cdot t(t-1)^{n-1},$$

где $[a]$ — целая часть числа a.

Рассмотрим множество $\tilde{S}_n \subset S_n$ перестановок σ, для которых набор $\tau \equiv \sigma \oplus \kappa \pmod n$ при фиксированном ключе $\kappa \in S_n$ не содержит элемента n. Несложно заметить, что $|\tilde{S}_n|=D_n$, где D_n совпадает с числом беспорядков на группе перестановок S_n [2].

Модифицированные многочлены Эйлера $\tilde{A}_m(t)=\sum_{k=1}^{m} \tilde{A}_{m,k} t^k$ зададим следующим образом: $\tilde{A}_0(t)=0$, $\tilde{A}_1(t)=1$,

$$\tilde{A}_m(t) = mt(\tilde{A}_{m-1}(t)+\tilde{A}_{m-2}(t))+t(1-t)\tilde{A}'_{m-1}(t), m \geq 2, m \in \mathbf{N}. \quad (2)$$

Из выражения (2) находим $\tilde{A}_{n-1}(1)=D_n$, $\tilde{A}_{0,k}=0$, $\tilde{A}_{1,k}=\delta_{1,|k|}$, $k \in \mathbf{Z}$ и при $m \geq 2$, $m \in \mathbf{N}$ имеет место соотношение

$$\tilde{A}_{m,k} = k\tilde{A}_{m-1,k} + (m-k+1)\tilde{A}_{m-1,k-1} + m\tilde{A}_{m-2,k-1}. \quad (3)$$

Аналогично теореме 1 с помощью выражения (3) доказывается

Теорема 4. *Статистика* IVP *на множестве $\tilde{S}_n$: а) не зависит от выбора ключа $\kappa \in S_n$; б) является модифицированной эйлеровой статистикой, т. е. справедлива формула $\tilde{A}_{n-1}(t)=\sum_{\sigma \in \tilde{S}_n} t^{\mathrm{IVP}(\sigma)}$.*

Из теоремы 4 следует, что величины $\{\tilde{A}_{n,k}/D_{n+1}\}_{k=1}^{n}$ задают модифицированное вероятностное распределение Эйлера, также асимптотически сходящееся к нормальному с параметрами $(n/2, \sqrt{n/12})$.

Пусть циркулянт $C{=}C(0, t^{1/n}, \ldots, t^{(n-1)/n})$ образован вектором $(0, t^{1/n}, \ldots, t^{(n-1)/n})$. Тогда элементы циркулянта $\{c_{ij}\}_{i,j=1}^{n}$ задаются равенствами: $c_{ii}{=}0$, $c_{ij}{=}t^{\tau_{ij}/n}$ при $i \neq j$, где $\tau_{ij}{\equiv}n{-}i{+}j(\mathrm{mod}\ n)$ — наименьшие положительные вычеты. Аналогом теоремы 2 является

Теорема 5. *Многочлен* $\tilde{A}_{n-1}(t)$ *имеет следующее представление* $\tilde{A}_{n-1}(t){=}\mathrm{per}\, C(0, t^{1/n}, \ldots, t^{(n-1)/n})$.

Также аналогом теоремы 3 является

Теорема 6. *При фиксированном ключе* $\kappa{\in}S_n$ *справедливо равенство* $\sum_{\sigma\in\tilde{S}_n} \mathrm{sgn}\,\sigma\, t^{\mathrm{IVP}(\sigma)}{=}\mathrm{sgn}\,\kappa \cdot (-1)^{[(n-1)/2]} \cdot (t^n{-}t)(t{-}1)^{-1}$.

Мультимножество $\{1^{m_1} \ldots n^{m_n}\}$ при фиксированном n определяется вектором кратностей его элементов $(m_1, \ldots, m_n)$. Отображение RISE для перестановок $S_{(m_1,\ldots,m_n)}$ этого мультимножества задает обобщенный многочлен Эйлера $A_{(m_1,\ldots,m_n)}(t)$, с помощью которого для мультимножества обобщается и определение 1 для E-статистики.

В этом смысле RISE и IMAL, как следует из [1], являются обобщенными E-статистиками, причем $|S_{(m_1,\ldots,m_n)}|$ совпадает с полиномиальным коэффициентом из m по $(m_1, \ldots, m_n)$, где $m{=}m_1{+}\ldots{+}m_n$.

Для данного случая определим $\mathrm{IVP}(\sigma)$ (индекс вектора перестановки $\sigma{\in}S_{(m_1,\ldots,m_n)}$) при ключе $\kappa{=}\kappa(1)^{m_1} \ldots \kappa(n)^{m_n}$, где $\kappa(i){=}n{-}i$ для $1{\leq}i{\leq}n{-}1$ и $\kappa(n){=}n$, соотношением $\mathrm{IVP}(\sigma){=}|\tau|/n{+}1$, причем в векторе $\tau{\equiv}\sigma{\oplus}\kappa(\mathrm{mod}\ n)$ записываются наименьшие неотрицательные вычеты. Следует отметить, что при $m_1{=}\ldots{=}m_n{=}1$ так определенная статистика IVP при заданном ключе $\kappa{=}n{-}1 \ldots 1n$ совпадает со статистикой IVP, используемой при доказательстве теоремы 1.

Теорема 7. *Для перестановок* $S_{(m_1,\ldots,m_n)}$ *мультимножества* $\{1^{m_1} \ldots n^{m_n}\}$ *характеристика* IVP *является обобщенной статистикой Эйлера, т. е.* $A_{(m_1,\ldots,m_n)}(t){=}\sum_{\sigma\in S_{(m_1,\ldots,m_n)}} t^{\mathrm{IVP}(\sigma)}$.

Доказательство теоремы 7 проводится на базе теоремы 1 методом математической индукции по вектору кратностей $(m_1, \ldots, m_n)$, причем учитывается, что при перестановке компонент фиксированного вектора кратностей статистика IVP не изменяется.

Список литературы

1. Фоата Д. Распределения типа Эйлера и Макмагона на группе перестановок // Проблемы комбинаторного анализа. — М.: Мир, 1980. — С. 120–141.

2. Риордан Дж. Введение в комбинаторный анализ. — М: ИЛ, 1963.

О ПРОИЗВОДЯЩЕЙ ФУНКЦИИ ПРЕДСТАВЛЕНИЙ

А. Б. Верёвкин (Ульяновск)

Рассмотрим степенной ряд $m(t)=\sum_{n>0}\mu(n)t^n$, где $\mu(n)$ — функция Мёбиуса. Он определяется формальным соотношением:

$$\sum\nolimits_{k>0} m(t^k) = t.$$

Как функция, $m(t)$ определена на интервале сходимости $(-1;1)$ и имеет на нём три интервала монотонности, а также:

1) локальный минимум $-0.5893921643...$ в $-0.5629868018509...$;

2) локальный максимум $0.182233934...$ в $0.32299390999...$;

3) одну точку перегиба $0.2794874955...$;

4) три нуля: $-0.78070089865...$, 0 и $+0.5802906245....$

Используя представление $\mu(n)$ в виде суммы примитивных корней из 1 степени n, можно получить выражение:

$$m(t) = \sum\nolimits_{\xi\in C^*} \xi\cdot t^{ord(\xi)},$$

что является частным случаем выражения вида $\sum_{g\in G}\chi(g)\cdot t^{ord(g)}$, где χ — характер представления группы G. Например, для тривиального представления той же группы $G\cong C^*$ мы получим ряд:

$$\sum\nolimits_{n>0}\varphi(n)t^n,$$

где $\varphi(n)$ — функция Эйлера.

Для регулярного представления ρ_G конечной группы G получим равенство:

$$\sum\nolimits_{g\in G} Tr(\rho_G(g))\cdot t^{ord(g)} = Tr(\rho_G(e))\cdot t^{ord(e)} = |G|\cdot t.$$

Ряд $m(t)$ и первообразная $\int m(t)t^{-1}dt = \sum_{n>0} t^n\mu(n)/n$ представляют интерес тем, что часто возникают при вычислении алгебраических инвариантов. К примеру, через последнюю незамкнутым образом выражается ряд Гильберта свободной, произвольно-градуированной алгебры Ли.

Работа выполнена при финансовой поддержке РФФИ, проект 04-01-00739.

О ЧИСЛЕ ВЫПОЛНЯЮЩИХ НАБОРОВ СЛУЧАЙНОЙ k-КНФ

Ф. Ю. Воробьев (Москва)

Пусть $x_1, \ldots, x_n$ — множество из n булевых переменных. Назовем k-буквенной скобкой дизъюнкцию вида $(x_{i_1}^{\sigma_1} \vee x_{i_2}^{\sigma_2} \vee \ldots \vee x_{i_k}^{\sigma_k})$. Построим случайную k-КНФ $F_k(n, m)$ путем случайного, равновероятностного и независимого выбора m скобок из числа $(2n)^k$ всех скобок. Пусть $S_k(n, r)$ — вероятность того, что $F_k(n, nr)$ выполнима. Определим

$$r_k \equiv \sup\{r : \lim_{n\to\infty} S_k(n, r) = 1\},$$

$$r_k^* \equiv \inf\{r : \lim_{n\to\infty} S_k(n, r) = 0\}.$$

Существует предположение, что $r_k = r_k^*$, такое число r_k называется порогом выполнимости.

Существование порога не доказано, но известно следующее утверждение:

Теорема 1 [2]. *Для любого $k \geq 2$ существует такая последовательность $r_k(n)$, что для любого $\varepsilon > 0$*

$$\lim_{n\to\infty} S_k\big(n, (1-\varepsilon)r_k(n)\big) = 1,$$

$$\lim_{n\to\infty} S_k\big(n, (1+\varepsilon)r_k(n)\big) = 0.$$

Следствие 1. *Зафиксируем $k \geq 2$. Если $F_k(n, rn)$ выполнима с вероятностью $P_n > C > 0$, то $r_k > r$.*

В работе [1] удалось успешно применить метод вторых моментов для улучшения нижних оценок r_k.

Предлагаемый метод позволяет улучшить результаты [1] для k = 3, 4 и 5:

k	3	4	5
Верхняя оценка	4.51	10.23	21.33
Результат данной работы	2.82	8.09	18.91
Нижняя оценка [1]	2.68	7.91	18.79
Алгоритмическая нижняя оценка	3.52	5.54	9.63

Кроме того, улучшена оценка числа выполняющих наборов для $F_3(n, rn)$:

Теорема 2. *С высокой вероятностью ($P \to 1$ при $n \to \infty$) при $r \leq 2.77$ число выполняющих наборов у $F_3(n, rn)$ не меньше $2^{n(1-(2.77/r))}/(cn)$.*

Мы будем применять метод вторых моментов в следующем виде:

Лемма 1. *Для любой неотрицательной случайной величины X,*

$$P(X > 0) \geq \frac{M(X)^2}{M(X^2)}.$$

Итак, требуется выбрать такую случайную величину X, что из $X > 0$ следует выполнимость формулы, и к X применим метод вторых моментов. В [1] был найден целый класс случайных величин, удовлетворяющих этим свойствам.

Пусть c обозначает k-буквенную скобку, $\sigma \in \{0,1\}^n$, а $w(\sigma, c)$ — некоторая действительнозначная функция. Рассмотрим следующий класс случайных величин:

$$X = \sum_{\sigma} \prod_{c} w(\sigma, c).$$

Здесь сумма берется по всем $\sigma \in \{0,1\}^n$, а произведение — по всем скобкам случайной формулы.

Пусть для $\sigma \in \{0,1\}^n$ через $H(\sigma, F)$ обозначим разность числа букв формулы F, обращающихся в единицу на σ, и числа букв, обращающихся в ноль. Пусть $S^+ = \{\sigma \in \{0,1\}^n : H(\sigma, F) \geq 0\}$ — множество наборов, на которых не менее половины букв формулы F обращаются в единицу.

В [1] было показано, что основной вклад в $M(X^2)$ дают наборы, на которых в единицу обращается меньше половины букв формулы. Поэтому имеет смысл рассмотреть случайную величину

$$X_+ = \sum_{\sigma \in S^+} \prod_{c} w(\sigma, c).$$

При этом математическое ожидание произведения нельзя заменить на произведение математических ожиданий. Аналогичные трудности возникают при вычислении $M(X_+^2)$. Тем не менее, оказывается, что можно выбрать функцию $w(\sigma, c)$ таким образом, что к X_+ будет применим метод вторых моментов.

Теорема 3. *При $k = 3$, $r \leq 2.82$, при $k = 4$, $r \leq 8.09$, и при $k = 5$, $r \leq 18.91$ существует константа $C > 0$, такая что для любого n $M(X_+^2) < CM(X_+)^2$.*

Применяя метод вторых моментов, получим нижние оценки для r_k. Более того, по неравенству Пэли—Зигмунда

$$P(X_+ > t) \geq \frac{(M(X_+) - t)^2}{M(X^2)}.$$

Отсюда следует, что при $t = M(X_+)/(cn)$ вероятность того, что $X_+ > t$, не стремится к нулю. Согласно [3], это означает, что эта вероятность стремится к единице. Для 3-выполнимости это позволяет улучшить нижнюю оценку числа выполняющих наборов следующим образом: $M(X_+) \to 1/2M(X) = \frac{1}{2}2^n(M(w)/2^k)^m = 2^{n-km-1}$. Заметим, что число выполняющих наборов не меньше $X_+/W_{\max}$, где $W_{\max}$ — максимально возможное значение $\prod_c w(\sigma, c)$ при $\sigma \in S^+$. С высокой вероятностью $X_+ > 2^{n-km-1}/(cn)$, а, значит, с высокой вероятностью число выполняющих наборов $F_3(n, rn)$ не меньше $2^{n-km-1}/(cnW_{\max})$. Отсюда следует теорема 2.

Список литературы

1. Achlioptas D., Peres Y. The threshold for random k-SAT is $2^k \ln 2 - O(k)$ // J. Amer. math. soc. — 2004. — V. 17. — P. 947–973.

2. Friedgut E. Necessary and sufficient conditions for sharp thresholds of graph properties, and the k-SAT problem // J. Amer. math. soc. — 1999. — V. 12. — P. 1017–1054.

3. Achlioptas D., Ricci-Tersenghi F. On the solution-space geometry of random constraint satisfaction problems // Proc. 38th annual ACM symposium on theory of computing. — 2006. — P. 130–139.

К ТЕОРИИ ПЕРЕЧИСЛЕНИЯ ПЕРЕСТАНОВОК С ОГРАНИЧЕННЫМИ ПОЗИЦИЯМИ И ФИКСИРОВАННЫМ ЧИСЛОМ ЦИКЛОВ

А. М. Каменецкий (Москва)

В настоящей статье мы дадим определение матриц

$$K_{[k],t}^{[s,r]}(a_0, a_1, \ldots, a_t; z) \quad \text{и} \quad \Pi_{[k],t}^{[s,r]}(a_0, a_1, \ldots, a_t; z)$$

из [1], а также правильное определение функции $f(z, \binom{\bar{\alpha}}{\bar{\beta}})$, которая играет ключевую роль в построении всей теории, изложенной в

этой статье. На множестве упорядоченных пар $(\bar\alpha,\bar\beta)$ конечных последовательностей $\bar\alpha$ и $\bar\beta$ элементов множества A, таких, что $\bar\alpha\subseteq\bar\beta$, определим функцию $f(z,\binom{\bar\alpha}{\bar\beta})$ следующим образом. Пусть $\bar\alpha=(x_1,\dots,x_p)\in A^p$, $\bar\beta=(y_1,\dots,y_q)\in A^q$, $\{\bar\alpha\}=\{b_1^{\langle\ell_1\rangle},b_2^{\langle\ell_2\rangle},\dots,b_d^{\langle\ell_d\rangle}\}$, $A_i=\{i\in N_p|x_i=b_i\}$, $B_i=\{i\in N_q|y_i=b_i\}$. Тогда

$$f(z,\binom{\bar\alpha}{\bar\beta})=\Big(\prod_{i=1}^{d}|A_i|!\binom{|B|}{|A|}\Big)^{-1}\sum_{\substack{\varphi\in\mathrm{Inj}(\bigcup_{i=1}^{d}A_i,\bigcup_{i=1}^{d}B_i),\\ \varphi(A_i)\subseteq B_i,1\leqslant i\leqslant d}} z^{|\varphi|},\qquad(1)$$

где $|\varphi|$ — число циклов отображения φ. К сожалению, определение $f(z,\binom{\bar\alpha}{\bar\beta})$, которое было дано в [1], годится только для классического случая $k=1$. Пусть $\bar\alpha=(x_1,x_2,\dots,x_{s+kr+d})\in G^{(s,r)}_{[k],d,t}$, $\bar\alpha'=(x_1,\dots,x_s,\underbrace{0,0,\dots,0}_{k},x_{s+1},\dots,x_{s+rk+d})=(x'_1,x'_2,\dots,x'_{s+(r+1)k+d})$, $A\subseteq N_{s+(r+1)k}\setminus N_{s+rk}$, $\varphi\in\mathrm{Inj}(A,N_{s+(r+1)k+d})$. Обозначим через $\varphi(\bar\alpha'+1)$ последовательность, которая получается из последовательности $\bar\alpha'+1=(x'_1+1,\dots,x'_{s+(r+1)k+d}+1)$ следующим образом. Если $i\in A\cup\varphi(A)$, то компонента x'_i+1 вычеркивается. Если $i\to\dots\to j$, $i\in A\setminus(A\cup\varphi(A))$, $j\in\varphi(A)\setminus(A\cap\varphi(A))$, максимальная цепь инъективного отображения φ, то компонента x'_i+1 перемещается на место вычеркиваемой компоненты x'_j+1. Затем в полученной таким образом последовательности $(x''_1,\dots,x''_{s+rk+p})$ компоненты $x''_i=t+1$ заменяются на w, если $1\leqslant i\leqslant s+rk$, и компоненты $x''_i=t+1$ или w вычеркиваются, если $i>s+rk$. На множестве $\bigcup_{d=0}^{(t+1)k}G^{(s,r)}_{[k],d,t}$ определим квадратную матрицу $K^{(s,r)}_{[k],t}(a_0,\dots,a_t;z)=(a_{\bar\alpha,\bar\beta})_{\bar\alpha,\bar\beta\in\bigcup_{d=0}^{(t+1)k}G^{(s,r)}_{[k],d,t}}$ следующим образом: $K^{(0,0)}_{[k],0}(a_0;z)=\sum_{d=0}^{k}\binom{k}{d}(k-d+z)^{(d)}a_0^d$; если $t\geqslant 1$, то

$$a_{\bar\alpha,\bar\beta}=\sum_{A\subseteq N_{s+(r+1)k}\setminus N_{s+rk}}\ \sum_{\substack{\varphi\in\mathrm{Inj}(A,N_{s+(r+1)k+d}),\\ \varphi(\bar\alpha'+1)=\bar\beta',x'_{\varphi(t)}\in\{0,1,\dots,t\},i\in A}} z^{|\varphi|}\prod_{i\in A}a_{x'_{\varphi(i)}},\qquad(2),$$

где $(z)^{(k)}=\prod_{i=0}^{k-1}(z+i)$, $k\geqslant 1$, $(z)^{(0)}=1$. Из общего определения (2) особо выделяется случай $r=0$.

Пусть

$$(\bar\alpha = (x_1,\dots,x_s;1^{\langle\ell_1\rangle},2^{\langle\ell_2\rangle},\dots,t^{\langle\ell_t\rangle}),$$
$$\bar\beta = (y_1,\dots,y_s;1^{\langle q_1\rangle},\dots,t^{\langle q_t\rangle}) \in \bigcup_{d=0}^{kt} G^{(s,0)}_{[k],d,t},$$
$$B = \{i \in N_s | y_j = 1\}, \quad |B| = b.$$

Тогда в случае, когда $x_i \in N_t$ для всех $i \in B$, $\bar\beta = (y_1,\dots,y_s; 1^{\langle k-v-b+\sum_{i=1}^{t-1} p_i\rangle}, 2^{\langle \ell_1 - p_1\rangle},\dots,t^{\langle \ell_{t-1}-p_{t-1}\rangle})$, $0 \leqslant p_i \leqslant \ell_i$, $1 \leqslant i \leqslant t-1$, $\sum_{i=1}^{t-1} p_i \leqslant v \leqslant k-b$, $y_i = x_i + 1$ для всех $i \in N_s \setminus B$, полагаем

$$a_{\bar\alpha,\bar\beta} = \Big(\prod_{i\in B} a_{x_i}\Big)\binom{\ell_1}{\varphi_1}\binom{\ell_2}{\varphi_2}\dots\binom{\ell_{t-1}}{\varphi_{t-1}}\binom{k}{v-\sum_{i=1}^{t-1}p_i} a_0^{v-\sum_{i=1}^{t-1}p_i} \times$$
$$\times\, a_1^{p_1}\dots a_{t-1}^{p_{t-1}} \sum_{d=0}^{\min(\ell_t,k-v-b)} \Big(\frac{(k-v+\sum_{i=1}^{t-1}p_i)!}{(k-v-d-b)!}\times$$
$$\times\,(k-v+\sum_{i=1}^{t-1}p_i+z)^{(v-\sum_{i=1}^{t-1}p_i)}\binom{\ell_t}{d}a_t^d\Big);$$

в остальных случаях полагаем $a_{\bar\alpha,\bar\beta} = 0$.

Пусть $G^{(s,r)}_{[k],t} = \{\bar\alpha \in G^{(s,r)}_{[k],0,t} | w \neq \{\bar\alpha\}\}$. На множестве $G^{(s,r)}_{[k],t}$ определим квадратную матрицу $\Pi^{(s,r)}_{[k],t}(a_0,\dots,a_t;z) = (b_{\bar\alpha,\bar\beta})_{\bar\alpha,\bar\beta\in G^{(s,r)}_{[k],t}}$ следующим образом: $\Pi^{(0,0)}_{[k],0}(a_0,k) = (z)^{(k)}a_0^k$; если $t \geqslant 1$, $\bar\alpha = (x_1,\dots,x_{s+rk}) \in G^{(s,r)}_{[k],t}$, то

$$b_{\bar\alpha,\bar\beta} = \sum_{\substack{\varphi\in \mathrm{Inj}(N_{s+(r+1)k}\setminus N_{s+rk}, N_{s+(r+1)k}),\\ x'_{\varphi(i)}\in\{0,1,\dots,t\} \text{ для всех } i\in N_{s+(r+1)k}\setminus N_{s+rk},\\ \varphi(\bar\alpha'+1)=\bar\beta'}} z^{|\varphi|} \prod_{i\in N_{s+(r+1)k}\setminus N_{s+rk}} a_{x'_{\varphi(i)}}.$$

Пусть $\bar\alpha = (x_1,\dots,x_s)$, $\bar\beta = (y_1,\dots,y_s) \in G^{(s,0)}_{[k],t}$, $B = \{i \in N_s | y_i = 1\}$, $|B| = b$. Тогда, если $y_i = x_i + 1$, $x_i \neq t$ для всех $i \in N_s \setminus B$, то полагаем

$$b_{\bar\alpha,\bar\beta} = b!\binom{k}{b}(b+z)^{(k-b)}a_0^{k-b}\prod_{i\in B} a_{x_i};$$

в остальных случаях полагаем $b_{\bar{\alpha},\bar{\beta}} = 0$.

Если $\bar{\alpha}, \bar{\beta} \in \bigcup_{d=0}^{(t+r)k} G^{(s,r)}_{[k],d,t}$, то, по определению,

$$\left(K^{[s,r]}_{[k],t}(a_0,\dots,a_t;z)\right)[L([\bar{\alpha}])|L([\bar{\beta}])] = \\ = \sum_{\bar{\gamma}\sim\bar{\beta}} (K^{(s,r)}_{[k],t}(a_0,\dots,a_t;z))[L(\bar{\alpha})|L(\bar{\gamma})].$$

В теоремах 1 и 4 из [1] следует писать $\bar{\gamma}$ вместо $\gamma(s+kr)$, а в теореме 5 из [1] необходимо положить $\bar{\beta} = (1^{\langle k\rangle},\dots,r^{\langle k\rangle})$.

Список литературы

1. Каменецкий А. М. Рациональность производящих функций цикловых ладейных полиномов и цикловых перманентов кронекеровых произведений тёплицевых матриц и циркулянтов с матрицей J_k // Материалы VIII Международного семинара «Дискретная математика и ее приложения» (2–6 февраля 2004 г.). — М.: Изд-во механико-математического ф-та МГУ, 2004. — С. 191–197.

СУММАЦИОННЫЕ УРАВНЕНИЯ И ИХ ПРИМЕНЕНИЯ В ПЕРЕЧИСЛИТЕЛЬНОЙ КОМБИНАТОРИКЕ

Л. М. Коганов (Москва)

Суммационные (сокращенно Σ-) уравнения определяют последовательности неявно, точно так же как интегральные уравнения неявно определяют функции непрерывных переменных.

Рассматриваются перечислительные задачи, естественным путём приводящие не к разностным (сокращённо Δ-), а к Σ-уравнениям [1, гл. II, IV; 2], и решения этих уравнений.

Универсальным источником формирования различных Σ-уравнений является фундаментальный метод вложения В. А. Лисковца [3].

Можно проиллюстрировать сказанное следующим примером.

Пусть общий член перечисляющей последовательности $\{v_p(k)\}_{p\geq 1}$ есть число циклически несократимых слов (т. е. таких, в которых не сокращаются рядом стоящие и концевые символы) фиксированной длины p в симметричном алфавите $\mathcal{A} = \{a_1, a_1^{-1}, ..., a_k, a_k^{-1}\}$ свободной группы ранга k, где $a_1, ..., a_k$ суть все без исключения образующие.

Теорема. *Для последовательности* $\{v_p(k)\}_{p\geq 1}$ *имеет место система из двух* Σ*-уравнений* (1)–(1′) *вида:*

$$\sum_p v_p(k)[(2k-2)(2k-1)^{q-1}] + v_n(k) = 2k(2k-1)^{n-1}; \qquad (1),\ (1')$$

где n *— соответственно нечётное или чётное натуральное.*

В сумме (1) *при при нечётных* n *переменный индекс суммирования* p *принимает, начиная с* $p = 1$*, все последовательные нечётные значения. В соотношении* (1′) *при чётных* n *индекс суммирования* p *принимает все последовательные чётные значения, начиная с* $p = 2$*. В обоих случаях верхний предел суммирования в зависимости от* n *один и тот же, а именно* $p = n-2$*, при этом дополнительный индекс* q *определяется общим условием* $p + 2q = n$*, т. е.* $q = \frac{n-p}{2}$*, откуда* $q \geq 1$*.*

Ясно, что циклически несократимое слово (ц.н.с.) есть специальный с дополнительными ограничениями случай несократимого слова (н.с.) и может вкладываться по Лисковцу в систему всевозможных n-буквенных н.с. либо операцией синхронного префиксно-суффиксного окаймления, либо целиком без окаймления (см. последние выделенные слева слагаемые в (1)–(1′)).

Согласованное окаймление $t...ax...za^{-1}...t^{-1}$ исходного ц.н.с. $x...z$ достигается с помощью любых *взаимно обратных* н.с. $t...a$ и $a^{-1}...t^{-1}$. При этом, разумеется, должна выполняться система условий $a \neq x^{-1}$; $a \neq z$.

Поскольку для ц.н.с. $x...z$ имеем $x^{-1} \neq z$, то при добавке a слева от x и "зеркальной" добавке a^{-1} справа от z вышеуказанная система условий исключает 2 различных элемента из алфавита $\mathcal{A}$, а сам выбор добавки буквы a осуществим $2k-2$ способами ($k > 1$). Остальные $q-1$ элементов-символов префикса и зеркально однозначно ими определяемые символы суффикса (как соответствующие обратные) могут после добавки a быть последовательно доставляемы (в префиксе от a справа налево, в суффиксе от a^{-1} далее слева направо) $2k-1$ способом каждый последующий.

Положим для удобства выкладок $2k - 1 = \alpha$. При этом решение (1) и (1′) осуществляется порознь введением соответствующих производящих функций.

Строятся раздельные энумераторы правых частей (1) и (1′):

$$U_{odd} = 2kx \sum_{n=1,3,5...} [(2k-1)x]^{n-1} = (\alpha+1)x\frac{1}{1-\alpha^2x^2}; \qquad (2)$$

$$U_{even} = \sum_{n=2,4,6\ldots} 2k(2k-1)^{n-1}x^n = \frac{(\alpha+1)\alpha x^2}{1-\alpha^2 x^2}, \qquad (2')$$

где, для определённости, предполагается, что $|\alpha x| < 1$.

Для левых частей (1)–(1′) также раздельно по чётности индексов строятся энумераторы:

$$V_{odd/even} = \sum_n v_n(k)x^n. \qquad (3),\ (3')$$

В (3) переменный индекс n пробегает значения $1, 3, 5, \ldots$, соответственно, в (3′) — значения $2, 4, 6\ldots$.

Наконец, полагая с учётом сделанных замечаний:

$$Q = 1 + \sum_{q\geq 1}[(2k-2)(2k-1)^{q-1}]x^{2q} = \frac{1-x^2}{1-\alpha x^2},$$

систему (1)–(1′) можно переписать в "операционной" форме в виде

$$V_{odd/even} = \frac{U_{odd/even}}{Q}. \qquad (4),\ (4')$$

Используя домножение на геометрический ряд, и (или) разложение на элементарные дроби из (4) и, соответственно, из (4′) имеем:

$$v_{2m+1}(k) = Coef_{x^{2m+1}} \frac{U_{odd}}{Q} = (\alpha+1)\, Coef_{x^{2m}} \frac{1-\alpha x^2}{1-\alpha^2 x^2} \cdot \frac{1}{1-x^2} =$$

$$= (\alpha+1)\, Coef_{y^m} \frac{1-\alpha y}{1-\alpha^2 y} \cdot \frac{1}{1-y} = \alpha^{2m+1} + 1; \qquad (5)$$

$$v_{2m}(k) = Coef_{x^{2m}} \frac{U_{even}}{Q} = (\alpha+1)\alpha\, Coef_{y^m} \frac{y}{1-\alpha^2 y} \cdot \frac{1-\alpha y}{1-y} =$$

$$= \alpha \left[(\alpha+1)\, Coef_{y^{m-1}} \frac{1-\alpha}{1-\alpha^2 y} \cdot \frac{1}{1-y}\right] = \alpha^{2m} + \alpha. \qquad (5')$$

Соотношения (5)–(5′) были независимо получены спектральными методами линейной алгебры в [4, 5], где в явном виде разрешалось предварительно построенное Δ-уравнение: $v_n - v_{n-2} = (\alpha^2-1)\alpha^{n-2}$; $n \geq 3$; $v_1 = \alpha + 1$; $v_2 = \alpha^2 + \alpha$, определяющее искомую перечисляющую последовательность с общим членом $v_n = v_n(k)$.

Список литературы

1. Коганов Л. М. Псевдопорождаемые двухиндексные последовательности. — М.: Недра, 1989.

2. Коганов Л. М. Новое доказательство одной теоремы М. А. Алексеева // Сборник научных трудов математического факультета МГПУ. —М.: Изд-во Мос. гор. пед. ун-та, 2005. — С. 207–211.

3. Лисковец В. А. Об одном рекуррентном методе подсчёта графов с отмеченными вершинами //Докл. АН СССР. — 1969. — Т. 184, № 6. — С. 1284–1287.

4. Rivin I. Growth in free groups (and other stories) // arXiv.math. CO/9911076. — 7 Dec. 1999. — V. 2. — P. 1–31.

5. Коганов Л. М. Число циклически несократимых слов в алфавите свободной группы // Проблемы теоретической кибернетики. Тезисы докладов XIII Международной конференции (Казань, 27–31 мая 2002 г.). Часть I. — М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2002. — С. 85.

О ЧИСЛЕ ПЕРВИЧНЫХ ПЕРИОДИЧНОСТЕЙ

Р. М. Колпаков (Москва)

Пусть $w = a_1 \dots a_n$ — конечное слово. Через $w[i...j]$ обозначается подслово $a_i \dots a_j$ слова w. Два подслова $w[i'...j']$, $w[i''...j'']$ слова w, где $i' \le i''$, называются *смежными*, если $j' \ge i'' - 1$. Натуральное число p является периодом слова w, если $a_i = a_{i+p}$ для любого $i = 1, \dots, n-p$. Мы обозначаем через $p(w)$ минимальный период слова w и через $e(w)$ — отношение $|w|/(p(w))$.

Периодичностью в слове w называется любое подслово r такое, что $e(r) \ge 2$. Периодичность $r = w[i...j]$ в слове w называется *максимальной*, если выполняются два условия:

1) $a_{i-1} \ne a_{i-1+p(r)}$ при $i > 1$;

2) $a_{j+1-p(r)} \ne a_{j+1}$ при $j < n$.

Две периодичности r_1 и r_2 с одинаковым минимальным периодом p называются *однокоренными*, если для достаточно большого k эти периодичности являются подсловами одного и того же слова

$$\underbrace{uu \dots u}_{k},$$

где слово u имеет длину p.

Пусть $r' = w[i'...j']$, $r'' = w[i''...j'']$, где $i' < i''$, — две смежных однокоренных максимальных периодичности с минимальным периодом p в слове w. Мы говорим, что максимальная периодичность $r = w[i...j]$ *порождается* парой периодичностей r', r'', если $p(r) \geq p$, $i' + p \leq i < i''$ и $j' < j \leq j'' - p$. Если максимальная периодичность порождается некоторой парой периодичностей, то она называется также *вторичной* периодичностью. В противном случае данная периодичность называется *первичной* периодичностью. Некоторые свойства как первичных, так и вторичных периодичностей установлены в [1]. Обозначим через $R_p(n)$ максимальное число первичных периодичностей с минимальным периодом, не меньшим, чем p, в слове длины n. Тогда справедлива следующая

Теорема. $R_p(n) = \Theta(n/p)$.

Работа выполнена при финансовой поддержке Совета по грантам Президента РФ (грант НШ–5400.2006.1) и Российского фонда фундаментальных исследований (проект 05–01–00994).

Список литературы

1. Gasieniec L., Kolpakov R. M., Potapov I. Space efficient search for maximal repetitions // Theoretical Computer Science. — 2005. — V. 339. — P. 35–48.

О СЛОЖНОСТИ НАИХУДШЕГО СЛУЧАЯ В МЕТОДЕ ВЕТВЕЙ И ГРАНИЦ ДЛЯ ЗАДАЧИ ОБ ОДНОМЕРНОМ БУЛЕВОМ РАНЦЕ

Р. М. Колпаков, М. А. Посыпкин (Москва)

Задача о ранце формулируется следующим образом. Даны n предметов. Предмет i характеризуется весом w_i и ценой p_i. Требуется положить в ранец грузоподъемностью C набор предметов максимальной стоимости. Данное неформальное описание может быть математически записано следующим образом:

$$f(\overline{x}) = \sum_{i=1}^{n} p_i x_i \to \max; \quad \sum_{i=1}^{n} w_i x_i \leq C; x_i \in \{0, 1\}. \qquad (1)$$

Одним из основных методов решения данной задачи является метод ветвей и границ [1]. Этот метод заключается в последовательной

декомпозиции исходной задачи на две подзадачи, с отсевом подзадач, решение которых заведомо не приведет к нахождению оптимума исходной задачи. Отсев позволяет существенно сократить объем перебора.

Идея отсева заключается в том, что решается так называемая *оценочная задача*, которая позволяет получить верхнюю оценку для решения рассматриваемой подзадачи. Если оценочная задача не имеет решения или найденная оценка не превосходит наилучшее из найденных на данный момент значений целевой функции f, то подзадача исключается из дальнейшего рассмотрения.

В качестве оценочной часто выбирают линейную релаксацию задачи, которая получается заменой дискретных ограничений линейными:

$$\sum_{i=1}^{n} p_i x_i \to \max; \quad \sum_{i=1}^{n} w_i x_i \le C; 0 \le x_i \le 1.$$

Задача релаксации решается за линейное относительно числа переменных количество операций методом Данцига [1]. Известно, что ее решение достигается на наборе значений переменных $x_1, \ldots, x_n$, содержащем не более одного дробного (не целого) значения (переменную, принимающую это значение, будем называть *дробной* переменной).

Процесс решения задачи методом ветвей и границ можно представить в виде *дерева ветвления*, вершинам которого соответствуют создаваемые подзадачи. В качестве меры сложности можно взять число концевых вершин.

Следует отметить, что выбор очередной подзадачи для ветвления и декомпозиция могут осуществляться различными способами. Декомпозиция состоит в разбиении исходной задачи на две путем присваивания одной из переменных значений 0 и 1 и называется *ветвлением* задачи по переменной. Наиболее распространенными способами выбора переменной для ветвления являются выбор первой переменной в соответствии с некоторым порядком или выбор дробной переменной в задаче релаксации.

Важной характеристикой МВГ является *сложность наихудшего случая*, которая определяется как максимальная сложность решения задачи с числом переменных n. В работе [3] приводится пример следующей задачи:

$$f(\overline{x}) = \sum_{i=1}^{n} 2x_i \to \max; \quad \sum_{i=1}^{n} 2x_i \le 2\lfloor \frac{n}{2} \rfloor + 1; x_i \in \{0, 1\},$$

и показывается, что сложность решения этой задачи методом ветвей и границ при любом способе выбора переменной для ветвления составляет $\binom{n+1}{\lfloor \frac{n}{2} \rfloor + 1}$. В работе [4] показано, что если для ветвления выбирается переменная с наибольшим весом, то сложность решения задачи о ранце с n переменными не превосходит $\binom{n+1}{\lfloor \frac{n}{2} \rfloor + 1}$. В известных авторам работах не содержится ответа на вопрос, какова сложность наихудшего случая для вариантов МВГ, отличных от рассмотренного в [4]. Частичный ответ на этот вопрос предлагается в данной статье.

Теорема 1 является обобщением результата работы [3] — в ней сформулирована верхняя оценка сложности любого варианта МВГ для задач с ограничением на весовые коэффициенты.

Теорема 1. *Сложность решения задачи* (1), *коэффициенты которой подчиняются условию* $\lceil \frac{\max_{i=1}^{n} w_i}{\min_{i=1}^{n} w_i} \rceil = k$, *не превосходит* $k \cdot \binom{n+1}{\lfloor \frac{n}{2} \rfloor + 1}$.

Более точная оценка получена в теореме 2 для случая ветвления по дробной переменной.

Теорема 2. *Пусть* $P(T, m, k)$ — *семейство задач* $P(T, m, k)$ *о ранце, где* k — *целое число,* m — *целое неотрицательное число, а* $T = \{t_1, \ldots, t_n\}$ — *упорядоченное множество натуральных чисел длины* n. *Задача* $P(T, m, k)$ *имеет следующий вид:*

$$\sum_{i=1}^{m+n} w_i x_i \to \max; \sum_{i=1}^{m+n} w_i x_i \le ka + 1, \text{где } a \in \mathbb{N}, a \ge 2,$$

$$w_i = \begin{cases} a, & \text{если } 1 \le i \le m; \\ t_{n+m+1-i} \cdot a, & \text{если } m < i \le m + n. \end{cases}$$

Тогда для любого набора натуральных чисел $T = \{t_1, \ldots, t_n\}$ *справедливо соотношение для сложности* $S(T, m, k)$ *решения задачи* $P(T, m, k)$

$$\lim_{m \to \infty} \frac{\max_{k \in \mathbb{Z}} S(T, m, k)}{\binom{m+n}{\lfloor \frac{m}{2} \rfloor}} = 2 + \sum_{i=1}^{n} \left(\frac{1}{2^i} - \frac{1}{2^{i+t_i-1}} \right).$$

Из данного соотношения вытекает, что в асимптотике сложность решения задачи $P(T, m, k)$ методом ветвей и границ при ветвлении по дробной переменной не превосходит $\frac{3}{2}\binom{n+m+1}{\lfloor \frac{n+m+1}{2} \rfloor}$, но может

быть сколь угодно близкой к этому числу. Таким образом, для рассмотренного варианта метода ветвей и границ существуют задачи $P(T, m, k)$, сложность решения которых превосходит асимптотически в $\frac{3}{2} - \epsilon$ раза сложность решения задачи, рассмотренной в [3].

Работа выполнена при поддержке РФФИ, проекты 05-01-00495, 06-07-89079.

Список литературы

1. Сигал И. Х., Иванова А. П. Введение в прикладное дискретное программирование. — М.: Физматлит, 2002.

2. Гришухин В. П. Эффективность метода ветвей и границ в задачах с булевыми переменными // Исследования по дискретной оптимизации. — 1976. — С. 203–230.

3. Финкельштейн Ю. Ю. Приближенные методы и прикладные задачи дискретного программирования. — М.: Наука, 1976.

4. Колпаков Р. М., Посыпкин М. А., Сигал И. Х. О сложности решения задачи о булевом ранце // Дискретные модели в теории управляющих систем: VII Международная конференция. — М.: МАКС Пресс, 2006.

ОБОБЩЕННЫЕ ПИРАМИДЫ ПАСКАЛЯ И ИМ ОБРАТНЫЕ

О. В. Кузьмин, А. А. Балагура (Иркутск)

В [1] рассматривались обращения линейных соотношений, содержащих в качестве коэффициентов комбинаторные числа, описываемые обобщенным треугольником Паскаля. В настоящей работе построены некоторые обращения линейных соотношений, в которых участвуют комбинаторные объекты, описываемые обобщенной пирамидой Паскаля [2].

Обобщенной пирамидой Паскаля называется трехгранный пирамидальный массив, элементы которого удовлетворяют рекуррентным соотношениям:

$$V(n,k,l) = \alpha_{n,k-1,l}V(n-1,k-1,l) + \beta_{n,k,l-1}V(n-1,k,l-1)+$$

$$+\gamma_{n,k,l}V(n-1,k,l) \qquad (1)$$

с граничными условиями $V(0,0,0) = V_0$; $V(n,k,l) = 0$, если $\min(n,k,l,n-k-l) < 0$.

Следуя [2], рассмотрим важные частные случаи обобщенной пирамиды Паскаля — A- и B-пирамиды, в каждом сечении которых расположены обобщенные триномиальные коэффициенты второго и первого рода соответственно.

Пусть $\alpha \sim \{\alpha_s\}_0^\infty$, $\beta \sim \{\beta_s\}_0^\infty$, $\gamma \sim \{\gamma_s\}_0^\infty$ — последовательности, которые назовем базовыми последовательностями или *базами*.

Используя члены баз α, β, γ, строим следующие разложения:

$$\sum_{k=0}^{n}\sum_{l=0}^{n-k} B_{k,l}^n \cdot x^k \cdot y^l = \prod_{i=0}^{n-1}(\alpha_i x + \beta_i y + \gamma_i), n \geq 1, \tag{2}$$

$$\sum_{l=0}^{\infty}\sum_{n=k+l}^{\infty} A_{k,l}^n \cdot y^l \cdot z^n = z^k \prod_{j=0}^{k-1}\alpha_j \prod_{i=0}^{k}(1-\beta_i yz - \gamma_i z)^{-1}, k \geq 0. \tag{3}$$

Числа $B_{k,l}^n$ и $A_{k,l}^n$ в левых частях выражений (2) и (3), которые называют *обобщенными триномиальными коэффициентами* первого и второго рода соответственно, можно задать рекуррентными соотношениями:

$$B_{k,l}^n = \alpha_{n-1}B_{k-1,l}^{n-1} + \beta_{n-1}B_{k,l-1}^{n-1} + \gamma_{n-1}B_{k,l}^{n-1},$$

$$A_{k,l}^n = \alpha_{k-1}A_{k-1,l}^{n-1} + \beta_k A_{k,l-1}^{n-1} + \gamma_k A_{k,l}^{n-1},$$

$n \geq 1$, $0 \leq k \leq n$, $0 \leq l \leq n-k$, с начальными условиями $B_{0,0}^0 = A_{0,0}^0 = 1$; $B_{k,l}^n = A_{k,l}^n = 0$, если $\min(n, l, k, n-k-l) < 0$. Эти формулы также могут быть получены из (1).

Парой обратимых соотношений [1] называют систему линейных соотношений:

$$F_n = \sum_k a_{nk} \cdot f_k, \ n \geq 0,$$

$$f_n = \sum_k b_{nk} \cdot F_k, \ n \geq 0$$

между членами последовательностей $\{F_n\}_{n=0}^\infty$ и $\{f_n\}_{n=0}^\infty$, если матрицы коэффициентов $\|a_{nk}\|$ и $\|b_{nk}\|$ — двусторонние взаимо-обратные.

Обозначим $C_\alpha = C_n(\alpha) = \prod_{i=0}^{n-1}\alpha_i$, аналогично определяются C_β и C_γ. Положим $\frac{\alpha}{\beta} \sim \{\frac{\alpha_s}{\beta_s}\}_{s=0}^\infty$. Базы $\frac{\gamma}{\beta}$, $\frac{\beta}{\alpha}$, $\frac{\gamma}{\alpha}$, $\frac{\alpha}{\gamma}$, $\frac{\beta}{\gamma}$ определяются аналогично.

Пусть $\tilde{A}^r_{i,j}$ строятся на базах α, $\frac{\beta}{\alpha}$, $\frac{\gamma}{\alpha}$; $\hat{A}^r_{i,j}$ — на базах β, $\frac{\alpha}{\beta}$, $\frac{\gamma}{\beta}$; $\bar{A}^r_{i,j}$ — на базах γ, $\frac{\beta}{\gamma}$, $\frac{\alpha}{\gamma}$.

Верны следующие теоремы.

Теорема 1. *Система линейных выражений*

$$\psi_n = \frac{1}{C_\alpha} \sum_{k=0}^{n} \sum_{l=0}^{n-k} B^n_{k,l} \cdot \varphi_k,\ n \geq 0, \tag{4}$$

$$\varphi_n = \frac{1}{C_\alpha} \sum_{k=0}^{n} \sum_{l=0}^{n-k} (-1)^{n-k} \cdot \tilde{A}^n_{k,l} \cdot \psi_k,\ n \geq 0 \tag{5}$$

образует пару обратимых соотношений.

Теорема 2. *Система линейных выражений*

$$\phi_n = \frac{1}{C_\beta} \sum_{l=0}^{n} \sum_{k=0}^{n-l} B^n_{k,l} \cdot \chi_l,\ n \geq 0, \tag{6}$$

$$\chi_n = \frac{1}{C_\beta} \sum_{l=0}^{n} \sum_{k=0}^{n-l} (-1)^{n-l} \cdot \hat{A}^n_{l,k} \cdot \phi_l,\ n \geq 0 \tag{7}$$

образует пару обратимых соотношений.

Теорема 3. *Система линейных выражений*

$$\xi_n = \frac{1}{C_\gamma} \sum_{m=0}^{n} \sum_{k=0}^{m} B^n_{k,m-k} \cdot \zeta_{n-m},\ n \geq 0, \tag{8}$$

$$\zeta_n = \frac{1}{C_\gamma} \sum_{m=0}^{n} \sum_{k=0}^{m} (-1)^m \cdot \bar{A}^n_{n-m,m-k} \cdot \xi_{n-m},\ n \geq 0 \tag{9}$$

образует пару обратимых соотношений.

В условиях теорем 1–3 при абсолютной сходимости рассматриваемых рядов систем верны союзные пары [1] обратимых соотношений.

Заданием в формулах (4)–(9) членов баз соответствующим образом, получены формулы для обобщенных триномиальных коэффициентов, трехмерных обобщений чисел Стирлинга первого и второго рода, трехмерных обобщений чисел Уитни первого и второго рода, формулы связи обобщенных триномиальных коэффициентов и обобщенных чисел Стирлинга.

Пусть $A_n = \{\frac{\beta_0+\gamma_0}{\alpha_0}, ..., \frac{\beta_{n-1}+\gamma_{n-1}}{\alpha_{n-1}}\}$ — конечное множество, элементы которого — вещественные числа. Рассмотрим множество G_n всех возможных произведений различных элементов множества A_n. На множестве G_n вводим частичную упорядоченность, считая, что $x \leq y$ в G_n, если произведение y содержит каждый из сомножителей входящих в произведение x. С применением теоремы обращения Мебиуса на G_n, получен аналог теоремы 1. Заданием множеств $A_n = \{\frac{\alpha_0+\gamma_0}{\beta_0}, ..., \frac{\alpha_{n-1}+\gamma_{n-1}}{\beta_{n-1}}\}$ и $A_n = \{\frac{\alpha_0+\beta_0}{\gamma_0}, ..., \frac{\alpha_{n-1}+\beta_{n-1}}{\gamma_{n-1}}\}$, получены аналоги теорем 2 и 3.

Для построения примеров к полученным теоремам была разработана программа, реализующая рекурсивный алгоритм построения комбинаторных объектов, описываемых обобщенной пирамидой Паскаля.

Список литературы

1. Платонов М. Л. Комбинаторные числа класса отображений и их приложения. — М.: Наука, 1979.

2. Кузьмин О. В. Обобщенные пирамиды Паскаля и их приложения. — Новосибирск: Наука (Сибирская издательская фирма РАН), 2000.

АЛГОРИТМЫ ПРЕОБРАЗОВАНИЯ ОБОБЩЕННЫХ ЧИСЕЛ СТИРЛИНГА В ОБОБЩЕННЫЕ ТРИНОМИАЛЬНЫЕ КОЭФФИЦИЕНТЫ

О. В. Кузьмин, Т. А. Логинов (Иркутск)

Комбинаторные задачи алгоритмического характера на дискретных математических структурах встречаются на практике постоянно. Можно выделить два класса прикладных задач: создание программ с преобладанием вычислений комбинаторного характера и алгоритмов, осуществляющих конструктивное перечисление объектов заданного класса. В последнем случае используется либо исчерпывающий последовательный перебор, либо некоторые его модификации, позволяющие ограничить объем перебора. В [1] предложен метод, состоящий в нахождении и использовании изоморфного преобразования элементов известного множества комбинаторных объектов в элементы искомого множества.

Из членов базы $\{\mu_i\}_{i=0}^{\infty}$ строим следующие разложения:

$$\prod_{i=0}^{n-1}(x+\mu_i)=\sum_{k=0}^{n}B_k^n x^k, n\geq 1,$$

$$x^k\prod_{i=0}^{k}(1-\mu_i x)^{-1}=\sum_{n=k}^{\infty}A_k^n x^n, k\geq 1,$$

которые определяют обобщенные числа Стирлинга первого и второго рода соответственно.

Аналогично из членов баз $\{\alpha_i\}_{i=0}^{\infty}$, $\{\beta_i\}_{i=0}^{\infty}$ и $\{\gamma_i\}_{i=0}^{\infty}$ строим разложения:

$$\prod_{i-0}^{n-1}(\alpha_i x+\beta_i y+\gamma_i)=\sum_{k=0}^{n}\sum_{l=0}^{n-k}B_{k,l}^n x^k y^l, n\geq 1,$$

$$z^k\prod_{j=0}^{k-1}\alpha_j\prod_{i=0}^{k}(1-\beta_i yz-\gamma_i z)^{-1}=\sum_{l=0}^{\infty}\sum_{n=k+l}^{\infty}A_{k,l}^n y^l z^n, k\geq 0,$$

которые определяют обобщенные триномиальные коэффициенты первого и второго рода.

В данной статье рассмотрен ряд задач алгоритмического характера на конечных математических структурах: построение детерминированных алгоритмов преобразования обобщенных чисел Стирлинга первого рода B_k^n в обобщенные триномиальные коэффициенты первого рода $B_{k,l}^n$, обобщенных чисел Стирлинга второго рода A_k^n в обобщенные триномиальные коэффициенты второго рода $A_{k,l}^n$.

Для решения этих задач были получены новые взаимосвязи между рассматриваемыми классами симметрических функций. Построены комбинаторные алгоритмы преобразований элементарных симметрических B_k^n и полных симметрических функций A_k^n в обобщенные триномиальные коэффициенты, соответственно.

Рассмотрим задачу построения обобщенных триномиальных коэффициентов первого рода на основе обобщенных чисел Стирлинга первого рода.

Пусть $I=\{0,1,\ldots,n-1\}$ — множество индексов, $\overline{T}_n$ — множество векторов $t=(t_0,t_1,\ldots,t_{n-1})$, координатами которых могут быть члены баз $\{\alpha_i\}_0^{n-1}$, $\{\beta_i\}_0^{n-1}$ или $\{\gamma_i\}_0^{n-1}$. Если $t_i=\alpha_i$, то считаем $i\in I_\alpha$.

Пусть Θ_α — преобразование на множестве $\overline{T}_n$, которое заменяет на α_i все координаты t_i, если $i \in I_\alpha$.

Пусть $\omega = \Theta_\gamma \circ \Theta_\alpha \circ \Theta_\beta$, где преобразования действуют последовательно и каждое последующее действует на вектор t с перенумерованной базой индексов: Θ_γ на I, Θ_α на $I \backslash I_\gamma$, Θ_β на $I \backslash I_\gamma \backslash I_\alpha$.

Перенумерование при текущем преобразовании производится следующим образом: из начальной базы индексов убираются индексы, вошедшие в предыдущие базы, затем всем индексам присваиваются вспомогательные номера, которые рассматриваются как индексы при текущем преобразовании, но при записи результата берутся оригинальные индексы, соответствующие вспомогательным номерам.

Теорема 1. *Пусть B^n_{k+l} построены из элементов базы $\gamma_{\overline{n}}$, $\bar{B}^{k+l}_l$ — из $\alpha_{\overline{n}}$, $\tilde{B}^l_0$ — из $\beta_{\overline{n}}$. Тогда*

$$\omega(B^n_{k+l} \cdot \bar{B}^{k+1}_l \cdot \tilde{B}^l_0) = B^n_{k,l}, n \geq 1, 0 \leq k \leq n-1,$$

где $B^n_{k,l}$ построены из элементов баз $\alpha_{\overline{n}}$, $\beta_{\overline{n}}$ и $\gamma_{\overline{n}}$.

На основании теоремы 1 построен алгоритм полиномиальной трудоемкости преобразования произведения $B^n_k \cdot \bar{B}^{k+l}_l \cdot \tilde{B}^l_0$ в $B^n_{k,l}$.

Рассмотрим задачу построения обобщенных триномиальных коэффициентов второго рода на основе обобщенных чисел Стирлинга второго рода.

Пусть оператор φ действует на произведение $A^n_{k+l} \cdot \bar{A}^{k+l}_l \cdot \tilde{A^n_k}$ на множестве $\overline{T}_n$ следующим образом: 1) сначала производится перемножение $\bar{A}^{k+l}_l$ и $\tilde{A}^l_0$; 2) в получившемся произведении индексы сомножителей $\bar{A}^{k+l}_l$ заменяются на ноль, при этом индексы сомножителей $\tilde{A}^l_0$ равномерно увеличиваются на сумму индексов $\bar{A}^{k+l}_l$; 3) сомножители $\bar{A}^{k+l}_l$ выносятся за скобки; 4) Производится перемножение измененного $\tilde{A}^l_0$ на A^n_k; 5) в получившемся произведении индексы сомножителей базы A^n_{k+l} понижаются на единицу, если они умножены на сомножитель базы $\tilde{A^l_0}$ с меньшим индексом.

Теорема 2. *Пусть A^n_{k+l} построены из элементов базы $\gamma_{\overline{n}}$, $\bar{A}^{k+l}_l$ — из $\alpha_{\overline{n}}$, $\tilde{A}^l_0$ — из $\beta_{\overline{n}}$. Тогда*

$$\varphi(A^n_{k+l} \cdot \bar{A}^{k+1}_l \cdot \tilde{A}^l_0) = A^n_{k,l}, n \geq 1, 0 \leq k \leq n-1,$$

где $A^n_{k,l}$ построены из элементов баз $\alpha_{\overline{n}}$, $\beta_{\overline{n}}$ и $\gamma_{\overline{n}}$.

На основании теоремы 2 построен алгоритм полиномиальной трудоемкости преобразования произведения $A^n_{k+l} \cdot \bar{A}^{k+l}_l \cdot \tilde{A^n_k}$ в $A^n_{k,l}$.

Рассмотрим задачу построения $B^n_{k,l}$ непосредственно из B^n_k.

Пусть $R^x_y = \sum\limits_{i\geq 0} x_i t_i y_i^{t_i-1}$, где t_i — показатель кратности y_i в преобразуемом полиноме.

Теорема 3. *Если B^n_k построены на базе $\gamma+\beta$, а $B^n_{k,l}$ на базах α, β и γ, то:*

$$B^n_{k,l} = (l!)^{-1} \prod_{i=0}^{k} \alpha_i (R^\beta_\gamma)^l B^n_k.$$

На основании теоремы 3 построен алгоритм полиномиальной трудоемкости преобразования B^n_k в $B^n_{k,l}$.

Рассмотрим задачу построения $A^n_{k,l}$ непосредственно из A^n_k.

Теорема 4. *Если A^n_k построены на базе $\gamma+\beta$, а $A^n_{k,l}$ на базах α, β и γ, то:*

$$A^n_{k,l} = (l!)^{-1} \prod_{i=0}^{k} \alpha_i (R^\beta_\gamma)^l A^n_k.$$

На основании теоремы 4 построен алгоритм полиномиальной трудоемкости преобразования A^n_k в $A^n_{k,l}$.

Список литературы

1. Кузьмин О. В. Обобщенные пирамиды Паскаля и их приложения. — Новосибирск: Наука, 2000.

НАСЛЕДСТВЕННЫЕ СИСТЕМЫ И РЕШЕТКИ

О. Г. Кукина, В. П. Ильев (Омск)

Пусть V — непустое конечное множество, $\mathcal{A}$ — непустое семейство его подмножеств. Пара $(V, \mathcal{A})$ называется *системой независимости*, или *наследственной системой*, если семейство $\mathcal{A}$ удовлетворяет следующей *аксиоме наследственности*:

$(A1)$ $A \in \mathcal{A}, A_1 \subseteq A \Rightarrow A_1 \in \mathcal{A}$.

Множества семейства $\mathcal{A}$ называются *независимыми*. Наследственная система $(V, \mathcal{A})$ называется *матроидом*, если семейство $\mathcal{A}$ удовлетворяет следующей аксиоме:

$(A2)$ $A, A_1 \in \mathcal{A}, |A_1| = |A| + 1 \Rightarrow \exists a \in A_1 \setminus A : A \cup a \in \mathcal{A}$.

В данной работе исследуются комбинаторные свойства наследственных систем. Дано определение наследственной системы, аналогичное определению матроида в терминах оператора замыкания. Доказано, что семейство замкнутых множеств наследственной системы образует полную решетку. Получено описание решеток замкнутых множеств наследственных систем графов.

Дадим эквивалентное определение наследственной системы, аналогичное определению матроида в терминах оператора замыкания.

Пусть V — непустое конечное множество. Отображение $X \xrightarrow{\varphi} \overline{X}$ множества 2^V в себя называется *оператором замыкания*, если для всех $X, Y \subseteq V$ выполняются следующие условия:

(φ1) $X \subseteq \overline{X}$, (φ2) $X \subseteq Y \Rightarrow \overline{X} \subseteq \overline{Y}$, ($\varphi$3) $\overline{\overline{X}} = \overline{X}$.

Хорошо известно [1], что приведенное во введении определение матроида в терминах независимых множеств эквивалентно следующему.

Пара (V, φ) называется *матроидом* на V, если для всех $X \subseteq V$ и для всех $p, q \in V$ выполняется *аксиома замены*:

(φ4) $p \notin \overline{X}$, $p \in \overline{X \cup q} \Rightarrow q \in \overline{X \cup p}$.

Покажем, что наследственная система также может быть определена в терминах замыкания.

Лемма 1. *Определение наследственной системы в терминах независимых множеств эквивалентно следующему. Непустое конечное множество V вместе с отображением $X \xrightarrow{\varphi} \overline{X}$ называется наследственной системой, если выполняются условия* (φ1), (φ2) *и* (φ4).

Доказательство. Пусть $(V, \mathcal{A})$ — наследственная система. Определим замыкание любого множества $X \subseteq V$ так же, как это сделано в случае матроидов (см. [1]):

$$\overline{X} = X \cup \{v \in V \mid \exists A \subseteq X \text{ такое, что } A \in \mathcal{A} \text{ и } A \cup v \notin \mathcal{A}\}. \qquad (1)$$

Тогда для отображения $X \xrightarrow{\varphi} \overline{X}$ свойства (φ1), (φ2), очевидно, выполнены. Докажем свойство (φ4). Пусть $p \notin \overline{X}$, $p \in \overline{X \cup q}$. Из (1) следует, что существует такое $A \subseteq X \cup q$, что $A \in \mathcal{A}$ и $A \cup p \notin \mathcal{A}$. Поскольку $p \notin \overline{X}$, то $q \in A$ и $(A \setminus q) \cup p \in \mathcal{A}$. Таким образом, существует множество $A' = (A \setminus q) \cup p \subseteq X \cup p$ такое, что $A' \in \mathcal{A}$ и $A' \cup q = A \cup p \notin \mathcal{A}$. Поэтому $q \in \overline{X \cup p}$ в силу (1).

Обратно, пусть (V, φ) — наследственная система, где φ — отображение множества 2^V в себя, удовлетворяющее условиям (φ1), (φ2) и (φ4). Так же, как в случае матроидов, определим семейство

$\mathcal{A}$ по правилу:

$$\mathcal{A} = \{A \subseteq V \mid a \notin \overline{A \setminus a} \text{ для всех } a \in A\}. \qquad (2)$$

Нетрудно проверить, что семейство $\mathcal{A}$ удовлетворяет аксиоме $(A1)$.

Рассмотрим произвольную наследственную систему (V, φ). Множество $X \subseteq V$ называется *замкнутым*, или *листом*, если $X = \overline{X}$.

Теорема 1. *Семейство листов произвольной наследственной системы образует полную решетку.*

Доказательство. Используя свойства $(\varphi 1)$, $(\varphi 2)$ и $(\varphi 4)$, нетрудно показать, что семейство $\mathcal{F}$ всех листов произвольной наследственной системы на множестве V является *муровским семейством*, т. е. $\mathcal{F}$ замкнуто относительно пересечений и $V \in \mathcal{F}$. Окончание доказательства следует из того факта, что любое муровское семейство подмножеств множества V образует полную решетку относительно теоретико-множественного включения [2].

Если наследственная система является матроидом, имеет место следующая теорема.

Теорема 2 (Биркгоф — Уитни) [1]. *Пусть (V, φ) — матроид на множестве V. Тогда решетка его листов — геометрическая. И наоборот, любая геометрическая решетка изоморфна решетке листов некоторого матроида.*

Однако, как будет показано далее, существуют наследственные системы, отличные от матроидов, решетки листов которых также являются геометрическими.

Наследственная система $(V, \mathcal{A})$ называется *наследственной системой графа*, если $\mathcal{A}$ — семейство всех независимых множеств вершин некоторого графа $G = (V, E)$ без петель.

Хорошо известно, что наследственная система графа является матроидом тогда и только тогда, когда каждая компонента связности графа есть полный граф.

Лемма 2. *Пусть (V, φ) — наследственная система k-компонентного графа $G = (V, E)$ без петель. Тогда ее листами являются пустое множество вершин, множества вершин компонент связности графа G, всевозможные объединения множеств вершин компонент связности графа G, и только они.*

Доказательство. В силу (1) множество X — лист тогда и только тогда, когда $\{v \in V \mid \exists A \subseteq X$ такое, что $A \in \mathcal{A}$ и $A \cup v \notin \mathcal{A}\} = \emptyset$. Последнее равносильно тому, что для любого ребра uv графа G обе вершины u, v одновременно входят или не входят в X. Значит, множество вершин X либо пусто, либо порождает подграф, состоящий из одной или нескольких компонент связности графа G.

Теорема 3. *Пусть* (V, φ) *— наследственная система графа. Тогда семейство всех ее листов образует геометрическую дистрибутивную решетку. И наоборот, любая такая решетка изоморфна решетке листов наследственной системы некоторого графа.*

Доказательство. Из леммы 2 следует, что решетка листов $L(V)$ наследственной системы графа $G = (V, E)$ изоморфна булевой алгебре $\mathcal{B}(k)$, где k — число компонент связности графа G. А поскольку дистрибутивные решетки — это булевы алгебры, и только они [1], мы получаем требуемое утверждение.

Список литературы

1. Айгнер М. Комбинаторная теория. — М.: Мир, 1982.
2. Биркгоф Г. Теория решеток. — М.: Наука, 1984.

ОЦЕНКА АБСОЛЮТНОЙ ПОГРЕШНОСТИ ПРИБЛИЖЕННОГО РЕШЕНИЯ NP-ТРУДНЫХ ЗАДАЧ ТЕОРИИ РАСПИСАНИЙ

А. А. Лазарев (Москва)

Рассматривается подход построения приближенного решения с гарантированной абсолютной погрешностью для NP-трудных в сильном смысле задач минимизации максимального временно́го смещения $P, Q, R|prec, r_j|L_{max}$. Имеется n требований $j \in N = \{1, \ldots, n\}$ и m приборов $M_1, \ldots, M_m$. Для каждого требования $j \in N$ даны: момент возможного начала обслуживания r_j; длительности обслуживания $0 \leq p_{ji} \leq \infty$ (продолжительность обслуживания требования j на приборе i) и директивный срок d_j. Отношения предшествования между требованиями представлены ацикличным ориентированным графом G. Каждое требование может быть обслужено только одним прибором, а каждый прибор не может одновременно обслуживать более одного требования. Необходимо найти допустимое расписание π, на котором достигается минимум максимального временно́го смещения $L_{\max}(\pi) = \max_{j \in N}\{C_j(\pi) - d_j\}$, где $C_j(\pi)$ — момент завершения обслуживания требования j при расписании π. Идея подхода состоит в построении по исходному примеру A примера B (с тем же количеством требований) с минимальной оценкой абсолютной погрешности.

Определим следующие функции:

$$\rho(A,B) = \rho_d(A,B) + \rho_r(A,B) + \rho_p(A,B),$$

где

$$\rho_d(A,B) = \max_{j\in N}\{d_j^A - d_j^B\} - \min_{j\in N}\{d_j^A - d_j^B\},$$

$$\rho_r(A,B) = \max_{j\in N}\{r_j^A - r_j^B\} - \min_{j\in N}\{r_j^A - r_j^B\},$$

$$\rho_p(A,B) = \sum_{j\in N}\left(\max_{i\in M}\{p_{ji}^A - p_{ji}^B, 0\} - \min_{i\in M}\{p_{ji}^A - p_{ji}^B, 0\}\right).$$

Если положить $r_1 = d_1 = 0$, что не ограничивает общности исследуемых задач, тогда функция $\rho(A,B)$ удовлетворяет свойствам метрики в евклидовом пространстве параметров примеров.

Будем обозначать через π^A и π^B — оптимальные расписания для примеров A и B, соответственно.

Теорема 1. *Пусть* $A = \left\{G, \left(r_j^A, p_{ji}^A, d_j^A\right) | j \in N, i \in M\right\}$ *и* $B = \left\{G, \left(r_j^B, p_{ji}^B, d_j^B\right) | j \in N, i \in M\right\}$ *(с идентичным графом предшествования* G*) — два примера, тогда*

$$0 \le L_{\max}^A(\pi^B) - L_{\max}^A(\pi^A) \le \rho(A,B).$$

Теорема 2. *Пусть* $A = \left\{G, \left(r_j^A, p_{ji}^A, d_j^A\right) | j \in N, i \in M\right\}$ *и* $B = \left\{G, \left(r_j^B, p_{ji}^B, d_j^B\right) | j \in N, i \in M\right\}$ *(с идентичным графом предшествования* G*) — два примера, тогда для приближенного расписания* $\overline{\pi}$ *(примера* B*) верно*

$$0 \le L_{max}^A(\overline{\pi}) - L_{max}^A(\pi^A) \le \delta^B(\overline{\pi}) + \rho(A,B),$$

где $\delta^B(\overline{\pi}) = L_{max}^B(\overline{\pi}) - L_{max}^B(\pi^B)$.

Предлагаемый подход состоит из двух шагов. На первом шаге в исходном примере $A = \left\{G, \left(r_j^A, p_{ji}^A, d_j^A\right) | j \in N, i \in M\right\}$ так изменяем параметры r_j, p_{ji} и d_j, $\forall j \in N$, $\forall i \in M$, что получаем пример $B = \left\{G, \left(r_j^B, p_{ji}^B, d_j^B\right) | j \in N, i \in M\right\}$, принадлежащий некоторому полиномиально разрешимому классу исходной задачи с минимальным расстоянием $\rho(A,B)$. На втором шаге мы находим оптимальное расписание для примера B. Согласно теореме 1, расписание π^B для примера A имеет оценку абсолютной погрешности: $0 \le L_{\max}^A(\pi^B) - L_{\max}^A(\pi^A) \le \rho(A,B)$.

Рассмотрим случай, когда полиномиально разрешимый класс примеров задается системой из k линейных неравенств

$$\mathbf{X} \times R + \mathbf{Y} \times P + \mathbf{Z} \times D \leq H,$$

где $R = (r_1, \ldots, r_n)^T$, $D = (d_1, \ldots, d_n)^T$, $P = (P_1, \ldots, P_n)^T$, $P_j = (p_{j1}, \ldots, p_{jm})$, $\forall j \in N$; $\mathbf{X}$ и $\mathbf{Z}$ — матрицы размером $k \times n$, $\mathbf{Y}$ — матрица размером $k \times nm$ и H — k-мерный вектор (верхний индекс T обозначает операцию транспонирования). Следует отметить, что указанная полиномиально разрешимая область примеров может быть невыпуклой областью. Обычно число ограничений $k = O(nm)$. Далее в классе примеров, заданном системой неравенств, мы находим пример с минимальным "расстоянием" $\rho(A, B)$ (до исходного примера A), решая следующую задачу

$$\begin{cases} \min\,(x^d - y^d + x^r - y^r) + \sum_{j \in N}(x_j^p - y_j^p), \\ y^d \leq d_j^A - d_j^B \leq x^d, \quad \forall j \in N, \\ y^r \leq r_j^A - r_j^B \leq x^r, \quad \forall j \in N, \\ y_j^p \leq p_{ji}^A - p_{ji}^B \leq x_j^p, \quad \forall j \in N, \forall i \in M, \\ y_j^p \leq 0 \leq x_j^p, \quad \forall j \in N, \\ \mathbf{X} * R^B + \mathbf{Y} * P^B + \mathbf{Z} * D^B \leq H. \end{cases}$$

Задача линейного программирования с $(4 + 4n + nm)$ переменными $\left(x^d,\, y^d,\, x^r,\, y^r; x_j^p, y_j^p, r_j^B, d_j^B,\, \forall j \in N; p_{ji}^B, \forall j \in N, \forall i \in M\right)$ и $(6n + 2nm + k)$ неравенствами может быть решена за полиномиальное время при некоторых специальных линейных ограничениях. Схемы нахождения приближенного решения для задачи $1|r_j|L_{\max}$ рассмотрены в [1] (трудоемкость не превышает $O(n^3 \log n)$ операций), другие схемы рассмотрены в [2]. В случае, когда для исходной задачи нет полиномиально разрешимых выделенных подслучаев либо "расстояние" $\rho(A, C)$ до любого полиномиально разрешимого примера C "слишком велико". Но для некоторого примера B оценка абсолютной погрешности максимального временно́го смещения приближенного расписания $\overline{\pi}$ является "приемлемой", тогда для исходного примера A приближенное расписание $\overline{\pi}$ имеет гарантированную погрешность от оптимального значения целевой функции, согласно теореме 2, не превышающую $0 \leq L_{max}^A(\overline{\pi}) - L_{max}^A(\pi^A) \leq \delta^B(\overline{\pi}) + \rho(A, B)$. Величина $\delta^B(\overline{\pi}) + \rho(A, B)$ порой оказывается существенно меньше, чем $\rho(A, C)$ для любого полиномиально разрешимого примера C.

Список литературы

1. Лазарев А. А., Садыков Р. Р., Севастьянов С. В. Схема нахождения приближенного решения задачи $1||L_{\max}$ // Дискретный анализ и исследование операций. Сер. 2. — 2006. — Т. 13, № 1. — С. 57–76.

2. Лазарев А. А., Скиндерев С. А. Схемы нахождения приближенного решения для задач теории расписаний // Труды V Московской международной конференции по исследованию операций (10–14 апреля 2007 г.). — М.: Изд-во факультета ВМиК МГУ, 2007. — С. 251–253.

СХЕМЫ НАХОЖДЕНИЯ ПРИБЛИЖЕННОГО РЕШЕНИЯ NP-ТРУДНЫХ ЗАДАЧ ТЕОРИИ РАСПИСАНИЙ

А. А. Лазарев, С. А. Скиндерев (Москва)

Рассматриваются NP-трудные в сильном смысле задачи $Q, R|prec, r_j|L_{\max}$. Имеется n требований $j \in N = \{1, \ldots, n\}$ и m приборов $M_1, \ldots, M_m$. Для каждого требования $j \in N$ заданы: момент возможного начала обслуживания r_j, длительности обслуживания $0 \leq p_{ji} \leq \infty$ (длительность обслуживания требования j на приборе i) и директивный срок d_j. Также могут быть заданы отношения предшествования между требованиями в виде ацикличного ориентированного графа G. Каждое требование может быть обслужено только одним прибором, а каждый прибор не может одновременно обслуживать более одного требования. Необходимо построить допустимое расписание π, при котором достигается минимум максимального временно́го смещения $L_{\max}(\pi) = max_{j \in N}\{C_j(\pi) - d_j\}$, где $C_j(\pi)$ — момент завершения обслуживания требования j при расписании π. Предлагаются схемы нахождения приближенного решения, когда для исходного примера A строится решение с гарантированной абсолютной погрешностью значения целевой функции $L_{\max}$. Через $L^A_{\max}(\pi)$ будем обозначать значение целевой функции для примера A при расписании π. В [1] проведен анализ оценки абсолютной погрешности для задач $P, Q, R|prec, r_j|L_{max}$ и была доказана следующая

Теорема. *Пусть* $A = \{G, (r_j^A, p_{ji}^A, d_j^A) | \, j \in N, i \in M\}$ *и* $B = \{G, (r_j^B, p_{ji}^B, d_j^B) | j \in N, i \in M\}$ *(с идентичным графом предшествования* G*) — два примера, тогда*

$$0 \le L_{max}^A(\overline{\pi}) - L_{max}^A(\pi^A) \le \delta^B(\overline{\pi}) + \rho(A, B),$$

где $\delta^B(\overline{\pi}) = L_{max}^B(\overline{\pi}) - L_{max}^B(\pi^B)$ *и*

$$\rho(A,B) = \max_{j\in N}\{d_j^A - d_j^B\} - \min_{j\in N}\{d_j^A - d_j^B\} + \max_{j\in N}\{r_j^A - r_j^B\} - \min_{j\in N}\{r_j^A - r_j^B\} +$$

$$+ \sum_{j\in N}\left(\max_{i\in M}\{(p_{ji}^A - p_{ji}^B), 0\} - \min_{i\in M}\{(p_{ji}^A - p_{ji}^B), 0\}\right),$$

π^A, π^B *— оптимальные расписания для примеров* A *и* B*, соответственно.*

Таким образом, для любого исходного примера A мы находим пример B, принадлежащий некоторому полиномиально разрешимому классу, при котором "расстояние" $\rho(A, B)$ минимально.

Пусть необходимо найти оптимальное расписание для примера A задачи $\alpha|\beta|L_{\max}$ и известно, что соответствующая задача $\alpha|\beta|C_{\max}$ полиномиально разрешима, где α — характеристики приборов, β — характеристики требований, $C_{\max} = \max_{j\in N} C_j(\pi^B)$. Тогда

$$L_{\max}^A(\pi^B) - L_{\max}^A(\pi^A) \le \rho(A, B) = \max_{j\in N} d_j^A - \min_{j\in N} d_j^A.$$

Пусть необходимо найти оптимальное расписание для примера A задачи $\alpha|\beta|L_{\max}$ и известно, что соответствующая задача $\alpha|\beta, p_j = p|L_{\max}$ полиномиально разрешима. Тогда необходимо решить следующую оптимизационную задачу

$$\rho(A, B) = \sum_j |p_j - p| \to \min_p.$$

Решение этой задачи $p^* = p_{[\frac{n+1}{2}]}$ (если $p_1 \le \cdots \le p_n$). В итоге получаем

$$L_{\max}^A(\pi^B) - L_{\max}^A(\pi^A) \le \sum_{j=1}^{n} \left| p_j - p_{[\frac{n+1}{2}]} \right|.$$

Если вместо ограничения $p_j = p$ для всех j из N дано $p_j = 1$, тогда абсолютная погрешность целевой функции удовлетворяет условию

$$L^A_{\max}(\pi^B) - L^A_{\max}(\pi^A) \le \sum_{j=1}^{n} \left| p_j - p_{[\frac{n+1}{2}]} \right| + 2p_{[\frac{n+1}{2}]}.$$

Пусть исследуемая задача $R|\beta|L_{\max}$ или $Q|\beta|L_{\max}$, для произвольного примера A мы рассматриваем соответствующий пример B задачи $P|\beta|L_{\max}$. Тогда нам необходимо решить следующую задачу

$$\rho(A,B) = \sum_{j\in N} \left(\max_{i\in M}\{(p^A_{ji} - p^B_j), 0\} - \min_{i\in M}\{(p^A_{ji} - p^B_j), 0\} \right) \to \min_{p_j}.$$

Решением данной задачи будет любое значение для p^B_j из отрезка $[\min\limits_{i\in M} p^A_{ji}, \max\limits_{i\in M} p^A_{ji}], \forall j \in N$, и

$$L^A_{\max}(\pi^B) - L^A_{\max}(\pi^A) \le \sum_{j\in N} \left(\max_{i\in M} p^A_{ji} - \min_{i\in M} p^A_{ji} \right).$$

Пусть необходимо найти оптимальное расписание для примера A из класса $R|\beta|L_{\max}$ и известно, что соответствующая задача $Q|\beta|L_{\max}$ полиномиально разрешима. Тогда необходимо решить следующую задачу

$$\rho(A,B) = \sum_{j\in N} \left(\max_{i\in M}\{(p^A_{ji} - p^B_j\sigma^B_i), 0\} - \min_{i\in M}\{(p^A_{ji} - p^B_j\sigma^B_i), 0\} \right) \to \min_{p^B_j, \sigma^B_i}.$$

Эта задача может быть представлена в виде

$$\begin{cases} \sum\limits_{j\in N} (\alpha_j - \beta_j) \to \min\limits_{\alpha_j, \beta_j, p^B_j, \sigma^B_i}, \\ \beta_j \le p^A_{ji} - p^B_j\sigma^B_i \le \alpha_j, & \forall j \in N, \forall i \in M, \\ \beta_j \le 0 \le \alpha_j, & \forall j \in N. \end{cases}$$

Список литературы

1. Лазарев А. А. Оценка абсолютной погрешности приближенного решения NP-трудных задач теории расписаний // Материалы IX Международного семинара "Дискретная математика и

ее приложения" (18–23 июня 2007 г.). — М.: Изд-во механико-математического факультета МГУ, 2007.

РАНГ ШЕЙНА БУЛЕВЫХ МАТРИЦ И КОДИРОВАНИЕ ДВУДОЛЬНЫХ ГРАФОВ

Е. Е. Маренич (Мурманск)

Пусть $P = \{\widetilde{0}, \widetilde{1}\}$ — двухэлементная булева решетка, $P^{m\times n}$ — множество всех $m\times n$ матриц с элементами из множества P, матрица $A \in P^{m\times n}$.

Из книги Ки Ханг Кима [1] известно, что определение ранга Шейна, над двухэлементной булевой решеткой $P = \{\widetilde{0}, \widetilde{1}\}$, принадлежит Б. М. Шейну. Определение ранга Шейна, над полукольцами, дано в статье Ки Ханг Кима и Ф. Роуша [2]. Методы вычисления ранга Шейна над цепями рассматривались в работах [3, 4].

Пусть $\Gamma = \Gamma(V_1 \cup V_2, E)$ — двудольный граф, U — конечное множество.

Функция $f : V_1 \cup V_2 \to 2^U$ называется *кодированием* двудольного графа Γ подмножествами множества U, если для любых вершин $v_1 \in V_1$ и $v_2 \in V_2$ условие

$$(v_1, v_2) \in E$$

равносильно условию

$$f(v_1) \cap f(v_2) \neq \emptyset.$$

Значение $f(v)$ называется *кодом* вершины $v \in V$.

Заметим, что существует кодирование всякого двудольного графа Γ подмножествами некоторого конечного множества.

Наименьшее число элементов во множестве U, подмножествами которого можно осуществить кодирование графа Γ, называется *числом пересечений* двудольного графа Γ и обозначается $n\mathrm{int}_\emptyset(\Gamma)$.

Кликой двудольного графа Γ называется любой максимальный полный двудольный подграф, содержащий хотя бы одно ребро.

Будем говорить, что подграфы $\Gamma_1, \ldots, \Gamma_k$ графа Γ *покрывают* граф, если каждое каждая вершина и каждое ребро графа, принадлежат хотя бы одному подграфу.

Покажем, что вычисление числа пересечений двудольного графа сводится к изучению клик, покрывающих граф.

Теорема 1. *Пусть $\Gamma = \Gamma(V_1 \cup V_2, E)$ — двудольный граф без изолированных вершин. Тогда число пересечений двудольного графа Γ равно наименьшему числу клик, покрывающих граф.*

Пусть граф Γ' получен из графа Γ удалением всех изолированных вершин. Тогда $n\mathrm{int}_\emptyset(\Gamma) = n\mathrm{int}_\emptyset(\Gamma')$.

Каждая матрица A определяет двудольный граф

$$\Gamma(A) = \Gamma(V_1 \cup V_2, E)$$

такой, что:

$$V_1 = \{1, \ldots, m\}, \quad V_2 = \{1', 2', \ldots, n'\};$$

$\{i, j'\} \in E$ тогда и только тогда, когда $a_{ij} = \widetilde{1}$.

Будем говорить, что граф $\Gamma(A)$ *ассоциирован* с матрицей A.

Следующая теорема сводит вычисление ранга Шейна матрицы A к вычислению числа пересечений двудольного графа $\Gamma(A)$, ассоциированного с матрицей A.

Теорема 2. *Пусть $P = \{\widetilde{0}, \widetilde{1}\}$ — двухэлементная булева решетка, матрица $A \in P^{m\times n}$. Тогда ранг Шейна матрицы A равен числу пересечений двудольного графа $\Gamma(A)$, ассоциированного с матрицей A.*

Следствие 1. *Пусть $P = \{\widetilde{0}, \widetilde{1}\}$ — двухэлементная булева решетка, матрица $A \in P^{m\times n}$. Тогда ранг Шейна матрицы A равен наименьшему числу клик, покрывающих граф Γ', полученный из графа $\Gamma(A)$ удалением всех изолированных вершин.*

Из следствия 1 очевидно следует, что ранг Шейна единичной булевой матрицы $E = E_{n\times n} \in P^{n\times n}$ равен n.

Справедлив следующий критерий того, что матрица A является CR-матрицей.

Следствие 2. *Пусть $P = \{\widetilde{0}, \widetilde{1}\}$ — двухэлементная булева решетка, ненулевая матрица $A \in P^{m\times n}$, $\Gamma(A)$ — двудольный граф, ассоциированный с матрицей A. Следующие утверждения равносильны.*

1) *Ранг Шейна матрицы A равен* 1.

2) *Граф Γ', полученный из графа $\Gamma(A)$ удалением всех изолированных вершин, является полным двудольным графом.*

Теорема 2 сводит вычисление ранга Шейна матрицы A к нахождению наименьшего числа клик, покрывающих граф, то есть к решению задачи о наименьшем покрытии.

Рассмотрим еще одно применение теоремы 1.

Теорема 3. *Пусть $P = \{\widetilde{0}, \widetilde{1}\}$ — двухэлементная булева решетка, единичная матрица $E = E_{n\times n} \in P^{n\times n}$, $\overline{E}$ — матрица дополнений единичной матрицы E. Тогда ранг Шейна матрицы дополнений $\overline{E}$ равен наименьшему числу k, для которого справедливо неравенство $n \le \binom{k}{[k/2]}$.*

Работа осуществляется в соответствии с Тематическим планом Федерального агентства по образованию, тема № 1.03.07.

Список литературы

1. Kim K. X. Boolean matrix theory and applications. — New York: Marcel Dekker, 1982.

2. Kim K. X., Roush F. W. Generalized fuzzy matrices // Fuzzy Sets Systems. — 1980. — V. 4. — P. 293–315.

3. Di Nola, Sessa S. On the Schein rank of matrices over linear lattice // Linear Algebra Appl. — 1989. — V. 118. — P. 155–158.

4. Di Nola, Sessa S. Determining the Schein rank of matrices over linear lattice and finite relational equations // Journal of Fuzzy Mathematics. — 1993. — V. 1, № 1. — P. 33–38.

СТРОЧЕЧНЫЕ И СТОЛБЦОВЫЕ РЕШЕТКИ МАТРИЦЫ

В. Е. Маренич (Мурманск)

Пусть $(P, \wedge, \vee, \leq)$ — решетка, $P^{m\times n}$ — множество всех $m \times n$ матриц с элементами из множества P, матрица $A \in P^{m\times n}$.

Брауэровой решеткой называется решетка $(P, \wedge, \vee, \leq)$, в которой для любых $a, b \in P$ множество всех элементов $x \in P$ таких, что $a \wedge x \leq b$, имеет наибольший элемент $\left\langle {b \atop a} \right\rangle_P = \left\langle {b \atop a} \right\rangle$, называемый *относительным псевдодополнением* элемента a до элемента b.

Частично упорядоченное множество $(P^{m\times 1}, \leq)$ является решеткой, решеточные операции которой обозначены $\vee$ и $\wedge$.

Строчечным подпространством матрицы A называется линейная оболочка векторов-строк матрицы A. *Столбцовым подпространством* матрицы A называется линейная оболочка векторов-столбцов матрицы A. Строчечные и столбцовые подпространства матрицы A обозначаются, соответственно, $Row(A)$ и $Column(A)$.

Пусть $(Column(A), \leq)$ — частично упорядоченное множество, относительно индуцированного решеткой $(P^{m\times 1}, \leq)$ частичного порядка $\leq$. Аналогично, $(Row(A), \leq)$ — частично упорядоченное множество относительно индуцированного решеткой $(P^{1\times n}, \leq)$ частичного порядка $\leq$.

Частично упорядоченное множество $(Column(A), \leq)$ — верхняя полурешетка, в которой операция объединения $\widetilde{\vee}$ совпадает с операцией объединения $\vee$ в решетке $(P^{m\times 1}, \leq)$,

$$u\widetilde{\vee}v = u + v = u \vee v \text{ для } u, v \in Column(A).$$

Если $(P, \wedge, \vee, \leq)$ — полная дистрибутивная решетка и для любого подмножества S подпространства $Column(A)$ верхняя грань $\vee S \in Column(A)$, то частично упорядоченное множество $(Column(A), \leq)$ является полной решеткой, в которой операция объединения $\widetilde{\vee}$ совпадает с операцией объединения $\vee$ в решетке $(P^{m\times 1}, \leq)$.

Если $(P, \wedge, \vee, \leq)$ — конечная дистрибутивная решетка, то частично упорядоченное множество $(Column(A), \leq)$ является решеткой.

В некоторых случаях операция $\widetilde{\wedge}$ в решетке $(Column(A), \leq)$ может быть задана формулами.

Теорема 1. *Пусть $(P, \wedge, \vee, \leq)$ — брауэрова решетка, матрица $A \in P^{m\times n}$. Тогда справедливы следующие утверждения*:

1) *Если $(P, \wedge, \vee, \leq)$ — полная брауэрова решетка, то частично упорядоченное множество $(Column(A), \leq)$ является полной решеткой с решеточными операциями объединения $\widetilde{\vee}$ и пересечения $\widetilde{\wedge}$, где операция $\widetilde{\wedge}$ задана формулой*

$$\widetilde{\wedge}S = A \left\langle \begin{array}{c} \wedge S \\ A \end{array} \right\rangle, \quad S \subseteq Column(A).$$

2) *Если $(P, \wedge, \vee, \leq)$ — брауэрова решетка, то ЧУМ $(Column(A), \leq)$ является решеткой с решеточными операциями объединения $\widetilde{\vee}$ и пересечения $\widetilde{\wedge}$, где операция пересечения $\widetilde{\wedge}$ задана формулой*

$$u\widetilde{\wedge}v = A \left\langle \begin{array}{c} u \wedge v \\ A \end{array} \right\rangle = A \left(\left\langle \begin{array}{c} u \\ A \end{array} \right\rangle \wedge \left\langle \begin{array}{c} v \\ A \end{array} \right\rangle \right),$$

$$u, v \in Column(A).$$

3) *Если $(P, \vee, \wedge, \leq)$ — булева решетка, то ЧУМ $(Column(A), \leq)$ является решеткой с решеточными операциями объединения $\widetilde{\vee}$ и пересечения $\widetilde{\wedge}$, где операция пересечения $\widetilde{\wedge}$ задана формулой*

$$u\widetilde{\wedge}v = A \cdot \overline{{}^{t}A \cdot (\overline{u} + \overline{v})}, \quad u, v \in Column(A).$$

В некоторых столбцовых решетках операция пересечения $\widetilde{\wedge}$ определяется более простыми формулами.

Теорема 2. *Пусть* $(P, \wedge, \vee, \leq)$ — *брауэрова решетка, идемпотент* $A \in P^{n\times n}$. *Тогда справедливы следующие утверждения*:

1) *Операция пересечения* $\widetilde{\wedge}$ *в решетке* $(Column(A), \leq)$ *задана формулой* $u\widetilde{\wedge}v = A\,(u \wedge v)\,,\ u, v \in Column(A)$.

2) *Решетка* $(Column(A), \leq)$ *дистрибутивна.*

Аналогичная теорема справедлива для строчечных решеток.

Теорема 3. *Пусть* $(P, \wedge, \vee, \leq)$ — *брауэрова решетка, идемпотент* $A \in P^{n\times n}$. *Тогда справедливы следующие утверждения*:

1) *Операция пересечения* $\widetilde{\wedge}$ *в решетке* $(Row(A), \leq)$ *задана формулой* $u\widetilde{\wedge}v = (u \wedge v)\,A,\ u, v \in Row(A)$.

2) *Решетка* $(Row(A), \leq)$ *дистрибутивна.*

Матрица A называется *регулярной*, если существует матрица $B \in P^{n\times n}$ такая, что $ABA = A$. Известно, [1], что матрица A регулярна тогда и только тогда, когда существует идемпотент C такой, что $Column(A) = Column(C)$.

Следующую теорему называют критерием К. А. Зарецкого регулярности булевых матриц, [2].

Теорема (Критерий Зарецкого). *Пусть* $P = \{\widetilde{0}, \widetilde{1}\}$ — *двухэлементная булева решетка, матрица* $A \in P^{n\times n}$. *Тогда следующие утверждения равносильны*:

1) *Решетка* $(Column(A), \leq)$ *дистрибутивна.*

2) *Матрица* A *регулярна.*

Следующая теорема является обобщением теоремы К. А. Зарецкого.

Теорема 4. *Пусть* $(P, \wedge, \vee, \leq)$ — *брауэрова решетка, регулярная матрица* $A \in P^{n\times n}$, *идемпотент* $C \in P^{n\times n}$ *такой, что*

$$Column(A) = Column(C).$$

Тогда справедливы следующие утверждения:

1) *Операция пересечения* $\widetilde{\wedge}$ *в решетке* $(Column(A), \leq)$ *задана формулой* $u\widetilde{\wedge}v = C\,(u \wedge v)\,,\ u, v \in Column(A)$.

2) *Решетка* $(Column(A), \leq)$ *дистрибутивна.*

Утверждение 2 теоремы 4 доказано Зарецким [2], для полугруппы бинарных отношений. В работе Ки Ханг Кима и Ф. Роуша [3], утверждение 2 теоремы 4 доказано для нечеткой решетки.

Работа осуществляется в соответствии с Тематическим планом Федерального агентства по образованию, тема № 1.03.07.

Список литературы

1. Kim K. H. Boolean matrix theory and applications. — New York: Marcel Dekker, 1982.

2. Зарецкий К. А. Регулярные элементы полугруппы бинарных отношений // Успехи мат. наук. — 1962. — Т. XVII, вып. 3 (105). — С. 177–179.

3. Ки Ханг Ким, Роуш Ф. Generalized fuzzy matrices // Fuzzy Sets Systems. — 1980. — V. 4. — P. 293–315.

ОЦЕНКА РОДА 3-СКЛЕЙКИ ПРОСТЫХ ГРАФОВ

В. И. Петренюк (Кировоград)

Задача состоит в исследовании свойств графов G без вершин степени 2, с заданным эйлеровым родом γ и заданным разбиением на два подграфа G_i меньшего рода γ_i, $i = 1, 2$, общие вершины которых составляют множество M порядка $k, k > 2$. Граф G будем называть k-склейкой графов G_i. Результат получен методом φ-преобразований графов, предложенный в 1973 г. Н. П. Хоменко, который рассмотрел граф как топологическое подпространство замкнутого ориентированного 2-многообразия рода γ. Им же было введено число достижимости некоторого множества X точек графа G как наименьшее число 2-клеток на границы которых выходят все точки из X. Обозначим через $G - v$ непустой подграф графа G, полученный путём удаления из графа G вершины v, принадлежащей множеству M, вместе со всеми рёбрами, инцидентными этой вершине.

В [1] предложены две новых характеристики — θ и $\partial\theta$ множества X, состоящего из вершин или внутренних точек рёбер графа G, роль которых заключается в измерении циклической и цепочной структур дуального графа Ω графа G. В [2] получена оценка: $\gamma(G) \leq \gamma(G - v) + t - \theta - \partial\theta - 1$, где $X = \{a_i^*\}_1^n$, $t_{G-v}(X) = t$, $\theta_{G-v}(X) = \theta$, $\partial\theta_{G-v}(X) = \partial\theta$, $t > 1, \cdot\theta \geq 0$, $\partial\theta \geq 0$.

Основная идея решения задачи состоит в рекурсивном подходе к оценке рода графа G, где $G = G(k)$, который является φ-образом графа $G(k-1) + St_n(v)$ при φ-преобразовании путём попарного отождествления точек из множества X с n концевыми вершинами звезды $St_n(v)$, где $v \in M$. Это φ-преобразование запишем следующим образом:

$$\varphi(G(k-1) + St_n(g_0), \sum_{i=1}^{n} a_i + g_i) \to (G(k), \{a_i^*\}_1^n),$$

где $X = \{a_i\}_1^n, t_{G(k-1)}(X) = t,\ t > 1, D = \{g_i\}_1^n, t_{St_n(g_0)}(D) = 1$ являются множествами точек графов $G(k-1)$, $St_n(g_0)$ с числами достижимости $t, 1$ соответственно. Обозначим через $\alpha_{G_i}(M_i)$ наименьшую сумму чисел $\theta_{G_i}(M_i) + \partial\theta_{G_i}(M_i)$, вычисленную для каждой вершины, принадлежащей множеству M_i, где $M_i = (\varphi)^{-1}(M) \cap G_i, i = 1, 2$.

Теорема. *Выполняются неравенства*

$$2 \leq \gamma(G) - \sum_{i=1}^{2} \gamma(G_i) \leq 2 + \sum_{i=1}^{2} (\alpha_{G_i}(M_i)).$$

Этот результат был частично опубликован в [3, 4].

Список литературы

1. Petrenjuk V. I. Two characteristics of the planar graph dual graph // Materials of the International Conference "Artificial Intellect. Intellectual and Multiprocessor Systems". (September 20–25, 2004, Crimea, Ukraine). — P. 230–231.

2. Petrenjuk V. I. Generalized estimation of the simple graph genus // The research collection "Artificial Intellect". — 2004. — V. 4. — P. 34–45.

3. Петренюк В. И. Природа неадитивності ейлерового роду простого графа. 1 // Штучний інтелект. — Донецк, 2005. — № 3. — С. 215–238.

4. Петренюк В. И. Природа неадитивності ейлерового роду простого графа. I // Штучний інтелект. — Донецк, 2005. — № 4. — С. 256–267.

О МАГИЧНОСТИ «УЩЕРБЛЁННЫХ» ПОЛНЫХ ГРАФОВ

Л. П. Петренюк (Кировоград)

В определениях [1] (см. также [2, 3]) исследуем задачу о магичности графов серии $A_n = K_n - ab$, где A_n получается в результате удаления из полного n-вершинного графа одного его ребра, соединявшего вершины a и b. Из элементарных соображений заключаем, что при $n \leq 4$ дает немагические графы. Для пятого графа серии существует магическая нумерация φ магической силы 2, которую мы задаем нижеследующей таблицей.

xy	1,2	1,3	1,a	1,b	2,3	2,a	2,b	3,a	3,b
$\varphi(xy)$	1	1	2	1	2	2	2	2	2

Теорема 1. *При четных значениях* $n \geq 6$ *графы* A_n — *магические и имеют магическую силу* 2.

Доказательство. В графе $A_n = K_n - ab$, кроме вершин a и b, укажем четыре разные вершины c, d, e, f. Остальные $n-6$ вершин разобьем на непересекающиеся пары x_i, y_i, $i = 1, ..., (n-6)/2$. (В случае $n = 6$ множество пар пустое.) Построим нумерацию ребер графа A_n, приписав ребрам ac, ad, be, bf и $(x_i, y_i), i = 1, ..., (n-6)/2$ номера 2, а всем остальным ребрам — номера 1. Легко убедиться, что построена магическая нумерация графа A_n магической силы 2, и этим теорема доказана.

Теорема 2. *При нечетных значениях* $n = 5$ *и* $n \geq 9$ *графы* A_n — *магические и имеют магическую силу* 2.

Доказательство. При $n = 5$ теорема следует из существования магической нумерации, приведенной в начале. Пусть теперь $n \geq 9$. Укажем в графе A_n три разные вершины c, d, e, отличные от a и b. Количество оставшихся необозначенными вершин равно $n - 5 > 3$. Дадим им обозначения $x_1, ..., x_{(n-5)}$. Построим теперь реберную нумерацию графа A_n. Для этого припишем номера 2 ребрам ac, ad, ae, bc, bd, be и ребрам некоторого цикла, построенного на вершинах $x_1, ..., x_{(n-5)}$, а остальным ребрам графа A_n присвоим номера 1. Легко увидеть, что построенная нумерация графа A_n является магической и имеет магическую силу 2, что доказывает теорему. Остался нерешённым случай $n = 7$. Тот факт, что в этом случае справедлив вывод теоремы 2, обосновывается наличием следующей нумерации графа A_7.

xy	a,3	a,4	a,5	a,7	b,3	b,4	b,5	b,6	b,7
$\varphi(xy)$	1	2	2	2	1	2	1	2	1

xy	3,4	3,5	3,6	3,7	4,5	4,6	4,7	5,6	5,7	6,7
$\varphi(xy)$	2	2	1	1	1	1	1	1	1	2

В завершение сформулируем обобщения рассмотренной задачи. Есть необходимость решать задачу о магичности графа $K_n - g$, где g — произвольный подграф графа K_n. В частности, интересны случаи с 1) $g = K_r, r < n$; 2) $g = C_r$, $3 \leq r \leq n$; 3) $g = F_r$, где F_r — регулярный r-реберный подграф степени 1 графа K_n; 4) $g = Z_r$, где Z_r — подграф-звезда порядка $r < n - 1$; 5) $g = T_r$, где T_r — подграф-дерево порядка $r \leq n$.

Список литературы

1. Петренюк А. Я. Магическая сила цилиндрических решеток // Материалы IX Международного семинара «Дискретная математика и ее приложения», посвященного 75-летию со дня рождения академика О. Б. Лупанова (Москва, МГУ, 18–23 июня 2007 г.). — М.: Изд-во механико-математического факультета МГУ, 2007.

2. Kong M. C., Sin-min Lee, Sun H. S. A. On the magic strength of graphs // Ars Combinatoria. — 1997. — V. 45. — P. 193–200.

3. Сапроненко Т. Про магічну силу графу // "Студентська наука: проблеми і перспективи XXI століття". Зб. матеріалів Четвертої Всеукранської студентської науково-практичної конференції (14–15 травня 2004 року). — Кіровоград, 2004. — P. 113–114.

О ПРЕДСТАВИМОСТИ МАТРОИДОВ

А. М. Ревякин (Москва)

Пусть $P(S)$ — множество всех подмножеств конечного множества S. Система $\mathcal{I} \subseteq P(S)$ подмножеств из S называется матроидом $M = (S, \mathcal{I})$, а множества из $\mathcal{I}$ — независимыми, если выполняются следующие условия: 1) $\oslash \in \mathcal{I}$; 2) если $A \subseteq B$ и $B \in \mathcal{I}$, то $A \in \mathcal{I}$; 3) если $A, B \in \mathcal{I}$ и $|A| > |B|$, то найдется $a \in A \setminus B$ такое, что $B \cup \{a\} \in \mathcal{I}$.

Пусть имеется $n+1$ множество $S_0, S_1, \ldots, S_n$. Произвольная $(M \times (n+1))$-матрица V, строки которой имеют вид $v = (v_0, v_1, \ldots, v_n)$, где $v_i \in S_i$, называется матрицей СРС, а ее строки — правилами распределения секрета. Для произвольного подмножества $B \subset \{0, 1, \ldots, n\}$ через V_B обозначим $(M \times |B|)$-матрицу, полученную из матрицы V удалением столбцов, номера которых не принадлежат множеству B. Говорят, что матрица V задает совершенную СРС, реализующую структуру доступа Γ, если $||V_{A\cup 0}|| = ||V_A|| \times ||V_0||^{\delta_\Gamma(A)}$, где $||V||$ — число различных строк в матрице V; $\delta_\Gamma(A) = 0$, если $A \in \Gamma$, и $\delta_\Gamma(A) = 1$ в противном случае. Совершенная СРС называется идеальной, если $|S_i| = |S_0|$ для всех $i = 1, \ldots, n$. Оказывается, что для любой совершенной идеальной СРС, реализующей структуру доступа Γ, семейство I подмножеств A, для которых $h(A) = |A|$, где $h(A) = \log_q ||V_A||$ и $q = |S_0|$, являюся множеством независимых

множеств некоторого матроида M на множестве $\{0, 1, \ldots, n\}$. Заметим, что функция $h(A)$ совпадает с ранговой функцией этого матроида. Все циклы матроида M, содержащие 0, имеют вид $0 \cup A$, где A — минимальные (по включению) множества из Γ. Разным идеальным СРС, реализующим данную структуру доступа Γ, всегда соответствует один и тот же матроид, поскольку матроид однозначно определяется семейством циклов, проходящих через фиксированную точку. Матроид M назовем СРС-матроидом, если существует совершенная идеальная СРС, матроид которой изоморфен M.

Каждый пример матроида обычно является источником "внутренних" проблем (представимости, координатизации, характеризации матроидов списком запрещенных миноров и т. д.) и мотивирует многие из последующих шагов развития теории.

Матроид M на множестве S называется представимым над полем F, если существует линейное пространство V над полем F и отображение $\phi : S \longrightarrow V$, при котором $A \subseteq S$ независимо в M тогда и только тогда, когда $\phi|_A$ взаимно однозначно и $\phi(A)$ — линейно независимое множество векторов в V. При этом отображение ϕ называется координатизацией матроида над полем F.

Пусть $\mathrm{GF}(q)$ — конечное поле характеристики q. Матроид, представимый над полем $\mathrm{GF}(2)$ или $\mathrm{GF}(3)$, называется бинарным или тернарным соответственно. Матроид, представимый над каждым полем, называются унимодулярным.

Матроид M на 10-элементном множестве называется дезарговым, если он изоморфен конфигурации Дезарга. Если в матроиде Дезарга трехточечную прямую заменить тремя тривиальными прямыми, то получим новый матроид ("не-дезаргов" матроид), не представимый ни над каким полем F. Конфигурации типа дезарговых и папповых представимы над любым полем F.

Лазарсон построил пример матроида M_p, представимого только над полями характеристики p. Т. Брилавский и Д. Кэлли построили матроид, который представим над полем F тогда и только тогда, когда характеристика поля F равна 1103 или 2089. Матрица представления этого матроида над полем характеристики 1103 имеет вид:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & \ldots & 1 & 0 \\ 0 & 1 & 0 & -1 & -1 & 0 & 1 & -2 & 0 & 1 & 0 & 1 & 0 & 1 & \ldots & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 2 & 2 & 4 & 4 & 8 & 8 & \ldots & 2^{28} & 2^{28} \end{pmatrix}.$$

Характеристическим множеством $Char(M)$ матроида M называется такое множество $Char(M)$, что $p \in Char(M)$ тогда и только

тогда, когда M линейно представим над некоторым полем характеристики p. Пусть Z — множество простых чисел и 0. Тогда проблему координатизации можно сформулировать в виде: "для каждого подмножества Q множества Z найти матроид, линейно представимый над всеми полями с характеристиками из Q и не представимый ни над каким полем характеристики p, если $p \notin Q$".

Матроиды Вамоса и "не-дезаргов" не представимы над каким полем. Для матроида Фано характеристическое множество равно $\{2\}$, для матроида Φ^- — $Z \setminus \{2\}$, для матроида Лазарсона — $\{p\}$, где p — простое число, а для унимодулярных и циклических матроидов ориентированных графов — Z.

Известный результат У. Татта утверждает, что если $p \neq 2$ и $\{2, p\} \subseteq Char(M)$, то $Char(M) = Z$. Поэтому представляет особый интерес проблема представимости небинарных матроидов, а в свете результата Т. Брилавского и Д. Кэлли о наличии матроида M с $Char(M) = \{1103, 2089\}$ — следующая открытая проблема: существуют ли матроиды M с $Char(M) = \{p, q\}$, где p и q — различные простые числа, отличные от 2.

Установлено, что матроид представим над полями GF(3) и GF(5) тогда и только тогда, когда он представим над GF(3) и полем рациональных чисел (или, что эквивалентно, над GF(p) для всех нечетных простых чисел p). Доказано, что матроид представим над GF(3) и полем комплексных чисел тогда и только тогда, когда он представим над GF(3) и GF(7). Матроид представим над полями GF(3), GF(4) и GF(5) в том и только в том случае, когда он представим над каждым полем, за исключением, быть может, GF(2). Показано, что если матроид представим над GF(p) для каждого нечетного простого p, то он представим над полем рациональных чисел.

Многие проблемы теории матроидов касаются вопроса о внутренней характеризации классов матроидов. Такие характеризации обычно получают в виде: "Существует некоторый минимальный, но возможно бесконечный, список $\mathcal{S}$ такой, что матроид M лежит в классе L тогда и только тогда, когда M не содержит миноров, изоморфных элементам из $\mathcal{S}$" и называют характеризациями классов матроидов с помощью списка запрещенных миноров.

Характеризации с помощью списка запрещенных миноров получены для большинства известных классов матроидов (бинарных, тернарных, унимодулярных, графических и кографических). Однако, не найдено такой характеризации для класса трансверсальных матроидов.

Построен пример нелинейного CPC-матроида. Показано, что нелинейный матроид Вамоса не может быть получен как матроид иде-

альной CPC. Поэтому задача характеризации класса CPC-матроидов представляется интересной.

Список литературы

1. Ревякин А. М. Координатизация и представимость матроидов // Комбинатор. анализ. Вып. 8. — М.: МГУ, 1989. — С. 6–37.

2. Brickell E. F., Davenport D. M. On the classification of ideal secret sharing schemes // J. Cryptology. — 1991. — № 4. — С. 123–134.

3. Revyakin A. M. On some classes of linear representable matroids // Formal Power Series and Algebraic Combinatorics: 12 International Conference; proceedings (Moscow, Russia, June 2000). — Berlin, N.Y.: Springer, 2000. — С. 564–574.

4. Welsh D. J. A. Matroid theory. — London: Acad. Press, 1976.

О ЧИСЛЕ ОБРАТИМЫХ МАТРИЦ НАД КОЛЬЦОМ ВЫЧЕТОВ

С. В. Сидоров (Нижний Новгород)

Рассмотрим кольцо квадратных матриц $\mathbf{K}^{n\times n}$, где $\mathbf{K} = \mathbf{Z}/\mathbf{m}$ — кольцо вычетов по модулю m. Пусть $m = p_1^{k_1}\cdot\ldots\cdot p_s^{k_s}$ — каноническое разложение числа m на простые множители, где $p_1,\ldots,p_s$ — различные простые числа. Обозначим число обратимых матриц в этом кольце через $\alpha_n(m)$, а через $\gamma_n(m)$ — долю обратимых матриц среди всех, т. е. $\gamma_n(m) = \frac{\alpha_n(m)}{m^{n^2}}$. Известно (см., например, [1]), что $\alpha_n(m) = \prod\limits_{i=1}^{s}\alpha_n(m_i) = \prod\limits_{i=1}^{s}\left(p_i^{k_i n^2}\prod\limits_{t=1}^{n}\left(1-\frac{1}{p_i^t}\right)\right) = m^{n^2}\prod\limits_{i=1}^{s}\prod\limits_{t=1}^{n}\left(1-\frac{1}{p_i^t}\right)$, где $m_i = p_i^{k_i}$. В частности, если $m = p$ — простое число, то $\alpha_n(p) = (p^n-1)(p^n-p)\cdot\ldots\cdot(p^n-p^{n-1}) = p^{n^2}\prod\limits_{t=1}^{n}\left(1-\frac{1}{p^t}\right)$. Если $m = p^k$, то $\alpha_n(p^k) = p^{(k-1)n^2}\alpha_n(p) = p^{kn^2}\prod\limits_{t=1}^{n}\left(1-\frac{1}{p^t}\right)$. Отсюда доля $\gamma_n(m)$ обратимых матриц равна $\gamma_n(m) = \frac{\alpha_n(m)}{m^{n^2}} = \prod\limits_{i=1}^{s}\prod\limits_{t=1}^{n}\left(1-\frac{1}{p_i^t}\right) = \prod\limits_{i=1}^{s}\gamma_n(m_i)$. Видно, что величина $\gamma_n(m)$ зависит от простых множителей, входящих в разложение числа m и не зависит от их кратностей. Таким образом, достаточно рассматривать m вида $m = p_1\cdot\ldots\cdot p_s$, т. е. свободные от квадратов. Исследуем поведение величины $\gamma_n(m)$

при больших n и m. Ясно, что достаточно рассмотреть случай, когда $m = p$ — простое. Рассмотрим числовую последовательность $\gamma_n = \gamma_n(p) = \prod\limits_{t=1}^{n} \left(1 - \frac{1}{p^t}\right)$ при фиксированном p. Она сходится, так как монотонно убывает и ограничена снизу нулем. Пусть $\gamma = \gamma(p) = \lim\limits_{n\to\infty} \gamma_n(p)$ — предел этой последовательности. Вычислить его не удается, поэтому попытаемся оценить его величину. Дальнейшие выкладки будут справедливы для любого вещественного $p > 1$.

Теорема. *Для доли обратимых матриц в кольце* $(\mathbf{Z}/\mathbf{p^k})^{n\times n}$ *верно следующее неравенство*

$$e^{-\frac{p}{(p-1)^2}\left(1-\frac{1}{p^n}\right)} \le \gamma_n(p) \le e^{\frac{1}{1-p}\left(1-\frac{1}{p^n}\right)}. \qquad (1)$$

Доказательство. Обозначим $s_n = \ln \gamma_n = \sum\limits_{t=1}^{n} \ln\left(1 - \frac{1}{p^t}\right)$. Известно, что $\ln(1-x) \le -x$, если $0 \le x < 1$. Значит, $a_n = \ln\left(1 - \frac{1}{p^t}\right) \le -\frac{1}{p^t}$, так как $p > 1$. Тогда $\ln \gamma_n \le -\sum\limits_{t=1}^{n} \frac{1}{p^t} = \frac{1-p^n}{p^n(1-p)} = \frac{1}{1-p}\left(1 - \frac{1}{p^n}\right)$. Откуда $\gamma_n \le e^{\frac{1}{1-p}\left(1-\frac{1}{p^n}\right)}$.

Теперь докажем, что $\ln\left(1 - \frac{1}{p^t}\right) \ge \frac{1}{(1-p)p^{t-1}}$. Действительно, $-\ln\left(1 - \frac{1}{p^t}\right) = \frac{1}{p^t} + \frac{1}{2p^{2t}} + \ldots + \frac{1}{np^{nt}} + \ldots \le \frac{1}{p^t} + \frac{1}{p^{2t}} + \ldots + \frac{1}{p^{nt}} + \ldots = \frac{1}{p^t - 1} = \frac{1}{p^{t-1}\left(p - \frac{1}{p^{t-1}}\right)} \le \frac{1}{p^{t-1}(p-1)}$, так как $p > 1$. Следовательно, $\ln \gamma_n = \sum\limits_{t=1}^{n} \ln\left(1 - \frac{1}{p^t}\right) \ge \frac{1}{1-p} \sum\limits_{t=1}^{n} \frac{1}{p^{t-1}} = \frac{1}{1-p} \cdot \frac{(p^n-1)p}{p^n(p-1)} = -\frac{p}{(p-1)^2}\left(1 - \frac{1}{p^n}\right)$, откуда $\gamma_n \ge e^{-\frac{p}{(p-1)^2}\left(1-\frac{1}{p^n}\right)}$. Теорема доказана.

Так как $\gamma_n(m) = \prod\limits_{i=1}^{s} \gamma_n(m_i)$, то имеет место следующее утверждение.

Следствие 1. *Для доли обратимых матриц* $\gamma_n(m)$ *в кольце* $(\mathbf{Z}/\mathbf{m})^{n\times n}$, *где* $m = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$, *справедливо неравенство*

$$e^{-\sum\limits_{i=1}^{s} \frac{p_i}{(p_i-1)^2}\left(1-\frac{1}{p_i^n}\right)} \le \gamma_n(m) \le e^{\sum\limits_{i=1}^{s} \frac{1}{1-p_i}\left(1-\frac{1}{p_i^n}\right)}.$$

Переходя в неравенстве (1) к пределу при $n \to \infty$, получаем следующее утверждение.

Следствие 2. *Для величины* $\gamma(p) = \lim\limits_{n\to\infty} \gamma_n(p)$ *верно неравенство*

$$e^{-\frac{p}{(p-1)^2}} \le \gamma(p) \le e^{\frac{1}{1-p}}. \qquad (2)$$

Из неравенства (2) при $p = 2$ получаем $0,13 < 1/e^2 \le \gamma(2) \le 1/e < 0,37$. Эта оценка слишком грубая. В [2, стр. 103] приведено неравенство $\gamma_n(2) \ge \frac{1}{4} + \frac{1}{2^{n+1}}$, откуда $\gamma(2) > 0,25$. Тем не менее при больших p неравенство (2) хорошо оценивает величину $\gamma(p)$.

Следствие 3. $\delta = \lim\limits_{p\to\infty} \gamma_n(p) = 1$.

Следствие 3 выражает тот факт, что при стремлении p к бесконечности доля обратимых матриц в кольце $(\mathbf{Z}/\mathbf{p^k})^{n\times n}$ стремится к 1 для любого n. В то время как при стремлении порядка матриц к бесконечности доля обратимых матриц стремится к числу, которое строго больше 0 и строго меньше 1.

Приведем приближенные значения величин $\gamma(p)$ для некоторых простых p: $\gamma(2) \approx 0,288788$, $\gamma(3) \approx 0,560126$, $\gamma(5) \approx 0,760333$, $\gamma(7) \approx 0,836795$, $\gamma(11) \approx 0,900833$.

Заметим, что если рассмотреть последовательность, элементами которой являются произведения последовательных простых чисел $a_s = p_1 \cdot \ldots \cdot p_s$, то $\lim\limits_{s\to\infty} \gamma_n(a_s) = 0$ (это вытекает из следствия 1).

Работа выполнена при частичной финансовой поддержке РФФИ. Код проекта 05-01-00552-а.

Список литературы

1. Farahat H. K. The multiplicative groups of a ring // Math. Zeitsch. — 1965. — V. 87. — P. 378–384.

2. Шевченко В. Н. Качественные вопросы целочисленного программирования — М.: Наука, 1995.

СИНГУЛЯРНЫЙ МНОГОЧЛЕН МАТРИЦЫ ИНЦИДЕНЦИЙ d-МЕРНОГО КУБА

Е. Б. Титова, В. Н. Шевченко (Нижний Новгород)

Обозначим $p\times q$-матрицу, каждый элемент которой равен 1, через $\mathbf{1}^{p\times q}$, единичную матрицу n-го порядка — через E_n. Пусть A —

целочисленная $m \times n$-матрица ($m \le n$), r — ее ранг, $A^\top$ — матрица, транспонированная к A, $A \times B$ — кронекерово произведение матриц A и B (определение и свойства см., например, в [1]).

Обозначим сумму квадратов миноров i-го порядка через $s_i(A) = \sum det^2 A(I,J)$, где суммирование идёт по всем i-элементным подмножествам $I \subseteq \{1,\dots,m\}$ и $J \subseteq \{1,\dots,n\}$, а $A(I,J)$ — подматрица матрицы A, номера строк которой принадлежат подмножеству $I \subseteq \{1,\dots,m\}$, а номера столбцов — подмножеству $J \subseteq \{1,\dots,n\}$. Тогда характеристический многочлен матрицы $AA^\top$

$$det(\lambda E_m - AA^\top) = \sum_{i=0}^{m} (-1)^i s_i(A) \lambda^{m-i} = \lambda^{m-r} \varphi(\lambda, A),$$

где многочлен $\varphi(\lambda, A) = \sum_{i=0}^{r} (-1)^i s_i(A) \lambda^{r-i}$ назовем сингулярным многочленом матрицы A, а его корни — сингулярными числами.

Рассмотрим d-индексную аксиальную транспортную задачу при $n = 2$ (обозначения и определение см., например, в [2]). Ее ограничения-равенства с неотрицательными переменными $t_{j_1,\dots,j_d}$ можно записать следующим образом:

$$\sum_{j_1=1}^{2} \cdots \sum_{j_{i-1}=1}^{2} \sum_{j_{i+1}=1}^{2} \cdots \sum_{j_k=1}^{2} t_{j_1,\dots,j_d} = b_{ij_i}, \qquad (1)$$

где $j_i = 1, 2$; $i = 1, \dots, d$ и b_{ij_i} — заданные неотрицательные числа.

Если ограничения (1) представить в матричном виде $Tt = b$ и лексикографически упорядочить индексы переменных $t_{j_1,\dots,j_d}$ и правых частей уравнений, то нетрудно видеть, что матрица $T = T(d-1, d, 2)$ имеет следующее рекурсивное задание

$$T = T(d-1, d, 2) = \left[\frac{\mathbf{1}^{1\times 2} \times T(d-2, d-1, 2)}{E_2 \times \mathbf{1}^{1\times 2(d-1)}} \right].$$

Обозначим через B_d матрицу, полученную удалением из T всех строк с четными номерами. Очевидно, что B_d состоит из 2^d различных столбцов, которые можно интерпретировать как вершины d-мерного куба C_d, заданного системой неравенств

$$0 \le x_j \le 1 \qquad (1 \le j \le d). \qquad (2)$$

Грань максимальной размерности (фасета) куба C_d есть пересечение C_d с гиперплоскостью $x_i = 0$ или $x_i = 1$. В первом случае будем

называть ее нечетной фасетой и присвоим ей номер $2i-1$, а во втором — четной с номером $2i$.

Утверждение 1. *Матрица T является матрицей инциденций фасеты-вершины d-мерного куба C_d.*

Обозначим через B_{di} матрицу, полученную добавлением к B_d строки матрицы T с номером $2i$.

Утверждение 2. *Для каждого $i = 1, \ldots, d$ матрица B_{di} является строчечной базой (максимальной линейно независимой подсистемой строк) матрицы T.*

Утверждение 3. *Число строчечных баз матрицы T равно $d\ 2^{d-1}$.*

Утверждение 4 [2]. *Базисом из собственных векторов для матрицы $TT^\top$ являются столбцы матрицы $Q_d \times Q_2$, где*

$$Q_i = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & -1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \ldots & -1 \end{pmatrix}$$

— матрица i-го порядка. Сингулярный многочлен матрицы T

$$\varphi(\lambda, T) = (\lambda - 2^{d-1})^d (\lambda - d\ 2^{d-1}).$$

Утверждение 5 [3]. *Базисом из собственных векторов для матрицы $T^\top T$ являются столбцы матрицы Адамара H_d, заданной рекурсивно формулой $H_d = H_1^{<d>} = H_1 \times H_{d-1} = H_1 \times \ldots \times H_1$, где $H_1 = Q_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.*

Зададим матрицу T_d следующим образом: $T_d = \left(\dfrac{\mathbf{1}^{1 \times 2^d}}{B_d} \right)$. Таким образом, будет задан конус, соответствующий выпуклой оболочке куба C_d.

Утверждение 6. *Сингулярные многочлены матриц B_d и T_d вычисляются по следующим формулам*

$$\varphi(\lambda, B_d) = (\lambda - 2^{d-2})^{d-1} (\lambda - (d+1) 2^{d-2}),$$

$$\varphi(\lambda, T_d) = det(\lambda E_{d+1} - T_d T_d^\top) = (\lambda - 2^{d-2})^{d-1} (\lambda^2 - (5+d) 2^{d-2} \lambda + 4^{d-1}).$$

Работа выполнена при частичной финансовой поддержке РФФИ. Код проекта 05-01-00552-а.

Список литературы

1. Воеводин В. В., Кузнецов Ю. А. СМБ. Матрицы и вычисления. — М.: Наука, 1984.

2. Титова Е. Б., Шевченко В. Н. Среднее значение квадрата минора матрицы ограничений аксиальной транспортной задачи // Автоматика и телемеханика. — 2004. — № 2. — С. 113–117.

3. Шевченко В. Н. Многогранники многоиндексных транспортных задач: алгебраический подход. // Материалы конференции "Дискретный анализ и исследование операций" (28 июня – 2 июля 2004). — Новосибирск: Изд-во ин-та математики, 2004. — С. 64–70.

КВАЗИПОРЯДКОВАЯ РАЗМЕРНОСТЬ ЧАСТИЧНО УПОРЯДОЧЕННЫХ МНОЖЕСТВ

В. Ю. Филимонов (Мурманск)

Пусть P — конечное множество. Определим на множестве P частично упорядоченные множества: $Qord(P) = (qord(P), \subseteq)$ — решетка квазипорядков, $Ord(P) = (ord(P), \subseteq)$ — нижняя полурешетка частичных порядков, $Top(P) = (top(P), \subseteq)$ — решетка топологий, $Top_0(P) = (top_0(P), \subseteq)$ — верхняя полурешетка T_0 топологий.

Линейно упорядоченное n-элементное множество будем обозначать $Chain(n)$.

Определим частично упорядоченное множество $(2^U, \subseteq)$ всех подмножеств множества U, которое будем называть булеаном множества U и обозначать $Bul(n)$, где $|U| = n$, $n \geq 0$. Число n назовем рангом булеана.

Инъекция $\varphi : P \to 2^U$ называется вложением частично упорядоченного множества (P, T) в булеан $(2^U, \subseteq)$, если aTb равносильно $\varphi(a) \subseteq \varphi(b)$ для всех $a, b \in P$.

Квазипорядковой размерностью квазиупорядоченного множества (P, Q) (квазипорядка Q), обозначается $\dim_q(P, Q)$ или $\dim_q(Q)$, назовем наименьшее число коатомов решётки $Qord(P)$, пересечение которых равно квазипорядку Q.

Следующая теорема устанавливает связь между квазипорядковой размерностью частично упорядоченного множества (P, T) и наименьшим рангом булеана, в который вложимо частично упорядоченное множество (P, T).

Теорема 1. *Квазипорядковая размерность частичного порядка T равна наименьшему целому числу $m \geq 0$, для которого существует вложение частично упорядоченного множества (P,T) в булеан $Bul(m)$.*

Троттер [1] определил для целого $k \geq 2$ порядковую k-размерность частично упорядоченного множества (P,T) (обозначается $\dim_k(P,T)$ или $\dim_k(T)$) как наименьшее число k-элементных цепей, в прямое произведение которых вложимо частично упорядоченное множество (P,T).

Из теоремы 1 следует, что для частично упорядоченного множества (P,T) справедливо равенство $\dim_2(P,T) = \dim_q(P,T)$. Поэтому порядковую 2-размерность частично упорядоченного множества (P,T) будем также называть квазипорядковой размерностью.

В монографии Айгнера [2] сформулирована теорема о вложении конечной дистрибутивной решетки в булеан. Переформулируем эту теорему в терминах рассматриваемой теории.

Теорема 2. *Квазипорядковая размерность конечной дистрибутивной решетки $(P,\leq)$ равна числу $\vee$-неразложимых, не равных $\widetilde{0}$, элементов решетки $(P,\leq)$.*

Следствие. *Квазипорядковая размерность прямого произведения k конечных цепей $Chain(n_1),...,Chain(n_k)$ равна*

$$(\sum_{i=1}^{k} n_i) - k, \text{ где } n_i \geq 1,\ k \geq 1.$$

Теорема 3. *Пусть (P,T) — частично упорядоченное множество, $|P| \geq 2$, $u \in P$, T' — сужение отношения T на множество $P - \{u\}$. Тогда $\dim_2(P,T) \leq 2 + \dim_2(P - \{u\},T')$.*

Теорема 4. *Пусть (P,T) — частично упорядоченное множество, u — изолированная вершина, T' — сужение отношения T на множество $P - \{u\}$. Справедливы формулы:*

1. $\dim_2(P,T) = 1 + \dim_2(P - \{u\},T')$, *если* $\tilde{0} \in P - \{u\}$ *либо* $\tilde{1} \in P - \{u\}$.

2. $\dim_2(P,T) = 2 + \dim_2(P - \{u\},T')$, *если* $\tilde{0},\tilde{1} \in P - \{u\}$.

Теорема 5. *Если в частично упорядоченном множестве (P,T) для некоторого $u \in P$ существуют единственные $a,b \in P$ такие что $a \lessdot u \lessdot b$, то $\dim_2(P,T) \leq 1 + \dim_2(P - \{u\},T')$, где $\lessdot$ — отношение покрытия, порожденное частичным порядком T, T' — сужение отношения T на множество $P - \{u\}$.*

Другие результататы, подобные теоремам 2–5, можно найти в монографии Троттера [3].

Далее, пусть P — конечное n-элементное множество, $n,\ m,\ k$ — натуральные числа.

Теорема 6. $\mathrm{Dim}_2 Ord(P) = n(n-1)$.

Следствие 1. $\mathrm{Dim}_2 Qord(P) = \dim_2 Top(P) = \dim_2 Top_0(P) = n(n-1)$.

Пусть $(\{\tilde{0},\tilde{1}\},\leq)$ — решетка. Обозначим $\{\tilde{0},\tilde{1}\}^{m\times n}$ множество всех $m \times n$ матриц с элементами из $\{\tilde{0},\tilde{1}\}$. Для любых матриц $A \in \{\tilde{0},\tilde{1}\}^{m\times k}, B \in \{\tilde{0},\tilde{1}\}^{k\times n}$ положим $A \cdot B = AB = C_{m\times n}$, где $i = 1,...,m,\ j = 1,...,n$

$$c_{ij} = \bigvee_{r=1}^{k}(a_{ir} \wedge b_{rj}).$$

Квадратная матрица $A \in \{\tilde{0},\tilde{1}\}^{n\times n}$ называется идемпотентной, если $A^2 = A \cdot A = A$. Множество идемпотентных $n \times n$ матриц над решеткой $(\{\tilde{0},\tilde{1}\},\leq)$ будем обозначать $idemp_n(\{\tilde{0},\tilde{1}\},\leq)$. Определим частично упорядоченное множество идемпотентных матриц $Idemp_n(\{\tilde{0},\tilde{1}\},\leq) = (idemp_n(\{\tilde{0},\tilde{1}\},\leq),\leq)$ относительно частичного порядка индуцированного множеством $(\{\tilde{0},\tilde{1}\}^{n\times n},\leq)$. Свойства решетки $Idemp_n(\{\tilde{0},\tilde{1}\},\leq)$ рассмотрены в работе [3].

Следствие 2. $\mathrm{Dim}_2 Idemp_n(\{\tilde{0},\tilde{1}\},\leq) = n^2$.

Работа выполнена в соответствии с тематическим планом научно-исследовательских работ Федерального агентства по образованию (тема 1.3.07).

Список литературы

1. Trotter W. T. Embedding finite posets in cubes // Discrete Math. — 1975. — V. 12. — P. 165–172.

2. Айгнер М. Комбинаторная теория. —М.: Мир, 1982.

3. Trotter W. T. Combinatorics and partially ordered sets: dimension theory. — John Hopkins University Press, 1992.

4. Кумаров В. Г. Решетка идемпотентных матриц над дистрибутивными решетками. — Препринт.

5. Dushnik B., Miller E. W. Partially ordered sets // Amer. J. Math. — 1941. — V. 63. — P. 600–610.

6. Hiraguchi T. On the dimension of partially ordered sets // Science Report of the Kanazawa University. — 1951. — V. 1. — P. 77–94.

7. Оре О. Теория графов. — М.: Наука, 1980.

8. Kelly D., Trotter W. T. Dimension theory for ordered sets // Ordered Sets. — Dordrecht: Reidel, 1982. — P. 171–211.

ОБ ЭКСТРЕМАЛЬНЫХ ХАРАКТЕРИСТИКАХ РАВНОМЕРНЫХ ГИПЕРГРАФОВ

Д. А. Шабанов (Москва)

В докладе рассматривается классическая задача экстремальной теории гиперграфов. Впервые эта задача была поставлена П. Эрдешем в 60-е годы следующим образом: найти величину $m(n)$, равную наименьшему возможному числу ребер у n-равномерных гиперграфов с хроматическим числом больше двух. Напомним, что гиперграф *n-равномерен*, если каждое его ребро содержит ровно n вершин, а *хроматическим числом* гиперграфа называется минимальное число цветов, которое требуется для такой раскраски множества вершин гиперграфа, чтобы в ней все ребра гиперграфа были неодноцветны.

Известны следующие оценки величины $m(n)$. Сам Эрдеш [1, 2] с помощью несложного вероятностного метода показал, что

$$2^{n-1} \le m(n) \le (1+o(1))\frac{e\ln 2}{4}n^2 2^n.$$

Позднее нижняя оценка была улучшена Дж. Беком [3]. Он установил асимптотическое неравенство $m(n) \ge C(\delta)2^n n^{\frac{1}{3}-\delta}$, где δ может быть выбрано сколь угодно малым ($C(\delta) > 0$ — некоторая константа). Наконец Дж. Радхакришнан и А. Сринивазан обосновали следующий результат [4]:

$$m(n) \ge c2^n \left(\frac{n}{\ln n}\right)^{\frac{1}{2}},$$

где c — произвольная константа из интервала $(0, \sqrt{2}^{-1})$. Этот результат остается наилучшим из известных на сегодняшний день.

В докладе мы представим более общую постановку задачи и некоторые новые результаты, полученные в этой более общей задаче. Пусть k — натуральное число. Скажем, что гиперграф обладает свойством B_k, если существует такая раскраска множества его вершин в два цвета, при которой в любом его ребре окажется не менее k вершин каждого из этих цветов. Отметим также, что параметр k, вообще говоря, зависит от n и, соответственно, может расти с ростом n. При этом, конечно, $k(n) \le \frac{n}{2}$. Через $m_k(n)$ мы обозначим минимум из всех таких m, что существует n-равномерный гиперграф, имеющий m ребер и не обладающий свойством B_k. Ясно, что $m(n) = m_1(n) \ge m_2(n) \ge \ldots$

В работах [5, 6] были получены оценки величины $m_k(n)$. Если $k^2 = O(\ln n)$, то при больших n

$$m_k(n) \geq c_1 \left(\frac{n}{\ln n}\right)^{\frac{1}{3}} \frac{2^n}{C_n^{k-1}}$$

для некоторой константы $c_1 > 0$. Верхняя оценка была найдена при более слабых условиях на функцию $k = k(n)$. Если $k = o(\frac{n}{\ln n})$, то

$$m_k(n) \leq (1 + o(1)) \frac{e \ln 2}{4} n^2 \frac{2^n}{C_n^{k-1}}.$$

Новый результат улучшает известную ранее нижнюю оценку, расширяя при этом область значений параметра k. Выполнена

Теорема 1. *Пусть задана целочисленная функция $k = k(n)$ и число $\delta \in (0, (\ln 2 + \frac{1}{2})^{-1})$. Пусть число $c > 0$ удовлетворяет неравенству $c(1-\delta)^{-1} + \frac{c^2}{2} < 1$. Если функция k удовлетворяет неравенству*

$$k - 1 \leq \frac{\delta \ln\left(\frac{n}{\ln n}\right)}{2 + 4\delta}$$

для всех $n \geq N_0$, тогда существует такое натуральное число N_1, что для всех $n \geq N_1$

$$m_k(n) \geq c \left(\frac{n}{\ln n}\right)^{\frac{1}{2}} \frac{2^{1-k} e^{-\frac{k}{2}}}{\sqrt{2k-1}} \frac{2^{n-1}}{C_n^{k-1}}.$$

Из теоремы 1 следует, что в случае $k = o(\ln n)$, величина $m_k(n)$ оценивается снизу выражением вида $\Omega\left(n^{\frac{1}{2}} e^{o(\ln n)} \frac{2^{n-1}}{C_n^{k-1}}\right)$. В случае, если функция k имеет порядок роста $\ln n$ (для таких k ранее не было получено нетривиальных нижних оценок), оценка имеет вид $\Omega\left(n^{\frac{1}{2}-\varepsilon} \frac{2^{n-1}}{C_n^{k-1}}\right)$, где ε — некоторая константа из интервала $(0, \frac{1}{2})$.

В подобных задачах бывает интересно ограничить множество рассматриваемых гиперграфов некоторым определенным классом и искать экстремальные характеристики уже на новом множестве. Например, можно рассматривать "простые" гиперграфы (нет пересечений ребер мощности 2 и больше). Обратным свойством к данному является свойство A_h, где h — натуральное число. Скажем, что гиперграф обладает свойством A_h, если любые его ребра либо не пересекаются, либо пересекаются не менее, чем по h вершинам. Введем

величину $m_{k,h}(n)$ как минимум из всех таких m, что существует n-равномерный гиперграф, обладающий свойством A_h, имеющий m ребер и не обладающий свойством B_k. При каких соотношениях параметров k и h эта величина имеет смысл? Ответ дает следующая простая теорема.

Теорема 2. *Если гиперграф обладает свойством A_{2k} и каждое его ребро содержит не менее $2k$ вершин, то этот гиперграф обладает свойством B_k.*

Из теоремы 2 следует, что имеет смысл рассматривать только случай $h < 2k$. В таких условиях была получена [5, 6] нижняя оценка величины $m_{k,h}(n)$ при $k^2 = O(h \ln n)$:

$$m_{k,h}(n) = \Omega\left(\left(\frac{3n}{2h\ln n}\right)^{\frac{h}{3}} \frac{2^{n-1}}{C_n^{k-1}}\right).$$

Работа выполнена при финансовой поддержке РФФИ (грант 06-01-00383).

Список литературы

1. Erdös P. On a combinatorial problem, I // Nordisk Mat. Tidskr. — 1963. — V. 11. — P. 5–10.

2. Erdös P. On a combinatorial problem, II // Acta Math. Acad. Sci. Hungar. — 1964. — V. 15. — P. 445–447.

3. Beck J. On 3-chromatic hypergraphs // Disc. Math. — 1978. — V. 24. — P. 127–137.

4. Radhakrishnan J., Srinivasan A. Improved bounds and algorithms for hypergraph two-coloring // Random Structures and Algorithms. — 2000. — V. 16. — P. 4–32.

5. Шабанов Д. А. Об одной комбинаторной задаче Эрдеша // Доклады РАН. — 2004. — Т. 396, вып. 2. — С. 166–169.

6. Шабанов Д. А. Экстремальные задачи для раскрасок равномерных гиперграфов // Известия РАН. — 2007. — Т. 71, вып. 5.

Подсекция «Теория графов»

НЕКОТОРЫЕ ОЦЕНКИ ДЛЯ ДИАМЕТРА ГРАФА

А. С. Богомолов (Саратов)

Расстоянием между вершинами неориентированного графа называется длина кратчайшей простой цепи между ними. Диаметром графа называется максимальное расстояние между его вершинами. В работе предлагаются оценки диаметра графа в зависимости от количества его ребер.

Граф — пара $G = (S, D)$, где S — непустое множество из m вершин, D — множество из n ребер, неупорядоченных пар различных элементов S [1]. Расстоянием между вершинами s и t графа G называется длина кратчайшей простой цепи между ними, т. е. последовательность неповторяющихся вершин и ребер (если цепи не существуют, то расстояние полагают бесконечным). Диаметром графа называется наибольшее расстояние между его вершинами. Граф с конечным диаметром называется связным.

Теорема 1. *Если количество ребер графа* $n > \frac{1}{2}(m-1)(m-2)$, *то его диаметр не превышает* 2. *Существует несвязный граф с* $n = \frac{1}{2}(m-1)(m-2)$.

Теорема 2. *Если в графе степень каждой вершины не менее* $d > 0$, *и при этом* $n > \frac{1}{2}(m-2)(m-3) - d^2 + 2d$, *то диаметр графа не превышает* 3. *При этом если* $m > 2d+1$, *то существует граф с* $n = \frac{1}{2}(m-2)(m-3) - d^2 + 2d$ *ребрами диаметра более трех*

Замечание. Если $m < 2d + 2$, то диаметр графа всегда не превышает 2 без дополнительных условий на n.

Список литературы

1. Харари Ф. Теория графов. — М.: Мир, 1973.

РЕШЕНИЕ ЗАДАЧИ РАЗВОЗКИ МЕТОДОМ ЛИТТЛА

И. Ф. Борханов, В. Р. Фазылов (Казань)

В докладе предлагается точный метод решения задачи развозки, известной как CVRP. Метод является модификацией метода Литтла для задачи коммивояжера, в ходе которого матрица стоимостей изменяется в соответствии с требованиями решаемой задачи.

Даны n пунктов $V = \{1, \ldots, n\}$, где пункт с номером 1 является базовым. В базовом пункте имеются одинаковые транспортные средства вместимостью D. Для каждой пары пунктов (i, j) задана стоимость переезда c_{ij}, а для каждого небазового пункта задан неотрицательный объем заявки d_i $(i = 2, \ldots, n)$. Требуется построить такой набор маршрутов наименьшей суммарной стоимости, чтобы каждый маршрут начинался и заканчивался в базовом пункте, каждый небазовый пункт был обслужен только один раз, и суммарная загрузка по любому маршруту (сумма заявок пунктов маршрута) не должна превышать D.

Одним из путей сведения задачи развозки к задаче коммивояжера является расширение матрицы стоимостей введением нескольких дубликатов базового пункта. Но так как заранее неизвестно, сколько маршрутов содержит оптимальное решение задачи, то и неизвестно, сколько дублей базового пункта нужно добавить. Поэтому такой подход представляется неперспективным, если в дальнейшем применить к модифицированной указанным выше способом задаче метод Литтла.

Предлагаемый в докладе подход заключается в замене по мере необходимости стоимости переезда c_{ij} из пункта i в пункт j на стоимость транзитного переезда через базовый пункт: $c_{i1} + c_{1j}$. Такие дуги будем называть *модифицированными*.

Рассмотрим процедуру модификации матрицы стоимостей подробнее. Рассмотрим произвольный узел дерева просмотра решений в методе Литтла, ему соответствует некоторый набор зафиксированных дуг. Зафиксированные дуги образуют цепочки, концы которых характеризуются определенными суммарными загрузками. Заметим, что если цепочка не содержит модифицированные дуги или базовый пункт, то суммарные загрузки на концах цепочки будут совпадать. В противном случае они могут быть различными.

Далее рассматриваются все дуги между небазовыми пунктами, входящие в начало и исходящие из концов всех цепочек. Если очередная рассматриваемая дуга $i \to j$ не модифицирована и при присоединении ее к соответствующей цепочке нарушится ограничение на вместимость транспортного средства, то ее стоимость c_{ij} заменяем

на $c_{i1} + c_{1j}$. Это изменение будет действительно для всех порожденных узлов текущего узла дерева перебора решений.

Описанный метод был реализован и апробирован на известных тестовых задачах размера до 30 пунктов, размещенных в сети Интернет по адресу: http://neo.lcc.uma.es/radi-aeb/WebVRP//data//instances/Christ-Eilon/CE-VRP.zip. Максимальное время счета на компьютере Pentium 4 (3.0 Ггц, 512 Мб ОЗУ) не превышало одного часа.

ОПЕРАЦИОННЫЕ БАЗИСЫ ЗАМКНУТЫХ КЛАССОВ ГРАФОВ

Е. В. Бурков (Нижний Новгород)

Рассматриваются конечные неориентированные графы, допускающие петли и кратные ребра. К ним применяются операции *склейки* — объединения графов с отождествлением их изоморфных подграфов (подграфов склейки). Пусть P — множество графов, обладающих некоторым заданным свойством, H — система ограничений на операции склейки, обеспечивающая сохранение заданного свойства графов-операндов. Операции склейки, удовлетворяющие системе ограничений H, называются операциями *H-склейки*. Граф G является *H-суперпозицией* графов из P, если G принадлежит P, или может быть получен из графов множества P с помощью операций H-склейки. Процесс построения графа G определяет операцию H-суперпозиции графов из P. Множество $[P]_H$ всех графов, получаемых из P с помощью операций H-суперпозиции, образует *H-замыкание* P. Если $[P]_H = P$, то P является *H-замкнутым* классом графов. Минимальное по включению подмножество B_E графов из P образует *элементный базис* H-замкнутого класса P, если $[B_E]_H = P$. Операции H-склейки относятся к одному *типу*, если их подграфы склейки изоморфны. Множество типов операций H-склейки, достаточное для построения из B_E с помощью операций H-суперпозиции всех графов H-замкнутого класса P, образует *полную* систему операций H-склейки. Минимальная по включению полная система операций H-склейки образует *операционный базис* H-замкнутого класса P. Операционный базис задается множеством подграфов склейки. Совокупность системы ограничений H, элементного базиса B_E и операционного базиса B_O образует конструктивное описание H-замкнутого класса P.

В [1] доказано существование и единственность элементного базиса для любого H-замкнутого класса графов P. В данной работе рассматривается вопрос о существовании операционного базиса для любого H-замкнутого класса графов P.

Поставим каждому графу G во взаимно однозначное соответствие натуральное число $N(G)$ так, чтобы никакой граф с большим номером не являлся подграфом графа с меньшим номером. Обозначим $G(N)$ граф, соответствующий числу N. Далее поставим каждому H-замкнутому классу графов P в соответствие характеристическую дробь $0,\alpha_1\alpha_2\ldots\alpha_N\ldots$, где $\alpha_N = 1$, если $G(N)\in P$, иначе $\alpha_N = 0$. Так как каждая система операций склейки характеризуется множеством типов операций, получаем соответствие систем операций склейки десятичным дробям. Теперь можно говорить об инфинуме множества систем операций.

Лемма. *Для любого множества A полных систем операций инфинум A также является полной системой операций.*

Доказательство. Рассмотрим произвольный H-замкнутый класс графов P. Пусть B_E его элементный базис . По определению полной системы операций, для любой системы $a\in A$ выполняется $[B_E]_a = P$. На систему a можно смотреть как на множество типов операции склейки, соответствующих некоторому вещественному числу. Предположим, что система операций $\inf A$ неполна. Тогда существует граф $G\in P\setminus[B]_{\inf A}$. Из определения инфинума следует, что в A найдется система операций, которой соответствует характеристическая дробь, не превосходящая $(\inf A + 10 - N(G) - 1)$. Графы — типы операций — с номерами, большими $N(G)$, не являются подграфами G, а, следовательно, не могут быть использованы при его построении. Так как система операций полна, с ее помощью можно построить граф G, а значит, его можно построить и с помощью операций из $\inf A$, и $G\in[B]_{\inf A}$. Полученное противоречие доказывает лемму.

Теорема. *Каждый H-замкнутый класс графов P имеет операционный базис.*

Доказательство. Рассмотрим произвольный H-замкнутый класс графов P. Множество всех полных систем операций для данного класса графов не пусто, так как содержит, по крайней мере, систему всех операций. Пусть $\tilde{a}$ — инфинум этого множества. Система $\tilde{a}$ является полной системой операций по лемме. Система $\tilde{a}$ минимальна по включению, так как любое собственное подмножество соответствует меньшему числу, а полной системы операций, соответствующей меньшему числу, не существует. Следовательно, $\tilde{a}$ является операционным базисом. Теорема доказана.

В работе [2] для замкнутого класса эйлеровых планарных графов было установлено наличие двух различных операционных базисов. Таким образом, справедливо

Следствие. *Каждый H-замкнутый класс графов P имеет хотя бы один операционный базис.*

Список литературы

1. Иорданский М. А. Конструктивные описания графов // Дискретный анализ и исследование операций. — 1996. — Т. 3, № 4. — С. 33–63.

2. Иорданский М. А., Бурков Е. В. Конструктивные описания эйлеровых планарных графов // Дискретные модели в теории управляющих систем: VI Международная конференция: Москва, 7–11 декабря 2004 г. Труды. — М.: Изд. отдел факультета ВМК МГУ, 2004. — С. 167–169.

КОЛИЧЕСТВО РЕБЕР В k-ПОЧТИ ПЛАНАРНЫХ ГРАФАХ

В. А. Васильченко (Санкт-Петербург)

Всевозможные приближения к планарным графам — почти планарные графы вводились и изучались в течение долгого времени. При этом каждый автор подразумевает под этим термином что-то своё (см., например, [1, 2]), поэтому сразу оговорим, что мы пользуемся следующим определением.

Определение. Назовём граф G *k-почти планарным* $(k \geq 0)$, если у G нет петель и кратных рёбер, и его можно *нормально изобразить* на плоскости так, что любое ребро будет иметь не более k пересечений с другими рёбрами (определение нормального изображения см., например, в [3]). Очевидно, что 0-почти планарный граф — это просто планарный граф.

Нас интересует вопрос: как оценить сверху количество рёбер k-почти планарного графа через количество его вершин. Из формулы Эйлера для полиэдров, очевидно, следует, что при $k = 0$ имеется оценка $e \leq 3v-6$, которая достигается триангуляцией сферы. Также легко доказывается, что при $k = 1$ имеется оценка $e \leq 4v-8$, которая достигается разбиением сферы на четырёхугольники, в каждом из которых проведены обе диагонали.

В работе [4] мы доказали следующую теорему.

Теорема. *Для 2-почти планарного графа имеет место оценка* $e \leq 5v - 10$.

Приведенная в теореме оценка для 2-почти планарного графа достигается при $v \equiv 2 \pmod 3$ разбиением сферы на пятиугольники, в каждом из которых проведены все диагонали (при $v \equiv 1, 3 \pmod 3$ точной оценкой является $e \leq 5v - 11$).

Естественно, возникает вопрос о том, какие будут оценки при больших значениях k. Методы работы [4] не продолжаются для больших значений k. Оказывается, что при больших значениях k асимптотика количества ребер будет иметь порядок $\sqrt{k} \cdot v$. А именно, используя результаты работ [4–6] можно доказать, что при $k \geq 2$ имеет место следующая оценка сверху на количество рёбер в k-почти планарном графе: $e \leq \sqrt{\frac{243}{8}}\sqrt{k}v$. При этом строятся примеры, также имеющие порядок $\sqrt{k}v$. Однако, точных оценок для $k \geq 3$ пока не известно.

Заметим, что, при рассмотрении случаев $k = 0, 1, 2$, каждый раз, наложив определённые дополнительные условия, удавалось при доказательстве оценки сверху сразу получить пример, на котором эта оценка достигается. Причём этот пример обязательно оказывался разбиением сферы на некоторые n-угольники.

Предположим, что для некоторого значения k для любого v удаётся таким образом выбрать k-почти планарный граф на v вершинах с максимальным количеством рёбер (среди всех k-почти планарных графов на v вершинах), что некоторое его изображение (удовлетворяющее условию k-почти планарности) будет обладать следующим свойством: при одновременном выкидывании всех рёбер, имеющих пересечения, оставшийся граф оказывается связным. Тогда для этого значения k можно получить оценку сверху на количество ребер, решив следующую задачу (уже чисто комбинаторную): При фиксированых k и v найти максимум выражения $\frac{1+r_k(n)}{n-2}$ по всем $n = 1, \ldots, 2v$, где $r_k(n)$ — максимальное количество диагоналей (прямолинейных отрезков), которые можно провести в выпуклом n-угольнике так чтобы каждая имела не более k пересечений с другими диагоналями. Причём, если максимум достигается на некоторых $n_1, \ldots, n_j$ и при этом возможно замостить сферу несколькими копиями n_i-угольников ($i = 1, \ldots, j$) так, что требуемые диагонали не будут повторяться в разных многоугольниках (например, если каждый многоугольник имеет не более одной общей стороны с другими), тогда полученная оценка оказывается точной.

Исследования поддержаны грантом Президента РФ, проект НШ-8464.2006.1.

Список литературы

1. Bodendiek R., Wagner K. On almost-planar graphs // Graphentheorie und ihre Anwendungen. — 1988. — P. 9–12.
2. Wagner K. Fastplattbare graphen // Combinatorial theory. — 1967. — V. 3. — P. 326–365.
3. Szekely L. A. A successful concept for measuring non-planarity of graphs: the crossing number // Discrete Math. — 2004. — V. 276. — P. 331–352.
4. Васильченко В. А. Оценка количества рёбер в дважды почти планарном графе // Препринт ПОМИ, — № 03-2007.
5. Ajtai M., Chvatal V., Newborn M., Szemeredi E. Crossing-free subgraphs // Ann. Discrete Math. — 1982. — V. 12. — P. 9–12.
6. Leighton F. T. Complexity issues in VLSI. — Cambridge: MIT Press, 1983.

РЕШЕНИЕ УРАВНЕНИЯ СЕЛКОВА ДЛЯ ЭНУМЕРАТОРА ПОМЕЧЕННЫХ СВЯЗНЫХ ГРАФОВ ПО ЧИСЛУ ТОЧЕК СОЧЛЕНЕНИЯ

В. А. Воблый (Москва)

Обозначим через S_{mn} число помеченных связных графов с n вершинами, из которых m — точки сочленения, а через $S_m(z)$ — производящую функцию: $S_m(z) = \sum_{n=2}^{\infty} S_{mn}\frac{z^n}{n!}$. Пусть $S(x,z) = \sum_{m=0}^{\infty} S_m(z)x^m$, а $B(z) = \sum_{n=2}^{\infty} B_n\frac{z^n}{n!}$, где B_n — число помеченных блоков с n вершинами.

Селков [1] вывел следующее уравнение для $S(x,z)$:

$$z\frac{\partial S}{\partial z} - x\frac{\partial S}{\partial x} = zB'\left(z + xz\frac{\partial S}{\partial z} + x(1-x)\frac{\partial S}{\partial x}\right). \qquad (1)$$

В уравнении (1) сделаем замену переменной $u = xz, v = z$; $P(u,z) = S(u/z,z)$, $S(x,z) = P(xz,z)$; тогда имеем:

$$\frac{\partial S}{\partial x} = \frac{\partial P}{\partial u}\frac{\partial u}{\partial x} + \frac{\partial P}{\partial v}\frac{\partial v}{\partial x} = z\frac{\partial P}{\partial u}, \quad \frac{\partial S}{\partial z} = \frac{\partial P}{\partial u}\frac{\partial u}{\partial z} + \frac{\partial P}{\partial v}\frac{\partial v}{\partial z} = x\frac{\partial P}{\partial u} + \frac{\partial P}{\partial z}$$

и, следовательно, $z\frac{\partial S}{\partial z} - x\frac{\partial S}{\partial x} = z\frac{\partial P}{\partial z}$. После подстановки в уравнение (1) и сокращения на z получим

$$\frac{\partial P}{\partial z} = B'\left(z + u\frac{\partial P}{\partial u} + u\frac{\partial P}{\partial z}\right). \qquad (2)$$

Теорема. *Функция* $P(u,z) = \sum_{m=0}^{\infty} P_m(z)u^m$, *где*

$$P_0(z) = B(z), P_1(z) = e^{B'(z)} - B'(z) - 1,$$

$$P_m(z) = \frac{1}{m!}\left(B''(z)\left(e^{B'(z)} - 1\right)^m\right)^{(m-2)}, \quad m \geq 2,$$

удовлетворяет модифицированному уравнению Селкова (2).

Доказательство. Найдем частные производные 1-го порядка функции $P(u,z)$:

$$\frac{\partial P}{\partial z} = \sum_{m=0}^{\infty} P_m'(z)u^m, \ \frac{\partial P}{\partial u} = \sum_{m=1}^{\infty} mP_m(z)u^{m-1} = \sum_{m=0}^{\infty}(m+1)P_{m+1}(z)u^m.$$

Следовательно,

$$\frac{\partial P}{\partial z} + \frac{\partial P}{\partial u} = \sum_{m=0}^{\infty}(P_m'(z) + (m+1)P_{m+1}(z))u^m.$$

Выделим в сумме слагаемые для $m = 0$, $m = 1$ и подставим выражения для $P_0(z), P_1(z)$ и $P_m(z)$ при $m \geq 2$:

$$\frac{\partial P}{\partial z} + \frac{\partial P}{\partial u} = B'(z) + e^{B'(z)} - B'(z) - 1 + e^{B'(z)}B''(z)u - B''(z)u +$$

$$B''(z)\left(e^{B'(z)} - 1\right)^2 u + \sum_{m=2}^{\infty}(P_m'(z) + (m+1)P_{m+1}(z))u^m = e^{B'(z)} - 1$$

$$+B''(z)e^{B'(z)}\left(e^{B'(z)} - 1\right)u + \sum_{m=2}^{\infty}\left(\frac{1}{m!}\left(B''(z)\left(e^{B'(z)} - 1\right)^m\right)^{(m-1)}\right)$$

$$+\frac{m+1}{(m+1)!}\left(B''(z)\left(e^{B'(z)} - 1\right)^{m+1}\right)^{(m-1)}u^m.$$

Приводя подобные члены под знаком суммы, получаем:

$$\frac{\partial P}{\partial z}+\frac{\partial P}{\partial u}=e^{B'(z)}-1+B''(z)e^{B'(z)}\left(e^{B'(z)}-1\right)u+$$

$$+\sum_{m=2}^{\infty}\frac{1}{m!}\left(B''(z)e^{B'(z)}\left(e^{B'(z)}-1\right)^{m}\right)^{(m-1)}u^{m}=$$

$$=e^{B'(z)}-1+\sum_{m=1}^{\infty}\frac{1}{m!}\left(B''(z)e^{B'(z)}\left(e^{B'(z)}-1\right)^{m}\right)^{(m-1)}u^{m}.$$

Поскольку

$$B''(z)e^{B'(z)}\left(e^{B'(z)}-1\right)^{m}=\frac{1}{m+1}\left(\left(e^{B'(z)}-1\right)^{m+1}\right)',$$

имеем:

$$\frac{\partial P}{\partial z}+\frac{\partial P}{\partial u}=e^{B'(z)}-1+\sum_{m=1}^{\infty}\frac{1}{(m+1)!}\left(\left(e^{B'(z)}-1\right)^{m+1}\right)^{(m)}u^{m}=$$

$$=\sum_{m=0}^{\infty}\frac{1}{(m+1)!}\left(\left(e^{B'(z)}-1\right)^{m+1}\right)^{(m)}u^{m},$$

и, следовательно, после сдвига индекса суммирования получим

$$u\left(\frac{\partial P}{\partial z}+\frac{\partial P}{\partial u}\right)=\sum_{m=1}^{\infty}\left(\left(e^{B'(z)}-1\right)^{m}\right)^{(m-1)}u^{m}.$$

Известна теорема Лагранжа [2, с. 186]:

$$f(x)=f(z)+\sum_{m=1}^{\infty}\frac{1}{m!}u^{m}\left[f'(z)\phi^{m}(z)\right]^{(m-1)},$$

где $x=z+u\phi(z)$. В нашем случае $f(x)=x,\phi(x)=e^{B'(x)}-1$, поэтому $z+u\left(\frac{\partial P}{\partial z}+\frac{\partial P}{\partial u}\right)=x$, где $x=z+u\left(e^{B'(x)}-1\right)$ и правая часть уравнения (2) равна $B'(x)$. С другой стороны,

$$\frac{\partial P}{\partial z}=B'(z)+B''(z)\left(e^{B'(z)}-1\right)u+$$

$$+\sum_{m=2}^{\infty}\frac{1}{m!}\left(B''(z)\left(e^{B'(z)}-1\right)^m\right)^{(m-1)}u^m=$$

$$=B'(z)+\sum_{m=1}^{\infty}\frac{1}{m!}\left(B''(z)\left(e^{B'(z)}-1\right)^m\right)^{(m-1)}u^m.$$

Применяя опять теорему Лагранжа, где $f(x)=B'(x)$, $\phi(x)=e^{B'(x)}-1$, $x=z+u\left(e^{B'(x)}-1\right)$, получим, что левая часть уравнения (2) также равна $B'(x)$. Теорема доказана.

Очевидно, $S_m(z)=z^mP_m(z)$. В работе автора [3] дано комбинаторное доказательство формулы для $S_m(z)$.

Список литературы

1. Selkow S. M., The enumeration of labeled graphs by number of cutpoints // Discrete Math. — 1998. — V. 185. — P. 183–191.

2. Уиттекер Э. Т., Ватсон Дж. Курс современного анализа, т. I. — М.: ГИФМЛ, 1963.

3. Воблый В. А. О перечислении помеченных связных графов по числу точек сочленения //Дискретная математика. — 2007. — (В печати).

ПОСТРОЕНИЕ ОСТОВНОГО ДЕРЕВА ГРАФА С БОЛЬШИМ КОЛИЧЕСТВОМ ЛИСТЬЕВ

Н. В. Гравин (Санкт-Петербург)

В. Г. Визинг [1] в 1968 году поставил проблему поиска в связном графе остовного дерева с наибольшим числом висячих вершин. В 1973 году в [2] предложен алгоритм выделения в связном графе дерева с масимально возможным количеством висячих вершин. Известно, что задача поиска в связном графе остовного дерева с наибольшим количеством висячих вершин является NP-полной даже в классе кубических графов.

Определение. Определим $L(G)$, как максимум количества висячих вершин в остовных деревьях графа G.

В 1981 году в работе [3] заявлено, что $L(G)\geq\frac{1}{4}N+2$ для всех 3-регулярных графов на N вершинах. Затем Линьял выдвинул гипотезу, что $L(G)\geq\frac{k-2}{k+1}N+c_k$ для графов с минимальной степенью

хотя бы k, где c_k зависит только от k. В работе [4] была доказана гипотеза для $k = 4, k = 5$ (для $k = 3$ гипотеза была доказана еще раньше в работе [5] с помощью метода "мертвых вершин"). Там же, в работе [4], построена бесконечная серия примеров показывающая, что эта оценка асимптотически точна для $k = 4, k = 5, k = 3$ и $c_k = 2$.

Основным результатом работы [6] является:

Теорема. Если в произвольном графе G есть k вершин степени хотя бы четыре и k' вершин степени три, то можно выделить остовное дерево с количеством висячих вершин по крайней мере $\lceil \frac{2}{5} \cdot k + \frac{2}{15} \cdot k' \rceil$.

В работе [6] оценка доказывается для *произвольного* графа, в отличие от предыдущих работ, без ограничений на минимальную степень. Таким образом, если пытаться оценить $L(G)$ через количество вершин степени хотя бы 4, то вершины степени 2 и 1 "не мешают" в этой оценке, а вершины степени 3 даже немного увеличивают количество висячих вершин. Из работы [4] следует, что коэффициент $\frac{2}{5}$ асимптотически точен. В работе [6] предъявляется алгоритм, работающий полиномиальное время, на выходе выдающий остовное дерево, количество висячих вершин которого удовлетворяет неравенству из условия теоремы.

Определение. *Помеченным графом* $\widetilde{G}$ является пара (G, S), где G это граф, а $S \subset V(G)$, при этом подмножество вершин S графа G назовем *помеченными вершинами*.

Оказывается, что проводить рассуждения связанные с понятием остовного леса в категории *помеченных графов* удобнее, чем в категории обычных графов. Действительно, наличие множества *помеченных вершин* позволяет проводить индукционные рассуждения для построения остовного дерева, так как для этого достаточно на каждом шаге индукции строить остовный лес, у которого все корни деревьев помеченные вершины. Благодаря этой идее в работе [6] получен новый результат.

Список литературы

1. Визинг В. Г. Некоторые нерешенные задачи в теории графов // Успехи мат. наук. — 1968. — Т. 23. — С. 117–134.

2. Zelinka B. Finding a spanning tree of a graph with maximal number of terminal vertices // Kybernetika. — 1973. — V. 9, № 5. — P. 357–360.

3. Storer J. A. Constructing full spanning trees for cubic graphs // Inform. Process. Lett. — 1981. — V. 13, № 1. — P. 8–11.

4. Storer J., Griggs R., Mingshen Wu. Spanning trees in graphs of

minimum degree 4 or 5 // Discreet Mathematics. — 1992. — V. 104. — P. 167–183.

5. Kleitman D. J., West D. B. Spanning trees with many leaves // SIAM J. Discrete Math. — 1991. — V. 4, №1. — P. 99–106.

6. Гравин Н. В. Построение остовного дерева графа с большим количеством листьев. — Препринт ПОМИ. — № 4–2007.

КОНТРОЛЬНЫЙ ЭКСПЕРИМЕНТ С ШАХМАТНЫМИ ЛАБИРИНТАМИ

В. И. Грунская, М. Ю. Тихончев (Димитровград)

Рассматривается задача построения контрольного эксперимента для произвольного шахматного лабиринта и класса шахматных лабиринтов. Эти лабиринты наиболее часто используются в области исследований поведения автоматов в лабиринтах [1]. Построение контрольного эксперимента для лабиринта часто является одним из подходов к решению "проблемы проверки правильности карты" [2]. Эта проблема состоит в следующем: задан конечный эталон-лабиринт (карта) и определен класс исследуемых лабиринтов. Требуется, передвигаясь по произвольному лабиринту из этого класса и воспринимая некоторую локальную информацию о вершинах и дугах пройденных путей, проверить, изоморфен этот лабиринт эталону или нет. Процесс прохождения по лабиринту, восприятия локальной информации о вершинах и дугах и вывода заключений о свойствах лабиринта называется контрольным экспериментом. В работе найден конструктивный способ построения контрольного эксперимента для произвольных шахматного лабиринта-эталона и непустого класса лабиринтов.

Все неопределяемые понятия взяты из [1, 3].

Рассмотрим двумерное евклидово пространство и целочисленную решетку Z^2 в нем. Элементы (x, y) множества Z^2 будем обозначать v. Расстоянием между элементами $v = (x, y)$ и $v' = (x', y')$ будем называть число $\rho_z(v, v') = |x - x'| + |y - y'|$.

Пусть $\mathbf{B} = \{e, n, s, w\}$ — алфавит отметок дуг. Обозначим через θ пустой символ, $\mathbf{B}^0 = \mathbf{B} \cup \{\theta\}$, $\mathbf{A} = 2^B \backslash \{\emptyset\}$.

Шахматным лабиринтом $L = (V, E, a, b)$ назовем конечный связный симметрический ориентированный отмеченный граф, обладающий следующими свойствами: $V \subset Z^2$; $((v, v') \in E) \Longleftrightarrow (\rho_z(v, v') =$

1); отметка b каждой дуги (v, v'), где $v = (x, y)$, $v' = (x', y')$, соответствует ее направлению, т. е. $b = w$, если $x' = x - 1$; $b = e$, если $x' = x + 1$; $b = n$, если $y' = y + 1$; $b = s$, если $y' = y - 1$; отметка $a(v)$ каждой вершины v есть множество отметок всех исходящих из нее дуг.

Класс всех шахматных лабиринтов обозначим через $\mathbf{C}$. Через $|L|$ обозначим число вершин лабиринта L.

Будем говорить, что слово $t = (a_1, b_1)...(a_m, b_{m+1})$ и маршрут $p = v_1(v_1, v_2)v_2...v_m(v_m, v_{m+1})v_{m+1}$ в лабиринте L соответствуют друг другу, если $a_i = a(v_i)$ для всех $i \in \{1, ..., m+1\}$ и $b_i = b(v_i, v_{i+1})$ для всех $i \in \{1, ..., m\}$, $b_{m+1} = \theta$.

Каждой вершине v лабиринта L сопоставим множество слов λ_v, соответствующих всевозможным маршрутам, начинающимся в ней. *Языком лабиринта* $L = (V, X, a, b)$ назовем множество $\lambda_L = \bigcup_{v \in V} \lambda_v$. Пусть X — некоторое множество слов, обозначим через X^k множество всех слов из X длины меньше или равной k.

Вершины v лабиринта L и v' лабиринта L' назовем *неотличимыми*, если $\lambda_v = \lambda_{v'}$.

Лабиринты L и L' назовем *эквивалентными*, если для любой вершины одного из этих лабиринтов найдется неотличимая от нее вершина другого лабиринта. Лабиринты L и L' *k-эквивалентными*, если $\lambda_L^k = \lambda_{L'}^k$. Через $\varepsilon_k(L)$ обозначим класс всех лабиринтов из $\mathbf{C}$, k-эквивалентных L.

Лабиринты L и L' назовем *изоморфными*, если существует взаимно однозначное соответствие между множествами их вершин, сохраняющее смежность и отметки вершин и дуг.

Вершины лабиринта L с отметкой $\{e, n, w, s\}$ назовем *внутренними*, все остальные вершины — *граничными*. Для произвольной вершины v обозначим через β_v множество всех слов, соответствующих всем простым путям из v в граничные вершины лабиринта L.

Пусть $L \in \mathbf{C}$, $F \subseteq \mathbf{C}, F \neq \emptyset$. *Контрольным экспериментом* (*КЭ*) для L относительно F назовем такое множество слов $\Lambda \subseteq \mathbf{A} \times \mathbf{B}^0$, для которого $\Lambda \subseteq \lambda_L$, и, если $\Lambda \subseteq \lambda_{L'}$, где $L' \in F$, то L и L' изоморфны.

На лабиринтах из класса C введем следующую метрику. *Расстоянием между двумя любыми лабиринтами* $L, L' \in \mathbf{C}$ такими, что $\lambda_L \neq \lambda_{L'}$, назовем величину $\rho(L, L') = \frac{1}{k}$ такую, что $\lambda_L^k \neq \lambda_{L'}^k$ и $\lambda_L^{k-1} = \lambda_{L'}^{k-1}$. Если $\lambda_L = \lambda_{L'}$, то положим $\rho(L, L') = 0$.

Будем называть лабиринт $L \in \mathbf{C}$ *предельным лабиринтом класса* $F \subseteq C$ и обозначать это $L \in \lim F$, если для любого $\varepsilon > 0$ найдется лабиринт $L' \in F - \{L\}$ такой, что $\rho(L, L') < \varepsilon$. В противном случае будем писать $L \notin \lim F$.

Теорема 1. *Пусть* $L \in \mathbf{C}$, $F \subseteq \mathbf{C}, F \neq \emptyset$. *Тогда следующие утверждения равносильны*:

1) *существует КЭ для лабиринта* L *относительно класса* F;

2) *множество* λ_L^k *является КЭ для лабиринта* L *относительно класса* F *для некоторого* k;

3) $\varepsilon_k(L) \cap F \subseteq \{L\}$ *для некоторого* k;

4) $L \notin \lim F$.

Эта теорема аналогична утверждениям, полученным в [4] для конечных автоматов и в [5] для отмеченных неориентированных графов, которые в общем случае не являются конструктивными.

В [6] доказана справедливость следующей теоремы.

Теорема 2. *Для шахматных лабиринтов следующие утверждения эквивалентны*:

1) *некоторые вершины* v *лабиринта* L *и* v' *лабиринта* L' *неотличимы*;

2) *множества* β_v *и* $\beta_{v'}$ *равны*;

3) *лабиринты* L *и* L' *эквивалентны*;

4) *лабиринты* L *и* L' *изоморфны*.

Из теоремы 2 следует, что шахматные лабиринты L и L' эквивалентны тогда и только тогда, когда $\lambda_L^n = \lambda_{L'}^n$, где $n = \min\{|L|, |L'|\}$. Следовательно, для произвольных шахматного лабиринта L и непустого подкласса F класса $\mathbf{C}$ теорема 1 является конструктивным критерием, и $\lambda_L^{|L|}$ является КЭ для L относительно F.

Список литературы

1. Килибарда Г., Кудрявцев В. Б., Ушчумлич Щ. Независимые системы автоматов в лабиринтах // Дискретная математика. — 2003, — Т. 15, вып. 2. — С. 3–39.

2. Dudek G., Jenkin M., Milios E., Wilkes D. Map validation and robot self-location in a graph-like world // Robotics and Autonomous Systems. — 1997, — V. 22 (2). — P. 159–178.

3. Харари Ф. Теория графов. — М.: Мир, 1973.

4. Максименко И. И. Эксперименты в финитно-определенных метрических пространствах автоматов: Автореф. дисс. ... канд. физ.-мат. наук. — Саратов, 2000.

5. Тихончев М. Ю. Автоматный анализ детерминированных графов: Автореф. дисс. ... канд. физ.-мат. наук. — Саратов, 2005.

6. Грунская В. И. Об отличимости плоских шахматных лабиринтов // Интеллектуальные системы. — 2004. — Т. 8. — С. 457–464.

СИЛЬНО РЕГУЛЯРНЫЕ ГРАФЫ С УСЛОВИЕМ ХОФФМАНА

В. В. Кабанов, С. В. Унегов (Екатеринбург)

Мы рассматриваем только конечные неориентированные графы без петель и кратных ребер. Приведем сначала некоторые необходимые определения и обозначения. В тех случаях, когда нет устоявшегося определения или обозначения мы следуем монографии [1]. Далее всюду *подграф* будет означать *порожденный подграф*, то есть подграф, две вершины из которого смежны в том и только в том случае, если эти вершины смежны в исходном графе. Пусть x вершина графа Γ. Через $[x]$ будем обозначать *окрестность вершины* x в Γ, то есть множество всех вершин, смежных с x в Γ. Граф называется *регулярным* степени k, если число вершин в $[x]$ не зависит от выбора вершины x и равно k. Пересечение $[x] \cap [y]$ для двух различных вершин x и y в Γ будем обозначать через $M(x,y)$, если $x \not\sim y$, и через $\Lambda(x,y)$, если $x \sim y$. Подграф, порожденный множеством $M(x,y)$, будем называть *μ-подграфом* вершин x и y, если эти вершины находятся на расстоянии 2 в графе. Подграф, порожденный множеством $\Lambda(x,y)$, будем называть *λ-подграфом* вершин x и y. Граф называется *сильно регулярным графом с параметрами* (v,k,λ,μ), если он является регулярным степени k графом на v вершинах таким, что $|\Lambda(x,y)| = \lambda$ для любых двух смежных вершин x, y и $|M(x,y)| = \mu$ для любых двух несмежных вершин x, y. *m-лапой* будем называть полный двудольных граф $K_{1,m}$ с долями порядка 1 и m при $m \geq 2$. Через $\{p; q_1, \ldots, q_m\}$ обозначается m-лапа с долями $\{p\}$ и $\{q_1, \ldots, q_m\}$. Будем говорить, что граф Γ удовлетворяет *условию Хоффмана*, если для любой 3-лапы $\{p; q_1, q_2, q_3\}$ из графа Γ любая вершина r, отличная от p и смежная с q_1 и q_2, смежна с вершиной p, но не смежна с вершиной q_3. Заметим, что условие Хоффмана имеет содержательный смысл только для тех сильно регулярных графов, в которых найдется хотя бы одна 3-лапа и у которых $\mu > 1$. Реберным графом $\mathcal{L}(\Gamma)$ графа Γ называется граф на ребрах графа Γ, причем два ребра смежны в нем в том и только в том случае, когда они имеют одну общую вершину.

Реберный граф $\mathcal{L}(K_n)$ полного графа K_n называется треугольным графом и обозначается через $T(n)$. Этот граф является сильно регулярным графом с параметрами $(\frac{n(n-1)}{2}, 2(n-2), n-2, 4)$. В работах 1949–60 годов Л. С. Чанг [2, 3] и А. Дж. Хоффман [4, 5] показали, что треугольный граф $T(n)$ однозначно определяется своими параметрами для всех n за исключением случая $n = 8$, когда кроме графа

$T(8)$ существует ровно три графа, имеющих такие же параметры. Эти три графа были найдены Чангом и мы будем их называть графами Чанга. Аналогичный результат был получил С. С. Шрикханд в [6] для реберного графа $\mathcal{L}(K_{n,n})$, называемого решетчатым $n \times n$-графом и являющегося сильно регулярным графом с параметрами $(n^2, 2n-2, n-2, 2)$. Шрикханд показал, что решетчатый $n \times n$-граф однозначно определяется своими параметрами кроме случая $n = 4$, когда существует еще ровно один граф с такими же параметрами, который мы будем называть графом Шрикханда.

Под матрицей смежности графа Γ будем понимать матрицу $A = (a_{ij})$, строки и столбцы которой перенумерованы вершинами графа Γ, причем $a_{ij} = 1$, если ij является ребром в Γ и $a_{ij} = 0$ в противном случае. *Собственными значениями графа* мы будем называть собственные значения его матрицы смежности. Известно, что для всякого сильно регулярного графа с параметрами (v, k, λ, μ), кроме собственного значения, равного k, есть еще ровно два действительных собственных значения разных знаков (см., например, [1]). Нетрудно проверить, что во всех вышеупомянутых результатах рассматриваемые графы имеют отрицательное собственное значение равное -2. Дж. Дж. Зейделю в работе [7] удалось определить все сильно регулярные графы, для которых -2 является собственным значением. В список попали треугольные графы, три графа Чанга, решетчатые $n \times n$-графы, граф Шрикханда, дополнительные графы к лестничным графам, граф Шлефли, граф Клебша и граф Петерсена. Чуть позже М. Д. Хестенс и Д. Г. Хигман в работе [8] нашли другое доказательство этого утверждения. При этом они существенно воспользовались фактом, замеченным А. Дж. Хоффманом в [4], что любой граф, имеющий минимальное собственное значение, равное -2, удовлетворяет вышеприведенному условию Хоффмана. В настоящей заметке получено обратное утверждение.

Теорема. *Если граф Γ является сильно регулярным графом с параметрами (v, k, λ, μ) для $\mu > 1$, содержит 3-лапу и удовлетворяет условию Хоффмана, то -2 является собственным значением графа Γ.*

Среди сильно регулярных графов, для которых -2 является собственным значением, только граф Шрикханда и три графа Чанга содержат 3-лапу и удовлетворяют условию $\mu > 1$. Поэтому из теоремы очевидным образом вытекает следствие.

Следствие. *Если граф Γ является сильно регулярным графом с параметрами (v, k, λ, μ) для $\mu > 1$, содержит 3-лапу и удовлетворяет условию Хоффмана, то граф Γ является либо графом Шрикханда, либо одним из трех графов Чанга.*

Доказательство теоремы опирается на результаты о графах без 3-лап и без корон, полученные первым из авторов совместно с А. А. Махневым и Д. В. Падучих [9, 10].

Работа выполнена при финансовой поддержке РФФИ (проект 05-01-00046) и совместный РФФИ-ГФЕН Китая (проект 05-01-39000).

Список литературы

1. Brouwer A. E., Cohen A. M., Neumaier A. Distance-regular graphs. — Springer-Verlag, 1989.

2. Chang L. C. The unqueness and nonuniqueness of triangular association schemes // Sci. Record. — 1949. — V. 3. — P. 604–613.

3. Chang L. C. Association schemes of partially balanced block designs with parameters $v = 28$, $n_1 = 12$, $n_0 = 15$ and $p_{11}^2 = 4$ // Sci. Record. — 1950. — V. 4. — P. 12–18.

4. Hoffman A. J. On the uniqueness of the triangular association scheme // Ann. Math. Stat. — 1960. — V. 31. — P. 492–497.

5. Hoffman A. J. On the exceptional case in a characterization of the arcs of complete graphs // IBM J. Res. Develop. — 1960. — V. 4. — P. 487–496.

6. Shrickhande S. S. The uniqueness of the L_2 association scheme // Ann. Math. Stat. — 1959. — V. 30. — 781–798.

7. Seidel J. J. Strongly regular graphs with (-1, 1, 0) adjacency matrix having eigenvalue 3 // Linear algebra and Appl. — 1968. — V. 1. — P. 281–298.

8. Hestens M. D., Higman D.G. Rank 3 groups and strongly regular graphs // SIAM-AMS Proceedings. — Providence, 1971. — V. 4. — P. 141–159.

9. Кабанов В. В., Махнев А. А. Графы без 3-лап с равномощными μ-подграфами // Известия Уральского гос. университета. — Екатеринбург, 1998. — Т. 10. — С. 44–68.

10. Кабанов В. В., Махнев А. А., Падучих Д.В. О графах без корон с регулярными μ-подграфами II // Матем. заметки. — 2003. — Т. 74, № 3. — С. 375–384.

СТРУКТУРА РАЗБИЕНИЯ ТРЕХСВЯЗНОГО ГРАФА

Д. В. Карпов, А. В. Пастор (Санкт-Петербург)

Структура разбиения связного графа его точками сочленения широко известна [1, 2]. В 1966 году Татт [3] описал структуру вза-

имного расположения двухвершинных разделяющих множеств в двусвязном графе и показал, что она имеет много общего со структурой точек сочленения. В работе [4] был разработан новый подход к изучению структуры взаимного расположения k-разделяющих множеств k-связного графа, использующий понятие *части разбиения* графа несколькими разделяющими множествами.

Настоящая работа поясвящена изучению структуры взаимного расположения трехвершинных разделяющих множеств трехсвязного графа G (далее мы будем называть такие множества 3-разделяющими). Семейство всех 3-разделяющих множеств графа G мы будем обозначать через $\mathfrak{R}_3(G)$.

Определение. Пусть $\mathfrak{S} \subset \mathfrak{R}_3(G)$. *Часть* разбиения графа G набором $\mathfrak{S}$ (или часть $\mathfrak{S}$-разбиения) — это максимальное по включению множество $A \subset V(G)$ такое, что никакое множество $S \in \mathfrak{S}$ не разделяет A. Обозначим через $P(\mathfrak{S})$ множество всех таких частей. Определим *границу* части A, как множество $R(A)$ из всех вершин части A, входящих хотя бы в одно из множеств набора $\mathfrak{S}$.

Будем называть множества $S, T \in \mathfrak{R}_3(G)$ *независимыми*, если S не разделяет T и T не разделяет S и *зависимыми* в противном случае. Из-за наличия пар зависимых множеств возникают трудности в описании структуры взаимного расположения множеств из $\mathfrak{R}_3(G)$.

Основной идеологией нашей работы является разбиение семейства $\mathfrak{R}_3(G)$ на подсемейства нескольких типов, которые мы будем называть *комплексами*. Для каждого типа комплексов мы опишем разбиение графа множествами такого комплекса и взаимное расположение множеств этого комплекса. Ниже мы кратко опишем типы комплексов.

Мы покажем, что для любых двух комплексов $\mathcal{C}$ и $\mathcal{C}'$ существует единственная часть A из разбиения $P(\mathcal{C})$, имеющая непустое пересечение со всеми множествами комплекса $\mathcal{C}'$ (будем говорить, что эта часть A содержит комплекс $\mathcal{C}'$). Назовем два комплекса $\mathcal{C}_1$ и $\mathcal{C}_2$ *соседними*, если для любого отличного от них комплекса $\mathcal{C}$ одна и та же часть разбиения $P(\mathcal{C})$ содержит комплексы $\mathcal{C}_1$ и $\mathcal{C}_2$.

Взаимное расположение разных комплексов описывается с помощью гиперграфа $T(G)$, вершины которого соответствуют комплексам, а гиперребра являются максимальными по включению множествами попарно соседних комплексов.

Теорема. *Граф $T(G)$ является* гипердеревом (*то есть, этот граф связен и любой цикл в этом графе есть подмножество гиперребра*).

Комплексы будут следующих четырех типов: *одиночные* комплексы (состоящие из одного множества, независимого ни с одним из

множеств набора $\mathfrak{R}_3(G)$), комплексы *ромашек*, комплексы *разрезов* и *тройные комплексы*.

1. Ромашки. Набор $F = (p; q_1, \ldots, q_m)$ вершин графа G будем называть *ромашкой*, если существует такой набор $\mathfrak{S} \subset \mathfrak{R}_3(F)$, что разбиение $P(\mathfrak{S})$ состоит из m частей $G_{1,2}$, $G_{2,3}$, $\ldots$, $G_{m,1}$, причем $R(G_{i,i+1}) = Q_{i,i+1}$. Вершину p мы будем называть *центром*, а вершины $q_1, \ldots, q_m$ — *лепестками* этой ромашки.

В [4] было доказано, что все множества $Q_{i,j}$, где $j \notin \{i, i+1, i-1\}$ являются разделяющими. Такие множества мы будем называть *внутренними*, а множества вида $Q_{i,i+1}$ — *граничными* множествами ромашки. Назовем ромашку F *максимальной*, если не существует ромашки F' с тем же центром, содержащей все лепестки F и еще хотя бы один лепесток.

Если $d(p) = 3$, то множество $T(p)$ вершин, смежных с p назовем *окрестностью* центра ромашки.

Комплексом ромашки мы будем называть семейство, состоящее из всех ее внутренних разделяющих множеств максимальной ромашки и, в случае $d(p) = 3$, окрестности ее центра.

2. Вершинно-реберные разрезы. Назовем множество $M = \{a, b, c\}$, каждый из элементов которого — вершина или ребро графа G, *разделяющим*, если граф $G - M$ несвязен. Такие множества мы будем также называть *разрезами* графа G. Назовем разрез M *максимальным*, если его нельзя дополнить до другого разреза, заменив одну из содержащихся в M вершин v на ребро, инцидентное v. Будем говорить, что трехвершинное множество S *содержится* в разрезе M, если S содержит все вершины из M и ровно по одному концу каждого из ребер M.

Пусть разрез M содержит хотя бы одно ребро, тогда вершины графа $G - M$ распадаются на две компоненты связности H_1 и H_2. Несложно показать, что в каждой из частей H_1 и H_2 лежит ровно одно трехвершинное множество, содержащееся в M; назовем эти два трехвершинных множества границами разреза M.

Несложно понять, что любое множество, содержащееся в M (кроме, возможно границ этого разреза), является разделяющим. Такие множества мы будем называть *внутренними* множествами разреза.

Разрез, содержащий хотя бы два ребра, будем называть *большим*. Максимальный разрез, содержащий ровно одно ребро, входящее еще хотя бы в один разрез — *малым*. *Комплексом разреза* M будем называть набор всех его внутренних разделяющих множеств, если разрез M — большой, и набор, состоящий из тех границ M, которые не являются одиночными множествами, если разрез M — малый.

3. Тройные комплексы. Пусть $S \in \mathfrak{R}_3(G)$, $P(S) = \{A_1, A_2, A_3\}$. Назовем *вырожденной* вершину $a \in S$, если $d(a) = 3$. Множество вершин, смежных с a, будем называть *окрестностью* вершины a. Определим *окрестность* $O(S)$ множества S, как объединение S и окрестностей всех вырожденных вершин множества S.

Рассмотрим множество M_1, состоящее из невырожденных вершин множества S и ребер, соединяющих вырожденные вершины S с вершинами их окрестностей, лежащими в $I(A_1)$. Аналогично определим M_2 и M_3. Легко видеть, что M_1, M_2, M_3 — разрезы. Определим *тройной комплекс* $\mathfrak{C}(S)$, как набор, состоящий из множества S, окрестностей его вырожденных вершин и множеств, содержащихся в разрезах M_1, M_2, M_3 и отличных от границ этих разрезов.

Работа выполнена при финансовой поддержке программы фундаментальных исследований РАН «Современные проблемы теоретической математики», гранта Президента РФ НШ-8664.2006.1, гранта INTAS 04-77-7173 и гранта РФФИ 05-0100932.

Список литературы

1. Оре О. Теория графов. — М.: Наука, 1968.

2. Харари Ф. Теория графов. — М.: Мир, 1973.

3. Tutte W. T. Connectivity in graphs. — Toronto: Univ. Toronto Press, 1966.

4. Карпов Д. В. Разделяющие множества в k-связном графе. — Препринт ПОМИ. — № 15/2005.

ПРОТИВОРЕЧИВОСТЬ В ЗАДАЧАХ СОСТАВЛЕНИЯ РАСПИСАНИЙ

В. П. Козырев (Москва)

Задача $Z = \{[a_i, b - i], \tau_i\}$ составления многопроцессорных расписаний заключается в нахождении порядка выполнения n (вычислительных) работ на минимальном числе идентичных процессоров, когда каждая работа $i (1 \le i \le n)$, имеющая длительность $\tau_i > 0$, выполняется в директивные сроки $[a_i, b_i]$ без прерывания, и на каждом процессоре в любой момент времени реализуется не более одной работы. Эта задача является NP-полной в сильном смысле даже для одного процессора и даже при условии, что все параметры $a_i, b_i (1 \le i \le n)$ принимают два значения.

Вводится понятие чередующегося цикла (П-цикла) и доказывается, что в произвольной задаче Z нет противоречивых П-циклов.

Пусть $\alpha_i = a_i + \tau_i$, $\beta_i = b_i - \tau_i$, т. е. α_i — самое раннее время окончания работы i, β_i — самое позднее начало выполнения работы i. На множестве пар работ $i \neq j$ определяются три типа бинарных отношений: пара i, j 2-совместима, если $\alpha_i \leq \beta_j, \alpha_j \leq \beta_i$ или $\tau_i + \tau_j \leq b_j - a_i$, $b_i - a_j$ (работы i, j могут быть выполнены на одном и том же процессоре); 2-несовместима, если $\alpha_i > \beta_j$, $\alpha_j > \beta_i$ или $\tau_i + \tau_j > b_j - a_i, b_i - a_j$ (работы i, j не могут быть выполнены на одном процессоре в любом порядке); 1-совместима, если $\alpha_i \leq \beta_j$, $\beta_i < \alpha_j$ или $b_i - a_j < \tau_i + \tau_j \leq b_j - a_i$ (на одном процессоре может выполняться сначала работа i, а затем работа j, но не наоборот). Естественно возникает геометрическая интерпретация элементов: ребро (i, j), неребро $(\overline{i, j})$, и дуга $(\overrightarrow{i, j})$ соответственно. Для $i = j$ определяются петли (i, i), если $\alpha_i \leq \beta_i$, и непетли $(\overline{i, i})$, если $\alpha_i > \beta_i$, то есть соответственно, петля, если $\tau_i \leq \frac{b_i - a_i}{2}$ или непетля, если $\tau_i > \frac{b_i - a_i}{2}$.

Последовательность ребер, неребер, дуг, петель и непетель называется чередующимся циклом (кратко П-циклом), если для любого ее элемента соседние элементы относятся к разным типам, или соседние по циклу элементы являются дугами. Каждой П-цепи ставится в соответствие последовательность неравенств, связывающих параметры α_i, β_i, соседних вершин (работ) параметр. Замкнутая П-цепь называется П-циклом. П-цикл противоречивый, если по цепочке неравенств можно получить соотношения $\alpha_i < \alpha_i$ или $\beta_j < \beta_j$. Любая задача составления расписаний обладает свойством — она не содержит противоречивых П-циклов.

Теорема. *Если на множестве V работ (вершин) имеется противоречивый П-цикл с k элементами, то на этом множестве вершин имеется противоречивый П-цикл с четырьмя элементами.*

Укажем все чередующиеся циклы с 4 элементами (с точностью до изоморфизма). Будем представлять дугу числом 2, ребро и петлю — числом 1, неребро и непетлю — числом 0. Тогда П-циклы будут представляться 4-мерными векторами с координатами, равными 2,1,0. Каждый цикл представляем максимальным вектором. Все максимальные вектора 1010,2010,2101,2020,2120,2121,$2^2$01,$2^2$10,$2^3$0,$2^3$1,2^4, где 2^4=2222. Из этих 11 П-циклов 10 циклов являются противоречивыми, и только один 2120 является непротиворечивым. Исключительный цикл имеет вид $((\overrightarrow{1, 2}), (2, 3), (\overrightarrow{3, 4}), (\overline{4, 1}))$ и для него определяются две α, β-последовательности $\alpha_3 \leq \beta_4 < \alpha_1 \leq \beta_2$, $\beta_1 < \alpha_2 \leq \beta_3 < \alpha_4$. Кроме реализаций 4-мерных векторов П-циклами с 4 вершинами для каждого из векторов, кроме вектора 2^4, существуют реали-

зации П-циклов с тремя вершинами и одной петлей или одной непетлей. Так, для вектора 2121 имеем циклы $((\overline{1,1}),(\overrightarrow{1,2}),(2,3),(\overrightarrow{3,1}))$ и $((\overrightarrow{1,2}),(2,2),(\overrightarrow{2,3}),(3,1))$, а для вектора 2120 $((\overline{1,1}),(\overrightarrow{1,2}),(2,3),(\overrightarrow{3,1}))$ и $((\overrightarrow{1,3}),(2,2),(\overrightarrow{2,3}),(\overline{3,1}))$. Все указанные П-циклы, кроме 2120, не могут содержаться во всех задачах составления расписаний и являются запрещенными.

Следствие. *Задача проверки отсутствия противоречивых П-циклов является полиномиальной проблемой.*

Отсутствие противоречивых П-циклов — важное структурное свойство, позволившее для шести классов задач составления расписаний достижимые верхние и нижние оценки минимального числа необходимых процессоров. Это классы задач, в которых только: 1) одни ребра, 2) одни дуги, 3) одни ребра и неребра, 4) одни ребра и дуги, 5)одни неребра и дуги, 6)ребра, неребра, дуги, образующие чередующиеся цепи определенного вида.

Существуют П-циклы, не являющиеся противоречивыми, определяющие полностью строение задач составления расписаний. П-цикл $(\overrightarrow{1,2}),(\overrightarrow{2,3}),(\overline{3,4}),\ldots,(\overrightarrow{2i,2i+1}),(\overline{2i+1,2i+2}),\ldots,(\overline{2r+1,1})$.В пятом классе порождаются все дуги и неребра, причем неребра образуют полный граф с $(r+1)$ вершинами, поэтому минимальное число процессоров равно $r+1$. Другой класс (случай 6) получаем с помощью П-цикла $(\overrightarrow{1,2}),(\overrightarrow{2,3}),\ldots,(\overrightarrow{2r,2r+1}),(2r+1,1)$, когда однозначно порождаются все ребра, неребра и дуги так, чтобы опять не образовывались противоречивые П-циклы. Тогда минимальное число процессоров равно r или $r+1$; указываются условия реализации каждого из этих значений.

РАССТОЯНИЕ МЕЖДУ ТРЕУГОЛЬНЫМИ ВЛОЖЕНИЯМИ ПОЛНОГО ГРАФА В ПОВЕРХНОСТЬ

В. П. Коржик (Черновцы)

Треугольным вложением (ТВ) полного графа в поверхность (ориентируемую или неориентируемую) называется такое 2-клеточное вложение этого графа, все грани которого треугольные. Известно, что треугольное ориентируемое (соотв. неориентируемое) вложение графа K_n существует для $n \equiv 0,3,4,7 \bmod 12$ (соотв. $n \equiv$

$0, 1 \bmod 3$). Построение ТВ полных графов было одним из основных шагов в доказательстве теоремы о раскраске карт [1].

ТВ полного графа задаётся множеством граней этого вложения, которое представляет собой множество неупорядоченных троек $\{x, y, z\}$, где тройка $\{x, y, z\}$ обозначает грань, инцидентную вершинам x, y, и z вложенного графа. Зафиксируем множество вершин полного графа. Два ТВ этого полного графа называются *изоморфными*, если мы можем перепометить вершины этого графа в одном из этих вложений так, что множество граней полученного после перепомечивания вложения совпадает с множеством граней второго вложения.

Известно, что число неизоморфных ТВ графа K_n увеличивается очень сильно с ростом n. Например, число неизоморфных неориентируемых ТВ графа K_{12} (соотв. K_{13}) есть 182 200 (соотв. 243 088 286). Доказано, что скорость роста числа неизоморфных ТВ графа K_n лежит между $2^{\beta n^2}$ и $2^{\beta n^2 \ln n}$.

Изучение структуры множества всех ТВ полного графа представляет большой математический интерес. Первым шагом в этом направлении является изучение различий между ТВ. С этой целью мы вводим понятие расстояния $d(f, f')$ между двумя ТВ f и f' полного графа. Расстояние $d(f, f')$ есть минимальное целое число t такое, что мы можем в f заменить t граней на новые грани, получив, в результате, ТВ, изоморфное вложению f'.

Теорема 1 [2]. *Минимальное ненулевое расстояние между двумя ТВ f и f' полного графа есть 4 в случае ориентируемых f и f', и есть 6 в случае неориентируемых f и f', и в случае, когда одно из этих вложений есть ориентируемое, а другое — неориентируемое.*

Теорема 2 [3]. *Для каждого целого числа $s \geq 9$, если $4s+1$ есть простое число и 2 есть первообразный корень по модулю $4s + 1$, то тогда существуют такие неориентируемые ТВ f и f' графа K_{12s+4}, что*

$$d(f, f') \geq \frac{1}{2}(4s + 1)(12s + 4) - O(s),$$

где $(4s + 1)(12s + 4)$ есть число граней ТВ графа K_{12s+4}.

Можно привести теоретико-числовые аргументы, связанные с известной гипотезой Артина, в пользу того, что есть бесконечно много значений s, удовлетворяющих условию теоремы 2. Численные расчёты показывают, что интервалы $[0, 1000]$, $[1001, 2000]$, $[2001, 3000]$, $[3001, 4000]$, $[4001, 5000]$ содержат, соответственно, 193, 149, 154, 141,

150 значений k таких, что $8k+5$ есть простое число и 2 есть первообразный корень по модулю $8k+5$.

Гипотеза 1. *Есть константа $0 < c < 1$ такая, что для каждого n, для которого K_n имеет ТВ, для каждых двух ТВ f and f' графа K_n выполняется*

$$d(f, f') \leq c \cdot \frac{n(n-1)}{3},$$

где $n(n-1)/3$ есть число граней ТВ графа K_n.

Другими словами, эта гипотеза утверждает, что всякие два ТВ графа K_n имеют большое число (не менее $(1-c) \cdot \frac{n(n-1)}{3}$) общих (с точностью до перепомечивания вершин этого графа) граней. Любой ответ, положительный или отрицательный, на эту гипотезу будет интересным и даст нам понимание того, насколько различными могут быть ТВ полного графа.

Понятие расстояния может быть использовано при рассмотрении задачи описания произвольного ТВ полного графа.

Теорема 1 показывает, что для однозначного определения ТВ графа необходимо задать список не менее чем $\frac{n(n-1)}{3} - 3$ граней этого вложения. Некоторые ТВ полного графа имеют простое описание. Например, используя графы токов, можно построить такое симметричное ТВ полного графа, что множество граней этого вложения имеет циклическую группу автоморфизмов. Чтобы задать такое множество граней, достаточно задать по одной грани для каждой орбиты действия этой группы автоморфизмов. Однако, представляется вероятным, что почти все ТВ полного графа являются асимметричными (их множества граней не имеют нетривиальных автоморфизмов).

Проблема 1. *Есть ли более простое описание произвольного асимметричного ТВ графа K_n, чем задание списка $\frac{n(n-1)}{3} - 3$ граней этого вложения?*

Если бы максимальное расстояние между ТВ полного графа было бы малым, то тогда простое описание асимметричного ТВ f полного графа можно было бы пытаться получить следующим образом. Берём ТВ f', допускающее простое описание, и затем простое описание вложения множества граней вложения f получается, если мы даём простое описание множества граней вложения f' и указываем то малое число $d(f, f')$ новых граней, которыми необходимо заменить $d(f, f')$ граней вложения f', чтобы получить f. Однако, теорема 2 показывает, что максимальное расстояние между двумя ТВ графа K_n есть, скорее всего, не менее $\frac{n(n-1)}{6}$.

Гипотеза 2. *Есть такая функция $c(n) = O(n)$, что если граф K_n имеет ТВ, то существует такое множество $\mathcal{A}$ ТВ этого графа, имеющих простое описание, что для каждого ТВ f этого графа есть ТВ $f' \in \mathcal{A}$ такое, что $d(f, f') \leq c(n)$.*

Важно отметить, что аналогичным образом можно ввести расстояние между парами других комбинаторных объектов: троек Штейнера, латинских квадратов, т. д. Затем мы можем формулировать для этих комбинаторных объектов проблемы и гипотезы, аналогичные приведенным выше для ТВ полного графа.

Список литературы

1. Рингель Г. Теорема о раскраске карт. —М.: Мир, 1977.

2. Grannell M. J., Griggs T. S., Korzhik V., Siran J. On the minimal distance between triangular embeddings of a complete graph // Discrete Math. — 2003. — V. 269. — P. 149–160.

3. Korzhik V. On the maximal distance between triangular embeddings of a complete graph // J. Combin. Theory. Ser. B — 2006. — V. 96. — P. 426–435.

НЕКОТОРЫЕ СЛУЧАИ ДЕФРАГМЕНТАЦИИ МАТРИЦ ПЕРЕСТАНОВОК

А. М. Магомедов (Махачкала)

Предлагается обобщение результатов сообщения [1].

Матрицу, где ненулевые элементы каждой строки расположены в подряд идущих ячейках, а в каждом столбце ненулевые элементы попарно различны, назовем *дефрагментированной*. Такое преобразование матрицы к дефрагментированному виду, при котором в каждой строке и каждом столбце матрицы сохраняются исходные наборы элементов, будем называть *дефрагментацией*.

Через $1..n$ обозначим множество первых n натуральных чисел, $|S|$ — мощность множества S. Пусть $L, m, n \in Z^+$. Матрицу M порядка $L \times m$, каждый столбец которой содержит множество $1..n$ и $L - n$ нулей, назовем *матрицей перестановок*. Введем обозначения: $M[i, *]$ и $M[*, k]$ — наборы ненулевых элементов i-ой строки и k-го столбца матрицы M соответственно; $M(S)$ — семейство наборов ненулевых элементов строк матрицы M, в каждой из которых количество ненулевых элементов представлено элементом множества S; $P_Q^{L,m,n}$ — семейство матриц перестановок M порядка $L \times m$, таких,

что $|M[i,*]| \in Q\ \forall i \in 1..L$; $sgn(M)$ — матрица, полученная заменой ненулевых элементов матрицы M на единицы.

Утверждение 1. *Набор ненулевых элементов дефрагментированной матрицы перестановок M допускает разбиение на n трансверсалей семейства $\{M[*,k]; k \in 1..m\}$, удовлетворяющих условию: трансверсаль, включающая какой-либо ненулевой элемент строки, включает и все ненулевые элементы этой строки.*

Утверждение 2. 1) *Для дефрагментации матрицы $M \in P^{L,m,n}_{1,m-1,m}$ необходимо и достаточно существование $m-2$ трансверсалей у семейства $\{M(m-1,m)\}$.*

2) *Для дефрагментации матрицы $M \in P^{L,m,n}_{2,m-2,m}$ необходимо и достаточно существование $m-4$ трансверсалей у семейства $\{M(m-2,m)\}$.*

Утверждение 3. *Пусть $M \in P^{L,2k,n}_{k}$, k — четное, семейство наборов $\{M[i,*], i \in 1..L\}$ произвольным образом разбито на $\frac{L}{2}$ подсемейств, каждое из которых содержит по два набора. Обменами вида "два элемента одного набора перемещаются в другой набор и наоборот" между наборами внутри подсемейств можно преобразовать матрицу M в матрицу $M' \in P^{L,2k,n}_{k}$, которая допускает дефрагментацию.*

Список литературы

1. Магомедов А. М. Дефрагментация матриц перестановок с сохранением наборов элементов в линиях // Проблемы теоретической кибернетики. Тезисы докладов XIV Международной конференции (23–28 мая 2005 г.). — М.: Изд-во механико-математического факультета МГУ, 2005. — С. 92.

NP-ПОЛНОТА ЗАДАЧИ ДООПРЕДЕЛЕНИЯ ЧАСТИЧНЫХ МОНОТОННЫХ БУЛЕВЫХ ФУНКЦИЙ

Г. А. Махина (Симферополь), А. А. Сапоженко (Москва)

Задачу распознавания образов (см. например, [1, 2]) можно рассматривать как задачу доопределения частичной монотонной булевой функции (ЧМБФ). Пусть ЧМБФ f задана двумя списками $N_{\bar{f}}$ и N_f двоичных наборов длины n, которые являются соответственно *множествами нулей и единиц функции f. Доопределением* ЧМБФ f называется произвольная ЧМБФ g, определяемая парой множеств

$O(g)$, $Z(g)$, называемых соответственно *множествами нижних единиц* и *верхних нулей* функции g, такая, что для всякого $\mathbf{a} \in N_{\bar{f}}$ (а также для всякого $\mathbf{a} \in N_{\bar{g}}$) существует $\mathbf{b} \in Z(g)$, т. ч. $\mathbf{b} \geq \mathbf{a}$, и для всякого $\mathbf{a} \in N_f$ (а также для всякого $\mathbf{a} \in N_g$) существует $\mathbf{b} \in Z(g)$ такое, что $\mathbf{b} \leq \mathbf{a}$. В случае, когда ЧМБФ f от n переменных задана m нулями и k единицами, будем говорить, что функция f принадлежит классу $K(n, m, k)$. Назовем задачей *«доопределение»* задачу построения для произвольной функции $f \in K(n, m, k)$ и числа l доопределения g, такого, что $|O(g)| + |Z(g)| \leq l$. Не определяемые здесь понятия можно найти в [2, 3]. Целью статьи является следующая

Теорема. *Задача* «доопределение» *для функций из класса* $K(n, m, k)$ *является NP-полной.*

Доказательство. Пусть $L \preceq K$ означает "задача (язык) L полиномиально сводится к задаче (языку) K". Здесь используется терминология из [4]. Задача описывается входом и свойством. Доказательство NP-полноты задачи «доопределение» проведем последующей схеме:

$$\text{«покрытие»} \preceq \text{«1-доопределение»} \preceq \text{«доопределение»} \in \text{NP},$$

где задача «покрытие» определяется так: *вход* — семейство множеств $F = \{A_1, ..., A_s\}$, число h, *свойство* — существует $P \subseteq F$, такое, что $|P| \leq h$ и $\bigcup_{A \in P} A = \bigcup_{A \in F} A$; а задача «1-доопределение» так: *вход* — ЧМБФ f из класса $K(n, 1, k)$ (т. е. пара множеств $(N_{\bar{f}}, N_f)$), где $|N_{\bar{f}}| = 1$, и число l, *свойство* — существует доопределение g функции f, т. ч.

$$|O(g)| + |Z(g)| = |O(g)| + 1 \leq l, \tag{1}$$

где $O(g)$, $Z(g)$ — соответственно множества нижних единиц и верхних нулей функции g.

Докажем сведение задачи «покрытие» к задаче «1-доопределение».

Пусть (F, h) — вход задачи «1-доопределение», где $F = \{A_1, ..., A_s\}$. Положим $U = \bigcup_{i=1}^{s} A_i$ и пусть $U = \{u_1, ..., u_t\}$. Пусть далее $n = s + 1$. Через B^n и B_i^n обозначим соответственно n-мерный куб и его i-й слой. Определим отображение $\psi : U \to B^n$, положив $\psi(u) = (a_1, ..., a_{n-1}, 0)$, где $a_i = 1$ при $u \in A_i$ и $a_i = 0$ иначе, для всякого $u \in U$ и i=1,...,n-1. Определим ЧМБФ f равенствами $N_f = \{\psi(u_1), ..., \psi(u_t)\}$, $N_{\bar{f}} = \{\tilde{\beta}\}$, где $N_{\bar{f}} = \{\tilde{\beta}\} = \{(0, ..., 0, 1)\}$. Положим еще $l = h + 1$. Тем самым задан вход (f, l) задачи «1-доопределение», соответствующий входу (F, h) задачи «покрытие».

Докажем, что свойства задач выполняются или не выполняются одновременно. Пусть $P \subseteq F$, $P = \{A_{i_1}, ..., A_{i_p}\}$, $\bigcup_{A \in P} A = U$ — некоторое покрытие семейства F, такое, что $|P| \leq h$. Укажем доопределение g функции f, соответствующее покрытию P, удовлетворяющее неравенству (1) с $l = h+1$. Положим $O(g) = \{\tilde{e}_{i_1}, ..., \tilde{e}_{i_p}\}$, где $\tilde{e}_i \in B_1^n$ — набор с единицей в i-й координате. Пусть $V = B_1^n \setminus \{\tilde{e}_{i_1}, ..., \tilde{e}_{i_p}\}$ и $Z(g) = \{\tilde{\gamma}\}$, где $\tilde{\gamma} = \bigvee\limits_{\tilde{e}_p \in V} \tilde{e}_p$.

Доопределение g функции f называется *тупиковым*, если для любых $u \in Z_g$ и $v < u$ (для любых $u \in O_g$ и $v > u$) существует $a \in N_{\bar{f}}$, $v < a$ (соответственно $a \in N_f$, $v > a$). Пусть существует доопределение g функции f, удовлетворяющее (1). Тогда существует ее тупиковое доопределение, также удовлетворяющее (1). В [3] доказано, что всякое тупиковое доопределение g функции $f \in K(n, 1, k)$ удовлетворяет следующим условиям: $O(g) \subseteq B_1^n$ и $|Z(g)| = 1$. Пусть $O(g) = \{\tilde{e}_{i_1}, ..., \tilde{e}_{i_p}\}$. Ясно, что тогда множество $P = \{A_{i_1}, ..., A_{i_p}\}$ является покрытием F и при этом $p \leq h = l - 1$ поскольку g удовлетворяет (1).

Теперь докажем сведение задачи «1-доопределение» к задаче «доопределение». Задача «доопределение» имеет вид: *вход* — множества $N_{\bar{f}'} = \{\mathbf{a}'_1, ..., \mathbf{a}'_\mathbf{m}\})$, $N_f = \{\mathbf{b}'_1, ..., \mathbf{b}'_{\mathbf{k}'}\}$, число l'; *свойство* — существует доопределение g' функции f', удовлетворяющее неравенству:

$$|O(g')| + |Z(g')| \leq l'. \tag{2}$$

Определим $f' = f'(x_1, ...x_{n+1})$, задав множества $N_{\bar{f}'}$ и $N_{f'}$. Положим $N_{f'} = \{\mathbf{b}'_1, ..., \mathbf{b}'_{\mathbf{k}'}\}$, где $\mathbf{b}'_\mathbf{i}$ получено из $\mathbf{b_i} \in N_f$ приписыванием 1 в качестве $(n+1)$-й координаты. В качестве $N_{\bar{f}'}$ возьмем произвольное множество из $m-1$ наборов вида $(a_1, ..., a_n, 0)$, включающее набор $(1, ..., 1, 0)$ и, кроме того, набор, полученный добавлением единичной $n+1$-й координаты к единственному набору из $N_{\bar{f}}$. Положим $l' = l + 1$. Ясно, что преобразование входов полиномиально, а неравенства (1) и (2) выполняются или не выполняются одновременно.

Докажем теперь принадлежность задачи «доопределение» классу NP. Для этого достаточно убедиться в существовании детерминированной машины Тьюринга, проверяющей за полиномиальное время по четверке множеств $(Z(g), (O(g)), N_{\bar{f}}, N_f)$ и числу l следующий факт: пара множеств $(Z(g), (O(g))$ представляет собой пару множеств верхних нулей и нижних единиц функции g, являющейся доопределением ЧМБФ f с множеством нулей $N_{\bar{f}}$ и множеством еди-

ниц N_f, и при этом удовлетворяется условие (2). Ясно, что такая машина Тьюринга существует.

Список литературы

1. Воронцов К. В. Оптимизационные методы линейной и монотонной коррекции в алгебраическом подходе к проблеме распознавания // ЖВМ и МФ. — 2000. — Т. 40, № 1. — С. 166–176.

2. Сапоженко А. А., Сумкина Н. В. О тупиковых доопределениях частичных монотонных булевых функций // Математические вопросы кибернетики. Вып. 13, М.: Физматлит, 2004. — С. 289–294.

3. Махина Г. А. Тупиковые доопределения частичных монотонных булевых функций из класса $(n, 1, k)$ // Таврический вестник информатики и математики. — 2006. — № 2. — С. 69–74.

4. Карп Р. М. Сводимость комбинаторных проблем //Кибернетический сборник. Вып. 12. — М.: Мир, 1975. — С. 16–38.

К ВОПРОСУ О МАТЕМАТИЧЕСКОМ МОДЕЛИРОВАНИИ НА ГРАФАХ ЗАДАЧИ ЗЕМЛЕПОЛЬЗОВАНИЯ

В. А. Перепелица (Ставрополь), Ф. Б. Тебуева (Черкесск)

Предметом исследования настоящей работы являются различные постановки дискретных задач управления: задача землепользования [1], задача обучения сотрудников организации [2], задача назначения учителей в классы с учетом технологий обучения [3], задача выбора стратегии ведения строительства строительной компанией [4] и т. д. Для математического моделирования значительного количества дискретных систем оказывается вполне достаточным использование аппарата теории графов. Однако, нередки случаи, когда не удается достичь требуемой адекватности в силу невозможности отразить в системном единстве сложную организацию их внутренних возможностей. Поэтому возникает необходимость использования инструментария гиперграфов [5].

Математическая модель задачи землепользования, которая в [1] представлена на 2-дольном графе, в случае учета ограниченного ресурса удобрений обобщается путем использования инструментария гиперграфов при выполнении следующего условия: имеющийся запас удобрений разделен на “порции”, каждая из которых используется

полностью для какой-либо пары вида "культура, поле" из определенного для фиксированной "порции" перечня (в работе [1] эти пары представлены соответственно ребрами 2-дольного графа). Список "всех порций" удобрений будем представлять в виде множества вершин $V_3^0 = \left\{v_1^3, v_2^3, ..., v_n^3\right\}$.

Для определения допустимого решения рассматриваемой задачи используется следующее

Определение 1. *Звездой гиперграфа* $G = (V, E)$ называется такая его связная часть $z = (V_z, E_z)$, в которой всякая пара ребер $e', e'' \in E_z$ пересекается в одной же вершине $v_0 \in V$ и не пересекаются ни в какой-либо другой вершине $v \neq v_0$. При этом вершина v_0 называется центром звезды z, а число ребер $|E_z|$ называется ее степенью.

Определение 2. Для заданных натуральных чисел

$$q_k, \quad k = \overline{1, m}, \quad \sum_{k=1}^{m} q_k = n \tag{1}$$

допустимым покрытием 3*-дольного* 3*-однородного гиперграфа* $G = (V_1, V_2, V_3, E)$ *звездами* является всякий его остовный подгиперграф $x = (V_1, V_2, V_3, E_x)$, состоящий из m компонент, каждая из которых является звездой с центром в одной из вершин первой доли V_1; при этом звезда с центром $v_k^1 \in V_1$ имеет степень, равную числу q_k, $1 \leqslant k \leqslant m$.

Допустимое покрытие гиперграфа G называем допустимым решением; множество всех допустимых решений (МДР) обозначим через $X = X(G) = \{x\}$.

Цель какой-либо конкретной (индивидуальной [6]) задачи землепользования — найти такое допустимое решение $x^0 \in X$, на котором целевая функция (ЦФ) принимает требуемое экстремальное значение (min или max):

$$F(x) = \sum_{e \in E_x} w(e) \to extr, \quad extr \in \{\max, \min\}. \tag{2}$$

Определение 3. Для (nl)-вершинного l-однородного гиперграфа его сочетание $S(n)$, состоящее из n ребер, называется *совершенным сочетанием* (СС).

Определение 4. Термин "задача о совершенном сочетании" подразумевает нахождение во взвешенном гиперграфе такого СС, на котором ЦФ вида (1) достигает требуемого экстремума.

В определении 2 сформулирована с учетом (1) задача покрытия графа звездами $m + 2n$-вершинного 3-дольного гиперграфа

$$G = (V_1, V_2, V_3, E), \quad |V_1| = m, \quad |V_2| = |V_3| = n, \quad m < n. \qquad (3)$$

Эта задачу можно свести к задаче о совершенном сочетании на гиперграфе вида (3).

Утверждение 1. *Задача покрытия звездами 3-дольного 3-однородного гиперграфа G полиномиально сводится к задаче о совершенном сочетании гиперграфа $\overline{G}$, производного от G.*

Утверждение 2. *Задача распознавания покрытия 3-дольного 3-однородного графа является NP-полной, в оптимизационной постановке эта задача является NP-трудной.*

Из утверждения 2 вытекает, что к настоящему времени отсутствуют полиномиальные алгоритмы для задач покрытия гиперграфов звездами (совершенными паросочетаниями). Отсюда очевидна актуальность нахождения полиномиально разрешимых подклассов, в которых выполняются следующие условия:

1) МДР $X = \{x\}$ определяется на 3-дольном 3-однородном гиперграфе $G = (V_1, V_2, V_3, E)$ вида (3) и состоит из допустимых покрытий этого гиперграфа звездами;

2) ЦФ имеет вид (2);

3) для каждого ребра $e = \left(v_k^1, v_i^2, v_j^3\right) \in E$ его вес $w(e)$ определяется равенством вида $w(e) = \varphi(k, i) + \delta_j \varphi(k, i)$.

Содержательный смысл последнего условия можно проиллюстрировать в терминах экономико-математической модели землепользования: внесение конкретной "порции" удобрения повышает урожай на процент, одинаковый для каждой культуры и зависящей только от номера j вносимой "порции".

При выполнении условий 1–3 нахождение оптимального решения $x^0 \in X(G)$ сводится к решению двух задач о назначениях размерности n. Отсюда вычислительная сложность нахождения x^0 ограничена сверху полиномом $O\left(n^3\right)$.

Работа выполнена при поддержке РФФИ, проект № 06-01-00020а.

Список литературы

1. Максишко Н. К., Перепелица В. А., Заховалко Т. В. Теоретико-графовая эколого-экономическая модель задачи землепользования //Вісник Східоукраінського національного університету ім. В. Даля. — 2002. — № 2 (48). — С. 92–100.

2. Джуэлл Л. Индустриально-организационная психология. — СПб.: Питер, 2001.

3. Пищулин Н. П., Ананишнев В. М. Образование и управление. — М.: Жизнь и мысль, 1999.

4. Ильин Н. И., Лукманова И. Г. и др. Управление проектами. — СПб.: Два-Три, 1996.

5. Емеличев В. А., Мельников О. И., Сарванов В. И., Тышкевич Р. И. Лекции по теории графов. — М.: Наука, 1990.

6. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

МАГИЧЕСКАЯ СИЛА ЦИЛИНДРИЧЕСКИХ РЕШЕТОК

А. Я. Петренюк (Кировоград)

Нумерацией графа $G = (V, E)$ называют отображение $\varphi : E \to N$ множества E ребер графа G во множество натуральных чисел. Номером ребра $xy \in E$ называют образ $\varphi(xy)$ этого ребра при отображении φ. Назовем стяжкой вершины $x, x \in V$, сумму номеров всех тех ребер графа G, которые инцидентны вершине x. Нумерация графа называется магической, если все вершины графа имеют в этой нумерации одну и ту же стяжку. Общее значение стяжек вершин называют стяжкой (магической) нумерации. Граф G магический, если он допускает магическую нумерацию. Магической силой нумерации φ графа G называют наибольший из номеров ребер, присутствующий в этой нумерации. Магическая сила $\mu(G)$ графа G — наименьшая магическая сила допускаемых графом G магических нумераций. Задача состоит в том, чтобы для данного графа G выяснить, магический он или нет, и если G магический — определелить $\mu(G)$. Цилиндрическая $m \times n$ решетка $Cyl(m, n)$ получается склейкой двух ее противоположных сторон, имеющих длины n.

Теорема 1. *Цилиндрическая $m \times n$ решетка $Cyl(m, n)$ при произвольном четном $m \geq 4$ и $n \geq 2$ представляет собой магический граф с магической силой* 2.

Доказательство дает магическая нумерация, получаемая присвоением номера 2 тем ребрам, которые лежат на краях цилиндрической решетки, через одно; остальным ребрам присваиваются номера 1. Графы $Cyl(m, n)$ при $n = 1, 2$ и произвольных значениях $m \geq 3$ являются регулярными и, следовательно, магическими с магической силой 1. В случае нечетных $m \geq 3$ полного решения задачи мы пока представить не можем. Даем решение отдельных случаев.

Теорема 2. *Граф $Cyl(3, 3)$ магический и $\mu(Cyl(3, 3)) = 3$.*

В качестве доказательства приводим две магические нумерации φ_1 и φ_2 графа $Cyl(3,3)$ с магической силой 3.

xy	12	13	14	23	25	36	45	46	47	56	58	69
$\varphi_1(xy)$	3	2	1	2	1	2	3	1	1	1	1	2
$\varphi_2(xy)$	3	2	1	2	1	2	2	2	1	1	2	1

xy	78	79	89
$\varphi_1(xy)$	3	2	2
$\varphi_2(xy)$	2	3	2

Теорема 3. *Граф* $Cyl(3,4)$ *магический и имеет магическую силу* 3.

Вот соответствующая магическая нумерация этого графа.

xy	12	13	14	23	25	36	45	46	47	56	58
$\varphi(xy)$	3	2	1	2	1	2	3	1	1	1	1

69	78	79	7,10	89	8,11	9,12	10,11	10,12	11,12
2	1	1	3	1	3	2	1	2	2

Предположение. При всех нечетных значениях $m \geq 3$ граф $Cyl(m,n)$ магический и имеет магическую силу 3.

Список литературы

1. Kong M. C., Sin-min Lee, Sun H. S. A. On the magic strength of graphs // Ars Combinatoria. — 1997. — V. 45. — P. 193–200.

2. Сапроненко Т. Про магічну силу графу // Студентська наука: проблеми і перспективи XXI століття. Зб. матеріалів Четвертої Всеукранської студентської науково-практичної конференції (14–15 травня 2004 року). — Кіровоград, 2004. — P. 113–114.

ИССЛЕДОВАНИЕ КУБИЧЕСКИХ РАЗЛОЖЕНИЙ ГРАФА K_{13}

Д. А. Петренюк (Киев)

В [1] получен полный список типов кубических разложений полных графов порядка 13. Он содержит 97 типов. На повестку дня

вышла задача перечисления, с точностью до изоморфизма, реализаций каждого типа. Мы начнем с указания на то, что в теории блок-схем имеется классический результат [2], который сегодня можно сформулировать в следующем виде.

Теорема 1. *С точностью до изоморфизма существует единственное кубическое разложение графа* K_{13} *типа* 97=(13,0,0,0,0).

Это подсказало начать исследование с тех разложений, которые имеют "много" малых компонент K_4. На этом пути мы получили результаты, представленные ниже.

Теорема 2. *С точностью до изоморфизма существует единственное кубическое разложение графа* K_{13} типа 94=(10,0,0.1).

Мы строили дополнения каждого кубического графа порядка 12, взятого из [3], такими наборами графов K_4, которые вместе с достраиваемым графом образовывали кубическое разложение графа K_{13}. Оказалось, что единственный граф из списка [3], допускающий такую достройку, тоже единственную, имеет номер 59 в этом списке. Соответствующее разложение таково: 1-2 1-3 1-4 2-3 2-5 3-6 4-7 4-8 5-9 5-10 6-11 6-12 7-8 7-9 8-11 9-10 10-12 11-12; 1 5 8 12; 1 6 7 10; 1 9 11 13; 2 4 10 11; 2 6 8 9; 2 7 12 13; 3 4 9 12; 3 5 7 11; 3 8 10 13; 4 5 6 13, где компонента порядка 12 задана списком ребер, а компоненты порядка 12 задана списком ребер, а компоненты порядка 4 — списками вершин.

Теорема 3. *Не существует кубических разложений порядка* 13, имеющих тип 96=(11,0,1,0.0).

В самом деле, оказалось, что с кубическими графами порядка 8, имеющими в списке [3] номера 1 и 2, совмещаются в K_{13} не более 9, а с остальными кубическими графами порядка 8 — не более 8 графов K_4.

Теорема 4. *Не существует кубических разложений порядка* 13, *имеющих тип* 95=(10,2,0,0.0).

Кубический граф порядка 6 (призма или K_{33}) совмещается в K_{13} не более, чем с 9 графами K_4, а это исключает существование разложений типа 95.

Теорема 5. *С точностью до изоморфизма, существует единственное кубическое разложение порядка* 13, *имеющее тип* 93=(9,1,0.1.0).

Это разложение имеет вид 1-2 1-3 1-4 2-3 2-5 3-6 4-7 4-8 5-7 5-9 6-8 6-10 7-9 8-10 9-10; 1 5 8 11; 1 6 9 12; 1 7 10 13; 2 4 10 12; 2 6 7 11; 2 8 9 13; 3 4 9 11; 3 7 8 12; 4 5 6 13; 3-5 3-10 3-13 5-10 5-12 10-11 11-12 11-13 12-13.

Теорема 6. *С точностью до изоморфизма существуют точно два кубических разложения порядка* 13, *имеющие тип* 92=(9,0,22.0.0).

Приводим эти разложения:

1) 1-2 1-3 1-4 2-3 2-4 3-5 4-6 5-7 5-8 6-7 6-8 7-8; 2-6 2-8 2-11 4-8 4-9 4-10 6-11 6-12 8-10 9-10 9-12 11-12; 1 5 6 9; 1 7 8 10; 1 11 12 13; 2 5 10 11; 2 6 7 12; 2 8 9 13; 3 4 7 11; 3 6 10 13; 4 9 10 12;

2) 1-2 1-3 1-4 2-3 2-5 3-6 4-5 4-7 5-8 6-7 6-8 7-8; 2-4 2-8 2-11 3-4 3-7 3-8 4-12 5-7 5-11 5-12 7-12 8-11; 1 5 6 9; 1 7 10 11; 1 8 12 13; 2 6 10 12; 2 7 9 13; 3 5 10 13; 3 9 11 12; 4 6 11 13; 4 8 9 10.

Список литературы

1. Петренюк Д. А. Перелік можливих типів кубічних розкладів графу K_{13} //Третя міжнародна науково-практична конференція "Математичне та програмне забезпечення інтелектуальних систем (MPZIS -2005)". Тези доповідей. (16–18 листопада 2005 року). — Дніпропетровськ, 2005. — С. 137–138.

2. MathonR., Rosa A. Tables of parameters of BIBDs with $r \leq 41$ including existence, enumeration and resolvability results: an update // Ars Combinatoria. — 1990. — V. 30. — P. 65–96.

3. Бараев А. М., Фараджев Н. А. Построение и исследование на ЭВМ однородных и однородных двудольных графов // Алгоритмические исследования в комбинаторике. — Москва, 1978. — С. 25–60.

МИНИМАЛЬНЫЕ ИДЕМПОТЕНТНЫЕ РАСШИРЕНИЯ СВЯЗНЫХ ГРАФОВ

В. Н. Салий (Саратов)

Пусть $\Pi = (\pi_1, \pi_2, \ldots, \pi_k)$ — некоторый набор графовых параметров. Через $\Pi_0 = (\pi_1^0, \pi_2^0, \ldots, \pi_k^0)$ обозначим одну из допустимых конкретизаций набора Π, а через $\Pi(G)$ — его конкретизацию, соответствующую графу G. Граф G называется Π_0-графом, если $\Pi(G)=\Pi_0$. Укажем те графовые параметры, которые встретятся нам далее: число связности c, индекс i, период p и число вершинного покрытия a. Число связности графа G — это количество $c(G)$ его компонент связности. Равенство $c(G) = 1$ означает, что G — связный граф. Пусть A — матрица смежности графа G. Наблюдая последовательность различных ее степеней $A, A^2, A^3, \ldots$, заметим, что эта последовательность конечна и что, если A^m — ее последний элемент, то $A^{m+1} = A^l$ для некоторого $l \leq m$. Число $i(A) = l - 1$ называется индексом матрицы A, а число $p(A) = (m + 1) - l$ называется ее

периодом. По определению $i(G) = i(A)$, $p(G) = p(A)$,— индекс и период графа G [1]. Число вершинного покрытия $a(G)$ графа G — это наименьшее количество вершин, в совокупности инцидентных всем дугам.

Положим $\Pi = (c, i, p)$ и $\Pi_0 = (1, 0, 1)$. Таким образом, Π_0-графом при таком выборе будет связный граф, у которого $A^2 = A$, т.е. матрица смежности идемпотентна, в этом случае и сам граф можно назвать идемпотентным.

Пусть G — произвольный связный граф. Для заданного Π_0 требуется найти граф $G' = (V, \alpha')$, где $\alpha \subseteq \alpha'$, такой, чтобы $\Pi(G') = \Pi_0$. Граф G' естественно назвать Π_0-расширением графа G. Особый интерес представляет случай, когда G' имеет наименьшее возможное число добавочных дуг, т.е. является минимальным Π_0-расширением для G. В доказываемой ниже теореме предлагается процедура отыскания минимального идемпотентного расширения связного графа.

Напомним, что отношение $\rho \subseteq V \times V$ на множестве V называется транзитивным, если $\rho^2 \subseteq \rho$, т.е. если $(x, y) \in \rho \& (y, z) \in \rho \Rightarrow (x, z) \in \rho$ для всех $x, y, z \in V$, и называется плотным, если $\rho \subseteq \rho^2$, т. е. если $(x, z) \in \rho \Rightarrow (\exists y \in V)((x, y) \in \rho \& (y, z) \in \rho$ для всех $x, y, z \in V$. Наименьшим транзитивным отношением, содержащим ρ, является транзитивное замыкание $\tau(\rho) = \bigcup_{k \geq 1} \rho^k$. Если множество V состоит из n элементов, то, как известно (см.[2]), $\tau(\rho) = \bigcup_{k=1}^{n} \rho^k$. Очевидным идемпотентным расширением отношения ρ является его транзитивно-рефлексивное замыкание $\tau_\Delta = \tau \cup \Delta_V$, где Δ_V — тождественное отношение на множестве V.

Теорема. *Следующая процедура строит для связного графа $G = (V, \alpha)$ одно из его минимальных идемпотентных расширений $G' = (V, \alpha')$.*

1) *Найти отношение $\tau_0 = \bigcup_{k \geq 2} \alpha^k$.*

2) *Если $\alpha - \tau_0 = \emptyset$, — конец: $\alpha' = \alpha \cup \tau_0 = \tau$ (транзитивное замыкание отношения α).*

3) *Если $\alpha - \tau_0 \neq \emptyset$, в графе $G_0 = (V_0, \alpha - \tau_0)$, где V_0 — множество всех вершин графа G, инцидентных дугам из $\alpha - \tau_0$, найти одно из вершинных покрытий V_a мощности $a(G_0)$.*

4) *Положить $\alpha' = \tau \cup \Delta_a$, где Δ_a — тождественное отношение на множестве V_a.*

Доказательство. Согласно замечаниям, сделанным перед формулировкой теоремы, если $G' = (V, \alpha')$ — искомое расширение графа G, то получаем, что $|\tau| \leq |\alpha'| \leq |\tau_\Delta|$.

Так как отношение τ транзитивно, то идемпотентным оно будет в том случае, когда обладает свойством плотности $\tau \subseteq \tau^2$. Покажем,

что это равносильно соотношению $\alpha - \tau_0 = \emptyset$.

В самом деле, если $\tau \subseteq \tau^2$, то для любой пары $(u, v) \in \alpha \subseteq \tau$ найдется вершина $w \in V$ такая, что $(u, w), (w, v) \in \tau$. Но тогда $(u, v) \in \tau_0$, откуда $\alpha \subseteq \tau_0$ и $\alpha - \tau_0 = \emptyset$. С другой стороны, пусть $\alpha - \tau_0 = \emptyset$, т.е. $\alpha \subset \tau_0$. Тогда $\tau = \alpha \cup \tau_0$. Следовательно, при $(u, v) \in \tau$ существуют $u_1, u_2, \ldots, u_k \in V$ такие, что $(u, u_1), (u_1, u_2), \ldots, (u_k, v) \in \alpha \subseteq \tau$. В силу транзитивности, $(u, v_k) \in \tau$. А так как $(u_k, v) \in \tau$, то $(u, v) \in \tau^2$. Итак, $\tau \subseteq \tau^2$. Таким образом, если $\alpha - \tau_0 = \emptyset$, то $\alpha' = \alpha \cup \tau_0 = \tau$.

Пусть теперь $\alpha - \tau_0 \neq \emptyset$. Если $(u, v) \in \alpha - \tau_0$, то в G не существует вершины w такой, что $(u, w), (w, v) \in \alpha$, и, значит, τ не содержится в τ^2. Найдем в графе $G_0 = (V_0, \alpha - \tau_0)$ одно из вершинных покрытий V_a мощности $a(G_0)$ и в графе (V, τ) каждую вершину, входящую в V_a снабдим петлей. Очевидно, что полученный граф $G' = (V, \alpha')$, где $\alpha' = \tau \cup \Delta_a$, является идемпотентным графом и содержит исходный граф G в качестве остовной части.

Покажем, что G' — минимальное идемпотентное расширение для G. Пусть $G^* = (V, \alpha^*)$ — произвольное идемпотентное расширение графа G. Так как $\alpha \subseteq \alpha^*$ и α^* транзитивно, то $\tau \subseteq \alpha^*$. Пусть $(u, v) \in \alpha - \tau_0$. Поскольку $\alpha \subseteq \alpha^*$, найдется вершина $w \in V$ такая, что $(u, w), (w, v) \in \alpha^*$. При этом по крайней мере одна из этих дуг не входит в τ, иначе $(u, v) \in \tau^2 \subseteq \tau_0$. Выберем эту дугу и поступим аналогично для каждой дуги из $\alpha - \tau_0$. Множество выбранных дуг обозначим через β. Отношение α^* разбивается на три части: τ, β и γ, где $\gamma = \alpha^* - (\tau \cup \beta)$.

Далее, для каждой дуги $(u, v) \in \alpha - \tau_0$ пометим вершину u, если в β есть дуга с началом u, и пометим вершину v, если в β есть дуга с концом v. Множество U помеченных вершин образует вершинное покрытие для множества дуг $\alpha - \tau_0$. При этом $|U| \leq |\beta|$. Покажем, что граф $G_U = (V, \tau \cup \Delta_U)$ является идемпотентным расширением для графа G. В самом деле, $(\tau \cup \Delta_U)^2 = \tau^2 \cup \tau \circ \Delta_U \cup \Delta_U \circ \tau \cup \Delta_U \subseteq \tau \cup \Delta_U$ (транзитивность) и, если $(u, v) \in \tau \cup \Delta_U$, то $(u, v) \in (\alpha - \tau_0) \cup \tau_0 \cup \Delta_U = ((\alpha - \tau_0) \cup \Delta_U) \cup \tau_0$, откуда $(u, v) \in (\alpha - \tau_0) \circ \Delta_U \cup \Delta_U \circ (\alpha - \tau_0) \subseteq \tau \circ \Delta_U \cup \Delta_U \circ \tau$ при $(u, v) \in \alpha - \tau_0$, или $(u, v) \in \tau_0^2 \subseteq \tau^2$ при $(u, v) \in \tau_0$, или $(u, v) \in \Delta_U$, т.е. $(u, v) \in (\tau \cup \Delta_U)^2$, откуда $\tau \cup \Delta_U \subseteq (\tau \cup \Delta_U)^2$ (плотность).

Поскольку U — это вершинное покрытие множества дуг $\alpha - \tau_0$, а V_a — минимальное вершинное покрытие для $\alpha - \tau_0$, то получаем: $|\alpha'| = |\tau \cup \Delta_a| \leq |\tau| + |\Delta_a| \leq |\tau| + |\beta| \leq |\alpha^*|$, так как $\alpha^* = \tau \cup \beta \cup \gamma$. Следовательно, $G' = (V, \alpha')$ — минимальное идемпотентное

расширение для G.

Теорема доказана.

Для оценки временной сложности процедуры, предложенной в теореме, заметим, что транзитивное замыкание отношения вычисляется за полиномиальное время, однако для нахождения минимального вершинного покрытия графа приходится просматривать все подмножества множества его вершин.

Работа выполнена при финансовой поддержке РФФИ (проект 05-08-18082).

Список литературы

1. Салий В. Н. Отказоустойчивость и оптимизация дискретных систем с заданными индексом и периодом // Вестник ТГУ. Приложение. — 2006. — № 17. — С. 222–225.

2. Schwarz St. On idempotent binary relations on a finite set // Czech. Math. J. — 1970. — V. 20 (95). — № 4. — P. 696–702.

ОБ ЭНТРОПИЙНОЙ МИНИМАЛЬНОСТИ ПРАВИЛЬНЫХ РЕГУЛЯРНЫХ КОМПОЗИЦИЙ В СЕМЕЙСТВЕ НАСЛЕДСТВЕННЫХ КЛАССОВ ЦВЕТНЫХ ГРАФОВ

С. В. Сорочан (Нижний Новгород)

В [1] было введено понятие *цветного графа*, или q*-графа*. Если $Q = \{1, 2, \ldots, q\}$ — множество цветов, то q*-графом* с множеством вершин V называется пара $G = (V, g)$, где $g : V^{(2)} \to Q$, а $V^{(2)}$ — множество всех неупорядоченных пар различных элементов множества V. Для произвольного непустого множества $M \subseteq Q$ через $\mathcal{O}^{\langle q \rangle}(M)$ будем обозначать класс таких q-графов, для которых $g(V^{(2)}) \subseteq M$.

Подграф G' цветного графа $G = (V, g)$, порожденный множеством $V' \subseteq V$ — это цветной граф (V', g'), где g' — ограничение g на V'. Этот подграф обозначается через $G\langle V' \rangle$.

Класс $\mathcal{X}^{\langle q \rangle}$ q-графов называется *наследственным* (или *фрагментно замкнутым*), если в нем содержится каждый q-граф, изоморфный порожденному подграфу графа $G \in \mathcal{X}^{\langle q \rangle}$.

Если V и U — непересекающиеся множества, то *двудольным* q*-графом* с неупорядоченными долями V и U [2] называется тройка

(V, U, g), где $g : V \times U \to Q$. Для непустого $P \subseteq Q$ множество всех двудольных q-графов, для которых $g(V \times U) \subseteq P$, будем обозначать через $\mathcal{B}^{\langle q \rangle}(P)$. Понятие наследственного класса распространяется на двудольные цветные графы очевидным образом. Двудольный подграф заданного q-графа G, порожденный долями V и U, $V, U \subseteq V(G)$, $V \cap U = \emptyset$ и удалением всех ребер, принадлежащих одной и той же доле, будем обозначать через $G\langle V, U\rangle$.

Пусть $\mathcal{X}$ и $\mathcal{Y}$ — произвольные бесконечные наследственные классы q-графов и двудольных q-графов соответственно. Обозначим через $\mathcal{X}_n$ совокупность q-графов из $\mathcal{X}$ с множеством вершин $\{1, \ldots, n\}$, а через $\mathcal{Y}_{n_1,n_2}$ — множество двудольных q-графов из $\mathcal{Y}$, в которых $V = \{1, 2, \ldots, n_1\}$, $U = \{n_1 + 1, n_1 + 2, \ldots, n_1 + n_2\}$. В [2] доказано, что существуют пределы $h(\mathcal{X}) = \lim\limits_{n\to\infty} \log_q |\mathcal{X}_n| \,/ \binom{n}{2}$ и $h_{\mathcal{B}}(\mathcal{Y}) = \lim\limits_{\substack{n_1\to\infty \\ n_2\to\infty}} \log_q |\mathcal{Y}_{n_1,n_2}|/(n_1 n_2)$, называемые соответственно *энтропией* класса $\mathcal{X}$ и *двудольной энтропией* класса $\mathcal{Y}$. В частности, $h(\mathcal{O}(M)) = \log_q |M|$ и $h_{\mathcal{B}}(\mathcal{B}(P)) = \log_q |P|$.

Наследственный класс $\mathcal{X}$ q-графов называется *минимальным* (*по включению*) [3] среди наследственных классов с энтропией, равной h, если энтропия любого наследственного класса, собственно содержащегося в $\mathcal{X}$, меньше h.

В [2, 3] были исследованы специальные фрагментно замкнутые классы q-графов, названные композициями. Они определяются следующим образом. Пусть для каждой пары (i, j), где $1 \le i \le j \le k$ и $k \ge 2$, при $i = j$ выбран некоторый бесконечный наследственный класс $\mathcal{X}^{ii}$ q-графов, а при $i \ne j$ — некоторый бесконечный наследственный класс $\mathcal{X}^{ij}$ двудольных q-графов. Положим $\mathcal{X}^{ji} = \mathcal{X}^{ij}$ при любых $i < j$. Множество всех выбранных классов обозначим через $\widetilde{\mathcal{X}}^{(k)}$. Тогда *$k$-композицией* $C(\widetilde{\mathcal{X}}^{(k)}) = \left\|\mathcal{X}^{ij}\right\|_{i,j=1}^{k}$ *наследственных классов q-графов из* $\widetilde{\mathcal{X}}^{(k)}$ [2, 3] называется совокупность таких q-графов G, что множество вершин в G можно разбить на непересекающиеся подмножества $V_1, \ldots, V_k$ (некоторые из них могут быть пустыми) так, что $G\langle V_i\rangle \in \mathcal{X}^{ii}$, $G\langle V_i, V_j\rangle \in \mathcal{X}^{ij}$ при всех $i \ne j$, $i, j = 1, \ldots, k$.

Каждой k-композиции $C(\widetilde{\mathcal{X}}^{(k)})$ соответствует симметрическая квадратная матрица $H_{(k)} \equiv H = (h^{ij})$ порядка k, в которой $h^{ii} = h(\mathcal{X}^{ii})$ и $h^{ij} = h_{\mathcal{B}}(\mathcal{X}^{ij})$, $i \ne j$, $i, j = 1, \ldots, k$, называемая *матрицей энтропий* k-композиции $C(\widetilde{\mathcal{X}}^{(k)})$.

Для описания значений энтропии композиций наследственных классов цветных графов в [2] было произведено их разделение на регулярные и нерегулярные композиции. Пусть H — матрица энтропий k-композиции $C(\widetilde{\mathcal{X}}^{(k)})$ наследствен ных классов q-графов из $\widetilde{\mathcal{X}}^{(k)}$, а Q — матрица размера $k \times (k-1)$, в столбцах которой записаны векторы произвольного базиса линейного пространства решений уравнения $\mathbf{1}^\top \mathbf{x} = 0$. Тогда $C(\widetilde{\mathcal{X}}^{(k)})$ называется *регулярной k-композицией* [2], если, во-первых, матрица $Q^\top H Q$ является отрицательно определенной (требование максимальности) и, во-вторых, справедливо векторное неравенство $H^{-1}\mathbf{1} > \mathbf{0}$, т. е. каждая компонента вектора $H^{-1}\mathbf{1}$ положительна (условие внутренней допустимости). В противном случае $C(\widetilde{\mathcal{X}}^{(k)})$ называется *нерегулярной* k-композицией.

Было доказано (теорема 2 из [2]), что энтропия каждой регулярной k-композиции $C(\widetilde{\mathcal{X}}^{(k)})$ вычисляется по формуле $h\left(C(\widetilde{\mathcal{X}}^{(k)})\right) = 1/(\mathbf{1}^\top H^{-1}\mathbf{1})$, а энтропия любой нерегулярной композиции равна максимальной энтропии целиком содержащейся в ней композиции с меньшим количеством секций.

Из этой теоремы следует, что любая нерегулярная композиция не является минимальным (по включению) классом среди наследственных классов q-графов с заданным значением энтропии.

Кроме того, из теоремы 2 [2] вытекает, что энтропийно минимальные наследственные классы q-графов имеет смысл искать в множестве регулярных композиций. В настоящей работе обнаружены некоторые энтропийно минимальные классы, являющиеся, в основном, представителями регулярных композиций.

Теорема 1. *Для каждого непустого множества $M \subseteq Q$ класс $\mathcal{O}^{\langle q \rangle}(M)$ является минимальным среди классов с энтропией, равной* $\log_q |M|$.

Композицию $C(\widetilde{\mathcal{X}}^{(k)})$ назовем *правильной k-композицией наследственных классов q-графов* [3], если $\mathcal{X}^{ii} = \mathcal{O}^{\langle q \rangle}(M_{ii})$ для некоторого непустого $M_{ii} \subset Q$, $i = 1, \ldots, k$, а $\mathcal{X}^{ji} = \mathcal{X}^{ij} = \mathcal{B}^{\langle q \rangle}(P_{ij})$ для некоторого непустого $P_{ij} \subseteq Q$, $1 \le i < j \le k$.

В [3] было установлено (теорема 2 из [3]), что каждая правильная регулярная композиция является энтропийно минимальным классом среди композиций наследственных классов q-графов. Оказывается, справедливо более сильное утверждение.

Теорема 2. *Каждая правильная регулярная композиция являет-*

ся энтропийно минимальным классом семейства всех наследственных классов q-графов.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проект 06-01-00553-а.

Список литературы

1. Алексеев В. Е. Область значений энтропии наследственных классов графов // Дискретная математика. — 1992. — Т. 4, вып. 2. — С. 148–157.

2. Сорочан С. В. Об энтропии композиций наследственных классов цветных графов // Дискретный анализ и исследование операций. Серия 1. — 2002. — Т. 9, № 1. — С. 59–83.

3. Сорочан С. В. О регулярных композициях наследственных классов цветных графов // Дискретный анализ и исследование операций. Серия 1. — 2003. — Т. 10, № 1. — С. 79–104.

РУССКИЕ СНАРКИ (О 4-ХРОМАТИЧЕСКИХ ПО РЕБРАМ КУБИЧЕСКИХ ГРАФАХ)

В. К. Титов (Москва)

Цель работы — закрепить приоритет автора в построении бесконечного класса графов, получивших название *снарки*, так как часто стали появляться ссылки на более поздние работы, повторяющие этот результат [1, 2].

Известно, что в любом кубическом (однородном со степенью вершин 3) графе ребра можно раскрасить правильно (так, чтобы смежные ребра имели разные цвета) в 3 или 4 цвета. Назовем кубический граф, ребра которого невозможно правильно раскрасить в 3 цвета 4-*хроматическим*. *Циклическим разрезом* графа называется множество его ребер, удаление которых приводит к несвязному графу, каждая компонента связности которого содержит хотя бы один цикл. Граф называется *k-циклически связным*, если он не имеет циклического разреза с числом ребер меньшим k. *Снарком* называется кубический 4-хроматический 4-циклически связный граф.

Широкий интерес к этим графам возник в связи со знаменитой гипотезой о четырех красках. С легкой руки известного популяризатора математики Мартина Гарднера эти графы получили название "снарки" [3]. Если бы удалось построить планарный снарк, это было

бы опровержением этой гипотезы. Долгая непробиваемость проблемы четырех красок и привела к поиску планарных снарков в уверенности, что гипотеза неверна. Но даже поиск непланарных снарков оказался нелегкой задачей. Поэтому М. Гарднер сравнил эти графы с неуловимыми животными, назвав их снарками, взяв этот термин из книги "Охота на снарка" известного английского писателя Льюиса Кэрролла, автора знаменитых "Алиса в стране чудес" и "Алиса в Зазеркалье".

Простейшим снарком является граф, известный как граф Петерсена (рис. 1), число скрещиваний которого равно 2 (наименьшее число пересечений ребер при расположении графа на плоскости, см. рис. 1-А). Первым, кто построил снарк, отличный от графа Петерсена, был Бланш Декарт [4] (псевдоним молодого У. Татта). Его граф, опубликованный в 1948 году, содержит 210 вершин.

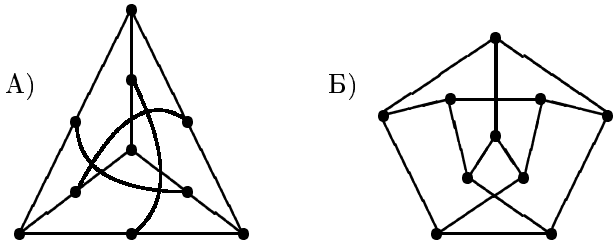


Рис. 1. Граф Петерсена.

Мною еще в 1970 году был построен бесконечный класс снарков, о чем был сделан доклад на расширенном семинаре по комбинаторной математике в МГУ в январе 1971 года, и что было опубликовано в 1973 году в трудах этого семинара [5, 6]. Построение снарков основано на введенной автором операции над двумя кубическими графами, названной *С-композицией графов* $G_1 * G_2$, показанной на рис. 2.

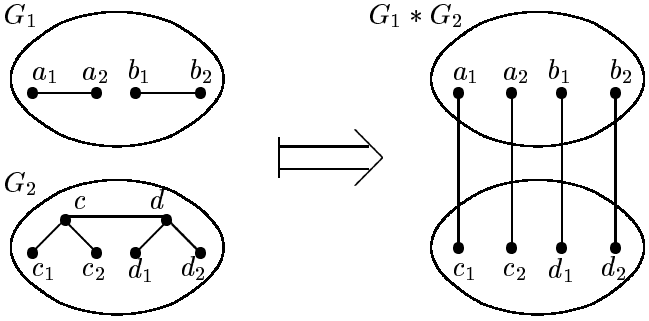


Рис. 2. С-композиция графов $G_1 * G_2$

В этой операции в одном из графов удаляются два несмежных ребра, в другом удаляются две смежные вершины с инцидентными им ребрами (удаляется 5 ребер). Затем в полученных графах вершины степени 2 соединяются 4-мя ребрами, как показано на рисунке.

Теорема 1 (теоремы 2 и 3 [5]). *Если G_1 и G_2 — снарки, то $G_1 * G_2$ — снарк.*

Теорема 2. (теорема 5 [5]). *Для любого четного $N \geq 18$ существует снарк с N вершинами.*

На рис. 3 показаны простейшие снарки после графа Петерсена с 18-ю вершинами, полученные из копий графа Петерсена C-композицией.

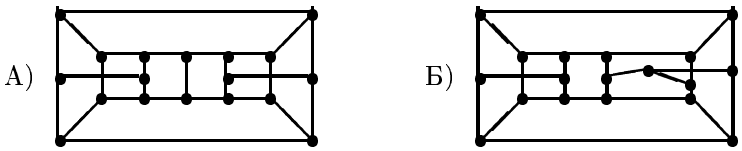


Рис. 3

Важно отметить, что C-композиция не увеличивает числа скрещиваний полученного графа по отношению к исходным графам, что видно на примере $K_{3,3} * K_{3,3}$, см. рис. 4.

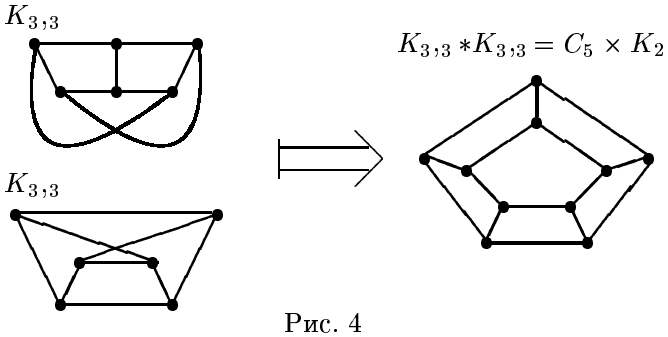


Рис. 4

В заключение отмечу, что дата нашей публикации оставляет приоритет в обсуждаемом вопросе за нами, что я и хотел подчеркнуть в названии работы: «Русские снарки».

Список литературы

1. Isaacs R. Infinite families of nontrivial trivalent graphs which are not Tait colorable // Amer. Math. Monthly. — 1975. — V. 82. — P. 221–239.

2. Preissmann M. Snarks of order 18 // Discrete Mathematics. — 1982. — V. 42. — P. 125–126.

3. Gardner M. Snarks, boojums and other conjectures related to the four-color-map theorem // Scientific American. — 1976. — V. 234, № 4. — P. 126–130.
4. Descartes B. Network-colourings // Math. Gazette. — London, 1948. — V. 32. — P. 67–69.
5. Адельсон-Вельский Г. М., Титов В. К. О 4-х хроматических по ребрам кубических графах // Вопросы кибернетики. Труды семинара по комбинаторной математике. — М.: Изд. АН СССР, 1973. — С. 5–14.
6. Титов В. К. К раскраске ребер графов с максимальной степенью вершин 3 // Вопросы кибернетики. Комбинаторный анализ и теория графов. — М.: Изд. АН СССР, 1976. — С. 98–110.

ИСПОЛЬЗОВАНИЕ СИСТЕМ РАЗЛИЧНЫХ ПРЕДСТАВИТЕЛЕЙ ПРИ РЕШЕНИИ ОПТИМИЗАЦИОННЫХ ЗАДАЧ НА ГРАФАХ

В. А. Турчина, Н. К. Федоренко (Днепропетровск)

Рассмотрим известную оптимизационную задачу упорядочения вершин графов.

Задача $S(G, l, h)$. По заданному графу G и заданной длине упорядочения $l(S)$ построить параллельное упорядочение S минимальной ширины $h(S)$ [1].

В общей постановке данная задача является NP-трудной. Представляет интерес выделение полиномиально разрешимых подклассов или поиск эффективных приближенных алгоритмов.

В работе рассматривается подход, основанный на использовании известного комбинаторного объекта — систем различных представителей — при решении данной задачи для одного частного случая.

Системой различных представителей (*СРП*) [2] для множеств $M_1 = \{m_1^1, m_1^2, \ldots, m_1^{k_1}\}$, $M_2 = \{m_2^1, m_2^2, \ldots, m_2^{k_2}\}$, $\ldots$, $M_n = \{m_n^1, m_n^2, \ldots, m_n^{k_n}\}$ называется такое множество $M = \{m^1, m^2, \ldots, m^n\}$, для которого выполняются следующие условия:

1) $m^i \in M_i, i = \overline{1, n}$;

2) $\forall i, j (i \neq j) : m^i \neq m^j$.

Обобщенной системой различных представителей (*ОСРП*) *с ограничением* h для множеств $M_1 = \{m_1^1, m_1^2, \ldots, m_1^{k_1}\}$, $M_2 =$

$\{m_2^1, m_2^2, \ldots, m_2^{k_2}\}$, $\ldots$, $M_n = \{m_n^1, m_n^2, \ldots, m_n^{k_n}\}$ называется такое множество $M = \{m^1, m^2, \ldots, m^n\}$, для которого выполняются следующие условия:

1) $m^i \in M_i, i = \overline{1,n}$;

2) $\forall i$ количество $m^j = m^i$ меньше h, где h — заданная константа.

Теорема (обобщение теоремы Холла). *Пусть I — конечное множество индексов, $I = \{1, 2, \ldots, n\}$, и M_i для каждого $i \in I$ — подмножество некоторого множества. Необходимым и достаточным условием существования ОСРП $M = \{m^1, m^2, \ldots, m^n\}$ с ограничением h является условие: для каждого $k = 1, 2, \ldots, n$ и каждой последовательности k различных индексов $i_1, i_2, \ldots, i_k$ в совокупности всех элементов подмножеств $M_{i_1}, M_{i_2}, \ldots, M_{i_k}$ содержится не менее $]\frac{k}{h}[$ различных элементов.*

Принято обзначать $\underline{S}$ ($\overline{S}$) такие допустимые упорядочения для графа G, в которых каждая вершина занимает соответственно крайнее левое (правое) допустимое место при неограниченной ширине. Тогда $\underline{l} = l(S)$, $\overline{l} = l(\overline{S}) = \underline{l}$, а $\underline{\mu_i}$ ($\overline{\mu_i}$) — номер места вершины i в упорядочении $\underline{S}$ ($\overline{S}$).

При решении задачи $S(G, \underline{l}, h)$ для каждой вершины i графа G построим множество — $\mu_i = \{t_i^j : t_i^j \in [\underline{\mu_i}, \overline{\mu_i}]\}$ — множество мест, на которых может стоять данная вершина.

Оптимальному упорядочению S вершин графа G поставим в соответствие множество $M = \{m^1, m^2, \ldots, m^n\}$, где m^i — номер места, занимаемого вершиной i в упорядочении M.

Очевидно, что множество $M = \{m^1, m^2, \ldots, m^n\}$ является ОСРП с ограничением h (h — ширина оптимального упорядочения S) для множеств μ_i.

Таким образом, построение оптимального упорядочения S для графа G можно свести, к построению ОСРП с ограничением h для множеств $\mu_i = t_i^j : t_i^j \in [\underline{\mu_i}, \overline{\mu_i}]$. Очевидным является также тот факт, что не всякой ОСРП будет соответствовать оптимальное упорядочение, поэтому при построении ОСРП следует учитывать порядок следования вершин, определяемый графом G.

Предлагается следующий алгоритм построения ОСРП и соответствующего ему оптимального упорядочения.

1. Для заданого графа G строим упорядочения $\underline{S}$, $\overline{S}$. Если $\underline{S} = \overline{S}$, то считаем, что оптимальное упорядочение $S = \underline{S} = \overline{S}$, конец алгоритма.

2. Для каждой вершины i графа G строим множество μ_i.

3. Оцениваем ширину оптимального упорядочения одним из известных способов, например:

$$h \geq \max \left(\left] \frac{n}{l} \right[, \widetilde{h} + \left] \max \left(0, \frac{|\widehat{S}| - \sum\limits_{r}^{i=1} \left(\widetilde{h} - |\widetilde{S}[i]| \right)}{r} \right) \right[\right),$$

где $\widetilde{S} = \overline{S} \cap \underline{S}, \widetilde{h} = h(\widetilde{S}), \widehat{S} = \overline{S}/\underline{S}$, $r : \widetilde{S}[m] \neq \emptyset$ и $\forall i \in (r, l] : \widehat{S}[i] = \emptyset$

4. Проверяем выполняется ли для множеств $\mu_i (i = \overline{1, n})$ условие обобщенной теоремы Холла; если нет увеличиваем h на 1 и повторяем шаг 4.

5. Каждому множеству μ_i ставим в соответствие метку ожидания d_i. Сначала полагаем все $d_i = 1$.

6. Полагаем $k = 1$ и $M = \emptyset$.

7. Вводим вспомогательные множества $U = \emptyset$ и $\widetilde{U} = \{j : k \in \mu_j$ и $d_j > 0\}$.

8. Выбираем i такое что:

$$i \in \widetilde{U}, |\mu_i| = \min_{\forall j \in \widetilde{U}} |\mu_j|, d_i = \max_{\forall j : |\mu_j| = |\mu_i|} d_j.$$

Если такого i не существует, то если $k = l$, увеличиваем h на 1 и переходим на шаг 6, иначе на шаг 12.

9. Если $\exists j : j \in U, d_j > d_i$ и ребро $(j, i) \in G$, переходим на шаг 11.

10. Полагаем $U = U \cup \{i\}, \widetilde{U} = \widetilde{U}/\{i\}, d_i = 0$. Если $|U| < h$, переходим на шаг 8, иначе на 12.

11. Полагаем $\widetilde{U} = \widetilde{U}/\{i\}$, переходим на шаг 8.

12. Полагаем $S[k] = U, M = M \cup U$.

13. $\forall i : d_i > 0$ и $k \in \mu_i$ полагаем $\mu_i = \mu_i/k$, $d_i = d_i + 1$.

14. Увеличиваем k на 1. Если $k \leq l$, переходим на шаг 6.

15. Если $|M| < |\underline{S}|$, то увеличиваем h на 1 и переходим на шаг 5.

16. Конец работы алгоритма.

Список литературы

1. Бурдюк В. Я., Турчина В. А. Алгоритмы параллельного упорядочения. — Днепропетровск: ДГУ, 1985.

2. Холл М. Комбинаторика. — М.: Мир, 1970.

Секция «Математическая теория интеллектуальных систем»

О ЗАМКНУТЫХ КЛАССАХ АВТОМАТНЫХ ФУНКЦИЙ ОТНОСИТЕЛЬНО СУПЕРПОЗИЦИИ

Д. Н. Бабин (Москва)

Рассматривается алгебра автоматов с операцией суперпозиции. Класс функций C имеет бесконечную высоту в надклассе D, если никакая конечная система функций из D не дополняет класс C до класса D. Исследована вложенная последовательность бесконечнопорожденных классов автоматов, имеющих бесконечную высоту в своем непосредственном надклассе. В частности, обозначим через G множество групповых автоматов, G_1 — замыкание множества одноместных групповых автоматов и булевых функций, R — множество групповых автоматов с разрешимыми группами, L — множество групповых автоматов с линейными переходами. Имеет место

Теорема. *Классы: L в R, R в G_1, G_1 в G имеют бесконечную высоту.*

Список литературы

1. Кудрявцев В. Б. Функциональные системы. — М.: Изд-во МГУ, 1982.

2. Бабин Д. Н. О полноте двухместных о.д.-функций относительно суперпозиции // Дискретная математика. — 1989. — Т. 1, вып. 4. — С. 86–91.

3. Бабин Д. Н. О суперпозициях в некоторых классах о.-д. функций // Логико-алгебраические конструкции. — Тверь, 1992. — С. 17–22.

ОБ АВТОМАТНОЙ МОДЕЛИ ПРЕСЛЕДОВАНИЯ

Н. Ю. Волков (Москва)

Обозначим множества натуральных и целых чисел как $\mathbb{N}$ и $\mathbb{Z}$, соответственно. Положим $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Множество клеток, на которые

плоскость разбивается целочисленной решеткой, обозначим $\mathbb{Z}^2$, сопоставляя каждой клетке координаты ее нижнего левого угла. Назовем r-окрестностью клетки (x_0, y_0) множество $D_{(x_0,y_0),r} = \{(x,y) \,|\, (\,|x - x_0| + |y - y_0|\,) \leq r\}$. Определим следующие лабиринты — подмножества $\mathbb{Z}^2$. $L_0 = \mathbb{Z}^2$, $L_1 = \{(x,y) \,|\, x \in \mathbb{Z}, y \in \mathbb{N}\}$, $L_2(l) = \{(x,y) \,|\, 0 < y \leq l, x, y \in \mathbb{Z}\}$, $L_3(l) = \{(x,y) \,|\, 0 < y \leq l, x, y \in \mathbb{N}\}$, $L_4 = \{(x,y) \,|\, x, y \in \mathbb{N}\}$, $L_5(l) = \{(x,y) \,|\, 0 < x \leq l, 0 < y \leq l, x, y \in \mathbb{N}\}$. Здесь $l \in \mathbb{N}$. Эти лабиринты назовем, соответственно, *плоскостью*, *полуплоскостью*, *l-полосой* и *l-полуполосой*, *квадрантом* и *l-квадратом*.

Рассмотрим автоматный аналог ситуации преследования хищниками своих жертв. В качестве пространства преследования будем рассматривать лабиринт L, являющийся одним из лабиринтов L_0, L_1, $L_2(l)$, $L_3(l)$, L_4, $L_5(l)$. Хищники и жертвы представляются в виде автоматов, которые, находясь в какой-либо клетке лабиринта, умеют обозревать некоторую ее окрестность, и, в зависимости от вида (конфигурации) этой окрестности и своего состояния, способны перемещаться в другую клетку лабиринта. Поведение каждого автомата определяется его начальным расположением в лабиринте, его "физическими параметрами" — обзором и скоростью, а также его внутренней логикой. Определим хищников и жертв более формально.

Под автоматом будем понимать инициальный конечный автомат вида $\mathcal{A} = (A, Q, B, \varphi, \psi, q_0)$, где A — входной, B — выходной, Q — внутренний алфавиты автомата $\mathcal{A}$, $\varphi : Q \times A \to Q$ и $\psi : Q \times A \to B$ — функции переходов и выходов $\mathcal{A}$, соответственно, $q_0 \in Q$ — его начальное состояние. Алфавит A определяет возможности $\mathcal{A}$ "видеть" происходящее вокруг, а алфавит B — его возможности перемещаться. Алфавит Q и функции φ и ψ задают внутреннюю логику автомата.

Выходным алфавитом автомата $\mathcal{A}$, перемещающегося в лабиринте L, является множество $B = D_{(0,0),V}$, где параметр $V \in \mathbb{N}$ называется *скоростью автомата* $\mathcal{A}$. Входной алфавит $\mathcal{A}$ зависит от параметра $R \in \mathbb{N}$ $(R \geq V)$, называемого *обзором автомата* $\mathcal{A}$ и способа взаимодействия $\mathcal{A}$ с другими автоматами. Возможны два случая такого взаимодействия: 1) $\mathcal{A}$ является элементом независимой системы (н.системы) автоматов; 2) $\mathcal{A}$ является элементом коллектива автоматов. Пусть автомат $\mathcal{A}$ со скоростью V и обзором R находится в клетке (x_0, y_0). Множество $D_{(x_0,y_0),R}$ называется *зоной обзора* $\mathcal{A}$.

Рассмотрим две системы автоматов $K = (\,W_1, \ldots, W_m\,)(R, V)$ и $S = (\,U_1, \ldots, U_n\,)(R', V')$ с обзорами R и R' и скоростями V и V', соответственно. Здесь S — н.система жертв, K — коллектив хищ-

ников. Фиксируем начальные расположения всех автоматов в лабиринте L.

Состояние зоны обзора U_i $(1 \le i \le n)$ в текущий такт времени определяется расположением U_i относительно границы лабиринта и расположением хищников в зоне обзора U_i. Такое состояние зоны обзора U_i будем называть U_i-конфигурацией (U_i-конф.). Состояние зоны обзора W_j $(1 \le j \le m)$ определяется расположением W_j относительно границы лабиринта, расположением жертв и хищников в зоне обзора W_j, а также состояниями хищников, попавших в зону обзора W_j. Такое состояние зоны обзора W_j будем называть W_j-конфигурацией (W_j-конф.). Таким образом, каждая жертва "не видит" других жертв, но "видит" границы лабиринта и хищников на расстоянии своего обзора, а хищники "видят" границы лабиринта, жертв и друг друга на расстоянии своего обзора.

Расположения и состояния жертв и хищников однозначно задают все U_i-конф. и W_j-конф. Множество U_i-конф. при всевозможных расположениях и состояниях жертв и хищников обозначим F', а множество всех W_j-конф. — F. Входным алфавитом каждой жертвы является множество $\{(\mathcal{F}_1, \mathcal{F}_2) \mid \mathcal{F}_1 \in (\{\emptyset\} \cup F'), \mathcal{F}_2 \in F'\}$. Входным алфавитом каждого хищника является множество $\{(\mathcal{F}_1, \mathcal{F}_2) \mid \mathcal{F}_1, \mathcal{F}_2 \in F\}$.

В четные такты каждая жертва U_i получает на вход пару, состоящую из текущей U_i-конф. и U_i-конф. в предыдущий такт (в нулевой такт вместо предыдущей U_i-конф. на вход поступает $\emptyset$). В соответствии со своими функциями переходов и выходов, U_i в четные такты перемещается в некоторую клетку и меняет свое состояние. В нечетные такты каждый хищник W_j получает на вход пару, состоящую из текущей и предыдущей W_j-конф. В соответствии со своими функциями переходов и выходов, W_j в нечетные такты перемещается и меняет свое состояние. Рассматриваются только такие автоматы, для которых перемещение на вектор, равный выходному символу, никогда не выводит за пределы лабиринта L. Жертва считается пойманной, если она оказалась в V-окрестности одного из хищников. Пойманная жертва исчезает из лабиринта. K "ловит" н.систему жертв, если в процессе преследования K ловит каждую жертву.

Расположение системы автоматов в лабиринте, при котором все они находятся в одной клетке, назовем *каноническим*. Вместо слов "начальное расположение" будем использовать сокращение "н.р.", а вместо "каноническое расположение" — "к.р.". Зафиксируем R, $V \in \mathbb{N}$, такие что $2 \le V \le R$. Получены следующие результаты.

Теорема 1. *Существуют коллективы хищников* $K_0(R,V)$, $K_1(R,V)$, $K_2(R,V)$, $K_3(R,V)$ *и* $K_4(R,V)$, *такие что*:

1. *Для каждого* $i = 0, 1$, *коллектив* K_i, *стартуя из любого к.р. в* L_i, *ловит любую конечную н.систему жертв* $S(R, V-1)$ *при любом их н.р. в* L_i;

2. *Для каждого* $i = 2, 3$, *коллектив* K_i, *при любом* l, *стартуя из любого к.р. в* $L_i(l)$, *ловит любую конечную н.систему жертв* $S(R, V-1)$ *при любом их н.р. в* $L_i(l)$;

3. *При* $V > 7 \cdot V'$, *коллектив* K_4, *стартуя из любого к.р. в* L_4, *ловит любую конечную н.систему жертв* $S(R, V')$ *при любом их н.р. в* L_4.

Теорема 2. *Верны следующие утверждения*:

1. *Для любой конечной н.системы жертв* $S(R, V-1)$, *существует коллектив хищников* $K_5(R, V)$, *который, при любом* l, *стартуя из любого к.р. в* $L_5(l)$, *ловит* $S(R, V-1)$ *при любом н.р. жертв в* $L_5(l)$;

2. *Для любого конечного коллектива хищников* $K(R, V)$ *существуют н.система жертв* $S(R, V-1)$ *и натуральное число* l, *такие что для любого н.р. хищников в* $L_5(l)$, *существует н.р. жертв в* $L_5(l)$, *при котором все они убегают от хищников.*

Автор работы выражает признательность В. Б. Кудрявцеву за научное руководство.

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — Наука, 1985.

2. Килибарда Г., Кудрявцев В. Б., Ушчумлич Ш. Независимые системы автоматов в лабиринтах // Дискретная математика. — 2003. — Т. 15, вып. 2.

3. Килибарда Г., Кудрявцев В. Б., Ушчумлич Ш. Коллективы автоматов в лабиринтах // Дискретная математика. — 2003. — Т. 15 вып. 3.

4. Грунская В. И. О динамическом взаимодействии автоматов // Математическая кибернетика и ее приложения к биологии. — М.: Изд-во МГУ, 1987. — С. 8–18.

5. Волков Н. Ю. Об автоматной модели преследования // Дискретная математика. — 2007. — Т. 19, вып. 2.

СЕМАНТИЧЕСКИЙ ВЕБ И ТЕОРЕТИКО-КАТЕГОРНЫЕ МОДЕЛИ

Н. М. Глазунов (Киев)

Целью семантического веба является обеспечение необходимых стандартов и инфраструктуры для преобразования интернета в более автоматизированную среду, в которой агенты имели бы возможность осуществлять поиск запрашиваемой информации автоматически [1, 2]. Важным элементом семантического веба являются онтологии, т. е. контролируемый словарь концепций, каждая из которых явно определена и обладает машинно-обрабатываемой (формальной) семантикой. Семантический веб развивается послойно. В настоящее время его структура может быть представлена схемой:

Интернет $\leftrightarrow$ RDF $\leftrightarrow$ OWL $\leftrightarrow$ логика и доказательства на вершине онтологий.

Здесь RDF означает рамки описания ресурсов, OWL означает язык сетевых онтологий.

В работе рассматриваются теоретико-категорные модели элементов семантического веба (интернета), которые относятся к выводу знаний. Системы вывода знаний называют иногда дедуктивными или переписывающими системами. Мы рассматриваем системы вывода знаний, основанные на категории путей графа, называем их системами вывода и вводим категорий таких систем. Основным результатом данного сообщения является

Теорема. *Если система вывода dP, соответствующая данной системе продукций P, является нетеровой и удовлетворяет условию Черча — Россера, то она является разрешимой.*

Введем необходимые определения, сформулируем вспомогательные результаты и набросок доказательства. Пусть V, E, W есть множества, т. е. объекты категории **Ens** множеств и их отображений. Под графом G понимает объект (V, E, s, t), где V есть множество вершин, E есть множество дуг, s, t функции

$$E \quad \stackrel{s}{\longrightarrow} \quad V, \quad E \quad \stackrel{t}{\longrightarrow} \quad V,$$

сопоставляющие дуге её начало и конец. Морфизмом графов $f : G_1 \to G_2$ называют пару отображений $f_v : V(G_1) \to V(G_2), f_e : E(G_1) \to E(G_2)$ таких, что $s(f_e(e)) = f_v(s(e)),\ t(f_e(e)) = f_v(t(e))$. Категорию графов обозначаем **Graphs**. Пусть **Cat** есть категория малых категорий, **C** — малая категория.

Лемма 1. *Существует стирающий функтор* $\underline{F}$: **Cat** $\to$ **Graphs**, *который ставит в соответствие малой категории* **C**

граф G, где V есть множество объектов, E есть множество морфизмов (стрелок) категории **C**, *начало и конец дуги есть, соответственно, область определения и область значения соответствующего морфизма (стрелки).*

Лемма 2. *По графу G можно построить категорию путей* **PathG**, *что определяет функтор $\underline{P}$: **Graphs** $\to$ **Cat**. Объектами* **PathG** *являются вершины графа G, множество морфизмов $PathE$ есть множество путей между вершинами графов. Каждой вершине сопоставляется единичный морфизм. Композиция морфизмов определяется умножением путей.*

Категории **PathG** соответствует новый граф $PathG = (V, PathE, s, t)$.

Системой продукций P называем 2-граф $(V, PathE, \mathfrak{P}, s, t, s_1, t_1)$, где граф (1-граф) $(V, PathE, s, t)$ определен выше,

$$PathE \xleftarrow{s_1} \mathfrak{P}, \quad PathE \xleftarrow{t_1} \mathfrak{P},$$

и для $x, y \in V, p, p_1 \in PathE, \alpha \in \mathfrak{P}, p = s_1(\alpha), p_1 = t_1(\alpha)$, функции s_1, t_1 удовлетворяют условиям $x = t(p) = t(p_1) = ts_1(\alpha) = tt_1(\alpha)$, $y = s(p) = s(p_1) = st_1(\alpha) = ss_1(\alpha)$.

Аналогично морфизму графов можно определить морфизм систем продукций и категорию систем продукций. Далее подобным образом определяются система элементарных выводов, система выводов, а также нормальные формы. Нетеровость дает, что любой вывод после конечного числа шагов приводит к нормально форме. Свойство Черча — Россера влечет, что две нормальные формы сводимы одна к другой, если у них есть общий наследник. Так как нормальные формы неприводимы, существование общего наследника возможно тогда и только тогда, когда нормальные формы совпадают.

Список литературы

1. Davies J., Fensel D., van Harmelen F. Towards the semantic Web: ontology-driven knowledge management. — N.-Y.: John Wiley & Sons, 2003.

2. Meditskos G., Bassiliades N. Towards an object-oriented reasoning system for OWL // Int. Workshop on OWL Experiences and Directions. (11–12 Nov. 2005). — Galway, Ireland, 2005. — P. 79–90.

3. Kontsevich M., Soibelman Y. Notes on A_∞–algebras, A_∞–categories and non-commutative geometry. I // `arXiv:math.RA/0606241 v1 11 Jun 2006.`

4. Goguen J. A. Category theory applications in computation and control // LNCS. — 1975. — V. 25. — P. 151–169.

5. Santocanale L. A Calculus of circular proofs and its categorical semantics // BRICS Report Series. — RS-01-15. — 2001.

6. Michael B., Charles W. Toposes, triples and theories // Reprints in Theory and Applications of Categories. — № 1. — P. 1–289.

ОБ ОСОБЕННОСТЯХ ДИНАМИКИ И ОТНОШЕНИЯ ИСТОРИИ В ДИНАМИЧЕСКОЙ ИНФОРМАЦИОННОЙ МОДЕЛИ DIM

А. А. Груздов, В. С. Рублев (Ярославль)

Динамическая информационная модель DIM [1] позволяет описывать любые дискретные объекты и детерминированные процессы, происходящие с этими объектами. Изменение значений свойств объектов составляет поведение объектов. Эти изменения происходят в результате взаимного влияния объектов друг на друга, которое называется взаимодействием объектов. Взаимодействия объектов могут приводить к более общей динамике объектов, при которой может заканчиваться время жизни одних объектов и начинаться время жизни других объектов.

Задание классов и свойств объектов с конструкцией взаимодействия делает систему полной относительно динамики изменения информации в системе, если введенные в систему объекты не перестают существовать или если после их удаления информация об этих объектах никогда не потребуется. Но, если история объектов после прекращения их существования все же необходима в системе, то описанных конструкций недостаточно.

Между объектами можно устанавливать несколько видов отношений. За динамику отвечают два вида отношений: отношение взаимодействия и отношение истории.

Для описания динамики изменения объектов вводятся следующие конструкции: момент рождения, момент смерти, отношение истории объектов, объекты-предшественники и объекты-последователи. Для классов вводятся аналогичные конструкции. Если изменение класса связано только с введением дополнительных параметров, то изменению подлежат только те объекты, для которых определяются непустые значения дополнительных параметров. Иначе все объекты класса претерпевают изменения и могут измениться также связи между классами и объектами.

Алгоритм основной модификации классов, параметров и связей DIM можно описать следующими шагами:

1) данные описания класса копируются в новый класс с новым идентификатором класса (при этом класс со старым идентификатором становится предшественником, а класс с новым идентификатором становится последователем в отношении истории классов);

2) клонируем объект (с добавлением в отношение истории);

3) добавляются параметры нового класса как дополнительные параметры;

4) для всех объектов нового класса определяются значения этих параметров;

5) группа каждого добавленного параметра нового класса изменяется в соответствии с необходимостью;

6) удаляются ненужные параметры нового класса, и проверяется ограничения целостности для объектов класса;

7) добавляются связи нового класса с другими классами и для объектов этих других классов определяются при необходимости связи с объектами нового класса (такие объекты получают новый идентификатор и связь с объектами старого идентификатора при помощи отношения истории объектов);

8) удаляются при необходимости ненужные связи нового класса с другими классами и одновременно удаляются связи между объектами этих классов; проверяются ограничения целостности для всех объектов, для которых старый класс содержал родительские объекты.

С отношением истории классов мы связываем также отношение истории взаимодействий. При изменении класса с новым идентификатором класса может быть связано старое взаимодействие, если произведенные изменения в классе не касаются процедуры выполнения взаимодействия. В противном случае новое взаимодействие связывается с новым классом, а со старым взаимодействием оно связывается отношением истории. С одним и тем же именем взаимодействия может быть связано несколько процедур взаимодействия, разграниченных отношением истории по времени, и, если взаимодействие выполняется для длительного промежутка времени жизни различных объектов, сменяющих друг друга в отношении истории, то процедура взаимодействия для обработки может быть каждый раз правильно выбрана в соответствии со временем жизни объектов.

Используя объектно-ориентированную реализацию DIM [2], вводим в базовый класс функционал, позволяющий манипулировать "жизненным циклом" объекта DIM. По завершении этого цикла объект попадает в историю. Это актуально для классов и объектов DIM. Значение динамического параметра DIM может не иметь нижней грани временного интервала, такой пример характеризует случай,

в котором время наступления значения не важно. Таким образом динамика здесь идёт несколько отдельно — мы имеем последовательность непересекающихся интервалов времени жизни нашего динамического параметра. Поэтому получить состояние в выбранный промежуток времени не составляет труда.

Из-за такой реализации манипулировать данными истории можно через расширение языка ODQL [3]. Для этого в синтаксис ODQL вводится ключевое слово "history". Если оно является префиксом временного свойства, то это означает выбор значения, предшествующего текущему, а если постфиксом — следующему за текущим. Для выбора объектов, существовавших в определеыннй период времени, во фразе for можно использовать врожденные свойства объектов "Дата рождения" и "Дата смерти".

Список литературы

1. Рублев В. С., Юсупов А. Р. Концепции объектной динамической информационной модели DIM // Математика в Ярославском университете. Сборник обзорных статей к 30-летию математического факультета. — Ярославль: ЯрГУ, 2006. — С. 355–394.

2. Писаренко Д. С., Груздов А. А. Архитектура объектно-ориентированной реализации динамической информационной модели DIM // Современные проблемы математики и информатики. Вып. 7. — Ярославль: ЯрГУ, 2005. — С. 204–215.

3. Чехранов Д. В., Юсупов А. Р. Язык запросов DQL и проблема реализации компилятора из языка DQL в язык OQL // Современные проблемы математики и информатики: сборник научных трудов молодых ученых, аспирантов и студентов. Вып. 6. — Ярославль: ЯрГУ, 2004. — С. 148–156.

МИНИМАЛЬНЫЕ ИДЕНТИФИКАТОРЫ ВЕРШИН ПОМЕЧЕННЫХ ГРАФОВ

И. С. Грунский, С. В. Сапунов (Донецк)

Управляющая система, функционирующая в среде, — это центральное понятие кибернетики [1]. В данной работе в качестве модели среды рассматриваются ориентированные и неориентированные графы с помеченными вершинами. В работе рассматриваются задача различения вершин графа с помеченными вершинами с помощью блуждающего по графу мобильного агента. Агент перемещается по дугам графа от вершины к вершине. При этом, находясь в вершине графа, он воспринимает ее метку и метки смежных ей вершин.

Траектории блуждания агента порождают слова в алфавите меток. Задача заключается в том, чтобы найти множества слов, т.н. идентификаторы, отделяющие одну вершину графа от всех других его вершин. Найдены условия существования и оценки высоты минимальных идентификаторов.

Простым конечным графом с помеченными вершинами (помеченным графом) назовем четверку $\mathrm{G} = (G, E(G), M, \mu_{\mathrm{G}})$, где G — конечное множество вершин, $E(G) \subseteq G \times G$ — конечное множество ребер, M — конечное множество меток вершин, $\mu_{\mathrm{G}} : G \to M$ — сюръективная функция разметки. Множеством преемников Γ_g вершины g называется множество всех вершин, являющихся концами исходящих из g дуг. Граф G назовем D-графом, если для любой вершины $g \in G$ и любых вершин $s, t \in \Gamma_{(g)}$ из $s \neq t$ следует, что $\mu_{\mathrm{G}}(s) \neq \mu_{\mathrm{G}}(t)$. Пусть G является неорграфом. Окрестностью O_g вершины $g \in G$ называется сама вершина g и множество всех смежных ей вершин. Неорграф G назовем SD-графом, если для любой вершины $g \in G$ и любых вершин $s, t \in O_g$ из $s \neq t$ следует, что $\mu_{\mathrm{G}}(s) \neq \mu_{\mathrm{G}}(t)$. Последовательность меток вершин $w = \mu_{\mathrm{G}}(g_1) \dots \mu_{\mathrm{G}}(g_k)$, соответствующую некоторому пути $g_1 \dots g_k$ в графе G, назовем словом, порожденным вершиной g_1. Инверсией слова $w = x_1 \dots x_k$ назовем слово $w^{rev} = x_k \dots x_1$. Для слов $u, w \in M^+$ введем их композицию $u \circ w$ по правилу: пусть $x, y \in M$, тогда $wx \circ xu = wxu$ и $wx \circ yu$ не определено, если $x \neq y$. Языком L_g вершины $g \in G$ назовем множество всех слов, порожденных этой вершиной. Две вершины $g, h \in G$ назовем неотличимыми, если $L_g = L_h$. В [2] было показано, что длина кратчайшего слова, различающего две вершины произвольного помеченного графа, равна $O\left(2^{2|G|}\right)$. Там же показано, что длина кратчайшего слова, различающего две вершины D-орграфа и SD-графа, не превосходит $|G| - |M| + 1$ и эта оценка достижима. Фактор-граф графа G по отношению неотличимости вершин назовем приведенным графом.

Идентификатором вершины $g \in G$ назовем конечное множество слов $W_g \subseteq M^*$ такое, что для любой вершины $h \in G$ равенство $W_g \cap L_g = W_g \cap L_h$ выполняется тогда и только тогда, когда $g = h$. Мощность идентификатора назовем его кратностью, а наибольшую из длин входящих в него слов — его высотой. Следующее утверждение устанавливает условия существования идентификаторов вершин помеченных графов.

Теорема 1. *Равносильны следующие утверждения:* (1) *существует идентификатор вершины* $g \in G$; (2) *существует идентификатор вершины* $g \in G$ *высоты не больше* $2^{2|G|}$ *и кратности не больше* $|G| - 1$; (3) $\varepsilon(g) = \{g\}$.

Из теоремы 1 вытекает следующее утверждение.

Теорема 2. (1) *Для любой вершины приведенного помеченного графа существует кратный идентификатор высоты не больше* $2^{2|G|}$ *и кратности не больше* $|G|-1$. (2) *Для любой вершины приведенного D-графа существует кратный идентификатор высоты не больше* $|G|-|M|+1$ *и кратности не больше* $|G|-1$.

Обозначим через $\mathbf{I}_g$ класс всех идентификаторов вершины $g \in G$. Очевидно, что для любой неизолированной вершины этот класс бесконечен. Пусть $L_1 \prec L_2$ означает, что каждое слово из L_1 является начальным отрезком некоторого слова из L_2. Это отношение является предпорядком и порождает эквивалентность $\equiv$. Через $\mathbf{K}(W_g)$ обозначим класс всех идентификаторов из $\mathbf{I}_g$ эквивалентных (по $\equiv$) идентификатору W_g. Идентификатор W_g назовем минимальным в $\mathbf{I}_g$, если для всех $W'_g \in \mathbf{I}_g$ из $W'_g \prec W_g$ следует $W_g \subseteq W'_g$.

Теорема 3. *Равносильны утверждения*: (1) W_g *минимален в* $(\mathbf{I}_g, \prec)$; (2) W_g *минимален в* $(\mathbf{K}(W_g), \subseteq)$ *и* W_g *минимален в* $\langle \mathbf{I}_g/_{\equiv}, \prec \rangle$; (3) *множество* W'_g, *полученное из* W_g *удалением хоть одного слова или заменой хоть одного слова его собственным начальным отрезком, идентификатором вершины* g *не является.*

Следующее утверждение оценивает высоту минимальных идентификаторов.

Теорема 4. *Для любых натуральных* $n \geq 3$ *и* $2 \leq m \leq n-1$ *существует приведенный граф с* n *вершинами и* m *метками и его вершина* g, *для которой найдется минимальный идентификатор как угодно большой высоты.*

Теорема 4 показывает, что множество минимальных идентификаторов в общем случае бесконечно. Аналогичная теорема имеет место для начальных идентификаторов состояний конечных детерминированных всюду определенных автоматов [3].

На множестве конечных слов W определим две операции: (1) если слово $w_1 \circ w_2 \circ w_2^{rev} \circ w_3 \in W$, то заменим его словами $w_1 \circ w_2$ и $w_1 \circ w_3$; (2) если слово $w \prec u$, где $w, u \in W$, то удалим w из W. Операцию, состоящую в многократном и исчерпывающем применении к множеству W операций 1 и 2 назовем операцией редукции, а ее результат обозначим через $\mathrm{Rd}(W)$ и назовем редуцированным множеством. Справедливо следующее утверждение.

Теорема 5. *Если множество слов* W *является идентификатором вершины* g *SD-графа* $\mathcal{G}$, *то редуцированное множество слов* $\mathrm{Rd}(W)$ *также является идентификатором вершины* g.

Теорема 5 показывает, что всякому идентификатору можно поставить в соответствие редуцированный идентификатор. Следую-

щее утверждение оценивает высоту редуцированных минимальных идентификаторов вершин SD-графов.

Теорема 6. *Пусть m и n некоторые натуральные числа такие, что $m \geq 4$ и $n-1$ кратно $m-1$. Тогда существует приведенный максимальный SD-граф с n вершинами и m метками и его вершина g, для которой найдется редуцированный минимальный идентификатор сколь угодно большой высоты.*

Теорема 6 показывает, что множество минимальных редуцированных идентификаторов в общем случае также бесконечно.

Список литературы

1. Гасанов Э. Э., Кудрявцев В. Б. Теория хранения и поиска информации. — М.: Физматлит, 2002.

2. Сапунов С. В. Контроль детерминированных графов // Труды ИПММ НАН Украины. — 2003. — Т. 8. — С. 106–110.

3. Грунский И. С. Анализ поведения конечных автоматов. — Луганск: Изд-во Луганск. гос. пед. ун-та, 2003.

О ПРОБЛЕМЕ ПОЛНОТЫ В КЛАССЕ АВТОМАТОВ БЕЗ ОБРАТНОЙ СВЯЗИ

Д. Н. Жук, Ю. Н. Присмотров (Москва)

В работе исследуется задача о полноте относительно операции суперпозиции для систем автоматов без обратной связи вида $P_2 \cup \nu$. Построен алгоритм проверки на полноту таких систем автоматов. Для каждого конечного ν он заключается в проверке непринадлежности ν конечному числу замкнутых классов.

Пусть P_2 — множество всех булевых функций. Рассмотрим конечные автоматы, имеющие ровно 1 выход и получающиеся при помощи операции суперпозиции из элементов, являющихся функциями из P_2 или единичной задержкой с начальным состоянием 0 или 1. Множество всех таких автоматов обозначим через $\mathcal{P}_a$. Автоматы такого вида не содержат циклов, т. е. операция обратной связи в них не реализуется.

Пусть $E_2 = \{0, 1\}$, ${E_2}^l$ — множество слов длины l, E — множество всех сверхслов в алфавите E_2. Множество E^n состоит из элементов $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, где $\alpha_i \in E$. Также элемент множества E^n иногда будем представлять как последовательность $(\vec{a}_1, \vec{a}_2, \ldots)$, где $\vec{a}_i \in {E_2}^n$. Будем говорить, что слово $\gamma \in {E_2}^d$ имеет период e, если

e делит d и $\gamma(i+1) = \gamma(i \pmod e + 1)$ для $i = 0, 1, \ldots, d-1$. Для конечного слова α сверхслово $\alpha^\infty = \alpha\alpha\alpha\ldots$.

Автомат без обратной связи можно интерпретировать как функцию $T : E^n \longrightarrow E$, которая переводит входную последовательность $(\vec{x}(1), \vec{x}(2), \ldots) \in E^n$ в последовательность $(y(1), y(2), \ldots) \in E$ следующим образом:

$$y(i) = f_i(\vec{x}(1), \vec{x}(2), \ldots, \vec{x}(i)) \text{ для } i = 1, 2, \ldots, h,$$
$$y(i) = f_h(\vec{x}(i-h+1), \vec{x}(i-h+2), \ldots, \vec{x}(i)) \text{ для } i = h+1, h+2, \ldots,$$

где $f_j : {(E_2{}^j)}^n \longrightarrow E_2$ для $j = 1, 2, \ldots, h$.

Тогда T будем называть автоматом без обратной связи высоты h. При этом предполагается, что значение h минимально. Функции f_j для $j = 1, \ldots, h-1$ определяют выход автомата в моменты времени от 1 до $h-1$. А функция f_h определяет выход автомата, начиная с момента времени h. Множество всех автоматов без обратной связи обозначим $\mathcal{P}_a$, а множество всех автоматов без обратной связи высоты не более h обозначим $\mathcal{P}_a{}^h$. Для $p > h$ определим

$$f_p(\vec{x}(1), \vec{x}(2), \ldots, \vec{x}(p)) = f_h(\vec{x}(p-h+1), \vec{x}(p-h+2), \ldots, \vec{x}(p)).$$

Таким образом, для любого s функция f_s определяет выход автомата в момент времени s.

Пусть $M \subset \mathcal{P}_a$, обозначим через $[M]$ множество всех автоматов без обратной связи, получающихся из M с помощью операции суперпозиции. Множество M называется полным, если $[M] = \mathcal{P}_a$.

Поведение автомата в моменты времени $t \geq h$ зависит только от функции f_h и не зависит от функций $f_1, f_2, \ldots, f_{h-1}$. Поэтому для изучения свойств автомата при $t \geq h$ введем искусственное отображение. Для произвольного автомата T высоты h с n входами определим отображение $G_T : E^n \longrightarrow E$. Для $\vec{a}(1), \vec{a}(2), \vec{a}(3), \ldots \in {E_2}^n$

$$G_T(\vec{a}(1), \vec{a}(2), \vec{a}(3), \ldots) = \beta, \text{ где}$$
$$\beta(i) = f_h(\vec{a}(i+h-1), \vec{a}(i+h-2), \ldots, \vec{a}(i+1), \vec{a}(i)) \text{ для любого } i.$$

В этом случае автомат преобразует сверхслова не с начала, а как бы с конца.

Каждую булевскую функцию можно считать автоматом высоты 1. Пусть $P_2 \subset M \subset \mathcal{P}_a$, $M \setminus P_2$ — конечное множество. В работе рассматривается проблема полноты для систем M указанного вида. Теперь опишем 5 семейств классов автоматов в $\mathcal{P}_a$. Обозначим через $h(T)$ высоту автомата T, а через $n(T)$ число входов автомата T.

Семейство $\mathfrak{A}$. Это семейство состоит из классов M_{pq}, где $1 \le p < q$. M_{pq} — множество автоматов T таких, что из равенства $\vec{x}(p) = \vec{x}(q)$ следует равенство $y(p) = y(q)$.

Семейство $\mathfrak{B}$. Это семейство состоит из одного класса $M_{1\infty}$. $M_{1\infty}$ — множество автоматов T таких, что для любого $\vec{a} \in {E_2}^{n(T)}$

$$f_{h(T)}(\vec{a}, \vec{a}, \ldots, \vec{a}) = f_1(\vec{a}).$$

Семейство $\mathfrak{C}$. Это семейство состоит из классов $S_p, p \ge 2$. S_p — множество автоматов T таких, что для любых $\vec{a}_1, \ldots, \vec{a}_p, \vec{b} \in {E_2}^{n(T)}$

$$f_p(\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_{p-2}, \vec{a}_{p-1}, \vec{a}_p) = f_p(\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_{p-2}, \vec{b}, \vec{a}_p).$$

Семейство $\mathfrak{D}$. Это семейство состоит из 4 классов L_1, L_2, L_3, L_4 : L_1 — множество автоматов T таких, что для любых $\vec{a}, \vec{b} \in {E_2}^{n(T)}$

$$f_{h(T)}(\vec{a}, \vec{a}, \ldots, \vec{a}, \vec{a}, \vec{a}) = f_{h(T)}(\vec{a}, \vec{a}, \ldots, \vec{a}, \vec{b}, \vec{a}).$$

L_2 — множество автоматов T таких, что для любых $\vec{a}, \vec{b} \in {E_2}^{n(T)}$

$$f_{h(T)}(\vec{a}, \vec{a}, \ldots, \vec{a}, \vec{a}, \vec{b}) = f_{h(T)}(\vec{a}, \vec{a}, \ldots, \vec{a}, \vec{b}, \vec{b}).$$

L_3 — множество автоматов T таких, что для любых $\vec{a}, \vec{b} \in {E_2}^{n(T)}$

$$f_{h(T)}(\ldots, \vec{b}, \vec{a}, \vec{b}, \vec{a}, \vec{b}) = f_{h(T)}(\ldots, \vec{a}, \vec{b}, \vec{a}, \vec{b}, \vec{b}).$$

L_4 — множество автоматов T таких, что для любых $\vec{a}, \vec{b} \in {E_2}^{n(T)}$

$$f_{h(T)}(\vec{a}, \ldots, \vec{a}, \vec{a}, \vec{b}) = f_{h(T)}(\vec{b}, \ldots, \vec{b}, \vec{b}, \vec{b}).$$

Семейство $\mathfrak{E}$. Пусть $d \ge 3$, $C \subset {E_2}^d$, и для любых $\gamma, \delta \in C$, $\overline{\gamma}$, $\gamma \vee \delta$, $\gamma \wedge \delta \in C$ (где все операции выполняются поэлементно). Пусть также для какого-то e в C есть слово с наименьшим периодом e, но C содержит не все слова периода e; C содержит слова 0^d и 1^d. Тогда пара (d, C) определяет класс R_d^C : автомат T с n входами принадлежит R_d^C тогда и только тогда, когда для любых $\alpha_1, \alpha_2, \ldots, \alpha_n \in C$ $G_T({\alpha_1}^\infty, {\alpha_2}^\infty, \ldots, {\alpha_n}^\infty) = \delta^\infty$, где $\delta \in C$. Семейство $\mathfrak{E}$ состоит из всех таких классов R_d^C.

Теорема 1. *Верны следующие утверждения*:

1) *Для любых натуральных p и q таких, что $p < q$, M_{pq} — предполный класс в $\mathcal{P}_a$;*

2) *$M_{1\infty}$ — предполный класс в $\mathcal{P}_a$;*

3) *для любого натурального $p \geq 2$ S_p — предполный класс в $\mathcal{P}_a$;*

4) *L_1, L_2, L_3, L_4 — предполные классы в $\mathcal{P}_a$;*

5) *R_d^C — замкнутый класс в $\mathcal{P}_a$.*

Теорема 2. *Пусть B — система автоматов из ${\mathcal{P}_a}^h$, $P_2 \subset B$. Система B полна тогда и только тогда, когда B не является подмножеством M_{pq} для $1 \leq p < q \leq 2h$, $M_{1\infty}$, S_p для $2 \leq p \leq h$, L_1, L_2, L_3, L_4, R_d^C для $d < (2h^2)^h$.*

Авторы работы выражают признательность В. Б. Кудрявцеву за научное руководство.

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

2. Бабин Д. Н. Разрешимый случай задачи о полноте автоматных функций // Дискретная математика. — 1992. — Т. 4.

3. Кудрявцев В. Б. Функциональные системы. — М.: Наука, 1990.

ЭКСТРЕМАЛЬНЫЕ ЗАДАЧИ С КРИТЕРИЕМ СИММЕТРИИ НА КОНЕЧНЫХ МНОЖЕСТВАХ

И. В. Козин (Запорожье)

Рассматривается конечное множество X. Преобразованием множества X называется любое взаимнооднозначное отображение $F : X \to X$ этого множества на себя. Группа G преобразований множества X изоморфна группе подстановок S_n, где n — число элементов множества X. Всякую подгруппу A группы G будем называть группой симметрий множества X. Для любого элемента $x \in X$ орбитой этого элемента при действии группы симметрии A называется множество $O_A(x) = \{y : y = g(x), g \in A\}$. Орбитой подмножества $Y \subseteq X$ будем называть объединение орбит всех его элементов и обозначать $O_A(Y)$. Очевидно, орбиты любых двух элементов множества X либо не пересекаются, либо совпадают. Также является очевидным, что для любого подмножества $Y \subseteq X$ и для любой группы симметрии $A \subseteq G$ имеет место включение $Y \subseteq O_A(Y)$.

Подмножество $Y \subseteq X$ называется инвариантным (или вполне симметричным) относительно действия группы $A \subseteq G$, если $\forall g \in A,\ \ g(Y) = Y$. Отметим очевидное определяющее свойство инвариантных множеств. Множество $Y \subseteq X$ инвариантно относительно действия группы A в том и только в том случае, когда оно совпадает со своей орбитой, то есть $Y = O_A(Y)$

Определим меру симметрии $\mu_A(Y)$ непустого подмножества $Y \subseteq X$ как отношение числа элементов этого множества к числу элементов его орбиты, то есть $\mu_A(Y) = |Y|/|O_A(Y)|$. Для пустого подмножества будем полагать по определению $\mu_A(\oslash) = 1$. Очевидно, что для любого подмножества $Y \subseteq X$ справедливо неравенство $|Y|/|X| \leq \mu_A(Y) \leq 1$. Инвариантные относительно действия группы симметрии A множества — это множества с максимальной мерой симметрии, то есть множества, для которых $\mu_A(Y) = 1$.

Вполне ассиметричным по отношению к группе симметрии A будем называть такое подмножество $Y \subseteq X$, каждый элемент $y \in Y$ которого обладает следующим свойством: $Y \cap O_A(y) = \{y\}$. То есть для любого элемента $y \in Y$ и любого преобразования $g \in A$, отличного от тождественного, $g(y) \notin Y$. Будем называть ядром симметрии или S_A-ядром множества Y любое его максимальное вполне ассиметричное подмножество.

Теорема. *Пусть Y — произвольное подмножество множества X, A — подгруппа группы G. Тогда мощности всех S_A-ядер множества Y одинаковы.*

Доказательство. Так как орбиты любых двух элементов множества X или не пересекаются или совпадают, то множество X оказывается разбитым на классы эквивалентности. Два элемента эквивалентны (принадлежат одному классу) в том и только в том случае, когда один из них может быть получен из другого с помощью преобразования из группы A. Ядро симметрии содержит ровно по одному элементу из каждого класса эквивалентности. Следовательно, его мощность равна количеству классов эквивалентности.

Теперь рассмотрим экстремальные задачи о симметричных подмножествах.

Простейшая оптимизационная задача с критерием симметрии формулируется следующим образом: для заданного множества X и его группы симметрии A найти множество заданной мощности m с максимальной мерой симметрии.

Как уже отмечалось ранее, множество X разбивается на классы, каждый из которых представляет собой орбиту некоторого элемента из X. Перенумеруем эти классы и далее будем полагать $X = O_1 \cup O_2 \cup \ldots \cup O_s$. Для каждого класса определим величину

$k_i = |O_i|$ — мощность этого класса. С каждым множеством $Y \subseteq X$ свяжем бинарный вектор

$$y = (y_1, y_2, \ldots, y_s), \text{ где } y_i = \begin{cases} 1, & \text{если } O_i \subseteq O(Y) \\ 0, & \text{если } O_i \nsubseteq O(Y) \end{cases}$$

При заданном m эадача отыскания множества Y мощности m с максимальной мерой симметрии сводится к решению следующей оптимизационной задачи:

$k_1 \cdot y_1 + k_2 \cdot y_2 + \ldots + k_s \cdot y_s \to min$
$k_1 \cdot y_1 + k_2 \cdot y_2 + \ldots + k_s \cdot y_s \geq m,$
$y_i \in 0, 1, i = 1, 2, \ldots, s$

Эта задача является классической задачей о ранце. Как следствие получаем, что задача о максимальном симметричном подмножестве NP-полна.

Быстрый эвристический алгоритм [1] решения этой задачи выглядит следующим образом. Упорядочиваем и перенумеровываем числа $k_i, i = 1, 2, \ldots, s$ по возрастанию и выбираем минимальный номер t, для которого $k_1 + k_2 + \ldots + k_t \geq m$. В качестве решения берем множество $Y = O_1 \cup O_2 \cup \ldots \cup O_{t-1} \cup B$, где множество $B \subseteq O_t$ и содержит любые $m - (k_1 + k_2 + \ldots + k_{t-1})$ элементов множества O_t.

Следующая задача отыскания подмножества заданной мощности m с минимальной мерой симметрии решается достаточно просто. Если $m \geq s$, то выбираем по одному элементу из каждого из s классов эквивалентности, а остальные $m - s$ выбираются произвольно. Мера симметрии полученного множества из m элементов будет равна m/n. Если $m < s$, то упорядочим классы $O_1, O_2, \ldots, O_s$ по убыванию их мощности. Выберем по одному элементу из первых m классов. Это и будет требуемое решение с минимальной мерой симметрии.

Более сложные задачи появляются, когда на множестве X задана структура, определенная некоторыми отношениями. Задача состоит в отыскании максимально симметричных (или ассиметричных) подмножеств, на которых сохранена заданная структура [2].

Список литературы

1. Сигал И. Х., Иванова А. П. Введение в прикладное дискретное программирование. Модели и вычислительные алгоритмы. — М.: Физматлит, 2002.

2. Козин И. В. Фрагментарный алгоритм для задачи симметричного размещения // Радиоэлектроника, информатика, управление. — Запорожье, 2005. — № 1. — С. 76–83.

КОНТРОЛЬНЫЕ ЭКСПЕРИМЕНТЫ В ЛОКАЛЬНО ОПРЕДЕЛЕННЫХ КЛАССАХ

В. А. Козловский, О. М. Копытова (Донецк)

Контрольные эксперименты с автоматами [1] обычно изучаются для достаточно обширных классов автоматов. На уровне абстрактного автомата огромное большинство таких классов можно рассматривать как результат последовательности специальных преобразований множества дуг автомата-эталона типа переброски дуг — замены конца одной из дуг графа переходов автомата другим состоянием, или замены в отметке дуги одного выходного символа другим. В [2] рассматривались так называемые m-плотные классы, охватывающие широкий круг классов автоматов, возникающих при достаточно произвольных перебросках дуг или изменении их отметок, возможно, даже с увеличением числа состояний. Для таких классов необходимым условием, при котором эксперимент становится контрольным, является обход по всем дугам графа переходов автомата-эталона. Однако это условие обычно не является достаточным, что является одной из причин высокой сложности задачи распознавания свойства "быть контрольным экспериментом" относительно этих классов (в ряде случаев это NP-полная проблема [3]). Исключением является класс локально порожденных из эталона автоматов [4], для которого, при наложении ограничений на поведение эталона, контрольный эксперимент "почти" совпадает с обходом по всем дугам автомата-эталона. Это сразу же определяет и полиномиальность указанной задачи распознавания в этом случае. Поэтому интерес представляет поиск классов, достаточно богатых по разнообразию составляющих их автоматов, для которых "почти" обходы определяют контрольные эксперименты. В данной работе вводятся такие классы автоматов, и дается характеризация контрольных экспериментов эталона относительно этих классов.

Под автоматом понимаем автомат Мили $A = (S, X, Y, \delta, \lambda)$, где S, X, Y — алфавиты состояний, входов и выходов соответственно, а δ, λ — функции переходов и выходов. Функции автомата обычным образом распространяются на множество X^* . Будем говорить, что вход-выходное слово $w = (p, q)$ порождается состоянием s автомата A, если $\lambda(s, p) = q$. С каждым состоянием s ассоциируется множество λ_s всех вход-выходных слов, порождаемых этим состоянием. Автомат A удобно задавать в виде графа переходов, вершинами которого являются состояния из S, а дугами — четверки $(s, x, y, t) = u$, где $\delta(s, x) = t$, $\lambda(s, x) = y$. Множество W вход-выходных слов назовем экспериментом автомата A, если $W \subseteq \lambda_s$ для некоторого состояния s . Эксперимент W называется простым, если он состоит из

одного вход-выходного слова, и кратным в противном случае. Через Φ_A обозначаем множество экспериментов автомата A . Эксперимент определяет множество путей в графе переходов автомата из состояния s, и если оно содержит (покрывает) все множество дуг графа переходов, то эксперимент называем обходом автомата из состояния s. Число вхождений дуги в пути, соответствующие эксперименту, назовем ее кратностью в эксперименте. Эксперимент $W \in \Phi_A$ называется контрольным для (A, F), если из того, что $W \in \Phi_B$, $B \in F$, следует, что B содержит подавтомат, эквивалентный A. Обычно класс F выбирается так, что вместо эквивалентности рассматривается изоморфизм.

Каждой паре $(s, x) \in S \times X$ автомата A поставим в соответствие множество состояний $O(s, x)$, причем так, что $s, \delta(s, x) \in O(s, x)$. Обозначим совокупность таких множеств через $O(A)$ и назовем ее локализацией A. Локально определенным (посредством локализации $O(A)$) классом назовем класс $LO(A)$ автоматов, образующихся из автомата A заменой в нем некоторой дуги (s, x, y, t) дугой (s, x, y, r), где $r \in O(s, x)$, или множеством таких замен. Локально диагностируемым (по локализации $O(A)$) назовем автомат, в котором для любых различных $r, t \in O(s, x)$, $(s, x) \in S \times X$, верно неравенство $\lambda(r, x') \neq \lambda(t, x')$ для любого $x' \in X$. Пусть A локально диагностируем и некоторое его состояние r имеет простой начальный идентификатор длины 1 [2], т. е. $\lambda(r, x) \neq \lambda(t, x)$ для какого-то $x \in X$ и любого состояния $t \neq s$. Для простоты полагаем, что A сильно связный.

Теорема 1. *Эксперимент W автомата A является контрольным для $(A, LO(A))$, если он является таким обходом автомата A из состояния r, что для каждого слова $w = v(x, y) \in W$ дуга, покрываемая парой $(x, y) \in X \times Y$, имеет кратность в эксперименте W больше* 1.

Следствие 1. *Длина минимального простого контрольного эксперимента для $(A, LO(A))$ не меньше $mn+1$ и не больше $(m+1)n+1/2(m-1)n(n-1)$, где n, m — число состояний и входов автомата A соответственно, и нижняя оценка достижима.*

Теорема может быть усилена, если при выборе локализации потребовать следующее. K-окрестностью состояния s в автомате A назовем множество его состояний, достижимых из s по словам длины не более k, или из которых достижимо s по словам такой же длины. Потребуем, чтобы любое множество $O(s, x) \in O(A)$ содержало k-окрестность состояния s. Класс автоматов по такой локализации обозначим $LOC_k(A)$. Тогда при замене в условиях теоремы 1 класса

$LO(A)$ на класс $LOC_k(A)$ справедлива

Теорема 2. *Эксперимент W автомата A является контрольным для $(A, LOC_k(A))$ при любом натуральном k тогда и только тогда, когда он является таким обходом автомата A, что для каждого слова $w = v(x,y) \in W$ дуга, покрываемая парой $(x,y) \in X \times Y$, имеет кратность в эксперименте W больше* 1.

Следствие 1 этом случае также можно усилить.

Следствие 2. *Длина минимального простого контрольного эксперимента для $(A, LOC_k(A))$ при любом натуральном k не меньше $mn+1$ и не больше $mn + 1/2(m-1)n(n-1) + 1$, где n, m — число состояний и входов автомата A соответственно, и обе оценки достижимы.*

Из полученных характеризаций следует полиномиальность задачи распознавания контрольных экспериментов для таких классов в отличие от других n-плотных классов (n-полного, групповых автоматов, без потери информации и др.), для которых эта задача является NP-полной даже при условии максимального разнообразия в поведении эталона [4].

Список литературы

1. Bhattacharyya A. Checking experiments on sequential machines. — New York: J. Wiley and Sons, 1989.

2. Козловский В. А., Копытова О. М. Представления автоматов относительно m-плотных классов // Матер. VIII Межд. семинара "Дискретная математика и ее приложения" (Москва, 2–6 февраля 2004 г.). — М.: Изд.-во мех-мат ф-та МГУ, 2004. — С. 277–280.

3. Грунский И. С., Козловский В. А. Синтез и идентификация автоматов. — Киев: Наукова думка, 2004.

4. Козловский В. А. Локальные неисправности автомата и их обнаружение // Математические вопросы кибернетики, вып. 3. — М.: Наука, 1991. — С. 167–186.

О 2-РАЗМЕЧЕННЫХ ЭКСПЕРИМЕНТАХ ГРУППОВЫХ АВТОМАТОВ

В. А. Козловский, Л. А. Мучникова (Донецк)

Контрольные эксперименты с автоматами относительно бесконечных классов существуют только при дополнительных допущениях о возможности наблюдения в эксперименте некоторой информации о внутренних состояниях исследуемого автомата. В работе [1]

такие допущения были введены в виде специальных меток, наблюдаемых в эксперименте и сигнализирующих о нахождении автомата в некоторых его состояниях. Было введено понятие размеченного эксперимента и подробно исследован случай единственной метки. При этом допущении были получены точные оценки длины таких экспериментов. Увеличение мощности множества наблюдаемых в эксперименте меток расширяет возможности экспериментатора и может приводить к более эффективным по длине экспериментам.

В настоящей работе рассмотрена ситуация, когда в размеченном эксперименте присутствуют две различные метки, и дана оценка выигрыша в длине эксперимента в этом случае по сравнению с вариантом одной метки.

Рассматриваются автоматы Мили $A= (S, X, Y, \delta, \lambda)$, где S, X, Y — множества состояний, входов и выходов соответственно, а δ, λ — функции переходов и выходов. Каждому символу $x \in X$ ставится в соответствие отображение множества состояний в себя $\delta_x(s)$, $\delta_x(s) = \delta(s, x)$. Множество всех таких отображений как образующих порождает полугруппу $G(A)$ преобразований множества состояний, которая называется опорной полугруппой автомата A. Автомат называется групповым или перестановочным, если его опорная полугруппа является группой.

Если $\lambda(s, p) = q$, $s \in S$, $p \in X^*$, $q \in Y^*$, то пару $w = (p, q)$ называем вход-выходным словом, порожденным автоматом A, а слово p — первой проекцией $pr_1 w$ слова w.

Пусть A — конечный связный приведенный групповой автомат, а $F(X, Y)$ — класс всех связных приведенных групповых автоматов в алфавитах X и Y. Обычно контрольным экспериментом с автоматом A относительно заданного класса автоматов F называется такое множество вход-выходных слов, порождаемых некоторым состоянием автомата, что его порождение некоторым состоянием другого автоматом B из заданного класса влечет изоморфизм автоматов A и B. Однако в этом случае не существует контрольных экспериментов в классическом понимании. В [2] введено и изучалось понятие размеченного эксперимента, которое обобщает понятие обычного эксперимента.

Зафиксируем некоторое множество M меток мощности k. Пусть $w = (p, q) \in \lambda_t$, где t — состояние некоторого автомата B . Пусть также $p = p_0 p_1 p_2 ... p_{k+1}$, $q = q_0 q_1 q_2 ... q_{k+1}$, где $\delta(t, p_0) = s_1$, $\delta(s_1, p_1) = s_2$, ... , $\delta(s_k, p_k) = s_{k+1}$, $\lambda(t, p_0) = q_0$, $\lambda(s_1, p_1) = q_1$, ... , $\lambda(s_k, p_k) = q_{k+1}$, и p_i непустое слово при $i = 1,..., k$.

Функцию φ, сопоставляющую каждому состоянию автомата некоторую метку или пустой символ e, назовем функцией разметки автомата B.

Состояние $s \in S_B$, для которого $\varphi(s) \neq e$, назовем отмеченным. Тогда размеченным словом (размеченным экспериментом) называется слово

$w_\varphi = (p_0, q_0)\ \varphi(s_1)\ (p_1, q_1)\varphi(s_2)\ ...\ \varphi(s_k)(p_k, q_k)\ \varphi(s_{k+1})(p_{k+1}, q_{k+1})$, если s_i — отмеченное состояние, $i = 1, ..., k+1$. Если $\varphi(s_i) = e$, то символ e в слове w_φ не указывается. Множество всевозможных размеченных экспериментов автомата B обозначим Φ_B.

Пусть F — некоторое подмножество полностью определенных сильно связных приведенных автоматов и $A \in F$ — эталон. Размеченный эксперимент $w_\varphi \in \Phi_A$ назовем контрольным размеченным экспериментом для A и F, если из принадлежности $w_\varphi \in \Phi_B$ для $B \in F$ следует равенство $A = B$.

Оценим длину минимальных контрольных размеченных экспериментов, в которых возможно наличие двух различных меток. Такие эксперименты назовем 2-размеченными, и рассматриваем их для автоматов $A \in K_{n,m}$ и бесконечного класса $F(X, Y)$, где $K_{n,m} \subset F(X, Y)$ класс групповых автоматов с n состояниями и m входными символами. При этом рассматриваются приведенные контрольные эксперименты, то есть такие эксперименты, удаление любого слова из которых приводит к эксперименту, не являющемуся контрольным.

Пусть $d_2^{n,m}$ — длина минимального контрольного 2-размеченного эксперимента для $A \in K_{n,m}$ и $F(X, Y)$.

Теорема. *Справедливо неравенство*

$$d_2^{n,m} \leq n(mn-n+1)+2[l/2]((m-1)[l/2]+m-2)+(m-1)l(l-2n+1)+ \\ + l - 2[l/2])([l/2]2(m-1) + 2m - 3),$$

где l — расстояние между отмеченными состояниями в графе переходо автомата A без учета ориентации.

В [2] приведены оценки длины $d_1^{n,m}$ минимального контрольного размеченного эксперимента с одной меткой для $A \in K_{n,m}$ и $F(X, Y)$: $d^{n,1} = n$; $2(k+1)(mn-n+1)+mn-2m/(m-1)(m^{k+1}-1) \leq d_1^{n,m} \leq n(mn-n+1)$, при $m > 1$ и $k = [\log_m((mn-n+1)/m)]$, причем обе оценки достижимы.

Сопоставляя ее с оценкой в случае двух меток, получаем, что в варианте двух меток имеется выигрыш по длине эксперимента, равный $2[l/2]((m-1)[l/2]+m-2)+(m-1)l(l-2n+1)+l-2[l/2])([l/2]2(m-1) + 2m - 3)$, где l — расстояние между отмеченными состояниями.

Список литературы

1. Козловский В. А., Толмачевская Л. А. Эксперименты с автоматами в алгебраически определенных классах // Материа-

лы IX Международной конференции "Интеллектуальные системы и компьютерные науки" (Москва, 23–27 октября 2006 г.). — М.: Изд-во механико-математического факультета МГУ, 2006. — Т. 1, часть 1. — С. 133–138.

2. Мучникова Л. А. Контрольные эксперименты с групповыми автоматами: Автореф. дисс. ... канд. физ-мат.наук. — Донецк, 2006.

О СВОЙСТВАХ КОНФИГУРАЦИЙ АБСТРАКТНОГО ПРОСТРАНСТВА ЗНАНИЙ

К. И. Костенко (Краснодар)

Абстрактное пространство знаний — это формальная модель, предназначенная для исследования концепции семейства знаний предметной области средствами математики и логики, которое должно обеспечить доказанными информационными структурами и алгоритмами современные технологии создания и использования конкретных цифровых пространств знаний.

Цифровое пространство знаний — это информационная среда, реализующая технологию создания и использования семейств предметных и профессиональных знаний с помощью систем инфомационных объектов, формирующих многообразие слабоструктурированных и слабоформализованных представлений знаний, применяемых пользователями для решения профессиональных задач методы, моделирующими процессы человеческого мышления.

Абстрактным пространством знаний называется алгебраическая категория K, семейство объектов которой $Ob(K)$ образуют классы семантических пространств $Ob(R)$, пространств конфигураций $Ob(M)$ и эволюций знаний $Ob(P)$.

Элементы семантических пространств используется для связывания отдельных абстрактных знаний и их фрагментов. Элементы пространств конфигураций образуют формальные представления знаний, имеющие вид иерархий. Пространства эволюций знаний составляют вычислимые последовательности конфигураций, реализующие жизненные циклы знаний.

Семантическим пространством называется алгебраическая система $R = (\Re, O, C)$, где $\Re$ — бесконечное нумерованное множество семантических связей. Если $r \in \Re$, то множество пар конфигураций, между которыми возможна связь r, является разрешимым. Множества функциональных и логических операций O и C на R включают

вычислимые операции $\cup$ и $\cap$ — нахождения верхних и нижних граней произвольных пар элементов $\Re$, а также операцию композиции c, позволяющую формировать иерархические структуры, представляющие с помощью отдельной семантической зависимости произвольные системы связей подконфигураций в составе пары связываемых этой зависимостью конфигураций. Для R алгоритмически разрешимо сравнение включения множеств пар конфигураций, представляющих элементы $\Re$.

Пространством конфигураций называется бесконечное нумерованное множество $\mathbf{M}$, на котором определена операция декомпозиции $\mathbf{d} = (\epsilon, \psi)$, где $\epsilon : \mathbf{M} \times \mathbf{M} \mapsto \mathbf{M}$ и $\psi : \mathbf{M} \times \mathbf{M} \mapsto \Re$ — вычислимые и всюду определенные функции. Отображение ϵ реализует последовательное разложение элементов $\mathbf{M}$ на подконфигурации вплоть до элементарных конфигураций, а ψ — задает значения семантических связей между парами элементов $\mathbf{M}$, на которые разлагаются отдельные конфигурации. Корню дерева $D(z)$, представляющего непустую конфигурацию z, сопоставлено отношение $\psi(z)$, а его левое и правое поддерево соответствуют представлениям первой и второй конфигураций из $\epsilon(z)$. Разложение ϵ называется конечным, если все деревья разложений конфигураций — конечные.

Рассматриваем только конечные разложения.

Конфигурация $z \in \mathbf{M}$ называется канонической, если элементы структур семантических связей, приписанных внутренним вершинам $D(z)$ представляют зависимости подконфигураций $z \in \mathbf{M}$, одна из которых входит в $\epsilon(z)$. Конфигурации $z_1 \in \mathbf{M}$ и $z_2 \in \mathbf{M}$ называются эквивалентными, если представляемые ими многообразия элементарных подконфигураций и интегрированных семантических связей между произвольными парами подконфигураций в z_1 и в z_2 совпадают.

Теорема 1. *Существует алгоритм, преобразующий всякую конфигурацию $z \in \mathbf{M}$ в эквивалентную ей каноническую конфигурацию.*

Возможность представления конфигурациями произвольных структур знаний (семантических представлений [1]) характеризуется следующей теоремой.

Теорема 2. *Всякая семантическая сеть может быть представлена конфигурацией пространства знаний.*

Если $z \in \mathbf{M}$, то множество висячих вершин дерева $D(z)$ обозначается как $O(z)$. Вершины бесконечного насыщенного бинарного дерева будем представлять двоичными наборами, так что корню дерева соответствует пустой набор. Изотонное отображение ξ вершин бесконечного бинарного дерева в себя называется трассированием

$z_1 \in \mathbf{M}$ в $z_2 \in \mathbf{M}$, если:

1) $\xi(D(z_1)) \subseteq \xi(D(z_2)) \wedge \forall \alpha \in D(z_1)(\alpha \in D(z_1) \setminus O(z_1) \leftrightarrow \xi(\alpha) \in D(z_2) \setminus O(z_2))$;

2) $\forall \alpha, \alpha\sigma \in D(z_1), \sigma \in \{0,1\}\ \exists\ \beta, \gamma \in I\ ((\xi(\alpha) \subset \xi(\alpha\sigma) \rightarrow \xi(\alpha\sigma) = \xi(\alpha)\beta\sigma\gamma)$.

Отображения трассирований конфигураций с дополнительными условиями на значения параметров β и γ предыдущего определения разбиваются на классы, включающие трассирования растяжения, сжатия и растяжения-сжатия [2].

Изотонное отображение $\xi : D(z) \mapsto D(z)$, сохраняющее свойства элементов $D(z)$ быть внутренними и висячими, определяет фрагмент z. Если такой фрагмент является конфигурацией, то ξ задаёт эпиморфизм конфигурации z в себя.

Эпиморфизмы конфигураций реализуют схемы извлечения знаний из знаний, основанные на отображениях трассирования. Изучение таких отображений связано с задачами интеграции систем знаний в новые знания, анализа многообразий знаний, эквивалентных сложным знаниям, отыскания в таких многообразиях отдельных знаний, имеющих минимальную комбинаторную сложность.

Теорема 3. *Множество эпиморфизмов конфигураций, порождаемых трассированиями растяжения замкнуто относительно операции суперпозиции.*

Множество всех эпиморфизмов конфигураций не является замкнутым для операции суперпозиции.

Работа выполнена при поддержке РФФИ, грант № 06-07-96618.

Список литературы

1. Кузнецов И. П. Семантическое представление. — М.: Наука, 1978.

2. Костенко К. И. Биморфизмы конфигураций абстрактных пространств знаний // Экологический вестник научных центров Черноморского экономического сотрудничества. — 2005. — № 2. — С. 6–14.

ОЦЕНКИ СЛОЖНОСТИ ПОИСКА ИДЕНТИЧНЫХ ОБЪЕКТОВ ДЛЯ СЛУЧАЙНЫХ БАЗ ДАННЫХ

Н. С. Кучеренко (Москва)

Теория хранения и поиска информации является важным разделом теории интеллектуальных систем. Одним из ключевых объектов

этой теории является информационный граф (ИГ) [1] — управляющая система, которая позволяет рассматривать имеющиеся модели данных и задачи, связанные с ними, с более общих позиций.

В данной работе в рамках информационно-графовой модели данных рассматривается задача поиска идентичных объектов (ЗПИО) на отрезке $[0,1]$. Формально ЗПИО на отрезке $[0,1]$ — это тройка $I = ([0,1], V, \rho_=)$, где V — конечное подмножество отрезка $[0,1]$, которое называется библиотекой, $\rho_=$ — отношение равенства [1]. С помощью информационных графов моделируются алгоритмы поиска в библиотеке, использующие только операции сравнения.

В предположении, что на множестве запросов задано вероятностное пространство, для информационного графа U вводится понятие сложности $T(U)$. Сложность $T(U)$ — это математическое ожидание сложности ИГ на запросе [1]. Сложностью задачи $T(I)$ определяется как инфимум сложности всех ИГ, которые решают задачу I. Информационный граф, на котором достигается инфимум, называется *оптимальным*. Для любой задачи $I = ([0,1], V, \rho_=)$ оптимальный информационный граф существует, также существует полиномиальный алгоритм его построения [3].

С помощью информационного графа всегда можно реализовать логарифмический поиск, который имеет сложность, равную логарифму от мощности библиотеки. Затраты на построение оптимального ИГ оцениваются квадратом от мощности библиотеки, при этом сложность оптимального ИГ может быть как константой, так и логарифмом, в зависимости от конкретной задачи.

В работе рассмотрен класс задач поиска идентичных объектов Υ_n^f, в котором элементы библиотеки $V_n = \{y_1, y_2, \ldots, y_n\}$ являются независимыми равномерно распределенными случайными величинами на отрезке $[0,1]$, а распределение запросов задается с помощью функции плотности $f(x)$. Обозначим сложность оптимального ИГ для задачи $([0,1], V_n, \rho_=) \in \Upsilon_n^f$ через $T^f(V_n)$. Тогда $T^f(V_n)$ будет случайной величиной, через $\mathbf{M}\,T^f(V_n)$ обозначим ее математическое ожидание.

Теорема. *Для любой интегрируемой по Риману функции f справедливо*

$$\mathbf{M}\,T^f(V_n) \sim \log_2 n \quad (n \to \infty).$$

В случае, когда $f(x) \equiv 1$, для любого фиксированного n

$$\mathbf{M}\,T^1(V_n) \geq \log_2(n+1) + \frac{\gamma_{n+1} - 1}{\ln 2},$$

где $\gamma_n = \sum_{i=1}^{n} \frac{i}{n} - \ln(n)$ *и последовательность* γ_n *сходится к постоянной Эйлера* $\gamma = 0,577\ldots$

Интерпретируя результат теоремы, можно сказать, что в среднем оптимальный ИГ не дает выигрыша по сравнению со стандартным методом деления пополам, поэтому затраты на оптимизацию не целесообразны.

Автор выражает благодарность своему научному руководителю профессору Гасанову Эльяру Эльдаровичу за постановку задачи, внимание к работе, ценные советы и обсуждения.

Список литературы

1. Гасанов Э. Э., Кудрявцев В. Б. Теория хранения и поиска информации. — М.: Физматлит, 2002.

2. Knuth D. E. Optimum binary search trees // Acta Informatica. — 1971. — Т. 1, № 1, — С. 14–25.

3. Кучеренко Н. С. О сложности поиска идентичных объектов для случайных баз данных // Материалы IX Международной конференции "Интеллектуальные системы и компьютерные науки" (23–27 октября 2006 г.). — М.: Изд-во механико-математического факультета МГУ, 2006. — С. 171.

ОБ АЛГЕБРАИЧЕСКИХ ОПЕРАЦИЯХ НА ГРАФАХ, СОХРАНЯЮЩИХ СТЕПЕННУЮ ПОСЛЕДОВАТЕЛЬНОСТЬ

М. И. Лашева (Москва)

В настоящей работе получены оригинальные алгоритмы для решения известной задачи о реализациях графической (степенной) последовательности, допускающие обобщения на случаи ориентированных графов и гиперграфов и использующие ограниченный ресурс памяти.

В общем случае графическая последовательность имеет несколько попарно неизоморфных реализаций. В установлении связи между графическими реализациями играет роль понятие переключения. Пусть $G = (V, E)$ — граф, a, b, c, d — четыре различные его вершины такие, что $\{a, b\}, \{c, d\} \in E$, $\{a, c\}, \{b, d\} \notin E$. Тогда говорят, что граф допускает переключение $\{\{a, b\}, \{c, d\}\}$, а результатом применения операции переключения $\{\{a, b\}, \{c, d\}\}$ является граф $G' = (V, E'), E' = (E \cup \{\{a, c\}, \{b, d\}\}) \setminus \{\{a, b\}, \{c, d\}\}$. Известен алгоритм, используя который при помощи операции переключения

ребер из любого графа с заданной степенной последовательностью может быть получен любой другой граф с той же степенной последовательностью. Время работы указанного алгоритма растет по порядку как $n^2 \log_2 n$. При этом алгоритм существенно использует возможность нелинейного (по размеру задачи) расширения либо оперативной, либо внешней памяти.

Рассмотрим некоторое подмножество $A(d(n))$ множества графов $M(d(n))$ с n занумерованными вершинами, обладающих заданной степенной последовательностью вершин $d(n)$. Определим операцию

$$\omega(A(d(n))) = \Big\{G' |\ \exists\, G = (V, E) \in A(d(n)),$$
$$\exists\, v_1, v_2, v_3, v_4 \in V,\ \{v_1, v_2\}, \{v_3, v_4\} \in E, \{v_1, v_3\}, \{v_2, v_4\} \notin E,$$
$$G' = (V, (E \cup \{\{v_1, v_3\}, \{v_2, v_4\}\}) \setminus \{\{v_1, v_2\}, \{v_3, v_4\}\})\Big\}.$$

Очевидно, что $\omega(A(d(n)))$ является подмножеством $M(d(n))$, то есть операция ω не меняет степенную последовательность вершин.

Конечно-автоматный алгоритм — это пара (A, T), где A — конечный автомат, T — некоторая двумерная таблица, каждый элемент t_{ij} которой является элементом некоторого конечного множества L. Автомат A применяется к таблице T в следующем смысле. В момент времени t автомат находится в некотором состоянии q_t. На вход автомата поступает некоторый элемент $t_{ij} \in T$. Выходом является элемент из L. Он записывается в эту клетку; автомат перемещается в одну из клеток с координатами $(i-1, j), (i, j-1), (i+1, j), (i, j+1)$ (при условии, что такая клетка существует) или остается на месте в клетке с координатами (i, j) и переходит в некоторое состояние q_{t+1}. В начальном состоянии q_0 автомат находится в клетке с координатами $(1, 1)$, и на вход автомату поступает элемент t_{11}. Работа автомата заканчивается, если он переходит в заключительное состояние q'.

Конечно-автоматный алгоритм работает по схеме: кодирование, обработка результатов кодирования некоторым конечным автоматом, декодирование.

Рассмотрим множество пятерок $L = \{\{c_1, c_2, I_1, I_2, I\},\ c_1 \in \{0, 1, 2, 3, 4\}, c_2 \in \{0, 1, 2, 3, 4\}, I_1 \in \{0, 1\}, I_2 \in \{0, 1\}, I \in \{0, 1, 2\}\}$.

Блок кодирования конечно-автоматного алгоритма паре графов $(G_1, G_2) \in \Gamma^2, G_i = (V_i, E_i),\ |V_i| = n, i = 1, 2$, взаимно однозначно сопоставляет таблицу специального вида — треугольник смежностей T размера n.

Треугольник смежностей размера n, сопоставленный паре графов $(G_1, G_2) \in \Gamma^2$, — это таблица с n строчками и n столбцами, $T = (t_{ij}), i = 1, 2, ..., n, j = i, i+1, ..., n$, каждый элемент t_{ij} которой является элементом некоторого конечного множества L.

Треугольник смежностей T взаимно однозначно сопоставляется паре графов $(G_1, G_2) \in \Gamma^2$ следующим образом: для $i \leq j$ положим $t_{ij} = \{c_1, c_2, I_1, I_2, I\}$, где $c_1 = c_2 = 0$, $I_k = 1$, если ребро $\{v_i, v_j\} \in E_k$; $I_k = 0$, — иначе, $k = 1, 2$. $I = 1$, если $i = j$, $i \neq 1, n$, $i \neq 1, n$, либо $i = 1, 1 < j < n$, либо $j = n$, $1 < i < n$; $I = 2$, если $i = j = 1$, $i = j = n$, $i = 1, j = n$; $I = 0$— иначе.

Автомат A перерабатывает треугольник смежностей T, в соответствии со схемой построенного общего алгоритма (ОА), в треугольник смежностей T', по которому взаимно однозначно восстанавливается пара графов (G'_1, G'_2) такая, что $G'_i \in \omega^{N_i}(\{G_i\}), i = 1, 2$, и $G'_1 \cong G'_2$.

Блок декодирования строит по T' такую пару (G'_1, G'_2) следующим образом: если $t_{ij} = \{c_1, c_2, I_1, I_2, I\}$, то при $I_k = 1$ $\{v_i, v_j\} \in E_k$, $k = 1, 2$, иначе — $\{v_i, v_j\} \notin E_k$.

Теорема 1. *Справедливы следующие утверждения:*

1. *ОА является конечно-автоматным.*

2. *Время работы ОА на графе G с n вершинами растет по порядку, как n^3.*

3. *Время работы ОА на графе G с n вершинами, степень каждой из которых растет не быстрее k (не более заданной константы K), равно по порядку $k^2 n$ (n).*

Аналогично построены обобщения ОА на ориентированные графы и гиперграфы.

Рассмотрим множество всех занумерованных графов $\{G_1, \ldots, G_m\}$, имеющих одинаковую степенную последовательность $d(n)$.

Метаграфом для данной степенной последовательности $d(n)$ называется неориентированный граф $MG(d(n)) = (V, E)$, такой что $V = \{G_1, ..., G_m\}$, и $\{G_i, G_j\} \in E$ тогда и только тогда, когда в графе G_i существует пара ребер, к которым применима операция ω и в результате её применения получается граф G_j.

Теорема 2. *Справедливы следующие утверждения:*

1. *Метаграф $MG(d(n))$ для любого n является связным графом.*

2. *Для любого n существует степенная последовательность $d(n)$, в метаграфе $MG(d(n))$ которой есть цепь длины, равной по порядку n^2.*

3. *Для любого n существует степенная последовательность $d(n)$, такая что наибольшая степень вершины в метаграфе $M(d(n))$ равна по порядку n^4.*

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

2. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1979.

3. Емеличев В. А., Мельников О. И., Сарванов В. И., Тышкевич Р. И. Лекции по теории графов. — М.: Наука, 1990.

ПРИБЛИЖЕННЫЙ АЛГОРИТМ ЗАДАЧИ ШТЕЙНЕРА ВОССОЗДАНИЯ ЭВОЛЮЦИИ ЕСТЕСТВЕННЫХ ЯЗЫКОВ

Э. Ю. Лернер (Казань)

Целью представляемой работы являлось воссоздание эволюции языков различных языковых групп на основе данных из базы ИЯз РАН “Языки мира” [1]. В этой базе каждый язык характеризуется с помощью 3821 бинарного признака, содержащих описания фонетики, морфологии и синтаксиса. Для тестирования были выбраны 42 языка из различных языковых семей. Отмечу, что были представлены как отдельностоящие языки, так и группы близких языков.

Пусть дан взвешенный полный граф G и выделено некоторое подмножество его вершин S. Задача Штейнера состоит в отыскании дерева T в этом графе, множество вершин которого включает в себя все вершины из S (но, возможно, не ограничивается ими), причем суммарный вес ребер этого дерева минимально возможный. При представлении нашей задачи как задачи Штейнера в качестве вершин графа рассматриваются всевозможные битовые последовательности длины $m = 3821$, а в качестве множества S те из них, которые соответствуют битовым последовательностям, отражающим признаки языков, выбраных для рассмотрения. Весом ребра между двумя битовыми последовательностями будем считать количество различных компонент в них. Задача построения дерева Штейнера как для произвольного графа, так и в рассматриваемом случае

является NP-полной. Был разработан простой приближенный алгоритм, идейно близкий к алгоритму Прима построения минимального остовного дерева, дающий гарантированную относительную погрешность меньшую двух. Другие приближенные алгоритмы (см., например, [2]) оказались неудобны для реализации в данной задаче.

Приближенный алгоритм решения задачи Штейнера:

1. Два наиболее близких битовых вектора из S соединяются ребром (в качестве ребра между векторами V_1 и V_2 рассматривается совокупность битовых векторов, у которых фиксированы значения в позициях, совпадающих у V_1 и V_2, а значения в остальных позициях произвольны). Это начальный кусок для последующего наращения дерева. Пусть S' — все остальные вектора из S.

2. Ищется вектор $V \in S'$, наиболее близко лежащий к уже построенной части дерева. В качестве расстояния от вектора до ребра используется минимальное из расстояний до образующий его векторов, а в качестве расстояния до дерева используется минимальное из расстояний до его ребер.

Из совокупности битовых векторов, соответствующих ближайшему к V ребру выбирается наиболее близко лежащий к V вектор V'. В случае, если V' не был до этого вершиной дерева, рассматриваемое ребро разбивается на две части относительно V'. После чего в дерево добавляется ребро из V в V'. Вектор V вычеркивается из S'.

3. В случае, если S' не пусто, перейти к шагу 2.

Алгоритм легко обобщается на случай произвольного графа G.

Теорема. *Относительная погрешность алгоритма меньше, чем* 2.

Лемма 1. *Вес построенного дерева меньше веса минимального остовного дерева в взвешенном графе с вершинами S и с ребрами, вес которых равен длине кратчайших путей в исходном графе.*

Лемма 2. *Половина веса минимального остовного дерева из леммы* 1 *больше веса оптимального дерева Штейнера.*

Теорема 1, очевидно, следует из лемм 1 и 2. Утверждение леммы 2 является фольклором евклидовой задачи Штейнера ([2]). Для доказательства леммы 1 докажем сначала вспомогательную лемму 3.

Лемма 3. *Пусть вершины некоторого дерева занумерованы в произвольном порядке. Тогда ребра дерева можно занумеровать так, что ребро с номером i соединяет вершину номер которой не превышает i, с вершиной номер которой больше, чем i.*

Доказательство леммы 3. Сопоставим номер 1 ребру, соединяющему 1-ю вершину с вершиной с минимальным номером; номер 2 — незанумерованному ребру, соединяющему вершину с номером, не большим 2, с вершиной с минимальным номером и т. д. Докажем,

что на шаге i множество незанумерованных ребер, исходящих из вершин с номерами не большими i, не пусто, причем все они соединяют эти вершины с вершинами, имеющими номера больше, чем i. Докажем сначала вторую часть утверждения. Допустим, что i — ребро, соединяющее вершины с номерами не большими i. Пусть j — последнее ребро, меньшее i, инцидентное вершине с номером большим, чем i. Тогда по построению все ребра с номерами $j+1, \ldots, i$ соединяют вершины внутри множества $\{j+1, \ldots, i\}$. Значит в графе существует цикл, что невозможно. Вторая часть утверждения доказана.

Осталось доказать существование на шаге i хотя бы одного незанумерованного ребра, исходящего из вершины с номером не большим i. Стянем все ребра, соединяющие вершины с номерами не большими i. Пусть их количество равно r. Как доказано выше, все они занумерованы. После стягивания вместо i вершин графа с номерами, не большими i, останется $i-r$ стянутых вершин. Они уже не могут быть связаны между собой, значит они связаны по крайней мере $i-r$ ребрами с вершинами с номерами большими i. Из этих ребер ровно $i+1-r$ ребер занумеровано ранее шага i. Значит среди них есть хотя бы одно незанумерованное ребро, что и требовалось доказать.

Доказательство леммы 1. Занумеруем вершины S минимального остовного дерева в том порядке, в котором они появляются при построении дерева Штейнера нашим алгоритмом. Занумеруем в соответствующем порядке (согласно лемме 3) ребра минимального остовного дерева. Тогда ребро с номером i соответствует пути, соединяющему вершины, одна из которых на шаге i нашего алгоритма принадлежала построенной части дерева, а другая — нет. Поскольку наш алгоритм выбирает минимальный из таких путей, то увеличение веса дерева Штейнера на шаге i ограничено сверху весом ребра i минимального остовного дерева, что т требовалось доказать.

Легко видеть, что рассматриваемый алгоритм имеет сложность $O(n^2m)$, где n — количество языков. Для рассматриваемой выборки языков он дал лучшие или примерно одинаковые результаты по сравнению с точными алгоритмами построения наиболее близкого (в смысле метрики L_∞) ультраметричного и аддитивного дерева, а так же известными эвристическими алгоритмами UPGMA и NJ [3].

Работа выполнена при поддержке РФФИ, грант № 07-06-00229а.

Список литературы

1. Поляков В. Н., Соловьев В. Д. Компьютерные модели и методы в типологии и компаративистике. — Казань: КГУ, 2007.

2. Robins G., Zelikovsky A. Tighter bounds for graph Steiner tree

approximation // SIAM Journal on Discrete Mathematics. — 2005. — V. 19, № 1. — P. 122–134.

3. Kim J., Warnow T. Tutorial on phylogenetic tree estimation // Intelligent Systems for Molecular Biology. — Heidelberg, 1999.

РАЗРЕШИМЫЙ СЛУЧАЙ ЗАДАЧИ ВЫРАЗИМОСТИ ДЛЯ АВТОМАТНЫХ ФУНКЦИЙ ОТНОСИТЕЛЬНО СУПЕРПОЗИЦИИ

А. А. Летуновский (Москва)

Рассматривается задача выразимости константных автоматных функций относительно суперпозиции. Показано, что для конечных систем автоматных функций, содержащих все истинностные функции и задержку, существует алгоритм выразимости константных автоматных функций. Также показано существование алгоритма для задачи бесконечности множества выразимых константных автоматных функций.

Пусть $E_k = \{0, 1, ..., k-1\}$, функции вида $g : E_k^n \to E_k$ называются функциями k-значной логики, их множество обозначается через P_k. Пусть E_k^∞ — множество всех сверхслов вида $a(1)a(2)...$, где $a(j) \in E_k$, $j = 1, 2, ...$ Через N обозначим множество натуральных чисел. Пусть $f : (E_k^\infty)^n \to (E_k^\infty)^m$ — автоматная функция(a-функция), т. е. она задается рекуррентно соотношениями (1)

$$\begin{cases} q_1(1) = q0_1, \\ ... \\ q_s(1) = q0_s, \\ q_1(t+1) = \phi_1(q_1(t), ..., q_s(t), a_1, ..., a_n), \\ ... \\ q_s(t+1) = \phi_s(q_1(t), ..., q_s(t), a_1, ..., a_n), \\ b_1(t) = \psi_1(q_1(t), ..., q_s(t), a_1, ..., a_n), \\ ... \\ b_m(t) = \psi_m(q_1(t), ..., q_s(t), a_1, ..., a_n). \end{cases} \tag{1}$$

Вектор $q = (q_1, ..., q_s)$ задает состояние a-функции f, $q0$ — её начальное состояние, буквы $a = (a_1, a_2..., a_n)$ и $b = (b_1, ..., b_m)$ называются входной и выходной буквами, а сверхслова $a(1)a(2)...$ и $b(1)b(2)...$ — входными и выходными сверхсловами, соответственно. Вектор-функции ϕ и ψ называются функциями переходов и выходной функцией, соответственно, а шестерка $(E_k^n, E_k^s, E_k^m, \phi, \psi, q0)$ —

автоматом, порождающим функцию f. Класс всех a-функций обозначим через P. В этом классе обычным образом введем операции суперпозиции.

Пусть $M \subseteq P$, обозначим через $[M]$ — множество a-функций, получающихся из M с помощью операций суперпозиции.

Автоматную функцию G_0, задаваемую уравнениями

$$\begin{cases} q(1) = 0, \\ q(t+1) = a(t), \\ b(t) = q(t), \end{cases}$$

называем автоматной функцией задержки; $P^{(1)}$ — множество автоматных функций с одним состоянием.

Константной автоматной функцией назовем автоматную функцию, выдающую одно и тоже периодическое выходное сверхслово на всех входных сверхсловах. Класс константных автоматных функций обозначим через K.

Сверхслово, получающееся на выходе константного автомата K_1 обозначим β_{K_1}.

Определение 1. Пусть сверхслово β можно представить в виде $\beta = \gamma\alpha^{\infty}$. Выберем из всех таких представлений такое, что γ и α имеют наименьшую длину. Для выбранного представления назовем γ — наименьшим предпериодом сверхслова, а α — наименьшим периодом сверхслова.

Для множества сверхслов K' обозначим $\Theta(K')$ — множество длин минимальных периодов сверхслов K'.

Мы будем рассматривать следующие задачи — по конечному множеству M и $\beta \in K$ проверить, верно ли что:

1) $\beta \in [M \cup \{G_0, P^{(1)}\}]$;

2) $\mid \Theta([M \cup \{G_0, P^{(1)}\}] \cap K) \mid < \infty$.

Теорема 1. *Пусть M — конечное множество автоматных функций и β — константная автоматная функция, тогда существует алгоритм, позволяющий проверить свойство $\beta \in [M \cup \{G_0, P^{(1)}\}]$.*

Теорема 2. *Пусть M — конечное множество автоматных функций, тогда существует алгоритм, позволябщий проверить свойство $\mid \Theta([M \cup \{G_0, P^{(1)}\}] \cap K) \mid < \infty$.*

Автор выражает благодарность Кудрявцеву В. Б. и Бабину Д. Н. за ценные замечания и внимание к работе.

Список литературы

1. Кудрявцев В. Б. О мощностях множеств предполных классов некоторых функциональных систем, связанных с автоматами // ДАН СССР. — 1963. — Т. 151, № 3. — С. 493–496.

2. Кратко М. И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов // ДАН СССР. — 1964. — Т. 155, № 1. — С. 35–37.

3. Бабин Д. Н. Разрешимый случай задачи о полноте автоматных функций // Дискретная математика. — 1992. — Т. 4, вып. 4. — С. 41–56.

4. Бабин Д. Н. О классификации автоматных базисов Поста по разрешимости свойств полноты и A-полноты // Доклады РАН. — 1999. — Т. 367, № 4. — С. 439–441.

5. Мальцев А. И. Итеративные алгебры и многообразие Поста // Алгебра и логика. — 1966. — Т. 5, № 2. — С. 5–24.

6. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

7. Летуновский А. А. О выразимости константных автоматнов // Интеллектуальные системы. — 2005. — Т. 9, вып. 1–4. — С. 457–469.

СЛЕЖЕНИЕ ЗА ГЛАЗАМИ ПО ИЗОБРАЖЕНИЮ ЛИЦА ОПЕРАТОРА, ПОЛУЧЕННОГО С ДВУХ КАМЕР

И. Л. Мазуренко, А. Б. Холоденко (Москва)

В настоящее время разрабатывается большое количество систем определения состояния человека, основанных на принципе бесконтактной работы. Такие системы используют дистанционно расположенные датчики и видеокамеры для слежения за различными показателями, которые можно считать с человека, и на основании этой информации определяют состояние человека. Одним из основных потоков информации, которые можно считать с человека посредством видеокамеры является информация о его глазах. Информация о глазах, вкупе с информацией о положении головы, позволяет получить информацию о том, куда смотрит человек, а информация о частоте и скорости морганий позволяет сделать вывод о состоянии человека.

Различные компании и отдельные исследовательские группы используют для решения задач, связанных со слежением за глазами оператора, различные платформы и программное обеспечение. В настоящее время существует большое количество закрытых систем, не доведённых до стадии промышленного применения. Работающий

макет системы слежения за глазами водителя транспортного средства, включающий в себя две видеокамеры и вычислительный комплекс был разработан специалистами нашей рабочей группы в 2004–2005 годах. Для решения этой задачи был использован метод слежения за характерными точками на лице оператора, что позволило восстанавливать положение головы человека в трёхмерном пространстве и устойчиво выделять изображение глаз [1–3].

Реализация данного проекта позволит в будущем значительно повысить точность определения состояния водителей и получить устойчиво работающую систему контроля состояния оператора для многих опасных производств. При этом рассматриваемая система может быть использована в качестве элементарного «кирпичика» для построения более сложных систем.

Для решения поставленной задачи использовалась установка, состоящая из компьютера и двух подключенных к нему видеокамер. На изображениях, получаемых с видеокамер, выделялись характерные точки. Затем, используя информацию о том, что голова человека представляет собой почти твёрдое тело, координаты найденных на изображении характерных точек преобразовывались в координаты головы в трёхмерном пространстве. Определение положения головы в трёхмерном пространстве позволяет надёжно определить области изображения, на которых расположены глаза, и детально исследовать их. Для определения направления взгляда определяется уровень закрытия век и положение центра зрачка по отношению к уголкам глаза. Вместе с информацией о положении головы в пространстве это позволяет определить направление взгляда человека.

Авторы выражают благодарность за постановку задачи своему научному руководителю д.ф.-м.н. Бабину Дмитрию Николаевичу.

Список литературы

1. Бабин Д. Н., Умяров А. Р. Восстановление ракурса динамического объекта по его изображениям // Материалы международного семинара "Супервычисления и математическое моделирование". — Саров, 2003. — С. 20-30.

2. Волченков М. П., Самоненко И. Ю. Об автоматическом распознавании лиц // Интеллектуальные системы. — № 9. — С. 135.

3. Бабин Д. Н., Холоденко А. Б., Волченков М. П. О решении задачи слежения методом выделения характерных точек // Труды VII Международной конференции "Дискретные модели в теории управляющих систем". — 2006. — С. 23–26.

ОБНАРУЖЕНИЕ ДОЛГОВРЕМЕННОЙ ЗАВИСИМОСТИ ВО ВРЕМЕННЫХ РЯДАХ НАГРУЗКИ НА ВЫЧИСЛИТЕЛЬНУЮ СИСТЕМУ

А. В. Николаев (Ставрополь)

На современном этапе развития систем информационной безопасности наблюдается смена парадигмы реагирования на производимые атаки: системы обнаружения вторжений уступают место активно развивающимся системам предотвращения вторжений. Основным недостатком систем обнаружения вторжений является необходимость их постоянного обновления или обучения по мере обнаружения новых уязвимостей, в то время как системы предотвращения вторжений более автономны и позволяют немедленно реагировать на потенциально опасное поведение.

Большинство существующих и разрабатываемых систем предотвращения вторжений уровня приложений основываются на таких способах, как перехват системных вызовов на уровне ядра, контроль переполнения буфера, поиск программных закладок и т. п., что привязывает их к конкретным реализациям архитектурам аппаратной и программной платформ [1].

Свободным от этого недостатка является подход к рассмотрению поведения информационной системы в виде временных рядов нагрузки на ее аппаратные ресурсы, например загруженность центрального процессора, частота и продолжительность обращений к оперативной памяти, системной шине, жестким дискам, сетевому адаптеру и т. д. Нагрузка на аппаратные ресурсы формируется поведением всех активных пользователей данной информационной системы. Прогнозируя будущие значения исследуемых временных рядов мы получаем возможность предсказать дальнейшее поведение пользователей в информационной системе, что позволяет нам принять своевременные меры в случае подготавливаемой атаки на информационную систему.

В ходе эксперимента с многопроцессорного терминального сервера под управлением ОС Windows были получены временные ряды 48 показателей длительностью около 9 часов — один рабочий день. Из них были отобраны 25 показателей, наиболее полным образом отражающих активность пользователей. Однако, полученные временные ряды не являются стационарными, что не позволяет применить к ним инструментарий математической статистики. Для прогнозирования таких временных рядов применимы методы нелинейной динамики [2]. В этом случае имеющиеся временные ряды необходимо проанализировать на предмет наличия в них долговременных зависимостей или самоподобности временного ряда, т. е. для таких временных рядов выполняется утверждение:

$r(k) \sim H(2H-1)k^{2H-2}$, при $k \to \infty$, где H — коэффициент Херста [2, 4], $r(k)$ — коэффициент корреляции.

Согласно [3], существует несколько равнозначных признаков, выявляющих долговременные зависимости во временных рядах:

— гиперболически затухающая корреляционная функция;

— дисперсия выборочного среднего затухает медленнее, чем величина, обратная размеру выборки;

— спектральная плотность вблизи 0 убывает с увеличением частоты по степенному закону, образуя так называемые "тяжелые хвосты";

— показатель Херста [2, 3] находится в интервале $0.5 < H < 1$.

Остановимся подробнее на четвертом признаке — показателе Херста H, так как кроме указания на самоподобие процесса, он играет важнейшую роль в формировании трех оставшихся перечисленных признаков долговременной зависимости.

Известно несколько методов определения самоподобности во временных рядах. Наиболее часто применяемые методы: анализ R/S-статистики; анализ графика изменения дисперсии; анализ особенностей спектральной функции; оценка Виттла; анализ, основанный на вейвлет-функциях. В случае, когда нам лишь требуется проверить наличие долговременной зависимости в ряде, применим анализ R/S-статистики, обладающий невысокой точностью определения показателя Херста, но достаточно простой в реализации и менее требовательный к вычислительным ресурсам.

Методика R/S-анализа к полученным временным рядам применялась следующим образом. Временной ряд $x(t)$ длины N разбивался на N/k непересекающихся отрезков размера k. В случае, если длина временного ряда не делится на N/k частей нацело, последний отрезок являлся набором значений $[x(t_{N-k}+1), x(N)]$. К каждому отрезку $[x(t_{(k-1)*i}+1), x(t_{k*i})]$, где i — порядковый номер отрезка, применялся алгоритм R/S-анализа. Среднее значение полученного ряда значений показателя Херста для отрезков использовалось для оценки долговременной зависимости во временном ряде.

Устойчивые значения показателя Херста в диапазоне черного шума $(0.67; 1)$ были обнаружены в показателях: процент времени прерываний; процент времени, истраченного данным потоком на выполнение кода в привилегированном режиме; процент загруженности центральных процессоров; число операций управления файлами в секунду; число переключений между потоками в секунду; системных вызовов в секунду.

Указанные временные ряды производительности вычислительных систем обладают ярко выраженными внутренними долговре-

менными зависимостями и представляют наибольшую перспективу для дальнейшего анализа и прогнозирования с помощью методов нелинейной динамики.

Работа выполнена при поддержке РФФИ, проект 06-01-00020а.

Список литературы

1. Michael R. Intrusion prevention and active response // Deploying Network and Host IPS. — Syngress Publishing Inc, 2005.

2. Петерс Э. Хаос и порядок на рынках капитала. — М.: Мир, 2000.

3. Шелухин О. И., Тенякшев А. М., Осин А. В. Фрактальные процессы в телекоммуникациях. — М.: Радиотехника, 2003.

4. Федер Е. Фракталы. — М.: Мир, 1991.

О РАСШИФРОВКЕ РАЗБИЕНИЯ БУЛЕВА КУБА НА ГРАНИ

В. В. Осокин (Москва)

Задача расшифровки разбиения булева куба на грани относится к классу задач расшифровки функций. Рассматривается некоторый класс функций и загадывается произвольная функция f из этого класса. Предполагается, что существует некоторый «черный ящик» (оператор $\mathcal{A}_f$), который «знает» функцию, т. е. в ответ на набор из области определения f оператор $\mathcal{A}_f$ выдает значение функции f на этом наборе. Требуется за минимальное число обращений к оператору $\mathcal{A}_f$ полностью восстановить таблицу значений функции f. Впервые задача расшифровки рассматривалась для класса монотонных функций [1]. Другим классом функций, для которого исследовалась задача расшифровки, является класс пороговых функций [2]. В настоящей статье нас будет интересовать класс функций, задающих разбиение булева куба на грани.

Среди задач, близких к исследуемой, можно упомянуть многие задачи теории тестов [3], машинного обучения, а также задачу текстовой классификации [4], привлекающую в последнее время все большее внимание, в частности, в связи с ростом Интернета. В последней требуется распределить документы из некоторого множества документов по заранее заданным категориям. Алгоритмы такой классификации, в основном, сравниваются эмпирически, путем тестирования на больших проанализированных вручную корпусах документов. Рассматриваемый в данной статье подход позволяет

свести задачу классификации текстов к задаче расшифровки разбиения булева куба на грани. Строится алгоритм точной расшифровки и доказывается его асимптотическая неулучшаемость.

Рассмотрим всюду определенную на k-мерном булевом кубе B^k функцию $R : B^k \to N$, такую что для любого числа i из ее области значений $R(B^k)$ прообраз $R^{-1}(i)$ этого числа является гранью B^k. Всякую такую функцию R будем называть *функцией граневого разбиения*, исходя из того, что эта функция разбивает k-мерный куб на непересекающиеся грани путем сопоставления уникального номера каждой грани разбиения.

Фиксируем некоторое $n \in N$. Пусть R — функция граневого разбиения арности k. Рассмотрим множество G^k всех функций $g : \{1, \ldots, k\} \to \{y_1, \ldots, y_n, 0, 1\}$, где $y_1, \ldots, y_n$ — некоторые булевы переменные. Положим $\Phi_R = \{R(g(1), \ldots, g(k)),\ g \in G^k\}$. Легко видеть, что Φ_R — это класс всех функций, полученных из R переименованием переменных, склеиванием переменных и фиксацией переменных константами. Каждая функция $f(y_1, \ldots, y_n)$ из Φ_R существенно зависит не более чем от k переменных. Фиксируем множество $\mathcal{R} = \{R_1, \ldots, R_m\}$ различных функций граневого разбиения. Через $k(R_i)$, $i \in \{1, \ldots, m\}$, обозначим арность функции R_i. По определению положим $\Phi_{\mathcal{R}} = \Phi_{R_1} \cup \Phi_{R_2} \cup \ldots \cup \Phi_{R_m}$. Это класс функций, производящих разбиение n-мерного булева куба на не более чем $2^{\max_{i \in \{1,\ldots,m\}} k(R_i)}$ непересекающихся граней.

Фиксируем натуральные числа n, m и k. Рассмотрим множество $\mathcal{F}$ алгоритмов, решающих задачу расшифровки функций из $\Phi_{\mathcal{R}}$ для любого множества $\mathcal{R}$ функций граневого разбиения, такого что $|\mathcal{R}| \le m$ и $\max_{i \in \{1,\ldots,m\}} k(R_i) \le k$. На вход любого такого алгоритма подаются функции $R_1, \ldots, R_m$ множества $\mathcal{R}$ и оператор $\mathcal{A}_f$, где $f \in \Phi_{\mathcal{R}}$. Работа алгоритма $F \in \mathcal{F}$ заключается в том, что он последовательно запрашивает значения оператора $\mathcal{A}_f$ на наборах из B^n. При этом алгоритм F предполагается условным, т. е. при выборе очередного набора он может пользоваться знаниями о значениях функции на ранее поданных им наборах. Пусть $\varphi(F, \mathcal{R}, n, m, k, f)$ — число обращений к оператору $\mathcal{A}_f$ в процессе восстановления таблицы значений функции f с помощью алгоритма F. Обозначим $\varphi(n, m, k) = \min_{F \in \mathcal{F}} \max_{\mathcal{R}} \max_{f \in \Phi_{\mathcal{R}}} \varphi(F, \mathcal{R}, n, m, k, f)$ — сложность расшифровки самой плохой функции самым хорошим алгоритмом. Целью настоящей статьи является описание асимптотического поведения функции $\varphi(n, m, k)$ при $n \to \infty$. Очевидна тривиальная оценка $\varphi(n, m, k) \le 2^n$. Доказана следующая теорема:

Теорема. *Если $k, n \to \infty$ и $k \le cn$, где $c < 1$, $m = o(\log_2 n)$, то*

имеет место $\varphi(n,m,k) \sim k\log_2 n$.

Лемма 1 (нижняя оценка). *Для любых натуральных* n, m, k *имеет место* $\varphi(n,m,k) \geq (k-]\log_2 k[)]\log_2(n-k+1)[$.

Лемма 1 доказывается путем построения по произвольному алгоритму «плохой» функции граневого разбиения R и функции $f \in \Phi_R$, таких, что указанный алгоритм не сможет расшифровать f, запросив менее $(k-]\log_2 k[)]\log_2(n-k+1)[$ значений оператора $\mathcal{A}_f$.

Лемма 2 (верхняя оценка). *Существует алгоритм* $F \in \mathcal{F}$, *такой что для любых функций граневого разбиения* $\mathcal{R} = \{R_1, \ldots, R_m\}$, *таких что* $\max_{R\in\mathcal{R}} k(R) \leq k$, *и для любой функции* $f \in \Phi_{R_1} \cup \Phi_{R_2} \cup \ldots \cup \Phi_{R_m}$ *арности* n *имеет место неравенство* $\varphi(F,\mathcal{R},n,m,k,f) \leq k(]\log_2 n[+1) + 2m(k+1)$.

Доказательство леммы 2 конструктивно. Оно заключается в построении указанного в лемме алгоритма F.

Вернемся к задаче текстовой классификации. Пусть в корпусе документов имеется n слов. Каждому документу корпуса сопоставляется вектор длины n, i-я компонента которого равна 1, если i-е слово есть в документе, и 0 в противном случае. При таком задании документов n-мерный булев куб можно считать множеством документов, а каждую функцию $f \in \Phi_{\mathcal{R}}$ — некоторым классификатором, сопоставляющим каждому документу номер темы, в которой он лежит. Тем самым задача текстовой классификации сводится к задаче расшифровки некоторой функции $f \in \Phi_{\mathcal{R}}$, разбивающей n-мерный булев куб на грани. Появляется модель корпуса документов, в которой темы задаются формально конъюнкциями, а принадлежность документа теме есть ни что иное, как принадлежность сопоставленного документу вектора грани n-мерного куба, задаваемой этой конъюнкцией. Согласно сформулированной теореме упомянутый алгоритм классифицирует документы за асимптотически неулучшаемое время.

Настоящая работа выполнена на кафедре МАТИС механико-математического факультета МГУ им. М. В. Ломоносова под руководством д.ф.-м.н., профессора Э. Э. Гасанова.

Список литературы

1. Коробков В. К. О монотонных функциях алгебры логики // Проблемы кибернетики, вып.13. — М.: Наука, 1965.

2. Золотых Н. Ю. Расшифровка пороговых и близких к ним функций многозначной логики: Дисс. ... канд. физ.-мат. наук. — Нижний Новгород, 1998.

3. Кудрявцев В. Б., Гасанов Э. Э., Долотова О. А., Погосян Г. Р. Теория тестирования логических устройств. — М.: Физматлит, 2006.

4. Sebastiani F. Machine learning in automated text categorization // ACM Computing Surveys. — 2002. — V. 34, № 1. — P. 1–47.

ПРОБЛЕМА ВЫЧИСЛИТЕЛЬНОЙ ПОЛНОТЫ ОБЪЕКТНОГО ЯЗЫКА ЗАПРОСОВ ODQL ДИНАМИЧЕСКОЙ ИНФОРМАЦИОННОЙ МОДЕЛИ DIM

Д. С. Писаренко, В. С. Рублев, Д. В. Чехранов (Ярославль)

Известно, что SQL (стандарт SQL92) не является вычислительно полным языком: не всякий алгоритм можно реализовать его средствами. Одним из критериев вычислительной полноты является возможность реализовать средствами языка произвольную машину Тьюринга (МТ). В свою очередь для этого необходимо реализовать шаг произвольной МТ средствами языка и обеспечить повторение шагов до перехода МТ в состояние останова. Для реализации шага МТ достаточно ввести 4 таблицы: таблицу переходов МТ, ленту памяти в виде таблицы, таблицу текущего состояния МТ и промежуточную таблицу для сохранения данных.

Произвольный шаг МТ можно описать тремя SQL-операторами UPDATE:

1. Текущее состояние МТ сохраняется в промежуточную таблицу.

2. Обновляется текущее состояние и положение головки.

3. Обновляется символ на ленте, используя данные промежуточной таблицы.

Для работы МТ необходимо повторять этот шаг до тех пор, пока МТ не перейдет в состояние останова. Однако в SQL (стандарт SQL92) нет оператора, который бы выполнял последовательность SQL-операторов до тех пор, пока истинно некоторое условие. Вместо зацикливания с проверкой условия можно последовательно выполнять достаточно большое число шагов машины Тьюринга. Но при этом, какое бы большое число шагов мы не взяли, всегда найдется алгоритм, завершающийся за большее число шагов. Таким образом, выполняя шаги последовательно, без зацикливания, мы все равно не сможем реализовать машину Тьюринга средствами SQL.

Таким образом, для вычислительной полноты SQL не хватает оператора цикла.

Объектно-динамический язык запросов ODQL модели данных DIM [1–4] не является вычислительно полным по аналогичной причине, что и язык SQL, но можно таким же образом обосновать возможность реализации шага произвольной МТ.

Проблему вычислительной полноты ODQL можно разрешить одним из двух способов:

1. Дополнить ODQL конструкцией запроса, которая циклически повторяет произвольную последовательность запросов ODQL до выполнения некоторого условия (состояния останова).

2. Ввести расширение языка ODQL, которое позволило бы манипулировать объектами не только через операторы запросов, но и другими алгоритмическими конструкциями, дающими возможность реализовать алгоритмы взаимодействий объектов.

Для реализации первого способа введем 2 дополнительных конструкции в ODQL:

— <блок операторов ODQL>, которая представляет из себя последовательность операторов ODQL, разделенных фразой "THEN", начинающаяся фразой "BEGIN" и оканчивающаяся фразой "END".

— SELECT ... AFTERWHILE (<запрос>) <блок операторов ODQL>, где <запрос> — это обычный оператор SELECT. Эта конструкция в операторе SELECT выполняет <блок операторов ODQL>, пока условие в конструкции AFTERWHILE ложно, после чего выполняется SELECT.

Для реализации второго способа введем язык PL/ODQL, который работает с множествами объектов, классов и свойств объектов DIM, находящихся как в хранилище данных (через конструкции языка ODQL), так и в оперативной памяти (через конструкции расширения) и включает:

— Все конструкции языка ODQL.

— Типы скалярных переменных *string, integer, float, boolean* и *date* для организация работы со строковыми, числовыми, логическим данными и данными типа дата и время.

— Типы структурных переменных *object, class, property* для описания объектов, классов и свойств объектов и классов.

— Тип ***set*** для описания множеств скалярных и структурных переменных.

— Тип исключений *exception* для описания исключений.

— Операторы *присваивания, if, while* и *for* для организации ветвления и циклов алгоритмов.

— Оператор *foreach* для организации последовательного выбора элементов множеств.

— Операторы include, exclude для включения во множество и исключение из множества.

— Оператор *raise* для вызова исключений.

— Скалярные операции *арифметические, логические, строковые, временные.*

— Объектные операции *parent, ˜parent, inclusion, ˜inclusion, crossinclusion, frominteraction, tointeraction, whatinteraction, howinteraction, precursor, successor* для получения множеств объектов родительских, дочерних, включенных, включающих, включения, различных ролей взаимодействий, предшественников и последователей.

— Операция *properties* для выделения множества свойств объектов.

— Операции выделения объекта из множества.

— Операции над множествами переменных *and, or, not.*

— Описания блоков, процедур, функций и обработчиков исключений.

Список литературы

1. Рублев В. С., Юсупов А. Р. Концепции объектной динамической информационной модели DIM // Математика в Ярославском университете. Сборник обзорных статей к 30-летию математического факультета. — Ярославль: ЯрГУ, 2006. — С. 335–354.

2. Чехранов Д. В., Юсупов А. Р. Язык запросов DQL и проблема реализации компилятора из языка DQL в язык OQL // Современные проблемы математики и информатики. Сборник научных трудов молодых ученых, аспирантов и студентов. Вып. 6. — Ярославль: ЯрГУ, 2004. — С. 148–156.

3. Рублев В. С., Чехранов Д. В., Юсупов А. Р. Полнота объектно-динамического языка запросов динамической информационной модели DIM // Проблемы теоретической кибернетики. Тезисы докладов XIV Международной конференции (Пенза). — М.: МГУ, 2005. — С. 130.

4. Чехранов Д. В. Основные концепции объектно-динамического языка запросов ODQL динамической информационной модели DIM // Современные проблемы математики и информатики: Сборник научных трудов молодых ученых, аспирантов и студентов. Вып. 8. — Ярославль: ЯрГУ, 2006. — С. 143.

О ПОСТРОЕНИИ МИНИМАЛЬНЫХ ПО РАЗМЕРУ ДВУХЛЕНТОЧНЫХ АВТОМАТОВ

Р. И. Подловченко (Москва), В. Е. Хачатрян (Белгород)

Многоленточные автоматы были введены Рабиным и Скоттом в 1959 году как обобщение обычных конечных автоматов.

Их исследования установили принципиальное различие функциональных свойств конечных автоматов и введенного их обобщения:

— недетерминированные многоленточные автоматы являются более мощным средством вычислений, чем детерминированные их варианты;

— для недетерминированных многоленточных автоматов неразрешима проблема эквивалентности;

— для детерминированных многоленточных автоматов разрешима проблема эквивалентности, но неразрешима проблема включения.

Эти различия проявляются уже для двухленточных автоматов. Нами рассматривается множество двухленточных бинарных детерминированных автоматов, структурно близких к обычным конечным автоматам. Выявлено, что для таких автоматов, в общем случае, минимальный по размеру автомат в своем классе эквивалентности не является единственным. Возникла задача обобщенной минимизации, состоящая в поиске всех минимальных автоматов в классе эквивалентности, каким бы последний ни был. Работа посвящена построению процедуры, решающей эту задачу.

Обозначим M множество рассматриваемых автоматов. Алфавит, над которым строятся автоматы — это $\{0, 1\}$. Каждый автомат задается конечным ориентированным графом переходов, удовлетворяющим требованиям: в нем выделены три несовпадающие вершины-состояния *вход*, *выход* и *цикл*. Из каждого состояния, кроме выхода исходят две дуги, помеченные числами 0 и 1. Дуги, исходящие из вершины *цикл*, ведут в ту же вершину. Каждое состояние, за исключением состояний *выход* и *цикл*, помечено либо символом p, либо символом q, и называется p-состоянием или q-состоянием сответственно. Требуется также, чтобы дуга, исходящая из q-состояния и помеченная числом 1, непременно вела в бесконечный цикл. Основной результат дается теоремой 1.

Теорема 1. *Для множества M разрешима задача обобщенной минимизации.*

Ее доказательству предшествуют теоремы 2 и 3.

Теорема 2. *Существует система T эквивалентных преобразований, индуцируемая двумя аксиомами и одним правилом вывода, которая полна в M.*

Доказательство теоремы 2 проводится традиционным методом — построением канонического автомата в каждом классе эквивалентности из M, осуществляемым средствами системы T. Следствием теоремы 2 является разрешимость в M проблемы эквивалентности.

Теорема 3. *Проблема обобщенной минимизации в M сводится к одноименной проблеме в подмножестве $\overline{M}$ множества M, где $\overline{M}$*

состоит из всех таких автоматов из M, в которых имеются как p-состояния, так и q-состояния.

Построение минимальных автоматов в $\overline{M}$ базируется на следующем факте: произвольный класс эквивалентности K из множества $\overline{M}$ разбивается на подклассы, называемые *срезами* и обладающие тем свойством, что все автоматы из любого среза имеют одно и то же для данного среза число p-состояний. Стратегия построения минимальных автоматов в $\overline{M}$ состоит в следующем: отобрать все те срезы, в которых могут находиться минимальные в K автоматы (такие срезы именуются перспективными), доказать конечность их множества и предложить процедуру построения минимальных в них автоматов. Поскольку последних заведомо конечное множество, при выполнении замысла стратегии мы получим конечное множество автоматов, содержащее все минимальные в K автоматы, и этим будет решена проблема минимизации в $\overline{M}$. Реализация этой стратегии отталкивается от очевидного необходимого свойства перспективного среза: в нем должны быть тупиковые автоматы, т. е. не имющие различных эквивалентных состояний.

Свойством тупиковости обладает канонический автомат, который уже построен. К тому же содержащий его срез (он называется главным) характеризуется тем, что принадлежащие ему автоматы имеют минимальное число p-состояний. В связи с этим главный срез заведомо перспективен и исследуется в первую очередь. В результате описывается эффективная процедура построения всех автоматов, минимальных в главном срезе. Один из них выделяется как опорный при переходе от главногго среза к другим срезам. Учитывая размеры опорного автомата, вводится процедура построения по нему автомата, являющегося представителем среза, отличного от главного. Находится критерий того, когда получаемый срез является перспективным; критерий эффективно проверяем, и ему удовлетворяют срезы, составляющие конечное множество. Предлагается алгоритм построения минимальных автоматов в перспективном срезе. Таким образом, описанная выше стратегия полностью реализована, и теорема 1 доказана. Конкретными примерами автоматов подтверждается, что в общем случае канонический автомат не является минимальным в главном срезе, а минимальный в K автомат принадлежит срезу, отличному от главного. Полученный нами результат не имеет аналогов в литературе по многоленточным автоматам.

Работа выполнена при поддержке гранта РФФИ 06-01-00106.

Список литературы

1. Rabin M. O., Scott D. Finite automata and their decision problems // IBM Journal of R&D. — 1959. — V. 3, № 2. — P. 114–125.

2. Griffits T. V. The unsolvability of the equivalence problem for λ-

free nondeterministic generalized machines // Journal of the ACM. — 1968. — V. 15. — P. 409–413.

3. Bird M. The equivalence problem for deterministic two-tape automata // Journal of Computer System Science. — 1973. — V. 7, № 4. — P. 218–236.

4. Harju T., Karhumaki J. The equivalence problem of multitape finite automata // Theoretical Computer Science. — 1991. — v. 78, № 2. — P. 347–355.

5. Lukham D. C., Park D. M., Paterson M. S. On formalized computer programs // Journal of Computer System Science. — 1970. — V.4, № 3. — P. 220–249.

6. Хачатрян В. Е. Решение обобщенной проблемы минимизации конечных автоматов с одной фиксированной лентой // Доклады РАН. — 2006. — Т. 411, № 3. — С. 1–5.

7. Tamm H. On minimality and size reduction of one-tape and multitape finite automata. — University of Helsinki, 2004.

8. Подловченко Р. И. К вопросу об эквивалентных преобразованиях алгоритмов и программ // Математические вопросы кибернетики, вып. 9. — М.: Физматлит, 2000. — С. 25–36.

ПОСЛОЙНЫЙ АЛГОРИТМ ЦЕЛОЧИСЛЕННОГО СБАЛАНСИРОВАНИЯ ТРЕХМЕРНОЙ МАТРИЦЫ

В. С. Рублев, А. В. Смирнов (Ярославль)

В [1] рассмотрена задача сбалансирования 3-мерной матрицы.

Дана 3-мерная вещественная матрица A с неотрицательными элементами a_{ijp} ($i \in \overline{0,n}$, $j \in \overline{0,m}$, $p \in \overline{0,t}$), для которой выполнены условия баланса:

каждый элемент с некоторыми нулевыми индексами равен сумме всех элементов, для которых ненулевые индексы оставлены неизменными, а нулевые индексы заменены на все возможные ненулевые значения диапазонов соответствующих индексов.

Требуется так округлить элементы матрицы до целого значения сверху или снизу (элемент a_{000} округляется до ближайшего целого), чтобы остались выполнены условия баланса.

С целью решения поставленной задачи в [1] введено обобщение теории потоков Форда — Фалкерсона, названное кратными потоками и задачей о нахождении максимального кратного потока. Для

последней задачи разработан алгоритм «черных и красных пометок» ее решения. Показано, что задача о сбалансировании 3-мерной матрицы индуцирует задачу о наибольшем кратном потоке так, что решение первой является решением второй задачи. Однако нет полной сводимости первой задачи ко второй, так как решению задачи о максимальном кратном потоке может соответствовать такое целочисленное сбалансированное округление матрицы A, у которого некоторые элементы выходят за диапазон ближайших целых.

Предлагается новый алгоритм решения задачи о максимальном кратном потоке, который приводит к решению задачи о сбалансировании 3-мерной матрицы.

Идеи алгоритма основаны на выделении из кратной сети задачи кратных подсетей, названных слоями сети, которые соответствуют сечениям матрицы с элементами a_{ijp}, где $i = 0$ или $i = k$ для фиксированного значения $k \in \overline{1,n}$ (значение k определяет номер слоя).

На каждом шаге алгоритма рассматривается очередной k-й слой и для его подсети сначала *направленным* алгоритмом получается полный кратный поток (определение см. в [1]), а затем если этот поток не максимальный, то применяется алгоритм «черных и красных пометок» для увеличения потока (но при этом запрещается уменьшение уже полученного потока для предыдущих слоев) .

Основная идея состоит в применении направленного алгоритма получения полного кратного потока, который отвечает условию целочисленного округления при построении целочисленной сбалансированной матрицы. Для этого в кратной сети выделяются следующие множества дуг:

1) P_1 — состоит из дуг сети (X_{i00}, X'_{i00}) $(i \in \overline{1,n})$;

2) P_2 — состоит из дуг сети (X'_{0j0}, X_{0j0}) $(j \in \overline{1,m})$;

3) P_3 — состоит из дуг сети (X'_{00t}, X_{00t}) $(t \in \overline{1,p})$.

Тогда направленный алгоритм получения полного потока в k-м слое формулируется следующим образом:

— На множестве дуг $P_1 \cup P_2 \cup P_3$ временно считаем для этого шага нулевой пропускную способность и увеличиваем поток, пока это возможно.

— Предыдущий шаг повторяем для следующих множеств дуг и в этом порядке $P_2 \cup P_3$, $P_1 \cup P_2$, $P_1 \cup P_3$, P_3, P_1, P_2.

— Увеличиваем поток, пока это возможно, без ограничений пропускной способности на множествах дуг.

Для указанного алгоритма справедливы следующие утверждения.

Теорема 1. *Величина максимального потока в k-м слое равна*

$$c(X_{000}, X_{k00}) + min\{c(X_{000}, X'_{000}), c(X'_{000}, X_{k00})\},$$

где $c(A,B)$ *— пропускная способность дуги* (A,B).

Теорема 2. *Величина максимального кратного потока в кратной сети задачи целочисленного сбалансирования* 3*-мерной матрицы равна* $2[a_{000}+0.5]$. *Этот поток может быть найден послойным алгоритмом.*

Гипотеза. Если задача целочисленного сбалансирования 3-мерной матрицы имеет решение, то оно может быть получено решением задачи о максимальном кратном потоке при помощи послойного алгоритма.

Список литературы

1. Рублев В. С., Смирнов А. В. Целочисленное сбалансирование 3-мерной матрицы плана // Труды VII международной конференции «Дискретные модели в теории управляющих систем» (Покровское, 4–6 марта 2006 г.). — Москва: МГУ, 2006. — С. 302–308.

О ПРЕДСКАЗУЕМОСТИ ПОВЕДЕНИЯ ОДНОРОДНЫХ АВТОМАТНЫХ СЕТЕЙ

И. Ю. Самоненко (Москва)

Пусть $\mathfrak{A}=(A,Q,\varphi)$ — конечный автомат с входным алфавитом A, множеством состояний Q и функцией перехода $\varphi: Q\times A\to Q$. Автомат $\mathfrak{A}$ называется *r-предсказуемым*, если существует функция $f: Q^{r+1}\to Q$ и состояния $q_1,\ldots,q_r\in Q$, такие что для любого слова $\alpha\in A^*$ и любого состояния $q\in Q$, верно

$$\varphi(q,\alpha)=f(q,\varphi(q_1,\alpha),\ldots,\varphi(q_r,\alpha))$$

Состояния $q_1,\ldots,q_r$ называются *базисными*,а функция f называется *предсказывающей функцией*. Другими словами, автомат называется r-предсказуемым, если у него найдутся r состояний $q_1,\ldots,q_r\in Q$, таких что, зная только то, куда они перейдут по некоторому слову $\alpha\in A^*$, мы сможем определить (при помощи функции f), куда перейдет произвольное состояние $q\in Q$ по слову α.

Через $PR(n,r)$ обозначим класс всех r-предсказуемых автоматов с n состояниями.

Слово $\alpha\in A^*$ называется *синхронизирующим* для автомата $\mathfrak{A}=(A,Q,\varphi)$, если существует такое состояние $q_f\in Q$, что для любого состояния $q\in Q$ верно $\varphi(q.\alpha)=q_f$. Автомат называется *синхронизируемым*, если для него существует синхронизующее слово. Пусть

$\mathfrak{A} = (A, Q, \varphi)$ произвольный синхронизируемый автомат с n состояниями. Гипотеза Черни [1] утверждает, что длина минимального синхронизующего слова для $\mathfrak{A}$ не превышает $(n-1)^2$. Эта проблема до сих пор открыта. Наилучшая известная на сегодняшний день верхняя оценка длины минимального синхронизующего слова [2] равна $(n^3 - n)/6$.

Теорема 1. *Пусть автомат* $\mathfrak{A} = (A, Q, \varphi) \in Pr(n, r)$ *является синхронизуемым, тогда длина минимального синхронизующего слова не превосходит* $n + (r(r-1)(r-2))/6$.

Пусть $G = (V, E, \rho)$ — конечный ориентированный граф со множеством вершин V, множеством ребер E и функцией $\rho : E \to V \times V$, сопоставляющей каждому ребру пару вершин (соответственно начальную и конечную). Через $Out(v)$ обозначим множество ребер выходящих из вершины v, т. е. $Out(v) = \{e \in E | \exists v' \in V : \rho(v, v') = e\}$. Через $O_v = |Out(v)|$ обозначим число вершин, выходящих из вершины v.

Пусть Q — произвольное конечное множество. Для графа $G = (V, E, \rho)$ рассмотрим функцию разметки ребер λ_E и функцию разметки вершин λ_V. Для каждой вершины $v \in V$, функция λ_E нумерует множество $Out(v)$ начальным отрезком натурального ряда $\{1, \ldots, O_v\}$, а функция λ_V сопоставляет вершине v некоторую функцию $\lambda_E(v) : Q^{O_v} \to Q$.

Автономной автоматной сетью называется четверка $\mathfrak{R} = (Q, G, \lambda_E, \lambda_V)$, где Q — конечное множество состояний ячеек, $G = (V, E, \rho)$ — конечный ориентированный граф, λ_E — функция разметки ребер графа G, λ_V — функция разметки вершин графа G.

Множество всех автономных автоматных сетей, со множеством состояний ячеек Q и множеством вершин графа V обозначим через $ANet(Q, V)$.

Пусть $V = \{1, \ldots, n\}$ — множество вершин графа G. Через $\lambda(i, j)$ обозначим ту вершину, в которую идет ребро с меткой j из вершины i. С каждой автономной автоматной сетью $\mathfrak{R} = (Q, G, \lambda_E, \lambda_V)$ можно связать отображение $\Phi : Q^n \to Q^n$ следующим образом:

$$\Phi_{\mathfrak{R}}(q_1, \ldots, q_r) = (f_1(q_{\lambda(1,1)}, \ldots, q_{\lambda(1,O_1)}), \ldots, f_n(q_{\lambda(n,1)}, \ldots, q_{\lambda(n,O_n)})),$$

где $f_i = \lambda_V(i)$, $i = 1, \ldots, n$.

Автоматной сетью называется четверка $\mathfrak{N} = (A, Q, V, \eta)$, где A — конечный входной алфавит, Q — конечно множество состояний ячеек, V — множество вершин графа, $\eta : A \to ANet(Q, V)$ —

функция, сопоставляющая каждому входному символу некоторую автономную автоматную сеть.

С каждой автоматной сетью сетью $\mathfrak{N} = (A, Q, V, \eta)$ можно связать автомат $\mathfrak{A} = A(\mathfrak{N}) = (A, Q^n, \Phi)$, где $n = |V|$ и функция переходов Φ устроена следующим образом:

$$\Phi(a, (q_1, \ldots, q_n)) = \Phi_{\eta(a)}(q_1, \ldots, q_n)$$

Зафиксируем натуральные числа $d_1, \ldots, d_k \in \mathbb{N}$, в качестве множества вершин рассмотрим k-мерный целочисленный параллелограмм со сторонами $d_1, \ldots, d_k$, т.е. $V = E_{d_1} \times \cdots \times E_{d_k}$. Построим граф G следующим образом. Рассмотрим произвольный набор векторов $\overline{u}_1, \ldots, \overline{u}_s \in \mathbb{Z}^k$. Из каждой вершины $\overline{v} = (l_1, \ldots, l_k) \in V$ выпустим s ребер в вершины вершины $(\overline{v} + \overline{u}_1) \ mod \ (d_1, \ldots, d_k), \ldots, (\overline{v} + \overline{u}_1) \ mod \ (d_1, \ldots, d_k)$, где $(a_1, \ldots, a_k) \ mod \ (d_1, \ldots, d_k) = (a_1 \ mod \ d_1, \ldots, a_k \ mod \ d_k)$. Полученный граф обозначим через $G = G(V; \overline{u}_1, \ldots, \overline{u}_k)$ и назовем *однородным графом.*

Построим функцию разметки ребер λ_E следующим образом: если ребро $e \in E$ идет из вершины $\overline{v}$ в вершину $(\overline{v} + \overline{u}_i) \ mod \ (d_1, \ldots, d_k)$, то $\lambda_E(e) = i$.

Рассмотрим произвольную функцию $\varphi : Q^s \to Q$, и определим функцию разметки вершин $\lambda_V(v) = \varphi$.

Автономную автоматную сеть имеющую вид $\mathfrak{R} = (Q, G(E_{d_1} \times \cdots \times E_{d_k}; \overline{u}_1, \ldots, \overline{u}_s), \lambda_E, \lambda_V)$, где λ_E и λ_V определены выше, назовем *автономной однородной автоматной сетью.*

Через $HANet(Q; d_1, \ldots, d_k)$ обозначим множество всех автономных однородных автоматные сетей со множеством состояний ячеек Q и множеством вершин $E_{d_1} \times \cdots \times E_{d_k}$.

Однородной автоматной сетью размера $d_1 \times \cdots \times d_k$ называет автоматная сеть $\mathfrak{N} = (A, Q, V, \eta)$, где $\eta : A \to HANet(Q; d_1, \ldots, d_k)$.

Теорема 2. *Пусть $\mathfrak{N} = (A, Q, V, \eta)$ произвольная однородная автоматная сеть размера $d_1 \times \cdots \times d_k$, тогда автомат $A(\mathfrak{N}) \in PR(n, r(n))$, где $n = |Q|^{d_1 \ldots d_k}$ и $r(n) \lesssim \frac{n}{\log_{|Q|}(n)}$ при $d_1, \ldots, d_k \to \infty$.*

Автор выражает глубокую благодарность своему научному руководителю профессору Бабину Дмитрию Николаевичу за помощь в решении задачи.

Список литературы

1. Cerny J. Poznamka k homogennym eksperimentom s konechnymi automatami // Matematicko-Fyzikalny Casopis Slovensk. Akad. Vied. — 1964. — V. 14. — P. 208–216. 14

2. Клячко А. А., Рысцов И. К., Спивак М. А. Об одной экстремальной комбинаторной задаче, связанной с оценкой длины возвратного слова в автомате // Кибернетика. — 1987. — Т. 2.

ДИСКРЕТНЫЕ МОДЕЛИ ЯЗЫКОВОЙ ЭВОЛЮЦИИ

В. Д. Соловьев (Казань)

С конца XIX века стандартным является представление языковой эволюции деревом дивергенции языков. Реконструкция эволюционного дерева и протоязыков является одной из основных задач исторической лингвистики и представляет общенаучный интерес. Эта задача имеет много общего с задачей реконструкции дерева эволюции живых организмов, для решения которой разработаны разнообразные математические методы и алгоритмы в биоинформатике. В последние годы эволюционная лингвистика заимствует в биоинформатике широкий круг идей. Вся эта область известна как филогенетика. В докладе дается краткий обзор основных подходов в лингвистической филогенетике, а также излагаются некоторые последние результаты, полученные в этом направлении в Казанской школе математической лингвистики

Каждый из существующих языков представляется 1-мерным вектором значений признаков. Требуется построить дерево, листьями которого являются рассматриваемые языки и которое правдоподобно восстанавливает ход эволюции.

Первой проблемой является описание языков в виде векторов значений признаков. В биоинформатике им соответствуют активно расшифровываемые в последние годы геномы. К сожалению, представительных баз данных описаний языков очень мало. Принципиально новые возможности исследований в этом направлении открылись после появления в 2006 г. базы данных “Языки мира” (www.dblang.ru, [1]), созданной в ИЯ РАН и являющейся беспрецедентной по полноте описания языков (315 языков описано по 3821 параметру).

Следующая проблема — алгоритмы реконструкции деревьев. Основные, разработанные в биоинформатике и входящие в стандартный пакет PAUP* алгоритмы, — UPGMA, NJ, MP. Первые два из них являются вариантами алгоритмов кластерного анализа и основаны на идее близости: чем меньше расстояние между объектами по метрике Хемминга, тем они ближе в генетическом плане.

Третий алгоритм основан на иной идее. Он восстанавливает не только дерево, но и значения параметров для промежуточных вершин — предков. При этом, исходя из принципа "Бритва Оккама", требуется восстановить все промежуточные значения таким образом, чтобы в итоге оказалось минимальное число мутаций (изменений значений признаков на ребрах). К сожалению, эта задача оказалась NP-полна [2], так что приходится использовать приближенные алгоритмы.

Первые применения указанных алгоритмов в лингвистической филогенетике дали неоднозначные и, в целом, неудовлетворительные результаты. Вероятной причиной этого является более сложный характер языковой эволюции по сравнению с биологической за счет влияния различных социальных факторов, в первую очередь, широких заимствований между языками (соответствующий этому прямой перенос генов не встречается, по крайней мере, у сложных организмов). Поэтому актуальной является задача усовершенствования алгоритмов.

Нами предложено использовать развитый в кластерном анализе подход, связанный с применением λ-метрики [3]; λ-метрика рассчитывается по формуле $\lambda = \tau^2 d$, где d — нормированное расстояние, а τ характеризует локальную неоднородность плотности множества объектов [3]. Также разработаны новые алгоритмы (обсуждаются в докладе Э. Ю. Лернера на данном семинаре).

В настоящее время в Казанском государственном университете совместно с Институтом эволюционной антропологии им. Макса Планка (Лейпциг) проводятся исследования по тестированию различных алгоритмов на различных группах языков и различных базах данных. На выборке (из созданной в Германии базы данных WALS) из 6 пар языков индейцев Америки, принадлежащих к 6 разным семьям, наилучший результат дает алгоритм UPGMA с применением λ-метрики, правильно классифицирующий все языки. На выборке (из базы данных "Языки мира") из 6 пар языков разных семей Евроазиатского континента одинаковый результат дали три алгоритма: UPGMA, UPGMA с применением λ-метрики и NJ с применением λ-метрики, однако, они правильно классифицирует лишь 4 пары языков. Это указывает на значительно большую сложность эволюционных (в том числе миграционных) процессов на Евроазиатском континенте.

Проведены исследования зависимости качества кластеризации тестовых наборов языков от числа учитываемых признаков и от вида формулы при подсчете λ-расстояний. Лучшие результаты получены для указанной выше формулы и при максимальном числе признаков. Однако использование большого числа признаков замед-

ляет работу алгоритмов. Поэтому остается задача выделения наиболее информативных признаков, что позволит использовать более точные алгоритмы, требующие больших вычислительных ресурсов.

Хотя описываемый метод филогенетической реконструкции находится в начальной стадии разработки, уже сейчас он позволяет получать значимые лингвистические результаты. В частности, получены новые данные о принадлежности чукотско-камчатской семьи к бореальной макросемье. Перспективным направлением исследований является построение не древовидной, а сетевой модели эволюции языков, учитывающей заимствования [4]. В любом случае, данная область является серьезным вызовом алгоритмике, так как возникающие здесь вычислительные задачи крайне сложны и сохраняется потребность в быстрых и точных приближенных алгоритмах.

Работа выполнена при поддержке РФФИ, грант № 07-06-00229а.

Список литературы

1. Поляков В. Н., Соловьев В. Д., Компьютерные модели и методы в типологии и компаративистике. — Казань: КГУ, 2006.

2. Гасфилд Д. Строки, деревья и последовательности в алгоритмах. Информатика и вычислительная биология. — СПб.: Невский диалект, 2003.

3. Загоруйко Н. Г. Прикладные методы анализа данных и знаний. — Новосибирск: ИМ СО РАН, 1999.

4. Warnow T. Mathematical approaches to comparative linguistics // Proc. Nat. Acad. Sci. — 1997. — V. 94. — P. 6585–6590.

О МАРКОВСКИХ РЕГУЛЯРНЫХ ЯЗЫКАХ

А. Б. Холоденко (Москва)

Введём вначале несколько необходимых определений и обозначений.

Пусть $\mathfrak{A} = (A, Q, \varphi, Q_F, q_0)$ — конечный детерминированный автомат, где A — входной алфавит, Q — множество состояний, $Q_F \subseteq Q$ — множество финальных состояний, φ — функция переходов, q_0 — начальное состояние автомата.

$L_{\mathfrak{A}} = \{\alpha \in A^* | \varphi(q_0, \alpha) \in Q_F\}$ — язык, порождаемый автоматом $\mathfrak{A}$. Всюду далее будут рассматриваться только регулярные языки. При этом для краткости мы будем иногда опускать символ автомата.

Для $s \in \mathbb{N}$ обозначим через $L(s)$ множество слов языка L длины s. Через PL обозначим множество префиксов слов языка L, включая

сами слова: $PL = \{\alpha \in A^* | \exists \beta \in A^*, \alpha\beta \in L\}$ (мы считаем, что A^* содержит пустую букву Λ). Очевидно, $L \subseteq PL$.

Через L_γ обозначим множество слов языка L, оканчивающихся на слово $\gamma \in A^*$: $L_\gamma = \{\alpha \in A^* \in L | \exists \beta \in A^*, \alpha = \beta\gamma\}$.

В принятых обозначениях $PL_w(s)$ обозначает множество префиксов языка L, оканчивающихся на слово w и имеющих длину s. Через $l(s)$ обозначим мощность множества $PL_w(s)$: $l(s) = |PL_w(s)|$.

Введём $G_w(s)$ — частоту встречаемости слова w на s-ом месте как

$$G_w(s) = \frac{l_w(s)}{\sum\limits_{|w'|=|w|} l_{w'}(s)}$$

и $G_w = \lim\limits_{s\to\infty} G_w(s)$ — предельную частоту встречаемости слова w среди слов той же длины.

Для слова w и буквы a, $|wa| = n$ введём величину $\Gamma_{w,a}(s)$ как

$$\Gamma_{w,a}(s) = \frac{l_{wa}(s)}{\sum\limits_{|w'|=|w|} l_{w'a}(s)}.$$

Определение. *Символ* $\Gamma_{w,a} = \lim\limits_{s\to\infty} \Gamma_{w,a}(s)$, *если указанный предел существует, назовём* n*-граммой языка* L.

Символ $\Gamma_{w,a}$ в нашей модели имеет смысл частоты встречаемости буквы a после предыстории фиксированной длины. В случае $n = 1$ символ $\Gamma_{\Lambda,a} = G_a$ называется *униграммой* языка L, в случае $n = 2$ символ $\Gamma_{b,a}$ называется *биграммой* языка L.

Определение. *Язык* L *называется марковским порядка* n, *если* $\forall w \in A^*\ \forall a \in A$, $|wa| = n$ *существуют все* n*-граммы* $\Gamma_{w,a}$ *и все* G_{wa}.

Множество таких языков обозначим через $M(n)$. Через M обозначим класс марковских языков (то есть языков, являющихся марковскими при всех порядках n).

Утверждение. *Всякий сильносвязный автомат* A *порождает марковский язык.*

Таким образом, марковские языки существуют и их доля среди всех регулярных языков отлична от нуля. Тем не менее, не все языки являются марковскими. Следующие три теоремы показывают связь между классами $M(n_1)$ и $M(n_2)$ для различных значений n_1 и n_2:

Теорема 1. *Если* $L \in M(n)$, *то* $\forall k, k < n$ $L \in M(k)$.

Теорема 2. $\forall n \in \mathbb{N}$ *существует язык* L *такой, что* $L \in M(n-1)$, *но при этом* $L \notin M(n)$.

Таким образом,

$$M(1) \subsetneq M(2) \subsetneq \ldots \subsetneq M(n-1) \subsetneq M(n) \subsetneq \ldots.$$

Теорема 3. $\forall L$ *существует* $n_0 \in \mathbb{N}$ *такой, что* $\forall n > n_0$ *из* $L \in M(n_0)$ *следует* $L \in M(n)$.

Замечание. Если язык $L_{\mathfrak{A}}$ задан диаграммой переходов своего автомата $\mathfrak{A}$, то существует формальная процедура, позволяющая вычислить любой символ $\Gamma_{w,a}$ либо доказать, что он не существует.

К сожалению, класс марковских языков оказывается не замкнутым относительно теоретико-множественных операций.

Утверждение. *Справедливы следующие соотношения*:

1. *Существуют* $L_1 \in M$ *и* $L_2 \in M$ *такие, что* $L_1 \cup L_2 \notin M$.
2. *Существуют* $L_1 \in M$ *и* $L_2 \in M$ *такие, что* $L_1 \cap L_2 \notin M$.
3. *Существует* $L \in M$ *такой, что* $(A^* \setminus L) \notin M$.

Утверждение. *Класс дефинитных языков является замкнутым относительно операций объединения, пересечения, дополнения, итерации, но не является замкнутым относительно операции конкатенации; кроме того, этот класс является марковским.*

Определение. *Замыкание класса дефинитных языков относительно операций объединения, пересечения, дополнения, итерации и конкатенации назовём классом расширенных дефинитных языков.*

Пусть $\mathfrak{A}^1 = (A, Q^1, \varphi^1, Q^1_F, q^1_0)$, $\mathfrak{A}^2 = (A, Q^2, \varphi^2, Q^2_F, q^2_0)$. Пусть также $q^1 \in Q^1$ и $q^2 \in Q^2$. Введём операцию склейки двух автоматов по паре состояний (q^1, q^2).

Результатом склейки автоматов $\mathfrak{A}^1$ и $\mathfrak{A}^2$ называется автомат

$$\mathfrak{A} = (A, Q^1 \cup Q^2 \setminus \{q^1\}, \varphi, Q^1_F \cup Q^2_F \setminus \{q^1\}, q^1_0), \text{ где}$$

$$\varphi(q,a) = \begin{cases} \varphi^1(q,a), & \text{если } q \in Q^1 \setminus \{q^1\} \text{ и } \varphi^1(q,a) \neq q^1; \\ q^2, & \text{если } q \in Q^1 \setminus \{q^1\} \text{ и } \varphi^1(q,a) = q^1; \\ \varphi^1(q^2,a), & \text{если } q = q^1; \\ \varphi^2(q,a), & \text{если } q \in Q^2. \end{cases}$$

Введём теперь класс каскадно-дефинитных языков. Во-первых, дефинитные языки являются каскадно-дефинитными. Во-вторых, результат склейки каскадно-дефинитного языка с дефинитным снова является дефинитным.

Теорема 4. *Класс каскадно-дефинитных языков совпадает с классом расширенных дефинитных языков.*

Теорема 5. *Пусть* $\{\Gamma_{w,a}\}$ — *множество n-грамм некоторого регулярного языка* $L_{\mathfrak{A}}$, *задаваемого автоматом* $\mathfrak{A}$. *Тогда* $\forall \varepsilon \in \mathbb{R}, \varepsilon > 0$ *можно построить каскадно-дефинитный автомат* $\mathfrak{B}$, *задающий язык* $L_{\mathfrak{B}}$, *множество n-грамм которого* $\{\tilde{\Gamma}_{w,a}\}$ *обладает тем свойством, что* $\forall w \in A^* \ \forall a \in A$, $|wa| = n$ *выполнено* $|\Gamma_{w,a} - \tilde{\Gamma}_{w,a}| < \varepsilon$.

Таким образом, каскадно-дефинитные марковские языки образуют в указанном смысле всюду плотное множество в классе всех марковских языков.

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

2. Ахо А., Ульман Д. Теория синтаксического анализа, перевода и компиляции. — М.: Мир, 1978.

3. Холоденко А. Б. О построении статистических языковых моделей для систем распознавания русской речи // Интеллектуальные системы. — 2002. — Т. 6, вып. 1–4. — С. 381–394.

Секция «Дискретная геометрия»

О СКЛАДЫВАНИЯХ БУМАГИ, ПЕРЕВОДЯЩИХ ОДНО ЗАДАННОЕ МНОЖЕСТВО ТОЧЕК В ДРУГОЕ

А. В. Акопян, А. С. Тарасов (Москва)

Оригами — кусочно-линейная, непрерывная и сохраняющая внутреннюю метрику гомотопия в $\mathbb{E}^3$, переводящая первоначальный плоский лист бумаги в некоторую многогранную поверхность с краем. В случае, если конечный результат находится в плоскости, такая гомотопия называется *плоским оригами*. Кроме этого обычно на оригами накладываются дополнительные условия, например, кусочной изометричности (жесткости) или отсутствия самопересечений, в естественном для бумаги смысле.

Данная статья посвящена тесно связанному с оригами понятию PL-изометрии.

Определение. *PL-изометрией*, заданной на политопе Γ (лежащем в пространстве $\mathbb{E}^d$, $\mathbb{H}^d$ или $\mathbb{S}^d$), называется непрерывное отображение Γ в объемлющее пространство такое, что для него существует локально конечное разбиение на политопы (далее называемые *листами*), и на каждом политопе этого разбиения PL-изометрия действует как движение.

Каждое оригами является двумерной PL-изометрией. Обратное, вообще говоря, не верно, так как для PL-изометрии не запрещаются самопересечения. Кроме того, нас интересует только конечный результат отображения. Нами была доказана следующая

Теорема (о продолжении). *Пусть на конечном множестве точек в пространстве $\mathbb{E}^d$, $\mathbb{H}^d$ или $\mathbb{S}^d$ задано нерастягивающее отображение φ. Тогда это нерастягивающее отображение можно продолжить до PL-изометрии на все пространство.*

Доказательство этой теоремы конструктивное и чисто геометрическое. Эта теорема, в частности, дает ответ на вопрос, поставленный в [1], о поиске конструктивного доказательства знаменитой теоремы Киршбаума.

Отметим, что из теоремы о продолжении можно получить простые доказательства следующих известных фактов.

Следствие 1. *Любое нерастягивающее (короткое) отображение φ из компакта $\mathcal{K}$ во всеобъемлющее пространство* ($\mathbb{E}^d$, $\mathbb{H}^d$ *или*

$\mathbb{S}^d$) *можно приблизить PL-изометрией.*

Действительно, покроем компакт $\mathcal{K}$ ε-сетью и построим PL-изометрию, переводящую точки в их образы при отображении φ.

Следствие 2 [2]. *Пусть P^2 — конечный двумерный полиэдр. Тогда любое нерастягивающее (короткое) отображение $\varphi : P^2 \to \mathbb{E}^2$, можно приблизить PL-изометрией.*

Авторы этой теоремы называют её кусочно-линейным аналогом теоремы Нэша — Кейпера. С помощью теоремы о PL-продолжении можно получить её простое доказательство.

Следствие 3 [3, 4]. *Пусть на листе бумаги нарисовано несколько многоугольников. Тогда лист можно сложить так, что эти многоугольники можно вырезать одним разрезом ножниц.*

С помощью теоремы о продолжении легко получить аналогичную PL-изометрию. Для этого достаточно "натянуто" отобразить периметры многоугольников на заданную прямую и продолжить это отображение до PL-изометрии.

Данная работа была выполнена при поддержке РФФИ, грант № 06-01-00648

Список литературы

1. Данцер Л., Грюнбаум Б., Кли В. Теорема Хелли и её применения. — М.: Мир, 1968.

2. Krat S., Burago D., Petrunin A. Approximatings short maps by *pl*-isometies and Arnold's "Can You Make Your Dollar Biegger" problem // Spring Topology and Dynamics Conference. — 2000.

3. Demaine E. D., Demaine M. L., Lubiv A. Folding and cutting paper // Revised papers from Japan Conference on Discrete and Comptutional Geometry. (Tokyo, December 1998.). — Lecture Notes in Computer Science. — 1998. — V. 1763. — P. 104–117.

4. Demaine E. D., Demaine M. L., Lubiv A. Folding and one straight cut suffice // Proceedings of the 10th Annual ACM-SIAM Symposium on Discrete Algorithms. (Baltimore, January 1999.). — P. 891–892.

О РЕШЕТКАХ E_6, E_7 И E_8

Р. Г. Барыкинский (Москва)

В данной работе получен следующий результат:

Теорема. *Каждая точечная решетка, соответствующая плотнейшей решетчатой упаковке равных шаров в размерностях*

11 *и* 12, *не содержит в качестве своей полной подрешетки* (*с таким же арифметическим минимумом*) *решетку* E_8.

Так же в этой работе получены символы для решеток E_6, E_7 и E_8, которые опираются на символ Рышкова для 2-й совершенной формы.

О ЦЕНТРАЛЬНО-СИММЕТРИЧНЫХ МНОГОГРАННИКАХ С МИНИМАЛЬНЫМ ЧИСЛОМ ГРАНЕЙ

К. Е. Бауман (Москва)

Настоящая работа посвящена изучению вопроса о структуре центрально-симметричного выпуклого d-мерного многогранника. Существует гипотеза о том, что количество граней всех размерностей в таком многограннике не менее 3^d. Предполагается, что сам многогранник дает вклад 1, как несобственная d-мерная грань. Согласно этой гипотезе такой центрально-симметричный выпуклый многогранник как куб или дуальный ему многомерный аналог октаэдра (кросс-политоп) являются простейшими, т. е. для них количество граней в точности равно 3^d. Следовательно, у любого центрально-симметричного многогранника число граней не меньше, чем у куба той же размерности.

Существует гипотеза (Д. Калаи, подробнее см., например, [1]), что множество центрально-симметричных многогранников с наименьшим количеством граней есть совокупность кубов и всех многогранников, получающихся из них с помощью операции взятия дуального многогранника и с помощью операции прямого произведения. Ответ на нее неизвестен. Поэтому Н. П. Долбилин предложил исследовать класс многогранников с общим числом граней $\sum_{i=0}^{d} f_i = 3^d$. Такие многогранники мы называем критическими. Рассмотрение этого вопроса стало особенно актуально в связи с тем, что структуры разбиения евклидова пространства на параллелоэдры [2] очень близки к понятию критических многогранников.

В данной работе изучается связь этих понятий. Также показано, что критические многогранники могут быть получены из многомерных кубов с помощью операции взятия дуального многогранника и операции прямого произведения.

Множество критических многогранников всех размерностей обозначим через K.

Определение. Обозначим через K' минимальное множество всех выпуклых центрально-симметричных многогранников любой размерности, удовлетворяющих условиям: 1) содержит отрезок; 2) если $P \in K'$, то $P^* \in K'$; 3) если $P \in K'$ и $Q \in K'$, то $P \times Q \in K'$.

Заметим что кубы всех размерностей и дуальные им, кросс-политопы, а также их всевозможные прямые произведения принадлежат множеству K'.

Теорема 1. $K' \subset K$.

Перейдем к определению свойств антиподальности.

Определение. Скажем, что d-мерный центрально-симметричный выпуклый многогранник P обладает свойством *f-антиподальности,* если для любой его $(d-1)$-мерной грани P' найдется единственная грань P'' такая, что $P' \bigcap P'' = \emptyset$ и грань P'' центрально-симметрична P'.

Определение. Скажем, что d-мерный центрально-симметричный выпуклый многогранник P обладает свойством *v-антиподальности,* если для любых его вершин A' и A'' не являющихся центрально-симметричными, найдется гипергрань F^{d-1} такая, что A' и $A'' \in F^{d-1}$.

Таким образом, в P нет гиперграней свободных от двух противоположных вершин одновременно.

Определение. Множество всех выпуклых центрально-симметричных многогранников со свойством f-антиподальности (v-антиподальности) обозначим через A_f (A_v).

Теорема 2. *Классы A_f и A_v совпадают.*

Теорема 3. $K' \subset A_f$.

Лемма 1. *Если многогранники A и B критические, то $P = A \times B$ тоже критический.*

Лемма 2. *Если многогранник A критический, то A^* тоже критический.*

Доказательство теоремы 1 стороится на обосновании сохранения свойства критичности при индуктивном переходе при построении многогранников из K' и основывается на леммах 1 и 2.

Лемма 3. *Пусть $P \in A_v$. Тогда для любой пары центрально-симметричных вершин A и A' выполняется свойство, что любая гипергрань $F^{d-1} \in P$ содержит либо A, либо A'.*

Таким образом в P нет гиперграней, свободных от двух антиподальных вершин одновременно.

Следствие. *Пусть $P \in A_f$. Тогда для любой пары центрально-симметричных граней F и F' выполняется свойство, что любая вершина лежит либо на F, либо F'.*

Отсюда вытекает, что центрально-симметричные многогранники, обладающие свойством f-антиподальности, являются антипризмами на любой паре гиперграней.

Доказательство. Возьмем многогранник P^*, применим к нему лемму 3 и снова возьмем дуальный к нему. Тогда утверждение леммы превратится в утверждение следствия.

Доказательство теоремы 2 строится от противного и опирается на лемму 3. Из этой теоремы следует, что на центрально-симметричных многогранниках v-антиподальность влечет f-антиподальность и наоборот.

Лемма 4. *$A \in A_f$ и $B \in A_f$ тогда и только тогда, когда $A \times B = P \in A_f$.*

Аналогично теореме 1, доказательство теоремы 3 строится на обосновании сохранения свойства антиподальности при индуктивном переходе при построении многогранников из K'.

Список литературы

1. Grunbaum B. Convex polytopes. — 1964.

2. Долбилин Н. П. Теоремы Минковского о параллелоэдрах и их обобщения // УМН. — 2007. — Вып. 4. — (В печати.)

3. Stanley R. P. The number of faces of simplical polytopes and spheres // Discrete Geometry and Convexity. — New York, 1982.

4. Barany I., Lovasz L. Borsuk's theorem and the number of facets of centrally symmetric polytopes // Acta Mathematica Acad. Sci. Hung. — 1982. — V. 40. — P. 323–329.

ПЕРЕБОР ВСЕХ ШТРАССЕНОВСКИХ АЛГОРИТМОВ ДЛЯ (2×2)-МАТРИЦ

А. Я. Белянков (Москва)

Рассматриваются $(n \times n)$-матричные тождества вида

$$(AB)_{ij} \equiv \sum_{1 \le \rho \le r} \langle \Lambda^\rho, A \rangle \, \langle \mathrm{M}^\rho, B \rangle \, \mathrm{N}^\rho_{ji} \quad (\text{по } A, B) \tag{1}$$

(здесь $\langle X, Y \rangle = \mathrm{tr}(X^T Y)$) или, эквивалентно,

$$\sum_{1 \le \rho \le r} \langle \Lambda^\rho, A \rangle \, \langle \mathrm{M}^\rho, B \rangle \, \langle \mathrm{N}^\rho, C \rangle \equiv \mathrm{tr}(ABC) \quad (\text{по } A, B, C) \tag{2}$$

над коммутативным кольцом R с единицей, где r по возможности невелико. Каждому такому тождеству соответствует алгоритм перемножения $(N\times N)$-матриц над R трудоемкости $O(N^\omega)$, $\omega=\log_n r$ [1].

Согласно [1] существуют тождества (2) с $n=2$, $r=7$, причем $\Lambda^\rho_{ij},\mathrm{M}^\rho_{ij},\mathrm{N}^\rho_{ij}\in\{0,\pm1\}$ для всех ρ,i,j. Это приводит к алгоритмам перемножения $(N\times N)$-матриц трудоемкости $O(N^\omega)$, $\omega=\log_2 7\approx 2.81$, над любым кольцом R. Уменьшить значение $r=7$ невозможно [2]. Ниже приводится пример таких $\Lambda^\rho,\mathrm{M}^\rho,\mathrm{N}^\rho$, где ради экономии места числа 0, 1, -1 заменены символами "$\circ$", "$+$", "$-$", а (2×2)-блочные строки изображают $(\Lambda^1,\dots,\Lambda^7)$, $(\mathrm{M}^1,\dots,\mathrm{M}^7)$ и $(\mathrm{N}^1,\dots,\mathrm{N}^7)$ соответственно:

$$\left[\begin{array}{cccccccccccccc}
- & \circ & \circ & \circ & \circ & - & \circ & \circ & + & + & + & \circ & + & \circ\\
\circ & \circ & + & + & \circ & + & \circ & - & \circ & \circ & - & \circ & \circ & +\\
\circ & - & - & \circ & \circ & \circ & + & \circ & \circ & \circ & + & + & + & \circ\\
\circ & + & \circ & \circ & + & + & - & \circ & \circ & - & \circ & \circ & \circ & +\\
\circ & \circ & \circ & - & - & \circ & + & + & + & \circ & \circ & \circ & + & \circ\\
+ & + & \circ & + & \circ & \circ & \circ & \circ & - & \circ & \circ & - & \circ & +
\end{array}\right]. \quad (3)$$

Решаются следующие две задачи. Найти все тождества вида (2), для которых $n=2$, $r=7$, а на матричные элементы наложено одно из двух условий: 1) все элементы искомых матриц $\Lambda^\rho,\mathrm{M}^\rho,\mathrm{N}^\rho$ принадлежат множеству $\{0,\pm1\}$; 2) все матрицы в (2) рассматриваются над полем Z_2 классов вычетов $\bmod 2$.

Взаимосвязь этих двух задач показывает следующая очевидная

Теорема. *Для решения $\Lambda^\rho,\mathrm{M}^\rho,\mathrm{N}^\rho$ первой задачи матрицы*

$$\Lambda^\rho \bmod 2,\ \mathrm{M}^\rho \bmod 2,\ \mathrm{N}^\rho \bmod 2 \quad (4)$$

образуют решение второй задачи.

Следствие. *Для решения поставленных выше задач достаточно сначала решить вторую задачу (над полем Z_2). Затем, трактуя каждое Z_2-решение как результат применения отображения (4) к решению $\Lambda^\rho,\mathrm{M}^\rho,\mathrm{N}^\rho$ первой задачи, восстановить это решение (или решения, если их несколько) путем расстановки знаков.*

Таким образом, при поиске матриц с элементами из $\{0,\pm1\}$ удалось отделить задачу поиска расположения ненулевых элементов от задачи расстановки знаков ненулевых элементов.

Следующие трансформации набора $\Lambda^\rho,\mathrm{M}^\rho,\mathrm{N}^\rho$ сохраняют (2):

1. Переход к набору $\Lambda^{\sigma(\rho)},\mathrm{M}^{\sigma(\rho)},\mathrm{N}^{\sigma(\rho)}$, где σ — перестановка чисел $1,\dots,r$, просто переставляет слагаемые в левой части (2).

2. Пропорциональные наборы матриц $\lambda^\rho\Lambda^\rho, \mu^\rho\mathrm{M}^\rho, \nu^\rho\mathrm{N}^\rho$ с условиями $\lambda^\rho\mu^\rho\nu^\rho = 1$ дают те же самые слагаемые в левой части (2). Для задачи над Z_2 эта симметрия тривиальна.

3. Для всякой тройки матриц U, V, W из некоторого множества M невырожденных матриц замена вида

$$\Lambda^\rho \mapsto U^{-1}\Lambda^\rho V,\ \mathrm{M}^\rho \mapsto V^{-1}\mathrm{M}^\rho W,\ \mathrm{N}^\rho \mapsto W^{-1}\mathrm{N}^\rho U \tag{5}$$

сохраняет (2), поскольку

$$\mathrm{tr}\left((U^{-T}AV^T)(V^{-T}BW^T)(W^{-T}CU^T)\right) = \mathrm{tr}(ABC).$$

В случае второй задачи (над полем Z_2) множество M состоит из всех невырожденных матриц над Z_2. В случае первой задачи включим в M все те матрицы U с элементами из $\{0, \pm 1\}$, у которых элементы обратной матрицы U^{-1} также принадлежат $\{0, \pm 1\}$ (т. е. $\det(U) = \pm 1$). Если у матриц нового набора (5) не все элементы принадлежат $\{0, \pm 1\}$, то его рассмотрение прекращается.

Класс решений, преобразующихся друг в друга трансформациями 1–2, считаем за одно решение.

Для обеих задач любое решение $\Lambda^\rho, \mathrm{M}^\rho, \mathrm{N}^\rho$ $(1 \le \rho \le 7)$ переводится трансформациями 3 в любое другое. В частности, все решения можно получить из (3) (отметим, что $-1 = 1$ над Z_2). Первая задача имеет 288 различных решений, вторая — 36. Для каждого из 36 решений второй задачи полный прообраз относительно (4) состоит из 8 решений первой задачи.

Приравняем в (2) коэффициенты при произведениях $A_{ij}B_{kl}C_{mn}$:

$$\sum_{1\le\rho\le r} \Lambda^\rho_{i(t)j(t)}\mathrm{M}^\rho_{k(t)l(t)}\mathrm{N}^\rho_{m(t)n(t)} = \delta_{j(t)k(t)}\delta_{l(t)m(t)}\delta_{n(t)i(t)}, \tag{6}$$

где индекс t, $1 \le t \le 64$, нумерует одночлены $A_{ij}B_{kl}C_{mn}$ в некотором порядке, от выбора которого значительно зависит время перебора.

При решении второй задачи последовательно в порядке возрастания $t = 1, \ldots, 64$ варьируются r-битовые наборы $\Lambda^\rho_{i(t)j(t)}$ и $\mathrm{M}^\rho_{k(t)l(t)}$, а относительно переменных N^ρ_{mn} уравнения (6) образуют линейную систему над Z_2. Варьирование обрывается, если при текущем t добавление (6) в текущую линейную систему влечет несовместность. При совместности вплоть до $t = 64$ множество решений пополняется.

При полученном решении второй задачи трактуем его как носитель решения первой задачи, а уравнения (6) — как определяющие

расстановку знаков λ^ρ_{ij}, μ^ρ_{kl}, ν^ρ_{mn} имеющих известное расположение ненулевых элементов $\Lambda^\rho_{ij} = (-1)^{\lambda^\rho_{ij}}$, $\mathrm{M}^\rho_{kl} = (-1)^{\mu^\rho_{kl}}$, $\mathrm{N}^\rho_{mn} = (-1)^{\nu^\rho_{mn}}$.

Для задачи вида $\sum_{\rho\in P(t)}(-1)^{\sigma_\rho} = R(t)$, где $R(t)$ — правая часть (6), а $P(t) = \{\rho \mid \Lambda^\rho_{i(t)j(t)}\mathrm{M}^\rho_{k(t)l(t)}\mathrm{N}^\rho_{m(t)n(t)} \neq 0\}$, множество $S(t) \subset {Z_2}^r$ решений $(\sigma_1, \ldots, \sigma_r)$ вкладывается в объединение аффинных многообразий $M_{t1}, M_{t2}, \ldots \subset {Z_2}^r$. Для уменьшения количества многообразий в ограниченной мере допускаются их непустые пересечения и наличие в них не принадлежащих $S(t)$ точек. Все такие задачи рассматриваются заранее, а наборы многообразий запоминаются. Легко видеть, что многообразию M_{ts} соответствует некоторая система Σ_{ts} линейных уравнений над Z_2 относительно переменных $\lambda^\rho_{i(t)j(t)}$, $\mu^\rho_{k(t)l(t)}$, $\nu^\rho_{m(t)n(t)}$.

При решении первой задачи в порядке возрастания $t = 1, \ldots, 64$ варьируется система Σ_{ts}, добавляемая в текущую систему, определяющую знаки λ^ρ_{ij}, μ^ρ_{kl}, ν^ρ_{mn}. При появлении несовместности — обрыв варьирования. Так как возможны "лишние решения", то при совместности вплоть до $t = 64$ необходима прямая проверка решений.

Список литературы

1. Strassen V. Gaussian elimination is not optimal // Numer. Math. —1969. — V. 13, № 4. — P. 354–356.

2. Hopcroft J. E., Kerr L. R. On minimizing the number of multiplications necessary for matrix multiplication // SIAM J. Appl. Math. — 1971. —V. 20, № 1. — P. 30–36.

ОСТРОУГОЛЬНЫЕ ТРЕУГОЛЬНИКИ ДАНЦЕРА — ГРЮНБАУМА

Л. В. Бучок (Москва)

Данная работа посвящена оценкам мощностей множеств точек евклидова пространства, в которых никакие три точки не образуют прямого или тупого угла. Введём обозначения: $a(n)$ — мощность максимального множества $S \subseteq \mathbb{R}^n$, обладающего указанным свойством; $k(n)$ — мощность максимального множества $S \subseteq \{0,1\}^n$, обладающего тем же свойством. Очевидно, $k(n) \leq a(n)$. Кроме того, известно, что $a(n) \leq 2^n$.

В 1962 году Л. Данцер и Б. Грюнбаум [1] высказали гипотезу о том, что $a(n) = 2n - 1$. В 1983 году эта гипотеза была опровергнута П. Эрдешем и З. Фюреди [2], доказавшими с помощью вероятностного метода, что $k(n) \geq \left\lfloor \frac{1}{2}\left(\frac{2}{\sqrt{3}}\right)^n \right\rfloor$. В 2006 году Д. Беван [3] путём изменения параметров в методе Эрдеша — Фюреди показал, что

$$k(n) \geq 2\left\lfloor \frac{\sqrt{6}}{9}\left(\frac{2}{\sqrt{3}}\right)^n \right\rfloor = 0.544\cdots \times (1.154\ldots)^n.$$

Д. Беван также получил оценку

$$a(n) \geq 2\left\lfloor \frac{1}{3}\left(\frac{2}{\sqrt{3}}\right)^{n+1} \right\rfloor = 0.770\cdots \times (1.154\ldots)^n$$

и ряд результатов для малых размерностей n, вследствие чего гипотеза Данцера — Грюнбаума была опровергнута при $n \geq 7$. Отметим, что при $n \leq 3$ гипотеза справедлива, и неясность сохраняется лишь при $n = 4, 5, 6$.

Теорема 1 (Эрдеш, Фюреди, 1983). *Имеет место неравенство*

$$k(n) \geq \left\lfloor \frac{1}{2}\left(\frac{2}{\sqrt{3}}\right)^n \right\rfloor.$$

Схема доказательства. Положим $m = \left\lfloor \frac{1}{2}\left(\frac{2}{\sqrt{3}}\right)^n \right\rfloor$ и возьмём случайное (мульти)множество $S \subseteq \{0,1\}^n$ из $2m$ (не обязательно различных) $(0,1)$-векторов; при этом координаты каждого вектора $\vec{v} = (v_1, v_2, \ldots, v_n) \in S$ мы выберем независимо, с вероятностью

$$P(v_i = 0) = P(v_i = 1) = \frac{1}{2}, \quad 1 \leq i \leq n;$$

выбор самих векторов мы также осуществим независимо, именно поэтому некоторые векторы могут получиться одинаковыми.

Назовём тройку векторов $(\vec{u}, \vec{v}, \vec{w}) \subset S$ *обобщённым прямым углом* с вершиной в $\vec{w}$, если $(\vec{u} - \vec{w}, \vec{v} - \vec{w}) = 0$. Все прямые углы в нашем множестве, очевидно, являются обобщёнными прямыми углами. Заметим, что отрицательных значений упомянутое скалярное произведение принимать не может, соответственно, тупых углов тройки из множества S не образуют. Тройка $(\vec{u}, \vec{v}, \vec{w})$ является обобщённым прямым углом с вершиной в $\vec{w}$ тогда и только тогда, когда

набор (u_i, v_i, w_i) не имеет вид $(0,0,1)$ или $(1,1,0)$ ни для какого $i \in 1, \ldots, n$. Вероятность последнего события равна $\left(\frac{3}{4}\right)^n$. Значит, математическое ожидание количества обобщённых прямых углов в S равно $3C_{2m}^3 \left(\frac{3}{4}\right)^n$. Поскольку

$$3C_{2m}^3 \left(\frac{3}{4}\right)^n \leq 3\frac{(2m)^3}{6}\left(\frac{3}{4}\right)^n = m(2m)^2\left(\frac{3}{4}\right)^n = m,$$

найдётся множество S из $2m$ векторов, в котором не более m обобщённых прямых углов. Если мы удалим из S вершины всех этих углов, останется множество из не менее m различных точек, никакие три из которых не образуют прямой угол. Таким образом, $k(n) \geq m$, и схема доказательства теоремы завершена.

Автором данной работы был создан алгоритм удаления точек из обобщённых прямых углов, основанный на том, что одна точка может принадлежать нескольким прямоугольным треугольникам одновременно. Таким образом, было доказано следующее утверждение.

Теорема 2. *Имеют место неравенства*

$$k(n) \geq \frac{3}{2}\left\lfloor \frac{11\sqrt{66}}{243}\left(\frac{2}{\sqrt{3}}\right)^n \right\rfloor = 0.551\cdots \times (1.154\ldots)^n,$$

$$a(n) \geq \frac{3}{2}\left\lfloor \frac{22\sqrt{33}}{243}\left(\frac{2}{\sqrt{3}}\right)^n \right\rfloor = 0.780\cdots \times (1.154\ldots)^n.$$

Работа выполнена при финансовой поддержке гранта РФФИ № 06-01-00383.

Список литературы

1. Danzer L., Grünbaum B. Über zwei Probleme bezüglich konvexer Körper von P. Erdős und von V. L. Klee // Math. Zeitschrift. — 1962. — V. 79. — P. 95–99.

2. Erdős P., Füredi Z. The greatest angle among n points in the d-dimensional Euclidean space // Annals of Discrete Math. — 1983. — V. 17. — P. 275–283.

3. Bevan D. Sets of points determining only acute angles and some related colouring problems // The Electronic Journal of Combinatorics. — 2006. — V.13. — R12.

ОБОБЩЕННЫЙ ПРИМЕР К. МУРТИ И «ЛИНЕЙНАЯ» ГИПОТЕЗА ХИРША

М. Н. Вялый, С. П. Тарасов (Москва)

К. Мурти [1] построил пример линейной задачи о дополнительности, у которой все так называемые конусы дополнительности "протыкаются" одной прямой. Эта конструкция эквивалентна существованию прямой в двойственном пространстве, пересекающей внутренности всех d-мерных конусов нормального веера выпуклого многогранника $P \subset \mathbf{R}^d$, комбинаторно эквивалентному d-мерному кубу.

Мы приводим простое геометрическое обоснование конструкции К. Мурти, позволяющее перенести доказательство на другие многогранники, например, на знаменитый гиперкуб Кли — Минти [2]. Используя эту конструкцию, мы построим контрпример к "линейной" версии известной гипотезы Хирша о реберном диаметре выпуклого многогранника.

Веером в $\mathbf{R}^d$ называется семейство $\mathcal{F}$ выпуклых полиэдральных конусов, замкнутых относительно пересечения и таких, что любая грань любого конуса семейства принадлежит $\mathcal{F}$. Будем называть k-мерные конуса $\mathcal{F}$ *k-конусами.*

Веер называется *полным* в конусе K, если объединение всех его конусов равно K. Пусть $P \subseteq \mathbf{R}^d$ — выпуклый многранник и Γ его грань. По определению, *нормальный конус* $N_\Gamma P \subseteq (\mathbf{R}^d)^*$ состоит из всех линейных функционалов, максимум которых на P достигается (на всей) грани Γ. В частности, если v — вершина P, то $N_v(P) = K_v^*$ — это *конус оптимальности* вершины v, то есть двойственный конус к *граничному конусу* K_v многогранника P в вершине v (по определению, K_v является пересечением всех опорных полупространств к P, граница которых содержит v). Пусть P задан списком полупространств $P = \{x \in \mathbf{R}^d \mid a_i x \le b_i,\ i = 1, 2, \ldots n\}$. Выделим подмножество $F(v) \subset \{1, \ldots, n\}$ так, что для любого $j \in F(v)$ выполнено $a_j v = b_j$. Тогда граничный конус представим в виде: $K_v = \{x \in \mathbf{R}^d \mid a_j(x - v) \le 0,\ j \in F(v)\}$. Следовательно, двойственный конус представляется в виде: $N_v(P) = K_v^* \stackrel{def}{=} \{y \in \mathbf{R}^d \mid xy \le 0$ для всех $x - v \in K_v\}$ и по лемме Фаркаша: $N_v(P) = \{\sum_{j \in F(v)} \lambda_j a_j,\ \lambda_j \ge 0, j \in F(v)\}$. Семейство $\mathcal{N}(P)$ всех нормальных конусов N_Γ для всех граней $\Gamma \subset P$ образует полный во всем пространстве веер, называемый *нормальным веером* P. Например, если C^d это стандартный d-мерный куб то $\mathcal{N}(C^d)$ образуют 2^d ортантов $\mathbf{R}^d$.

Будем говорить, что прямая l *трансверсально пересекает* или *протыкает* конус $K \subseteq \mathbf{R}^d$, если l пересекает относительную внутренность K. Нас интересует следующий вопрос. Рассмотрим класс выпуклых многогранников $\mathcal{C}_d$, комбинаторно эквивалентных стандартному d-кубу. Пусть $P \in \mathcal{C}_d$. Какое максимальное число $\nu(P)$ d-конусов нормального веера $\mathcal{N}(P)$ может протыкать прямая (в двойственном пространстве)?

В случае стандартного d-куба C^d ответ очевиден: $\nu(C^d) = d + 1$.

Теперь построим семейство многогранников из $\mathcal{C}_d$, для которого величина ν_d принимает максимальное значение. Для каждого $\mu \in [0, 1]$ рассмотрим выпуклый многогранник $P_d^\mu \subset \mathbf{R}^d$, задаваемый следующей системой $\mathcal{I}^\mu$ линейных неравенств:

$$\begin{cases} \sum\limits_{j=1}^{k-1} 2(2-\mu)^{k-j} x_j + x_k & \leq & (5-\mu)^k & (1 \leq k \leq d) \\ -x_k & \leq & 0 & (1 \leq k \leq d) \end{cases}$$

Отметим, что при $\mu = 0$ мы получаем стандартный скошенный куб В. Кли и Д. Минти (см. [3]), а при $\mu = 1$ получаем d-куб К. Мурти.

Теорема 1. *При $\mu \in [0, 1]$ многогранник P_d^μ комбинаторно эквивалентен d-мерному кубу.*

Теорема 2. *При $\mu \in [0, 1]$ выполнено $\nu(P_d^\mu) = 2^d$.*

Заметим, что величина $\nu(\cdot)$ веера конусов дополнительности дает оценки числа итераций для алгоритма К. Лемке решения линейной задачи о дополнительности [1] и, в контексте задачи линейного программирования, для самодвойственного алгоритма Д. Данцига [4]. Кроме того, подобно тому, как это делается в [5], многогранники семейства P_d^μ можно использовать для конструкции задач *параметрического линейного программирования* с экспоненциальным по размерности числом переключений. Описанная конструкция в некоторой степени связана с известной гипотезой Хирша (1957), утверждающей, что реберный диаметр $D(d, n)$ компактного выпуклого d-мерного многогранника P, имеющего n граней максимальной размерности, не превышает $n - d$.

Будем говорить, что отрезок $[s, t]$ двойственного пространства расположен *в общем положении по отношению к вееру* $\mathcal{N}(P)$, если $[s, t]$ не пересекает никакой конус коразмерности 2 из $\mathcal{N}(P)$. Для пары вершин v, u обозначим через $\mathcal{G}(v, u)$ множество всех отрезков $[s, t]$, расположенных в общем положении по отношению к $\mathcal{N}(P)$ и

таких, что $s \in \mathrm{relint}(K_v^*)$, $t \in \mathrm{relint}(K_u^*)$. Определим также параметр $\mathrm{sd}(v, u)$ как наименьшее число фасет конусов из $\mathcal{N}(P)$, которые пересекает отрезок $[s, t] \in \mathcal{G}(v, u)$. Величина $\max_{v,u} \mathrm{sd}(v, u)$ служит верхней оценкой диаметра многогранника P. (Чтобы аналогичным образом получить диаметр многогранника, нужно заменить отрезки на произвольные ломаные.) Можно высказать гипотезу, которую естественно назвать "линейной" гипотезой Хирша: $\max_{v,u} \mathrm{sd}(v, u)$ не превосходит $n - d$ (или, в ослабленном варианте меньше некоторого полинома от n и d). Эта гипотеза намного сильнее гипотезы Хирша и, используя построенные выше многогранники, можно показать, что она неверна.

Теорема 3. *Существует простой d-мерный многогранник с $4d$ фасетами, для некоторых вершин u, v которого выполняется* $\mathrm{sd}(v, u) \geq 2^d + 2$.

Работа выполнена при финансовой поддержке РФФИ, проекты 05–01–01019, 05–01–02803, и гранта Президента РФ по поддержке ведущих научных школ НШ 5833.2006.1.

Список литературы

1. Murty K. Computational complexity of complementarity pivot methods // Mathematical Programming Study. — 1978. — V. 7. — P. 61–73.

2. Klee V., Minty G. How good is the simplex algorithm? // Inequalities III. — Academic Press, 1972. — P. 159–175.

3. Schrijver A. Theory of linear and integer programming. — Chichester: Wiley-Interscience, 1986.

4. Smale S. On the average number of steps in the simplex method of linear programming // Mathematical Programming. — 1983. — V. 27. — P. 241–262.

5. Murty K. Computational complexity of parametric linear programming // Mathematical Programming. — 1980. — V. 19. — P. 213–219.

6. Kalai G., Kleitman D. A quasi-polynomial bound for the diameter of graphs of polyhedra // Bulletin Amer. Math. Soc. — 1992. — V. 26. — P. 315–316.

СЛОЖНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ ПО В. И. АРНОЛЬДУ

А. И. Гарбер (Москва)

Пусть p — некоторое простое число. Рассмотрим множество всех p-ичных последовательностей длины n, они образуют множество $\mathbb{Z}_p^n$.

Пусть $\mathcal{A} : \mathbb{Z}_p^n \to \mathbb{Z}_p^n$ — *оператор первой конечной разности*, то есть $\mathcal{A}$ действует на последовательность $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ следующим образом: $\mathcal{A}\boldsymbol{x} = \boldsymbol{y}$, — где последовательность $\boldsymbol{y}$ имеет вид $\boldsymbol{y} = (x_2 - x_1, x_3 - x_2, \ldots, x_n - x_{n-1}, x_1 - x_n)$.

Оператор $\mathcal{A}$ определяет направленный граф G_n без кратных ребер. Вершинами G_n являются все p^n точек пространства $\mathbb{Z}_p^n$. Направленное ребро из точки $\boldsymbol{x}$ в точку $\boldsymbol{y}$ существует в том и только том случае, если $\mathcal{A}\boldsymbol{x} = \boldsymbol{y}$.

В работе [1] (см. также [2–4]) В. И. Арнольдом была доказана следующая

Теорема 1. *Каждая компонента связности графа G_n представляет собой единственный ориентированный цикл, каждая вершина которого служит корнем некоторого дерева, возможно пустого. Причем все ребра дерева направлены к его корню, т. е. к вершине цикла.*

Мы будем говорить что все вершины всех деревьев одной компоненты связности *притягиваются* циклом, принадлежащим этой же компоненте.

Согласно определению В. И. Арнольда, последовательность $\boldsymbol{x}$ *сложнее* последовательности $\boldsymbol{y}$ если цикл, притягивающий точку $\boldsymbol{x}$, длиннее цикла, притягивающего точку $\boldsymbol{y}$. Если же последовательности $\boldsymbol{x}$ и $\boldsymbol{y}$ притягиваются циклами одинаковых длин, то сложнее та из них, которая находится дальше от корня соответствующего дерева.

В 2006 году В. И. Арнольдом [3] была поставлена следующая задача: исследовать структуру графа G_n, длины циклов в нем, количество сложных последовательностей.

Первая гипотеза, которая была сформулирована В. И. Арнольдом, на основе вычислений при малых n при $p = 2$, состоит в том, что длина максимального цикла в графе G_n делится на n, за исключением случая, когда p — степень двойки. В работе [5] исследование гипотезы Арнольда сведено к исследованию порядка многочлена z в мультипликативной группе остатков по модулю p-ичного многочлена $P_n(z) = \frac{(z+1)^n - 1}{z^{p^\alpha}}$, где α — степень вхождения числа p в разложение n на простые множители. Более того, в [5] доказана следующая теорема о длине максимального цикла:

Теорема 2. *Если n не равняется p^α и $2p^\alpha$, то длина максимального цикла $L(n)$ делится на n.*

Другие исследования о длине максимального цикла при $p = 2$ можно найти в [6].

В результате компьютерных исследований при $p = 2$ и $n < 100$ была сформулирована

Гипотеза. *a) Пусть $C(n)$ общее количество циклов, а $C_{max}(n)$ — количество циклов максимальной длины. Тогда отношение $\frac{C_{max}(n)}{C(n)}$, или доля циклов максимальной длины, стремится к единице, когда n стремится к бесконечности.*

b) (более слабый вариант) Пусть $v_{max}(n)$ — доля вершин, притягиваемых циклами максимальной длины. Тогда $v_{max}(n) \to 1$ при $n \to \infty$.

Позднее в работе [7] вычисления были проделаны и для других n и p (при $p = 2$ для $n \leq 300$ при $p = 3$ для $n \geq 50$).

При помощи анализа корней многочлена $P_n(z)$ в алгебраическом расширении поля $\mathbb{Z}_p$ в работе [5] была доказана следующая

Теорема 3. *Если n пробегает только степени простых чисел и стремится к бесконечности, то при этом $v_{max}(n)$ стремится к единице.*

Таким образом частично доказан слабый вариант гипотезы (вариант b)).

Список литературы

1. Арнольд В. И. Сложность конечных последовательностей нулей и единиц и геометрия конечных функциональных пространств // `http://mms.math-net.ru/meetings/2005/arnold.pdf`.

2. Arnold V. I. Complexity of finite sequences of zeros and ones and geometry of finite spaces of functions // Functional Analysis and Other Mathematics. — 2006. — V. 1, № 1. — P. 1–18.

3. Арнольд В. И. Сложность конечных последовательностей нулей и единиц и геометрия конечных функциональных пространств. Лекция // `http://elementy.ru/lib/430178/430281`. — 2006.

4. Арнольд В. И. Complexity of finite sequences of zeros and ones and geometry of finite spaces of functions // Abdus Salam International Center Math. Phys. ICTP (Miramare, March 2006). — Preprint.

5. Garber A. I. Graph of difference operator for p-ary sequences // Functional Analysis and Other Mathematics. — 2006. — V. 1, № 2. — P. 179–195.

6. Karpenkov O. N. On examples of difference operator for 0,1-valued function over finite sets // Functional Analysis and Other Mathematics. — 2006. — V. 1, № 2. — P. 197–202.

7. Лернер Э. Ю. Мультипликативная функция вместо логарифма // `http://kek.ksu.ru/kek2/MyArnold.pdf`.

О НОВОМ СВОЙСТВЕ ПОЛИЭДРАЛЬНЫХ РАЗБИЕНИЙ

А. А. Глазырин (Москва)

Пусть $\mathbb{E}^n$ обозначает n-мерное евклидово пространство. *Выпуклым многогранником* является ограниченное пересечение конечного числа замкнутых полупространств. *Шаровой многогранник* — это пересечение шара с центром O с конечным числом таких полупространств k_i, что $\{O\} \in \bigcap_i k_i$. Набор многогранников $\mathcal{T} = \{T_n\}_{n\geq 0}$, являющийся упаковкой, а также покрытием $\mathbb{E}^n$, называется *разбиением* на многогранники. Разбиение $\mathcal{T}$ называется *локально конечным*, если каждое открытое множество $U \in \mathbb{E}^n$ пересекается только с конечным числом элементов разбиения $\mathcal{T}$. Следующая проблема была поставлена Дирком Фреттле в рамках локально конечной сложности самоподобных разбиений [1].

Вопрос: правда ли, что у локально конечного разбиения $\mathcal{T}$ в $\mathbb{E}^n$, у которого все элементы разбиения выпуклые многогранники, каждая вершина разбиения является вершиной по меньшей мере двух элементов разбиения $\mathcal{T}$?

В этой работе показано, что ответ положителен в общем случае.

Определим для каждого n-мерного шарового многогранника P соответствующую ему характеристическую функцию $\mathbf{I}_P$, равную 1 во внутренних точках P и 0 — во всех остальных точках пространства $\mathbb{R}^n$. Далее будем считать равными функции, которые равны всюду, кроме множества точек меры ноль по Лебегу. Будем называть n-мерные шаровые многогранники B-многогранниками, если их граница содержит две диаметрально противоположные точки сферы, и A-многогранниками — в противоположном случае. Докажем следующее утверждение:

Теорема 1. *Характеристическая функция любого A-многогранника не может равняться линейной комбинации характеристических функций конечного числа B-многогранников.*

Доказательство теоремы проведем индукцией по размерности. База индукции: $n = 1$. Переход индукции. Итак, мы уже знаем, что утверждение верно для размерности $n-1$. Докажем, что оно верно и в случае размерности n. Будем доказывать от противного. Пусть существует такой n-мерный A-многогранник P и B-многогранники $Q_1, \ldots, Q_k$, что $\mathbf{I}_P - \sum_1^k \alpha_i \mathbf{I}_{Q_i} = 0$. Рассмотрим произвольную $(n-1)$-мерную гиперплоскость проходящую через центр шара. Пусть это для определенности плоскость $x_1 = 0$. Пусть также задана некоторая функция $f : \mathbb{R}^n \to \mathbb{R}$. Определим функции f_0^+ и f_0^- следующим

образом:

$$f_0^+(x_2,\ldots,x_n) = \lim_{m\to\infty} f(\frac{1}{2^m}, x_2, \ldots, x_n)$$

$$f_0^-(x_2,\ldots,x_n) = \lim_{m\to\infty} f(-\frac{1}{2^m}, x_2, \ldots, x_n).$$

Пусть P — произвольный выпуклый n-мерный шаровой многогранник, $P_0 = P \cap \{x_1 = 0\}$. Заметим, что P_0 является выпуклым шаровым многогранником не больше чем $(n-1)$-й размерности — это нам понадобится в дальнейшем. Если $f = \mathbf{I}_P$, то верна следующая

Лемма 1. *Функция f_0^+ существует и при этом $f_0^+ = \boldsymbol{I}_{P_0}$ в случае если не все внутренние точки P лежат в отрицательном полупространстве и $f_0^+ = 0$ в обратном случае.*

Аналогичная лемма верна и для f_0^-.

Рассмотрим теперь $f = \mathbf{I}_P - \sum_1^k \alpha_i \mathbf{I}_{Q_i}$. Будем считать, что одна из $(n-1)$-мерных гиперграней P лежит в гиперплоскости $x_1 = 0$, а сам P лежит в положительном полупространстве. По лемме существует f_0^+ и при этом $f_0^+ = \mathbf{I}_{P_0} - \sum_1^k \alpha_i \mathbf{I}_{Q_i^+}$, где $Q_i^+ = Q_i \cap \{x_1 = 0\}$ в том случае, если какие-то внутренние точки Q_i лежат в положительном полупространстве и 0 в ином случае. Аналогично $f_0^- = -\sum_1^k \alpha_i \mathbf{I}_{Q_i^-}$, где Q_i^- определяются абсолютно так же. Заметим, что $f_0^+ = 0$ и $f_0^- = 0$ как пределы последовательностей, равных нулю. Пусть $g = f_0^+ - f_0^-$. Тогда $g = 0$ и $g = \mathbf{I}_{P_0} - \sum_1^k \alpha_i (\mathbf{I}_{Q_i^+} - \mathbf{I}_{Q_i^-})$. Если Q_i пересекает гиперплоскость $x_1 = 0$, то $Q_i^+ = Q_i^-$ и соответствующие члены суммы обнуляются. Если же Q_i касается гиперплоскости, то один из членов в скобках равен 0. Получаем

$$0 = \mathbf{I}_{P_0} - \sum_1^k \beta_i \mathbf{I}_{S_i},$$

где $S_i = \varnothing$, если Q_i пересекает гиперплоскость, $S_i = Q_i^+$ и $\beta_i = \alpha_i$, если Q_i касается гиперплоскости и лежит в положительном полупространстве, $S_i = Q_i^-$ и $\beta_i = -\alpha_i$, если касается и лежит в отрицательном полупространстве. Заметим, что верна следующая лемма:

Лемма 2. *Если B-многогранник касается гиперплоскости, проходящей через центр шара, то многогранник касания также является B-многогранником.*

Итак, все S_i являются B-многогранниками, а P_0 — A-многогранник, тем самым мы пришли к противоречию, так как по предположению индукции утверждение теоремы верно для меньших размерностей.

Теорема 2. *Шар любой размерности нельзя разбить на B-многогранники и один A-многогранник.*

Пусть шар можно разбить на один A-многогранник P и B-многогранники $Q_1, \ldots, Q_k$. Пусть M_1 и M_2 — это два полушария, дополняющие друг друга до шара. Тогда

$$\mathbf{I}_P + \sum_1^k \mathbf{I}_{Q_i} - \mathbf{I}_{M_1} - \mathbf{I}_{M_2} = 0,$$

что противоречит теореме 1.

Рассмотрим произвольное локально конечное разбиение $\mathcal{T}$ пространства $\mathbb{R}^n$ на многогранники.

Теорема 3. *Никакая точка C пространства $\mathbb{R}^n$ не может быть вершиной ровно одного из многогранников разбиения $\mathcal{T}$.*

Построим такой шар с центром в C, чтобы он пересекал только те грани многогранников разбиения, которые содержат C. Заметим, что если C является вершиной многогранника разбиения, то его пересечение с шаром будет A-многогранником, а если нет, то B-многогранником. Поскольку ровно одного A-многогранника быть не может из теоремы 2, то и C не может быть вершиной ровно одного многогранника разбиения.

Следствие. *Пусть $\mathcal{T}$ — локально конечное разбиение пространства $\mathbb{E}^n$ на многогранники. Тогда нет такого подпространства $F \subset \mathbb{E}^n$, что F содержит грань размерности k ровно одного из многогранников разбиения.*

Список литературы

1. Frettlöh D. Nichtperiodische Pflasterungen mit ganzzahligem. — Inflationsfaktor, Ph. D. Thesis. — Dortmund, 2002. — `http://hdl.handle.net/2003/2309`.

2. Frettlöh D. Duality of model sets generated by substitutions // Rev. Roumaine Math. Pures Appl. — 2005. — V. 50. — P. 619–639.

АНТИ-ДЮРЕР ГИПОТЕЗА ДЛЯ НЕВЫПУКЛЫХ МНОГОГРАННИКОВ

А. А. Глазырин, А. С. Тарасов (Москва)

В 1528 году Дюрером [1] была поставлена следующая проблема — существует ли реберная развертка из одного многоугольника для любого выпуклого многогранника. Несмотря на столь давний возраст и достаточную известность, про эту проблему до сих пор мало что известно. Долгое время она была сформулирована именно для выпуклых многогранников, однако, тот же вопрос для невыпуклых многогранников не изучался вовсе. В 1996 году Н. П. Долбилиным была поставлена та же задача для невыпуклых многогранников с выпуклыми гранями. В [3] был предъявлен пример многогранника, не имеющего реберной развертки из одного многоугольника. Реберная развертка, состоящая из двух компонент связности, для этого примера уже существовала.

Определение. Разверткой многогранника будем называть совокупность многоугольников с указанием правила склеивания.

Определение. Реберной разверткой назовем развертку, в которой стороны многоугольников развертки целиком составлены из ребер многогранника. При этом будем называть ребро многогранника ребром разреза, если оно лежит на стороне одного из многоугольников развертки.

Определение. Обозначим через $C(P)$ минимальное число многоугольников реберной развертки.

Тогда возникает вопрос, каков верхний предел $C(P)$ по всем многогранникам. Н. П. Долбилиным была поставлена в [2] гипотеза что $\sup C(P)$ для класса выпуклых многогранников равен $+\infty$. Покажем, что подобное утверждение верно для класса невыпуклых многогранников с выпуклыми гранями, т. е. для любого N предъявим многогранник P_N, такой что $C(P_N) > N$.

Для начала сформулируем и докажем обобщение теоремы Татта, которое понадобится нам в дальнейшем. Напомним саму теорему Татта [4]:

Теорема 1 (Татт). *Существует пример регулярного планарного графа из* 25 *областей, у которого нет гамильтонова цикла.*

Определение. Назовем связный подграф H планарного графа G *разрезанием*, если для каждой вершины графа G есть как минимум два инцидентных ребра, принадлежащих H.

Разрезание с числом граней, равным двум эквивалентно гамильтонову циклу.

Обозначим через T фрагмент Татта, граф на котором строится контрпример Татта, этот граф состоит из 15 вершин, с тремя ключе-

выми вершинами A, B, C. Этот фрагмент обладает следующим свойством: не существует гамильтонова пути между вершинами B и C.

Построим с помощью этого фрагмента граф T_N, состоящий из N фрагментов Татта, в которых последовательно правая боковая вершина C_i соединена ребром с левой боковой вершиной следующего фрагмента B_{i+1}. А все верхние вершины A_i соединены с дополнительной вершиной O. Граф T_3 является графом Татта.

Теперь можно сформулировать следующую теорему, которая в некотором смысле является обобщением теоремы Татта:

Теорема 2. *Для любого $N > 3$ в планарном трехсвязном графе T_N число граней любого разрезания не менее $\frac{N}{3} + 1$.*

Теперь займемся построением шипа. Пусть V — некоторая простая вершина выпуклого многогранника с суммой плоских углов больше π (далее для краткости будем называть такие вершины "хорошими"). Пусть d — минимальная длина ребра прилегающего к V. Выберем на ребрах выходящих из V точки V_1, V_2, V_3 так, чтобы $VV_1 = VV_2 = VV_3 = r$. Отрежем вершину вместе с треугольной пирамидой $VV_1V_2V_3$.

Построим *шип* — пирамиду с основанием $V_1V_2V_3$ и вершиной V', проекция которой на плоскость $V_1V_2V_3$ лежит внутри основания, так, чтобы плоские углы боковых граней пирамиды при основании были больше $max\{\pi/2 - \alpha/8, \pi - (1/2)(\angle V_1VV_2 + \angle V_2VV_3 + \angle V_3VV_1)\}$, где α — минимальный плоский угол при вершине V; а расстояния $V'V_i$ больше $2r$.

Выберем $r < d/2cos(\pi/2 - \alpha/2) = d/2sin(\alpha/2)$.

Определение. Будем называть *многогранником с краем* сильносвязное объединение граней телесного многогранника.

Для многогранника с краем аналогично можно определить реберную развертку.

Боковые стороны шипа и смежные с ними грани многогранника образуют многогранник с краем P_V.

Для этого выполняется следующая лемма.

Лемма 1. *Многогранник P_V обладает следующими свойствами:*

1) *часть границы произвольного многоугольника развертки, являющаяся краем многогранника P_V, связна;*

2) $C(P_V) > 1$.

Первое свойство сложно формулируется, а по сути обозначает, что если две большие грани находятся в одной компоненте развертки, то от одной грани к другой можно пройти, не проходя через грани шипа.

Пусть Q_N — выпуклый многогранник, реберный остов которого изоморфен графу T_N. Такой многогранник существует [5].

Построим на каждой "хорошей" вершине многогранника Q_N по шипу. Пусть Q'_N — полученный многогранник.

Теорема 3. *Реберная развертка многогранника Q'_N имеет не меньше $\frac{N}{3} - 4$ компонент.*

Список литературы

1. Dürer A. The painter's manual: a manual of measurement of lines, areas, and solids my mean of compass and rules assembled by Albrecht Dürer for the use of all lovers of art with appropriate illustrations arranged and printed in the year MDXXV. — Abaris Books.

2. Долбилин Н. П. Устное сообщение. — 2006.

3. Тарасов А. С. Многогранники, не допускающие натуральных разверток // Успехи математических наук. — 1999. — Т. 54, вып. 3.

4. Tutte W. T. On hamiltonian circuits // J. London Math. Soc. — 1946. — V. 21. — P. 98–101.

5. Steinitz E., Rademacher H. Vorlesungen über die Theorie der Polyeder. — Berlin: Springer, 1934.

ХРОМАТИЧЕСКИЕ ЧИСЛА ПРОСТРАНСТВ $\mathbb{R}^2$ И $\mathbb{R}^3$ С ИНТЕРВАЛАМИ ЗАПРЕЩЕННЫХ РАССТОЯНИЙ

Л. Л. Иванов (Москва)

В середине двадцатого столетия была сформулирована одна из наиболее ярких задач комбинаторной геометрии. В задаче требуется отыскать минимальное число $\chi(\mathbb{R}^2)$ цветов, необходимое для такой покраски евклидовой плоскости, что никакие две точки на расстоянии 1 не покрашены в один цвет. Величину $\chi(\mathbb{R}^2)$ называют *хроматическим числом* плоскости.

Классическое обобщение задачи состоит в отыскании хроматического числа $\chi(\mathbb{R}^n)$ для n-мерного евклидового пространства. Истоки этой проблематики восходят к Эдварду Нельсону и Гуго Хадвигеру [1].

Существует более общее понятие хроматического числа метрического пространства (M, ρ) с множеством A *запрещенных расстояний*:

$$\chi((M,\rho),A) = \min\{k \mid M = M_1 \sqcup \ldots \sqcup M_k, \forall i\ \forall x,y \in M_i\ \rho(x,y) \notin A\}.$$

Другими словами, мы запрещаем точкам одного цвета находиться на расстоянии из множества A.

В дальнейшем мы будем использовать краткую запись

$$\chi_A(\mathbb{R}^n) = \chi((\mathbb{R}^n, |\cdot|), A).$$

В докладе будет рассмотрена ситуация, когда множество A является отрезком. Без ограничения общности можно считать, что отрезок имеет вид $[1, d]$. Через $\chi_d(\mathbb{R}^n)$ обозначим для краткости величину $\chi_{[1,d]}(\mathbb{R}^n)$. В случае $d = 1$ отрезок вырождается в точку и мы возвращаемся к классическому хроматическому числу $\chi(\mathbb{R}^n)$.

Для величины $\chi(\mathbb{R}^n)$ в малых размерностях были получены следующие результаты:

$$4 \le \chi(\mathbb{R}^2) \le 7 \quad \text{(см. [1, 2])};$$
$$6 \le \chi(\mathbb{R}^3) \le 15 \quad \text{(см. [3, 4])};$$
$$7 \le \chi(\mathbb{R}^4) \le 49 \quad \text{(см. [5])}.$$

В то же время о величине $\chi_d(\mathbb{R}^n)$ при $d > 1$ практически ничего не было известно.

Заметим, что в одномерном случае удается точно определить хроматическое число при всех d: $\chi_d(\mathbb{R}) = \lceil d \rceil + 1$. Однако двумерный и трехмерный случаи ощутимо более сложные.

Перейдем к некоторым новым результатам, представленным в следующих теоремах.

Теорема 1. *В случае $n = 2$ выполнены неравенства:*

$d \le$	$\chi_d(\mathbb{R}^2) \le$
1.322876	7
1.732051	9
2	12
2.179449	13
2.598076	16
2.783882	19
3.041381	21

Теорема 2. *В случае $n = 3$ выполнены неравенства:*

$d \le$	$\chi_d(\mathbb{R}^3) \le$
1.048809	15
1.115838	18
1.149718	19
1.316854	21
1.324932	23
1.549193	27

Представленные выше результаты были получены при помощи решетчатых разбиений пространств на области Вороного.

Работа выполнена при финансовой поддержке гранта РФФИ (06-01-00383).

Список литературы

1. Soifer A. Chromatic number of the plane: a historical essay // Geombinatorics. — 1991. — P. 13–15.

2. Hadwiger H. Ungelöste probleme N 40 // Elemente der Math. — 1961. — V. 16. — P. 103–104.

3. Nechushtan O. Note on the space chromatic number // Discrete mathematics. — 2002. — V. 256. — P. 499–507.

4. Coulson D. A 15-colouring of 3-space omitting distance one // Discrete mathematics. — 2002. — V. 256, № 1–2. — P. 83–90.

5. Иванов Л. Л. Оценка хроматического числа пространства $\mathbb{R}^4$ // Успехи математических наук — 2006. — Т. 61, вып. 5. — С. 181–182.

О ЛОКАЛЬНЫХ УСЛОВИЯХ БИПРАВИЛЬНЫХ ТРИАНГУЛЯЦИЙ ЕВКЛИДОВОЙ ПЛОСКОСТИ

Е. В. Коломейкина (Москва)

В ряде работ 1970–1990 гг. был развит общий локальный подход к изучению кристаллических разбиений [1–4]. В данной работе рассматривается задача описать локальные условия биправильных триангуляций евклидовой плоскости. Другими словами, какой радиус конгруэнтности нужно потребовать, чтобы обеспечить для данного разбиения его биправильность. Среди основных результатов теории разбиений, имеется работа Долбилина, Дресса, Хусона [4], в которой дается оценка сверху для числа гиперграней любой ячейки в m-эдральном разбиении пространства R^d. Из этой работы следует существование такого целого числа $k = k(d, m)$, что если все неполные (полные) короны радиуса k данного разбиения T распадаются в не более, чем m классов, то разбиение T является m-эдральным. Оценка числа $k(d, m)$ радиуса конгруэнтности очень велика, отсюда следует актуальность нашей задачи.

Напомним, что разбиение называется m-эдральным, если множество ячеек этого разбиения распадается в m орбит относительно группы симметрий разбиения. Если $m = 2$, то разбиение называется биправильным. Обозначим через N_i и N_i^* число классов неполных и

соответственно полных корон радиуса i, а через S_i и S_i^* обозначим соответствующие группы симметрий этих корон.

Итак, имеется нормальное разбиение евклидовой плоскости на треугольники. Если в разбиении число классов неполных корон $N_1^* = 1$, то по теореме из [3] такое разбиение является правильным. Чтобы разбиение T было биправильным, необходимо выполнение $N_1 = 2$. Существует пример разбиения, показывающий, что это условие не является достаточным.

Теорема 1. *Нормальное разбиение T евклидовой плоскости на треугольники является биправильным тогда и только тогда, когда число классов $N_1^* = 2$.*

Доказательство условия достаточности использует следующую обобщенную локальную теорему [2].

Теорема 2. *Для целого $m > 0$ разбиение T является m-эдральным тогда и только тогда, когда существует такое натуральное k, что*

(1) $N_{k-1} = N_k = m$;

(2) *для каждого $P \in T$ выполняется $S_{k-1}(P) = S_k(P)$.*

Группа $S_0(P)$ симметрий треугольника P может быть одной из следующих: D_3, D_1, E. Группа $S_1(P)$ симметрий первой неполной короны радиуса 1 треугольника P, а также группа $S_1^*(P)$ симметрий первой полной короны радиуса 1 треугольника P, может быть одной из D_3, C_3, D_1, E. Причем $S_0(P) \supseteq S_1(P) \supseteq S_1^*(P)$. Заметим, что если $S_0(P) = C_3$, то это означает, что треугольник правильный, значит, на самом деле $S_0(P) = D_3$.

Идея доказательства. Если $S_0(P_i) = D_3$, $i = 1, 2$, то данное разбиение является разбиением на правильные треугольники, не удовлетворяющее условию теоремы $N_1^* = 2$. Поэтому нам нужно рассмотреть случаи, когда хотя бы одна из ячеек P_i, $i = 1, 2$, не является правильным треугольником. Выпишем всевозможные пары (группа симметрий $S_0(P_i)$ ячейки P_i, группа симметрий $S_1^*(P_i)$ полной короны ячейки P_i):

1)	$(D_3, D_3); (D_1, D_1)$;	2)	$(D_3, D_3); (D_1, E)$;
3)	$(D_3, D_3); (E, E)$;	4)	$(D_3, C_3); (D_1, D_1)$;
5)	$(D_3, C_3); (D_1, E)$;	6)	$(D_3, C_3); (E, E)$;
7)	$(D_3, D_1); (D_1, D_1)$;	8)	$(D_3, D_1); (D_1, E)$;
9)	$(D_3, D_1); (E, E)$;	10)	$(D_3, E); (D_1, E)$;
11)	$(D_3, E); (E, E)$;	12)	$(D_1, D_1); (D_1, D_1)$;
13)	$(D_1, D_1); (D_1, E)$;	14)	$(D_1, D_1); (E, E)$;
15)	$(D_1, E); (D_1, E)$;	16)	$(D_1, E); (E, E)$;
17)	$(E, E); (E, E)$.		

Рассматриваются различные случаи.

Случай 1. Разбиение с 2 прототайлами ($P_1 \ncong P_2$). Тогда выполняется равенство $N_0 = N_1 = 2$, а также $N_0 = N_1^* = 2$.

Случай 1.1. В разбиении $S_0(P_i) = S_1^*(P_i)$ для каждого P_i, где $i = 1, 2$, (что соответствует парам 1, 3, 12, 14 или 17). Тогда биправильность такого разбиения следует из теоремы 2.

Случай 1.2. $S_0(P_1) = S_1^*(P_1)$, но $S_0(P_2) \supset S_1^*(P_2)$ (что соответствует парам 2, 4, 6, 7, 9, 11, 13 или 16). Тогда см. теорему 3.

Случай 1.3. $S_0(P_i) \supset S_1^*(P_i)$ для для каждого P_i, где $i = 1, 2$. Тогда возможны подслучаи:

Случай 1.3.1. $S_0(P_i) = D_1$, $S_1^*(P_i) = E$ для для каждого P_i, где $i = 1, 2$. Этот случай рассмотрен в теореме 4.

Случай 1.3.2. $S_0(P_1) = D_3 \supset D_1 = S_1^*(P_1)$ и $S_0(P_2) = D_1 \supset E = S_1^*(P_2)$. Этот случай рассмотрен в теореме 5.

Заметим, что разбиения с условиями 5 и 10 невозможны, поскольку любая попытка построить соответствующее разбиение с двумя классами полных корон радиуса 1 в некоторой вершине не дает сумму подходящих к ней углов, равную 2π.

Случай 2. Пусть имеется разбиение T с одним прототайлом, то есть $P_1 \cong P_2$ для любых P_1 и P_2 из T. Тогда выполняется $N_0 = 1$, $N_1 = 2$. Случаю 2 соответствуют пары 12, 13, 15, 17. Их биправильность доказывается в теореме 6.

Теорема 3. *Пусть T — триангуляция плоскости с двумя прототайлами $\bar{P}_1$ и $\bar{P}_2$ и двумя полными протокоронами радиуса* 1, *причем $S_0(P_1) = S_1^*(P_1)$. Тогда T является биправильным разбиением.*

Теорема 4. *Пусть триангуляция T с двумя прототайлами и двумя полными протокоронами радиуса* 1 *соответствует паре* 15) : $(D_1, E); (D_1, E)$. *Тогда разбиение T является биправильным.*

Теорема 5. *Пусть триангуляция T с двумя прототайлами и двумя полными протокоронами радиуса* 1 *соответствует паре* 8) : $(D_3, D_1); (D_1, E)$. *Тогда разбиение T является биправильным.*

Теорема 6. *Нормальная триангуляция евклидовой плоскости с одним прототайлом и двумя классами полных корон радиуса* 1 *является биправильной.*

Автор благодарен Н. П. Долбилину за постановку задачи и внимание к работе.

Список литературы

1. Делоне Б. Н., Долбилин Н. П., Штогрин М. И., Галиулин Р. В. Локальный критерий правильности системы точек // ДАН СССР. — 1976. — Т. 227, вып. 1. — С. 319–322.

2. Dolbilin N. P. Which clusters can form a crystal? // Voronoi's impact on modern science. — Kyiv, 1998. — Book 2. — P. 96–104.

3. Dolbilin N. P., Schattschneider D. The local theorem for tilings // Quasicrystals and discrete geometry. — 1998. — V. 10. — P. 193–200.

4. Dolbilin N. P., Dress A. W. M., Huson D. H. Two finiteness theorems for periodic tilings of d-dimensional euclidean space // Discrete and Computational Geometry. — 1998. — V. 20. — P. 143–153.

О ПРОБЛЕМЕ ЭРДЕША — СЕКЕРЕША

В. А. Кошелев (Москва)

В 1935 году П. Эрдеш и Д. Секереш сформулировали следующую проблему [1, 2] (первая проблема Эрдеша — Секереша): *для любого целого $n \geq 3$ найти минимальное положительное число $g(n)$, такое, что из любого множества точек на плоскости, находящегося в общем положении и содержащего по крайней мере $g(n)$ точек, можно выбрать подмножество мощности n, элементы которого являются вершинами выпуклого n-угольника.*

В 1978 году Эрдеш предложил следующую модификацию первой проблемы [3] (вторая проблема Эрдеша — Секереша): *для любого целого $n \geq 3$ найти минимальное положительное число $h(n)$, такое, что из любого множества точек X на плоскости, находящегося в общем положении и содержащего по крайней мере $h(n)$ точек, можно выбрать подмножество мощности n, элементы которого являются вершинами выпуклого и пустого n-угольника, то есть этот n-угольник не содержит внутри себя других точек из X.*

Напомним, что множество точек находится в общем положении, если никакие три его элемента не лежат на одной прямой.

Первую проблему Эрдеш и Секереш рассмотрели в статье [1]. Они доказали существование $g(n)$ для произвольного n, обосновав верхнюю оценку $g(n) \leq \binom{2n-4}{n-2} + 1$, а также высказали следующую гипотезу: $g(n) = 2^{n-2} + 1$. Эта гипотеза подтверждена для $n \leq 6$. Здесь случай $g(3) = 3$ очевиден; равенство $g(4) = 5$ было доказано Э. Кляйн в 1935 году; выражение $g(5) = 9$ получил Э. Макаи (см. [2]); факт $g(6) = 17$ считается доказанным, однако соответствующих публикаций нет. Кроме того, в 1961 году Эрдеш и Секереш доказали [2] и нижнюю оценку $g(n) \geq 2^{n-2} + 1$.

Неравенство $g(n) \leq \binom{2n-4}{n-2} + 1$ неоднократно улучшалось. Так, в 1998 году было получено сразу три последовательных улучшения.

Первое из них принадлежит Ф. Чанг и Р. Грэхему [4]: $g(n) \leq \binom{2n-4}{n-2}$. Второе улучшение получили Д. Клейтман и Л. Пахтер [5]: $g(n) \leq \binom{2n-4}{n-2} + 7 - 2n$. Наконец, третье улучшение принадлежит Г. Тоту и П. Вальтру [6]: $g(n) \leq \binom{2n-5}{n-3} + 2$. В 2005 году Тот и Вальтр немного усилили [7] последнее неравенство, заменив его оценкой $g(n) \leq \binom{2n-5}{n-3} + 1$, и это наиболее точный на данный момент результат. Тем самым, гипотеза Эрдеша — Секереша до сих пор не доказана и не опровергнута.

Вторая проблема изучена более глубоко. Для нее равенства $h(3) = 3$ и $h(4) = 5$ очевидны. Выражение $h(5) = 10$ получил Х. Харборт в 1978 году [8]. А в 1983 году Дж. Хортон доказал [9], что $h(n)$ не существует при $n \geq 7$. Вопрос о существовании и значении величины $h(6)$ долгое время оставался открытым. В 2006 году Т. Геркен доказал [10] существование h(6), обосновав верхнюю оценку $h(6) \leq g(9) \leq \binom{13}{6} + 1 = 1717$. Все нижние оценки для $h(6)$ были получены компьютерным перебором. Первая из них [11] принадлежит М. Овермарсу, Б. Шолтен и И. Винсент и относится к 1988 году: $h(6) \geq 27$. Следующая оценка была получена в 2001 году Овермарсом [12], и она является самой лучшей на данный момент: $h(6) \geq 30$. Основной результат настоящей работы сформулирован в следующей теореме.

Теорема. *Имеет место неравенство*

$$h(6) \leq \max\{g(8), 400\} \leq 463.$$

Таким образом, получается, что на сегодняшний день доказаны оценки $30 \leq h(6) \leq 463$. Заметим также, что с историей задач можно ознакомиться, например, по обзору [13].

Настоящая работа выполнена при финансовой поддержке гранта РФФИ номер 06-01-00383.

Список литературы

1. Erdős P., Szekeres G. A combinatorial problem in geometry // Compositio Math. — 1935. — V. 2. — P. 463–470.

2. Erdős P., Szekeres G. On some extremum problems in elementary geometry // Ann. Univ. Sci. Budapest Eötvös Sect. Math. — 1961. — V. 3–4. — P. 53–62.

3. Erdős P. Some more problems in elementary geometry // Austral. Math. Soc. Gaz. — 1978. — V. 5. — P. 52–54.

4. Chung F., Graham R. Forced convex n-gons in the plane // Discrete Comput. Geom. — 1998. — V. 19. — P. 367–371.

5. Kleitman D. Pachter L. Finding convex sets among points in the plane // Discrete Comput. Geom. — 1998. — V. 19. — P. 405–410.

6. Tóth G., Valtr P. Note on the Erdős–Szekeres theorem // Discrete Comput. Geom. — 1998. — V. 19. — P. 457–459.

7. Tóth G., Valtr P. The Erdős–Szekeres theorem: upper bounds and related results // Combinatorial and Computational geometry, MSRI Publication. — 2005. — V. 52. — P. 557–568.

8. Harborth H. Konvexe Fünfecke in ebenen Punktmengen // Elem. Math. — 1978. — V. 33. — P. 116–118.

9. Horton J. D. Sets with no empty 7-gons // Canad. Math. Bull. — 1983. — V. 26. — P. 482–484.

10. Gerken T. On empty convex hexagons in planar point set // Submitted.

11. Overmars M., Scholten B., Vincent I. Sets without empty convex 6-gons // Bull. European Assoc. Theor. Comput. Sci. — 1989. — V. 37. — P. 160–168.

12. Overmars M. Finding sets of points without empty convex 6-gons // Discrete Comput. Geom. — 2003. — V. 29. — P. 153–158.

13. Morris W., Soltan V. The Erdős – Szekeres problem on points in convex position // Bulletin (new series) of the Amer. Math. Soc. — 2000. — V. 37, № 4. — P. 437–458.

ЗАДАЧА О СИММЕТРИИ ДВУХ ТЕЛ

Я. В. Кучериненко (Москва)

Рассматривается взаимосвязь симметрии пары фигур в пространстве $X^d \in S^d, E^d, H^d$ с симметрией каждой из них, а также с симметрией описаний их взаимных расположений.

Из работ [1, 2] следует взаимосвязь всех различных описаний одного и того же взаимного расположения двух фигур. Эти описания можно рассмотреть как движения пространства, которые, вообще говоря, не образуют группу, но сами являются орбитой относительно некоторой вполне определённой группы операторов, зависящей от симметрии рассматриваемых фигур. В данной работе обнаружена взаимосвязь группы операторов, сохраняющих движение, задающее взаимное расположение фигур (группы стабилизатора орбиты) с группой симметрии рассматриваемой пары фигур. Доказана теорема об изоморфизме этих двух групп. В частном случае, рассматривающем взаимную ориентацию двух фигур в трехмерном евклидовом пространстве, движения их симметрии представимы в виде

кватернионов, которые, в свою очередь можно изобразить точками на трёхмерной сфере. Тогда рассмотренная выше группа операторов есть точечная группа симметрии, действующая на трёхмерной сфере. Для этого случая удалось не только доказать изоморфизм стабилизатора орбиты с группой симметрии пары фигур, но и объяснить геометрическое сходство этих двух групп.

Автор благодарит профессоров Н. П. Долбилина и В. С. Макарова за обсуждение работы и ценные замечания.

Список литературы

1. Кучериненко Я. В. О взаимной ориентации двух фигур в R^3 // Материалы VII Международного семинара "Дискретная математика и ее приложения" (29 января – 2 февраля 2001 г.). Часть 2. — М.: Изд-во механико-математического факультета МГУ, 2001. — С. 268–270.

2. Кучериненко Я. В. О взаимном расположении двух фигур в пространствах постоянной кривизны // Материалы VIII Международного семинара "Дискретная математика и ее приложения" (2–6 февраля 2004 г.). — М.: Изд-во механико-математического факультета МГУ, 2004. — С. 398–401.

О НЕКОТОРЫХ ОБОБЩЕННЫХ ПРАВИЛЬНЫХ МНОГОГРАННИКАХ ПРОСТРАНСТВА ЛОБАЧЕВСКОГО

В. С. Макаров (Москва)

Напомним, следуя [1], построение правильных бесконечных многогранников пространства Лобачевского. Относительно легко показать, что на эквидистантной поверхности как и на орисфере вершины правильного (конечного) геодезического многоугольника лежат в одной плоскости. Но внутренняя геометрия орисферы — эвклидова, а эвклидова плоскость правильно разбивается на равные конечные правильные многоугольники только трех видов: треугольники, квадраты или шестиугольники. Переходя от геодезических многоугольников к обычным линейным, мы получим три (вписанных в орисферу) правильных многогранника с бесконечным числом граней. Здесь и далее правильность многогранника (и правильность разбиения) понимается в смысле возможности совмещения любых его флагов движением из группы симметрии многогранника (разбиения).

На эквидистантной поверхности внутренняя геометрия — планиметрия Лобачевского. Как показывает В. Ф. Каган, при ортогональном проектировании правильного разбиения этой поверхности равными конечными геодезическими правильными многоугольниками на базовую плоскость на последней образуется аналогичное правильное разбиение плоскости на равные правильные многоугольники и, обратно, всякое правильное разбиение базы на конгруэнтные конечные правильные многоугольники можно "поднять" (при помощи прямых цилиндров) на эквидистантную поверхность. Вопрос о разбиении Λ^2 на равные (конечные) правильные многоугольники решается легко: угол m-угольника на Λ^2 монотонно убывает от его эвклидовой величины до нуля при возрастании радиуса R описанной около многоугольника окружности от нуля до бесконечности. Например, для треугольника его угол меняется от $2\pi/6$ до нуля и, следовательно, проходит через значения $2\pi/7$, $2\pi/8$, $2\pi/9$,..., откуда следует, что Λ^2 разбивается на треугольники, которые сходятся в узлах разбиения по k штук, где $k = 7, 8, 9, ...$ (при $m = 4$ — $k = 5, 6, 7, ...$; при $m = 5, 6$ — $k = 4, 5, 6, ...$; при $m \geq 7$ — $k = 3, 4, 5, ...$). "Поднимая" такие разбиения на эквидистантные поверхности и переходя к плоским многоугольникам, мы получаем бесконечные серии правильных многогранников, вписанных в эквидистантную поверхность. Отметим здесь же, что отражением в базовой плоскости поверхности такого многогранника мы получаем (между исходной поверхностью и ее образом) новый правильный многогранник, вписанный в пару эквидистантных поверхностей (назовем его линзой).

Вернемся, однако, к Λ^2. Разбив орицикл на равные дуги и соединив последовательно точки дробления, мы получим на Λ^2 правильный бесконечный многоугольник, вписанный в орицикл. Проделав тоже самое с эквидистантой, мы получим бесконечный правильный многоугольник, вписанный в эквидистанту. Если возьмем пару конгруэнтных эквидистант с общей базой и проделаем аналогичную операцию не нарушая симметрию в осях, ортогональных базе, то получим двумерную линзу. Легко видеть, что угол любого из этих правильных многоугольников (непрерывно и монотонно) меняется от π до 0 при возрастании соответствующих метрических параметров и, следовательно, такие правильные многоугольники правильно разбивают Λ^2, сходясь по k в узлах разбиения, $k = 3, 4, 5, ...$

Отметим одну интересную деталь. Если разбить Λ^2 на односторонние правильные эквидистантные многоугольники, то не трудно заметить, что база эквидистант при этом формируют бесконечный правильный выпуклый "разветвленный" "многоугольник", описанный около правильной системы окружностей плоскости Λ^2. Все ре-

бра разбиения оказываются внутри этого многоугольника. Ребрами "разветвленного" "многоугольника" являются прямые, вершины отсутствуют (его правильнее было бы назвать многосторонником [2]). Не трудно видеть, что аналогичные многосторонники могут быть описаны и около других правильных систем кривых постоянной кривизны на Λ^2. Если границу каждого эквидистантного (одностороннего) многоугольника отразить в его базе, то образы этих границ сформируют бесконечный правильный выпуклый "разветвленный" многоугольник (с ребрами — отрезками и конечными вершинами), так же описанный около правильной системы окружности на Λ^2.

Используем полученные разбиения Λ^2 для построения новых правильных многогранников в Λ^3. Для простоты, рассмотрим лишь случай разбиения Λ^2 на односторонние эквидистантные многоугольники, считая, что в узле разбиения сходится по три многоугольника. Восстановив в узлах разбиения плоскости нормали, отложив на них (с одной стороны от плоскости) отрезки равной длины H и соединив "соседние" концы отрезками, мы получим бесконечный правильный трехмерный многогранник. Гранями этого многогранника являются (односторонние) правильные эквидистантные многоугольники. Их базы совпадают с базами тех многоугольников плоскости, над которыми они построены. Плоскости этих граней пересекают базовую плоскость по указанным прямым. Его многогранные углы — правильные тригоноэдры. При возрастании высоты H эквидистантной поверхности от нуля до бесконечности двугранный угол многогранника убывает от π до $2\pi/6$ и, следовательно, при некотором $H = H_0$ он становится равным $2\pi/3$. При таких размерах этот новый правильный эквидистантногранный многогранник разбивает Λ^3 и при этом в узлах разбиения многогранники сходятся симплициально. Это позволяет над полученным разбиением Λ^3 построить правильный четырехмерный многогранник с симплициальными гоноэдрами. Величина двугранного угла этого многогранника меняется от π до $\alpha_3 < \pi/2$ (где $\alpha_3 \approx 70.5^0$ — двугранный угол правильного трехмерного эвклидова симплекса). Это позволяет получить разбиение Λ^4 на такие многогранники; в узлах разбиения схождение гоноэдров опять симплициальное. Сделать шаг индукции от $(n-1)$ к n оставим читателю. В заключение отметим лишь, что из любого (в том числе и вновь построенного) n-мерного правильного многогранника "ортогональным усечением" легко строятся "разветвленные" правильные многогранники, аналогичные указанным на Λ^2.

Работа поддержана грантом РФФИ — АН Молдовы 06-01-90-845 и грантом РФФИ 05-01-00170.

Список литературы

1. Каган В. Ф. Основания геометрии. Т. I. — М.—Л.: ГТТЛ, 1949.

2. Заморзаев А. М. О правильных многосторонниках и многогранниках пространства Лобачевского // Уч. зап. Кишиневского ун-та. — 1959. — Т. 39. — С. 195–206.

ТРЕХМЕРНЫЕ ЭКВИДИСТАНТНЫЕ ПРАВИЛЬНЫЕ ЗВЕЗДНЫЕ МНОГОГРАННИКИ ПРОСТРАНСТВА ЛОБАЧЕВСКОГО

П. В. Макаров (Москва)

Известно, что звездных многогранников, вписанных в сферу (так сказать сферических) всего четыре. Два из них были указаны И. Кеплером, а два других — Л. Пуансо. Полнота этого списка была доказана О. Коши. Но, как и в случае выпуклых правильных многогранников, не лишено смысла рассмотреть вопрос о существовании звездных правильных многогранников с бесконечным числом граней, вписанных в орисферу или эквидистантную поверхность (или, быть может, только описанных около одной из них). Для этого, придерживаясь схемы вывода правильных сферических звездных многогранников, естественным образом вводится понятие ядра правильного многогранника, как пересечения подпространств, определяемых плоскостями граней и центром (бесконечно удаленным или идеальным). Проверяется, что ядро — выпуклый правильный многогранник с тем же числом сторон у грани и с бесконечным числом граней. Так как грани ядра лежат в тех же плоскостях, что и грани исходного многогранника, то вид звездного многогранника будет определятся тем, какие из этих плоскостей будут определять смежные грани звездного многогранника. При этом представляются две возможности: 1) смежными в звездном являются грани, которые смежны и в исходном правильном выпуклом многограннике (т. е. ядре); тогда ребра звездного многогранника лежат на тех же прямых, что и ребра ядра, и грань звездного получается путем продолжения ребер ядра (так сказать, “озвездением” граней); при этом грани звездного — звездчатые многоугольники; 2) смежными гранями в звездном являются не смежные грани ядра; в этом случае надо взять плоскость грани ядра и пересечь ее с подходяще подобранными плоскостями не смежных по ребру граней ядра (при этом число выбранных граней ядра должно равняться числу сторон

у грани ядра и выбранные грани должны быть одинаково расположенными относительно друг друга); грани звездного при этом могут оказаться как выпуклыми, так и звездчатыми. Ко всему этому нужно добавить, что, находясь в пространстве Лобачевского, мы должны еще весьма внимательно следить за поведением рассматриваемых объектов (прямых, плоскостей): а пересекаются ли они? Но первое, в чем следует убедиться, так это в вопросе существования таких звездных правильных многогранников с бесконечным числом (равных правильных) конечных граней. Нет ничего лучшего, как убедится в их существовании на конкретных примерах, пару из которых мы и приводим ниже.

Возьмем разбиение плоскости Лобачевского Λ^2 на правильные равные выпуклые семиугольники, сходящиеся по три в узле разбиения (о существовании такого см. [1, с. 441]) и "озвездим" его клетки, беря пересечения сторон через одну (т. е. продолжая первую сторону до пересечения с третьей и с предпоследней, вторую — до пересечения с четвертой и с последней и т. д.). Тогда каждый 7-угольник породит звездный 7-угольник $\{7/2\}$. Если же мы всю эту конструкцию из звездных 7-угольников поднимем на эквидистантную поверхность, то получим вписанный в эквидистантную поверхность правильный звездный бесконечный эквидистантный многогранник $\{7/2, 7\}$ (символика Шлефли), гранями которого будут указанные звездные 7-угольники. В вершинах они будут образовывать семигранные правильные выпуклые гоноэдры. Читателю рекомендуется нарисовать фрагмент такого многогранника, используя соответствующий фрагмент разбиения $\{7, 3\}$ плоскости Лобачевского Λ^2.

Если же мы поступим с разбиением $\{7, 3\}$ плоскости Лобачевского Λ^2 таким же образом, как поступали с разбиением сферы на пятиугольники, т. е. с правильным додекаэдром, при получении из него звездного додекаэдра $\{5, 5/2\}$, то мы очевидно получим над правильным эквидистантным многогранником звездный эквидистантный многогранник $\{7, 7/2\}$. Читатель может легко представить себе его фрагмент (вместе с соответствующим фрагментом ядра); рисунки указанных фрагментов даны в [2].

Оставляя в стороне орисферические многогранники, остановимся лишь на эквидистантных. Отметим, что если рассматривается правильное разбиение плоскости на равные выпуклые правильные нечетноугольники, сходящиеся по три в узле (или же, сразу, разбиение эквидистантной поверхности на геодезические правильные выпуклые нечетноугольники), то картина в принципе ничем не отличается от рассмотренных выше примеров (разбиения на четноугольники приводит, при указанной схеме схождения в узлах, к распа-

дению четноугольника на пару выпуклых правильных многоугольников). К сожалению, здесь приходится сразу отметить, что если в узле разбиения Λ^2 на выпуклые правильные многоугольники сходится четыре или более многоугольника или же мы стороны берем не "через одну", то ничего хорошего не получается. Оказывается, что тогда рассматриваемые прямые, на которых лежат ребра, не пересекаются, что доказать не столь уж сложно.

Действительно, если в узлах разбиения сходится четыре или более выпуклых правильных k-угольников ($k \geq 7$, k — нечетное), то прямые образуют со стороной, соединяющей вершины продолжаемых ребер, нетупые углы (при $k = 4$ углы прямые, при $k \geq 5$ — острые). Тогда, соединяя отрезком две другие вершины рассматриваемых сторон, мы видим, что получили аналог равнобочной трапеции все углы которой — острые. Из этого следует, что прямые, на которых лежат продолжаемые стороны, расходятся (общий перпендикуляр рассматриваемых прямых должен располагаться со стороны острых углов как относительно верхнего, так и относительно нижнего оснований трапеции). Ровно таким же образом доказывается, что расходятся и пары сторон выпуклого правильного многоугольника, разбивающего Λ^2 симплициально (т. е. в узлах разбиения многоугольники сходятся по три), если эти пары сторон не соединены одной стороной, т. е. при построении звездчатой грани (при "звездении") пропускается не одна, а две или более сторон (это легко следует из подсчета величин углов аналогичной равнобочной трапеции с учетом того, что угол нечетноугольника равен $2\pi/3$, ибо в узле сходится три таких многоугольника). Не имея возможности остановиться здесь подробнее на втором пути получения звездных бесконечногранных многогранников (рассмотрение вопроса занимает много страниц), все же позволим себе отметить факт существования описанных, но не вписанных в эквидистантную поверхность звездных многогранников: достаточно "загнать" вершины звездного на абсолют (аналогичное утверждение верно, конечно, и для сферических звездных многогранников Кеплера — Пуансо).

Работа поддержана грантом РФФИ — АН Молдовы 06-01-90-845.

Список литературы

1. Каган В. Ф. Основания геометрии. Т. I. — М.—Л.: ГТТЛ, 1949.

2. Дамиан Ф. Л., Макаров П. В. О правильных звездных многогранниках в пространстве Лобачевского // Труды II Всероссийской научной школы "Математические исследования в кристаллографии, минералогии и петрографии". — Апатиты: K & M, 2006. — С. 58–60.

О ВЛОЖИМОСТИ КОНЕЧНЫХ ГРАФОВ РАССТОЯНИЙ С БОЛЬШИМ ХРОМАТИЧЕСКИМ ЧИСЛОМ В СЛУЧАЙНЫЕ ГРАФЫ

С. В. Нагаева (Москва)

Настоящая работа возникла в связи с известной задачей Нельсона — Эрдеша — Хадвигера, которая состоит в отыскании *хроматического числа* $\chi(\mathbb{R}^d)$ *евклидова пространства* $\mathbb{R}^d$. Напомним, что

$$\chi(\mathbb{R}^d) = \min\{\chi : \exists X_1, ..., X_\chi, \mathbb{R}^d = X_1 \sqcup X_2 \sqcup ... \sqcup X_\chi,$$
$$\forall i = 1, .., \chi, \ \ \forall \overline{x}, \overline{y} \in X_i \ \ |\overline{x} - \overline{y}| \neq 1\}.$$

Можно переформулировать проблему Нельсона — Эрдеша — Хадвигера в терминах теории графов. Для этого рассмотрим (бесконечный) *полный граф расстояний* $\mathbf{G}^d = (\mathbf{V}^d, \mathbf{E}^d)$, у которого множество вершин $\mathbf{V}^d$ совпадает с $\mathbb{R}^d$, а множество ребер $\mathbf{E}^d$ имеет вид:

$$\mathbf{E}^d = \{(\overline{x}, \overline{y}) \in \mathbf{V}^d \times \mathbf{V}^d : |\overline{x} - \overline{y}| = 1\}.$$

Ясно, что $\chi(\mathbb{R}^d) = \chi(\mathbf{G}^d)$, где $\chi(\mathbf{G}^d)$ — обычное хроматическое число графа $\mathbf{G}^d$ (см. [1]). Более того, $\chi(\mathbf{G}^d) = \max\limits_G \chi(G)$, где максимум берется по всем конечным подграфам полного графа расстояний $\mathbf{G}^d$ (см. [2]). Такие конечные графы мы будем называть *конечными графами расстояний*.

Относительно проблемы Нельсона — Эрдеша — Хадвигера в разное время были получены многочисленные результаты [3, 4]. Зазор между нижними и верхними оценками велик даже для случая $d = 2$ ($4 \leq \chi(\mathbb{R}^2) \leq 7$ (см. [5, 6])), а при $d \to \infty$ этот зазор растет экспоненциально ($((1.239... + o(1))^d \leq \chi(\mathbb{R}^d) \leq (3 + o(1))^d, d \to \infty$ (см. [3, 7])). В связи с этим в работах [8–10] А. М. Райгородский ввел некоторую величину, в определенном смысле характеризующую трудность отыскания в $\mathbb{R}^d$ конечного графа расстояний с большим хроматическим числом. Определим эту величину.

Обозначим через $G(n, p) = (\Omega_n, \mathcal{B}_n, P_n)$ вероятностное пространство *случайных графов* с n вершинами и вероятностью ребра $p = p(n)$ (ребра выбираются независимо друг от друга, см. [11]). Пусть χ_d — это самая лучшая известная нижняя оценка величины $\chi(\mathbb{R}^d)$. Например, $\chi_2 = 4$. Для каждого $k = 1, ..., n$ рассмотрим свойство Q_k случайного графа: в графе $G = (V, E) \in \Omega_n$ существует такой

индуцированный подграф $H = (U, F)$, что $|U| = k$, $\chi(H) \geq \chi_d$ и H изоморфен некоторому конечному графу расстояний. Положим

$$t(d,n,p) = \begin{cases} 0, & \text{если } \{k \in \{1,..,n\} : P_n(Q_k) \geq \frac{1}{2}\} = \emptyset; \\ \max\{k \in \{1,..,n\} : P_n(Q_k) \geq \frac{1}{2}\}, & \text{иначе.} \end{cases}$$

В работах [8–10] дана мотивировка рассмотрения величины $t(d,n,p)$ и получен ряд оценок этой величины. В данной заметке нас будут интересовать верхние оценки $t(d,n,p)$. Смысл подобных оценок пояснить несложно. Допустим, $t(d,n,p) < k$, тогда $P_n(Q_k) < \frac{1}{2}$. Каждому конечному графу расстояний $H = (U, F)$ в $\mathbb{R}^d$, у которого $|U| \geq k$ и $\chi(H) \geq \chi_d$, сопоставим множество $A(H) \in \mathcal{B}_n$ таких графов $G \in \Omega_n$, что G содержит изоморфную копию H в качестве индуцированного подграфа. Получается, что $P_n\left(\bigcup\limits_H A(H)\right) < \frac{1}{2}$. Иными словами, несмотря на то, что, казалось бы, графов H, обладающих указанными свойствами много, и каждому из них отвечает достаточно богатое множество $A(H)$, мера объединения всех таких множеств $A(H)$ сравнительно мала. Это косвенно свидетельствует о том, что в $\mathbb{R}^d$ мало попарно неизоморфных графов расстояний с большим хроматическим числом и количеством вершин $\geq k$.

Далее мы приведем некоторые верхние оценки величины $t(d,n,p)$. Следующие две теоремы доказаны А. М. Райгородским в [10].

Теорема 1. *Пусть $l = l(n,p)$ — это любая функция, с которой имеет место асимптотическое выражение $C_n^l(1-p)^{C_l^2} \to 0, n \to \infty$. Тогда $t(d,n,p) \leq l\chi(\mathbb{R}^d)$.*

Теорема 2. *Пусть $m = m(n)$ — это некоторая целочисленная функция, удовлетворяющая условиям $m \in \{1,...,n\}, m \to \infty$ при $n \to \infty$. Для каждого m определим $k_0 = k_0(m)$ из неравенств $C_m^{k_0} 2^{-C_{k_0}^2} < 1 < C_m^{k_0-1} 2^{-C_{k_0-1}^2}$ и положим $k_1 = k_0 - 4$. Допустим, что для любого $\delta = \delta(n) = o(1)$ выполнено $C_n^m e^{-\frac{m^2}{4k^8}(1+\delta)} \to 0$ при $n \to \infty$ и что $k_1(m) \geq d + 2 = d(n) + 2$. Тогда $t(d,n,\frac{1}{2}) \leq m$.*

Из теоремы 1 нетрудно получить

Следствие. *Имеет место неравенство*

$$t(d,n,p) \leq 2\chi(\mathbb{R}^d)\frac{\ln n}{\ln \frac{1}{1-p}} + 1.$$

Основной результат настоящей работы сформулирован в следующей теореме.

Теорема 3. *Для любых* n *и* $d = d(n)$:

$$\text{если } p < \left(\frac{(2(d+2)!)^{\frac{1}{d}}}{(d+2)^{8+\frac{4}{d}}\ln n}\right)^{\frac{2}{d-1}}, \text{ то } t(d,n,p) < \left(\frac{2(d+2)!}{(d+2)^4}\right)^{\frac{1}{d}}\left(\frac{1}{p}\right)^{\frac{d+3}{2}};$$

$$\text{если } p \geq \left(\frac{(2(d+2)!)^{\frac{1}{d}}}{(d+2)^{8+\frac{4}{d}}\ln n}\right)^{\frac{2}{d-1}}, \quad \text{то } t(d,n,p) < \left(\frac{1}{p}\right)^2 (d+2)^8 \ln n.$$

Список литературы

1. Харари Ф. Теория графов — М., Мир. — 1973.
2. De Bruijn N. G., Erdös P. A colour problem for infinite graphs and a problem in the theory of relations // Proc. Koninkl. Nederl. Acad. Wet., Ser. A. — 1951. — V. 54, № 5. — P. 371–373.
3. Райгородский А. М. Проблема Борсука и хроматические числа некоторых метрических пространств // Успехи математических наук. — 2001. — Т. 56, № 1. — С. 107–146.
4. Brass P., Moser W., Pach J. Research problems in discrete geometry. — Springer, 2005.
5. Moser L., Moser W. Solution to problem 10 // Canad. Math. Bull. — 1961. — V. 4. — P. 187–189.
6. Hadwiger H. Unelöste Probleme N 40 // Elemente der Math. — 1961. — V. 16. — P. 103–104.
7. Larman D. G., Rogers C. A. The realization of distances within sets in Euclidean space // Mathematika. — 1972. — V. 19. — P. 1–24.
8. Райгородский А. М. Проблема Нельсона — Эрдеша — Хадвигера и вложения случайных графов в геометрический // Доклады РАН. — 2005. — Т. 403, № 2. — С. 169–171.
9. Райгородский А. М. Раскраски пространств и случайные графы // Фундаментальная и прикладная математика. — 2005. — Т. 11, № 6. — С. 131–141.
10. Райгородский А. М. Проблема Нельсона — Эрдеша — Хадвигера и реализация случайного графа в пространстве // УМН. — 2006. — Т. 61, № 4. — С. 195–196.
11. Bollobás B. Random graphs. — Cambridge Univ. Press, 2001.

О НЕКОТОРЫХ КЛАССАХ ЦЕНТРАЛЬНО-СИММЕТРИЧНЫХ МНОГОГРАННИКОВ

М. С. Панов (Москва)

В данной работе исследуются вопросы, связанные со старой нерешенной проблемой: доказать, что у выпуклого d-мерного центрально-симметричного многогранника общее число граней не меньше 3^d.

Р. Стэнли [1], создав мощный алгебро-комбинаторный метод, доказал справедливость этой гипотезы для симплициальных и, соответственно, дуальных им простых многогранников. Симплициальный кросс-политоп и дуальный ему простой куб имеют 3^d граней каждый. Назовем центрально-симметричный выпуклый d-многогранник с 3^d гранями критическим. Ясно, что класс $\mathbb{K}$, состоящий из кубов и кросс-политопов и всех центрально симметричных многогранников, получающихся из них путем взятия дуального многогранника и прямого произведения, состоит из критических многогранников. Д. Калаи [2] предположил, что других критических многогранников нет.

В работе Н. П. Долбилина [3], при обобщении теорем Минковского о параллелоэдрах, была найдена связь между локальной структурой разбиений пространства на параллелоэдры и между выпуклыми центрально-симметричными многогранниками со следующим свойством антиподальности: для каждой гиперграни многогранника лишь симметричная ей гипергрань не пересекается с изначальной. Н. П. Долбилин поставил задачу: исследовать класс $\mathbb{K}$ и выяснить, не совпадает ли он с классом $\mathbb{D}$ типов многогранников, обладающих свойством антиподальности. Эта задача тесно связана с нерешенной пока задачей классификации локального устройства разбиений на параллелоэдры в максимальных общих гранях.

В данной работе нас интересуют прежде всего комбинаторные типы. Многогранники будем обозначать прописными латинскими буквами, а их комбинаторные типы соответствующими прописными готическими буквами. Рассмотрим следующую ситуацию:

Пусть дано пространство $\mathbb{R}^d$. Пусть $\mathbb{R}^k$ и $\mathbb{R}^l$, $k+l=d$ — его подпространства, размерностей k и l соответственно, $\mathbb{R}^k \cap \mathbb{R}^l = \{0\}$ и $\mathbb{R}^k \perp \mathbb{R}^l$. Пусть $A \subset \mathbb{R}^k$ и $B \subset \mathbb{R}^l$ — центрально-симметричные многогранники размерностей k и l, соответственно, такие, что их центры симметрии совпадают с 0.

Определение. *Будем говорить, что тип* $\mathfrak{C}$ *является прямым произведением типов* $\mathfrak{A}$ *и* $\mathfrak{B}$, *и писать* $\mathfrak{C} = \mathfrak{A} \otimes \mathfrak{B}$, *если существуют многогранники* C, A *и* B, *представляющие данные типы, расположенные так, как описанно выше, при условии, что* $C = A \otimes B$.

Определение. *Запись* $C = CH(A, B)$ *означает, что* A *и* B *расположены так, как описано выше, и* $C = conv\{A, B\}$.

Будем говорить, что тип $\mathfrak{C}$ *является оболочкой типов* $\mathfrak{A}$ *и* $\mathfrak{B}$ *и писать* $\mathfrak{C} = CH(\mathfrak{A}, \mathfrak{B})$, *если существуют многогранники* C, A *и* B, *представляющие данные типы, такие, что* $C = CH\{A, B\}$.

Определение. *Будем говорить, что многогранник* $D \subset \mathbb{R}^d$ *является двойственным (или дуальным) к многограннику* $C \subset \mathbb{R}^d$, $0 \in intC$, *если выполнено равенство* $D = \{y \in \mathbb{R}^d \mid \forall x \in C\ (x, y) \leq 1\}$, *где* (x, y) *обозначает евклидово скалярное произведение двух векторов. Двойственный к* C *многогранник будем обозначать* C^*.

При этом комбинаторные типы многогранников C и C^* двойственны в обычном смысле.

Теперь дадим индуктивные определения класса комбинаторных типов $\mathbb{K}$ и класса комбинаторных типов $\mathbb{M}$.

Определим *класс* $\mathbb{K}$, как минимальное множество всех типов многогранников со следующими свойствами:

1) класс отрезка принадлежит $\mathbb{K}$;

2) если $\mathfrak{A} \in \mathbb{K}$, то $\mathfrak{A}^* \in \mathbb{K}$;

3) если $\mathfrak{A} \in \mathbb{K}$ и $\mathfrak{B} \in \mathbb{K}$, то $\mathfrak{A} \otimes \mathfrak{B} \in \mathbb{K}$.

Определим *класс* $\mathbb{M}$, как минимальное множество всех типов многогранников со следующими свойствами:

1) класс отрезка принадлежит $\mathbb{M}$;

2) если $\mathfrak{A} \in \mathbb{M}$ и $\mathfrak{B} \in \mathbb{M}$, то $\mathfrak{A} \otimes \mathfrak{B} \in \mathbb{M}$;

3) если $\mathfrak{A} \in \mathbb{M}$ и $\mathfrak{B} \in \mathbb{M}$, то $CH(\mathfrak{A}^*, \mathfrak{B}^*) \in \mathbb{M}$.

Теорема. *Справедливы равенства*:

$$CH(\mathfrak{A}, \mathfrak{B}) = (\,\mathfrak{A}^* \otimes \mathfrak{B}^*\,)^*,$$

$$\mathfrak{A} \otimes \mathfrak{B} = (\,CH(\mathfrak{A}^*, \mathfrak{B}^*)\,)^*.$$

Из этой теоремы следует, что классы $\mathbb{K}$ и $\mathbb{M}$ совпадают. Действительно, то, что $\mathbb{M} \subset \mathbb{K}$ сразу следует из первого равенства теоремы. Обратное включение доказывается индукцией по размерности типов многогранников при помощи второго равенства теоремы. Это позволяет переформулировать предположение Калаи в терминах операции $\otimes$ и CH.

Также возникает множество проблем связанных с этим операциями в классе $\mathbb{K}$. Например, квадрат может быть представлен как прямое произведение двух отрезков и как результат применения операции CH к двум отрезкам. Однако, не ясно, существуют ли в классе $\mathbb{K}$ еще какой-нибудь тип, отличный от типа квадрата, который можно представить как прямое произведение двух типов и как результат применения операции CH к некоторым типам.

Список литературы

1. Stanley R. Combinatoric and commutative algebra. — Birkhauser, 1996.

2. Kalai G. The number of faces of centrally-symmetric polytopes // Graphs and combinatorics. — 1989. — V. 5.

3. Долбилин Н. П. Теоремы Минковского о выпуклых многогранниках и параллелоэдрах и их обобщения // УМН. — 2007. — Вып. 4 (в печати).

ОБ ОДНОЙ СЕРИИ ЗАДАЧ, СВЯЗАННЫХ С ПРОБЛЕМАМИ БОРСУКА И НЕЛСОНА — ЭРДЕША — ХАДВИГЕРА

А. М. Райгородский, М. М. Китяев (Москва)

Широко известны две старые проблемы комбинаторной геометрии — проблема Борсука и проблема Нелсона — Эрдеша — Хадвигера. Проблема Борсука была сформулирована [1] в 1933 году, и состоит она в отыскании минимального числа $f(n)$ частей меньшего диаметра, на которые разбивается произвольное ограниченное неоднородное множество в евклидовом пространстве $\mathbb{R}^n$. Величина $f(n)$ называется *числом Борсука*. Проблема Нелсона — Эрдеша — Хадвигера возникла на рубеже 40-х и 50-х годов XX века. Она сводится к определению величины $\chi(\mathbb{R}^n)$, равной наименьшему количеству цветов, в которые можно так покрасить все точки пространства $\mathbb{R}^n$, чтобы точки одного цвета не могли отстоять друг от друга на расстояние 1. Величина $\chi(\mathbb{R}^n)$ называется *хроматическим числом пространства*. К настоящему времени существует обширная литература по обеим задачам [2–7]. Здесь мы лишь заметим, что наилучшие на данный момент оценки рассмотренных выше величин имеют вид

$$(1.225... + o(1))^{\sqrt{n}} \leq f(n) \leq (1.224... + o(1))^n,$$

$$(1.239... + o(1))^n \leq \chi(\mathbb{R}^n) \leq (3 + o(1))^n.$$

Нижние оценки в обоих случаях принадлежат А. М. Райгородскому [4]; верхняя оценка числа Борсука доказана О. Шраммом в [8]; верхняя оценка хроматического числа установлена Д. Ларманом и К. А. Роджерсом в [9].

Определим величину $\chi(n, a, d)$ как минимальное число цветов, в которые можно так покрасить все точки произвольного множества

$\Omega \subset \mathbb{R}^n$, имеющего диаметр d, чтобы между точками одного цвета не было расстояния a. Понятно, что, не ограничивая общности, можно изучать величину $\chi(n, a, 1)$, где, разумеется, $a \in (0, 1]$. Очевидно, что при $a = 1$ получается аналог числа Борсука, а при $a \to 0$ — аналог хроматического числа пространства. В целом же, возникает серия новых задач, которые образуют нечто вроде "непрерывной цепочки", соединяющей две классические проблемы.

Относительно поведения величины $\chi(n, a, 1)$ удается доказать ряд нетривиальных результатов. Мы не станем приводить в этой краткой заметке самые общие и точные оценки. Мы лишь сформулируем ниже две наиболее показательные теоремы.

Теорема 1. *Возможны два случая.*

1. *Положим* $b = \left[\frac{n}{2}\right]$. *Рассмотрим любое простое* $p = p(n)$, *для которого* $b - 2p < 0$ *и* $p \leq b$. *Пусть* $l = l(n) = b - p$, $a = a(n) = \sqrt{\frac{b-l}{b}}$. *Тогда верно неравенство* $\chi(n, a, 1) \geq C_n^b \Big/ \sum\limits_{i=0}^{p-1} C_n^i$.

2. *Пусть* $d \in \mathbb{N}$, *а* $n = d^2$. *Положим* $b = \left[\frac{d}{2}\right]$. *Рассмотрим любое простое* $p = p(d) = p(n)$, *лежащее в интервале* $\left(\frac{d}{4}, \frac{d}{4} + \varphi(d)\right)$, *где* $\varphi(d)$ — *произвольная функция вида* $\varphi(d) = o(d)$. *Пусть* $\xi = \min |(\mathbf{x}, \mathbf{y})|$; *здесь минимум скалярных произведений берется по всем парам* d-*мерных* $(-1, 1)$-*векторов, у каждого из которых первая координата равна* 1, *а число положительных координат равно* b. *Возьмем* $a = a(d) = a(n) = \sqrt{\frac{d^2-(d-4p)^2}{d^2-\xi^2}}$. *Тогда верно неравенство* $\chi(n, a, 1) \geq (\gamma + o(1))^{\sqrt{n}}$, *где* $\gamma > 1$ — *абсолютная постоянная.*

Теорема 2. *Положим* $b = \left[\frac{n}{4}\right]$. *Рассмотрим любое простое* $p = p(n)$, *для которого* $l = l(n) = 2b - p < 0$. *Пусть* $a = a(n) = \sqrt{\frac{2b-l}{4b}}$. *Тогда верно неравенство* $\chi(n, a, 1) \geq C_n^{2b} C_{2b}^b \Big/ \sum\limits_{q=0}^{p-1} \sum\limits_{i=0}^{\left[\frac{q}{2}\right]} C_n^i C_{n-i}^{q-2i}$.

Обе теоремы доказываются с помощью линейно-алгебраического метода в комбинаторике [6, 10]. Заметим, что каждая из этих теорем применима, конечно, далеко не ко всем значениям $a \in (0, 1]$. Данная проблема (не без труда) преодолевается, и здесь мы об этом более подробно говорить не станем.

Смысл теорем, несмотря на кажущуюся громоздкость их формулировок, пояснить не сложно. В самом деле, предположим, что, например, в теореме 1 выполнено $l \gg \sqrt{n}$. Тогда, как показывает

стандартный анализ вкупе с формулой Стирлинга, оценка из первой части формулировки сильнее оценки из второй части. Далее, если $l \asymp n$, то оценка принимает вид $(c + o(1))^n, c > 1$. Однако понятно, что, чем больше l, тем ближе a к нулю, а стало быть, тем ближе наша задача к задаче Нелсона — Эрдеша — Хадвигера. Таким образом, оценка, полученная в первой части теоремы 1, полностью соответствует нашим ожиданиям, ведь, как мы помним, $\chi(\mathbb{R}^n) \geq (1.239... + o(1))^n$. С другой стороны, если $l \ll \sqrt{n}$, то вторая часть теоремы 1 содержит более точный результат. В то же время, при малых l величина a асимптотически равна единице, и всякое a из второй части формулировки этим свойством обладает. Значит, мы имеем дело с аналогом проблемы Борсука. А для нее как раз верна оценка $f(n) \geq (1.225... + o(1))^{\sqrt{n}}$. Итак, в теореме 1 мы фактически имеем плавный переход от результатов, касающихся проблемы Нелсона — Эрдеша — Хадвигера, к результатам, связанным с задачей Борсука, причем величина $\chi(n, a, 1)$ становится практически неотличимой от числа Борсука уже при $a = 1 - O\left(\frac{1}{\sqrt{n}}\right)$ и практически неотличимой от хроматического числа пространства при $a = \text{const} < 1$. Подчеркнем, что в наших рассмотрениях величина a вполне может зависеть от n и самые интересные эффекты, наиболее точно отражающие переход от проблемы Борсука к проблеме Нелсона — Эрдеша — Хадвигера, наблюдаются именно при $a = \text{const} + o(1)$.

Список литературы

1. Borsuk K. Drei Sätze über die n-dimensionale euklidische Sphäre // Fundamenta Math. — 1933 — V. 20. — P. 177–190.

2. Райгородский А. М. Хроматические числа. — М.: МЦНМО, 2003.

3. Райгородский А. М. Проблема Борсука. — М.: МЦНМО, 2006.

4. Болтянский В. Г., Гохберг И. Ц. Теоремы и задачи комбинаторной геометрии. — М.: Наука, 1965.

5. Boltyanski V. G., Martini H., Soltan P. S. Excursions into combinatorial geometry. — Berlin: Springer, 1997.

6. Райгородский А. М. Проблема Борсука и хроматические числа некоторых метрических пространств // Успехи матем. наук — 2001 — Т. 56, вып. 1. — P. 107–146.

7. Сойфер А. Хроматическое число плоскости: его прошлое, настоящее и будущее // Матем. просвещение — 2004 — вып. 8.

8. Schramm O. Illuminating sets of constant width // Mathematika — 1988 — V. 35. — P. 180–189.

9. Larman D. G., Rogers C. A. The realization of distances within sets in Euclidean space. // Mathematika — 1972 — V. 19. — P. 1–24.

10. Райгородский А. М. Линейно-алгебраический метод в комбинаторике. — М.: МЦНМО, 2007.

ХРОМАТИЧЕСКИЕ ЧИСЛА ГРАФОВ РАССТОЯНИЙ, НЕ СОДЕРЖАЩИХ СИМПЛЕКСОВ

О. И. Рубанов (Москва)

Под *графом расстояний* $G = (V, E)$ мы подразумеваем произвольный граф, множество вершин V которого лежит в метрическом пространстве (X, ρ) (например, в евклидовом пространстве $(\mathbb{R}^n, |\cdot|_2)$); при этом множество рёбер E состоит из всех пар вершин, удалённых друг от друга на определённое расстояние. Одной из классических проблем, связанных с графами расстояний, является проблема нахождения так называемого *хроматического числа*

$$\chi((X, \rho), \mathcal{A})$$

пространства (X, ρ) с набором *запрещённых расстояний* $\mathcal{A}$ [1, 2], которое определяется как минимальное количество цветов, необходимое для такой раскраски точек пространства, что точки, находящиеся на любом расстоянии $a \in \mathcal{A}$, покрашены в разные цвета.

Хорошо известно, что выполнено неравенство

$$\chi((\mathbb{R}^2, |\cdot|_2), \{1\}) \geq 4,$$

однако проблема получения лучшей нижней оценки или доказательства того, что

$$\chi((\mathbb{R}^2, |\cdot|_2), \{1\}) = 4,$$

до сих пор остаётся открытой.

В 1976 году Эрдеш [3] сформулировал задачу отыскания графа расстояний без треугольников (или, в более общей постановке, без циклов длины $\leq k$) с хроматическим числом 4 на плоскости (все существовавшие на тот момент примеры содержали треугольники). Эта задача была решена уже три года спустя Уормалдом [4], конструкция которого содержала 6448 вершин и не содержала циклов длины 3 (но содержала циклы длины 4). В 1996 году О'Доннелл и

Хохберг [5] построили граф без 3-циклов на 23 вершинах и граф без 3- и 4-циклов на 45 вершинах.

Естественным обобщением этой задачи является задача построения n-мерных графов расстояний, имеющих "большое" хроматическое число и не содержащих клик "большого" размера. Под "большим" хроматическим числом мы подразумеваем хроматическое число, близкое к наилучшим известным нижним оценкам величины

$$\chi(\mathbb{R}^n, |\cdot|_2), \{1\}).$$

Отметим, что наилучшая нижняя оценка в размерности 3 на сегодняшний день принадлежит Нечуштану [6]:

$$\chi((\mathbb{R}^3, |\cdot|_2), \{1\}) \geq 6,$$

а предыдущая оценка

$$\chi((\mathbb{R}^3, |\cdot|_2), \{1\}) \geq 5$$

оставалась неулучшенной на протяжении более пятидесяти лет (см. [7]). При $n \to \infty$ наилучшая оценка [8] имеет вид

$$\chi((\mathbb{R}^n, |\cdot|_2), \{1\}) \geq (1.239... + o(1))^n.$$

Основные результаты настоящей работы сформулированы в следующих теоремах.

Теорема 1. *В пространстве $\mathbb{R}^3$ существует граф расстояний, имеющий хроматическое число 5 и не содержащий тетраэдров.*

Теорема 2. *В пространстве $\mathbb{R}^n$ существует граф расстояний, имеющий хроматическое число $n+2$ и не содержащий n-мерных симплексов.*

Теорема 3. *Существуют константы $\gamma > 1$, $\beta \in \mathbb{N}$ и $n_0 \in \mathbb{N}$, при которых для всех $n \geq n_0$ найдётся такой граф расстояний $G = (V, E)$, $V \subset \mathbb{R}^n$, что $\chi(G) \geq \gamma^n$ и G не содержит клик размера $\geq \beta$.*

Доказательства первых двух теорем полностью конструктивны, а построенные в них графы содержат малое число вершин. Тем не менее, для больших n нижние оценки хроматических чисел этих графов довольно слабые. В доказательстве последней теоремы конструкция графа не указывается явно; факт её существования доказывается с помощью вероятностных методов. Преимущество теоремы 3 состоит в том, что получающаяся в ней нижняя оценка хроматического числа графа близка к наилучшей известной нижней оценке хроматического числа пространства.

Настоящая работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант № 06-01-00383).

Список литературы

1. Райгородский А. М. Проблема Борсука и хроматические числа некоторых метрических пространств // Успехи матем. наук. — 2001. — Т. 56, № 1. — С. 107–146.

2. Soifer A. Chromatic number of the plane: a historical essay // Geombinatorics. — 1991. — P. 13–15.

3. Erdős P. Unsolved problems // Congress Numerantium XV Proceedings of the 5th British Comb. Conf. — 1975 (1976). — P. 681.

4. Wormald N. A 4-Chromatic graph with a special plane drawing // The Journal of the Australian Mathematical Society (Series A). — 1979. — V. 28. — P. 1–8.

5. O'Donnel P., Hochberg R. Some 4-chromatic unit-distance graphs without small cycles // Geombinatorics. — 1996. — V. 5, № 4. — P. 137–142.

6. Nechushtan O. Note on the space chromatic number // Discrete Mathematics. — 2002. — V. 256. — P. 499–507.

7. Райский Д. Е. Реализация всех расстояний при разбиении пространства $\mathbf{R}^n$ на $n+1$ часть // Матем. заметки. — 1970. — Т. 7. — С. 319–323.

8. Райгородский А. М. О хроматическом числе пространства // Успехи матем. наук. — 2000. — Т. 55, № 2. — С. 147–148.

ИЗОМЕТРИЧЕСКИЕ ДЕФОРМАЦИИ МНОГОГРАННИКОВ, УВЕЛИЧИВАЮЩИЕ СОДЕРЖАЩИЙСЯ В НИХ ОБЪЕМ

Г. А. Самарин (Москва)

Как выглядит фигура, содержащая максимальный объем, среди фигур с данной боковой поверхностью? Ответ на этот вопрос не известен даже для поверхностей правильных многогранников.

Рассмотрим выпуклый многогранник. По теореме А. Д. Александрова (Погорелова) о единственности [1], любая выпуклая поверхность изометричная многограннику — конгруэнтна ему. Все остальные реализации — невыпуклые. В начале 1990-х гг. была найдена невыпуклая реализация правильного тетраэдра с объемом, значительно превышающим объём самого тетраэдра [2]. А в 1996 году

Бликером [3] было доказано, что изометрической деформацией можно увеличить объем любого выпуклого симплициального многогранника.

Н. П. Долбилин поставил задачу доказать, что не только выпуклая и симплициальная, но и любая поверхность ограниченного конечного замкнутого и самонепересекающегося многогранника может быть изометрично продеформирована с увеличением объема. Недавно одновременно, независимо и разными методами положительное ее решение было получено Игорем Паком [4] и мною.

Определение. Деформация поверхности S в евклидовом трехмерном пространстве $\mathbf{R}^3$ — это непрерывное отображение $h : S \times [0, \varepsilon] \to \mathbf{R}^3$ такое, что $h_\tau(\cdot) := h(\cdot, \tau)$, где h_τ вложение S в $\mathbf{R}^3$. Деформация h является изометрической деформацией, если длина любой спрямляемой кривой ν в S сохраняется при деформации, т. е. $L(h_\tau \circ \nu) = L(\nu)$, для всех $\tau \in [0, \varepsilon]$.

Определение. Многогранником называют совокупность многоугольников в трёхмерном пространстве такую, что:

1) любые два многоугольника либо не пересекаются, либо имеют ровно одну общую вершину, либо ровно одну общую сторону;

2) от одного многоугольника к другому можно перейти, идя по многоугольникам, имеющим общие стороны;

3) по каждой стороне одного многоугольника прилегает один и только один многоугольник из совокупности;

4) многоугольники, имеющие одну общую точку(вершину), образуют замкнутый цикл.

Теперь мы можем перейти к построению. Рассмотрим пирамиду W с основанием $A_1A_2...A_n$ (вообще говоря невыпуклым) и вершиной O. Боковые грани, суть треугольники, (A_1A_2O), (A_2A_3O), ..., (A_nA_1O) обозначим через $G^1, G^2, ..., G^n$ соответственно. Опустим из вершины O перпендикуляр OH на основание пирамиды, где H лежит в основании. Выберем на отрезке OH точку O', отличную от H. Назовем W' пирамиду с основанием $A_1A_2...A_n$ и вершиной O'. Обозначим $\frac{A_iO'}{A_iO} := \cos t_i$ и пусть $\vec{t} = (t_1, ..., t_n)$.

Пусть M_i — середина бокового ребра A_iO', K_i — середина ребра при основании A_iA_{i+1} (через K_n естественно обозначатить середину ребра A_nA_1), $i = 1, \ldots, n$

Проведём биссекторы (биссекторные плоскости) всех двугранных углов пирамиды W' и обозначим через π_i биссектор двугранного угла при боковом ребре A_iO', Π_i — биссектор двугранного угла при ребре основания A_iA_{i+1}. Без ограничения общности считаем, что у нашей пирамиды нет боковых ребер, двугранный угол при которых равен π.

Определение. Будем называть ребро ограниченного замкнутого многогранника *ребром выпуклости*, если двугранный угол между гранями, пересекающимися по данному ребру, меньше π. Остальные рёбра назовём *ребрами вогнутости.*

Для каждого ребра выпуклости A_iO' в биссекторе π_i выберем точку Q_i из внутренности W' такую, что $|A_iQ_i| = |Q_iO'| = \frac{|A_iO|}{2}$. Для каждого ребра вогнутости A_iO' в плоскости π_i выберем точку Q_i из внешности W' такую, что $|A_iQ_i| = |Q_iO'| = \frac{|A_iO|}{2}$.

$R_i(r_i)$ — точка, лежащая на перпендикуляре к π_i, восстановленном из точки Q_i в полупространство, содержащее грань $(A_iA_{i+1}O')$, причём $|Q_iR_i(r_i)| = r_i$.

$L_{i-1}(l_{i-1})$ — точка, лежащая на перпендикуляре к π_i восстановленом из точки Q_i в полупространство, содержащее грань $(A_{i-1}A_iO')$, причём $|Q_iL_{i-1}(l_{i-1})| = l_{i-1}$.

На перпендикуляре к плоскости Π_i, восстановленном из K_i, выберем точку $K_i(k_i)$, лежащую в полупространстве, содержащем грань $(A_iA_{i+1}O')$ так, что $|K_iK_i(k_i)| = k_i$.

Невыпуклую поверхность, состоящую из девяти треугольников $A_iK_i(k_i)R_i(r_i)$, $A_{i+1}K_i(k_i)L_i(l_i)$, $A_iK_i(k_i)A_{i+1}$, $Q_iR_i(r_i)A_i$, $Q_iR_i(r_i)O'$, $Q_{i+1}L_i(l_i)O'$, $Q_{i+1}L_i(l_i)A_{i+1}$, $K_i(k_i)L_i(l_i)R_i(r_i)$, $L_i(l_i)R_i(r_i)O'$ и склеивающуюся по общим (совпадающим) сторонам, обозначим G_B^i. Невыпуклый многогранник, являющийся объединением G_B^i и основания $A_1A_2...A_n$, обозначим W_B.

Теперь рассмотрим выражения:

$$f_{i,l} := |R_i(r_i)K_i(k_i)|^2 - |N_{i,r}(r_i)N_{i,k}(k_i)|^2,$$
$$f_{i,r} := |K_i(k_i)L_i(l_i)|^2 - |N_{i,k}(k_i)N_{i,l}(l_i)|^2,$$
$$f_{i,k} := |R_i(r_i)L_i(l_i)|^2 - |N_{i,r}(r_i)N_{i,l}(l_i)|^2.$$

Тогда из условия $f_{i,j} = 0$ следует, что развёртки G^i и G_B^i составлены из одних и тех же треугольников, с одним и тем же правилом склейки, т. е. развёртки изометричны. А, следовательно, и развертки W и W_B изометричны.

Рассмотрим $f_{i,j}$ как функции от l_i,r_i,k_i и $\vec{t}$. Задав плоские углы, ребра и двугранные углы между гранями в W' как функции от $\vec{t}$, мы получим из теоремы о неявной функции, что для достаточно малого $||\vec{t}||$ всегда существует и единственен набор положительных констант l_i,r_i,k_i. Откуда вытекает

Теорема. *Для любой пирамиды W в R^3, существует изометрическая деформация ее поверхности, увеличивающая объем.*

Откуда напрямую следует основной результат (отделим плоскостью одну из вершин).

Следствие. *Пусть имеется ограниченный замкнутый многогранник в R^3, тогда существует изометрическая деформация его поверхности, увеличивающая объем.*

Список литературы

1. Александров А. Д. Выпуклые многогранники. — М.—Л.: ГИТТЛ, 1950.

2. Долбилин Н. П. Устное сообщение.

3. Bleecker D. D. Volume increasing isometric deformations of convex polyhedra // J. Differential Geometry. — 1996. — V. 43. — P. 505–526.

4. Pak I. Inflating polyhedral surface // `http://www-math.mit.edu/~pak/pillow4.pdf`.

СПЕКТРЫ ДЛЯ ГЕОМЕТРИЧЕСКИХ ОБРАЗОВ АВТОМАТОВ И ИХ СВЯЗЬ С ПОСЛЕДОВАТЕЛЬНОСТЯМИ И ФИГУРАМИ

В. А. Твердохлебов (Саратов)

Математический конструктивизм уточняется с использованием понятий последовательности и алгоритма. В работах [1–2] показано, что последовательность может быть использована как средство для установления взаимосвязей между законами функционирования автоматов, геометрическими фигурами на плоскости и алгоритмами, определяющими порождение последовательностей рекуррентными формами. Базовой структурой полагается последовательность, а основным средством для представления свойств законов функционирования автомата — спектры динамических параметров, характеризующих рекуррентные формы и правила их применения при порождении последовательностей. В основе лежит преобразование законов функционирования автоматов из символьной формы (таблиц, символьных матриц, графов) в числовые структуры в виде геометрических образов. Для этого вводится линейный порядок на автоматном отображении, показывается, что между упорядоченным

автоматным отображением и последовательностью вторых координат точек этого отображения имеется взаимнооднозначное соответствие. Это позволяет исследование некоторых свойств законов функционирования автомата заменять исследованием свойств последовательности. Геометрический образ законов функционирования автомата (фазовая картина поведения) и конкретное функционирование (фазовая траектория) получают единую структуру в виде графика. Это позволяет для анализа и синтеза законов функционирования автомата использовать классические средства интерполяции, экстраполяции, задания функции переходов и выходов автомата числовыми уравнениями и т. п. Разработан метод преобразования геометрических фигур на плоскости в законы функционирования автомата на основе выбора множества точек на фигуре и выбора обхода фигуры по точкам, рассмотрения такой последовательности как последовательности вторых координат точек упорядоченного автоматного отображения. Спектры позволяют ввести новую классификацию законов функционирования автоматов, выражать характеристики законов функционирования автоматов через структуры последовательностей, представляющих законы функционирования. Математические структуры в форме последовательностей имеют самостоятельное фундаментальное значение и входят как существенные составляющие в более сложные структуры. В данной работе иллюстрируется применение спектра для оценки сложности законов функционирования автоматов, представленных последовательностями вторых координат точек геометрического образа автомата. В качестве таких последовательностей рассмотрены начальные отрезки последовательностей, задающих фундаментальные математические величины, а исследуемым свойством полагается сложность определения последовательностей рекуррентными формами.

Под сложностью последовательности $\xi \in U^*$ понимается сложность процесса ее определения последовательностью правил из выбранного множества правил $P = \{P_i\}_{i \in I}$. Для обеспечения точности и простоты таких правил используются правила в виде рекуррентных форм $F_i^m(z_1, z_2, ..., z_m) = z_{m+1}$, $m = 1, 2, ...$, и логических условий их применения. Полнота средств для оценки сложности процесса определения последовательности ξ достигается, во-первых, использованием наборов рекуррентных форм различных порядков $F^1 = \left\{F_{i_1}^1\right\}_{i_1 \in I_1}$, $F^2 = \left\{F_{i_2}^2\right\}_{i_2 \in I_2}$,... , $F^k = \left\{F_{i_k}^k\right\}_{i_k \in I_k}$, а во-вторых, применением каждой рекуррентной формы F_i^m на наибольшем по длине, определяемом по правилам, отрезке последовательности ξ.

Существенным является выбор правил $\boldsymbol{L}$ применения рекуррентных форм при определении последовательности ξ. Каждая рекуррентная форма F_i^m с учетом отношения $\xi \in U^*$ определяется функ-

цией $f_i^m : U^* \to U$ и применяется для определения одного или нескольких отрезков в зависимости от структуры последовательности ξ. Полагается, что рекуррентная форма применяется отдельными вариантами вхождений рекуррентной формы в последовательность правил, определяющих рассматриваемую последовательность ξ. Вариант применения рекуррентной формы F_i^m оканчивается в каждом из следующих случаев: 1) применение F_i^m не соответствует функции f_i^m; 2) дальнейшее и соответствующее функции f_i^m применение F_i^m связано с (первым) повторным применением рекуррентной формы к уже использованным для определяемого отрезка набора аргументов.

Во втором случае применение F_i^m рассматривается как новый вариант использования F_i^m. Это условие требуется для выхода из циклов в последовательности отдельных правил определения ξ, образующих общее правило. Следовательно, при счете правил, использованных при определении последовательности ξ, пересчитываются варианты вхождения отдельных правил в общее правило.

Введём понятие спектра. Пусть $U = \{u_1, u_2, ..., u_k\}$ — конечное множество и ξ — последовательность элементов из множества U: $\xi = \langle u(1), u(2), ..., u(t), ...\rangle$. Множества всех конечных последовательностей, всех конечных последовательностей длины v и бесконечных последовательностей элементов из множества U будем обозначать соответственно U^*, U^v, U^∞. Спектр $\Omega(\xi)$ динамических характеристик последовательности $\xi \in U^* \cup U^\infty$ имеет иерархическую структуру, состоящую из уровней $\Omega(\xi) = (\Omega_1(\xi), \Omega_2(\xi), \Omega_3(\xi), \Omega_4(\xi))$. Каждый конкретный вариант реализации (представление значениями параметров) любого уровня $\Omega_i(\xi)$ определяет разбиение каждого из множеств U^*, U^v, U^∞ на подмножества по свойствам совпадения характеристик, соответствующих уровню. Подмножества такого разбиения будем рассматривать как классы эквивалентности последовательностей.

Пусть $\overline{\xi}$ — произвольная последовательность из U^v. Наименьший порядок рекуррентной формы, определяющей последовательность $\overline{\xi}$, будем обозначать $m_0(\overline{\xi})$. Для $m \in N^+$, где $1 \le m \le m_0(\overline{\xi})$, наибольшую длину начального отрезка последовательности $\overline{\xi}$, определяемого рекуррентной формой порядка m, будем обозначать $d^m(\overline{\xi})$. Для $m \in N^+$, где $1 \le m \le |\overline{\xi}| - 1$, число смен рекуррентных форм порядка m, требующихся при определении последовательности $\overline{\xi}$, будем обозначать $r^m(\overline{\xi})$. Для $m \in N^+$, где $1 \le m \le m_0(\overline{\xi})$ и j, где $1 \le j \le r^m(\overline{\xi})$, длину j-го отрезка в определении последовательности $\overline{\xi}$ будем обозначать $d_j^m(\overline{\xi})$.

Используя введенные обозначения определим спектр параметров, характеризующих последовательность, как следующую структуру: $\Omega_0(\overline{\xi}) = \langle m_0(\overline{\xi})\rangle$; $\Omega_1(\overline{\xi}) = \langle d^1(\overline{\xi}), d^2(\overline{\xi}), ..., d^\alpha(\overline{\xi})\rangle$; $\Omega_2(\overline{\xi}) = \langle r^1(\overline{\xi}), r^2(\overline{\xi}), ..., r^\alpha(\overline{\xi})\rangle$; $\Omega_3(\overline{\xi}) = \langle \Omega_3^1(\overline{\xi}), \Omega_3^2(\overline{\xi}), ..., \Omega_3^\alpha(\overline{\xi})\rangle$, где $\alpha = m_0(\overline{\xi})$ и $\Omega_3^j(\overline{\xi}) = \left\langle d_1^j(\overline{\xi}), d_2^j(\overline{\xi}), ..., d_{n_j}^j(\overline{\xi})\right\rangle$; ($n_j$ — номер последнего отрезка в определении последовательности $\overline{\xi}$ как последовательности отрезков, определяемых отдельными рекуррентными формами порядка j); $\Omega_4(\overline{\xi}) = \Theta(\Omega_3(\overline{\xi}))$, где Θ — оператор замены в $\Omega_3(\overline{\xi})$ величин длин отрезков весами использованных рекуррентных форм для определения отрезков.

Работа выполнена при финансовой поддержке РФФИ (07-08-00088-а).

Список литературы

1. Твердохлебов В. А. Геометрические образы конечных детерминированных автоматов // Известия Саратовского ун-та (Новая серия). — 2005. — Т. 5. Вып. 1. — С. 141–153.

2. Твердохлебов В. А. Методы интерполяции в техническом диагностировании // Проблемы управления. — 2007. — № 2. — С. 28–34.

ХРОМАТИЧЕСКИЕ ЧИСЛА МЕТРИЧЕСКИХ ПРОСТРАНСТВ С НЕСКОЛЬКИМИ ЗАПРЕЩЕННЫМИ РАССТОЯНИЯМИ И ИХ СВЯЗЬ С ПРОБЛЕМОЙ БОРСУКА

И. М. Шитова (Москва)

В работе рассмотрены две задачи: задача о хроматическом числе пространства, восходящая к Нелсону, Эрдешу и Хадвигеру, и задача Борсука о разбиении ограниченного множества положительного диаметра на части меньшего диаметра [1, 2]. *Хроматическим числом* $\chi(X, \rho, A)$ *метрического пространства* X *с метрикой* ρ *для множества запрещенных расстояний* A называется минимальное число цветов, в которые можно так раскрасить X, что никакие две точки одного цвета не будут находиться на расстоянии, принадлежащем A.

Изначально задача ставилась для $X = \mathbf{R}^n$, $\rho = |\cdot|_2$ (через $|\cdot|_2$ мы обозначаем евклидову метрику, аналогично определяется $|\cdot|_q$ для произвольного $q \geq 1$), $A = \{1\}$. Вообще говоря, в силу однородности

пространства вместо единичного расстояния здесь можно рассмотреть произвольное расстояние a, хроматическое число от этого не изменится. В дальнейшем значительное внимание было уделено таким пространствам, как $(\mathbf{R}^n, |\cdot|_q)$ и $(\mathbf{Q}^n, |\cdot|_q)$. Здесь в случае $\mathbf{Q}^n$ уже важно, какое запрещенное расстояние рассматривается.

Числом Борсука $f(n)$ называется минимальное число частей, на которое можно разбить произвольное ограниченное множество положительного диаметра так, чтобы диаметр каждой из частей был меньше диаметра исходного множества.

Задача о хроматическом числе была поставлена на рубеже 40–50-х годов XX века, и за прошедшие 60 лет были получены разнообразные результаты как в самой задаче, так и в ее обобщениях [1, 2].

Например, известно, что

$$(1.239... + o(1))^n \le \chi(\mathbf{R}^n, |\cdot|_2, \{1\}) \le (3 + o(1))^n \quad [3, 4],$$

$$(1.173... + o(1))^n \le \chi(\mathbf{Q}^n, |\cdot|_2, \{1\}) \le (3 + o(1))^n \quad [2, 4],$$

$$(1.365... + o(1))^n \le \chi(\mathbf{R}^n, |\cdot|_1, \{1\}) \le (5 + o(1))^n \quad [5, 6].$$

Когда множество запрещенных расстояний состоит более, чем из одного элемента, часто рассматривают не само хроматическое число, а его наибольшее значение при заданной мощности множества запрещенных расстояний. Здесь доказаны следующие оценки [2]:

$$\max_{A:|A|=2} \chi(\mathbf{R}^n, |\cdot|_2, A) \ge (1.439... + o(1))^n,$$

$$(c_1 k)^{c_2 n} \le \max_{A:|A|=k} \chi(\mathbf{R}^n, |\cdot|_2, A) \le (3 + o(1))^{kn}, c_1 > 0, c_2 > 0.$$

Автором этой работы была доказана следующая

Теорема 1. *Выполнены оценки*:

$$\max_{A:|A|=2} \chi(\mathbf{R}^n, |\cdot|_2, A) \ge (1.465... + o(1))^n,$$

$$\max_{A:|A|=3} \chi(\mathbf{R}^n, |\cdot|_2, A) \ge (1.664... + o(1))^n,$$

$$\max_{A:|A|=2} \chi(\mathbf{R}^n, |\cdot|_1, A) \ge (1.691... + o(1))^n,$$

$$\max_{A:|A|=3} \chi(\mathbf{R}^n, |\cdot|_1, A) \ge (2.000... + o(1))^n.$$

Подход, с помощью которого доказывается теорема, позволяет получать нижние оценки при любой мощности множества запрещенных расстояний. В доказательстве используется линейно-алгебраический метод в комбинаторике, анализ и компьютерный счет.

Дальнейшее усиление оценок из теоремы 1 — трудная задача. Однако иногда две оценки по отдельности бывает сложно улучшить, но можно доказать, что с гарантией одна из них допускает уточнение.

А. М. Райгородским в ряде статей была разработана техника альтернирования, позволяющая получать такого рода результаты [7, 8]. Нам удалось добиться уточнения некоторых оценок Райгородского.

Теорема 2. *Существует такая последовательность* $n_i \to \infty$, *что либо*

$$\chi(\mathbf{R}^{n_i}, |\cdot|_2, \{1\}) \geq (1.239... + 0.002 + o(1))^{n_i},$$

либо

$$\chi(\mathbf{Q}^{n_i}, |\cdot|_2, \{1\}) \geq (1.173... + 0.002 + o(1))^{n_i}.$$

Перейдем к условным оценкам числа Борсука и хроматического числа.

Известно [2, 9], что

$$(1.225... + o(1))^{\sqrt{n}} \leq f(n) \leq (1.224... + o(1))^n.$$

Райгородский доказал [8], что для некоторых $\{n_i \to \infty\}$ либо

$$\chi(\mathbf{R}^{n_i}, |\cdot|_2, \{1\}) \geq (1.239... + 0.001 + o(1))^{n_i},$$

либо

$$f(n_i) \geq (1.225... + 0.001 + o(1))^{n_i}.$$

Автору данной статьи удалось усилить этот результат и доказать следующую теорему.

Теорема 3. *Существует такая последовательность* $\{n_i\}$, *что либо*

$$\chi(\mathbf{R}^{n_i}, |\cdot|_2, \{1\}) \geq (1.239... + 0.017 + o(1))^{n_i},$$

либо

$$f(n_i) \geq (1.225... + 0.017 + o(1))^{n_i}.$$

Работа выполнена при финансовой поддержке гранта РФФИ (№ 06-01-00383).

Список литературы

1. Сойфер А. Хроматическое число плоскости: его прошлое, настоящее и будущее // Матем. просвещение. — 2004. — Вып. 8.

2. Райгородский А. М. Проблема Борсука и хроматические числа метрических пространств // Успехи матем. наук. — 2001. — Т. 56, вып. 1. — С. 107–146.

3. Райгородский А. М. О хроматическом числе пространства // Успехи матем. наук. — 2000. — Т. 55, вып. 2. — С. 147–148.

4. Larman D. G. and Rogers C. A. The realization of distances within sets in Euclidean space // Mathematika. — 1972. — V. 19. — P. 1–24.

5. Райгородский А. М. О хроматическом числе пространства с метрикой l_q // Успехи матем. наук. — 2004. — Т. 59, вып. 5. — С. 161–162.

6. Kang J.-H. and Füredi Z. Distance graphs on $\mathbf{Z}^n$ with l_1-norm // Theoretical Comp. Sci. — 2004. — V. 319, № 1–3. — P. 357–366.

7. Райгородский А. М. Проблема Эрдеша — Хадвигера и хроматические числа конечных геометрических графов // Матем. сборник. — 2005. — Т. 196. — С. 123–156.

8. Райгородский А. М. О числах Борсука и Эрдеша — Хадвигера // Матем. заметки. — 2006. — Т. 79, № 6. — С. 913–924.

9. Schramm O. Illuminating sets of constant width // Mathematika. — 1988. — V. 35. — P. 180–189.

Секция «Теория кодирования и смежные вопросы»

О НЕКОТОРЫХ АЛГЕБРАИЧЕСКИХ И КОМБИНАТОРНЫХ СВОЙСТВАХ МНОЖЕСТВА КОРРЕЛЯЦИОННО-ИММУННЫХ ФУНКЦИЙ В ЦЕЛОМ

Е. К. Алексеев (Москва)

Пусть $F_2 = GF(2)$, $V_n = F_2^n$ — линейное пространство размерности n над F_2, $\mathcal{F}_n = V_{2^n}$ — множество булевых функций от n переменных. Для $x \in V_n$ через $wt(x)$ обозначим вес Хэмминга вектора x. Если мы подставляем в функцию f константы $\sigma^{(i_1)}, ..., \sigma^{(i_s)}$, где $s \leq n$, вместо переменных $x^{(i_1)}, ..., x^{(i_s)}$ соответственно, то полученная подфункция обозначается $f^{\sigma^{(i_1)},...,\sigma^{(i_s)}}_{x^{(i_1)},...,x^{(i_s)}}$.

Преобразованием Уолша — Адамара булевой функции $f \in \mathcal{F}_n$ называется функция $W_f(u) = \sum_{x \in V_n} (-1)^{f(x) \oplus <x,u>}$, где $u \in V_n$.

Булева функция $f \in \mathcal{F}_n$ называется *корреляционно-иммунной* порядка $m, 0 < m \leq n$, если $W_f(u) = 0$ для любых наборов $u \in V_n$ таких, что $1 \leq wt(u) \leq m$. Введем следующее обозначение

$$corf = max\{m \in \mathbb{N} | f \text{ — корреляционно-иммунна порядка } m\}.$$

Определение. $CI(n)$=$\{f \in \mathcal{F}_n | corf \geq 1\}$.

Определение. Функция $f \in \mathcal{F}_n$ называется *четной*, если $f(x) = f(x \oplus \overline{1})$. Множество четных функций от n переменных обозначим через $Mir(n)$.

Определение. $Anmir(n)$= $\{f \in \mathcal{F}_n | f(x) = f(x \oplus \overline{1}) \Rightarrow f(x) = 0\}$.

Определение. $BCI(n)$= $\{f \in CI(n) | f(x) \cdot f(x \oplus \overline{1}) \equiv 0\}$.

Все не определенные здесь понятия можно найти в [1, 2].

В работе исследовались алгебраические свойства множества $CI(n)$. Вначале приведем полученные вспомогательные свойства.

Определение. *Ядром четности* функции $f \in \mathcal{F}_n$ назовем функцию $km(f) = f(x) \cdot f(x \oplus \overline{1})$.

Предложение 1. *Для любой* $f \in Mir(n)$ *справедливы равенства* $W_f(u) = 0$, *если* $wt(u) = 2k+1, k \geq 0$.

Следствие 1. *Любая четная функция является корреляционно-иммунной как минимум первого порядка.*

Следствие 2. *Для мощности множества* $CI(n)$ *выполнено неравенство* $\#CI(n) \geq 2^{2^{n-1}}$.

Предложение 2. *Для любой* $f \in \mathcal{F}_n$ *выполняется включение* $km(f) \in Mir(n)$.

Предложение 3. *Для любой* $f \in \mathcal{F}_n$ *выполняется равентсво* $dist(f, Mir(n)) = wt(f \oplus km(f))$.

Предложение 4. $Mir(n)$ *является линейным подпространством пространства* V_{2^n} *размерности* 2^{n-1}.

Предложение 5. *Для любой функции* $f \in CI(n)$ *справедливо включение* $(f \oplus km(f)) \in CI(n)$.

Следствие 3. *Для любой* $f \in CI(n)$ *справедливо равенство* $g = f \oplus km(f)$, $km(g) \equiv 0$, $g \in BCI(n)$.

Предложение 6. *Для любых двух функций* $f, g \in CI(n)$ *выполняется импликация* $f \cdot g \equiv 0 \Rightarrow f \oplus g \in CI(n)$.

На основе этих свойств может быть доказана следующая

Теорема 1. *Множество* $CI(n)$ *является объединением некоторого числа линейных многообразий пространства* V_{2^n}.

Введем вспомогательные определения для конструктивного описания множества $CI(n)$.

Определение. $Mir(n)|_g = \{f \in Mir(n) | f \cdot g \equiv 0\}$.

Предложение 7. $Mir(n)|_g$ — *линейное подпространство пространства* $Mir(n)$ *размерности* $2^{n-1} - wt(g)$.

Результат теоремы 1 можно описать конструктивно. Это описание дает теорема 2 и предложение 8.

Теорема 2. *Для множества* $CI(n)$ *верно следующее равенство:*

$$CI(n) = \bigcup_{g \in BCI(n)} (g \oplus Mir(n)|_g).$$

Предложение 8. *Линейные многообразия, представленные в теореме* 2 *образуют разбиение множества* $CI(n)$.

Определение. $BCI(n)|_{wt=w} = \{f \in BCI(n) | wt(f) = w\}$.

Из теоремы 2 следует выражение для мощности множества $CI(n)$. Это показывает, что проблема поиска формулы для $\#CI(n)$ сводится к поиску формулы мощности множеств $\#BCI(n)|_{wt=w}$ для $w = 0, ..., 2^{n-1}$. Это показывает следующее

Следствие 4. *Справедливо равентсво*:

$$\#CI(n) = \sum_{g \in BCI(n)} 2^{2^{n-1}-wt(g)} = \sum_{w=0}^{2^{n-1}} 2^{2^{n-1}-w} \cdot (\#BCI(n)|_{wt=w})$$

Это новое алгебро-геометрическое описание позволило доказать следующую конструктивную нижнюю оценку.

Теорема 3. *Справедливо неравенство*:

$$\#CI(n) \geq \sum_{m=0}^{2^{n-3}} \binom{2^{n-2}}{2m} \cdot \binom{2m}{m} \cdot 2^{2^{n-1}-4m}.$$

Для примера приведем соотношение между реальным значением $\#CI(5)$ и числами, которые были получены с помощью описанных оценок.

Обозначим полученную выше оценку через $M(n)$, тогда:

$$\frac{\#CI(5)}{M(5)} \approx 7.6, \quad \frac{\#CI(5)}{\#Mir(5)} \approx 48.$$

Список литературы

1. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004.

2. Винберг Э. Б. Курс алгебры. — М.: Факториал Пресс, 2002.

АЛГЕБРАИЧЕСКАЯ ИММУННОСТЬ ФИЛЬТРУЮЩЕЙ ФУНКЦИИ ГЕНЕРАТОРА WG

В. В. Баев (Москва)

Для булевой функции f значение алгебраической иммунности $AI(f)$ равно минимальному значению числа d, для которого существует ненулевая булева функция g степени d такая, что $fg = 0$ или $(f+1)g = 0$. Поскольку $(f+1)f = 0$, то $AI(f) \leqslant \deg f$. При анализе фильтрующих генераторов одним из важных показателей является алгебраическая иммунность булевых функций, используемых в этих генераторах [1, 2].

В данной работе представлен метод, позволяющий за приемлемое время вычислить значение алгебраической иммунности для фильтрующей булевой функции генератора WG. Этот генератор двоичной псевдослучайной последовательности был представлен на конкурсе eSTREAM [3]. Было доказано, что он обладает рядом хороших характеристик, но про значение алгебраической иммунности фильтрующей функции f_{WG} высказывались только предположения и приводились некоторые оценки.

Введём необходимые обозначения. Пусть $n = 29$ — количество булевых переменных функции f_{WG}; $GF(2^n)$ — поле Галуа из 2^n элементов; $\deg f$ — алгебраическая степень булевой функции f; $\mathcal{F}_n$ — множество всех булевых функций от n переменных; T_f — длина трэйс представления булевой функции f [3–5]; $d := \deg f_{WG} - 1 = 10$; $A_d^n(f) := \{g \in \mathcal{F}_n \mid fg = 0,\ \deg g \leqslant d\}$; $D := \sum_{k=0}^{d} \binom{n}{k}$ — количество булевых неизвестных в задаче поиска $AI(f_{WG})$, D и $T_{f_{WG}}$ характеризуют размер этой задачи, $D \approx 36 \cdot 10^6$, $T_{f_{WG}} = 145$.

Если для вычисления $A_d^n(f)$ применить алгоритмы, представленные ранее в [4, 6], то их сложность оценивается сверху как $O(2^n D^2)$ и $O(T_f D^3)$ соответственно, а общая нижняя оценка — $\Omega(D^2)$. Эти алгоритмы составляют систему линейных однородных уравнений на D неизвестных коэффициентов a_i многочлена Жегалкина функции $g \in A_d^n(f)$, а затем решают эту систему методом Гаусса. Нетрудно видеть, что для анализа функции f_{WG} этим алгоритмам понадобятся терабайты памяти (обработка матрицы размера $D \times D$), а значит они будут выполняться очень долго на рядовых вычислительных системах.

В данной работе был использован следующий приём. Вместо неизвестных булевых коэффициентов a_i использовались коэффициенты $b_i \in GF(2^n)$ трэйс представления функции $g \in A_d^n(f)$. Это позволило уменьшить сложность некоторых вычислений в n раз.

Новый метод представляет собой итерационный процесс, исключающий переменные b_i, для которых в полученной системе есть уравнения вида $b_i^{2^k} = 0$. Если на очередной итерации в модифицированной системе не нашлось таких переменных, то далее такая система решается методом Гаусса для поиска нетривиальных значений оставшихся (неисключённых) переменных. Сложность каждого шага итерационного процесса есть $O(T_f D \log(T_f D))$. То есть этот метод эффективен для булевых функций f с коротким трэйс представлением.

Новый метод был реализован на языке C++ и применён к функции f_{WG} на вычислительной машине с процессором IBM Power4 1,3

ГГц. При этом потребовалось около 2 ГБ оперативной памяти. Алгоритму понадобилось всего 6 итераций для того, чтобы исключить все переменные b_i. Время работы программы составило 250 секунд.

Результат работы программы показывает, что не существует ненулевой функции g степени $\leqslant d$ такой, что $fg = 0$ или $(f+1)g = 0$. Поскольку $d = \deg f_{WG} - 1$ и $(f+1)f = 0$, то результат проведённых вычислений доказывает, что

$$AI(f_{WG}) = \deg f_{WG} = 11.$$

Новый метод также позволяет находить для функции $f \in \mathcal{F}_n$ равенства вида

$$fg = h \quad (\deg g \leqslant e,\ \deg h \leqslant d), \tag{1}$$

где $e \leqslant d$. Оценки сложности такие же, как и при поиске алгебраической иммунности. Уравнения (1) тоже используются для анализа фильтрующих генераторов, [7]. Для функции $f = f_{WG}$ было найдено несколько десятков линейно независимых уравнений вида (1) для $d = 11$ и $e = 8$.

Работа выполнена при частичной финансовой поддержке РФФИ, проект номер 07-01-00154.

Список литературы

1. Алфёров А. П., Зубов А. Ю., Кузьмин А. С., Черёмушкин А. В. Основы криптографии. — М.: Гелиос АРВ, 2001 г.

2. Meier W., Pasalic E., Carlet C. Algebraic attacks and decomposition of boolean functions // Lecture notes in computer science (Eurocrypt-2004). — Springer, 2004. — V. 3027. — P. 474–491.

3. Nawaz Y., Gong G. The WG stream cipher // ECRYPT Stream Cipher Project Report 2005/033. — `http://www.ecrypt.eu.org/stream/`

4. Баев В. В. Некоторые нижние оценки на алгебраическую иммунность функций, заданных своими трэйс формами // Дискретные модели в теории управляющих систем: Труды VII Международной конференции (Покровское, 4–6 марта 2006 г.). — М.: МАКС Пресс, 2006. — С. 25–29.

5. Логачёв О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии — М.: МЦНМО, 2004.

6. Didier F., Tillich J.-P. Computing the algebraic immunity efficiently // Lecture notes in computer science (Eurocrypt-2006). — Springer, 2006. — V. 4047. — P. 359–374.

7. Courtois N. Fast algebraic attacks on stream ciphers with linear feedback // Lecture notes in computer science (Crypto-2003). — Springer, 2003. — V. 2729. — P. 176–194.

ОБ УРОВНЕ АФФИННОСТИ СИММЕТРИЧЕСКИХ БУЛЕВЫХ ФУНКЦИЙ

М. Л. Буряков (Москва)

Симметрические булевы функции характеризуются тем, что их значение зависит лишь от веса вектора своих переменных. В связи с этим, они могут быть представлены в компактной форме, что позволяет использовать на практике подобные функции с большим количеством переменных. Обширную информацию по криптографическим свойствам симметрических булевых функций можно найти, например, в [1]. В данной работе применительно к симметрическим булевым функциям рассматривается ещё один криптографический параметр — уровень аффинности, введённый в [2].

Введём некоторые обозначения. Пусть $\mathbb{F}_2$ — поле из двух элементов, $V_n = \mathbb{F}_2^n$ — линейное пространство вектор-столбцов размерности n над полем $\mathbb{F}_2$, $\mathcal{F}_n$ — множество булевых функций от n переменных. Любая функция $f \in \mathcal{F}_n$ может быть представлена единственным образом в виде полинома, называемого алгебраической нормальной формой (АНФ) этой функции [3]:

$$f(\mathbf{x}) = \bigoplus_{\mathbf{u}\in V_n} \lambda_f(\mathbf{u}) \left(\prod_{i=1}^{n} x_i^{u_i} \right), \text{ где } \lambda_f(\mathbf{u}) \in \mathbb{F}_2, \quad \lambda_f(\mathbf{u}) = \bigoplus_{\mathbf{x}\preccurlyeq\mathbf{u}} f(\mathbf{x});$$

$\deg f$ — степень этого полинома. Если для функции $f \in \mathcal{F}_n$ имеем $\deg f \leqslant 1$, то функция f называется аффинной. Множество всех аффинных функций от n переменных обозначим $\mathcal{A}_n$. Для наборов $1 \leqslant i_1 < \cdots < i_k \leqslant n$, $\mathbf{b} = \left(b^{(1)}, \ldots, b^{(k)}\right)^\top \in V_k$ при $k \leqslant n$ обозначим через $f_{i_1,\ldots,i_k}^{b^{(1)},\ldots,b^{(k)}}$ булеву функцию из $\mathcal{F}_{n-k}$, полученную из f фиксацией переменных $x^{(i_1)} = b^{(1)}, \ldots, x^{(i_k)} = b^{(k)}$ и называемую подфункцией функции f [3].

Следующие два определения даны в [2].

Определение. Булева функция f из $\mathcal{F}_n$ называется *k-аффинной*, $0 \leqslant k \leqslant n-1$, если существуют набор $1 \leqslant i_1 < \cdots < i_k \leqslant n$ и вектор $\mathbf{b} = \left(b^{(1)}, \ldots, b^{(k)}\right)^\top \in V_k$ такие, что $f_{i_1,\ldots,i_k}^{b^{(1)},\ldots,b^{(k)}} \in \mathcal{A}_{n-k}$.

Определение. *Уровнем аффинности* $\mathrm{la}f$ булевой функции f из $\mathcal{F}_n$ называется минимальное неотрицательное целое число k, для которого f является k-аффинной.

Индукцией по числу фиксируемых переменных можно доказать следующее утверждение.

Лемма. *Для коэффициентов АНФ произвольной булевой функции* $f \in \mathcal{F}_n$ *и произвольных наборов* $1 \leqslant i_1 < \cdots < i_k \leqslant n$, $\mathbf{a} = (a_1, \ldots, a_k)^\top \in V_k$ *справедливо равенство*

$$\lambda_{f_{i_1,\ldots,i_k}^{a_1,\ldots,a_k}}(\alpha') = \bigoplus_{\mathbf{v} \in V_k,\, \mathbf{v} \preccurlyeq \mathbf{a}} [\lambda_f]_{i_1,\ldots,i_k}^{v_1,\ldots,v_k}(\alpha').$$

Заметим, что любая подфункция симметрической функции также является симметрической.

Пусть $\mathbf{v}_f = (v_0, \ldots, v_n) \in V_n$ — *упрощённый вектор значений* симметрической функции f на векторах с весом i: $f(\mathbf{x}) = v_i$, если $\mathrm{wt}(\mathbf{x}) = i$.

Назовём *константным слоем* $L_{\mathrm{const}} \subseteq V_n$ для функции $f \in \mathcal{F}_n$ векторы с весом k, $i_1 \leqslant k \leqslant i_2$, $0 \leqslant i_1 \leqslant i_2 \leqslant n$, если $f(\mathbf{x}) = a$ для любого $x \in L_{\mathrm{const}}$ $(a \in \mathbb{F}_2)$. Аналогично назовём *чередующимся слоем* $L_{\mathrm{alter}} \subseteq V_n$ для функции f векторы с весом k, $i_1 \leqslant k \leqslant i_2$, $0 \leqslant i_1 \leqslant i_2 \leqslant n$, если $f(\mathbf{x}) = a$ для векторов $\mathbf{x} \in L_{\mathrm{alter}}$ с нечётным весом и $f(\mathbf{x}) = a \oplus 1$ для векторов $\mathbf{x} \in L_{\mathrm{alter}}$ с чётным весом $(a \in \mathbb{F}_2)$. Назовём *шириной слоя* L в этих обозначениях число $\mathrm{w}L = i_2 - i_1 + 1$. Пусть для функции f $\mathrm{w}L_{\mathrm{const}}^{\max}(f) = \max \mathrm{w}L_{\mathrm{const}}$, $\mathrm{w}L_{\mathrm{alter}}^{\max}(f) = \max \mathrm{w}L_{\mathrm{alter}}$, где максимум берётся по всем слоям соответствующего вида.

Теорема 1. *Пусть* $f \in \mathcal{F}_n$ — *симметрическая булева функция и* $\mathrm{w}L^{\max} = \max\{\mathrm{w}L_{\mathrm{const}}^{\max}(f), \mathrm{w}L_{\mathrm{alter}}^{\max}(f)\}$. *Тогда* $\mathrm{la}f = n - \mathrm{w}L^{\max} + 1$.

Доказательство. Пусть $\mathrm{w}L^{\max}$ достигается на слое L, состоящим из векторов с весом k для $i_1 \leqslant k \leqslant i_2$, $0 \leqslant i_1 \leqslant i_2 \leqslant n$. Рассмотрим фиксацию произвольных $n - i_2 + i_1$ переменных функции f, в которой ровно i_1 единиц и $n - i_2$ нулей. Нетрудно видеть, что соответствующая этой фиксации подфункция функции f есть сужение f на слой L. По свойству слоя L отсюда следует, что эта подфункция аффинна, то есть $\mathrm{la}f \leqslant n - \mathrm{w}L^{\max} + 1$.

Предположим, что $\mathrm{la}f = m < n - \mathrm{w}L^{\max} + 1$. Тогда существуют такие наборы $a_1, \ldots, a_m \in \mathbb{F}_2$, $0 \leqslant i_1 < \cdots < i_m \leqslant n$, что подфункция $f_{i_1,\ldots,i_m}^{a_1,\ldots,a_m} \in \mathcal{A}_n$. Но поскольку $f_{i_1,\ldots,i_m}^{a_1,\ldots,a_m}$ симметрическая, то несложно понять, что она либо константа, либо функция, существенно зависящая от всех своих переменных. В последнем случае $f_{i_1,\ldots,i_m}^{a_1,\ldots,a_m}(\mathbf{x}') = a$ на векторах $\mathbf{x}$ с чётным весом и $f_{i_1,\ldots,i_m}^{a_1,\ldots,a_m}(\mathbf{x}) = a \oplus 1$ на векторах $\mathbf{x}$ с нечётным весом $(a \in \mathbb{F}_2)$ Получаем, что эта подфункция есть сужение функции f на либо константный, либо чередующийся слой с шириной $n - m + 1$, что противоречит максимальности $\mathrm{w}L^{\max}$.

Следствие. *Максимальное значение уровня аффинности для симметрических булевых функций из* $\mathcal{F}_n$ *равно* $n - 1$ *и дости-*

гается на функциях h_1, $h_1 \oplus 1$, h_2, $h_2 \oplus 1$, *для которых* $\mathbf{v}_{h_1} = (0,0,1,1,0,0,\ldots)$, $\mathbf{v}_{h_2} = (0,1,1,0,0,\ldots)$.

Согласно [1, предложение 4] $\deg h_1 = \deg(h_1 \oplus 1) = \deg h_2 = \deg(h_2 \oplus 1) = 2$, что также вытекает из вида функций, принимающих максимальное значение уровня аффинности [4].

Теорема 2. *Пусть* $f \in \mathcal{F}_n$ *— симметрическая булева функция,* $\deg f = d$, $d > 1$. *Тогда* $\mathrm{la} f > n - d$.

Доказательство. Поскольку f симметрическая, то, учитывая лемму 1, для коэффициентов АНФ подфункции функции f имеем:

$$\lambda_{f^{a_1,\ldots,a_k}_{1,\ldots,k}}(\alpha') = [\lambda]^{0,\ldots,0}_{1,\ldots,k}(\alpha') \oplus \bigoplus_{\substack{\mathbf{v}\in V_k,\\ \mathbf{0}\prec\mathbf{v}\preccurlyeq\mathbf{a}}} [\lambda]^{v_1,\ldots,v_k}_{1,\ldots,k}(\alpha').$$

Так как $\deg f = d$ и f симметрическая, то $\lambda_f(\alpha) = 1$ для любого вектора $\alpha \in V_n$, $\mathrm{wt}(\alpha) = d$, и $\lambda_f(\beta) = 0$ для любого вектора $\beta \in V_n$, $\mathrm{wt}(\beta) > d$.

Пусть теперь $k \leqslant n-d$. Возьмём вектор $\alpha' = (0,\ldots,0,1,\ldots,1)^\top \in V_{n-k}$, где 1 стоят в последних d координатах. Тогда первое слагаемое правой части равенства (1) равно 1, а второе слагаемое равно 0 при любом выборе $\mathbf{a}$, то есть $\lambda_{f^{a_1,\ldots,a_k}_{1,\ldots,k}}(\alpha') = 1$ и $\deg f^{a_1,\ldots,a_k}_{1,\ldots,k} \geqslant d > 1$, следовательно $\mathrm{la} f > n - d$.

Работа поддержана РФФИ (номер проекта 07-01-00154).

Список литературы

1. Canteaut A., Videau M. Symmetric boolean functions // IEEE Transactions on Information Theory. — 2005. — V. 51, №. 8. — P. 2791–2811.

2. Логачёв О. А., Сальников А. А., Ященко В. В. Комбинирующие k-аффинные функции // МАБИТ 2003. Материалы конференции. (МГУ, 23–24 октября 2003 г.). — М.: МЦНМО, 2004. — С. 176–178.

3. Логачёв О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004.

4. Буряков М. Л., Логачёв О. А. Об уровне аффинности булевых функций // Дискретная математика. — 2005. — Т. 17, № 4. — С. 98–107.

КОМБИНАТОРИКА НУЛЬМЕРНЫХ ИДЕАЛОВ И МОДУЛЯРНОЕ РАЗДЕЛЕНИЕ СЕКРЕТА

Т. В. Галибус, Г. В. Матвеев (Минск)

Первоначально модулярное разделение секрета изучалось лишь в кольце целых чисел [1, 2]. При таком подходе секретом считается натуральное число s, а секретом i-го участника — натуральный модуль m_i и наименьший неотрицательный вычет s по этому модулю $s = s_i(\mathrm{mod} m_i)$. Группа участников A пытается восстановить секрет, решая систему сравнений $x \equiv s_i(\mathrm{mod} m_i), i \in A$.

Этот подход выдвинул несколько задач комбинаторного характера, касающихся построения модулей m_i и секрета s. Некоторые из них проще решаются в кольце полиномов $F_q[x]$ над полем Галуа [3, 4]. Сейчас мы предлагаем обобщение модулярного подхода на случай кольца полиномов от нескольких переменных $F_q[X]$, где $X = (x_1, x_2, .., x_m)$. В этом кольце есть все необходимое для модулярного разделения секрета. В качестве секрета берется полином $S(X) \in F_q[X]$, а в качестве модуля участника — нульмерный идеал I. В этом случае корректно определен вычет секрета по модулю идеала $S(X)(\mathrm{mod} I)$, при условии, что задано мономиальное упорядочение, а для восстановления секрета имеется CRT-алгоритм [5].

Будем говорить, что на множестве участников $\mathcal{P} = \{1, 2, ..., t\}$ задана структура доступа, если указано семейство Γ разрешенных подмножеств. Все остальные подмножества называются запрещенными. Предполагается выполненным условие монотонности $A \in \Gamma, A \subset A' \Rightarrow A' \in \Gamma$. Пусть I — нульмерный идеал в кольце $F_q[X]$. Назовем его степенью размерность фактор-кольца как векторного пространства над полем F_q, т.е. $\deg I = \dim_{F_q} F_q[X]/I$. Укажем несколько свойств нульмерных идеалов, аналогичных свойствам неприводимых полиномов, которые затем применяются для построения модулярных реализаций структур доступа. Первые два из них скорее всего известны, но мы не нашли ссылку.

Теорема 1. *Пусть I_1, I_2 — нульмерны и взаимно просты. Тогда* $\deg I_1 I_2 = \deg I_1 + \deg I_2$.

Доказательство следует из известного варианта CRT: $R/I_1 I_2 \cong R/I_1 \oplus R/I_2$.

Обозначим через $N_q(n)$ число нормированных неприводимых полиномов степени n в кольце $F_q[x]$, а через $\overline{N}_q(n)$ — число максимальных идеалов степени n в кольце $F_q[X]$.

Теорема 2. $\overline{N}_q(n) = N_{q^n}(n)$.

Доказательство. В классическом случае формула для $N_q(n)$ выводится из того, что $q^n = \deg \prod_{\deg f|n} f(x)$, где произведение распространено на все неприводимые полиномы $f(x), \deg(f(x))|n$. Применяя теорему 1, можно показать, что $\deg \prod_{\deg I|n} I = q^{mn}$, а затем применить обращение Мебиуса.

Обозначим через $C_q(n)$ максимальное число попарно взаимно простых радикальных идеалов степени n в кольце $F_q[X]$.

Теорема 3. $\overline{C}_q(n) = \sum_{l \leq \frac{n}{2}} N_{q^n}(l) + N_{q^m}(n)$, *при нечетном* n.

$\overline{C}_q(m) = \sum_{l \leq \frac{m-2}{2}} N_{q^m}(l) + [\frac{1}{2} N_{q^m}(\frac{n}{2})] + N_{q^m}(n)$, *при четном* n.

В случае $m = 1$ это утверждение доказано нами в работах [3, 4]. В общем случае, рассуждения легко обобщаются. Надо только воспользоваться тем, что для радикального идеала примарные компоненты являются максимальными идеалами.

Перейдем сейчас к модулярной реализации схемы доступа на множестве участников P. Напомним, что для модулярной реализации по Миньотту необходимо чтобы модули участников $P_1, P_2, ..., P_t$ и секрет $S(X) \in F_q[X]$ были такими, чтобы выполнялось условие:

$$S(X) = S(X)(\mathrm{mod} \bigcap_{i \in A} P_i), A \in \Gamma; S(X) \neq S(X)(\mathrm{mod} \bigcap_{i \in A} P_i), A \notin \Gamma,$$

где правая часть — результат приведения секрета $S(X)$ по указанному идеалу. Другими словами, секрет $S(X)$ должен быть приведен по модулю произведения для всех разрешенных подмножеств и не является таковым для запрещенных. Напомним, что для всякого идеала $I \in F_q[X]$ приведенными являются лишь линейные комбинации приведенных мономов из $RT(I)$ [5].

Имеется еще модулярная реализация и в смысле Асмуса—Блюма, отличающаяся тем, что секрет приводится по дополнительному модулю [1].

Теорема 4. *Любая схема доступа* Γ *имеет модулярные реализации в любом кольце* $F_q[X]$ *по Миньотту и Асмусу—Блюму.*

Доказательство. Рассмотрим случай реализации по Миньотту. Выберем сначала попарно взаимно простые нульмерные идеалы $P_1, P_2, ..., P_l$, где l — число максимальных по включению запрещенных подмножеств. По теореме 3 это возможно в любом кольце $F_q[X]$. Более того, можно считать, что все идеалы $P_1, P_2, .., P_l$ — одной степени. Первоначально присвоим каждому участнику единичный идеал. Берем затем какое-нибудь максимальное по включению запрещенное множество B и модули всех участников, не входящих

в B, умножаем на идеал P_1. Поступаем так с каждым максимальным запрещенным подмножеством. В результате всех умножений имеем следующее.

Для всякого разрешенного множества участников A пересечение (произведение) всех их модулей (идеалов) будет равно произведению $P_1P_2..P_l$, а для всякого запрещенного B соответствующее пересечение будет собственным делителем этого произведения. С точностью до нумерации, можно сказать, что $\bigcap_{i\in B} P_i = P_1P_2...P_{l_1}$, где $l_1 < l$. Следовательно, $RT(P_1P_2...P_{l_1}) \subset RT(P_1P_2...P_l)$.

Для каждого максимального запрещенного множества B выберем по одному моному $S_B(X)$ из $RT(P_1P_2...P_l)\backslash RT(P_1P_2...P_{l_1})$, а в качестве самого секрета возьмем линейную комбинацию мономов $S_B(X)$. Таким образом, полином $S(X)$ будет приведенным по $\mathrm{mod}(\bigcap_{i\in A} P_i)$ и неприведенным по $\mathrm{mod}(\bigcap_{i\in B} P_i)$. Один из мономов $S_B(X)$ может подходить для нескольких запрещенных множеств B. Поэтому общее число мономов секрета $S(X)$ не превосходит l.

Замечание. Теоремы 1–3 отчасти объясняют, почему мы используем лишь нульмерные идеалы.

Список литературы

1. Asmuth C. A., Bloom J. A modular approach to key safeguarding // IEEE Transactions on Information Theory. — 1983. — V. 29. — P. 156–169.

2. Mignotte M. How to share a secret // Lecture Notes in Computer Science. — 1983. — V. 149. — P. 371–375.

3. Galibus T., Matveev G. Generalized mignotte sequences in polynomial rings // Electronic Notes on Theoretical Computer Science. — 2007. — V. 186. — (To appear).

4. Galibus T., Matveev G. Mignotte sequences in polynomial rings // Proc. of ICS 2006, International Workshop on Information and Computer Security (Timisoara, Romania). — 2006. — P. 39–44.

5. Becker T., Weispfenning V. Gröbner Bases // A computational approach to commutative algebra. — Springer-Verlag, 1993.

О ВЕСОВОЙ ФУНКЦИИ КОДА, АССОЦИИРОВАННОГО С ПЛАТОВИДНОЙ ФУНКЦИЕЙ

М. П. Денисенко (Москва)

Конструкциии, связанные с булевыми функциями, занимают заметное место в теории кодирования и криптологии. Так коды Рида — Маллера, построенные на основе булевых функций, тесно связаны как с вопросами построения криптографических примитивов с одной стороны, так и с разработкой методов криптографического анализа — с другой. В работе [1] была предложена новая кодовая конструкция, основывающаяся уже не на классе булевых функций, а на конкретной булевой функции. С помощью этой конструкции в настоящей работе мы рассматриваем весовую характеризацию линейных кодов, ассоциированных с платовидными функциями. Получена весовая функция соответствующих кодов и дуальных к ним кодов.

Пусть $\mathbb{F}_2 = GF(2)$ и $\mathbb{N}$ — множество натуральных чисел. Для векторного пространства $\mathrm{V}_n = \mathbb{F}_2^n$, $n \in \mathbb{N}$ через $x = (x_1, \ldots, x_n)$ будем обозначать наборы длины n, являющиеся элементами этого пространства. Элементы x векторного пространства V_n будем называть векторами. Обозначим через " $\oplus$ " — операцию сложения по модулю 2 в поле $\mathbb{F}_2$. Пусть $f : \mathrm{V}_n \to \mathbb{F}_2$ — булева функция от n переменных — отображение из V_n в $\mathbb{F}_2$, $\mathcal{F}_n$ — множество всех булевых функций от n переменных.

Определение математических объектов, используемых в данной работе, и их основные свойства можно найти в [1–3].

Определение [1]. Пусть n — четное, $f \in \mathcal{F}_n$, $\mathrm{supp}(f) = \{\mathbf{u}^1, \mathbf{u}^2, \ldots, \mathbf{u}^t\}$, где $t = \mathrm{wt}(f)$. Рассмотрим матрицу G_f размера $n \times t$, столбцами которой являются векторы множества $\mathrm{supp}(f)$: $G_f = \left[\mathbf{u}^1\ \mathbf{u}^2\ \ldots\ \mathbf{u}^t\right]$. Код $\mathbf{C}_f$, порождаемый этой матрицей $\mathbf{C}_f = \{\mathbf{c}_\mathbf{v} \mid \mathbf{v} = (v_1, \ldots, v_n) \in \mathrm{V}_n\}$, где $\mathbf{c}_\mathbf{v} = \mathbf{v}G_f = \left(\langle \mathbf{v}, \mathbf{u}^1\rangle, \ldots, \langle \mathbf{v}, \mathbf{u}^t\rangle\right)$, называется *кодом, ассоциированным с булевой функцией* f.

Определение. Пусть $f \in \mathcal{F}_n$. Если существует натуральное число $r \in \mathbb{N}$, $0 \le r \le n$, такое, что квадрат каждого коэффициента Уолша — Адамара равен либо 2^{2n-2r}, либо 0, то функция f называется *платовидной функцией порядка* $2r$.

Для каждой платовидной функции f порядка $2r$ определен ее носитель — множество $S_f \subseteq \mathrm{V}_n$ такое, что $\sharp S_f = 2^{2r}$ и

$$W_f^2(\mathbf{u}) = \begin{cases} 2^{2n-2r}, & \text{если } \mathbf{u} \in S_f; \\ 0, & \text{в противном случае.} \end{cases}$$

Множество платовидных функций с фиксированным носителем $S \subseteq \mathrm{V}_n$ обозначим через $\mathcal{PF}_n(S)$.

Основная задача данной работы связана с вычислением весовой функции кода, ассоциированного с платовидной функцией $f \in \mathcal{PF}_n(S)$. При этом, для упрощения задачи, на множество-носитель платовидной функции S (вектора, на которых коэффициенты Уолша — Адамара отличны от нуля) накладывается ограничение: рассматриваются линейные подпространства или сдвиги линейных подпространства. После получения весовой функции соответствующего кода $\mathbf{C}_f$, используя тождество Мак-Вильямс, можно получить весовой спектр дуального к $\mathbf{C}_f$ кода.

Теорема. *Пусть* $f \in \mathcal{PF}_n$, $S \subseteq \mathrm{V}_n$ — *линейное подпространство пространства* V_n, $\dim S = 2r$,

$$\boldsymbol{C}_f = \{\, \boldsymbol{c}_v \mid \boldsymbol{v} = (v_1, \ldots, v_n) \in \mathrm{V}_n \}$$

является ассоциированным с f *кодом,* $\tilde{f}$ — *функция, дуальная к бент-функции* f.. *Тогда размерность кода* $\boldsymbol{C}_f$ *равна* n *и весовой спектр кода* $\boldsymbol{C}_f$ *имеет следующий вид*:

1)

$i = \mathrm{wt}(\boldsymbol{c}_v)$	$A_i = \sharp\{\boldsymbol{c}_v \in \boldsymbol{C}_f \mid i = \mathrm{wt}(\boldsymbol{c}_v)\}$
0	1
$2^{n-2} - 2^{n-r-1}$	$2^{2r-1} - 2^{r-1}$
$2^{n-2} - 2^{n-r-2}$	$2^n - 2^{2r}$
2^{n-2}	$2^{2r-1} + 2^{r-1} - 1$

, *если* $W_f(\mathbf{0}) > 0$, $W_{\tilde{f}}(\mathbf{0}) > 0$;

2)

$i = \mathrm{wt}(\boldsymbol{c}_v)$	$A_i = \sharp\{\boldsymbol{c}_v \in \boldsymbol{C}_f \mid i = \mathrm{wt}(\boldsymbol{c}_v)\}$
0	1
$2^{n-2} - 2^{n-r-2}$	$2^n - 2^{2r}$
2^{n-2}	$2^{2r-1} - 2^{r-1} - 1$
$2^{n-2} - 2^{n-r-1}$	$2^{2r-1} + 2^{r-1}$

, *если* $W_f(\mathbf{0}) > 0$, $W_{\tilde{f}}(\mathbf{0}) < 0$;

3)

$i = \mathrm{wt}(\boldsymbol{c}_v)$	$A_i = \sharp\{\boldsymbol{c}_v \in \boldsymbol{C}_f \mid i = \mathrm{wt}(\boldsymbol{c}_v)\}$
0	1
$2^{n-2} + 2^{n-r-2}$	$2^n - 2^{2r}$
2^{n-2}	$2^{2r-1} - 2^{r-1} - 1$
$2^{n-2} + 2^{n-r-1}$	$2^{2r-1} + 2^{r-1}$

, *если* $W_f(\mathbf{0}) < 0$, $W_{\tilde{f}}(\mathbf{0}) > 0$;

4)

$i = \mathrm{wt}(\boldsymbol{c}_v)$	$A_i = \sharp\{\boldsymbol{c}_v \in \boldsymbol{C}_f \mid i = \mathrm{wt}(\boldsymbol{c}_v)\}$
0	1
$2^{n-2} + 2^{n-r-2}$	$2^n - 2^{2r}$
2^{n-2}	$2^{2r-1} - 2^{r-1} - 1$
$2^{n-2} + 2^{n-r-1}$	$2^{2r-1} + 2^{r-1}$

, *если* $W_f(\mathbf{0}) < 0$, $W_{\tilde{f}}(\mathbf{0}) < 0$.

Теорема 2. *Пусть* $f \in \mathcal{PF}_n$, $S \subseteq \mathrm{V}_n$ — *некоторое подмножество линейного пространства* V_n, $\sharp S = 2^{2r}$, $r \in \mathbb{N}$, $\boldsymbol{C}_f = \{\boldsymbol{c}_v \mid \boldsymbol{v} = (v_1, \ldots, v_n) \in \mathrm{V}_n\}$ *является ассоциированным с* f *кодом. Тогда вес кодового слова* $\boldsymbol{c}_v$ *принимает одно из следующих значений*:

$$2^{n-2} \pm 2^{n-r-2},\ 2^{n-2} \pm 2^{n-r-1},\ 2^{n-2},\ 0.$$

Список литературы

1. Carlet C. Boolean functions for cryptography and error correcting codes. — `http://www-rocq.inria.fr/codes/Claude.Carlet/chap-fcts-Bool.pdf`.

2. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004.

3. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. — М.: Связь, 1979.

СВОЙСТВА ДЕРЕВЬЕВ ВЫВОДА СЛОВ В СТОХАСТИЧЕСКОЙ КС-ГРАММАТИКЕ С НЕСКОЛЬКИМИ КЛАССАМИ НЕТЕРМИНАЛОВ

Л. П. Жильцова, М. Н. Корокозов (Нижниий Новгород)

Рассматриваются свойства деревьев вывода слов для одного класса разложимых стохастических КС-грамматик. Грамматики из рассматриваемого класса содержат в отличие от ранее рассмотренных случаев [1, 2] произвольное число классов нетерминальных символов (нетерминалов).

Стохастической порождающей КС-грамматикой называется система $G = < V_T, V_N, R, s >$, где V_T и V_N — алфавиты терминальных и нетерминальных символов (терминалов и нетерминалов) соответственно; $s \in V_N$ — аксиома, R — конечное множество правил, $R = \cup_{i=1}^{k} R_i$, где k — мощность алфавита V_N и $R_i = \{r_{i1}, \ldots, r_{i,n_i}\}$ — множество правил с одинаковой левой частью A_i. Каждое правило в R_i имеет вид:

$$r_{ij} : A_i \xrightarrow{p_{ij}} \beta_{ij}, j = 1, ..., n_i, \text{ где } A_i \in V_N, \beta_{ij} \in (V_T \cup V_N)^*,$$

где p_{ij} — вероятность применения правила r_{ij}, которая удовлетворяет условиям: $0 < p_{ij} \leq 1$, $\sum_{j=1}^{n_i} p_{ij} = 1$.

Слову α КС-языка соответствует последовательность правил грамматики (вывод), с помощью которой α выводится из аксиомы

s, а выводу соответствует дерево вывода [3]. Вероятность вывода и соответствующего ему дерева вывода определяется как произведение вероятностей правил, образующих вывод. В работе рассматриваются согласованные КС-грамматики, т. е. грамматики, в которых вероятности выводов задают распределение вероятностей на множестве деревьев вывода слов языка.

Будем говорить, что нетерминал A_j следует за нетерминалом A_i ($A_i \to A_j$), если из A_i выводимо хотя бы одно слово, содержащее нетерминал A_j. Классом нетерминалов назовем максимальное по включению подмножество $K \subseteq V_N$ такое, что $A_i \to A_j$ для любых $A_i, A_j \in K$. Будем говорить, что класс K_i предшествует классу K_j ($K_i \preceq K_j$), если для любых $A_{i_1} \in K_i$, $A_{i_2} \in K_j$ верно $A_{i_1} \to A_{i_2}$. Множество нетерминалов грамматики является объединением конечного числа непересекающихся классов.

В работе рассматривается грамматика с классами $\{K_0, K_1, \ldots, K_m\}$ нетерминалов, причем $K_0 \preceq K_i$ для $i = 1 \ldots, m$ и $K_i \not\preceq K_j$ при $i, j \in \{1, \ldots, m\}$ и $i \neq j$. Аксиому грамматики будем обозначать далее через A_1 и считать, что $A_1 \in K_0$.

Важной характеристикой для стохастической КС-грамматики является матрица первых моментов A.

Значение элемента a_l^i матрицы есть математическое ожидание числа нетерминальных символов A_l в правых частях правил грамматики с одинаковым нетерминалом A_i в левой части.

Максимальный по модулю собственный корень матрицы первых моментов (перронов корень) обозначим через r. Известно, что для согласованной КС-грамматики $r \leq 1$. В работе исследуется докритический случай, т. е. случай, когда $r < 1$.

Матрица A первых моментов рассматриваемой грамматики имеет следующий вид:

$$A = \begin{pmatrix} C_0 & C_{01} & \ldots & C_{0m} \\ 0 & C_1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & C_m \end{pmatrix}, \qquad (1)$$

где C_i — неразложимая подматрица, соответствующая классу K_i ($i = 0, 1, \ldots, m$), и C_{0i} — подматрица на пересечении строк, соответствующих классу K_0, и столбцов, соответствующих классу K_i ($i = 1, \ldots, m$).

Обозначим через r_i перронов корень матрицы C_i. Очевидно, перронов корень всей матрицы первых моментов удовлетворяет условию $r = \max\{r_0, r_1, \ldots, r_m\}$. Определим множество индексов $J = \{j \in \{0, 1, \ldots, m\} | r_j = r\}$.

Рассмотрим множество D^t деревьев вывода высоты t, корень которых помечен аксиомой A_1.

Пусть A_i — нетерминал грамматики из класса K_l и r_{ij} — правило с A_i в левой части. Через $M_{ij}(t,\tau)$ обозначим математическое ожидание числа применений правила r_{ij} на ярусе τ в деревьях вывода из D^t.

В зависимости от значений собственных корней матрицы первых моментов A можно выделить три основных случая, определяющих значение $M_{ij}(t,\tau)$: a) $0 \in J$ и $\mid J \mid > 1$; b) $0 \in J$ и $\mid J \mid = 1$; c) $0 \notin J$.

Теорема 1. *Пусть G — стохастическая КС-грамматика с матрицей первых моментов вида* (1)*, для которой $0 \in J$, $\mid J \mid > 1$ и $A_i \in K_l$. Тогда при $t \to \infty$, $\tau \to \infty$, $t - \tau \to \infty$:*

1) $M_{ij}(t,\tau) \sim \frac{p_{ij} \cdot (t-\tau)}{t} \cdot (Q_{ij} + G_i)$ *для* $l = 0$;

2) $M_{ij}(t,\tau) \sim \frac{p_{ij} \cdot (t-\tau)}{t} \cdot G_i$ *для* $l \notin J$;

3) $M_{ij}(t,\tau) \sim \frac{p_{ij}}{t} \cdot \left(\left(Q_{ij} + G_i^{'} \right) \cdot \tau + G_i \cdot (t-\tau) \right)$ *для* $l \in J$, $l \neq 0$.

Теорема 2. *Пусть G — стохастическая КС-грамматика с матрицей первых моментов вида* (1) *и $J = \{0\}$ или $0 \notin J$. Тогда при $t \to \infty$, $\tau \to \infty$, $t - \tau \to \infty$ для любого правила r_{ij}*

$$M_{ij}(t,\tau) \to w_{ij},$$

где w_{ij} — константа, определяемая грамматикой G.

Работа выполнена при финансовой поддержке РФФИ (проект 07-01-00739-а).

Список литературы

1. Жильцова Л. П. Закономерности применения правил грамматики в выводах слов стохастического контекстно-свободного языка // Математические вопросы кибернетики. Вып. 9. — М.: Наука, 2000. — С. 101–126.

2. Борисов А. Е. О свойствах стохастического КС-языка, порожденного грамматикой с двумя классами нетерминальных символов // Дискретный анализ и исследование операций. Серия 1. — 2005. — Т. 12, № 3. — С. 3–31.

3. Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции. Том 1. — М.: Мир, 1978.

О ПРИВОДИМОСТИ n-АРНЫХ КВАЗИГРУПП И СВИТЧИНГОВОЙ РАЗДЕЛИМОСТИ ГРАФОВ

Д. С. Кротов, В. Н. Потапов (Новосибирск)

Множество Σ с заданной n-арной операцией $Q(\cdot) : \Sigma^n \to \Sigma$ называется n-арной квазигруппой порядка $|\Sigma|$ (обозначаемой той же буквой Q), если в отношении $x_0 = Q(x_1, \ldots, x_n)$ любые n элементов из x_0, x_1, …, x_n однозначно определяют оставшийся элемент.

Определение симметрично относительно всех $n+1$ переменных z_0, z_1, …, z_n, поэтому иногда удобно использовать симметричную форму для отношения $z_0 = Q(z_1, \ldots, z_n)$, которую обозначим следующим образом: $Q\langle z_0, z_1, \ldots, z_n\rangle \iff z_0 = Q(z_1, \ldots, z_n)$.

Если мы зафиксируем значения $l \in \{1, \ldots, n\}$ переменных в предикате $Q\langle z_0, \ldots, z_n\rangle$ то полученный $(n-l+1)$-арный предикат соответствует некоторой $(n-l)$-арной квазигруппе. Эта квазигруппа называется *ретрактом* Q. Скажем, что n-арная квазигруппа Q является A-*приводимой*, если

$Q\langle z_0, \ldots, z_n\rangle \iff Q'(z_{a_1}, \ldots, z_{a_k}) = Q''(z_{b_1}, \ldots, z_{b_{n-k+1}})$,

где $A = \{a_1, \ldots, a_k\} = \{0, \ldots, n\} \backslash \{b_1, \ldots, b_{n-k+1}\}$ и Q', Q'' есть k-арная и $(n-k+1)$-арная квазигруппы. n-Арная квазигруппа *перестановочно приводима* (далее просто *приводима*), если она A-приводима для некоторого $A \subset \{0, \ldots, n\}$, $1 < |A| < n$.

Рассмотрим n-арные квазигруппы над множеством $\Sigma = Z_2^2 = \{[0,0], [0,1], [1,0], [1,1]\}$ и частичные булевы функции, определенные на подмножестве E_0^{n+1} булева n-куба $E^{n+1} = \{0,1\}^{n+1}$, состоящем из всех слов с четным числом единиц. Заметим, что, поскольку любая координата в E_0^{n+1} есть сумма остальных, частичную булеву функцию, определенную на E_0^{n+1}, можно рассматривать как булеву функцию на E^n, однако, форма, симметричная относительно всех $n+1$ координат, для нас опять более удобна.

Для функции $\lambda : E_0^{n+1} \to \{0,1\}$ определим n-арную квазигруппу Q_λ: $Q_\lambda\langle [x_0, y_0], ..., [x_n, y_n]\rangle \iff \sum x_i = 0 \ \& \ \sum y_i = \lambda(x_0, ..., x_n)$.

Также определим частичную квадратичную булеву функцию $\lambda_G : E_0^{n+1} \to \{0,1\}$, связанную с (простым) графом $G = (\{0, ..., n\}, E)$:

$$\lambda_G(x_0, \ldots, x_1) = \bigoplus_{\{a,b\} \in E, a<b} x_a x_b.$$

Граф $G = (V, E)$ назовем *свитчингово разделимым*, если для некоторого множества $U \subset V$ граф $(V, E \triangle E_{U, V\backslash U})$ состоит из двух

несвязных между собой частей, в каждой больше одной вершины ($E_{U,V\setminus U}$ есть множество всех ребер из U в $V \setminus U$).

Теорема 1. *Для того, чтобы n-арная квазигруппа Q_{λ_G} была приводима, необходимо и достаточно, чтобы граф G был свитчингово разделим.*

Обозначим через $\kappa(Q)$ максимальную арность неразделимого ретракта n-арной квазигруппы Q. Очевидно, $\kappa(Q) \in \{2, \ldots, n-1\}$.

Теорема 2. *Пусть Q есть n-арная квазигруппа над Σ, $n \geq 4$. Тогда*:

1. *Если $\kappa(Q) \leq n-3$, то n-арная квазигруппа Q приводима.*
2. *Если $\kappa(Q) = n-2$ и порядок $|\Sigma|$ простой, то Q приводима.*
3. *Если $\kappa(Q) = n-2$, n четно и порядок $|\Sigma|$ кратен 4 или бесконечен, то существует пример неприводимой Q.*
4. *Для любого $|\Sigma| > 3$ существует неприводимая Q с $\kappa(Q) = n-1$.*

Следствие. *Любая неприводимая n-арная квазигруппа простого порядка имеет неприводимый $(n-1)$-арный ретракт, что неверно для порядка, кратного 4.*

Для графа $G = (V, E)$ обозначим через $\kappa(G)$ максимальное число вершин собственного порожденного подграфа G, не являющегося свитчингово разделимым ($\kappa(G) \in \{3, \ldots, |V|-1\}$).

Теорема 3. *Справедливы следующие утверждения*:

1. *Если $\kappa(G) \leq |V|-3$, то G свитчингово разделим.*
2. *Для любого нечетного $|V| \geq 5$ существует свитчингово неразделимый граф G с $\kappa(G) = |V|-2$.*
3. *Если $\kappa(G) \leq |V|-2$ и $|V| \in \{6, 8\}$ то G свитчингово разделим.*

Аналогичная теорема верна для разделимости частичных булевых функций $E_0^{n+1} \to \{0, 1\}$, где разделимость понимается как представимость в виде дизъюнктной суммы булевых функций от двух и более аргументов. Заметим, что, согласно теореме 1, п. 1 теоремы 3 следует из п. 1 теоремы 2, а п. 3 теоремы 2 для порядка 4 — из п. 2 теоремы 3. Некоторые подслучаи теорем разобраны в работах [1–4].

Список литературы

1. Krotov D. S., Potapov V. N. n-Ary quasigroups of order 4 // `arXiv:math/0701519.`

2. Krotov D. S. On reducibility of n-quasigroups // Submitted to Discr. Math. — `arXiv:math/0607284.`

3. Krotov D. S. On irreducible n-ary quasigroups with reducible retracts // Eur. J. Comb. — (In press.) — `DOI: 10.1016/j.ejc.2007.01.005.`

4. Krotov D. S., Potapov V. N. On reconstructing reducible n-ary quasigroups and switching subquasigroups // arXiv:math/0608269.

НОВЫЙ ПОДХОД К ОЦЕНКЕ НЕЛИНЕЙНОСТИ ВЫСОКИХ ПОРЯДКОВ БУЛЕВОЙ ФУНКЦИИ ЧЕРЕЗ ЗНАЧЕНИЕ ЕЕ АЛГЕБРАИЧЕСКОЙ ИММУННОСТИ

М. С. Лобанов (Москва)

В работе рассматривается вопрос о взаимосвязи двух важных криптографических свойств булевых функций — алгебраической иммунности и нелинейности r-го порядка. Мы дадим новый подход к проблеме нахождения нижней оценки нелинейности r-го порядка функции через значение ее алгебраической иммунности, а также получим новую оценку, улучшающую известные ранее результаты.

В работах [1, 2] были получены результаты, эквивалентные следующим оценкам на нелинейность r-го порядка: $nl_r(f) \geq \sum_{i=0}^{k-r-1} \binom{n}{i}$; $nl_r(f) \geq 2\sum_{i=0}^{k-r-1} \binom{n-r}{i}$, где k — алгебраическая иммунность функции f от n переменных.

Отметим, что ни одна из двух приведенных выше оценок для нелинейности r-го порядка не влечет другую.

В данной работе мы покажем, что задача получения оценки нелинейность r-го порядка через значение алгебраической иммунности полностью сводиться к оценки размерности определенного линейного пространства. И как следствие из этого получим новую оценку, перекрывающую обе существовавшие ранее.

Известно, что булева функция единственным образом представляется полиномом.

Степенью булевой функции называется длина самого длинного слагаемого в ее полиноме (количество переменных в этом слагаемом).

Булева функция g над F_2^n называется *аннигилятором* булевой функции f над F_2^n, если $fg = 0$.

Очевидно, что аннигиляторы f образуют линейное подпространство в пространстве всех булевых функций от n переменных.

Алгебраической иммунностью $AI(F)$ булевой функции f над F_2^n называется степень булевой функции g над F_2^n, где g не равная

тождественно нулю функция с минимальной степенью, такая что $fg = 0$ или $(f+1)g = 0$.

Известно [3], что для любой f над F_2^n выполнено $AI(f) \leq \lceil \frac{n}{2} \rceil$.

Весом $wt(x)$ набора x из F_2^n называется число единиц в x.

Расстояние между булевыми функциями f_1 и f_2 определяется как $d(f_1, f_2) = \mid \{x \in F_2^n \mid f_1(x) \neq f_2(x)\} \mid$.

Нелинейностью r-го порядка $nl_r(f)$ булевой функции f над F_2^n называется $\min\limits_{l,\ deg(l) \leq r} d(f, l)$.

Пусть h — булева функция от n переменных. Обозначим через $An_k(h)$ линейное пространство аннигиляторов степени не выше k и через $d_{k,h}$ его размерность.

Пусть $C = \{\overline{x}_1, \ldots, \overline{x}_n\}$ — множество двоичных наборов длины n. Для любого $k \leq n$, произвольному набору $x = (x_1, \ldots, x_n)$ можно сопоставить однородное линейное уравнение $g = 0$, где

$$g = a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j + \cdots + \sum_{1 \leq i_1 \leq \ldots \leq i_k \leq n} a_{i_1 \ldots i_k} x_{i_1} \ldots x_{i_k}.$$

Назовем *k-рангом* множества C ранг системы линейных уравнений, полученных таким образом из наборов множества C. Обозначим его через $r_k(C)$.

Ищем для функции f аннигиляторы степени не выше k методом неопределенных коэффициентов. Функция g является аннигилятором f тогда и только тогда, когда равенство $f(x) = 1$ влечет равенство $g(x) = 0$. Получаем систему линейных уравнений. Несложно заметить, что $d_{k,f} = \dim(An_k(f)) = \sum_{i=0}^{k} \binom{n}{i} - r_k(supp(f))$.

Утверждение 1. Пусть f и f_0 функции от n переменных, $AI(f_0) \geq k$. Тогда $d(f, f_0) \geq \dim(An_{k-1}(f)) + \dim(An_{k-1}(f+1))$.

Пусть h булева функция от n переменных. Обозначим через $B_k(h)$ линейное пространство функций от n переменных степени не выше k, которые при умножении на h снова дают функции степени не выше k.

Утверждение 2. $\dim(An_k(f)) + \dim(An_k(f+1)) = \dim(B_k(f))$.

Лемма 1. *Пусть* $r_k(supp(f)) = wt(f)$, *где* $k < \lceil \frac{n}{2} \rceil$, *тогда* $\dim(An_k(f+1)) = 0$.

Следствие. *Пусть* $\dim(An_k(f)) = \sum_{i=0}^{k} \binom{n}{i} - wt(f)$, *где* $k \leq \lceil \frac{n}{2} \rceil$, *тогда* $\dim(An_{\lceil \frac{n}{2} \rceil - 1}(f+1)) = 0$.

Следствие. *Пусть* $n = 2k+1$ *и* $An_k(f) = 0$, *тогда* $AI(f) = k+1$.

Утверждение 3. *Пусть* $deg(f) \leq \lceil \frac{n}{2} \rceil$, $k \leq \lceil \frac{n}{2} \rceil$, *тогда существует функция* g, *такая что* $AI(g) = k$ *и* $d(f,g) = \dim(B_{k-1}(f))$.

Таким образом, с учетом утверждений 1–3 мы доказали, что задача нахождения наиболее сильной оценки нелинейности r-го порядка функции через значение ее алгебраической иммунности k полностью сводиться к нахождению $\min_{deg(g)\leq r} \dim(B_{k-1}(g))$. Сформулируем это в качестве теоремы.

Теорема. *Пусть* $f(x_1, \ldots, x_n)$ *имеет* $AI(f) = k$. *Тогда*:

1) $nl_r(f) \geq \min_{deg(g)\leq r} \dim(B_{k-1}(g))$;

2) *существует функция* f_0 *удовлетворяющая условию* $AI(f_0)=k$, *для которой* $nl_r(f_0) = \min_{deg(g)\leq r} \dim(B_{k-1}(g))$.

Утверждение 4. *Пусть* $deg(f) = r$. *Тогда*

$$\dim(B_{k-1}(f)) \leq \sum_{i=0}^{k-r-1} \binom{n}{i} + \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i}.$$

Доказательство. Можно считать, что полином f содержит слагаемое $x_1 x_2 \ldots x_r$. Рассмотрим функции вида $g_1 + f g_2$, где g_1 любая функции степени не более $(k-r-1)$, а g_2 любая функция от $x_{r+1}, \ldots, x_n$ степени не более $(k-r-1)$, содержащая лишь мономы длины не менее $k-2r$.

Несложно проверить, что все такие функции принадлежат $B_{k-1}(f)$. Проверка того, что все функции различны, сводится к проверке того, что из $g_1 + f g_2 = 0$ следует $g_1 = 0$ и $g_2 = 0$. Равенство $g_2 = 0$ следует из того, что в противном случае функция $f g_2$ содержала бы моном длины не менее $(k-r)$, который был бы и в полиноме f (т. к. $\deg(f_1) \leq (k-r-1)$). Равенство $g_1 = 0$ следует непосредственно из $g_1 + f g_2 = 0$ и $g_2 = 0$.

Следствие. *Пусть* $AI(g) = k$. *Тогда*

$$nl_r(g) \geq \sum_{i=0}^{k-r-1} \binom{n}{i} + \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i}.$$

Таким образом, получена оценка, которая улучшает обе существовавших ранее оценки.

Список литературы

1. Dalai D. K., Gupta K. C., Maitra S. Results on algebraic immunity for cryptographically significant boolean functions // Lecture Notes in Computer Science. — Springer-Verlag, 2004. — V. 3348 (Indocrypt-2004). — P. 92–106.

2. Carlet C. On the higher order nonlinearities of algebraic immune functions // Lecture Notes in Computer Science. — Springer-Verlag, 2006. — V. 4117 (Crypto-2006). — P. 584–601.

3. Courtois N., Meier W. Algebraic attacks on stream ciphers with linear feedback // Lecture Notes in Computer Science. — Springer-Verlag, 2003. — V. 2656 (Eurocrypt-2003). — P. 345–359.

ОЦЕНКА РЕШЕНИЙ СРАВНЕНИЯ $R^x \equiv x \pmod{p^n}$

А. А. Логачев (Москва)

Рассмотрим задачу нахождения $x \in \mathbb{Z}$ такого, что

$$R^x \equiv x \pmod{p^n} \tag{1}$$

где $R \in \mathbb{Z}$, p — простое число, n — натуральное число.

Определение. Назовем $x \in \mathbb{R}$ *действительным решением* сравнения (1), если существует целое k: $R^x = x + kp^n$.

Понятно, что все решения сравнения (1) будут действительными решениями.

Рассмотрим семейство последовательностей $a_{k,n}$:

$$a_{k,1} = \log_R kp^n,$$
$$a_{k,m+1} = \log_R(kp^n + a_{k,m}).$$

Каждая последовательность в семействе будет возрастающей и ограниченной суммой геометрической прогрессии с первым членом $\log_R kp^n$ и знаменателем $\frac{1}{kp^n}$ (то есть числом $\frac{kp^n}{kp^n-1}\log_R kp^n$). Так как последовательность возрастает и ограничена, то она имеет предел. Положим

$$x_k = \lim_{m\to\infty} a_{k,m}.$$

Нетрудно показать, что x_k будет действительным решением сравнения (1).

Кроме того, для любых k, m выполнено $x_k > a_{k,m}$.

Таким образом для любых k:

$$\log_R kp^n < x_k \le \frac{kp^n}{kp^n - 1}\log_R kp^n. \tag{2}$$

Если $x \in \mathbb{Z}$ — решение сравнения (1), то для него существует такое k, что $x_k = x$, и, исходя из неравенств (2), получаем, что

$$|x - \log_R kp^n| \leq \frac{1}{kp^n - 1} \log_R kp^n. \tag{3}$$

Пусть a_1, a_2, b_1, b_2 — целые числа, $\Lambda = b_1 \ln a_1 + b_2 \ln a_2, \ln B = \ln(\frac{b_1}{\ln a_2} + \frac{b_2}{\ln a_1}) + \ln\ln 2 + 0,47$. Тогда из [1] слудует, что

$$\ln|\Lambda| \geq -106 \ln a_1 \ln a_2 (\ln B)^2. \tag{4}$$

Пусть a_1, a_2, a_3, b_1, b_2, b_3 — целые числа, $\Lambda = b_1 \ln a_1 + b_2 \ln a_2 + b_3 \ln a_3, B = \max\{1, \max\{|b_i| \ln a_i / \ln a_3 : 1 \leq i \leq 3\}\}$ тогда из теоремы Матвеева [2] следует, что

$$\ln|\Lambda| \geq -c \ln a_1 \ln a_2 \ln a_3 \ln(1,5B), \tag{5}$$

где c не зависит от a_1, a_2, a_3, b_1, b_2, b_3.

Без ограничения общности можем считать, что x является решением сравнения $R^x \equiv x \pmod{p^n}$ и не является решением сравнения $R^x \equiv x \pmod{p^n + 1}$. В противном случае можно перейти от n к $n+1$. В силу этого можем считать, что p не делит k в оценке (3).

Также будем считать, что $R \neq H^r$ни для каких натуральных H и $r, r > 1$.

Теорема. *Справедливы следующие утверждения*:

1. *Существует такое N_0, что для всех $n > N_0$ уравнение $R^x = x + R^s p^n$ не имеет целых решений относительно x для всех натуральных s.*

2. *Существует неограниченно возрастающая функция $K(N)$, такая, что при фиксированном N для всех $n > N$ сравнение $R^x \equiv x \pmod{p^n}$ не имеет целых решений на отрезке $x \in [0, \log_R K(N) p^n]$.*

Доказательство. 1. Применением (4) к функции $\Lambda = n \ln p - (x - s) \ln R$ и получим:

$$\ln|\Lambda| \geq -35.1 (\ln B)^2 \ln R \ln p (\ln 2)^{-3} \geq -106 \ln R \ln p (\ln B)^2,$$

где $B = \ln(\frac{n}{\ln R}(\frac{2p^n - 1}{p^n - 1})) + \ln\ln 2 + 0.47$.

Кроме того, для решений x сравнения (1) из (3) при $k = R^s$ следует, что:

$$\begin{aligned}
\ln|\Lambda| = \ln|\ln p^n - (x - s)\ln R| = \ln(\ln R\,|\log_R p^n - (x - s)|) \leq \\
\leq \ln(\ln R \frac{\log_R R^s p^n}{R^s p^n - 1}) = \ln(\frac{n \ln p + s \ln R}{R^s p^n - 1}) = \\
= -\ln(R^s p^n - 1) + \ln(n \ln p + s \ln R).
\end{aligned}$$

Рассмотрим случай, когда эти оценки несовместимы:

$$-\ln(R^s p^n - 1) + \ln(n \ln p + s \ln R) \leq -106 \ln R \ln p (\ln B)^2$$

$$\ln(R^s p^n - 1) \geq 107 \ln R \ln p (\ln(\frac{n}{\ln R}(\frac{2p^n - 1}{p^n - 1})) + \ln\ln 2 + 0.47)^2 + \\ + \ln(n \ln p + s \ln R).$$

В левой части неравенства зависимость от n по существу линейная, справа же, n стоит под логарифмом. Таким образом, существует такое N_0, что для всех $n > N_0$ неравенство выполнено, что и доказывает пункт 1 теоремы.

2. Применим (5) к функции $\Lambda = \ln k + n \ln p - x \ln R$:

$$\ln|\Lambda| \geq -c \ln(1.5 \frac{kp^n}{kp^n - 1} \log_R kp^n) \ln k \ln p \ln R,$$

где c — константа, не зависящая от R, p, n, k.

С другой стороны, из (3) получаем:

$$\ln|\Lambda| < -\ln(kp^n - 1) + \ln\ln kp^n.$$

Для получения противоречия достаточно, чтобы выполнялось неравенство

$$\ln(kp^n - 1) - \ln\ln kp^n > c \ln(1.5 \frac{kp^n}{kp^n - 1} \log_R kp^n) \ln k \ln p \ln R.$$

При фиксированном K и любых $k \leq K$, в силу того, что левая часть по существу линейна по n, а в правой n стоит под логарифмом, неравенство выполнено для n начиная с некоторого. То есть, существует неограниченно возрастающая функция $N_0(K)$ такая, что для любых $n > N_0(K)$ неравентсво выполнено при $k < K$. Таким образом, для любых $k \leq K$ x_k и $n > N_0(K)$ не является решением сравнения (1). Теорема доказана.

Список литературы

1. Laurent M., Mignotte M., Nesterenko Yu. Formes lineaires en deux logarithmes et determinants d'interpolation // Journal of Number Theory. — 1977. — V. 9. — P. 87–106.

2. Матвеев Е. М. Явная нижняя оценка однородной рациональной линейной формы от логарифмов алгебраических чисел // Вестник РАН. Серия Математика. — 2000. — Т. 64, № 6. — С. 124–180.

О ЛОКАЛЬНОЙ ОБРАТИМОСТИ ОДНОГО КЛАССА БУЛЕВЫХ ОТОБРАЖЕНИЙ

О. А. Логачёв (Москва)

Пусть $\mathbb{F}_2 = GF(2)$ и $\mathbb{N}$ — множество натуральных чисел. Для векторного пространства $\mathrm{V}_n = \mathbb{F}_2^n$, $n \in \mathbb{N}$ через $x = (x_1, \ldots, x_n)$ будем обозначать наборы длины n, являющиеся элементами этого пространства. Пусть $\mathcal{V} = \mathbb{F}_2^\infty$ — пространство всех бесконечных вправо последовательностей в алфавите $\mathbb{F}$. Элементы пространства $\mathcal{V}$ будем обозначать $x = (x_i)_{i=1}^\infty$. Для любой последовательности x из $\mathcal{V}$ определим оператор редуцирования:

1. $(x)_{i,s} = (x_i, x_{i+1}, \ldots, x_{i+s-1}) \in \mathrm{V}_s$, $i = 1, 2, \ldots$; $s = 1, 2, \ldots$.

2. $(x)_{i,\infty} = (x_i, x_{i+1}, \ldots, x_{i+t}, \ldots) \in \mathcal{V}_s$, $i = 1, 2, \ldots$; $s = \infty$.

Аналогичным образом определим оператор редуцирования для набора x из V_n:

$$(x)_{i,s} = (x_i, x_{i+1}, \ldots, x_{i+s-1}) \in \mathrm{V}_s, \quad 1 \le i \le n,\ 1 \le s \le n - i + 1.$$

Пусть $f : \mathrm{V}_n \to \mathbb{F}_2$ — булева функция от n переменных, $\mathcal{F}_n$ — множество всех булевых функций от n переменных. Через f^* обозначим отображение из $\mathcal{V}$ в $\mathcal{V}$ вида

$$f^*(x) = \left(f\left((x)_{1,n}\right), f\left((x)_{2,n}\right), \ldots, f\left((x)_{t,n}\right), \ldots\right)$$

для любой последовательности x из $\mathcal{V}$, реализуемое двоичным регистром сдвига длины n с фильтрующей функцией f.

Определение. *Пусть $f \in \mathcal{F}_n$. Отображение f^* обладает свойством локальной обратимости, если для некоторого $m \in \mathbb{N}$ существует набор $y \in \mathrm{V}_m$, удовлетворяющий условиям*:

1) $\mathcal{D}(f^*, y) = \left\{z \in \mathcal{V} | (f^*)^{-1}(y, z) \ne \emptyset\right\} \ne \emptyset$;

2) *если $w, w' \in (f^*)^{-1}(y, z)$, $z \in \mathcal{D}(f^*, y)$, то выполняется соотношение $(w)_{m+1,\infty} = (w')_{m+1,\infty}$.*

Множество таких наборов y для отображения f^* будем обозначать $\mathrm{Inv}(f^*)$.

Пусть $\rho_f(\cdot, \varepsilon) : \mathrm{V}_n \to \mathrm{V}_n$, $\varepsilon = 0, 1$ — отображения, осуществляемые неавтономным регистром сдвига с функцией обратной связи $f \in \mathcal{F}_n$:

$$\rho_f(x, \varepsilon) = \rho_f\left((x_1, \ldots, x_n), \varepsilon\right) = (x_2, \ldots, x_n, f(x_1, \ldots, x_n) \oplus \varepsilon),$$

где $x \in \mathrm{V}_n$, $\varepsilon \in \mathbb{F}_2$ и $\oplus$ — сложение по модулю 2. Эти отображения естественно могут быть продолжены до отображений, соответствующих произвольному набору $u \in \mathrm{V}_l$. Если $u = (u_1, u_2, \ldots, u_l)$, то

$$\rho_f(x, u) = \rho_f(\ldots, \rho_f(\rho_f(x, u_1), u_2), \ldots, u_l),$$

т. е. $\rho_f(x,u)$ — последовательное применение отображений $\rho(\cdot,u_i)$, $i=1,2,\ldots,l$.

Воспользовавшись терминологией работы [1], приведем следующее свойство булевой функции.

Определение. *Пусть $f\in\mathcal{F}_n$. Будем говорить, что функция f обладает возвратным свойством, если $y\in \mathrm{V}_l$ для некоторых $l\in\mathbb{N}$ и $z=z(y)\in \mathrm{V}_n$ таких, что*

$$\rho_f(x,y)=z=z(y)$$

для любого $x\in \mathrm{V}_n$. Набор y будем называть возвратным набором.

Справедливо следующее утверждение.

Предложение. *Функция $f\in\mathcal{F}_n$ обладает возвратным свойством тогда и только тогда, когда для любых $x,x'\in \mathrm{V}_n$ существует набор $y=y(x,x')\in \mathrm{V}_s$, $s=s(x,x')$ такой, что $\rho_f(x,y)=\rho_f(x',y)$.*

Теорема. *Пусть $f\in\mathcal{F}_{n+1}$ имеет вид*

$$f(x_1,\ldots,x_n,x_{n+1})=g(x_1,\ldots,x_n)\oplus x_{n+1},$$

где $g\in\mathcal{F}_n$. Отображение f^* обладает свойством локальной обратимости тогда и только тогда, когда функция g обладает возвратным свойством.

Пример 1. *Пусть $f\in\mathcal{F}_n$ и $f(x_1\oplus 1,\ldots,x_n\oplus 1)=f(x_1,\ldots,x_n)$. Функция f не обладает свойством локальной обратимости. Если набор y, $|y|=m$ таков, что $(f^*)^{-1}(y)\neq\emptyset$, и $x=(x_1,\ldots,x_{m+n-1})\in (f^*)^{-1}(y)$, то $x'=(x_1\oplus 1,\ldots,x_{m+n-1}\oplus 1)\in\in (f^*)^{-1}(y)$.*

Наличие у фильтрующего генератора псевдослучайных последовательностей свойства локальной обратимости может быть использовано для построения метода определения его ключа. Вычисление параметров эффективности и надежности этого метода связано в частности с выяснением структуры множества $\mathrm{Inv}(f^*)$. Формально реализация такого метода представляет собой просмотр выходных последовательностей генератора и поиска в них элементов из $\mathrm{Inv}(f^*)$. В случае нахождения такового, начиная с соответствующего знака и далее линейная рекуррентная последовательность (ЛРП), генерируемая LFSR, определяется однозначно. Поскольку каждый знак ЛРП является линейной функцией от ключа, мы получаем возможность определять ключ, решая систему линейных уравнений.

Пример 2. *Пусть n — нечетное натуральное число и $g\in\mathcal{F}_n$ — функция голосования*:

$$g(x)=g(x_1,\ldots,x_n)=\begin{cases}1, & \text{если } \sum_{i=1}^n x_i\geq (n+1)/2;\\ 0, & \text{если } \sum_{i=1}^n x_i\leq (n-1)/2.\end{cases}$$

Тогда функция

$$f(x_1, \ldots, x_n, x_{n+1}) = g(x_1, \ldots, x_n) \oplus x_{n+1}$$

обладает свойством локальной обратимости.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 07-01-00154).

Список литературы

1. Рысцов И. К. Возвратные слова для разрешимых автоматов // Кибернетика и системный анализ. — 1994. — № 6. — С. 21–26.

БАЗИСНЫЕ НАБОРЫ В РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ

Ф. М. Малышев (Москва)

Для рекуррентной последовательности $x_{i+m} = f(x_i, x_{i+k_1}, ..., x_{i+k_s})$, $i \in \mathbb{Z}$, с $0 = k_0 < k_1 < k_2 < ... < k_s < k_{s+1} = m$, НОД$(m, k_1, ..., k_s) = 1$, подмножество $S \subset \mathbb{Z}$ мощности m называем базисным, если при некотором $I \in \mathbb{Z}$ для всех $i \geq I$ знак x_i представим формулой, содержащей кроме скобок и запятых символы f и x_t, $t \in S$. Примеры таковых $S - \{1 + j, ..., m + j\}$. Базисные подмножества рассматриваем с точностью до сдвига на целое число. Это понятие не зависит от конкретных $f : X^{s+1} \to X$. Такие S содержат по одному элементу из каждого класса вычетов по mod$m$. Пусть $\pi : \mathbb{Z} \to \mathbb{Z}_m$ канонический гомоморфизм на группу вычетов по mod$m$. Если для $\sigma : \mathbb{Z}_m \to \mathbb{Z} \quad \pi(\sigma(y)) = y \quad \forall y \in \mathbb{Z}_m$, то *$Im\sigma$ базисный набор тогда и только тогда, когда* $\sigma(y + \pi(k_j)) \leq \sigma(y) + k_j$ *для всех* $y \in \mathbb{Z}_m$ и $j = 1, ..., s$.

Для описания базисных наборов используется следующая конструкция. Пусть $\Phi : \mathbb{R}^s \to \mathbb{R}$, $\Phi(x_1, ..., x_s) = \sum\limits_{i=1}^{s} x_i k_i$, $\varphi = \Phi|_{\mathbb{Z}^s}$. Тогда имеем вложение $\mathbb{Z}_m \cong \mathbb{Z}^s / \ker(\varphi \circ \pi)$ в тор $T^s = \mathbb{R}^s / \ker(\varphi \circ \pi)$. Аналогично, отображения $\Psi : \mathbb{R}^{s+1} \to \mathbb{R}$, $\Psi(x_1, ..., x_s, x_{s+1}) = \sum\limits_{i=1}^{s} x_i k_i + x_{s+1} m$, $\psi = \Psi|_{\mathbb{Z}^{s+1}}$ задают вложение $\mathbb{Z} \cong \mathbb{Z}^{s+1} / \ker \psi$ в цилиндр $C^{s+1} = \mathbb{R}^{s+1} / \ker \psi$, при этом естественная проекция $\mathbb{R}^{s+1} \to \mathbb{R}^s$, $(x_1, ..., x_s, x_{s+1}) \mapsto (x_1, ..., x_s)$, индуцирует отображение $\Pi : C^{s+1} \to T^s$, для которого $\Pi|_{\mathbb{Z}} = \pi$. При естественном накрытии

$\mathbb{R}^{s+1} \to C^{s+1}$ гиперповерхности из $\mathbb{R}^{s+1}$, задаваемые равенствами $x_{s+1} = i$, $i = 0, 1, ..., d-1$, переходят в s-мерные цилиндры C_i^s, содержащие $\{z \in \mathbb{Z} | z \equiv i \bmod d\}$. Отображения $\Pi|_{C_i^s} : C_i^s \to T^s$ осуществляют бесконечнолистные накрытия.

Рассмотрим в T^s гомеоморфные и гомотопные тору $T^{s-1} = \ker \Phi / \ker \varphi$ гиперповерхности $M_1, ..., M_d$, не пересекающиеся друг с другом и с $\mathbb{Z}_m$, $d = \text{НОД}(k_1, ..., k_s)$. Через $h_i(v) \geq 0$, $v \in \mathbb{Z}_m$, $i = 1, ..., s$, обозначим число пересечений направленного отрезка $[v, v + \pi(k_i)]$ с гиперповерхностями $M_1, ..., M_d$ (для исключения касаний и других особенностей, отрезок может быть слегка деформирован; пересечения учитываются с разными знаками, в зависимости от того с положительной на отрицательную стороны гиперповерхности переходим, или наоборот; знаки сторонам гиперповерхностей приписаны так, что в каждом цилиндре из $T^s \setminus \bigcup_{i=1}^{d} M_i$ знаки у оснований разные).

Теорема. *Для заданных d гиперповерхностей на торе T^s равенства*

$$\sigma(0) = 0; \quad \sigma(v + \pi(k_i)) = \sigma(v) + k_i - h_i(v)m, \quad v \in \mathbb{Z}_m, \quad i = 1, ..., s,$$

корректным образом задают отображение $\sigma : \mathbb{Z}_m \to \mathbb{Z}$, для которого $Im\sigma$ является базисным набором. Обратно, любой базисный набор S после возможного сдвига может быть реализован таким способом.

В этой теореме гиперповерхности $M_1, ..., M_d$ можно выбирать из более узкого класса, среди параллельных сдвигов так называемых монотонных гиперповерхностей, составленных из ячеек в виде $(s-1)$-мерных граней элементарных кубиков с вершинами из $\mathbb{Z}_m$, которые являются образами при естественном накрытии $\mathbb{R}^s \to T^s$ гиперповерхностей в $\mathbb{R}^s$, составленных из аналогичных ячеек, инвариантных относительно $\ker \varphi$ и пересекающихся в единственной точке с каждой прямой, параллельной вектору $(1, ..., 1) \in \mathbb{R}^s$. Для монотонных гиперповерхностей допускаются самокасания по целым ячейкам — многократное вхождение некоторых ячеек в гиперповерхность. При таком уточнении теорема позволяет оценивать число N базисных наборов.

Следствие. Справедливо неравенство $N \geq 2^{k_1 - 1}$, причем *равенство достигается тогда и только тогда, когда $k_j = k_1 + j - 1$, $j = 2, ..., k_1$. Если $s = 1$, то $N = \frac{1}{k_1 + m} \begin{pmatrix} k_1 + m \\ k_1 \end{pmatrix}$. Если $s = 2$, $(k_1, k_2) = 1$, то при достаточно больших $m \geq m(k_1, k_2)$ $N =$*

$\frac{1}{k_1+k_2}\begin{pmatrix} k_1+k_2 \\ k_1 \end{pmatrix}$. *Если* $s=2$, $(k_1,k_2)=d>1$, *то при* $m\to\infty$ *и ограниченных* k_1,k_2 *имеем*: $N=\left[\frac{d}{k_1+k_2}\begin{pmatrix} (k_1+k_2)/d \\ k_1/d \end{pmatrix}\right]^d \frac{m^{d-1}}{d!}(1+o(1))$. *Если* $s\geq 3$, $m\to\infty, k_1,\ldots,k_s$ *ограничены, то* $N=O(m^{d-1})$.

СИСТЕМЫ СЧИСЛЕНИЯ С АЛГЕБРАИЧЕСКИМИ ОСНОВАНИЯМИ

Н. Ф. Мануилов (Смоленск)

В работе продолжены исследования по теории позиционных систем счисления, начатые в [1, 2].

Пусть Z — кольцо целых чисел, $Z[x]$ — кольцо многочленов с целыми коэффициентами.

Теорема 1. *Если все корни многочлена* $M\in Z[x]$, $M=m_0+m_1x+\ldots+m_nx^n$ $(n\geq 1)$ *по модулю больше единицы, то какова бы ни была полная система* S *представителей классов факторкольца* $Z/(m_0)$ *для любой рациональной функции* $\frac{A}{B}$ $(A,B\in Z[x])$, *знаменатель* B *которой взаимно прост в кольце* $Z[x]$ *с многочленом* M, *существует единственное представление в виде*

$$\frac{A}{B}=f+M\frac{A_1}{B_1},$$

где f — *рациональная функция, имеющая в окрестности точки* $x=0$ *разложение в ряд*

$$f=\sum_{k=k_0}^{\infty}c_kx^k(k_0>-\infty),$$

в котором при любом k $c_k\in S$ *и последовательность* (c_k) *периодическая, начиная с некоторого* k, *многочлены* $A_1,B_1\in Z[x]$, *многочлен* B_1 *взаимно прост с* M.

Доказательство основано на ряде вспомогательных предложений приведем формулировку одного из них.

Лемма. *Любой идеал в кольце* $Z[x]$, *порожденный парой взаимно простых элементов, содержит многочлен вида* $z^k-z^l(k>l\geq 0)$.

Теорема 2. *Пусть многочлен* $M \in Z[x]$, $M = m_0 + m_1 x + ... + m_n x^n$ $(n \geq 1)$ *не имеет корней по модулю равных единице, его коэффициенты натуральные числа, удовлетворяющие условию* $m_0 \geq m_1 \geq ... \geq m_n$. *Тогда для любого многочлена* A $(A \in Z[x])$ *существует единственное представление в виде*

$$A = B + MC,$$

где $B, C \in Z[x]$, $B = \sum_{k=0}^{p} b_k x^k$, $0 \leq b_k < m_0$ $(k = 0, 1, ..., p)$.

Доказательство опускаем.

Теорема 3. *Пусть многочлен* $M(x) \in Z[x]$ *степени* $n (n \geq 1)$ *с взаимно простыми коэффициентами и положительным коэффициентом при* x^n *является минимальным многочленом алгебраического числа* θ. *Тогда найдется число* $k > 0$ *такое, что при любом натуральном* $m > k$ *существуют представления*:

1. *Для любого* $a \in Z[\theta]$

$$a = \sum_{j=0}^{p(m)} c_j(m)(\theta - m)^j,$$

где при фиксированном m $c_j(m) \in Z$, $0 \leq c_j(m) < M(m)$ $(j = 0, 1, ..., p(m))$;

2. *Для любого* $b \in Q(\theta)$

$$b = \sum_{j=k(m)}^{\infty} d_j(m)(\theta - m)^{-j},$$

где при каждом m $d_j(m) \in Z$, $0 \leq d_j(m) < M(m)$, *последовательность* $(d_j(m))$ *периодическая (начиная с некоторого значения* j, *зависящего от* m), *притом представление в п.* 1 *единственно.*

Доказательство опускаем.

Полученные результаты оказалось возможным применить в системах кодирования.

Список литературы

1. Мануилов Н. Ф. О системах счисления в полях алгебраических чисел // Деп.ВИНИТИ. — 1990.

2. Мануилов Н. Ф. Системы счисления в полях алгебраических чисел // Тезисы III международной конференции по теории чисел. — Тула, 1996.

ГРАНИЦЫ ДЛЯ КОДОВ И УПАКОВОК ШАРОВ С ПОМОЩЬЮ ВЫПУКЛОГО ПРОГРАММИРОВАНИЯ

О. Р. Мусин (Москва)

В 1970-х годах Ф. Дельсарт, В. М. Сидельников, Г. А. Кабатянский и В. И. Левенштейн предложили мощный подход для оценки размеров кодов — так называемый метод Дельсарта. С его помощью были улучшены верхние границы для двоичных и равновесных кодов, плотности упаковки шаров, контактных чисел, асимптотики сферических кодов и т. д. [1].

Основой метода Дельсарта является линейное программирование (ЛП). В недавних работах [2–7] были рассмотрены новые методы для теории кодирования, основанные на выпуклом программировании (ВП). Метод ВП во многих случаях улучшает верхние границы для двоичных и сферических кодов, полученных методом ЛП.

Заметим, что в настоящее время ВП (используется также название *полуопределенное программирование* или SDP (semidefinite programming)) широко применяется не только для непрерывных задач, но также и для задач дискретной математики и комбинаторики.

В настоящей заметке для ВП обсуждается два независимых подхода: подход основанный на положительной определенности зональных сферических функций и обобщение метода Дельсарта для многочленов от нескольких переменных. В работах [3–9] было показано, что эти методы улучшают некоторые верхние границы для контактных чисел $k(n)$ (максимальное число точек на единичной сфере в $\mathbf{R}^n$ с угловым расстоянием не менее $\pi/3$), и чисел $B(n)$ — максимальное число точек на единичной полусфере в $\mathbf{R}^n$ с угловым расстоянием не менее $\pi/3$.

Положительная определенность зональных сферических функций. С каждым компактным дважды однородным пространством M однозначно связаны функция расстояния τ и набор *зональных сферических функций* $\Phi_k(t), k = 0, 1, 2, \ldots$ (см. [1, гл. 9]). Для всех известных примеров: $\Phi_k(t)$ — многочлен степени k. В частности, если M — пространство Хэмминга, то это многочлены Кравчука, а для сферы — многочлены Гегенбауэра.

Важнейшим свойством зональных сферических функций является свойство положительной определенности (СПО), впервые доказанное Бохнером и Шёнбергом в 1941 г.: *для произвольного набора точек $p_1, \ldots, p_r$ из M и для любого k матрица $T_k = \big(\Phi_k(\tau(p_i, p_j))\big)$ неотрицательно определена.*

ВП и СПО. Если матрица неотрицательно определена, то сумма ее элементов не может быть отрицательной. Применяя это свойство

для матрицы T_k получаем так называемое *неравенство о среднем* для Φ_k.

Дельсарт предложил использовать неравенства о среднем как линейные неравенства на спектр расстояний произвольного кода в M. Это позволяет рассматривать проблему нахождения размера кода как задачу ЛП (см. детали в [1]). В случае непрерывного M (например, сфера) прямая задача ЛП является бесконечномерной. В методе Дельсарта рассматривается двойственная задача ЛП, которую легче приблизить конечномерной.

Работа автора [6] основана на методе (теореме) Сильвестра для вычисления количества положительных корней многочлена. Было показано, что если вместо спектра расстояний рассмотреть в качестве переменных степенные суммы расстояний, то размер кода ограничен решением определенной *конечномерной* задачи ВП. В работе [6] доказано, что если в качестве условий на расстояния рассмотреть только неравенства о среднем, то границы ЛП и ВП совпадают. Кроме того, если использовать, как дополнительные, неравенства из работ [9] (основной результат работы — доказательство гипотезы: $k(4) = 24$) и [5] (доказано, что $B(4) = 18$), то эти равенства могут быть получены с помощью ВП. В работе [6] на основе СПО предложен общий метод, в частности, позволяющий существенно улучшить границы для $B(n), n < 10$, полученные в [8].

Обобщение метода Дельсарта для многих переменных. Недавно для пространства Хэмминга [2] и для сферы [3] найдено обобщение СПО для многочленов от трех переменных. Из этих неравенств вытекают "неравенства о среднем" (здесь сумма берется по тройкам точек) для многочленов, в некотором смысле, обобщающим зональные сферические функции. Эти неравенства с помощью ВП позволили улучшить некоторые границы для двоичных и сферических кодов, в частности, для $k(n), n = 5, 6, 7, 9, 10$ [3], и для $B(n), 5 \leq n \leq 10$ [4].

В работа автора [7] для случая сферы получено обобщение СПО для "многочленов Гегенбауэра" от $2m + 1$ переменных, где $0 \leq m \leq n - 2$. В частности, для $m = 1$ из этих неравенств легко вытекают неравенства из [3]. Вместе с тем, наше доказательство неравенств существенно проще.

В работе [7] показано, что с ростом m неравенства "становятся строже". Стало быть, можно ожидать, что увеличивая m границы ВП будут улучшаться. Однако, и размер задачи ВП растет экспоненциально от m. Даже для случая $m = 2$ (т. е. многочлены от пяти переменных) размер задачи столь велик, что не позволяет

вычислить границы на компьютере. Здесь остается надеятся. что возможно "угадать" явные выражения для комбинаций обобщенных СПО, тем самым уменьшить размер задачи, получить новые границы для сферических кодов и, в частности, для контактных чисел.

Список литературы

1. Конвей Дж., Слоэн Н. Упаковки шаров, решетки и группы. — М: Мир, 1990.

2. Schrijver A. New code upper bounds from the Terwilliger algebra and semidefinite programming // IEEE Trans. Inform. Theory. — 2005. — V. 51. — P. 2859–2866.

3. Bachoc C., Vallentin F. New upper bounds for kissing numbers from semidefinite programming // Preprint. — August 2006. — arXiv:math.MG/0608523.

4. Bachoc C., Vallentin F. Semidefinite programming, multivariate orthogonal polynomials, and codes in spherical caps // Preprint. — October 2006. — arXiv:math.MG/0610856.

5. Musin O. R. The one-sided kissing number in four dimensions // Periodica Math. Hungar. — 2006. — V. 53. — P. 209–225.

6. Musin O. R. Bounds for codes by semidefinite programming // Preprint. — September 2006. — arXiv:math.CO/0609155.

7. Musin O. R. Multivariate positive definite functions on spheres // Preprint. — January 2007. — arXiv:math.MG/0701083.

8. Barg A., Musin O. R. Codes in spherical caps // Advances in Mathematics of Communication. — 2007. — V. 1. — P. 131–149.

9. Musin O. R. The kissing number in four dimensions // Preprint. — April 2005. — arXiv:math.MG/0309430. — (To appear in Annals of Math.)

СРАВНЕНИЕ ФУНКЦИЙ «ИСКЛЮЧАЮЩЕЕ ИЛИ» И «ГОЛОСОВАНИЕ» С КРИПТОГРАФИЧЕСКОЙ ТОЧКИ ЗРЕНИЯ

Х. Т. Нгуен, Г. А. Карпунин (Москва)

В 1990 году в [1] была разработана хэш-функция MD4, которая послужила основой для многих хэш-функций, ставших впоследствии наиболее популярными. Среди хэш-функций типа MD4 можно выделить MD5, семейство SHAx, семейство RIPEMDx, Haval. Автор хэш-функции MD4 утверждал, что она удовлетворяет стандартным

криптографическим требованиям, в частности, требованию стойкости к нахождению коллизий. Однако в 1996 году в работе [2] был построен вероятностный алгоритм, который за несколько секунд на персональном компьютере находит коллизии для хэш-функции MD4.

При построении этого алгоритма использовались свойства булевой функции "голосование" $MAJ = xy \vee xz \vee yz$, от которой существенно зависит второй раунд в сжимающем преобразовании MD4. В данной работе мы заменяем функцию MAJ на функцию "исключающее или" $XOR = x \oplus y \oplus z$ и сравниваем влияние функций MAJ и XOR на устойчивость соответствующих вариантов MD4 к методу из [2].

На одном из этапов построения алгоритма из [2] возникает система уравнений, вероятность решения (количество решений) которой определяет вероятность успеха этого алгоритма. Рассмотрим эту систему уравнений в наиболее общем виде:

$$G_i(X_1, X_2, \ldots, X_n) = G_i(X_1 + A_{i1}, X_2 + A_{i2}, \ldots, X_n + A_{in}) + A_{i0}, \quad (\#)$$

где $i = \overline{1,m}$, m — количество уравнений в системе; $X_j \in \mathbb{F}_2^T$, $j = \overline{1,n}$, — T-битные переменные, T — натуральное число, $\mathbb{F}_2 = \{0,1\}$ — поле из двух элементов; $A_{ij} \in \mathbb{F}_2^T$, $j = \overline{0,n}$, — T-битные фиксированные константы; "+" — сложение по модулю 2^T; функция $G_i : (\mathbb{F}_2^T)^n \to \mathbb{F}_2^T$ действует на аргументах побитово одинаковым образом, т. е. k-й бит результата зависит только от k-х битов аргументов: $G_i^{(k)}(X_1, X_2, \ldots, X_n) = g_i(X_1^{(k)}, X_2^{(k)}, \ldots, X_n^{(k)})$, $k = \overline{0, T-1}$, g_i — булева функция от n переменных.

Заметим, что система (#) возникает во многих методах дифференциального криптоанализа хэш-функций типа MD4. Задача криптоаналитика — выбором констант A_{ij} максимизировать вероятность решения этой системы. С другой стороны, задача криптографа — выбором булевых функций g_i сделать задачу криптоаналитика более трудной.

Обозначим через $P_g^T(A_0, A_1, \ldots, A_n)$ вероятность решения отдельного уравнения

$$G(X_1, X_2, \ldots, X_n) = G(X_1 + A_1, X_2 + A_2, \ldots, X_n + A_n) + A_0, \quad (*)$$

и определим степень податливости этого уравнения к процедуре максимизации вероятности решения системы (#) как среднее значение вероятности $P_g^T(A_0, A_1, \ldots, A_n)$ по всем наборам констант $(A_0, A_1, \ldots, A_n) \in 2^{Tn}$. Обозначим это среднее значение через EP_g^T

и сформулируем в его терминах криптографический критерий сравнения устойчивости булевых функций.

Критерий сравнения: Будем считать, что булева функция g_1 более устойчива чем g_2 к методам дифференциального криптоанализа хэш-функций типа MD4, если $EP_{g_1}^T < EP_{g_2}^T$.

Обозначим через $P^T_{g;\alpha_0\alpha_1\ldots\alpha_n}(A_0, A_1, \ldots, A_n)$, $(\alpha_0\alpha_1\ldots\alpha_n) \in \mathbb{F}_2^{n+1}$, вероятностную меру тех решений уравнения $(*)$, для которых переносы в $(T+1)$-ый бит выражений $G(X_1 + A_1, X_2 + A_2, \ldots, X_n + A_n) + A_0$, $X_1 + A_1$, $\ldots$, $X_n + A_n$ равны α_0, α_1, $\ldots$, α_n соответственно. Рассмотрим 2^{n+1} матриц $M_{a_0a_1\ldots a_n}$, $(a_0a_1\ldots a_n) \in \mathbb{F}_2^n$, размера $2^{n+1} \times 2^{n+1}$, строчки и столбцы которых заиндексированы двоичными векторами $(\alpha_0\alpha_1\ldots\alpha_n) \in \mathbb{F}_2^{n+1}$ и $(\beta_0\beta_1\ldots\beta_n) \in \mathbb{F}_2^{n+1}$ соответственно:

$$M_{a_0a_1\ldots a_n} = \left(P^1_{g;\alpha_0\alpha_1\ldots\alpha_n}(a_0 + \beta_0, a_1 + \beta_1, \ldots, a_n + \beta_n)\right).$$

Следующие две теоремы позволяют с помощью матриц $M_{a_0a_1\ldots a_n}$ вычислять вероятность $P_g^T(A_0, A_1, \ldots, A_n)$ и ее среднее значение EP_g^T. Через $SFC(M)$ обозначим сумму элементов первого столбца матрицы M.

Теорема 1. *Имеет место равенство*

$$P_g^T(A_0, A_1, \ldots, A_n) = SFC\left(\prod_{k=0}^{T-1} M_{A_0^{(k)}A_1^{(k)}\ldots A_n^{(k)}}\right).$$

Теорема 2. *Имеет место равенство*

$$EP_g^T = SFC\left(\left(\frac{1}{2^{n+1}} \sum_{(a_0a_1\ldots a_n)\in\mathbb{F}_2^{n+1}} M_{a_0a_1\ldots a_n}\right)^T\right).$$

Рассмотрим наиболее часто встречающееся в методе из работы [2] уравнение вида $(*)$: $G(X_1, X_2, X_3) = G(X_1, X_2 + B, X_3 + C)$, определяемого булевой функцией g. Для этого уравнения имеют место следующие утверждения.

Утверждение 1. *Если функция* $g = XOR$, *то* $EP^{32}_{XOR} = 2.33 \cdot 10^{-10}$.

Утверждение 2. *Если функция* $g = MAJ$, *то* $EP^{32}_{MAJ} = 2.94 \cdot 10^{-7}$.

Из этих утверждений можно сделать следующий криптографический

Вывод. *Функция "исключающее или" является более устойчивой к методу из* [2]*, чем функция "голосование".*

В пользу выбора функции XOR также говорят следующие два утверждения.

Утверждение 3. *Доля тех констант* (B, C)*, для которых* $P^{32}_{XOR}(B, C) > 0$*, равна* $\frac{1}{3}(1 + \frac{1}{2^{63}})$.

Утверждение 4. *Для любых констант* (B, C) *вероятность* $P^{32}_{MAJ}(B, C) > 0$.

Список литературы

1. Rivest R. The MD4 message digest algorithm // Proceedings Crypto'90. — LNCS 537. — Springer-Verlag, 1991. — P. 303–311.

2. Dobbertin H. Cryptanalysis of MD4 // Journal of Cryptology. — 1998. — V. 11. — P. 253–271.

О ВЕРХНЕЙ ОЦЕНКЕ ДЛИНЫ ЗАПРЕТА k-ЗНАЧНОЙ ФУНКЦИИ

Н. В. Никонов (Москва)

В представленной работе рассматриваются системы уравнений сдвигового типа:

$$f^k(x_{1+i}, \ldots, x_{n+i}) = \gamma_{1+i}, \qquad i = 0, 1, \ldots, N-1, \tag{1}$$

где $f^k(x_1, \ldots, x_n)$ — функция k-значной логики ($k \geqslant 2$), порожденные схемой, получившей название фильтрующего генератора [1]. Одним из основных вопросов, возникающих при анализе систем вида (1), является задача установления ее совместности, которая тесно связана с теорией запретов. Основы теории запретов, как самостоятельного направления дискретной математики, были заложены С. Н. Сумароковым в работе [2].

Определение 1. *Последовательность знаков* $\gamma_1, \ldots, \gamma_N$ *называется запретом функции* f^k*, если система вида* (1) *— несовместна (не имеет решений). Число* N*, при этом, называется длиной запрета* k*-значной функции* f^k.

В противном случае принято говорить, что f^k не имеет запрета.

Для теории запретов одной из актуальных задач является нахождение оценки длины запрета, что имеет теоретический и прикладной интерес. В работе [2] для булевых функций С. Н. Сумароковым был сформулирован и доказан критерий отсутствия запрета у функции, который легко распространяется и на k-значную область.

Теорема 1. *Функция f^k не имеет запрета тогда и только тогда, когда она сильно равновероятна.*

Доказательство критерия базируется на том факте, что если f^k не является сильно равновероятной функцией, то у нее существует запрет вида

$$\overline{\gamma}^*,\ \gamma_1^{(1)},\dots,\gamma_{n-1}^{(1)},\overline{\gamma}^*,\dots,\overline{\gamma}^*,\ \gamma_1^{(t)},\dots,\gamma_{n-1}^{(t)},\overline{\gamma}^*, \tag{2}$$

где $\overline{\gamma}^* = (\gamma_1^*,\dots,\gamma_v^*)$ — некоторая v-грамма, при которой нарушается условие сильной равновероятности, то есть система уравнений вида (1) с правой частью $\overline{\gamma}^*$ имеет $(k^{n-1}-\alpha)$ решений, где

$$1 \leqslant \alpha \leqslant k^{n-1}-1, \tag{3}$$

а знаки $\gamma_i^{(j)}$, $i=\overline{1,\ n-1}$, $j=\overline{1,\ t}$ — произвольны. Длина выходной последовательности (2) равна

$$N = t(v+n-1)+v. \tag{4}$$

Далее вводится в рассмотрение величина μ_t, характеризующая среднее число входных последовательностей, порождающих комбинации вида (2) и показывается, что при достаточно большом t выполняется

$$\mu_t \leqslant \frac{\left(k^{n-1}-\alpha\right)^{t+1}}{\left(k^{n-1}\right)^t} < 1. \tag{5}$$

Оценив t из неравенства (5), с учетом (4) можно получить оценку длины запрета. С. Н. Сумароковым была предложена следующая оценка длины запрета функции f^k:

$$M \leqslant ((k^{n-1}-1)^2-1)(v+n-1)+v, \tag{6}$$

опубликованная в ряде работ [2, 3]. Предложим вывод ещё одной оценки длины запрета, ассимптотически лучшей при $k^{n-1}\to\infty$ оценок, приведенных в работах [2–5].

Теорема 2. *Если $n \geqslant 3$ и для функции f^k найдется выходная v-грамма $\overline{\gamma}^*$, формирующая систему вида (1) с $\left(k^{n-1} - \alpha\right)$ решениями, где α удовлетворяет (3), то у функции существует запрет длины*

$$M^{'} \leqslant \left[\left(\frac{k^{n-1}}{\alpha} - \frac{1}{2}\right)\ (n-1)\ln k\right](v+n-1) + v. \tag{7}$$

Кратко рассмотрим схему доказательства теоремы 2. Найдем оценку тех значений t, при которых условие (5) верно, то есть выполняется неравенство:

$$\left(1 - \frac{\alpha}{k^{n-1}}\right)^{t+1} < \frac{1}{k^{n-1}}. \tag{8}$$

Прологарифмировав обе части (8), с учетом (3) имеем:

$$(t+1) > \frac{\ln k^{n-1}}{\ln\left(\frac{k^{n-1}}{k^{n-1}-\alpha}\right)}. \tag{9}$$

Оценим логарифм, стоящий в знаменателе, для чего представим его в виде:

$$\ln\left(\frac{k^{n-1}}{k^{n-1}-\alpha}\right) = \ln\left(\frac{1+\frac{\alpha}{2k^{n-1}-\alpha}}{1-\frac{\alpha}{2k^{n-1}-\alpha}}\right) = \ln(1+\beta) - \ln(1-\beta),$$

где $\beta = \frac{\alpha}{2k^{n-1}-\alpha}$. Исходя из (3), $\beta \in (0,1)$, следовательно оцениваемый логарифм равен:

$$\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n}\beta^n - \sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n}(-\beta)^n = \sum_{n=1}^{\infty}\frac{(-1)^{n-1}+1}{n}\beta^n. \tag{10}$$

Нетрудно заметить, что при четных n члены ряда (10) — нулевые, поэтому:

$$\ln\left(\frac{k^{n-1}}{k^{n-1}-\alpha}\right) = 2\beta\sum_{n=0}^{\infty}\frac{\beta^{2n}}{2n+1} > 2\beta = \frac{2\alpha}{2k^{n-1}-\alpha}. \tag{11}$$

Неравенство (9) — достаточное условие существования запрета вида (2). Тогда, с учетом (11), следующее неравенство будет тем более достаточным:

$$(t+1) \geqslant \left(\frac{2k^{n-1}-\alpha}{2\alpha}\right)\ln k^{n-1},$$

откуда с учетом (4) следует обоснованность формулы (7).

Работа выполнена при поддержке гранта Президента РФ (НШ-8564.2006.10).

Список литературы

1. Фомичев В. М. Дискретная математика и криптология. Курс лекций. — М.: Диалог-МИФИ, 2003.

2. Сумароков С. Н. Запреты двоичных функций и обратимость для одного класса кодирующих устройств // Обозрение прикладной и промышленной математики. — М.: ТВП, 1994. — Т. 1, вып. 1.

3. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004.

4. Никонов Н. В. О снижении оценки С. Н. Сумарокова длины запрета // Обозрение прикладной и промышленной математики — М.: ОПиПМ, 2006. — Т. 13, вып. 6.

5. Никонов Н. В. Снижение оценки длины запрета С. Н. Сумарокова // Лесной вестник. — Мытищи.: МГУЛ, 2007. — Т. 1.

МЕТРИКИ СПЛЕТЕНИЯ СИММЕТРИЧЕСКИХ ГРУПП

М. А. Пудовкина (Москва)

Метрические свойства возникают при изучении различных комбинаторных объектов. В работах [1, 2] дано полное описание подметрик метрики Хемминга как метрик, соответствующих орбиталам надгрупп группы Джевонса. Иные классы метрик, связанные с метриками Хемминга и схемами отношений рассматривались в работе [3]. Вместе с тем представляют интерес метрики связанные с другими часто встречающимися группами (или схемами отношений). Одной из таких групп является группа сплетений, метрики которой будут описаны ниже. Все необходимые сведения из теории групп подстановок можно посмотреть, например, в [4].

Будем придерживаться следующих обозначений: N — множество натуральных чисел, (G, X) — группа G, действующая на множестве X, $V_n = V_n(2)$, $G_{\{A\}} = \{g \in G | A^g = A\}$, G^A — ограничение действия группы $G \leq S(X)$ на множество $A \subseteq X$; $(\alpha, \beta)^G = \{(\alpha^g, \beta^g) | g \in G\}$, $\bar{\Psi}$ — граф орбитала Ψ, $\{\overline{a, b}\} = a, a+1, ..., b$, $a < b$.

Пусть $k \in \{\overline{1, n-1}\}$, $A_1, ..., A_{2^{n-k}}$ — произвольное разбиение пространства V_n на 2^{n-k} блоков мощности 2^k каждый. Рассмотрим группу $G = S_{2^k} \int S_{2^{n-k}}$ с блоками импримитивности $A_1, ..., A_{2^{n-k}}$

и опишем метрики ее орбиталов. Очевидно, что для любого блока импримитивности A группы G конституента $G^A_{\{A\}} \cong S_{2^k}$ и образ $\bar{G}$ группы G при естественном гомоморфизме изоморфен $S_{2^{n-k}}$. Используя эти свойства нетрудно описать орбиты стабилизатора группы G и ее орбиты при действии на упорядоченных парах векторов, приводимые далее.

Утверждение 1. *Пусть* $k \in \{\overline{1, n-1}\}$, $G \leq S(V_n)$, $G = S_{2^k} \int S_{2^{n-k}}$, $A_1, ..., A_{2^{n-k}}$ — *блоки импримитивности* G. *Тогда*:

1. *Если* $\alpha \in A_i, i \in \{\overline{1, 2^{n-k}}\}$, *то орбитами группы* G_α *являются множества* $\{\alpha\}$, $A_i \backslash \{\alpha\}$ *и* $\bigcup\limits_{\substack{j=1,\\ j\neq i}}^{2^{n-k}} A_i$.

2. *Если* $\alpha \in A_i, \beta \in A_j, i, j \in \{\overline{1, 2^{n-k}}\}$, *то*

$$(\alpha, \beta)^G = \begin{cases} \{(\alpha', \alpha') | \alpha' \in V_n\}, \alpha = \beta, \\ \{(\alpha', \beta') | \alpha' \in A_r, \beta' \in A_r, r = \overline{1, 2^{n-k}}\}, i = j, \alpha \neq \beta, \\ \{(\alpha', \beta') | \alpha' \in A_r, \beta' \in A_t, \{r, t\} \subseteq \{\overline{1, 2^{n-k}}\}, t \neq r\}, i \neq j. \end{cases}$$

3. *Для любого* $(\alpha, \beta) \in V_n \times V_n$ *существует подстановка* $g \in G$ *такая, что* $(\alpha^g, \beta^g) = (\beta, \alpha)$.

Из утверждения 1 следует, что группе G соответствуют три орбитала:

$$\Gamma_0 = (V_n, \{(\alpha, \alpha) | \alpha \in V_n\}), \Gamma_1 = (V_n, \{(\alpha, \beta) | \alpha, \beta \in A_r, r = \overline{1, 2^{n-k}}\}),$$

$$\Gamma_2 = (V_n, \{(\alpha, \beta) | \alpha \in A_r, \beta \in A_t, \{r, t\} \subseteq \{\overline{1, 2^{n-k}}\}, t \neq r\}),$$

являющиеся самопарными.

Обозначим через μ_i метрику i-го орбитала, $i \in \{0, 1, 2\}$, т. е. $\mu_i(\alpha, \beta)$ — наименьшее расстояние между вершинами α, β в графе $\bar{\Gamma}_i = (V_n, \Gamma_i)$. Опишем свойства графа $\bar{\Gamma}_i$ и приведем метрику i-го орбитала в явном виде, $i \in \{0, 1, 2\}$. Положим $\mu_i(\alpha, \beta) = 0$ при $\alpha = \beta, i \in \{0, 1, 2\}$.

Утверждение 2.

1. *Число компонент связности графа* $\bar{\Gamma}_0$ *равно* 2^n, *число вершин каждой компоненты связности равно единице. Для любых* $\alpha, \beta \in V_n$ *метрика* μ_0 *удовлетворяет равенству*

$$\mu_0(\alpha, \beta) = \begin{cases} 0, & \alpha = \beta, \\ \infty, & \textit{иначе.} \end{cases}$$

2. *Число компонент связности графа* $\bar{\Gamma}_1$ *равно* 2^{n-k}, *все компоненты связности изоморфны* 2^k *вершинному полному графу. Для любых* $\alpha, \beta \in V_n$ *метрика* μ_1 *удовлетворяет равенству*

$$\mu_1(\alpha,\beta) = \begin{cases} 1, & \text{если } \alpha,\beta \in A_r, r \in \left\{\overline{1,2^{n-k}}\right\}, \\ \infty, & \text{иначе.} \end{cases}$$

3. *Граф* $\bar{\Gamma}_2$ — *связный диаметра* 2. *Для любых* $\alpha, \beta \in V_n$ *метрика* μ_2 *удовлетворяет равенству*

$$\mu_2(\alpha,\beta) = \begin{cases} 1, & \alpha \in A_j, \beta \in A_r, \{j,r\} \subseteq \left\{\overline{1,2^{n-k}}\right\}, j \neq r, \\ 2, & \alpha,\beta \in A_r, r \in \left\{\overline{1,2^{n-k}}\right\}. \end{cases}$$

Получим связь между метриками группы $S_{2^k} \int S_{2^{n-k}}$ с разными системами блоков импримитивности. Обозначим через $\mu_{i,A}$ метрику i-го орбитала группы $G = S_{2^k} \int S_{2^{n-k}}$ с блоками импримитивности $\mathrm{A} = \{A_1, .., A_{2^{n-k}}\}$.

Утверждение 3. *Пусть блоками импримитивности групп* $G, G' \leq S(V_n)$, *подобных* $S_{2^k} \int S_{2^{n-k}}$, *являются* $\mathrm{A} = \{A_1, .., A_{2^{n-k}}\}$, $\mathrm{B} = \{B_1, .., B_{2^{n-k}}\}$, *соответственно. Пусть также* $B_i = A_i^s$, $i = \overline{1,2^{n-k}}$, *для некоторой подстановки* $s \in S(V_n)$. *Тогда* $\mu_{j,B}(\alpha,\beta) = \mu_{j,A}(\alpha^{s^{-1}}, \beta^{s^{-1}})$ *для любых векторов* $\alpha, \beta \in V_n, j \in \{0,1,2\}$.

Работа выполнена при поддержке гранта Президента РФ НШ № 8564.2006.10.

Список литературы

1. Погорелов Б. А. Подметрики метрики Хемминга и теорема А. А. Маркова // Труды по дискретной математике. — АК РФ, 2006. — Т. 9.

2. Погорелов Б. А., Пудовкина М. А. Подметрики метрики Хемминга и преобразования, распространяющие искажения в заданное число раз // Труды по дискретной математике. — АК РФ, 2007. — Т. 10.

3. Сидельников В. М. Ассоциативные схемы и метрики на конечной группе // Докл. РАН. — 2004. — Т. 396, № 4. — С. 455–459.

4. Погорелов Б. А. Основы теории групп подстановок. Часть 1. Общие вопросы. — М., 1986.

ОПТИМАЛЬНОЕ КОДИРОВАНИЕ В КЛАССЕ ЛОКАЛЬНО-ПРЕФИКСНЫХ КОДОВ

Т. Г. Смирнова (Нижний Новгород)

Рассматривается кодирование локальных моделей языков глубины 1, приводящее к расширению класса префиксных кодов [1].

Всякой локальной модели $M = \{\epsilon_1, \ldots, \epsilon_n\}$ языка L в алфавите $B = \{b_1, \ldots, b_m\}$, где $\epsilon_i \subseteq B$, $i = 1, \ldots, n$, соответствует граф антипрефиксности $G = K(\epsilon_1) \cup \ldots \cup K(\epsilon_n)$, где $K(\epsilon)$ — полный граф на множестве вершин ϵ. Код $V = \{v_1, \ldots, v_m\}$ называется локально-префиксным относительно графа G, если смежным вершинам соответствуют кодовые слова, находящиеся в отношении антипрефиксности. Вектор $d(V) = (d_1, \ldots, d_m)$, где d_i — длина кодового слова v_i для всех $i = 1, \ldots, m$, называется спектром длин локально-префиксного кода V.

Необходимое условие реализуемости спектра $d(V) = (d_1, \ldots, d_m)$ q-ичным локально-префиксным относительно G кодом записывается в виде системы неравенств Мак-Миллана для каждой из клик $K(\epsilon_1), \ldots, K(\epsilon_n)$ графа G:

$$\sum_{b_i \in K_j} q^{-d_i} \leq 1 \quad (j = 1, \ldots, n). \tag{1}$$

При $n = 1$, 2 система неравенств (1) определяет также и достаточное условие реализуемости спектра, однако при $n \geq 3$ подобное утверждение не имеет места.

Множество всех спектров, реализуемых q-ичными локально-префиксными относительно G кодами, монотонно отросительно отношения частичного порядка, определенного покомпонентной сравнимостью векторов. Минимальные элементы этого множества образуют матрицу $M(G)$ оптимального локально-префиксного кодирования локальных моделей, представимых графом G. Это множество конечно для любого графа по теореме Диксона и для любого графа может быть расшифровано.

Пусть на множестве букв алфавита $B = \{b_1, \ldots, b_m\}$ определено распределение вероятностей $P = (p_1, \ldots, p_m)$, где $0 \leq p_i \leq 1$, $\sum_{i=1}^{m} p_i = 1$, тогда величина

$$C(V, P) = \sum_{i=1}^{m} p_i \cdot d_i$$

называется избыточностью кода V, а код V^*, минимизирующий $C(V,P)$, называется оптимальным для заданного распределения P.

Если граф антипрефиксности $G = K_m$ — полный граф с m вершинами, тогда задача локально-префиксного кодирования совпадает с задачей префиксного кодирования и вопросы, связанные с оптимизацией алфавитного кодирования, эффективно разрешимы. Известен алгоритм Хаффмена [2], который строит оптимальный код в классе префиксных кодов.

Задача построения оптимального локально-префиксного кода для заданного распределения P относится к классу NP-трудных задач [3]. С ней связаны две проблемы: во-первых, построение матрицы оптимального локально-префиксного кодирования и, во-вторых, задача минимизации линейной формы на конечном множестве наборов с неотрицательными целыми компонентами.

В работе предлагается полиномиальный алгоритм построения оптимального локально-префиксного кода для некоторого подкласса кографов, т.е. графов, которые получаются из одновершинных графов путем операций сложения и умножения графов. Обозначим через $]K_1[$ класс кографов и обратим внимание на некоторые свойства этого класса. В [3] доказано, что система неравенств (1) является достаточным условием реализуемости спектра локально-префиксным кодом относительно кографа. В [4] установлено, что класс $]K_1[$ является наследственным и может быть описан при помощи запрещенных порожденных подграфов, а именно $]K_1[= Z(P_4)$. В [5] описывается линейный алгоритм распознавания кографов. Для каждого кографа можно построить кодерево, которое представляет собой корневое дерево, ориентированное от корня, листьями этого дерева являются вершины исходного кографа.

Далее $]K_1(2)[$ — класс связных кографов, кодеревья которых состоят из не более чем двух ярусов. Этот класс графов является наследственным и имеет место следующий результат.

Теорема 1. $]K_1(2)[= Z(P_4,\ K_1 \cdot (K_1 + K_2))$.

Пусть граф $G \in]K_1(2)[$, тогда для него определена производящая функция Яблонского

$$f_G(V) = (b_{1\,1} \vee \ldots \vee b_{1\,i_1}) \cdot \ldots \cdot (b_{r\,1} \vee \ldots \vee b_{r\,i_r}),$$

перечисляющая клики G, $P = (p_{1\,1}, \ldots, p_{1\,i_1}, \ldots, p_{r\,1}, \ldots, p_{r\,i_r})$ — распределение вероятностей.

Теорема 2. *Пусть* $V' = (v'_1, \ldots, v'_r)$ — *оптимальный* q*-ичный префиксный код относительно полного графа* K_r *с распределением*

вероятностей $P' = (p'_1, \ldots, p'_r)$, *где*

$$p'_k = \sum_{j=1}^{i_k} p_{k\,j} \quad (k = 1, \ldots, r),$$

тогда код

$$V = (v_{1\,1}, \ldots, v_{1\,i_1}, \ldots, v_{r\,1}, \ldots, v_{r\,i_r}),$$

где $v_{k\,1} = \ldots = v_{k\,i_k} = v'_k$ *для всех* $k = 1, \ldots, r$, *является оптимальным локально-префиксным кодом относительно графа* G *с распределением вероятностей* P.

Список литературы

1. Марков Ал. А. Введение в теорию кодирования. — М.: Наука, 1982.

2. Huffman D. A. A method for construction of minimum redundancy codes // Proc. JRE. — 1952. — V. 40, № 9. — P. 1098–1101.

3. Марков Ал. А., Смирнова Т. Г. О словарных раскрасках и некоторых совершенных графах // Дискретная математика. — 1990. — Т. 2, вып. 2. — С. 16–32.

4. Алексеев В. Е. Наследственные классы и кодирование графов // Проблемы кибернетики. Вып. 39. — М.: Наука, 1982. — С. 151–164.

5. Corneil D. G., Perl Y., Stewart L. K. A linear recognition algorithm for cographs // SIAM Journal on Computing. — 1985. — V. 14, № 4. — P. 926–934.

ПОЧТИ ВСЕ ЛАТИНСКИЕ КВАДРАТЫ ИМЕЮТ ТРИВИАЛЬНУЮ ГРУППУ АВТОСТРОФИЙ

А. В. Черемушкин (Москва)

Пусть $I_n = \{1, 2, \ldots, n\}$. Каждый латинский квадрат L порядка n можно рассматривать как табличное задание квазигрупповой операции "$\circ$", либо как ортогональный массив OA(n,3,1)

$$L = \{(i, j, k) \mid i, j \in I_n, k = i \circ j\}.$$

Изотопия — это тройка подстановок $\alpha = (r, c, s) \in S_n^3$. Действие группы изотопий на множестве латинских квадратов определяется как $\alpha : L \to L^\alpha$, где

$$L^\alpha = \{(i^r, j^c, k^s) \mid (i, j, k) \in L\}.$$

Если $L^\alpha = L$, то $\alpha \in S_n^3$ назвается автотопией. Изострофия — это преобразование $\sigma = (\alpha, \beta)$, где $\alpha \in S_n^3$, а $\beta \in S_3$ действует на I_n путем перестановки координат векторов $(i, j, k) \in I_n$, причем

$$L^{(\alpha,\beta)} = \{(i^r, j^c, k^s)^\beta \ : \ (i, j, k) \in L\}.$$

Наконец, σ — автострофия, если $L^\sigma = L$.

Основным результатом доклада является следующая

Теорема. *При $n \to \infty$ почти все бинарные квазигруппы порядка n имеют тривиальную группу автострофий.*

Ранее в [1] этот факт был установлен для группы автотопий. Доказательство основано на следующей лемме из работы [2].

Лемма. *Пусть L — латинский квадрат с нетривиальной группой автострофий. Тогда найдется некоторый изостофный ему латинский квадрат L', имеющий изострофию σ с одной из следующих структур*:

1) *для некоторого простого числа p $\sigma = (r, c, s)$, где r, c имеют порядок p и имеют одинаковое число m неподвижных точек,* $1 \le m \le n/2$;

2) *для некоторого простого числа p делящего n $\sigma = (r, c, s)$, где r, c имеют порядок p и не имеют неподвижных точек, а s имеет порядок* 1 *или p; более того, если $p = 2$ и $n \equiv 2 \pmod 4$, то s имеет по крайней мере две неподвижные точки*;

3) *$\sigma = (1, 1, s, (RC))$, где s имеет порядок* 1 *или* 2 *и по крайней мере одну неподвижную точку*;

4) $\sigma = (RCS)$.

Здесь символы R, C и S в цикловой записи подстановки β относятся к стобцам, строкам и элементам латинского квадрата соответственно.

С использованием этой леммы число квазигрупп с нетривиальной группой изострофий можно оценить сверху выражением $Q_n \le S_1 + S_2 + S_3 + S_4$, где слагаемые соответствуют числу квазигрупп порядка n, содержащих с точностью до сопряжения автотопии вида 1)–4), соответственно. Показано, что при $n \to \infty$

$$Q_n \le \frac{n^{n^2}}{e^{n^2}} \exp\{-\frac{1}{4} n^2 \ln n (1 - O(\ln^{-1} n)\}.$$

Поэтому долю таких квазигрупп среди всех квазигрупп с использованием нижней оценки числа квазигрупп L_n из [3,стр.141]

$$L_n > \frac{n^{n^2}}{e^{n^2}}$$

можно оценить сверху при $n \to \infty$ выражением

$$\frac{Q_n}{L_n} \le \exp\{-\frac{1}{4}n^2 \ln n\ (1 - O(\ln^{-1} n))\}.$$

Следствие. *При $n \to \infty$ число N_n классов эквивалентности бинарных квазигрупп порядка n относительно группы изострофий (главных классов) асимптотически оценивается следующим образом*:

$$\frac{L_n}{6(n!)^3} < N_n \le \frac{L_n}{6(n!)^3}(1 + o(1)).$$

Работа выполнена при финансовой поддержке гранта Президента РФ НШ 8564.2006.10.

Список литературы

1. Черемушкин А. В. Некоторые асимптотические оценки для класса сильно зависимых функций // Вестник ТГУ. Приложение. — Томск: Изд-во ТГУ. — № 17. — Август, 2006. — С. 87–94.

2. McKay B. D., Meynet A., Myrvold W. Small latin squares, quasigroups and loops // J. Combin. Designs. — Vol. 15, № 2. — P. 98–119.

3. Минк М. Перманенты. — М.: Мир, 1982.

ЭКВИВАЛЕНТНЫЕ КЛЮЧИ КРИПТОСИСТЕМЫ МАК-ЭЛИСА — СИДЕЛЬНИКОВА

И. В. Чижов (Москва)

Криптосистема Мак-Элиса — Сидельникова относится к классу кодовых криптосистем, то есть криптосистем, построенных на основе сложных задач из теории кодов, исправляющих ошибки. Она была предложена В. М. Сидельниковым в работе [1]. Эта криптосистема строится на основе кодов Рида — Маллера и является модификацией криптосистемы Мак-Элиса.

В работе исследуются вопросы, связанные с пространством эквивалентных секретных ключей, то есть секретных ключей, порождающих одинаковые открытые ключи, новой криптосистемы.

Опишем устройство криптосистемы Мак-Элиса — Сидельникова. Параметры криптосистемы: натуральные числа $u > 1$, r, m, $r < m/2$. Секретным ключом криптосистемы является кортеж

$$(H_1, H_2, \ldots, H_u, \Gamma).$$

Здесь $H_1, H_2, \ldots, H_u$ — невырожденные $k \times k$-матрицы над полем $F_2 = \{0, 1\}$, которые выбираются случайно и равновероятно из множества всех двоичных невырожденных $k \times k$-матриц. Матрица Γ имеет размеры $u \cdot n \times u \cdot n$ и является перестановочной.

Открытым ключом криптосистемы Мак-Элиса — Сидельникова является матрица

$$G' = (H_1 R \| H_2 R \| \ldots \| H_u R) \cdot \Gamma,$$

где символом $\|$ обозначена конкатенация матриц по столбцам, а R — порождающая матрица кода Рида–Маллера. Каждую матрицу $H_i R$ будем называть блоком, при этом $H_1 R$ — первым блоком, $H_2 R$ — вторым и т.д.

Определение. Два секретных ключа $(H_1, H_2, \ldots, H_u, \Gamma)$ и $(H'_1, H'_2, \ldots, H'_u, \Gamma')$ назовём *эквивалентными*, если соответствующие им открытые ключи совпадают, то есть выполняется соотношение

$$(H_1 R \| H_2 R \| \ldots \| H_u R) \cdot \Gamma = (H'_1 R \| H'_2 R \| \ldots \| H'_u R) \cdot \Gamma'.$$

Класс эквивалентности с представителем $(H_1, \ldots, H_u, \Gamma)$ будем обозначать как $[(H_1, \ldots, H_u, \Gamma)]$.

Верна следующая

Теорема 1. *Справедливы неравенства на мощность множества $\mathcal{E}$ открытых ключей*

$$\frac{h_k (u \cdot n)!}{(u!)^n |Aut(RM(r,m))|^u} \leqslant |\mathcal{E}| < \frac{(u \cdot n)! (h_k)^u}{u! |Aut(RM(r,m))|^u},$$

где h_k — число невырожденных матриц размерности k над полем F_2; $|Aut(RM(r,m))|$ — мощность группы автоморфизмов кода Рида-Маллера $RM(r,m)$.

Оценка сверху была доказана Г. А. Карпуниным [2].

Рассмотрим множество

$$\mathcal{G}(H_1, H_2, \ldots, H_u) = \{\Gamma \in S_{un} : \exists H'_1, H'_2, \ldots H'_u \text{ такие, что } (H_1 R \| H_2 R \| \ldots \| H_u R)\Gamma = (H'_1 R \| H'_2 R \| \ldots \| H'_u R)\}$$

Справедливо следующее

Утверждение 1. *Существует взаимно однозначное соответствие между классом эквивалентности $[(H_1, H_2, \ldots, H_u, \Gamma)]$ и множеством $\mathcal{G}(H_1, H_2, \ldots, H_u)$.*

Тем самым вопрос изучения эквивалентных секретных ключей сводится к описанию множеств $\mathcal{G}(H_1, \ldots, H_u)$.

Рассмотрим некоторую перестановку P из группы автоморфизмов кода Рида–Маллера $RM(r, m)$. Построим по ней i перестановок $\mathcal{P}[i] \in S_{un}$ следующим образом. $\mathcal{P}[i](j) = j$ для любого $j \notin I = \{(i-1) \cdot n + 1, (i-1) \cdot n + 2, \ldots, i \cdot n\}$, а $\mathcal{P}[i](I) = P(I)$. Другими слова перестановка $\mathcal{P}[i]$ в i-том блоке совпадает с перестановкой P, а во всех остальных блоках — совпадает с единичной перестановкой. Перестановки $P[i]$ будем называть моделирующими некоторый автоморфизм кода Рида–Маллера.

Следующее утверждение в немного другом виде было получено Г. А. Карпуниным [2].

Утверждение 2. *Множество $\mathcal{G}(E, \ldots, E)$ состоит из перестановок вида $\Gamma \cdot \mathcal{P}$, где Γ переставляет группы одинаковых столбцов матрицы $(R\|\ldots\|R)$, а $\mathcal{P}$ — произведение перестановок, моделирующих некоторый автоморфизм кода Рида — Маллера $RM(r, m)$.*

Теорема 2. *Пусть невырожденные матрицы $D_1, D_2, \ldots, D_u$ таковы, что существуют перестановки $P_1, P_2, \ldots, P_u$ из группы автоморфизмов кода Рида — Маллера $RM(r, m)$, что*

$$D_1 R = RP_1,\ D_2 R = RP_2,\ \ldots,\ D_u R = RP_u.$$

Обозначим далее через $\mathcal{P}_1[1], \mathcal{P}_2[2] \ldots, \mathcal{P}_u[u]$ перестановки моделирующие перестановки $P_1, \ldots, P_u$ соответственно. И пусть H — любая невырожденная матрица.

Тогда

$$\mathcal{G}(E, \ldots, E) = \mathcal{P}_1[1] \cdot \mathcal{P}_2[2] \ldots \mathcal{P}_u[u] \cdot \mathcal{G}(HD_1, \ldots, HD_u);$$

$$|\mathcal{G}(E, \ldots, E)| = |\mathcal{G}(HD_1, \ldots, HD_u)|.$$

Для случая $u = 2$ задача поиска эквивалентных ключей криптосистемы Мак-Элиса — Сидельникова основывается на изучении множеств $\mathcal{G}(E, H)$. В случае когда матрица H задаёт автоморфизм кода $RM(r, m)$ описание множества $\mathcal{G}(E, H)$ даёт теорема из раздела 5. Интересно получить описание этого множества в случае каких-то других матриц H.

Рассмотрим матрицу $T^i_{\tilde{\alpha}}$, получающуюся из единичной матрицы заменой i-той строки на вектор $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_m)$. Предполагается, что $\alpha_i = 1$.

Теорема 3. *Пусть $i = 1$. Тогда*

$$\mathcal{G}(H, HT^i_{\tilde{\alpha}}) = \{\Gamma \in \mathcal{G}(E, E) | (0\|\|(e^i \oplus \tilde{\alpha})R)\Gamma \in RM(r, m) \times RM(r, m)\}.$$

Пусть $i > 1$. *Тогда*

$$\mathcal{G}(H, HT^i_{\tilde{\alpha}}) \supseteq \{\Gamma \in \mathcal{G}(E,E) | (0 \| (e^i \oplus \tilde{\alpha})R)\Gamma \in RM(r,m) \times RM(r,m)\}.$$

Везде символом e^i *обозначен вектор, у которого на* i*-том месте стоит* 1, *а на всех остальных местах* — 0.

Список литературы

1. Сидельников В. М. Открытое шифрование на основе двоичных кодов Рида — Маллера // Дискретная математика. — 1994. — Т. 6, вып. 3. — С. 3–20.

2. Карпунин Г. А. О ключевом пространстве криптосистемы Мак-Элиса на основе двоичных кодов Рида-Маллера // Дискретная математика. — 2004. — Т. 16, вып. 2. — С. 79–84.

ДВОИЧНЫЕ КОДЫ ПОЧТИ ВСЕХ МОЩНОСТЕЙ НЕ МОГУТ БЫТЬ РАВНОМЕРНО РАСПРЕДЕЛЕННЫМИ ПО ШАРАМ

М. С. Ярыкина (Москва)

Двоичные коды, равномерно распределенные по подкубам, изучались в нескольких областях математики и в приложениях, например, двоичные коды с наибольшим дуальным расстоянием, корреляционно-иммунные и устойчивые функции, ортогональные массивы. Двоичные коды, равномерно распределенные по шарам, впервые исследовались в работе [1]. Такие коды могут использоваться в кодировании в качестве хеширующей функции, а также когда мы хотим, чтобы у всех слов после передачи по каналу связи (с ошибками) была примерно одинаковая вероятность декодирования.

Введем некоторые определения. Мы будем рассматривать двоичные коды. *Кодом* C (множеством двоичных наборов) назовем произвольное подмножество булевого куба размерности n. *Мощностью* $|C|$ называется число двоичных наборов в нем. *Расстоянием* $d(x,y)$ между двумя наборами x и y называется число компонент, в которых эти наборы различаются. *Шаром* $S_r(x)$ с центром $x \in V^n$ радиуса r называется множество $S_r(x) = \{y \in V^n \,|\, d(x,y) \leqslant r\}$. *Весом* $wt(S_r(x), C)$ шара $S_r(x)$ для кода C называется мощность множества $S_r(x) \cap C$.

Определение. Пусть l — натуральное. Код $C \subseteq V^n$ называется *равномерно распределенным по шарам со степенью* l (или l-РРШ кодом), если для любого $0 \leqslant r \leqslant n$, выполняется

$$\max\{wt((S_r(x), C)\} - \min\{wt((S_r(y), C)\} \leqslant l.$$

Мы будем рассматривать только коды мощности $|C| \leq 2^{n-1}$, поскольку в противном случае мы можем вместо кода C рассмотреть его дополнение. Полное описание 1-РРШ кодов было дано в работе [1], в том числе было получено количество 1-РРШ кодов для любого n. В частности, в работе [1] было доказано, что не существует 1-РРШ кодов мощности $|C| \geq 3$ в случае, когда $n \geq 7$. В данной работе показывается, что для любого натурального l не существует l-РРШ кодов мощности $|C| \geq 2l + 1$ для достаточно больших n (в отличие от случая $l = 1$ точно указать n_0, начиная с которого не существует искомых кодов, удалось только для некоторого диапазона мощностей).

Теорема 1 (коды малой мощности). *Пусть* $l \in \mathbb{N}$ *и* $m = m(n) \geqslant 2l + 1$. *Тогда, для достаточно больших* n *не существует* l-РРШ *кодов мощности* m *при* $\frac{m}{\sqrt{n}e^{\frac{n}{4^{l+1}}}} \underset{n\to\infty}{\longrightarrow} 0$.

Доказательство приведено в работе [2].

Теорема 2 (коды средней мощности). *Пусть* $l \in \mathbb{N}$. *Тогда существует некоторое* $k_0(l)$ *такое, что при достаточно больших* n *не существует кодов, равномерно распределенных по шарам со степенью* l, *мощности* m, *удовлетворяющего неравенствам*:

$$8nl < m < \frac{2^n}{\sum\limits_{i=0}^{k_0(l)} \binom{n}{i}}.$$

Замечание. В случае $l = 2$ имеем $k_0 = 52$.

Идея доказательства. Пусть C — l-РРШ код. В нем существует шар радиуса $k = k_0$ веса 0. Докажем по индукции, что существует шар радиуса $k + 1$ веса 0.

Шаг индукции. 1) Можно доказать, что существует шар радиуса $R \geqslant \left\lfloor \frac{2^l}{2^l-1} k \right\rfloor$ веса не более, чем l (и вес любого шара радиуса R на превосходит $2l$). 2) Если $n < 2 \cdot \frac{2^l}{2^l-1} k + 2^l + 2$, то весь булев куб покрываем $4n$ шарами радиуса R. И вес кода не превосходит $2l + 2l(4n - 1) = 8nl$. Противоречие. Если $n \geqslant 2 \cdot \frac{2^l}{2^l-1} k + 2^l + 2$, то

средний вес шара радиуса $k+1$ меньше единицы и существует шар радиуса $k+1$ веса 0.

Поскольку k растет, а n фиксированно, когда-нибудь выполнится условие $n < 2 \cdot \frac{2^l}{2^l-1}k + 2^l + 2$, то есть на каком-то шаге индукции мы придем к противоречию.

Теорема 3 (коды большой мощности, семейство 1). *Пусть $l \in \mathbb{N}$, $s \in \mathbb{N}$, $u > 1$, c_s — некоторая константа (своя для каждого s). Тогда, для достаточно больших n не существует l-РРШ кодов мощности m при*

$$\frac{ul^2}{4}\frac{2^n}{\sum\limits_{i=0}^{s}\binom{n}{i}} \leqslant m \leqslant \left(\frac{n}{s^2}+c_s\right)\frac{2^n}{\sum\limits_{i=0}^{s}\binom{n}{i}}, \qquad \text{для } s \geqslant 2.$$

$$\frac{ul^2}{4}\cdot\frac{2^n}{n+1} \leqslant m \leqslant 2^{n-1}, \qquad \text{для } s = 1.$$

В случае $s = 1$ не существует l-РРШ кодов для n, удовлетворяющих следующим условиям:

$$n > \frac{u}{u-1}\left(3l+1+\frac{ul^2}{4}\right), \quad n \geqslant 6l+3+\frac{ul^2}{2}.$$

Доказательство приведено в работе [2]. Причем для доказательства теоремы рассматриваются шары радиуса не более $2s$.

Заметим, что коды мощности m, удовлетворяющие случаю $s = 1$ — это почти все двоичные коды размерности n. Уравновешенные коды также относятся к этому случаю.

Теорема 4 (коды большой мощности, семейство 2). *Пусть $l \in \mathbb{N}$, $s \in \mathbb{N}$, λ_1, λ_2 — некоторые положительные числа и m такое что*

$$\lambda_1\frac{2^n}{\sum\limits_{i=0}^{s}\binom{n}{i}} \leqslant m \leqslant \lambda_2\frac{2^n}{\sum\limits_{i=0}^{s}\binom{n}{i}}$$

Тогда для достаточно больших n не существует l-РРШ кодов мощности m.

Замечание. Числа λ_1 и λ_2 выбираем так, чтобы первое и второе семейства мощностей пересекались.

Идея доказательства. Пусть C — l-РРШ код. Оценим число пар кодовых слов во всех шарах радиуса s двумя способами.

Первый способ заключается в том, что в каждом шаре радиуса s веса t содержится $\binom{t}{2}$ пар наборов на расстоянии не более $2s$. Причем известно, что максимальное и минимальное значения t отличаются не более, чем на l. Второй способ заключается в том, что мы рассмотрим все шары радиуса $2s$ с центром в кодовых словах.

Разобьем эти шары на сферы радиусом от 1 до $2s$, оценим вес каждой сферы (веса двух сфер одного радиуса отличаются не более, чем на $2l$), и оценим число пар кодовых слов на расстоянии 1, 2 и так далее до $2s$ отдельно. Сравнив две полученные оценки, придем к противоречию.

Список литературы

1. Таранников Ю. В. О классе булевых функций, равномерно распределенных по шарам со степенью 1 // Вестник Московского Университета. Серия 1. Математика. Механика. — 1997. — Вып. 52, № 5. — С. 18–22.

2. Ярыкина М. С. Применение оценок для сумм биномиальных коэффициентов при решении некоторых задач теории кодирования и криптографии // Математические вопросы кибернетики. Вып. 12. — М.: Физматлит, 2003. — С. 87–108.

СПИСОК ПЛЕНАРНЫХ ДОКЛАДОВ, ПРОЧИТАННЫХ НА СЕМИНАРЕ

О. М. Касим-Заде (Москва) *О работах О. Б. Лупанова*
Н. П. Редькин (Москва) *Минимальные и асимптотически минимальные схемы для некоторых индивидуальных булевых функций*
А. М. Зубков (Москва) *Формула включения-исключения и оценки для вероятности объединения событий*

В. Н. Чубариков (Москва) *Распределение значений последовательностей*
М. Ю. Мошков, М. Пилищук, Б. Зелёско (Сосновец, Польша) *Приближенные покрытия, тесты и решающие правила*
В. Н. Козлов (Москва) *Симплекс-кодовый метод распознавания зрительных образов*
С. С. Марченков (Москва) *Суперпозиции элементарных арифметических функций*
Е. А. Окольнишникова (Новосибирск) *Нижние оценки сложности ветвящихся программ*

В. Б. Кудрявцев, А. С. Строгалов (Москва) *Компьютерные обучающие системы*
А. С. Подколзин (Москва) *Компьютерное моделирование логических процессов*
В. Н. Шевченко (Нижний Новгород) *Об исследовании миноров матрицы при помощи ее сингулярного многочлена*
С. А. Ложкин (Москва) *Асимптотические оценки высокой степени точности для сложности схем из некоторых классов*
В. И. Иванов (Тула) *Задача Дельсарта для разложений по многочленам Чебышева*

В. Б. Алексеев (Москва) *Об асимптотиках логарифма числа дискретных функций*
Э. Э. Гасанов (Москва) *Оптимизация хранения и поиска информации*
Д. Г. Фон-дер-Флаасс (Новосибирск) *Совершенные раскраски вершин булева куба*
Н. П. Долбилин (Москва) *Теоремы Минковского о многогранниках и параллелоэдрах*
Р. М. Колпаков (Москва) *О числе периодических структур в конечных словах (обзор)*
С. Б. Гашков (Москва) *О сложности вычислений в конечных полях (обзор)*

С О Д Е Р Ж А Н И Е

Пленарные доклады

Секция «Синтез, сложность и надежность управляющих систем»

Секция «Функциональные системы»

Секция «Комбинаторный анализ и теория графов»

Подсекция «Комбинаторный анализ»

Подсекция «Теория графов»

Секция «Математическая теория интеллектуальных систем»

Секция «Дискретная геометрия»

Секция «Теория кодирования и смежные вопросы»