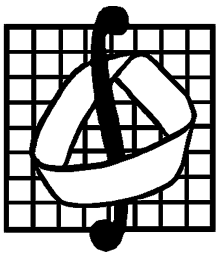
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

МАТЕРИАЛЫ

XIII Международного семинара

«ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ»

имени академика О. Б. ЛУПАНОВА

(Москва, 17–22 июня 2019 г.)

Издательство механико-математического факультета МГУ

Москва 2019

М34
УДК 519.7

М34 Материалы XIII Международного семинара «Дискретная математика и ее приложения» , имени академика О. Б. Лупанова (Москва, МГУ, 17–22 июня 2019 г.) / Под редакцией О. М. Касим-Заде. — М.: Изд-во механико-математического факультета МГУ, 2019. — 336 с.

Сборник содержит материалы XIII Международного семинара «Дискретная математика и ее приложения» имени академика О. Б. Лупанова, проходившего на механико-математическом факультете МГУ имени М. В. Ломоносова с 17 по 22 июня 2019 г. Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание

МАТЕРИАЛЫ
XIII МЕЖДУНАРОДНОГО СЕМИНАРА
«ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ»
имени академика О. Б. Лупанова
(Москва, МГУ, 17–22 июня 2019 г.)

Под общей редакцией О. М. КАСИМ-ЗАДЕ

Редакционная группа:
О. С. Дудакова, М. Д. Ковалев, Р. М. Колпаков, Ю. А. Комбаров, В. В. Кочергин, А. В. Чашкин

Ответственный за выпуск *Ю. А. Комбаров*

Н/К
ИД № 04059 от 20.02.2001 Подписано к печати 20.11.2019. Формат 60 × 90/16.
Бумага типогр. № 1. Печ. л. 21. Тираж 100 экз.
Издательство механико-математического факультета МГУ. 119991, Москва, Ленинские горы, МГУ.
Отпечатано с оригинал-макета в типографии «DIAMOND TEAM», Москва.

ПРЕДИСЛОВИЕ

XIII Международный семинар «Дискретная математика и ее приложения» имени О. Б. Лупанова, проходил на механико-математическом факультете МГУ имени М. В. Ломоносова с 17 по 22 июня 2019 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 более 100 участников (в том числе около 40 докторов наук) из 32 научных центров России, Беларуси, Молдовы и Узбекистана.

Работа семинара проходила в семи секциях:

— синтез, сложность и надежность управляющих систем,

— теория функциональных систем,

— комбинаторный анализ,

— теория графов,

— математическая теория интеллектуальных систем,

— дискретная геометрия,

— теория кодирования и математические вопросы теории защиты информации.

Всего было заслушано 12 пленарных и 82 секционных докладов; содержание большинства из них отражено в настоящем сборнике.

Тексты публикуются в авторской редакции (исправлены замеченные опечатки).

ПЛЕНАРНЫЕ ДОКЛАДЫ

ПОЛНОТА МНОЖЕСТВА СЛОВ И СТРУКТУРИРОВАННОЕ КОДИРОВАНИЕ В ЗАДАЧАХ ДИСКРЕТНОЙ МАТЕМАТИКИ

А. А Евдокимов (Новосибирск)

Множество S слов в конечном алфавите A называется полным, если любая бесконечная последовательность букв из A содержит в качестве подслова хотя бы одно слово из S. В этом случае говорят, что множество слов-запретов S блокирует любую бесконечную последовательность букв алфавита A. Исследования полноты множества слов и задач об избегании символьными последовательностями множества «запрещённых» подслов были начаты автором ещё в 70-х годах, а в общем виде проблема полноты была сформулирована в небольшой заметке [1] и в докладе «Бесповторные последовательности», сделанном на совместном российско-германском математическом коллоквиуме в 1979 г. в Ростоке (Грейсвальд). В [1] отмечена взаимосвязь сформулированной проблемы полноты с задачами из различных областей дискретной математики. Отмечена польза изучения комбинаторных задач о символьных последовательностях в их геометрической интерпретации на графах перекрытия слов (de Bruijn graphs), в частности, для эффективного алгоритмического распознавания свойства полноты конечного множества слов. Приводится результат В. А. Крайнева об ограниченности длины бесповторных в сильном смысле двоичных последовательностей (подробнее ниже). Даны ориентиры дальнейших исследований.

Интерес к этой тематике и постановка проблемы полноты в общем виде возникли у автора после решения им двух комбинаторных задач. Первая — это проблема венгерского математика П. Эрдёша о существовании бесконечной символьной последовательности в конечном алфавите, которая не содержит двух подряд повторяющихся отрезков с одинаковым составом букв в них. Была найдена конструкция бесконечной бесповторной символьной последовательности, которая избегает запреты таких повторений [2, 3]. Для задач о бесповторных последовательностях удалось довольно глубоко продвинуться в понимании трудностей исследования границы перехода от полноты к неполноте. В этом отношении интересен результат о конечности длины слов в бинарном алфавите для множества за-

претов более сильного типа, когда требуется отсутствие повторений подслов, равных по частотному составу букв в них, причём это верно для любого числа повторов [4]. Интересна геометрическая интерпретация этих задач. В частности, вопрос, поставленный автором ещё в 70-х годах. Существует ли бесконечный путь в положительном направлении ортов целочисленной решётки размерности n , который не содержит k точек, лежащих на одной прямой? Для $n = 2$ и любом $k > 2$ ответ отрицательный. Для алфавита мощности $n > 3$ и произвольного k задача окончательно не решена.

Исследования по комбинаторике бесповторных последовательностей имеют давнюю историю. Так, исследования норвежского математика А. Туэ по задачам алгоритмической разрешимости в ассоциативных исчислениях были выполнены ещё в начале прошлого столетия. В 20-е годы были опубликованы работы М. Морса по топологической динамике. В этих работах использовалась возможность простого конструктивного задания бесконечных бесповторных последовательностей. Позднее в 60-е годы возродился интерес к изучению различных вариаций свойства «сильной непериодичности», нерегулярности, псевдослучайности символьных последовательностей, сложности их определимости и вычислимости, что связано с интенсивным исследованием в этот период математических оснований Computer Science, кибернетики и прикладных задач информатики [5, 6].

Вторая задача, послужившая источником интереса и постановки проблемы полноты, известна в математической литературе под названием «Snake-in-the-Box Problem». Змея (snake) - это простой путь (или цикл) в булевом n-мерном кубе, который не содержит хорд, то есть является порождённым подграфом n-куба. Вопрос о максимальной длине такого пути возник при исследовании локальных алгоритмов минимизации булевых функций, представленных формулами в дизъюнктивной нормальной форме [6]. Задача о максимальной длине цепи и цикла исследовалась автором в интерпретации слов с запретами, когда пути в гиперкубе размерности n кодируются символьными последовательностями в n-буквенном алфавите с запретами на подслова. Причём нахождение порядка величины максимальной длины цикла и его конструкция существенно опираются на существование и построение бесконечной «управляющей» последовательности тоже с ограничениями-запретами специального вида на её подслова [7]. Много новых сведений о публикациях и приложениях по проблеме Snake-in-the-Box можно найти по поисковой системе Google. В том числе, по поиску с помощью современных компьютерных технологий «длинных змей» в гиперкубах малых размерностей.

При исследовании полноты множества слов возникает два типа вопросов. Во-первых, это исследование полноты конкретных конечных или бесконечных множеств запретов и построение избегающих запреты символьных последовательностей в случае неполноты множества слов. Во-вторых, исследования вопросов общего типа. Например, построение алгоритмов распознавания полноты, их сложность, исследование на полноту конструктивно определяемых классов бесконечных множеств, описание множества свободных от запретов слов и последовательностей, его мощность, оценки максимальной длины слов, свободных от запретов, функция роста числа слов длины n. В настоящее время интенсивно развиваются исследования в области, именуемой в более широком контексте рассматриваемых задач «комбинаторикой слов» [8, 9]. Слова и символьные последовательности — объект исследования в теории формальных языков [10], теории кодирования и сжатия информации, символической динамике, теории автоматов, математических основаниях криптографии и программирования. Задачи анализа строения и исследование свойств цепочек символов (strings of symbols) возникают во многих областях естественных наук. Нахождение эффективных алгоритмов решения этих задач является актуальной областью исследования, которой посвящено большое число публикаций.

Пусть S — полное множество, то есть множество $\hat{S}$ слов, свободных от запретов, конечно. Введем функции

$$L(\hat{S}) = \max_{X \in \hat{S}} |X|,$$

$$L(n) = \max_{S} L(\hat{S}),$$

где первый максимум берется по всем словам, свободным от запретов, а второй максимум — по всем полным множествам слов $S \subset A^n$.

Теорема ([11, 12])**.** $L(n) = C(n) + n - 1 = |A|^{n-1} + n - 2$*, где* $C(n)$ *— наибольшая длина простого пути без хорд в графе де Брёйна порядка* n*.*

Пусть $M(n) = \min_S |S|$, где S — полное множество, $S \subset A^n$.

Теорема ([11, 12])**.** $M(n) = \frac{1}{n}\Sigma_{d|n}\phi(\frac{n}{d})|A|^d$*, где* ϕ *— функция Эйлера.*

Заметим, что $M(n)$ $|A|^n/n$, и если $|A| = 2$, то $M(10) = 108$. Таким образом, любое множество двоичных слов длины 10, содержащее менее 108 слов, является избегаемым, и эта граница точна, то есть существует множество из 108 слов длины 10, блокирующее любую бесконечную двоичную последовательность.

Теперь об алгоритмах распознавания полноты множества слов $S \subset A$.

Теорема. *Полнота всякого множества $S \subset A^n$ распознаваема с трудоемкостью порядка $|S| \cdot n$.*

Доказательство использует интерпретацию задач о полноте на графах де Брёйна B_m^n и опирается на эквивалентность следующих утверждений:
1) S — полное множество слов;
2) множество $V(S)$ разрезает все контуры графа B_m^n;
3) подграф графа B_m^{n-1}, образованный множеством дуг $E(B_m^{n-1}) \setminus E(S)$ ациклический;
где $V(S)$ и $E(S)$ — множества вершин графа B_m^n и дуг графа B_m^{n-1}, которые соответствуют словам множества S. Эквивалентность утверждений 1-3 основывается на соответствии между словами X длины $|X| \geq n$ и ориентированными путями в графе B_m^n, проходящими через вершины, соответствующие подсловам длины n слова X. Эквивалентность утверждений 2 и 3 верна, поскольку граф B_m^n является реберным графом для B_m^{n-1} по определению графов де Брёйна. Таким образом, распознавание полноты множества слов S можно заменить проверкой отсутствия ориентированных контуров в подграфе, образованном множеством дуг $E(B_m^{n-1}) \setminus E(S)$. Остаётся заметить, что проверяя полноту множества S можно считать, что $|S| \geq |A|^n/n$, так как иначе S не полно по определению функции $M(n)$. Поэтому имеем

$$|E(B_m^{n-1}) \setminus E(S)| = |A|^n - |S| \leq O(|S|(n-1)) \tag{1}$$

Остаётся заметить, что проверка ацикличности ориентированного графа, например. алгоритмом поиска в глубину возможна с трудоемкостью порядка суммы чисел его вершин и дуг. Вместе с неравенством (1) и утверждениями 1-3 это доказывает теорему.

Уточним теперь вопрос о границе длин свободных от запретов слов множества $\hat{S}$, сформулировав его следующим образом. Пусть l есть некоторое натуральное число, S — полное множество слов, то есть множество $\hat{S}$ ограничено. Существует ли в $\hat{S}$ слово, длина которого превосходит l?

Теорема. *Задача распознавания существования в $\hat{S}$ слова длины не менее l является NP-полной.*

Таким образом, распознавание ограниченности длин слов, избегающих множество запрещенных подслов, возможно со сложностью $|S| \cdot n$, а вопрос о локализации этой границы имеет качественно иную

трудоёмкость. Ещё в ранних работах по полноте множества слов автором была поставлена следующая задача. Введём функцию

$$f(m,n) = \max \frac{|S_1|}{|S_2|},$$

где $m = |A|$, а максимум берется по всем парам $\{S_1, S_2\}, S_1 \subset A^n, S_2 \subset A^n$ полных неприводимых множеств (то есть таких, удаление любого слова из которого приводит к неполноте). Существуют полные неприводимые множества, мощность которых не минимальна. Например, множество из 7 слов $\{0000, 0001, 1001, 0101, 0110, 0111, 1111\}$ полное и неприводимое, но не минимальное, так как $M(4) = 6$.

Задача. *Насколько велико может быть различие мощностей полных неприводимых множеств? Как ведёт себя (например, по n при фиксированном m), функция $f(n,m)$? Точные оценки её роста значительно прояснили бы структуру полных множеств слов* [11–13].

Поясним идею ещё одного алгоритма распознавания полноты множества слов, представленного в [14]. Несмотря на простоту алгоритма, он оказывается полезным вот следующем отношении. К множеству слов S применяются определённые инвариантные преобразования, в результате которых получаем цепочку «производных от S» множеств с сохранением их свойства быть полным или неполным множеством. При этом на каждом шаге алгоритма производится сокращение описания получаемого множества запретов. Через конечное число шагов по результату однозначно имеем ответ «да, полное» или «нет». Тем самым мы получаем не только более компактное описание исходного множества запретов, но и эффективное «кодирование через запреты» множества $\hat{S}$ слов, свободных от запретов S.

Вопросы полноты множества слов естественно ставить не только по отношению к множеству всех слов, но и по отношению к любому бесконечному множеству M слов и ω-слов (слов бесконечной длины). Множество запретов S полно относительно M, если $P(\omega) \cap S \neq \emptyset$ для любого ω-слова из M, где $P(\omega)$ — множество всех подслов ω-слова. Если $P(\omega) \subset M$ для любого $\omega \in M$, то множество M назовём замкнутым. Это согласуется с обычным определением оператора замыкания по операции включения в M всех подслов каждого его слова. В подобном случае множество «объектов», замкнутое присоединением всех «подобъектов» называют ещё наследственно замкнутым.

Теорема. *Для любого наследственно замкнутого бесконечного M и произвольного S справедливо*

a) $\hat{S}$ — *замкнутое множество меры 0;*
b) *существует* ω*-слово, такое, что* $P(\omega) \subset M$*;*
c) S *полно относительно* M *тогда и только тогда, когда* $\hat{S} \cap M$ — *конечное множество;*
d) *во всяком бесконечном* S*, полном относительно* M*, существует конечное* $S' \subset S$ *также полное относительно* M*;*
e) *существуют такие бесконечные множества* S *и* M*, что* S *полно относительно* M *и остаётся полным после удаления из* S *любого его конечного подмножества.*

Заметим, что для множеств M, которые не являются наследственно замкнутыми, теорема, вообще говоря, неверна.

Как видно из теоремы, некоторые свойства фактически повторяют полноту запретов по отношению к множеству всех слов в произвольном конечном алфавите. Однако теперь существенным является выполнение свойства наследственной замкнутости множества, по отношению к которому рассматривается проблема полноты.

Выше уже говорилось о пользе «языка запретов» при кодировании множеств, в частности, описании задач вложения графов в гиперкубы и их решении. Например, это задачи существования и построения в гиперкубе гамильтоновых циклов с различными ограничениями-запретами на их структуру [15], задача Snake-in-the-Box , вложения в гиперкубы целочисленных решёток [16], деревьев, графов вычислительных структур. Вложения в гиперкубы мы рассматриваем как такие кодирования объектов (графов), которые сохраняют в образе-коде определённые структурные свойства кодируемых объектов и называем структурированным кодированием [17, 18]. При таком подходе большое значение имеет универсальность n-мерного куба, как множества слов длины n в конечном алфавите, которое может быть наделено различного типа структурами геометрического, алгебраического, порядкового или метрического типа: граф, частично упорядоченное множество, целочисленная решётка, абелева группа, метрическое векторное пространство с метрикой Хемминга, метрикой тора или другими метриками. Эта универсальность позволяет моделировать в образе-коде в гиперкубе различного типа структуры вкладываемых множеств, сохраняя в коде необходимые свойства исходных кодируемых структур.

Отметим, что структурированное кодирование, предполагая сохранение отображением различного типа свойств, позволяет распознавать и корректировать «ошибки» в образе проверяя и анализируя выполнение или невыполнение сохраняемых отображением свойств (обобщённая концепция помехоустойчивого кодирования). Задачи кодирования данных с сохранением их структурных свойств возни-

кают и в связи с реализацией в вычислительных системах гиперкубовой архитектуры, в которой информационное взаимодействие микропроцессоров определяется их соединением в структуру n-мерного куба. Для таких сетей возникают вопросы обмена информацией, распараллеливания вычислений и целый ряд других задач отображения структур данных на структуру вычислительной сети. Например, полное или частичное сохранение в кодах метрической структуры исходного множества при изометрическом или локально изометрическом его вложении в гиперкуб. Важный прикладной аспект структурированного кодирования состоит и в том, что оно позволяет удобно и быстро работать с элементами исходного множества уже в их машинных кодах с использованием операций, взаимосвязанных со структурой вычислительной сети. Это ускоряет обработку данных и повышает скорость вычисления.

Различные классы отображений, определяющих вложения дискретных метрических пространств рассматривались в [17, 18]. Это изометрические и локально изометрические отображения, вложения «с растяжением» расстояний, параметрическое семейство отображений ограниченного искажения, дискретный аналог гомеоморфных вложений. Последнее предполагает введение аналога непрерывности отображения для дискретного случая, когда отображение «близкие точки метрического пространства не разрывает, а далёкие точки не переводит в близкие». В [18] определения даны в различных вариантах: параметрические отображения ограниченного искажения, определение в топологических терминах дискретных окрестностей, в частности, дискретный аналог гомеоморфных вложений. Варьируя параметры и вид отображений, получаем различные классы вложений, определяющих тип структурированного кодирования, сохраняющего в сильной или слабой форме нужные структурные свойства кодируемого множества.

Рассмотренные направления исследований и полученные результаты докладывались на международных конференциях, семинарах и школах в России и зарубежных странах в различные периоды, начиная с 80-ых годов.

Работа выполнена при финансовой поддержке проекта РАН № 0314–2015–0011 и программы повышения конкурентоспособности Новосибирского государственного университета.

Список литературы

1. Евдокимов А. А., Крайнев В. А. Задачи о полноте систем слов // XXII Обл. научно-техн. конф. Новосибирск. — 1979. — С.105–107.

2. Евдокимов А. А. О сильно асимметричных последователь-

ностях, порожденных конечным числом символов // Докл. АН СССР. — 1968. — Т. 179, № 6. — С. 1268–1271. Перевод: Strongly asymmetric sequences generated by a finite number of symbols // Soviet Math. Dokl. — 1968. — V. 9. — P. 536–539.

3. Евдокимов А. А. Существование базиса, порождающего 7-значные бесповторные последовательности // Дискретный анализ. — 1971. — Вып. 18. — С. 25–30.

4. Крайнев В. А. Слова, не содержащие последовательных подслов, равных по частотному составу // Методы дискретного анализа в решении комбинаторных задач. — 1980. — Вып. 34. — С. 27–37.

5. Машины Тьюринга и рекурсивные функции. — М.: Мир. 1972.

6. Дискретная математика и математические вопросы кибернетики. — М.: Наука, 1974.

7. Евдокимов А. А. О максимальной длине цепи в единичном n-мерном кубе // Математические заметки. — 1969. — Т. 6, вып. 3. — С. 309-319. Перевод: On the maximal chain length of an unit n-dimensional cube // Math. Notes. — 1970. — V. 6. — P. 642–648.

8. Berstel J., Karhumaki J. Combinatorics on words — A tutorial // Bull. EATCS. — 2003. — 79. — P. 178–229.

9. Lothaire M. Applied Combinatorics on Words. — Cambridge: Cambridge University Press, 2005.

10. Саломаа А. Жемчужины теории формальных языков. — М.: Мир. 1986.

11. Евдокимов А. А. Полные множества слов и их числовые характеристики // Методы дискретного анализа в исследовании экстремальных структур. — 1983. — Вып. 39. — С. 7–19.

12. Евдокимов А. А. Исследование полноты множеств слов и языков с запретами // Вестник Томского государственного университета. Приложение. — 2004. — № 9(1). — С. 8–12.

13. Evdokimov A. A., Kitaev S. V. Crucial words and the complexity of some extremal problems for sets of prohibited words // J. Comb. Theory. Ser. A. — 2004. — V. 105. — P. 273–289.

14. Евдокимов А. А. Алгоритм распознавания полноты множества слов и динамика запретов // ПДМ. Приложение. — 2016. — № 9. — С. 10-–12.

15. Пережогин А. Л. Простые циклы в n-кубе с большой группой автоморфизмов // Дискретн. анализ и исслед. опер. — 2013. — 20(4). — С. 88–97.

16. Евдокимов А. А. Кодирование конечной целочисленной решётки в классе отображений ограниченного искажения // Прикладная дискретная математика. Приложение. — 2011. — № 4. — С. 8–9.

17. Евдокимов А. А. Метрические свойства вложений и коды, сохраняющие расстояния // Модели и методы оптимизации. Тр. АН СССР. Сибирское отделение. Ин-т математики; Т. 10. — Новосибирск: Наука, 1988. — С. 116–132.

18. Евдокимов А. А. Кодирование структурированной информации и вложения дискретных пространств // Дискретный анализ и исследование операций. — 2000. — Т. 7, № 4. — С. 48–58.

ОТ ЛОКАЛЬНОЙ ИДЕНТИЧНОСТИ К ГЛОБАЛЬНОЙ СИММЕТРИИ

Н. П. Долбилин (Москва)

Пусть X — дискретное множество точек в евклидовом пространстве $\mathbb{R}^d$ и $\mathrm{Sym}(X)$ — группа его симметрий, т.е. евклидовых изометрий пространства, которые отображают множество X на себя. Согласно принятой в кристаллографии концепции, предложенной великим кристаллографом Е. С. Федоровым [1], кристалл, здесь имеется в виду его атомная структура, есть дискретное множество точек, группа симметрий которого является кристаллографической группой. Напомним, что подгруппа группы $Iso(d)$ всех изометрий евклидова пространства $\mathbb{R}^d$ называется *кристаллографической* группой, если она действует разрывно (орбита любой точки относительно группы есть дискретное множество), а фундаментальная область компактна. Отметим, что все 230 кристаллографических групп в трехмерном пространстве были найдены Федоровым в 1891 г. одновременно с А.Шенфлисом [2].

Наличие у данного множества той или иной кристаллографической группы является свойством глобального характера, то есть свойством данного множества в целом. В то же время кристаллическая структура рождается из аморфной субстанции в процессе кристаллизации. Этот процесс имеет локальный характер, так как является результатом взаимодействия «близко расположенных» атомов. Появление периодичности в кристаллах обычно объясняют так: в процессе кристаллизации атомы «слипаются» друг с другом в устойчивые конфигурации (кластеры), соответствующие минимуму внутренней энергии. Кластеры, минимизирущие энергию для данного вида атомов, конгруэнтны друг другу. Возникающая таким образом повторяемость атомных кластеров в структуре и есть причина регулярности атомной структуры кристалла в целом.

Несмотря на отсутствие серьезных аргументов, связь между идентичностью относительно небольших кластеров в структуре и ее глобальной правильностью считалась очевидной, а поиск строгого доказательства, казалось, имел лишь абстрактный интерес. Однако в действительности дело обстоит гораздо сложнее. В частности, 1970-е гг. Р. Пенроуз представил ныне очень популярные *мозаики Пенроуза*, в которых, с одной стороны, каждая локальная конфигурациия повторяется неограниченное количество раз, подобно тому, как это происходит в кристалле. Более того, в мозаиках Пенроуза присутствуют и также многократно повторяются фрагменты неограниченных размеров с пятиугольной симметрией, что невозможно в

кристаллических структурах. И, действительно, несмотря, на повторяемость локальных кластеров, мозаика Пенроуза представляет собой некристаллографическую структуру. Впоследствии, в 1982 г. физик Д. Шехтман получил в лабораторных условиях реальный сплав алюминия и марганца с трехмерной структурой, обладающей симметриями 5-го порядка (нобелевская премия 2011 г. по химии за открытие квазикристаллов). Тем самым, открытые сначала в теории, а затем и в реальности структуры показали, что связь между повторяемостью и кристаллогрфической симметрией не столь очевидна.

Впрочем еще до этих результатов, а именно в 1974 году на вопрос о возможной связи между локальной идентичностью и глобальной регулярностью обратил внимание Б. Н. Делоне. Одной из основных целей развитой в отделе геометрии, реорганизованном впоследствии в отдел геометрии и топологии Математического института им. В. А. Стеклова, *локальной теории правильных систем* было доказательство строгих утверждений, описывающих в чисто геометрических терминах связь между локальными условиями и симметрией дискретного множества точек.

Здесь будет дан обзор некоторых результатов локальной теории правильных систем, а также будут изложены недавние результаты автором о так называемых $2R$-изометричных множествах.

Определения и общие результаты. Надо сказать, что весьма подходяшей моделью для атомной структуры любого твердого вещества, как кристаллического так и аморфного, является (r, R)-*система* или, как теперь говорят, *множество Делоне* [5, 6].

Напомним, множество $X \subset \mathbb{R}^d$ называется *множеством Делоне* (типа r, R), где r и R — положительные числа, если выполняются два условия:
(r) открытый шар $B^\circ_y(r)$ с центром в произвольной точке y пространства содержит не более одной точки из X;
(R) замкнутый шар $B_y(R)$ радиуса R содержит не менее одной точки из X.

Множество Делоне X называется *правильной системой*, если группа симметрий $\mathrm{Sym}(X)$ действует транзитивно на множестве X.

Нетрудно показать, что транзитивно действующая на множестве Делоне группа симметрий является кристаллографической группой. Так как кристалл по Федорову — это дискретное множество с кристаллографической группой, то кристалл есть объединение конечного числа правильных систем.

Отметим, что концепция правильной системы, с одной стороны, обобщает понятие решетки целых точек, на которой, как известно, действует транзитивно некоторая группа трансляций. С другой сто-

роны, по знаменитой теореме Шенфлиса–Бибербаха [2, 3] (которая является решением XVIII проблемы Гильберта [4]), любая кристаллографическая группа содержит подгруппу параллельных переносов конечного индекса. Поэтому всякая правильная система X есть объединение конечного числа решеток — трансляций некоторой решетки Λ:

$$X = \cup_{i=1}^{n}(\Lambda + t_i), \quad t_i \in \mathbb{R}^d.$$

Следовательно, правильная система в d-мерном пространстве является периодической в d линейно независимых направлениях.

Пусть $X \subset \mathbb{R}^d$ — множество Делоне, введем необходимые для дальнейшего определения, а также некоторые известные факты.

- Дано множество Делоне X, $x \in X$ и $\rho > 0$ подмножество $C_x(\rho) := \{x' \in X \quad | \quad |xx'| \leq \rho\}$ называется *ρ-кластером* точки x.
- Кластеры $C_x(\rho)$ и $C_{x'}(\rho)$, $x, x' \in X$ *эквивалентны/конгруэнтны*, если существует изометрия (движение) g, такая что $g(x) = x'$ и $g(C_x(\rho)) = C_{x'}(\rho)$
- $N(\rho)$ — мощность множества классов ρ-кластеров во множестве X. Очевидно, что для $0 \leq \rho < 2r$ в любом множестве Делоне $N(\rho) = 1$ (см. r-условие выше).
- Ранг ρ-кластера $\mathrm{rank}(C_x(\rho))$, т.е. размерность аффинной оболочки кластера $C_x(\rho)$, равен d для любого $\rho \geq 2R$.
- Если $N(\rho) < \infty$ для любого $\rho > 0$, то множество X *конечного типа*, а положительную целочисленную, *монотонно неубывающуь* функцию $N(\rho)$ назовем *перечисляющей функцией* (the *cluster counting function*-англ.) .
- Известно, что если $N(2R) < \infty$, то $N(\rho) < \infty$ для любого $\rho > 0$, т.е. X есть множество Делоне *конечного типа* (см., например, [10, 12]).
- Из определения правильной системы непосредственно вытекает, что множество Делоне есть правильная система тогда и только тогда, когда $N(\rho) = 1$ для всех $\rho \geq 0$.
- Вопрос, с которого начиналась локальная теория для правильных систем, состоял в следующем: существует ли такое положительное значение ρ_0, что эквивалентность ρ_0-кластеров в множестве Делоне X обеспечивало бы его правильность, или в терминах перечисляющей функции $N(\rho)$: $N(\rho_0) = 1 \Rightarrow N(\rho) = 1$ для всех $\rho \geq \rho_0$.
- Для данной размерности d обозначим через $\hat{\rho}_d$ *радиус регулярности* — такое значение радиуса кластера, что условие $N(\hat{\rho}_d) = 1$ гарантирует правильность множества Делоне X и

в то же время для любого $\varepsilon > 0$ существует множество Делоне с $N(\hat{\rho}_d - \varepsilon) = 1$, не являющееся правильной системой.

- $S_x(\rho) := \{s \in Iso(d) \,|\, s(x) = x,\ s(C_x(\rho)) = C_x(\rho)\}$ — *группа ρ-кластера* $C_x(\rho)$, то есть группа всех изометрий s, таких что $s(x) = x$ и $s(C_x(\rho)) = C_x(\rho)$.
- $S_x(\rho) \supset S_x(\rho')$ для $\rho > \rho'$. Далее, т.к. $\mathrm{rank}(C_x(2R)) = d$, группа $S_x(2R)$ конечна.

Первым результатом локальной теории была следующая теорема (см. [7]).

Теорема 1 (Локальный критерий для правильной системы)**.** *Множество Делоне $X \subset \mathbb{R}^d$ является правильной системой тогда и только тогда, когда для некоторого $\rho_0 > 0$ выполняются два условия:*
(1) $N(\rho_0 + 2R) = 1$*;*
(2) $S_x(\rho_0) = S_x(\rho_0 + 2R)$ *для* $x \in X$*.*

Прежде, чем говорить о следствиях из локального критерия, сформулируем его обобщение для случая кристалла, т.е. мультиправильной системы (см. [8], для доказательства [10, 12]).

Теорема 2 (Локальный критерий для кристалла)**.** *Множество Делоне $X \subset \mathbb{R}^d$ с параметрами r R является кристаллом, состоящим из m правильных систем, тогда и только тогда, когда при некотором $\rho_0 > 0$ выполняются два условия:*
(1) $N(\rho_0) = N(\rho_0 + 2R) = m$*;*
(2) $S_i(\rho_0) = S_i(\rho_0 + 2R)$, $\forall i \in [1, m]$, *где* $S_i(\rho_0)$ *— это класс сопряженных групп, соответствующий i-му классу ρ_0-кластеров. .*

Приведем теперь следствия, вытекающие из Локального критерия для правильных систем (теорема 1). Условие (1) означает, что $(\rho_0 + 2R)$-кластеры $C_x(\rho_0 + 2R)$ для всех $x \in X$ конгруэнтны. Конгруэнтные кластеры имеют сопряженные группы симметрий. Условие (2) означает, что группы ρ_0- и $(\rho_0 + 2R)$-кластеров совпадают. Поэтому из теоремы 1 немедленно следует

Теорема 3. *Пусть для множества Делоне $X \subset \mathbb{R}^d$ имеем $N(4R) = 1$ и пусть группа $S_x(2R)$ $2R$-кластера тривиальна. Тогда $N(\rho) \equiv 1, \forall \rho > 4R$, то есть X — правильная система.*

Рассмотрим теперь случай, когда все $2R$-кластеры $C_x(2R)$, $x \in X$ эквивалентны и $S_x(2RR) = G$ — конечная группа изометрий. Назовем подпоследовательность вложенных подгрупп $G = G_1 \supset G_2 \supset \cdots \supset G_m = \{e\}$, заканчивающуюся тривиальной группой, *башней*, а число m входящих в нее подгрупп *высотой*. Обозначим через $m(G)$ высоту наибольшей башни в G. Из локального критерия нетрудно

вывести теорему 4 (для доказательства см. [10, 12]).

Теорема 4 (о высоте башни)**.** *Если для множества Делоне X выполняется $N((m+1)2R) = 1$, где $m = m(S_x(2R))$, то X — правильная система.*

Требование конгруэнтности кластеров радиуса $(m(S_x(2R))+1)2R$ объясняется тем, что гарантировать стабилизацию группы кластера в общем случае можно, когда последовательность вложенных групп заканчивается тривиальной группой.

Для $d = 2$ в силу теоремы 5 требование $N(4R) = 1$ нельзя ослабить.

Теорема 5 ($(4R-\varepsilon)$-теорема)**.** *Для любого $\varepsilon > 0$ существует множество Делоне $X \subset \mathbb{R}^2$, такое что $N(4R-\varepsilon) = 1$, но X не является правильной системой.*

Доказательство состоит в предъявлении конструкции (см., например, [10, 12] множества Делоне X на плоскости с $N(4R-\varepsilon) = 1$, не являющегося правильной системой. В 2016 году автор показал эту конструкцию на конференции в Американском институте математики (AIM, Сан Хосе, США). Последовавшее за этим коллективное обсуждение в группе «Множества Делоне», созданной в рамках этой конференции, привело к обобщению нижней оценки для любой размерности d (теорема 6, доказательство в [13]). Интересно, что эта оценка линейно растет с ростом размерности.

Теорема 6. *Для множеств Делоне в $\mathbb{R}^d$ имеем: $\hat{\rho}_d \geq 2dR$.*

В связи с таким поведением нижней оценкой особенно интересно отметить, что в случае, когда во множестве Делоне X все $2R$-кластеры центрально симметричны, то согласно теореме 7, эквивалентность лишь $2R$-кластеров достаточна для того, чтобы множество X было правильной системой для любой размерности d (для доказательства см. [10, 11]).

Теорема 7. *Пусть для множества $X \subset \mathbb{R}^d$, $N(2R) = 1$ и $S_x(2R)$ содержит центральную симметрию. Тогда X — правильная система.*

Однако, если у $2R$-кластера нет центральной симметрии, то наличие у него нетривиальной группы затрудняет получение хорошей верхней оценки для радиуса регулярности $\hat{\rho}_d$ в целом.

Теорема 8 (Штогрин, Долбилин)**.** *Если для $X \subset \mathbb{R}^2$ имеем $N(4R) = 1$, то X — правильная система.*

В силу $(4R-\varepsilon)$-теоремы теорема 8 для плоскости дает неулучшаемый результат: $\hat{\rho}_2 = 4R$.

Из результатов, относящихся к радиусу регулярности для бо̀льших размерностей, отметим следующие:

при $d = 3$ имеем оценку: $6R \leq \hat{\rho}_3 \leq 10R$, нижняя следует из теоремы 7; о верхней оценке будет сказано ниже; для любого d имеем: $2dR \leq \hat{\rho}_d < c(d, r/R)R$; здесь верхняя оценка следует из теоремы 4.

$2R$-изометричные множества Делоне в $\boldsymbol{R}^3$ и оценка $\hat{\rho}_3 \leq 10R$. Были получены важные результаты для множеств Делоне в $\mathbb{R}^3$, у которых $2R$-кластеры попарно эквивалентны, где R, напомним, — параметр множества Делоне, а именно радиус наибольшего шара, не содержащего внутри ни одной точки их X. Случай $d = 3$, естественно, наиболее интересен в прикладном отношении. Множество Делоне с попарно эквивалентными $2R$-кластерами будем называть *$2R$-изометричными*. Условие $2R$-изометричности, являясь необходимым, не является, в силу оценки $\hat{\rho}_3 \geq 6R$, достаточным для того, чтобы множество X было правильной системой. Тем не менее $2R$-изометричные множества обладают рядом интересных свойств. В частности, упомянутая выше теорема 7 о $2R$-изометричных локально антиподальных множествах верна для любого d. Что касается $2R$-изометричных множеств в трехмерном пространстве, то для них в [9] установлен следующий важный факт.

Теорема 9 (М.И.Штогрин)**.** *Порядок оси поворота в группе $S_x(2R)$ симметрий $2R$-кластера в $2R$-изометричном множестве $X \subset \mathbb{R}^3$ не превышает* 6.

Мы приведем здесь доказательство более общего результата, относящегося к произвольным множествам Делоне (теорема 10), из которого немедленно следует теорема 9.

Хорошо известно, что вращение I рода в трехмерном пространстве вокруг неподвижной точки x есть поворот вокруг оси, проходящей через x. Так как в произвольном множестве Делоне X группа $S_x(2R)$, то все оси этой группы имеют конечный порядок. Для точки $x \in X$ обозначим через n_x максимальный порядок осей, входящих в группу $S_x(2R)$.

Теорема 10. *Пусть $X \subset \mathbb{R}^3$ — множество Делоне, тогда существует точка $y \in X$, для которой $n_y \leq 6$.*

Доказательство Прежде всего отметим, что мы не требуем от множества X не только $2R$-изометричности, но даже не требуем того, что множество X — конечного типа, то есть не требуем $N(2R) < \infty$.

Рассмотрим теперь для $x \in X$ кластер $C_x(2R)$ и пусть L_x – ось группы $S_x(2R)$ максимального порядка n_x для x. Вообще говоря, в группе $S_x(2R)$ может иметься несколько осей максимального порядка n_x. Для каждой из этих осей L_x существуют точки $y \in C_x(2R)$, которые не лежат на L_x. Мы выберем из них точку, находящуюся на наименьшем от центра x расстоянии, которое обозначим через r_x^*.

Так как все точки $x' \in X$, для которых $|xx'| < r_x^*$, лежат на оси L_x, то $r_x^* \leq 2R$.

Предположим противное: $n_x \geq 7$ для любой точки $x \in X$. Покажем тогда, что для выбранной точки $x \in X$ и точки $y \in C_x(2R) \setminus L_x$ с условием $|xy| = r_x^*$ расстояние r_y^* от y до ближайшей точки $z \in X$, не лежащей на оси L_y максимального порядка, удовлетворяет неравенству: $r_y^* \leq 2r_x^* \sin \pi/7 < 0.87 r_x^*$.

Действительно, орбита точки y под действием оси L_x состоит из вершин правильного n_x-угольника, $n_x \geq 7$. Его сторона равна $a := 2\bar{r}_x \sin \pi/n_x$, где $\bar{r}_x$ — расстояние от y до оси L_x, которое, заметим, равно радиусу описанной около n_x-угольника окружности. Так как $\bar{r}_x \leq r_x*$ и $n_x \geq 7$, для стороны n_x-угольника имеем: $a \leq 2r_x^* \sin \pi/7 < 0.87 r_x^*$.

Так как у вершины y n_x-угольника есть две соседние вершины z и z' на расстоянии $a < 2R$. Таким образом в $C_y(2R)$ на расстоянии a от y имеются две точки z и z', причем точки y, z, z' неколлинеарны. Поэтому из двух точек z и z' хотя бы одна, скажем z, не лежит на оси L_y максимального для y порядка n_y. Отсюда следует, что $r_y^* \leq |yz| = a$. Итак, получили, что $r_y^* < 0.87 r_x^*$. Применяя эти рассуждения к точке y и точке $u \in C_y(2R)$ с условиями $|yu| = r_y^*$ и $y \notin L_y$, аналогично получаем $r_u^* < 0.87 r_y^* < (0.87)^2 r_x^*$. Но такая бесконечно убывающая последовательность межточечных расстояний в силу r-условия невозможна во множестве Делоне. Полученное противоречие доказывает, что не для всех точек $y \in X$ $n_y \geq 7$. Теорема 10 доказана.

Теорема 9 немедленно следует из теоремы 10. В соответствии с теоремой 9 выделим из бесконечного числа конечных подгрупп группы $O(3)$ те группы, в которых порядок осей не превышают 6. Совокупность таких групп обозначим как Список L_6. Список L_6 состоит из всех осевых групп, у которых порядок осей не превосходит 6, а также полных групп правильного икосаэдра I_h и куба O_h, а также их подгрупп. В частности, среди этих групп содержится полная группа правильного тетраэдра T_h как подгруппа и группы O_h куба и группы икосаэдра I_h.

Непосредственной проверкой легко убедиться, что максимальная высота $m(G)$ башни у любой группы $G \in L_6$ не превышает 6. Отсюда по теореме 4 следует, что $\hat{\rho}_3 \leq 14R$.

Что касается оценки $\hat{\rho}_3 \leq 10R$, то хотя она была получена Штогриным и независимо Долбилиным в результате весьма трудоемкого анализа множеств Делоне с группами $2R$-кластеров $G \in L_6$, для

которых значения $m(G) \geq 5$, но соответствующие исследования в течение долгого времени оставались неопубликованнами.

Серьезное исследование $2R$-изометричных множеств Делоне, нацеленное на доказательство оценки $\hat{\rho}_3 \leq 10R$ содержится в работе автора [14]. В ней группы из Списка L_6 были распределены на четыре категории, вообще говоря, имеющие непустые пересечения:

1. Группы, содержащие центральную симметрию; для каждой такой группы G, если существует $2R$-изометричное множество Делоне X с $S_x(2R) = G$, то X — правильная система по теореме 7.
2. Группы, содержащие ось 6-го порядка; для каждой такой группы G можно показать, что если существует $2R$-изометричное множество X с $S_x(2R) = G$, то X — правильная система, более того, X — либо специальная решетка, либо специальная бирешетка. Этот результат анонсирован в [9].
3. Группы, не содержащие центральную симметрию, имеющие максимальную высоту башни 5 и 6; в эту категорию вошли, например, группы собственных вращений икосаэдра I, вращений куба O, полная группа правильного тетраэдра T_h и некоторые их подгруппы. В [14] при помощи трудоемких нетривиальных геометрических рассуждений было установлено, что если для группы G из этой категории существует $2R$-изометричное множество X, то X –правильная система.
4. Группы, не содержашие ни центральной симметрии, ни оси 6-го порядка, максимальная высота башен $m(G)$ которых не превосходит 4. Эти группы в [14] не рассматривались. В силу теоремы 4 для этих групп достаточно требовать эквивалентности $10R$-кластеров, чтобы гарантировать правильность множества X. Отметим также, что в силу работы [12] среди групп данной категории есть по крайней мере одна группа G, такая что для любого $\varepsilon > 0$ можно указать множество Делоне X с группой $S_x(2R) = G$ и условием $N(6R - \varepsilon) = 1$, которое тем не менее не является правильной системой.

Для каждой группы G из категории 4 имеем $m(G) \leq 4$. Поэтому всякое множество Делоне X с конгруэнтными $10R$-кластерами и с $S_x(2R) = G$, если такое существует, является правильной системой в силу теоремы 4.

С другой стороны, для каждой группы G из категорий 1–3 установлено, что если $2R$-изометричное множество X с группой $S_x(2R) = G$ существует, то оно является правильной системой.

Из вышесказанного следует верхняя оценка $\hat{\rho}_3 \leq 10R$. Однако здесь нужно отметить, что в работе [14] группа D_{4d} (это — груп-

па квадратной антипризмы) была из-за неаккуратности включена в категорию 1, как якобы содержащая центральную симметрию, вместо категории 3, как группа с максимальной высотой башни $m = 5$. Поэтому она не получила в [14] должного рассмотрения. Пробел относительно группы D_{4d}, на который указал мне А. Гарбер, был восполнен двумя разными способами в [15, 16]. Тем самым установление оценки $\hat{\rho}_3 \leq 10R$ можно считать завершенным.

В заключение сформулируем две проблемы.

1. «Приблизить» друг к другу верхнюю и нижнюю оценки для $\hat{\rho}_3$, в частности, улучшить верхнюю оценку $\hat{\rho}_3 \leq 8R$.
2. Сформулировать локальные условия для множеств Мейера (Meyer Sets). *Множество Мейера* — это множество Делоне X для которого разность Минковского $X - X$ является также множеством Делоне. Решетка, правильная система, мультиправильная система яаляются множествами Мейера. В то же время класс множеств Мейера значительно у́же класса множеств Делоне, у́же даже класса множеств Делоне конечного типа. Для нас класс множеств Мейера важен тем, что он содержит не только кристаллы, но и квазикристаллы, т. е. множества, полученные из решеток методом сечений и проекций (the cut-and-projection method). Так что решение залачи для множеств Мейера означало бы построение общей локальной теории для квазикристаллов.

Список литературы

1. Федоров Е. С. Начала учения о фигурах. — С.-Петербург, 1985.
2. Schoefliess A. Kristallsysteme und Kristallstruktur — Leipzig, 1981.
3. Bieberbach L. Üeber die Bewegungsgruppen des n-dimensionalen Euklidischen Räumes // Math. Ann. — I: 1911. — 70. — P. 207–336. II: 1912 — 72. — P. 400–412.
4. Проблемы Гильберта, Сб. под ред. П.С.Александрова. — Наука, 1969.
5. Delaunay B. Sur la sphere vide. A la memoire de Georges Voronoi // Известия Академии наук СССР. VII серия. Отделение математических и естественных наук — 1934. — № 6. — С. 793–800.
6. Делоне Б. Н. Геометрия положительных квадратичных форм // УМН. — 1937. — № 3. — С. 16–62.
7. Делоне Б. Н. , Долбилин Н. П., Штогрин М. И., Галиулин Р. В. Локальный критерий правильности системы точек // Докл. АН СССР. — 1976. — 227:1. — С. 19–21.
8. Долбилин Н. П., Штогрин М. И Локальный критерий для кристаллических структур // Тезисы IX Всесоюзной Геометрической

Конференции. — Кишинев, 1988.

9. Штогрин М. Об ограничении порядка оси паучка в локально правильной системе Делоне // Geometry, Topology, Algebra and Number Theory, Applications, The International Conference dedicated to the 120-th anniversary of Boris Nikolaevich Delone (1890-1980) (Moscow, August 16-20, 2010), Abstracts. — 2010. — С. 168–169.

10. Долбилин Н. П. Критерий кристалла и локально антиподальные множества Делоне // Тр. Международной конференции «Квантовая топология», Вестник ЧелГу — 2015. — №3 (358) — С. 6–17.

11. Долбилин Н. П., Магазинов А. Н. Локально антиподальные множества Делоне // УМН. — 2015. — 70:5 (425). — С. 179–180.

12. Dolbilin N. P. Delone Sets: Local Identity and Global Order // Discrete Geometry and Symmetry — 2018. — 234. — P. 616–629.

13. Baburin I. A., Bouniaev M. M., Dolbilin N. P., Erokhovets N. Yu., Garber A. I., Krivovichev S. V., Schulte E. On the Origin of Crystallinity: on a Lower Bound for the Regularity Radius for Delone Sets // Acta Crystallogr, Sect A. — 2018. —74:6. — P. 616–629.

14. Долбилин Н. П. Множества Делоне в $\mathbb{R}^3$ с $2R$-условиями регулярности // Топология и физика. Сб. статей. К 80-летию со дня рождения академика Сергея Петровича Новикова. Тр.МИАН. — 2018. — 302. — С. 176–201.

15. Dolbilin N. P., Garber A. I., Leopold U., Schulte E. (in preparation).

16. Dolbilin N. P. On Delone $2R$-isometric sets with the group $S_x(2R) = D_{4d}$ (in preparation).

О СЛОЖНОСТИ РЕАЛИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ С МАЛЫМ ЧИСЛОМ ЕДИНИЦ

Н. П. Редькин (Москва)

Рассматривается задача реализации булевых функций из некоторого узкого класса схемами из функциональных элементов в базисах $B_1 = \{x\&y, \bar{x}\}$ и $B_2 = \{x \vee y, \bar{x}\}$ [1]. Обозначим через $F(n,k)$ класс булевых функций, состоящий из всех тех функций от n переменных, каждая из которых обращается в единицу ровно на k наборах значений переменных. Если параметр k удовлетворяет условию $1 \le k \le \log n - c \log\log n$, где c — большая единицы константа, а «log» означает логарифм по основанию 2, то функции из $F(n,k)$ условимся считать функциями с малым числом единиц. Именно такие функции рассматриваются в данной работе.

Заметим, что в работе [2] установлена возможность реализации любой булевой функции с малым числом единиц схемой из функциональных элементов в любом конечном функционально полном базисе (и даже формулой над $\{x\&y, x \vee y, \bar{x}\}$), сложность которой по порядку не превосходит n. В [3] найдена асимптотика (при растущем n) для сложности реализации любой булевой функции с малым числом единиц в случае, когда схемы строятся в базисе, содержащем все булевы функции от двух переменных, кроме линейных функций $x \oplus y, x \oplus y \oplus 1$ (знак $\oplus$ означает сложение по модулю два), а сложность всякой схемы оценивается числом функциональных элементов в ней.

Для формулировки результатов данной работы напомним некоторые определения из [1] и [3]. Пусть B — некоторый базис, а S — произвольная схема из функциональных элементов в B; здесь B — некоторое множество $\{g_1, \ldots, g_r\}$ булевых функций или функциональных элементов $\{E_1, \ldots, E_r\}$, реализующих соответственно функции $g_1, \ldots, g_r$. Каждому элементу E_i базиса приписано неотрицательное число p_i — вес этого элемента ($i = 1, \ldots, r$). Сложность схемы S — это сумма весов всех элементов, составляющих данную схему; обозначаем сложность схемы S через $L_B(S)$. Пусть f — произвольная булева функция, а $L(f) = \min L_B(S)$, где минимум берется по всем схемам в базисе B, реализующим f; число $L_B(f)$ считается сложностью (реализации) функции f схемами в базисе B. Схема S, реализующая функцию f, считается минимальной, если $L_B(S) = L_B(f)$. Для класса $F(n,k)$ обычным образом вводится функция Шеннона $L_B(F(n,k)) = \max L_B(f)$, где максимум берется по всем функциям из $F(n,k)$.

Пусть $f(x_1, \ldots, x_n)$ — какая-нибудь функция из $F(n,k)$, обращающаяся в единицу на k булевых наборах $\tilde{a}_1, \ldots, \tilde{a}_k$ (значений переменных), где $\tilde{a}_i = (a_{i,1}, \ldots, a_{i,n})$, $i = 1, \ldots, k$, а $a_{i,j} \in \{0,1\}, j = 1, \ldots, n$. Функцию f зададим матрицей M_f, строками которой являются наборы $\tilde{a}_1, \ldots, \tilde{a}_k$; j-й столбец этой матрицы отвечает переменной x_j, $j = 1, \ldots, n$. Столбцы матрицы M_f разобьем на группы одинаковых между собой столбцов. Для произвольного столбца $\tilde{b}$ высоты k через $M_{\tilde{b}}$ обозначим группу столбцов (составляющих подматрицу матрицы M_f) равных $\tilde{b}$. Для каких-то $\tilde{b}$ группы $M_{\tilde{b}}$ могут оказаться пустыми (но не для всех одновременно). Группу столбцов $M_{\tilde{b}}$ назовем сильной, если она содержит не менее двух столбцов $\tilde{b}$ и в этих столбцах имеются как нули, так и единицы; переменные, отвечающие столбцам из сильной группы, также будем называть сильными. Все остальные непустые группы и не являющиеся сильными переменные будем называть слабыми. Группы слабых переменных, содержащие не менее чем по две переменные, и сами эти переменные будем считать невырожденными; таким группам отвечают подматрицы либо из одних нулей, либо из одних единиц, а каждая из этих подматриц содержит не менее двух столбцов. Остальные группы, содержащие ровно по одной слабой переменной, и сами переменные, отвечающие таким группам, будем считать вырожденными. Число сильных переменных функций f обозначим через $m(f)$ или просто через m, если известно, о какой функции идет речь. Число слабых невырожденных «нулевых» переменных, которым отвечает подматрица из одних нулей, обозначим через $m_0(f)$ (или просто m_0); соответственно через $m_1(f)$ (или m_1) обозначим число слабых невырожденных «единичных» переменных, которым отвечают подматрицы из одних единиц. Каждой функции f из $F(n,k)$ отвечают свои параметры m, m_0, m_1.

В работе [3] рассматривались схемы в базисе $B = P_2^{(2)} \setminus \{x_1 \oplus x_2, x_1 \oplus x_2 \oplus 1\}$, где $P_2^{(2)}$ — множество всех булевых функций от двух переменных. Вес каждого элемента базиса B предполагался равным 1, т.е. сложность схем оценивалась числом функциональных элементов в них. Было установлено, что если класс $F(n,k)$ состоит из булевых функций с малым числом единиц, то для любой функции f из $F(n,k)$ выполняется асимптотика (при растущем n) $L_B(f) \sim n+m(f)$, из которой следует (при $m = n$) асимптотика $L_B\big(F(n,k)\big) \sim 2n$.

В данной работе изучаются более простые базисы $B_1 = \{x\&y, \bar{x}\}$ и $B_2 = \{x \vee y, \bar{x}\}$; предполагается, что в каждом из базисов B_1, B_2

вес инвертора равен p_1, а вес двухвходового элемента (как конъюнктора, так и дизъюнктора) равен p_2, где p_1, p_2 — любые (фиксированные) строго положительные числа. Пусть $F(n,k,m_0,m_1)$ — подмножество булевых функций из $F(n,k)$ такое, что каждая функция из $F(n,k,m_0,m_1)$ имеет m_0 слабых невырожденных нулевых переменных и m_1 слабых невырожденных единичных переменных. Установлены следующие асимптотики, в которых предполагается $n \to \infty$, а каждому n отвечают свои параметры k, m_0, m_1.

Теорема 1. *Для подкласса $F(n,k,m_0,m_1)$ функций с малым числом единиц выполняются асимптотики*

$L_{B_1}(f) \sim (p_1+2p_2)n - p_2(m_0+m_1) - p_1 m_1$,

$L_{B_2}(f) \sim (p_1+2p_2)n - p_2(m_0+m_1) - p_1 m_0$.

Теорема 2. *Если класс $F(n,k)$ состоит из булевых функций с малым числом единиц и $k \geq 2$, то*

$L_{B_1}\big(F(n,k)\big) \sim L_{B_2}\big(F(n,k)\big) \sim (p_1+2p_2)n$.

Заметим, что утверждение теоремы 2 следует из теоремы 1 при $m_0 = m_1 = 0$.

Из приведенных результатов видно, что если сложность схем оценивать числом функциональных элементов в них, то при переходе от базиса $B = P_2^{(2)} \setminus \{x_1 \oplus x_2, x_1 \oplus x_2 \oplus 1\}$ к базисам B_1 и B_2 функция Шеннона увеличивается асимптотически в полтора раза. Например, для самой сложнореализуемой (асимптотически) фукнции $f(x_1,\ldots,x_n) = x_1 \ldots x_n \vee \bar{x}_1 \ldots \bar{x}_n$ из $F_{n,2}$ получаем $L_B(f) \sim 2n$, а $L_{B_1}(f) \sim 3n$ и $L_{B_2}(f) \sim 3n$.

Оценим теперь инверсионную сложность функций с малым числом единиц. Будем рассматривать схемы из функциональных элементов в базисе B_i, $i \in \{1,2\}$, и оценивать сложность схем числом инверторов в них. Для схемы S в базисе B_i через $L^-_{B_i}(S)$ обозначим число инверторов в ней. Положим $L^-_{B_i}(f) = \min L_{B_i}(S)$, где минимум берется по всем схемам в базисе B_i, реализующим f.

Теорема 3. *Для подкласса $F(n,k,m_0,m_1)$ функций с малым числом единиц с малым числом единиц выполняются следующие оценки для инверсионной сложности этой функции:*

$n - m_1 - 2^k \leq L^-_{B_1}(F(n,k,m_0,m_1)) \leq n - m_1 + 5 \cdot 2^k$,

$n - m_0 - 2^k \leq L^-_{B_2}(F(n,k,m_0,m_1)) \leq n - m_0 + 4 \cdot 2^k + 5$.

И в заключение приведем оценки для конъюнкторной и дизъюнкторной сложностей функций с малым числом единиц. Для схемы S в базисе B_1 через $L^{\&}_{B_1}(S)$ обозначим число конъюнкторов в ней и положим $L^{\&}_{B_1}(f) = \min L^{\&}_{B_1}(S)$, где минимум берется по всем схе-

мам в базисе B_1, реализующим f. Аналогичным образом определим дизъюнкторную сложность $L^{\vee}_{B_2}(f)$ функции f для базиса B_2. Для функций Шеннона $L^{\&}_{B_1}(f)$ и $L^{\vee}_{B_2}(f)$ получены такие оценки.

Теорема 4. *Если булева функция с малым числом единиц содержится в $F(n,k,m_0,m_1)$, то выполняются следующие оценки для конъюнкторной и дизъюнкторной сложностей этой функции:*

$$L^{\&}_{B_1}(f) \sim \begin{cases} n \text{ при } k=1, \\ 2n-m_0-m_1 \text{ при } k \geq 2. \end{cases}$$

$$L^{\vee}_{B_2}(f) \sim \begin{cases} n \text{ при } k=1, \\ 2n-m_0-m_1 \text{ при } k \geq 2. \end{cases}$$

Заметим, что полученные оценки для инверсионной, конъюнкторной и дизъюнкторной сложностей функций с малым числом единиц используются при доказательстве основной теоремы 1.

Работа выполнена при финансовой поддержке РФФИ, проект № 18-01-00337.

Список литературы

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

2. 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.

3. Редькин Н. П. О сложности булевых функций с малым числом единиц // Дискретная математика. — 2004. — Т. 16, № 4. — С. 20–31.

КОНЪЮНКТИВНЫЕ ФОРМЫ ДЛЯ ПРЕДИКАТОВ НА КОНЕЧНЫХ МНОЖЕСТВАХ, ИХ СВОЙСТВА И НЕКОТОРЫЕ ПРИМЕНЕНИЯ

С. Н. Селезнева (Москва)

В работе рассматривается представление предикатов на конечных множествах в виде обобщенных конъюнктивных нормальных форм (ОКНФ), которое обобщает конъюнктивные нормальные формы (КНФ) функций алгебры логики. Для этого представления доказываются свойства, обобщающие соответствующие свойства КНФ. В частности, вводится понятие сокращенной ОКНФ предиката на конечном множестве; показано, как по сокращенной ОКНФ предиката g, $g \neq 0$, быстро найти набор, на котором g обращается в единицу, и быстро получить сокращенную ОКНФ проекции g на любое множество переменных. Найдены виды сокращенных ОКНФ предикатов, инвариантных относительно некоторой функции почти единогласия или некоторой полурешеточной функции. Показано, как на основе этих видов ОКНФ можно быстро решать задачи обобщенной S-выполнимости в тех случаях, когда все предикаты из множества S инвариантны относительно некоторой функции почти единогласия или некоторой полурешеточной функции (см. [1–3]).

1. *Конъюнктивные формы для предикатов.* Пусть k — целое число, $k \geqslant 2$, $E_k = \{0, 1, \ldots, k-1\}$, $R_k^{(n)} = \{g \mid g : E_k^n \to E_2\}$ — множество n-местных предикатов ($n \geqslant 0$) и $R_k = \bigcup\limits_{n=0}^{\infty} R_k^{(n)}$ — множество всех предикатов на E_k. Если $g, h \in R_k$, то $\bar{g}$, $g\&h$, $g \vee h$ означают отрицание, конъюнкцию и дизъюнкцию соответствующих предикатов. Как правило, знак $\&$ будем заменять на $\cdot$ или вообще пропускать. Если $g \in R_k^{(n)}$, то для $a \in E_2$ положим $N_a(g) = \{\alpha \in E_k^n \mid g(\alpha) = a\}$, соответственно множества нулей и единиц предиката g.

Пусть на множестве E_k задан частичный порядок $\leqslant$, в котором любые два элемента $a, b \in E_k$ имеют единственную точную верхнюю грань $\sqcap(a, b)$. При этом в частично упорядоченном множестве $(E_k; \leqslant)$ найдется наибольший элемент, т. е. такой элемент, что все другие меньше него. Минимальными элементами частично упорядоченного множества $(E_k; \leqslant)$ являются все такие элементы, для каждого из которых не найдется ни одного другого элемента, меньшего него. Как обычно, если для элементов $a, b \in E_k$ верно $a \leqslant b$, $a \neq b$, то будем писать $a < b$, т. е. элемент a строго предшествует элементу b. Если $a < b$ и не найдется такого $c \in E_k$, что $a < c < b$, то будем записывать $a \lessdot b$, т. е. элемент a

непосредственно предшествует элементу b (или элемент b непосредственно следует за элементом a). Для элемента $a \in E_k$ введем $\check{S}(a) = \{b \in E_k \mid b \lessdot a\}$ и $\hat{S}(a) = \{b \in E_k \mid a \lessdot b\}$, соответственно множества непосредственно предшествующих ему и непосредственно следующих за ним элементов. Для элементов $a_1, \ldots, a_m \in E_k$ определим их точную верхнюю грань $\sqcap(a_1, \ldots, a_m)$ и точную нижнюю грань $\sqcup(a_1, \ldots, a_m)$, $m \geqslant 1$. Точная верхняя грань $\sqcap(a_1, \ldots, a_m)$: $\sqcap(a_1) = \sqcap(a_1, a_1)$, $\sqcap(a_1, \ldots, a_m) = \sqcap(\sqcap(a_1, \ldots, a_{m-1}), a_m), m \geqslant 3$. Точная нижняя грань $\sqcup(a_1, \ldots, a_m)$: $\sqcup(a_1, \ldots, a_m) = \sqcap\{b \in E_k \mid b \leqslant a_1, \ldots, b \leqslant a_m\}$, если справа получается пустое множество, то считаем, что $\sqcup(a_1, \ldots, a_m) = -1$, где $-1 \notin E_k$. Отметим, что $\sqcup(a_1, a_2, \ldots, a_m) \leqslant a_i$ для каждого a_i, $i = 1, \ldots, m$. Введем обозначения: $\hat{a} = \sqcap(E_k)$, $\check{a} = \sqcup(E_k)$. Отметим, что всегда $\hat{a} \in E_k$, это наибольший элемент частично упорядоченного множества $(E_k; \leqslant)$. Если $\check{a} \in E_k$ (т. е. $\check{a} \neq -1$), то в частично упорядоченном множестве $(E_k; \leqslant)$ существует наименьший элемент.

Теперь относительно частичного порядка $\leqslant$ определим одноместные ступенчатые предикаты $s_a(x), \bar{s}_a(x) \in R_k$ при $a \in E_k$, где $s_a(x) = 0$ при $x \leqslant a$ и $s_a(x) = 1$ иначе (см. [1–3]). Отметим, что $s_{\hat{a}}(x) = 0$. Иногда будем рассматривать ступенчатый предикат $\bar{s}_{-1}(x)$, выражающий константу 0, т. е. полагаем, что $-1 \leqslant a$ при $a \in E_k$. Назовем ступенчатые предикаты $s_a(x)$ при $a \neq \hat{a}$ — положительными, $\bar{s}_a(x)$ при $a \neq -1$ — отрицательными.

Утверждение 1.1 [2]. *Для любых* $a, a_1, a_2 \in E_k$, $b, b_1, b_2 \in E_k \cup \{-1\}$ *верны следующие свойства*:
1) $s_{a_1}(x) \vee s_{a_2}(x) = s_{a_1}(x)$, *если* $a_1 \leqslant a_2$;
2) $s_{a_1}(x) \vee s_{a_2}(x) = s_{\sqcup(a_1,a_2)}(x)$, *если* a_1 *и* a_2 *— не сравнимы*;
3) $\bar{s}_{b_1}(x) \vee \bar{s}_{b_2}(x) = \bar{s}_{b_2}(x)$, *если* $b_1 \leqslant b_2$;
4) $s_a(x) \vee \bar{s}_b(x) = 1$, *если* $a \leqslant b$;
5) $s_a(x) \vee \bar{s}_b(x) = s_a(x) \vee \bar{s}_{\sqcup(a,b)}(x)$, *если* a *и* b *— не сравнимы.*

Введем обозначение $s_a^\sigma(x)$, где $\sigma \in E_2$: $s_a^\sigma(x) = s_a(x)$ при $\sigma = 1$ и $s_a^\sigma(x) = \bar{s}_a(x)$ при $\sigma = 0$. Выражение $s_a^\sigma(x)$ назовем литералом (переменной x). Выражение вида $s_a(x) \vee \bar{s}_{b_1}(x) \vee \ldots \vee \bar{s}_{b_m}(x)$, где $a \in E_k$, $b_1, \ldots, b_m \in E_k \cup \{-1\}$, $b_1, \ldots, b_m < a$ и $b_1, \ldots, b_m$ — не сравнимы, назовем псевдолитералом (переменной x). Если в псевдолитерале выполняется $a = \hat{a}$, $b_1 = -1$, то он равен константе 0. Отметим, что любую дизъюнкцию литералов одной и той же переменной можно привести к какому-то псевдолитералу или к константе 1 применением свойств из утверждения 1.1. Примем, что любое выражение, явля-

ющееся дизъюнкцией литералов одной и той же переменной, всегда приведено к соответствующему псевдолитералу или к константе 1. Если $L_1(x)$, $L_2(x)$ — псевдолитералы, то L_1 назовем сужением L_2, если $N_0(L_2) \subseteq N_0(L_1)$. Отметим, что константа 0 является сужением любого литерала.

Обобщенной элементарной дизъюнкцией (ОЭД) ранга r при $r \geqslant 1$ назовем выражение вида $L_1(x_{i_1}) \vee \ldots \vee L_r(x_{i_r})$, где $L_1, \ldots, L_r$ — псевдолитералы, не равные константе 0, и $x_{i_1}, \ldots, x_{i_r}$ — различные переменные. Обобщенной элементарной дизъюнкцией ранга 0 назовем константу 0. При этом полагаем, что эта ОЭД содержит только псевдолитерал 0 (произвольной переменной). Считаем две ОЭД равными, если они отличаются только порядком псевдолитералов и порядком литералов в псевдолитералах. Отметим, что любую дизъюнкцию ступенчатых предикатов можно привести к некоторой ОЭД или к константе 1 применением свойств из утверждения 1.1. Примем, что любое выражение, являющееся дизъюнкцией литералов, всегда приведено к соответствующей ОЭД или к константе 1. Если D_1, D_2 — ОЭД, то D_1 называется сужением D_2, если $N_0(D_2) \subseteq N_0(D_1)$. Если ОЭД D_1 — сужение ОЭД D_2, то D_2 назовем расширением D_1. Сужение (или расширение) называется собственным, если ОЭД при этом не совпадают. Отметим, что если D_1 — сужение D_2, то для любого $\alpha \in E_k^n$ из $D_2(\alpha) = 0$ следует $D_1(\alpha) = 0$.

Обобщенной конъюнктивной нормальной формой (ОКНФ) длины l, $l \geqslant 1$, назовем конъюнкцию l различных ОЭД. Обобщенной конъюнктивной нормальной формой длины 0 назовем константу 1. Для любых ОЭД D_1, D_2 из $N_0(D_2) \subseteq N_0(D_1)$ следует $D_1 \cdot D_2 = D_1$ (правило поглощения). Примем, что в любой ОКНФ выполнены все возможные поглощения.

Каждая ОКНФ определяет некоторый предикат $g \in R_k$. Верно и обратное утверждение: каждый предикат $g \in R_k$ может быть представлен некоторой ОКНФ.

Утверждение 1.2 [1, 2]. *Если* $g(x_1, \ldots, x_n) \in R_k$, $g \neq 1$, *то*

$$g(x_1, \ldots, x_n) = \prod_{\substack{\alpha \in E_k^n : \\ g(\alpha) = 0}} \left(\bigvee_{i=1}^{n} \left(s_{\alpha(i)}(x_i) \vee \bigvee_{b \in \check{S}(\alpha(i))} \bar{s}_b(x_i) \right) \right).$$

Здесь и далее $\alpha(i)$ обозначает значение i-й координаты в наборе $\alpha \in E_k^n$.

Назовем имплицентой предиката $g \in R_k^{(n)}$ такую ОЭД D, что для

любого набора $\alpha \in E_k^n$ из $D(\alpha) = 0$ следует $g(\alpha) = 0$. Если к тому же никакое собственное сужение D' имплиценты D не является имплицентой предиката g, то ОЭД D называется простой имплицентой предиката g. Конъюнкция K_g всех простых имплицент предиката $g \in R_k$, $g \neq 1$, является ОКНФ, представляющей предикат g, и называется его сокращенной ОКНФ. Сокращенной ОКНФ предиката, равного константе 1, назовем константу 1. Для каждого предиката $g \in R_k$ его сокращенная ОКНФ K_g единственна и представляет этот предикат g [1, 2].

Утверждение 1.3 [2]. *Если ОЭД $D_1 = L_1(x) \vee D_1'$ и $D_2 = L_2(x) \vee D_2'$ являются имплицентами предиката $g \in R_k$, где $L_1(x), L_2(x)$ — псевдолитералы, а ОЭД D_1', D_2' не содержат переменную x, то для каждого такого псевдолитерала $L(x)$, что $N_0(L) \subseteq N_0(L_1 \cdot L_2)$, ОЭД $D = L(x) \vee D_1' \vee D_2'$ также является имплицентой предиката g.*

Для ОЭД $D_1 = L_1(x) \vee D_1'$ и $D_2 = L_2(x) \vee D_2'$, где $L_1(x), L_2(x)$ — псевдолитералы, а ОЭД D_1', D_2' не содержат переменную x, и каждого такого псевдолитерала $L(x)$, что $N_0(L) \subseteq N_0(L_1 \cdot L_2)$, ОЭД $D = L(x) \vee D_1' \vee D_2'$ назовем их (обобщенной) резольвентой. При этом скажем, что она получена применением правила обобщенной резолюции (по переменной x).

Если $\leqslant$ — линейный порядок на E_k, то можно указать явный вид обобщенной резольвенты двух ОЭД. Для ОЭД $D_1 = s_{a_1}(x) \vee \bar{s}_{b_1}(x) \vee D_1'$ и $D_2 = s_{a_2}(x) \vee \bar{s}_{b_2}(x) \vee D_2'$, где $b_2 \leqslant b_1 \leqslant a_2 \leqslant a_1$, а ОЭД D_1', D_2' не содержат переменную x, ОЭД $D = s_{a_1}(x) \vee \bar{s}_{b_2}(x) \vee D_1' \vee D_2'$ называется их (обобщенной) резольвентой.

Теорема 1.1 [1, 2]. *Если для каждой пары ОЭД D_1, D_2, входящих в ОКНФ K предиката $g \in R_k$, для любой их обобщенной резольвенты D в ОКНФ K найдется какое-то сужение D' этой резольвенты D, то ОКНФ K является сокращенной ОКНФ предиката g.*

Из теоремы 1.1 следует, что для любого предиката $g \in R_k$ его сокращенную ОКНФ K_g можно построить из его произвольной ОКНФ K, последовательно добавляя обобщенные резольвенты пар ОЭД из текущей ОКНФ, которые не поглощаются ни одной ее ОЭД, (и выполняя возможные поглощения) до тех пор, пока никакой новой ОЭД нельзя будет добавить.

2. *Свойства конъюнктивных форм.* В теории баз данных рассматриваются понятия t-согласованности и полной согласованности системы предикатов. В [4, 5] рассматривались алгоритмы приведения системы предикатов S к t-согласованной системе предикатов S' с сохранением множества наборов, на которых истинны все преди-

каты каждой из систем. Подобным образом определим понятия согласованности для ОКНФ. Скажем, что набор $\alpha \in E_k^t$ переменных $x_{i_1}, \ldots, x_{i_t}$, $t \geqslant 0$, не обнуляет ОЭД D, если подстановка в ОЭД D вместо каждой переменной x_{i_j} значения $\alpha(j)$, $j = 1, \ldots, t$, не приводит к ОЭД, равной константе 0. Например, набор $\alpha = (0,1) \in E_5^2$ переменных x_1, x_3 не обнуляет ОЭД $D_1 = s_1(x_1) \vee \bar{s}_3(x_2)$ и обнуляет ОЭД $D_2 = s_2(x_3)$. Считаем, что пустой набор (т.е. при $t = 0$) обнуляет только ОЭД, являющуюся константой 0. ОКНФ $K(x_1, \ldots, x_n)$ называется $(t+1)$-согласованной, если для любого набора $\alpha \in E_k^t$ переменных $x_{i_1}, \ldots, x_{i_t}$, не обнуляющего ни одну ОЭД в ОКНФ K, и для любой переменной $x_{i_{t+1}}$, не совпадающей ни с одной из переменных $x_{i_1}, \ldots, x_{i_t}$, можно подобрать такое $b \in E_k$, что набор $\beta = (\alpha(1), \ldots, \alpha(t), b) \in E_k^{t+1}$ переменных $x_{i_1}, \ldots, x_{i_t}, x_{i_{t+1}}$ не обнуляет ни одну ОЭД в ОКНФ K. ОКНФ K называется полностью согласованной, если она t-согласована для любого $t \geqslant 1$. Например, рассмотрим КНФ (при $k = 2$): $K_1 = (x_1 \vee x_2)(x_1 \vee \bar{x}_3 \vee \bar{x}_4)(\bar{x}_1 \vee x_3)(\bar{x}_2 \vee \bar{x}_4)$. Она не является 3-согласованной, т.к. при $x_2 = x_3 = 0$ получаем $(x_1 \vee 0)(x_1 \vee 1 \vee \bar{x}_4)(\bar{x}_1 \vee 0)(1 \vee \bar{x}_4) = 0$.

Теорема 2.1 [1, 2]**.** *Пусть $k \geqslant 2$. Для каждого предиката $g \in R_k$ его сокращенная ОКНФ K_g является полностью согласованной.*

Например, рассмотрим сокращенную КНФ (при $k = 2$): $K_2 = (\bar{x}_1 \vee \bar{x}_2)(x_1 \vee \bar{x}_3 \vee x_4)(\bar{x}_2 \vee \bar{x}_3 \vee x_4)$. Тогда при $x_1 = 0$ получаем $\bar{x}_3 \vee x_4$, далее можно положить $x_3 = 1$ и $x_4 = 1$. В итоге, находим $K_2(0, -, 1, 1) = 1$.

Если $g(x_1, \ldots, x_n) \in R_k$ и x_i — переменная, то положим $\exists x_i g = \bigvee\limits_{a \in E_k} g(x_1, \ldots, x_{i-1}, a, x_{i+1}, \ldots, x_n)$ при $1 \leqslant i \leqslant n$ и $\exists x_i g = g$ иначе. Далее, при $m \geqslant 2$ по индукции примем $\exists x_{i_1}, x_{i_2}, \ldots, x_{i_m} g = \exists x_{i_1} \exists x_{i_2}, \ldots, x_{i_m} g$. Предикат $\exists x_1, \ldots, x_m g$ называется проекцией предиката g на переменные $x_{m+1}, \ldots, x_n$ (или по переменным $x_1, \ldots, x_m$). Проекцию предиката $g(x_1, \ldots, x_n)$ на произвольные переменные $x_{i_1}, \ldots, x_{i_t}$, где $t \geqslant 1$, определяем аналогично. Проекция предиката $g(x_1, \ldots, x_n)$ на переменные $x_{i_1}, \ldots, x_{i_t}$ обозначается через $\pi_{\{x_{i_1}, \ldots, x_{i_t}\}}(g)$. Положим $\pi_{\{\emptyset\}}(g) = g$.

Теорема 2.2 [1, 2]**.** *Пусть $k \geqslant 2$. Для любого предиката $g(x_1, \ldots, x_n) \in R_k$ и для любых переменных $x_{i_1}, \ldots, x_{i_t}$, $t \geqslant 0$, конъюнкция всех простых имплицент предиката g, содержащих только переменные из множества $\{x_{i_1}, \ldots, x_{i_t}\}$, является сокращенной ОКНФ предиката $\pi_{\{x_{i_1}, \ldots, x_{i_t}\}}(g)$.*

Например, рассмотрим сокращенную КНФ (при $k = 2$) для $g \in R_2$: $K_g = (\bar{x}_1 \vee \bar{x}_2)(x_1 \vee \bar{x}_3 \vee x_4)(\bar{x}_2 \vee \bar{x}_3 \vee x_4)$. Тогда $\pi_{\{x_1\}}(g) = 1$, $\pi_{\{x_1,x_2\}}(g) = \bar{x}_1 \vee \bar{x}_2$.

3. *Задача обобщенной выполнимости.* Пусть $S \subseteq R_k$ и S — конечное множество. Рассмотрим задачу обобщенной S-выполнимости *S-ВЫП*. Она называется также задачей удовлетворения ограничениям CSP(S) (от англ. constraint satisfaction problem). *Задача S-ВЫП*, где $S \subseteq R_k$, $k \geqslant 2$, и S — конечно. *Вход*: предикат $g(x_1, \ldots, x_n) = \prod\limits_{j=1}^{l} g_j(x_{j_1}, \ldots, x_{j_{n_j}}) \in R_k$, где $g_j \in S$, $1 \leqslant j_1, \ldots, j_{n_j} \leqslant n$, $j = 1, \ldots, l$. *Вопрос*: является ли предикат g выполнимым, т. е. найдется ли такой набор $\alpha \in E_k^n$, что $g(\alpha) = 1$? Длиной входа $g(x_1, \ldots, x_n) = \prod\limits_{j=1}^{l} g_j(x_{j_1}, \ldots, x_{j_{n_j}}) \in R_k$, где $g_j \in S$, $1 \leqslant j_1, \ldots, j_{n_j} \leqslant n$, $j = 1, \ldots, l$, задачи *S-ВЫП* назовем величину $l(g) = \sum\limits_{j=1}^{l} n_j \cdot (\log_k n + |N_1(g_j)|)$, т. е. длину строки, представляющей собой номера переменных каждого предиката g_j, записанные в k-ичной системе счисления, и все наборы, на которых предикат g_j истинен.

Полная классификация вычислительной сложности задачи *S-ВЫП* получена Т. Шефером при $k = 2$ [6] и А. А. Булатовым при $k = 3$ [7]. В 1997–2017 г. г. было опубликовано множество работ, в которых исследовалась вычислительная сложность этой задачи при произвольных конечных [8–15]. В 2017 г. как итог ряда работ найдена полная классификация вычислительной сложности этой задачи при каждом конечном k (см. [13–15] и ссылки в них). Оказалось, что удобным средством исследования задачи *S-ВЫП* является алгебраический подход [8, 11], состоящий в том, чтобы рассматривать функции, сохраняющие все предикаты из множества S.

Напомним некоторые определения (см., например, [16]). Пусть $P_k^{(n)} = \{f \mid f : E_k^n \to E_k\}$ — множество n-местных ($n \geqslant 0$) и $P_k = \bigcup\limits_{n=0}^{\infty} P_k^{(n)}$ — множество всех функций над E_k. Функция $f \in P_k^{(m)}$ сохраняет предикат $g \in R_k^{(n)}$, если для любых наборов $\alpha_1, \ldots, \alpha_m \in E_k^n$ из $\alpha_1, \ldots, \alpha_m \in N_1(g)$ следует $(f(\alpha_1(1), \ldots, \alpha_m(1)), \ldots, f(\alpha_1(n), \ldots, \alpha_m(n))) \in N_1(g)$. Если функция $f \in P_k$ сохраняет предикат $g \in R_k$, то функция f называется полиморфизмом предиката g, а предикат g называется инвариантным

относительно функции f. Если $g \in R_k$, то множество всех полиморфизмов предиката g обозначается через $\mathrm{Pol}(g)$. Если $S \subseteq R_k$, то $\mathrm{Pol}(S) = \bigcap\limits_{g \in S} \mathrm{Pol}(g)$. Для любого $S \subseteq R_k$ множество $\mathrm{Pol}(S)$ является замкнутым классом функций и $x \in \mathrm{Pol}(S)$. Если $f \in P_k$, то множество всех предикатов, инвариантных относительно функции f, обозначается через $\mathrm{Inv}(f)$. Если $A \subseteq P_k$, то $\mathrm{Inv}(A) = \bigcap\limits_{f \in A} \mathrm{Inv}(f)$. Для любого $A \subseteq P_k$ множество $\mathrm{Inv}(A)$ является замкнутым классом предикатов и $0 \in \mathrm{Inv}(A)$.

Функция $f \in P_k^{(m)}$, где $m \geqslant 2$, называется слабой функцией почти единогласия, если $f(x, \ldots, x) = x$ и $f(y, x, \ldots, x) = f(x, y, x, \ldots, x) = \ldots = f(x, \ldots, x, y)$. В [13–15] показано, что полиномиальность или NP-полнота задачи обобщенной S-выполнимости зависит только от наличия в множестве $\mathrm{Pol}(S)$ слабой функции почти единогласия.

Рассмотрим частные случаи слабой функции почти единогласия: функцию почти единогласия и полурешеточную функцию. Функция $f \in P_k^{(m+1)}$, где $m \geqslant 2$, называется функцией почти единогласия, если $f(y, x, \ldots, x) = f(x, y, x, \ldots, x) = \ldots = f(x, \ldots, x, y) = x$. При $k = 2$ медиана $m(x, y, z) = xy \vee xz \vee yz$ является функцией почти единогласия. Она порождает класс $B = \mathrm{Inv}(m)$ биюнктивных предикатов на двухэлементном множестве, представимых в виде биюнктивных КНФ, т. е. КНФ, в которых любой конъюнкт содержит не более двух литералов. Если $S \subseteq B$, то задача *S-ВЫП* — полиномиальна [6]. Полиномиальный алгоритм основан на том, что можно рассматривать КНФ только с ограниченным числом литералов в ЭД (не более двух). В [8, 9] показано, что если $S \subseteq R_k$ содержит только предикаты, инвариантные относительно некоторой функции почти единогласия $f \in P_k^{(m+1)}$, то задача *S-ВЫП* — полиномиальна. Полиномиальный алгоритм опирается на свойство $(m+1)$-согласованности систем предикатов [4, 5]. В [9] получены свойства предикатов, инвариантных относительно некоторой функции единогласия.

Теорема 3.1 [1, 3]**.** *Пусть $f \in P_k^{(m+1)}$ — функция почти единогласия, $m \geqslant 2$. Если предикат $g \in R_k^{(n)}$ инвариантен относительно функции f, то этот предикат g можно представить полностью согласованной ОКНФ со ступенчатыми предикатами относительно любого линейного порядка $\leqslant$, в которой каждая ОЭД содержит не более m переменных.*

Предикат $g \in R_k$ назовем m-юнктивным, если он инвариантен от-

носительно некоторой $(m+1)$-местной функции почти единогласия. Полностью согласованную ОКНФ m-юнктивного предиката $g \in R_k$, в которой любая ОЭД содержит не более m переменных (существующую по теореме 3.1), назовем приведенным представлением этого предиката g. Конъюнкция всех простых имплицент m-юнктивного предиката g, содержащих не более m переменных, является приведенным представлением этого предиката g и называется его полным приведенным представлением.

Теорема 3.2 [1, 3]. *Пусть $f \in P_k^{(m+1)}$ — функция почти единогласия, $m \geqslant 2$. Существует полиномиальный алгоритм, который по полным приведенным представлениям K_j предикатов $g_j \in \mathrm{Inv}(f)$, $j = 1, \ldots, l$, находит полное приведенное представление K предиката $g = g_1 \cdot \ldots \cdot g_l \in R_k$.*

Функция $f(x, y) \in P_k$ называется полурешеточной функцией, если она обладает свойствами $f(x, x) = x$, $f(x, y) = f(y, x)$ и $f(f(x, y), z) = f(x, f(y, z))$. Каждая полурешеточная функция $f(x, y) \in P_k$ определяет на множестве E_k частичный порядок, в котором любые два элемента имеют единственную точную верхнюю грань. А именно, если $f(x, y) \in P_k$ — полурешеточная функция, то рассматривается частичный порядок $\leqslant_f$, в котором $a \leqslant_f b$ при $f(a, b) = b$ для всех $a, b \in E_k$. При $k = 2$ дизъюнкция $x \vee y$ и конъюнкция $x \cdot y$ являются полурешеточными функциями. Они порождают классы $WP = \mathrm{Inv}(x \vee y)$ и $WN = \mathrm{Inv}(x \cdot y)$ слабо положительных и слабо отрицательных предикатов на двухэлементном множестве, представимых в виде слабо положительных и слабо отрицательных КНФ, т. е. КНФ, в которых любой конъюнкт содержит соответственно не более одного отрицательного и не более одного положительного литерала. Если $S \subseteq WP$ или $S \subseteq WN$, то задача *S-ВЫП* — полиномиальна [6]. Полиномиальный алгоритм основан на том, что либо в КНФ есть ЭД, являющаяся литералом, либо КНФ выполнима на наибольшем (наименьшем) наборе. В [8] показано, что если $S \subseteq R_k$ содержит только предикаты, инвариантные относительно некоторой полурешеточной функции $f \in P_k^{(2)}$, то задача *S-ВЫП* — полиномиальна. Полиномиальный алгоритм состоит в приведении исходной системы предикатов к попарно согласованной и дальнейшего ограничения множества значений каждой переменной. В [10] рассматривалась задача *S-ВЫП* на линейно упорядоченных множествах.

ОЭД D (со ступенчатыми предикатами относительно какого-то частичного порядка $\leqslant$) назовем слабо положительной, если в нее входит не более одного отрицательного литерала. ОКНФ K назовем

слабо положительной, если каждая ее ОЭД слабо положительна.

Теорема 3.3 [2]. *Пусть $f(x,y) \in P_k$ — полурешеточная функция. Предикат $g \in R_k^{(n)}$ инвариантен относительно функции f тогда и только тогда, когда этот предикат g представим слабо положительной ОКНФ со ступенчатыми предикатами относительно частичного порядка $\leqslant_f$.*

Предикат $g \in R_k$ назовем слабо положительным, если его сохраняет некоторая полурешеточная функция. Приведенным представлением слабо положительного предиката $g \in R_k$, инвариантного относительно полурешеточной функции $f(x,y) \in P_k$, назовем его слабо положительную ОКНФ со ступенчатыми предикатами относительно частичного порядка $\leqslant_f$ (существующую по теореме 3.3). Сокращенная ОКНФ слабо положительного предиката g является приведенным представлением этого предиката g.

Теорема 3.4 [2]. *Пусть $\leqslant$ — частичный порядок на множестве E_k, в котором любые два элемента имеют единственную точную верхнюю грань. Существует полиномиальный алгоритм, который по слабо положительной ОКНФ $K(x_1,\ldots,x_n)$ со ступенчатыми предикатами относительно порядка $\leqslant$ проверяет выполнимость этой ОКНФ.*

Алгоритм опирается на следующие свойства конъюнкций ступенчатых предикатов.

Утверждение 3.1 [2]. *Для любых $a \in E_k$, $b, b_1, b_2 \in E_k \cup \{-1\}$ верны следующие свойства*:

1) $\bar{s}_{b_1}(x) \cdot \bar{s}_{b_2}(x) = \bar{s}_{b_1}(x)$, *если* $b_1 \leqslant b_2$;
2) $\bar{s}_{b_1}(x) \cdot \bar{s}_{b_2}(x) = \bar{s}_{\sqcup(b_1,b_2)}(x)$, *если* b_1 *и* b_2 *— не сравнимы*;
3) $\bar{s}_b(x) \cdot s_a(x) = 0$, *если* $b \leqslant a$;
4) $\bar{s}_b(x) \cdot s_a(x) = \bar{s}_b(x) \cdot s_{\sqcup(a,b)}(x)$, *если* a *и* b *— не сравнимы.*

На основе утверждения 3.1 любую слабо положительную ОКНФ можно быстро привести к виду, в котором либо найдется конъюнкт, являющийся отрицательным литералом, либо в каждом ее конъюнкте есть положительный литерал. Предлагаемый полиномиальный алгоритм опирается на эти свойства ОКНФ.

Работа поддержана РФФИ, гранты 17-01-00782-а и 19-01-00200-а.

Список литературы

1. Селезнева С. Н. О биюнктивных предикатах над конечным множеством // Дискретная математика. — 2017. — Т. 29, вып. 4. — С. 130–142.

2. Селезнева С. Н. О слабо положительных предикатах над конечным множеством // Дискретная математика. — 2018. — Т. 30, вып. 3. — С. 127–140.

3. Селезнева С. Н. Об m-юнктивных предикатах на конечном множестве // Дискретный анализ и исследование операций. — 2019. — В печати.

4. Dechter R. From local to global consistency // Artificial Intelligence. — 1992. — V. 55. — P. 87–107.

5. Cooper M. C. An optimal k-consistency algorithm // Artificial Intelligence. — 1989. — V. 41. — P. 89–95.

6. Schaefer T. Complexity of satisfiability problems // Proc. of the 10th ACM Symposium on Theory of Computing. — 1978. — P. 216–226.

7. Bulatov A. A. A dichotomy theorem for constraint satisfaction problems on a 3-element set // J. of the ACM. — 2006. — V. 53, no. 1. — P. 66–120.

8. Jeavons P., Coher D., Gyssens M. Closure properties of constraints // Journal of the ACM. — 1997. — V. 44. — P. 527–548.

9. Jeavons P., Cohen D., Cooper M. Constraints, consistency and closure // Artificial Intelligence. — 1998. — V. 101 (1–2). — P. 251–265.

10. Jeavons P. J., Cooper M. C. Tractable constraints on ordered domains // Artificial Intelligence. — 1995. — V. 79. — P. 327–339.

11. Bulatov A., Jeavons P., Krokhin A. Classifying the complexity of constraints using finite algebras // SIAM J. Comput. — 2005. — V. 34, no. 3. — P. 720–742.

12. Булатов А. А. Полиномиальность мальцевских задач CSP // Алгебра и логика. — 2006. — Т. 45, № 6. — С. 655–686.

13. Zhuk D. An algorithm for constraint satisfaction problem // Proc. of IEEE 47th International Symposium on Multiple-Valued Logic. — 2017. — P. 1–6.

14. Zhuk D. A proof of CSP dichotomy conjecture // In Proc. of IEEE 58th Annual Symposium on Foundations of Computer Science, Berkeley, CA. 2017. — P. 331-342.

15. Bulatov A. A. A dichotomy theorem for nonuniform CSPs // In Proc. of IEEE 58th Annual Symposium on Foundations of Computer Science, Berkeley, CA. 2017. — P. 319-330

16. Lau D. Function Algebras on Finite Sets. — Springer, 2006.

МАТРОИДЫ И ИХ НЕКОТОРЫЕ ПРИЛОЖЕНИЯ

А. М. Ревякин (Москва), А. Н. Исаченко (Минск)

Система $\mathcal{I}$ подмножеств конечного множества S называется *матроидом* $M = (S, \mathcal{I})$, а множества из $\mathcal{I}$ – *независимыми*, если выполняются 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 $B \cup \{a\} \in \mathcal{I}$.

Пара $(S, \mathcal{I})$, удовлетворяющая условиям 1) и 2) называется *системой независимости*. Подмножество A из S — *зависимо*, если $A \notin \mathcal{I}$. Минимальное по включению зависимое множество называется *циклом*, а максимальное независимое — *базой* матроида.

Ранговая функция матроида определяется как целочисленная функция $r(A)$, определенная для всех $A \subseteq S$, такая, что $r(A) = \max\{|X| : X \subseteq A, X \in \mathcal{I}\}$.

Впервые понятие матроида ввел в 1935 году Х. Уитни (H. Whitney), изучая двойственные графы. Хотя ранее Б. Л. Ван дер Варден (B. L. Van der Waerden) рассмотрел в книге «Современная алгебра» наряду с линейной зависимостью алгебраическую зависимость. Позднее С. Маклейн (S. Mac Lane) дал интерпретацию матроида в терминах проективной геометрии, а Г. Биркгоф (G. Birkhoff) ввел понятие M-структуры (матроидной решетки) и заметил, что проективные геометрии являются таковыми.

Матроид можно определить, используя различные его понятия, например: базы, циклы, функцию ранга, оператор замыкания и многие другие. Способы задания матроидов, когда за «новые» аксиомы в определении берутся такие свойства матроида, при которых «старые» аксиомы становятся «новыми» свойствами, называются криптоморфными. Существует много криптоморфных систем аксиом матроидов [1–5]. Удачный выбор той или иной системы при рассмотрении конкретной задачи значительно упрощает ее решение. Наиболее полное описание криптоморфных систем аксиом матроидов привел Т. Брилавский (T. Brylawski) в [3]. Приведем некоторые криптоморфные определения матроида.

Пара $M = (S, \mathcal{B})$, где $\mathcal{B}$ — семейство *баз*, образует матроид, если:
1) никакое собственное подмножество базы не является базой;
2) если $B_1, B_2 \in \mathcal{B}$ и $x \in B_1$, то $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$ для некоторого $y \in B_2$.

При этом подмножество $A \in \mathcal{I}(M)$, если найдется $B \in \mathcal{B}$ такое, что $A \subseteq B$.

Пара $M = (S, \mathcal{C})$, где $\mathcal{C}$ — семейство *циклов* из S — матроид, если:
1) никакое собственное подмножество цикла не является циклом;
2) если $C_1, C_2 \in \mathcal{C}$, $C_1 \neq C_2$ и $x \in C_1 \cap C_2$, то найдется цикл $C_3 \in \mathcal{C}$ такой, что $C_3 \subseteq (C_1 \cup C_2) \setminus \{x\}$.
Причем $A \in \mathcal{I}$, если A не содержит члены из $\mathcal{C}$.

Пара (S, r), где r — целочисленная функция (*ранг*), определенная на подмножествах конечного множества S, образует матроид, если для всех $A, B \subseteq S$ выполняются свойства:
1) $0 \leq r(A) \leq |A|$;
2) если $A \subseteq B$, то $r(A) \leq r(B)$;
3) $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.
При этом семейство $\mathcal{I}$ подмножеств множества S, для которых $r(A) = |A|$, образует матроид $(S, \mathcal{I})$ с ранговой функцией r.

Пусть $x \sim A$ означает, что x *зависит* от A. Тогда если для любых различных $x, y_1, \ldots, y_m, z_1, \ldots, z_n \in S$ выполняются условия:
1) $y_k \sim \{y_1, \ldots, y_m\}$, где $k = 1, 2, \ldots, m$;
2) если $m > 0, x \sim \{y_1, \ldots, y_m\}$ и x не зависит от $\{y_2, \ldots, y_m\}$, то $y_1 \sim \{x, y_2, \ldots, y_m\}$;
3) если $x \sim \{y_1, \ldots, y_m\}$ и $y_k \sim \{z_1, \ldots, z_n\}$ для всех $k, k = 1, 2, \ldots, m$, то $x \sim \{z_1, \ldots, z_n\}$;
то семейство $\mathcal{I}$ подмножеств A из S таких, что x не зависит от $A \setminus \{x\}$ для всех $x \notin A$, образует матроид $(S, \mathcal{I})$.

Пусть S — конечное множество S и для всех $A \subseteq S$ определен *оператор замыкания* $A \to \overline{A}$, для которого выполнены условия:
1) $A \subseteq \overline{A}$ для всех $A \subseteq S$;
2) если $A, B \subseteq S$ и $A \subseteq B$, то $\overline{A} \subseteq \overline{B}$;
3) $\overline{A} = \overline{\overline{A}}$ для всех $A \subseteq S$;
4) для любых $x, y \in S$ и всякого $A \subseteq S$ из $y \in \overline{A \cup \{x\}}$ и $y \notin \overline{A}$ следует, что $x \in \overline{A \cup \{y\}}$;
Тогда $(S, \overline{\ })$ — матроид. При этом семейство $\mathcal{I}$ подмножеств $A \subseteq S$ таких, что из $x \in A$ следует, что $x \notin \overline{A \setminus \{x\}}$, образует матроид $M = (S, \mathcal{I})$.

Задание матроида отличается от задания топологии на множестве S тем, что для замыкания не требуется выполнения условия $\overline{A} \cup \overline{B} = \overline{A \cup B}$ для всех $A, B \subseteq S$, но имеет место свойство 4), которое, вообще говоря, может не выполняться для замыкания топологии.

Если $\overline{A} = A$, то A называется *замкнутым* (или *плоскостью*) в M.

Пара $(S, \mathcal{F})$, где $\mathcal{F}$ — семейство плоскостей из S образует матроид, если:
1) $S \in \mathcal{F}$;
2) если $F_1, F_2 \in \mathcal{F}$, то $F_1 \cap F_2 \in \mathcal{F}$;
3) если $F_1, F_2, \ldots, F_k \in \mathcal{F}$ и F_i покрывает F (т.е. $F_i \supseteq F$ и не существует плоскости $F' \in \mathcal{F}$ такой, что $F_i \supset F' \supset F$) для всех i, $i = 1, 2, \ldots, k$, то $\{F_1 \setminus F, \ldots, F_k \setminus F\}$ — разбиение множества $S \setminus F$.
Причем семейство $\mathcal{I}$ подмножеств $A \subseteq S$ таких, что для всех $a \in A$ найдется подмножество $F \in \mathcal{F}$, для которого $A \setminus F = \{a\}$, является матроидом $(S, \mathcal{I})$.

Пусть $\mathcal{I}$ — семейство независимых множеств матроида M на S, $B \subseteq S$, $\mathcal{I}(M|B) = \{X : X \subseteq B, X \in \mathcal{I}\}$, а $\mathcal{I}(M.B)$ — семейство подмножеств Y из $S \backslash B$ такое, что $X \bigcup Y \in \mathcal{I}$. Матроид $M|B = (B, \mathcal{I}(M|B))$ называют *сужением* M на B, а матроид $M.B = (B, \mathcal{I}(M.B))$ — *сжатием* M на B. Пусть $A \subseteq S$. Тогда сужение $M|(S \backslash A)$ матроида M обозначают через $M - A$, а сжатие $M.(S \backslash A)$ через M/A и говорят, что $M - A$ получен из M *исключением*, а M/A *сжатием* подмножества A. Произвольная последовательность сжатий и исключений M называется *минором*.

Можно доказать, что $B^*(M) = \{S \setminus B : B \in \mathcal{B}(M)\}$ — множество баз некоторого матроида M^* на множестве S. Матроид M^* называют *двойственным* к M. Легко видеть, что $M^{**} = M$ и для всех $A \subseteq S$ имеет место соотношение $r^*(A) = |A| + r(S \setminus A) - r(S)$, где r и r^* – ранговые функции M и M^*. Матроид M называется *самодвойственным*, если он изоморфен двойственному матроиду M^*.

Матроид можно задать, также используя понятия: остовное множество, гиперплоскость, функции периметра и окружения ([5–8]). Учитывая двойственные соотношения, матроид можно определить также в терминах конезависимых множеств, кобазисов, коциклов и т.д.

Пусть $M = (S, \mathcal{I})$ — матроид, а u — некоторое понятие матроида. Если понятие определяет характер каждого множества $A \subseteq S$, то через $u(M)$ обозначим соответствующее семейство подмножеств матроида. Если u определяет функцию, то через $u(A, M)$ обозначим её значение для подмножества A на матроиде M. *Оракулом* $O(u)$ назовём инъективное отображение $W_u : (2^S, \mu) \to E(u)$, где $\mu(S)$ – совокупность всех матроидов на множестве S, $E(u)$ — множество конкретное для каждого понятия.

Так для понятий независимое, конезависимое, базис, кобазис, цикл, коцикл, остов, коостов, плоскоость, коплоскость, цикличе-

ское, коциклическое, гиперплоскость, когиперплоскость $E(u)$ ={ДА, НЕТ} и $W_u(A, M)$ ={ДА, если $A \in u(M)$; НЕТ, если $A \notin u(M)$}. Для понятий замыкание, козамыкание $E(u) = 2^S$, для понятий ранг, коранг, периметр, копериметр $E(u) = \{0, \ldots, |S|\}$, для понятий окружение, коокружение $E(u) = \{1, \ldots, |S|, \infty\}$. Для всех этих понятий $W_u(A, M) = u(A, M)$.

Если имеется задача Ω на матроиде $M = (S, \mathcal{I})$, заданном понятием u, то сложность её решения алгоритмом Λ относительно оракула $O(u)$ определяется как число элементарных операций, обозначим его через $m_u(\Omega, \Lambda, M)$, выполняемых алгоритмом. При этом одно обращение к оракулу $O(u)$, то есть получение значения $W_u(A, M)$, так же считается элементарной операцией. Сложность алгоритма Λ для задачи Ω относительно оракула $O(u)$ определяется как $\max_{M \in \mu(S)}(m_u(\Omega, \Lambda, M)$.

Возникает вопрос: отличается ли сложность алгоритма относительно разных оракулов? Будем говорить, что оракул $O(u_1)$ полиноминально сводим к оракулу $O(u_2)$, если значение $W_{u_1}(A, M)$ может быть получено за полиномиальное число обращений к оракулу $O(u_2)$. Относительно полиномиальной сводимости матроидных оракулов справедлива следующая теорема.

Теорема. *В орграфе на рисунке* 1*, вершинами которого являются матроидные оракулы, путь от вершины a к вершине b существует тогда и только тогда, когда оракул a полиномиально сводим к оракулу b.*

Приведем примеры матроидов.

1. Пусть S — n-элементное множество, k — некоторое целое такое, что $1 \leq k \leq n$, и $\mathcal{I} = \{A \subseteq S : |A| \leq k\}$. Матроид $(S, \mathcal{I})$ называется *однородным* и обозначается через $U_{k,n}$. Если $n = k$, то матроид $U_{k,n}$ называют *свободным* и обозначают его через F_n.

2. Пусть S — конечное подмножество векторов линейного пространства L над полем F и $A \subseteq S$. Скажем, что $A \in \mathcal{I}$, если A — линейно независимое множество векторов из L. Матроид $(S, \mathcal{I})$ называется *векторным матроидом* над полем F.

3. Пусть K — расширение поля F, S — конечное подмножество из K, $A \subseteq S$ и $A \in \mathcal{I}$, если элементы из A являются алгебраически независимыми над полем F. Тогда $\mathcal{I}$ – семейство независимых множеств некоторого матроида M. Матроид M называют *алгебраическим*.

4. Пусть G — простой граф с множествами вершин V и ребер E. Тогда семейство всех циклов графа G является множеством всех циклов некоторого матроида $M(G)$ на E, называемого *циклическим*

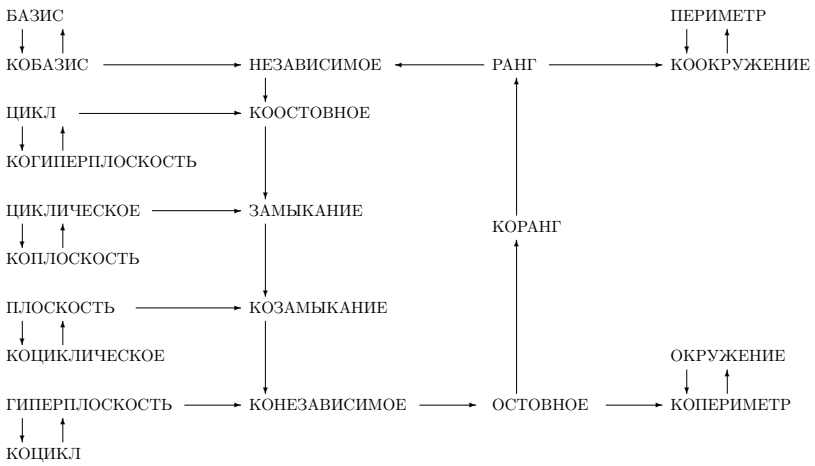


Рис. 1: Орграф сводимости матроидных оракулов

матроидом графа G. Матроид M называется *графическим*, если существует граф G, циклический матроид которого изоморфен M.

5. Семейство всех минимальных (по включению) разрезов графа G является в точности семейством циклов матроида $M^*(G)$ на E. Матроид $M^*(G)$ называется *матроидом разрезов* графа G. M называется *кографическим*, если существует граф G, матроид разрезов $M^*(G)$ которого изоморфен M.

6. Пусть $S = \{1, 2, 3, 4, 5, 6, 7\}$, B — семейство, состоящее из всех подмножеств множества S, содержащих 3 элемента, за исключением подмножеств $\{1, 3, 5\}, \{1, 4, 7\}, \{1, 2, 6\}, \{2, 3, 4\}, \{2, 5, 7\}, \{4, 5, 6\}$ и $\{3, 6, 7\}$. Тогда матроид Φ с семейством баз B называется *матроидом Фано*. Матроид Φ имеет 7 точек и 7 прямых. Матроид, получаемый из Φ заменой прямой $\{4, 5, 6\}$ на три тривиальные прямые $\{4, 5\}, \{4, 6\}$ и $\{5, 6\}$, будем обозначать через Φ^-.

7. Пусть $S = \{a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2\}$, $\mathcal{B}$ — семейство баз матроида, состоящее из всех подмножеств множества S, содержащих 4 элемента, за исключением подмножеств $\{a_1, a_2, b_1, b_2\}$, $\{a_1, a_2, c_1, c_2\}$, $\{b_1, b_2, d_1, d_2\}$, $\{c_1, c_2, d_1, d_2\}$ и $\{b_1, b_2, c_1, c_2\}$. Тогда $(S, \mathcal{B})$ называется *матроидом Вамоса*.

8. Матроид на шести элементах, базами которого являются все трехэлементные подмножества, кроме одной фиксированной тройки,

будем обозначать через P_6.

Матроид M на множестве S называется *линейно представимым* над полем F, если существует линейное пространство V над полем F и отображение $\phi : S \longrightarrow M$, 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* матроида M над полем F. Представимые матроиды на конечных множествах удобно описывать с помощью матриц.

Пусть P_8 — матроид на 8 элементах с матрицей представления $\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & -1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 & 1 & 1 & 0 \end{array}\right)$ над полем GF(3), а R_{10} — матроид на 10 элементах с матрицей $\left(\begin{array}{cccccccccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{array}\right)$ представления над полем GF(2).

Рассмотрим следующую задачу дискретной оптимизации. Пусть S — конечное множество, каждому элементу a которого приписан неотрицательный вес $w(a)$. Весом подмножества $A \subseteq S$ называется сумма весов его элементов. Пусть $\mathcal{I}$ — некоторое семейство подмножеств множества S. Требуется в $\mathcal{I}$ найти множество максимального веса.

Опишем, так называемый, «*жадный*» алгоритм.

а) упорядочить элементы множества S по убыванию весов;

б) $A = \emptyset, i = 1$;

в) если $A \bigcup \{a_i\} \in \mathcal{I}$, то $A := A \bigcup \{a_i\}$, иначе $A := A$. Перейти к пункту г);

г) если $i = n$, то конец, иначе $i = i + 1$ и перейти к пункту в).

Очевидно, что выходом жадного алгоритма является максимальное по включению множество из $\mathcal{I}$. Однако оно может оказаться не максимального веса. Например, если $S = \{a, b, c, d\}$, $\mathcal{I} = \{\{a\}, \{a, c\}, \{b, c, d\}, \{b, d\}\}$, $w(a) = 4, w(b) = 3, w(c) = w(d) = 2$, то алгоритм найдет множество $\{a, c\}$ с весом 6, хотя $\{b, c, d\}$ имеет вес 7.

Возникает вопрос: когда можно гарантировать получение подмножества максимального веса, решая задачу жадным алгоритмом? Ответ на это дает теорема Р. Радо (R. Rado) и Ж. Эдмондса (J. Edmonds) о том, что если $M = (S, \mathcal{I})$ — матроид, то множество A,

найденное жадным алгоритмом, является независимым множеством M с наибольшим весом. Напротив, если $(S, \mathcal{I})$ не является матроидом, то существует такая неотрицательная действительная функция $w(a)$ на S, что A не будет элементом семейства $\mathcal{I}$ с наибольшим весом.

Эффективность жадных алгоритмов вызывается тем, что элемент, один раз включенный в оптимальное решение, остается в нем до конца. Именно этим обусловлено широкое применение матроидов в задачах дискретной оптимизации для получения быстрых алгоритмов.

Таким образом, решение оптимизационной задачи возможно простым и эффективным «жадным» алгоритмом, если область допустимых решений задачи может быть представлена в виде матроида. Если задача не имеет «матроидной» структуры, то для оценки приближённого «жадного» решения можно воспользоваться результатами работы Б. Корте (B. Korte), Д. Хаусмана (D. Hausmann) [9]. В ней показано, что любая система независимости является пересечением конечного числа матроидов, каждый из которых определяется циклом системы независимости. Тем самым число матроидов в предлагаемом представлении совпадает с числом циклов системы независимости. Если система независимости является пересечением k матроидов, то отношение решения, полученного «жадным» алгоритмом, к точному решению не меньше $1/k$. Вопрос о получении семейства матроидов, дающего в пересечении исходную систему независимости и имеющую минимальное количество матроидов, остаётся открытым. Это связано с тем, что искомое минимальное семейство определяется, прежде всего, семантикой оптимизационной задачи. Например, любой матроид, являясь системой независимости, может быть представлен пересечением матроидов, порождаемых его циклами, число которых может быть больше одного. Например, задача о максимальном паросочетании двудольного графа является задачей на пересечении двух матроидов. В тоже время, в представлении системы независимости через пересечение матроидов, порождаемых циклами, число матроидов может превышать два. Задача о коммивояжере является задачей на пересечении трёх матроидов [10, 11]. При этом число циклов в исходной системе независимости может быть больше трёх.

Пусть $\mathrm{GF}(q)$ – поле характеристики q. Матроид, представимый над полем $\mathrm{GF}(2)$ или $\mathrm{GF}(3)$, называется *бинарным* или *тернарным* соответственно. Матроиды, представимые над любым полем, называются *унимодулярными* (или *регулярными*). Небинарные матроиды, представимые над всеми полями, кроме $\mathrm{GF}(2)$, называются *по-*

чти регулярными.

Перечислим интересные свойства для приведенных матроидов.

Матроид Вамоса и не представим ни над каким полем. Матроид Фано Ф является бинарным, но не представим ни над каким полем характеристики, отличной от 2. Графические и кографические матроиды являются унимодулярными, а Φ^- и P_8 — почти регулярными. Циклический матроид $M(K_4)$ полного графа K_4, $U_{3,6}$, P_6 и P_8 являются самодвойственными. Матроид P_6 является F–представимым тогда и только тогда, когда $|F| \geq 5$. Матроид P_8 не обладает минорами, изоморфными $M(K_4)$. Матроид R_{10} является унимодулярным и самодвойственным. Все миноры R_{10} являются либо графическими, либо кографическими, в то время, как сам R_{10} таковым не является. Исключение любого элемента из R_{10} ведет к образованию матроида, изоморфного циклическому матроиду графа $K_{3,3}$.

В 1953 году Лазарсон Т. (Lazarson T.) предложил для любого простого числа q конструкцию матроида, представимого только над полем $\mathrm{GF}(q)$. Брилавский Т. (Brylawski T.) и Кэлли Д. (Kelly D.) построили матроид, представимых только над полями характеристики 1103 и 2089. Пусть Z – множество простых чисел и $\emptyset$. 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 не из Q.

Многие проблемы теории матроидов касаются внутренней характеризации классов матроидов. Такие характеризации с помощью списка запрещенных миноров обычно получают в виде: «*Существует некоторый минимальный, но возможно бесконечный, список* Ω *такой, что матроид* M *лежит в классе* L *тогда и только тогда, когда* M *не содержит миноров, изоморфных элементам из* Ω».

Матроид M является бинарным тогда и только тогда, когда никакой его минор не изоморфен $U_{2,4}$.

Матроид M является тернарным тогда и только тогда, когда не содержит миноров, изоморфных $U_{2,5}, \Phi$, а также двойственным им.

Матроид M является унимодулярным тогда и только тогда, когда не содержит миноров, изоморфных $U_{2,4}, \Phi$ и двойственному ему Φ^*.

Матроид M является графическим тогда и только тогда, когда никакой его минор не изоморфен $U_{2,4}$, матроидам разрезов полных графов Куратовского K_5, $K_{5,5}$, матроиду Фано Ф или двойственному ему Φ^*.

Гипотеза (Rota G.C.)**.** *Матроиды, представимые над любым конечным полем* $\mathrm{GF}(q)$ *можно охарактеризовать в терминах конечного списка запрещенных миноров.*

Более чем двадцать пять лет не было никакого прогресса в ее решении. В 2000 году J. F. Geelen, A. M. H. Gerards и A. Kapoor [12] доказали:

Теорема. *Матроид M является* GF(4)*-представимым тогда и только тогда, когда не содержит миноров, изоморфных $U_{2,4}$, $U_{2,6}$, P_6, Φ^*, $(\Phi^-)^*$, P_8 и некоторому матроиду, получаемому из P_8 релаксацией единственной пары непересекающихся цикловгиперплоскостей.*

За этот результат в 2003 году авторам присуждена премия Фалкерсона. Начиная с 2000 года большое число публикаций было направлено на решением гипотезы Рота. В 2014 году J. Geelen, B. Gerards и G. Whittle объявили о решении гипотезы Рота, но полного доказательства до сих пор не опубликовано.

Сформируем еще несколько результатов об оракульной сводимости. Невозможно за полиномиальное число обращений к оракулу «независимый» проверить свойства матроида M быть однородным, самодвойственным, трансверсальным, линейно представимым, ориентируемым, двудольным или бинарным [7, 8].

В [13] введены понятия H- и L-периметров, H- и L-окружений в матроидах и показана полиномиальная сводимость к многих матроидных оракулов. Задачи нахождения в матроиде базы максимального веса, определения ранга произвольного подмножества в объединении k матроидов, нахождения подмножества максимального размера (или веса) независимого в двух заданных матроидах, минимизации субмодулярной функции, проверки на графичность (или регулярность) бинарного матроида являются полиноминально разрешимыми [6–8].

Пусть $M = (S, \mathcal{I})$ - матроид ранга $r(S)$, $r(S) = k < |S|$. Цикл C матроида M назовем гамильтоновым, если $|C| = k + 1$. Соответственно базу B матроида назовём гамильтоновой, если существует содержащий ее гамильтонов цикл. Матроид, содержащий гамильтонов цикл, так же будем называть гамильтоновым. Понятие гамильтоновых цикла, базы и матроида введено в работах [10, 11]. В них указан ряд свойств, касающихся сложности распознавания гамильтонова цикла матроида и доказано, что относительно оракула H-периметр задача распознавания гамильтонова цикла является полиноминально разрешимой.

Остановимся кратко на приложениях теории матроидов.

В 1991 году Брикэл Е. (Brickell E.), и Давенпорт Д. (Davenport D.) установили, что всякая совершенная идеальная схема разделения секрета (СРС) задает связный матроид [14]. Под совершенной СРС

обычно понимают схему, позволяющую распределить секрет между n участниками так, чтобы заданные разрешенные множества участников могли однозначно восстановить секрет (структуру доступа), а неразрешенные — не получали никакой дополнительной к имеющейся априорной информации о возможном значении секрета.

Пусть имеется $n+1$ множество $S_0, S_1, \ldots, S_n$. Произвольная $m \times (n+1))$-матрица R, 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 подмножества $B \subset 0, 1, \ldots, n$ обозначим через R_B $(m \times |B|)$-матрицу, полученную из матрицы R удалением столбцов, номера которых не принадлежат множеству B. Говорят, что матрица R задает *совершенную СРС*, реализующую структуру доступа Γ, если $\|R_{A \bigcup 0}\| = \|R_A\| \times \|R_0\|^{\delta(A)}$, где $\|R_A\|$ -– число различных строк в матрице R, $\delta(A) = 0$, если $A \in \Gamma$ и $\delta(A) = 1$ 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 $q = |S_0|$, являются множеством независимых множеств некоторого матроида M на множестве $0, 1, \ldots, n$. Причем функция $h(A)$ совпадает с ранговой функцией этого матроида [14].

Для задач, связанных с расчетом и синтезом электрических цепей, хорошо использовать кографический матроид, а для выбора выбора минимальных по размерности систем уравнений — матрицы фундаментальних циклов и разрезов соответствующих матроидов графов их электрических цепей [2, 15, 16].

Для электрических цепей, состоящих из резисторов и источников напряжения и тока выполняются законы Кирхгофа для токов (алгебраическая сумма токов, вытекающих из узла равна нулю) и напряжений (алгебраическая сумма напряжений в любом замкнутом контуре равна нулю), которые можно записать как $RI = 0$ и $CV = 0$, где R — матрица разрезов, I и V — вектор столбцы токов и напряжений соответственно на элементах электрической цепи.

Пусть T — остов цепи (орграфа), $\Phi = (\Phi_1|E)$ — матрица фундаментальных циклов, $K = (E|K_2$ — матрица фундаментальных разрезов относительно остова T, где E — единичные матрицы, а вектор-столбцы матриц, соответствующие хордам и ветвям остова T, отличаются подстрочными индексами. Тогда, в силу законов Киргофа, $\Phi_1|E) \cdot (I_1|I_2)^T = 0$ и $(E|K_2) \cdot (V_1|V_2)^T = 0$. Заметим, что $\Phi_1 = -K_2^T$. Отсюда, $I_2 = -\Phi_1 \cdot I_1 = K_2^T \cdot I_1$. Аналогично, $V_1 = K_2^T \cdot I_2$. Та-

ким образом, все токи, текущие через элементы электрической цепи, можно выразить линейной комбинацией хордовых токов, а все напряжения — линейной комбинацией напряжений на ветвях цепи.

Для электрических цепей, состоящих из источников тока и напряжений, а также (линейных/нелинейных) положительных сопротивлений, выполняются следующие свойства неусиления:
1) величина напряжения на любом из сопротивлений не больше суммы величин напряжений на всех источниках;
2) величина тока в любом сопротивлении с нулевым напряжением не больше суммы величин токов, текущих через источники.

Перечисленные результаты хорошо формулируются и описываются в терминах матроидов [2, 15, 16].

Рассмотрим плоскую ферму, состоящую из жестких стержней и соединяющих их шарниров, решетка которой состоит из одинаковых в каждом горизонтальном ряду прямоугольников. Для того, чтобы ферма была жесткой), необходимо добавить диагональные стержню в некоторые прямоугольники решетки. Пусть ферма имеет m строк и n столбцов. Определим двудольный граф $G = (V, E)$, вершины которого соответствуют строкам (первая доля) и столбцам (вторая доля) $V = \{v_1, \ldots, v_m, w_1, \ldots, w_n\}$, а ребра (v_i, w_j) соответствуют тем прямоугольникам решетки, в которых располагаются диагональные стержни. Ферма будет жесткой тогда и только тогда, когда граф G является связным [2, 17]. Минимальное множество диагональных стержней, придающее жесткость ферме с m строками и n столбцами, содержит $m + n - 1$ стержней и соответствует базе циклического матроида графа G.

Среди других приложений теории матроидов отметим использование матроидов в решении экономических задач [18, 19] и задач поиска условий жесткости строительных конструкций [2, 17].

Список литературы

1. Oxley J. G. Matroid Theory. — New York: Oxford Academ, 2006.

2. Recski A. Matroid theory and its applications in electric network theory and in statics. — Budapest: Akad. Kiado, 1989.

3. Matroid applications / Ed. White N. — Cambridge Univ. Press, 1992.

4. Revyakin A. M. Matroids. // J. Math. Sci. — 2002. — V. 108, no. 1. — P. 71–130.

5. Ревякин А. М. Матроиды: криптоморфные системы аксиом и жесткость ферм. // Вестник МГАДА — 2010. — № 5. — С. 96–106.

6. Исаченко А. Н. Полиномиальная сводимость матроидных оракулов // Известия АН БССР, сер.физ.-мат.наук. — 1984. — № 6. —

С. 33–36.

7. Исаченко А. Н. Об одном критерии для матроидов // Вестн. БГУ. Сер. 1. — 1983. — № 2. — С. 59–60.

8. Исаченко А. Н., Ревякин А. М. О сводимости матроидных оракулов // Вестник МГАДА. — 2011. — № 3 (9). — С. 117–127.

9. Korte B., Hausmann D. An analysis of the greedy heuristic for independence systems // Annals of Discrete Mathematics. —1978. — 2. — P. 65–74.

10. Исаченко А. Н., Исаченко Я. А. Периметр матроида и задача коммивояжера на матроиде // XI Белорусская математическая конференция: Тез. докл. Междунар. науч. конф. Минск, 5–9 ноября 2012 г. Часть 4. — Мн.: Институт математики НАН Беларуси, 2012. — С. 87–88.

11. Исаченко А. Н., Исаченко Я. А. Гамильтоновы циклы матроида // Проблемы теоретической кибернетики. Материалы XVII Международной конференции (Казань, 16–20 июня 2014 г.). — Казань: Отечество, 2014. — С. 116–118.

12. Geelen J. F., Gerards A. M. H., Kapoor A. The excluded minors for GF(4)-representable matroids // J. Combin. Theory. — 2000. — 79. — P. 247–299.

13. Исаченко А. Н., Исаченко Я. А., Ревякин А. М. О периметрах и окружениях для матроида // Вестник МГАДА. — 2013. — № 1 (20). – С. 63–67.

14. Ревякин А. М. Матроиды, коды и схемы разделения секретов // Вестник МГАДА. — 2010. — № 3. — С. 174–178.

15. Исаченко А. Н., Ревякин А. М. Электрические цепи и ориентированные матроиды // Электронные информационные системы. — 2019. — № 2 (21). — С. 105–111.

16. Ревякин А. М., Исаченко А. Н. Ориентированные матроиды и их приложения // Алгебра, теория чисел и дискретная геометрия: современные проблемы, приложения и проблемы истории: Материалы XVI Междунар. конф., посвященной 80-летию со дня рождения профессора Мишеля Деза. — Тула: Тул. гос. пед. ун-т им. Л. Н. Толстого, 2019. — С. 179–182.

17. Ревякин А. М., Речки А. Жесткость планарных ферм с удаленными фрагментами // Материалы VIII Международного семинара «Дискретная математика и ее приложения» (2–6 февраля 2004 г.). — М.: Изд-во механико-математического факультета МГУ, 2004. — С. 219–221.

18. Исаченко А. Н., Ревякин А. М. Матроиды в математическом моделировании экономических систем // Экономические и

социально-гуманитарные исследования — 2015. — № 1 (5). — С. 13–18.

19. Исаченко А. Н., Ревякин А. М. Матроиды и сильная связность орграфов в математическом моделировании экономических систем // Экономические и социально-гуманитарные исследования. — 2018. — №4 (20). — С. 36–40.

О ПРОБЛЕМЕ ПОЛНОТЫ В КЛАССАХ ЛИНЕЙНЫХ АВТОМАТОВ НАД КОНЕЧНЫМИ ПОЛЯМИ

А. А. Часовских (Москва)

Согласно [1], конечный инициальный автомат $\mathfrak{A}$ определяется шестеркой $(A, B, Q, \phi, \psi, \overline{q}_0)$, где A, B и Q — конечные множества, называемые входным алфавитом, выходным алфавитом и алфавитом состояний, соответственно, $\phi : Q \times A \to Q$ — функция переходов, $\psi : Q \times A \to B$ — функция выходов и $\overline{q}_0 \in Q$ — начальное состояние. Функционирование автомата $\mathfrak{A}$ происходит во времени. В начальный момент времени $t = 0$ он находится в состоянии $\overline{q}_0$. Если в некоторый момент времени t автомат находится в состоянии $\overline{q}(t)$, а входом в этот момент является буква $\overline{a}(t) \in A$, то выходом автомата в этот момент является буква $\psi\left(\overline{q}(t), \overline{a}(t)\right)$, а его состоянием в момент $t+1$ будет $\phi\left(\overline{q}(t), \overline{a}(t)\right)$.

В части [1], посвященной структурной теории конечных автоматов, в качестве входного алфавита и алфавита состояний рассматриваются конечные декартовы степени множества $E_2 = \{0, 1\}$, а выходной алфавит совпадает с E_2. В этой же работе определены операции композиции (суперпозиции и обратной связи) над такими автоматами, таким образом, строится класс $\mathfrak{P}_2$ конечных инициальных автоматов над E_2 с операциями композиции.

Как принято, замыкание множества M, $M \subseteq \mathfrak{P}_2$, по операциям композиции мы обозначаем $K(M)$, множество M называем полным, если $K(M) = \mathfrak{P}_2$. В случае $K(M) = M$ множество M называем замкнутым классом. Замкнутый класс называется предполным или максимальным, если он не совпадает с $\mathfrak{P}_2$, но, добавляя к нему любой автомат, в нем не содержащийся, получаем полное множество.

Мощность множества предполных классов в $\mathfrak{P}_2$ равно континууму [2], что существенно затрудняет исследования этого класса. Например, проблема полноты конечных подмножеств в нем алгоритмически не разрешима [3]. Попытка изменить оператор замыкания с использованием понятия аппроксимации [4] не привела к алгоритмической разрешимости аналогичной задачи. Классификация замкнутых классов Поста, используемых в качестве добавки к конечным множествам из $\mathfrak{P}_2$, по разрешимости свойств полноты и A-полноты была выполнена в [5].

Исследованию вопросов полноты для классов, связанных с $\mathfrak{P}_2$, посвящено значительное количество работ, в некоторых из которых изучаются выразительные свойства содержательных подклассов $\mathfrak{P}_2$.

Таким подклассом является, например, класс линейных автоматов.

Для определения линейного автомата мы перейдем от множества E_2 к полю E_k, состоящему из k элементов. При этом, как известно [6], для некоторого простого числа p и некоторого натурального числа m имеет место равенство $k = p^m$. Конечный инициальный автомат $\mathfrak{A}$, задаваемый шестеркой $(A, B, Q, \phi, \psi, \overline{q}_0)$, называется линейным, если, найдутся такие натуральные числа n и r, а также найдутся такие матрицы C, D, F, G с элементами из E_k, что:

$$A = E_k^n, \;\; Q = E_k^r, \;\; B = E_k,$$

$$|C| = r \times r, \;\; |D| = r \times n, \;\; |F| = 1 \times r, \;\; |G| = 1 \times n,$$

$\overline{q}_0 \in Q$, как и прежде, состояние автомата $\mathfrak{A}$ в начальный момент времени, а для функций переходов и выходов, соответственно, имеют место равенства:

$$\phi(\overline{q}, \overline{x}) = C\overline{q} + D\overline{x}, \;\; \psi(\overline{q}, \overline{x}) = F\overline{q} + G\overline{x},$$

при этом переменные $\overline{q}$ и $\overline{x}$ принимают значения из алфавитов Q и A, соответственно, $|\overline{q}| = r \times 1$, $|\overline{x}| = n \times 1$. В случае $r = 1$ или $n = 1$ вместо векторной записи переменной $\overline{q}$ или $\overline{x}$ мы используем запись q или x, соответственно. Таким образом, мы определяем линейный автомат в соответствии с работой [7], который теперь можем задавать системой канонических уравнений:

$$\begin{gathered} \overline{q}(0) = \overline{q}_0, \\ \overline{q}(t+1) = C\overline{q}(t) + D\overline{x}(t), \\ y(t) = F\overline{q}(t) + G\overline{x}(t). \end{gathered}$$

Линейными автоматами являются, например, сумматор $x_1 + x_2 + \cdots + x_n$, усилитель (умножитель) $a \cdot x$, $a \in E_k$, задержка $\xi_a(x)$ с начальным состоянием a, $a \in E_k$, которые задаются, соответственно, следующими системами канонических уравнений:

$$\begin{gathered} q(0) = 0, \\ q(t+1) = q(t), \\ y(t) = x_1(t) + x_2(t) + \cdots + x_n(t); \end{gathered}$$

$$\begin{gathered} q(0) = 0, \\ q(t+1) = q(t), \\ y(t) = a \cdot x(t); \end{gathered}$$

$$q(0) = a,$$
$$q(t+1) = x(t),$$
$$y(t) = q(t).$$

Множество линейных автоматов над полем E_k обозначим $\mathfrak{L}_k$. К элементам этого множества в соответствии с [1] могут применяться операции композиции (суперпозиции и обратной связи). Замыкание множества M, $M \subseteq \mathfrak{L}_k$, по этим операциям будем обозначать $K(M)$. Множество M называется замкнутым, если $K(M) = M$. В случае $K(M) = \mathfrak{L}_k$ множество M называется полным.

Как нетрудно видеть, множество $\{x_1 + x_2, a \cdot x, \xi_a(x) \mid a \in E_k\}$ является полным.

Замкнутый в $\mathfrak{L}_k$ класс M называется предполным или максимальным, если $M \neq \mathfrak{L}_k$, но для любого f, $f \in \mathfrak{L}_k \setminus M$, множество $M \cup \{f\}$ полно.

В работе [8] для случая простого k были найдены все предполные классы и получен алгоритм проверки полноты конечных множеств. Далее в [9] доказана алгоритмическая разрешимость задачи проверки полноты конечных множеств для случая произвольного конечного поля E_k.

В настоящей работе для общего случая, когда k не является простым, определены все предполные классы, с использованием которых, построен алгоритм проверки полноты конечных множеств и получена верхняя оценка времени работы этого алгоритма.

Пусть в момент времени t, $t = 0, 1, \ldots$, на вход x_i линейного автомата со входами x_1, x_2, $\ldots$, x_n подается $a_i(t)$, $a_i(t) \in E_k$, а на выходе в этот момент времени получается $b(t)$, $b(t) \in E_k$. Через $\alpha_i(\xi)$ обозначим следующий формальный ряд переменной ξ:

$$\sum_{t=0}^{\infty} a_i(t)\xi^t,$$

и, кроме того, положим:

$$\beta(\xi) = \sum_{t=0}^{\infty} b(t)\xi^t.$$

Таким образом, рассматриваемый линейный автомат каждому набору рядов $(\alpha_1(\xi), \alpha_2(\xi), \ldots, \alpha_n(\xi))$ сопоставляет некоторый ряд $\beta(\xi)$.

Кольцо формальных степенных рядов переменной ξ с коэффициентами из E_k обозначим $R_k(\xi)$, а его подкольцо, состоящее из рядов,

коэффициенты которых образуют периодическую (с предпериодом) последовательность, обозначим $E'_k(\xi)$. Нетрудно видеть, что $E'_k(\xi)$ является кольцом отношений многочленов со знаменателями, не делящимися на ξ.

Лемма. *Линейный автомат с n входами из $\mathfrak{L}_k$ — это отображение $f(x_1, \ldots, x_n)$ из $R_k(\xi)^n$ в $R_k(\xi)$, для которого в $E'_k(\xi)$ найдутся такие μ_i, $i = 0, 1, \ldots, n$, что выполнено равенство:*

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0.$$

Если линейный автомат f задан равенством

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0,$$

то через $U(f)$ обозначим множество

$$\{\ \mu_i \mid i = 1, 2, \ldots, n\ \}.$$

Таким образом, $U(f) \subset E'_k(\xi)$. Множество $E'_k(\xi)$ будем рассматривать вместе с операциями сложения, умножения и двуместной операцией «fb», применимой к паре (μ_1, μ_2) в точности тогда, когда $\mu_2(0) = 0$, и, в случае применимости, результатом является дробь:

$$\frac{\mu_1}{1 - \mu_2}.$$

Следующая лемма приводит к изучению алгебры $E'_k(\xi)$.

Лемма. *Пусть линейный автомат задан равенством*

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0.$$

Если автомат f_1 получен из f переименованием входов, без отождествления, то $U(f) = U(f_1)$.

Если автомат f_2 получен из f отождествлением входов x_1 и x_2, то

$$U(f_2) = \{\ \mu_1 + \mu_2,\ \ \mu_i \mid i = 3, 4, \ldots, n\ \}.$$

Если автомат f_3 получен подстановкой автомата f' на вход x_1 автомата f, то

$$U(f_3) = \{\ \mu_1\mu'\ \mid\ \mu' \in U(f')\ \} \cup \{\ \mu_i\ \mid\ i = 2, 3, \ldots, n\ \}.$$

Если автомат f_4 получен применением операции обратной связи к переменной x_1 автомата f, то

$$U(f_4) = \left\{\ \frac{\mu_i}{1-\mu_1}\ \mid\ i = 2, 3, \ldots, n\ \right\}.$$

Замыкание множества M, $M \subseteq E'_k(\xi)$, по операциям сложения, умножения и операции «fb» обозначим $K^{(1)}(M)$. В алгебре $E'_k(\xi)$ вводим понятие замкнутого класса, полного множества и предполного класса аналогично тому, как это было сделано для $\mathfrak{L}_k$, только вместо K-замыкания используется $K^{(1)}$-замыкание.

Мы найдем все предполные классы в алгебре $E'_k(\xi)$, каждый из которых относится к одному из трех типов.

Классы типа P. Пусть, как и ранее, $k = p^m$, для некоторого простого p и натурального m, $m > 1$. Разложим m в произведение степеней различных простых чисел:

$$m = q_1^{r_1} \cdot q_2^{r_2} \cdot \cdots \cdot q_l^{r_l}.$$

Положим:

$$k_s = p^{m/q_s},\ \ s = 1, 2, \ldots, l.$$

Собственное подполе поля E_k, не содержащееся ни в каком другом собственном подполе этого поля, назовем максимальным подполем. Согласно [6], в поле E_k содержится единственное подполе, состоящее из k_s элементов. Это подполе обозначим E_{k_s}. Из [6] следует, что E_{k_1}, E_{k_2}, …, E_{k_l} — максимальные подполя в E_k и других максимальных подполей в E_k нет.

Теперь определим классы типа P, положив:

$$P_s^{(1)} = \{\ \mu\ \mid\ \mu \in E'_k(\xi),\ \ \mu(0) \in E_{k_s}\ \},$$

$s = 1, 2, \ldots, l$.

Классы типа M. Для определения этих классов нам понадобятся некоторые гомоморфизмы колец. Сначала определим эти кольца.

$$\tilde{M}_0^{(1)} = \left\{\ \mu\ \mid\ \mu \in E'_k(\xi),\ \ \mu = \frac{u}{v},\ \ \deg u \le \deg v\ \right\},$$

$$E_k^2 = \{\ (a_1, a_2)\ \mid\ a_i \in E_k, i = 1, 2\ \}.$$

Упорядочим все неприводимые приведенные многочлены кольца $E_k[\xi]$ многочленов переменной ξ с коэффициентами из E_k:

$$p_1(\xi), p_2(\xi), \dots$$

так, что $p_1(\xi) = \xi$. Положим:

$$\tilde{M}_i^{(1)} = \left\{\ \mu\ \mid\ \mu \in E_k'(\xi),\ \ \mu = \frac{u}{v},\ \ p_i\ \text{не делит}\ v\ \right\},$$

$i = 2, 3, \dots,$

$$E_{k,i} = \{\ (a, u)\ \mid\ a \in E_k,\ \ u \in E_k[\xi],\ \ \deg u < \deg p_i\ \},$$

$i = 2, 3, \dots.$

Нетрудно видеть, что множество $\tilde{M}_i^{(1)}$ является кольцом с операциями сложения и умножения для каждого i, $i \in \{0, 2, 3, \dots\}$, а E_k^2 и $E_{k,i}$ — кольца с операциями покомпонентного сложения и умножения. При этом умножение многочленов во второй компоненте пар из $\tilde{M}_i^{(1)}$ выполняется по модулю многочлена p_i, $i = 2, 3, \dots$.

Заметим далее, что для любого μ, $\mu \in \tilde{M}_0^{(1)}$, найдутся r, u', v', a, a', b, b' такие, что $r \in \mathbb{N}$, $u' \in E_k[\xi]$, $v' \in E_k[\xi]$, $\deg u' < r - 1$, $\deg v' < r - 1$, $\{a, a', b, b'\} \subset E_k$, $b \neq 0$, $b' \neq 0$ и выполнено тождество:

$$\mu = \frac{a + \xi u' + a'\xi^r}{b + \xi v' + b'\xi^r}.$$

Несложно показать, что отображение Ψ_0, определенное равенством

$$\Psi_0(\mu) = \left(\frac{a}{b}, \frac{a'}{b'}\right),$$

является гомоморфизмом кольца $\tilde{M}_0^{(1)}$ на кольцо E_k^2.

Далее, пусть $i \in \{2, 3, \dots\}$. Для каждого μ, $\mu \in \tilde{M}_i^{(1)}$, найдутся и, притом, единственным образом такие u' и μ', $u' \in E_k[\xi]$, $\deg u' < \deg p_i$, $\mu' \in \tilde{M}_i^{(1)}$, что выполнено равенство:

$$\mu = u' + p_i\mu'.$$

Тогда положим:

$$\Psi_i(\mu) = (\mu(0), u')\,.$$

Для каждого i, $i \in \{2, 3, \dots\}$, отображение Ψ_i является гомоморфизмом кольца $\tilde{M}_i^{(1)}$ на кольцо $E_{k,i}$.

Известно, что поле E_k имеет m автоморфизмов [6], множество которых обозначим Ω_k. Для каждого автоморфизма ω из Ω_k определим следующие классы типа M:

$$M_{i,\omega}^{(1)} = \left\{ \ \mu \ \mid \ \mu \in \tilde{M}_i^{(1)}, \ \ \Psi_i(\mu) = (\mu(0), \omega(\mu(0))) \ \right\},$$

$i = 0, 2, 3 \dots$.

Кроме этих классов, имеется еще один класс типа M:

$$M_1^{(1)} = \left\{ \ \mu \ \mid \ \mu \in E_k'(\xi), \ \ \mu(\xi) - \mu(0) \in \xi^2 E_k'(\xi) \ \right\}.$$

Классы типа R.

$$R_0^{(1)} = \left\{ \ \mu \ \mid \ \mu \in E_k'(\xi), \ \ \mu = \frac{u}{v}, \ \ \deg u < \deg v \ \right\},$$

$$R_i^{(1)} = \left\{ \ \mu \ \mid \ \mu \in E_k'(\xi), \ \ \mu = \frac{u}{v}, \ \ (u, v) = 1, \ \ p_i \ \text{делит} \ \ u \ \right\},$$

$i = 2, 3, \dots$.

Положим:

$$J_k^{(1)} = \left\{ \ P_s^{(1)}, \ \ M_{i,\omega}^{(1)}, \ \ M_1^{(1)}, \ \ R_i^{(1)} \ \mid \right.$$
$$\left. s = 1, 2, \dots, l, \ \ i = 0, 2, 3, \dots, \ \ \omega \in \Omega_k \ \right\}.$$

Теорема. *Множество $J_k^{(1)}$ состоит из предполных в $E_k'(\xi)$ классов и все предполные классы $E_k'(\xi)$ содержатся в $J_k^{(1)}$.*

Множество замкнутых классов в заданной алгебре называется критериальной системой, если для любого подмножества этой алгебры его полнота равносильна не включению в каждый замкнутый класс этого множества. Критериальная система, любое собственное подмножество которой не является критериальной системой, называется приведенной. Известно [1], что множество предполных классов в конечнопорожденной алгебре составляет приведенную критериальную систему. Таким образом, множество $J_k^{(1)}$ является приведенной критериальной системой в $E_k'(\xi)$.

Далее нам понадобятся некоторые подмножества $\mathfrak{L}_k$, а также определения, с использованием которых эти подмножества будут получены.

Для заданного a, $a \in E_k$, через T_a обозначим множество всех линейных автоматов из $\mathfrak{L}_k$, сохраняющих a в начальный момент времени.

Пусть линейный автомат задан равенством

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0.$$

Вход x_i этого автомата называется существенным, если $\mu_i \neq 0$. В случае $\mu_i(0) \neq 0$ вход x_i называется непосредственным.

Множество, состоящее из автоматов $\mathfrak{L}_k$, имеющих не более одного непосредственного входа, обозначим V_1.

Положим далее:

$$V_p = \left\{ \; f \;\mid\; f \in \mathfrak{L}_k, \quad \sum_{\mu \in U(f)} \mu_i(0) = 1 \; \right\}.$$

Для каждого $\Theta^{(1)}$,

$$\Theta^{(1)} \in \Big\{ \; P_s^{(1)}, \;\; M_{i,\omega}^{(1)}, \;\; M_1^{(1)} \;\mid$$
$$s = 1, 2, \ldots, l, \;\; i = 0, 2, 3, \ldots, \;\; \omega \in \Omega_k \; \Big\},$$

через Θ обозначим следующее множество линейных автоматов:

$$\Theta = \Big\{ \; f \;\mid\; f \in \mathfrak{L}_k, \;\; U(f) \subset \Theta^{(1)} \; \Big\}.$$

Тем самым мы получим следующие множества:

$$P_s, \;\; M_{i,\omega}, \;\; M_1,$$

$s = 1, 2, \ldots, l, \;\; i = 0, 2, 3, \ldots, \;\; \omega \in \Omega_k$.

Введем еще множества R_i^e и R_i^d:

$$R_i^e = \{ \; f \;\mid\; f \in \mathfrak{L}_k, \;\; \text{имеет место равенство}$$

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0,$$

если x_j — единственная существенная переменная автомата f,

то $\mu_j \in \tilde{M}_i^{(1)}$, в противном случае: $\mu_j \in R_i^{(1)}, \;\; j = 1, 2, \ldots, n \; \Big\}$,

$$R_i^d = \{\ f\ \mid\ f \in \mathfrak{L}_k,\ \text{имеет место равенство}$$

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} \mu_i x_i + \mu_0,$$

если x_j — единственная непосредственная переменная автомата f,

то $\mu_j \in \tilde{M}_i^{(1)}$, в противном случае: $\mu_j \in R_i^{(1)},\ j = 1, 2, \ldots, n\ \Big\}$,

$i = 0, 2, 3, \ldots$.

Теорема. *Множество* J_k,

$$J_k = \Big\{\ T_a,\ V_1,\ V_p,\ P_s,\ M_{i,\omega},\ M_1,\ R_i^e,\ R_i^d\ \mid$$
$$a \in E_k,\ \ s \in \{1, 2, \ldots, l\},\ \ i \in \{0, 2, 3, \ldots\},\ \ \omega \in \Omega_k\ \Big\},$$

является множеством всех предполных классов в $\mathfrak{L}_k$.

Приведенный здесь перечень предполных классов исправляет результат, опубликованный ранее в работе [10].

Для оценки времени работы алгоритма, проверяющего конечное множество M, $M \subset \mathfrak{L}_k$, на полноту, будем использовать следующие параметры:

- r — количество автоматов в множестве M;
- n — максимальное количество входов в автоматах из M;
- d — максимальная степень дробей из множества $U(M)$,

$$U(M) = \bigcup_{f \in M} U(f),$$

при этом, как принято, для несократимой дроби $\frac{u}{v}$,

$$\deg \frac{u}{v} = \max(\deg u, \deg v);$$

- k — количество элементов поля E_k;
- m — количество автоморфизмов поля E_k.

Теорема. *Алгоритм проверки полноты может быть реализован со сложностью по времени*

$$O(rnk) + O\left(rnd^2 m\right).$$

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов — М.: Наука, 1985. — 320 с.

2. Кудрявцев В. Б. О мощности множеств предполных классов некоторых функциональных систем, связанных с автоматами // Проблемы кибернетики. Вып. 13. — М.: Наука, 1965. — С. 45–74.

3. Кратко М. И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов // ДАН СССР. — М.: 1964. — Т. 155, № 1. — С. 35–37.

4. Буевич В. А. Об алгоритмической неразрешимости распознавания A-полноты для о.-д. функций // Математические заметки. — М.: 1972. — Вып. 6. — С. 687–697.

5. Бабин Д. Н. О классификации автоматных базисов Поста по разрешимости свойств полноты и А-полноты // Доклады РАН. — 1999. — Т. 367, № 4. — С. 439–441.

6. Лидл, Р., Нидеррайтер Г. Конечные поля: в 2 т. — М.: Мир, 1988. — Т. 1. 425 с.

7. Гилл А. Линейные последовательностные машины — М.: Наука, 1974. — 288 с.

8. Часовских А. А. Условия полноты линейно-р-автоматных функций // Интеллектуальные системы. Теория и приложения. — 2014. — Т. 18, вып. 3. — С. 203–252.

9. Часовских А. А. Проблема полноты для класса линейно-автоматных функций // Дискретная математика. — 2015. — Т. 27, № 2. — С. 134–151.

10. Часовских А. А. Приведенные критериальные системы предполных классов в классах линейных автоматов над конечными полями // Интеллектуальные системы. Теория и приложения. — 2018. — Т. 22, вып. 4. — С. 115–134.

КЛАССЫ ГРАФОВ С ОПЕРАЦИЯМИ

М. А. Иорданский (Нижний Новгород)

При изучении классов графов с операциями используется методология исследований, принятая в математической кибернетике. Множества графов с операциями задают класс управляющих систем (УС). Схемы УС описывают процессы построения одних графов из других с помощью теоретико-множественных операций. В роли функций, реализуемых схемами УС, выступают графы, сохраняющие заданные характеристические свойства при выполнении над ними определенных операций. Объектом изучения являются процессы построения графов, взаимосвязь между ограничениями, накладываемыми на используемые операции, и свойствами получаемых при этом графов.

Определения и обозначения. Графы представляют собой сложные комбинаторные объекты, к которым применимы разнообразные операции. Следуя классификации А.А.Зыкова [1], операции над графами можно разбить на три группы:

1. Операции *сборки* (композиции), при выполнении которых из нескольких графов образуется новый граф, в каком-то смысле более сложный, чем каждый из исходных. К таким операциям относятся, например, операции объединения, соединения и произведения графов [38].

2. Операции *разборки*, когда исходный граф превращается в несколько графов, каждый из которых в некотором смысле проще исходного. В качестве примера здесь можно привести операции удаления ребра или вершины вместе с инцидентными ребрами (петлями), являющихся обратными по отношению к операциям сборки.

3. Операции *преобразования* графа, изменяющие его структуру. К ним относятся, например, такие операции, как стягивание ребра или расщепление вершины.

В работе рассматриваются операции первого вида. В качестве операций сборки используются операции *бинарной склейки*. Пусть G_1 и G_2 — графы из исходного запаса или построенные на их основе, содержащие изоморфные подграфы $G_1' \subseteq G_1$ и $G_2' \subseteq G_2$. Объединение графов G_1 и G_2 путем отождествления их изоморфных подграфов G_1' и G_2' реализует операцию склейки графов G_1 и G_2. Пусть отождествляемые подграфы операции склейки изоморфны графу $\tilde{G}$. Для результирующего графа G операции склейки графов G_1 и G_2 по $\tilde{G}$ используется обозначение $G = (G_1 \circ G_2)\tilde{G}$. Подграф $\tilde{G}$ называется *подграфом склейки*.Операция склейки называется *тривиальной*,

если подграф $G'_1 = G_1$ или (и) $G'_2 = G_2$. При этом результирующий граф изоморфен хотя бы одному из графов-операндов.

Введенные операции не являются однозначными. При фиксированных графах-операндах результат операции склейки может зависеть от вида отождествляемых подграфов (рис.1), их выбора в графах-операндах (рис.2) и даже способа отождествления (рис.3).

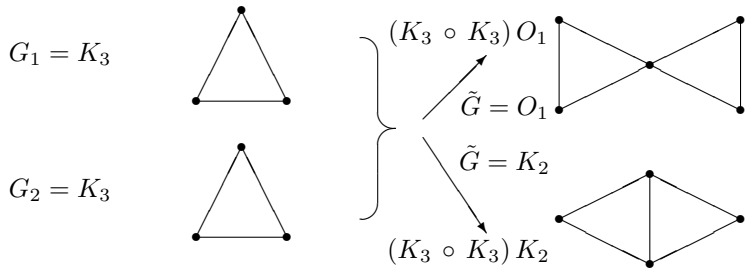


Рис. 1. Результат операции зависит от вида подграфа склейки $\tilde{G}$.

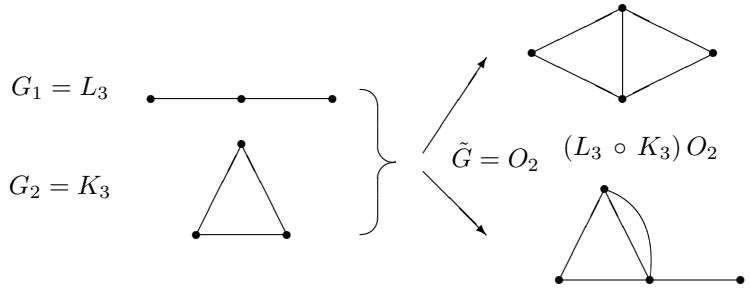


Рис. 2. Результат операции зависит от выбора отождествляемых подграфов O_2 в графах-операндах G_1 и G_2.

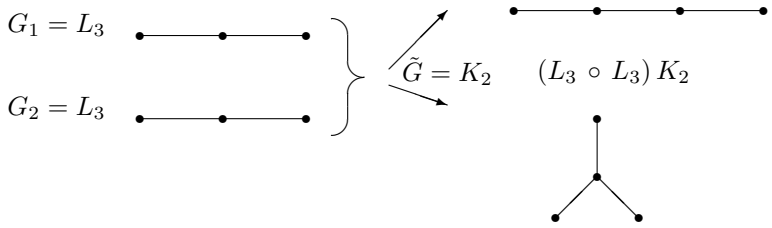


Рис. 3. Результат операции зависит от выбора способа отождествления фиксированных подграфов K_2 графов операндов G_1 и G_2.

Способы порождения и структура замкнутых классов графов. Результирующий граф любой операции склейки, очевидно, сохраняет такие свойства графов-операндов, как отсутствие изолированных вершин, петель и ребер. Для сохранения других характеристических свойств графов необходимо наложение системы H соответствующих ограничений на операции склейки. Операции, удовлетворяющие системе ограничений H, называются операциями *H-склейки.*

Пусть P множество графов, обладающих некоторым характеристическим свойством. Граф G называется *H-суперпозицией* графов из P, если $G \in P$ или G можно получить путем последовательного применения операций H-склейки к графам из P и к графам, полученным из P с помощью операций H-склейки. Процесс построения графа G из графов множества P с помощью операций H-склейки задает *операцию H-суперпозиции* графов из P (операцию H-суперпозиции над P).

Множество $[P]_H$ всех графов, получаемых из P с помощью операций H-суперпозиции, образует *H-замыкание* множества P. Если выполняется равенство $[P]_H = P$, то P называется *H-замкнутым* классом графов.

Подмножество графов $P' \subset P$ образуют *полную систему графов* H-замкнутого класса P, если $[P']_H = P$.

Минимальная по включению полная система графов B_e из P образует *элементный базис* H-замкнутого класса P, если $[B_e]_H = P$. В [2] установлен следующий факт.

Теорема 1. *Каждый H-замкнутый класс графов P имеет единственный элементный базис.*

Доказательство этой теоремы интересно тем, что оно проводится на основе анализа структуры бесконечного ориентированного графа G_H^P, сопоставляемого произвольному H-замкнутому классу графов P. Вершины графа G_H^P соответствуют графам из класса P. Дуга (v_i, v_j), $v_i, v_j \in V(G_H^P)$, $i \neq j$, проводится тогда и только тогда, когда граф G_i, соответствующий вершине v_i, является графом-операндом хотя бы одной нетривиальной операции H-склейки, реализующей граф G_j, соответствующий вершине v_j.

Так как при проведении дуг графа G_H^P учитываются лишь нетривиальные операции склейки, то из конечности рассматриваемых графов следует, что все пути, ведущие в любую вершину графа G_H^P, содержат конечное число разных вершин. В графе G_H^P не может быть контуров, поскольку при этом использовались бы тривиальные операции склейки. Таким образом, все пути, ведущие в любую вершину графа G_H^P, имеют конечную длину. Отсюда следует наличие в графе

G_H^P вершин с полустепенями захода равными нулю, образующими единственный элементный базис H-замкнутого класса P.

Следствие 1. *Мощность множества всех H-замкнутых классов графов континуальна.*

Для доказательства этого факта достаточно выделить счетную последовательность графов, в которой ни один из графов не может быть получен из других графов этой последовательности с помощью операции суперпозиции операций H-склейки. Тогда замыкания всех подмножеств этой последовательности порождают континуум H-замкнутых классов графов. Примером такой последовательности может быть последовательность $C_n, n = 1, 2, ...$

Операции H-склейки с изоморфными подграфами склейки $\tilde{G}$ относятся к одному *типу* операций. Для сохранения операциями H-склейки заданного характеристического свойства графов-операндов необходимо в общем случае накладывать ограничения на вид подграфов склейки, их выбор в графах-операндах и способ отождествления

Ограничение на вид подграфов склейки задается множеством типов операций H-склейки (подграфов $\tilde{G}$), использования которых достаточно для построения всех графов класса P, исходя из графов элементного базиса B_e. Каждому такому множеству соответствует *полная система типов операций* H-склейки. Минимальная по включению полная система типов операций H-склейки образует *операционный базис* B_o класса P.

Из определения полной системы типов операций H-склейки следует, что каждый H-замкнутый класс графов имеет непустое множество A полных систем типов операций H-склейки, так как A содержит, по крайней мере, систему всех типов операций H-склейки. В [3] был получен следующий результат.

Теорема 2. *Каждый H-замкнутый класс графов P имеет операционный базис.*

Доказательство этой теоремы может служить иллюстрацией единства математики дискретной и непрерывной.

Поставим каждому графу G во взаимно-однозначное соответствие натуральное число $n(G)$ так, чтобы никакой граф с большим номером не был бы изоморфен подграфу графа с меньшим номером. Это всегда можно сделать, например, нумеруя графы в порядке неубывания суммы числа их вершин и ребер. Граф, соответствующий числу n, обозначим через $G(n)$.

Каждому множеству графов R можно поставить в соответствие характеристическую десятичную дробь $0, a_1a_2...a_n...$, в которой $a_n = 0$, если $G(n)$ не принадлежит множеству R и $a_n = 1$, если $G(n)$ принадлежит множеству R. При этом множеству A всех

полных систем типов операций H-склейки класса P будет соответствовать некоторое множество вещественных чисел. Система типов операций H-склейки, соответствующая числу $\inf A$, также является полной в H-замкнутом классе графов P. Эта полная система типов операций H-склейки минимальна по включению, так как любое ее собственное подмножество соответствует меньшему числу, а полной системы типов операций, соответствующей числу меньшему $\inf A$ не существует. Таким образом, система типов операций, соответствующая числу $\inf A$, является операционным базисом H-замкнутого класса графов P.

Совокупность элементного и операционного базисов вместе с системой ограничений H на операции склейки определяют *конструктивное описание* класса графов, обладающих заданным характеристическим свойством.

Конструктивный подход к представлению графов О.Б.Лупанов называл «функциональным подходом», имея в виду аналогичную постановку задач выразимости и полноты для функциональных систем с операциями. В этом плане интересно сравнить систему графы с суперпозицией операций склеек с системами функций алгебры (P_2) и k-значной логики $(P_k, k \geq 3)$ с операциями суперпозиции:

1. Каждый замкнутые класс из P_2 имеет конечный базис, в P_k существуют замкнутые классы, не имеющие базиса или не имеющие конечного базиса. Мощность множества всех замкнутых классов в P_2 — счетная, а в P_k — континуальная [4].

2. Каждый H-замкнутый класс графов имеет два вида порождающих базиса: элементный и операционный. В зависимости от характеристического свойства класса графов каждый из порождающих базисов может быть как конечным, так и счетным. При этом один и тот же H-замкнутый класс графов может иметь несколько операционных базисов. Общее число H-замкнутых классов графов континуально.

В P_2 при изучении структуры замкнутых классов важную роль играет понятие предполного класса. Замкнутый класс $R_1 \subset R_2$ называется *предполным* в замкнутом классе R_2, если его замыкание $[R_1] \neq R_2$ но при добавлении к R_1 любого элемента $r \in R_2 \setminus R_1$ замыкание $[R_1 \cup r] = R_2$. Для системы графы с операциями понятие предполного класса оказывается малоинформативным, поскольку все предполные классы графов являются *тривиальным*, не содержащими лишь один граф из соответствующего надкласса. Тривиальность предполных классов следует из того, что графы-операнды изоморфны подграфам результирующего графа любой операции склейки.

Для замкнутых классов графов содержательным является понятие *базисной предполноты*. Класс $\Im_1$ является базисно предполным в $\Im_2$ по элементному базису, если B_e класса $\Im_1$ не содержит одного из графов элементного базиса класса $\Im_2$ и при этом операционные базисы обоих классов совпадают. Аналогично, класс $\Im_1$ является предполным в $\Im_2$ по операционному базису, если B_o класса $\Im_1$ не содержит одного из графов операционного базиса класса $\Im_2$ и при этом элементные базисы обоих классов совпадают.

Конструктивные описания классов графов. Задачи конструктивного описания H-замкнутых классов графов можно разбить на два класса: прямые и обратные задачи.

1. Прямые задачи — заданы характеристические свойства графов, необходимо найти конструктивные описания соответствующих H-замкнутых классов графов.

К настоящему времени получены конструктивные описания для H-замкнутых классов всех графов, мультиграфов, обыкновенных графов, триангулированных, планарных, двудольных, расщепляемых, эйлеровых, гамильтоновых, а также для графов с различными комбинациями указанных свойств [2, 5–9].

В системы ограничений H на операции склейки накладывались как *внутренние ограничения*, обеспечивающие лишь сохранение требуемого характеристического свойства (свойств), так и *внешние ограничения*, оказывающих дополнительное влияющие на вид подграфов склейки, их выбор в графах операндах и способ отождествления. Наличие внешних ограничений оказывает существенное влияние на сложность конструктивных описаний.

Например, класс обыкновенных графов при использовании только внутренних ограничений имеет конечные порождающие базисы, а при добавлении внешнего ограничения — требования, чтобы отождествляемые подграфы были порожденными, оба базиса становятся счетными.

Для класса обыкновенных связных планарных графов с внутренними ограничениями на операции склейки имеем $|B_e| = |B_o| = 2$. При последовательном добавлении внешних ограничений, требующих, чтобы вершины подграфов склейки образовывали разделяющие множества в результирующих графах, минимальные разделяющие множества, минимальные разделяющие множества с минимальным числом ребер в подграфах склейки, получаем $|B_e| = 4$, а операционный базис $|B_o| = 5; 15; 21$.

Класс эйлеровых графов имеет счетные порождающие базисы, а при добавлении требования, чтобы графы были также и планарные, операционные базисы становятся конечными, но их число возрастает

до трех.

2. Обратные задачи — заданы конструктивные описания H-замкнутых классов графов, необходимо определить характеристические свойства графов. Была построена решетка всех базисно предполных замкнутых классов графов, порождаемых подмножествами элементного и операционного базисов замкнутого класса всех графов [10].

Теорема 3. *В H-замкнутом классе всех графов $\Im$ содержится 35 нетривиальных замкнутых подклассов, являющихся базисно предполными в своих надклассах.*

Для каждого из этих классов было установлено их характеристическое свойство. В таблице приведены свойства для нетривиальных замкнутых подклассов связных графов. Число вершин и ребер в графах (подграфах) обозначаются соответственно через $N(n)$ и $M(m)$

$B_e \setminus B_o$	O_1, O_2	O_2	O_1
O_1, C_1, K_2	Все связные графы	Граф C_1 или мультиграфы с $N \leq 2$	Графы без циклов C_n, $n \geq 2$
C_1, K_2	Графы с $M \geq 1$	Граф C_1 или мультиграфы с $N = 2$	Графы с $M \geq 1$ без циклов C_n, $n \geq 2$
O_1, K_2	Мультиграфы	Мультиграфы с $N \leq 2$	Деревья
K_2	Мультиграфы с $N \geq 2$	Мультиграфы с $N = 2$	Деревья с $N \geq 2$
O_1, C_1	—	—	Графы с $N = 1$
C_1	—	—	Графы с $N = 1$ и $M \geq 1$

Характеристические свойства формулируются на основе анализа типов операций склейки, используемых при построении графов. Графы, представляющие собой объединение графов G_1 и G_2 без пересечения, реализуются операциями $(G_1 \circ G_2)\, O_0$. Графы, получа-

ющиеся добавлением ребра к текущему графу G, реализуются операциями $(G \circ K_2)\, O_2$. Графы, получающиеся добавлением петли к текущему графу G, реализуются операциями $(G \circ C_1)\, O_1$. Графы, получающиеся добавлением ребра с вершиной к текущему графу G, реализуются операциями $(G \circ K_2)\, O_1$ или $((G \circ O_1)\, O_0 \circ K_2)\, O_2$.

В качестве элементных базисов выбираются всевозможные подмножества графов из B_e, а в качестве операционных — минимальные по включению подмножества графов из B_o, задающих типы операций, применимых к суперпозициям графов выбранных элементных базисов.

Минимальность по включению означает, что замкнутый класс с тем же характеристическим свойством нельзя получить, используя любые собственные подмножества из B_o. Подмножествам графов из B_o, не удовлетворяющих указанным ограничениям для выбранных элементных базисов, соответствуют пустые клетки в таблице.

На основе конструктивных описаний H-замкнутых классов графов можно классифицировать характеристические свойства графов: чем больше ограничений необходимо использовать для сохранения заданного свойства, тем оно считается «слабее» и наоборот.

Так, графы из H-замкнутых классов таблицы обладают наиболее «сильными» характеристическими свойствами — для их конструктивного описания достаточно задания конечных элементных и операционных базисов. Для сохранения других характеристических свойств графов, в общем случае, требуются ограничения не только на порождающие базисы, но также на выбор отождествляемых подграфов в графах-операндах и сам способ отождествления.

Задачи синтеза графов. Использование при построении графов операций склейки вносит избыточность в задание информации о графе, позволяя за счет этого единообразно формулировать ограничения на операции с целью сохранения различных свойств графов. Это обстоятельство приводит к постановке задач синтеза графов, минимизирующих величину избыточности задания.Оценки величин избыточности конструктивных описания для классов эйлеровых и гамильтоновых графов можно найти в работах [11–13].

Наличие нескольких операционных базисов для ряда классов графов позволяет ставить задачи синтеза в более традиционной постановке. Например, необходимо построить граф, используя минимальное число операций склейки.

Учитывая сложность задач физико-математического суперкомпьютерного моделирования, возникающих при проектировании графов большой размерности, актуальными становятся задачи синтеза графов с помощью унарных операций расклейки. Эти операции

можно отнести к операциям преобразования графов. При их выполнении производится дублирование некоторых подграфов графа с полным или частичным сохранением их окрестностей в исходном графе. Такие операции называются *операциями клонирования* [14]. Вид клонируемых подграфов определяется техническими ограничениями. Здесь задача синтеза ставится так: на основе исходного графа небольшой размерности необходимо построить граф большой размерности за минимальное числа операций клонирования. Такая задача рассматривается для деревьев и двудольных графов в статье автора, включенной в данный сборник по секции «Теория графов».

Отмечу в заключение, что материал из многих цитировавшихся выше работ можно найти в монографии [15].

Список литературы

1.Зыков А. А. Теория конечных графов. — Новосибирск: Наука. Сибирское отделение, 1969. — 543с.

2.Иорданский М. А. Конструктивные описания графов // Дискретный анализ и исследование операций. — 1996. — Т. 3, № 4. — С. 35–63.

3.Бурков Е. В. Операционные базисы замкнутых классов графов // Материалы IX международного семинара «Дискретная математика и её приложения», Москва, 18–23 июня 2007г. — М.: Изд-во мехмата МГУ. — 2007. — С. 105–116.

4. Яблонский С. В. Введение в дискретную математику. — М.: Наука., 2001. — 354с.

5. Иорданский М. А. Конструктивные описания двудольных графов // Проблемы теоретической кибернетики. Тезисы докладов XV Международной конференции (Казань, 2–7 июня 2008г.). — Казань: Отечество. — 2008. — С. 44.

6. Иорданский М. А. Конструктивные описания расщепляемых графов // Материалы X Международного семинара «Дискретная математика и её приложения» (Москва, МГУ, 1–6 февраля 2010 г.) — М.: Изд-во механико-математического факультета МГУ. — 2010. — С. 306–308.

7.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.: Издательский отдел факультета ВМиК МГУ им. М.В.Ломоносова,2004. — С. 167–169.

8. Иорданский М. А. Конструктивные описания гамильтоновых графов // Вестник Нижегородского государственного университета. Математика. — 2012. — № 3(1). — С. 137–140.

9. Бурков Е. В. Конструктивные описания планарных и эйлеровых графов // Вестник Нижегородского государственного университета. Математика. — 2010. — № 5(1). — С. 165–170.

10. Иорданский М. А. Конструктивная классификация графов // Моделирование и анализ информационных систем. — 2012. — Т.19, № 4. — С. 144–153.

11. Иорданский М. А. Избыточность конструктивных описаний гамильтоновых планарных графов // Материалы XI Международного семинара "Дискретная математика и её приложения"(Москва, МГУ, 18-22 июня 2012 г.) — М.: Изд-во механико-математического факультета МГУ. — 2012. — С. 285–288.

12. Иорданский М. А. Избыточность конструктивных описаний эйлеровых графов // Проблемы теоретической кибернетики. Материалы XVII Международной конференции (Казань,16-20 июня 2014г.). — Казань: Отечество, 2014. — С. 115–116.

13. Иорданский М. А. Избыточность конструктивных описаний (r,s)-деревьев // Дискретные модели в теории управляющих систем: IX Международная конференция, Москва и Подмосковье, 20–22 мая 2015 г. — М.: МАКС Пресс, 2015. — С. 90–91.

14. Иорданский М. А. Клонирование графов // Проблемы теоретической кибернетики: XVIII международная конференция (Пенза, 19-23 июня 2017 г.). — М.: МАКС Пресс, 2017, — С. 108–110.

15. Иорданский М. А. Конструктивная теория графов и ее приложения. — Н.Новгород: Кириллица, 2016. — 172 с.

О ТЕОРЕМЕ КЕМПЕ И ВОПРОСАХ ГЕОМЕТРИИ ШАРНИРНЫХ КОНСТРУКЦИЙ

М. Д. Ковалёв (Москва)

Доклад состоит из двух частей. Первая посвящена теореме Кемпе о возможности черчения по частям произвольной плоской алгебраической кривой шарниром плоского шарнирного механизма. Абстрактными математиками[1] недавно был высказан ряд претензий к рассуждениям Кемпе. Я постараюсь показать, что эти претензии и заявления об ошибках Кемпе несправедливы. Геометрическая привлекательность теории шарнирных конструкций отнюдь не ограничивается вопросами, сосредоточенными вокруг теоремы Кемпе. Во второй части речь пойдёт о других и новых важных вопросах из этой области, имеющих на мой взгляд несомненный геометрический интерес. Круг этих вопросов не пересекается с вопросами, затронутыми в тезисах «О проекциях конфигурационных пространств шарнирных механизмов», помещёнными в этом сборнике.

Определения понятий, которыми я буду пользоваться, приведены в вышеупомянутых тезисах. Здесь я на них буду опираться, но повторять не стану.

О теореме Кемпе. В 1876 ученик Артура Кэли Альфред Кемпе опубликовал статью «Об общем методе черчения шарнирным механизмом плоских кривых n-ой степени» [1]. С тех пор считалось, что он доказал теорему о возможности начертить по частям произвольную плоскую алгебраическую кривую с помощью шарнирных механизмов. Однако, работа Кемпе не содержит формулировок каких-либо теорем. И это даёт возможность различной её трактовки, что впоследствии и произошло. После всплеска в девятнадцатом веке интереса математиков к шарнирным конструкциям, связанного с нуждами техники, наступило длительное затишье. Его прервал в 1970-х известный американский математик У. Тёрстон, обративший внимание на теорему Кемпе. В своих докладах он формулировал эффектное утверждение: можно соорудить шарнирный механизм, подделывающий вашу подпись. Хотя Тёрстон не публиковал статей по механизмам, но его выступления вдохновили других. Начиная с 1998 года появились работа М. Каповича и Дж. Миллсона [2], а также ряд статей Г. Кинга [3–5], посвящённых истолкованию результата Кемпе на языке современной алгебраической геометрии. Их авторы утверждали, что рассуждения Кемпе содержат существенные пробелы и даже ошибки, и это мнение получило распространение среди математиков [6, 7]. Но при анализе претензий к Кемпе вскрывается их

[1] Себя к абстрактным математикам я не отношу.

надуманность. По существу, абстрактные математики приписывают Кемпе свою формулировку его результата, и указывают на недостаточность его аргументов для доказательства их теоремы.

Корень возникших претензий и недоразумений лежит в нетрадиционной трактовке абстрактными математиками понятия механизма. Как классический образец приведу определение шарнирного механизма, данное Д. Гильбертом в его лекциях [8] по наглядной геометрии: «Плоским шарнирным механизмом называется всякая плоская система жестких стержней, частично соединенных между собой или скрепленных с неподвижными точками плоскости, вокруг которых они могут вращаться, так что вся система еще сохраняет подвижность в ее плоскости». Это общепринятое определение не является математическим. Его достаточно для ответа на вопрос: является ли данная конструкция из жестких стержней плоским шарнирным механизмом? Но оно не дает способа описания индивидуального механизма и различения механизмов между собой.

В соответствии с этим классическим пониманием я определяю конфигурационное пространство шарнирного механизма как неодноточечную компоненту связности полного прообраза $F^{-1}(\mathbf{d})$ точки $\mathbf{d}$(КШС) при рычажном отображении. Соответственно, шарнирный механизм есть конструкция с таким связным множеством положений. Основное свойство механизма состоит в том, что его можно непрерывно (не разбирая и заново собирая) переводить из одного его положения в любое другое его положение. По своей природе механизмы предназначены для передачи движения от одной своей части к другой. Другой основной класс конструкций в инженерии называется фермами. Их нельзя непрерывно двигать не нарушая связей их элементов.

Абстрактные же математики определяют конфигурационное пространство шарнирного механизма как полный прообраз[2] $F^{-1}(\mathbf{d})$ точки $\mathbf{d}$. У них «механизмом» является и простейшая жёсткая плоская конструкция из свободного шарнира p_1, соединённого рычагами с двумя закреплёнными шарнирами p_2 и p_3. Конфигурационное про-

[2]Вот определение шарнирного механизма по Г.Кингу [3] (механизм рассматривается в плоскости C комплексного переменного): An abstract linkage is a finite graph L with a positive number $l(vw)$ assigned to each edge vw. A planar realization of an abstract linkage (L, l) is a mapping φ from the vertices of L to C so that $|\varphi(v) - \varphi(w)| = l(vw)$ for all edges vw. If L is a finite graph, we let $V(L)$ denote the set of vertices of L and let $E(L)$ denote the set of edges of L. We will often wish to fix some of the vertices of a linkage whenever we take a planar realization. So we say that a linkage L is a foursome (L, l, V, μ) where (L, l) is an abstract linkage, $V \supset V(L)$ is a subset of its vertices, and $\mu : V \to C$. So V is the set of fixed vertices and μ tells where to fix them. The configuration space of realizations is defined by: $C(L) = \{\varphi : V(L) \to C \mid \varphi(v) = \mu(v)$ if $v \in V$, and $|\varphi(v) - \varphi(w)| = l(vw)$ for all edges $vw\}$.

странство этого «механизма» состоит из двух точек, которым отвечают зеркально симметричные относительно прямой p_2p_3 фермы.

Доказательство Кемпе. Хотя Кемпе и не формулировал теоремы, мы приведём его результат в виде «наивной» теоремы. Как его понимали дольше века.

Теорема. *Всякий достаточно малый кусок произвольной плоской алгебраической кривой представляет собой множество положений шарнира плоского шарнирного механизма, движущегося с одной степенью свободы.*

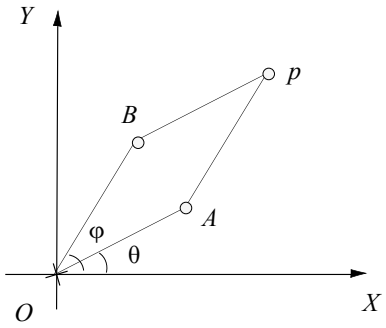


Рис. 1:

Доказательство Кемпе состоит в указании способа построения нужного механизма из простейших механизмов-кирпичиков, выполняющих определённые алгебраические действия. Чтобы построить кривую $f(x,y) = \sum_{kl} A_{kl}x^k y^l = 0$ Кемпе берёт шарнирный ромб (рис. 1) с рычагами $|OA| = |OB| = a$ постоянной длины. Координатная система выбрана так, что точка p, лежащая на этой кривой, не совпадает с её началом O. Пусть $\angle XOA = \theta$, $\angle XOB = \varphi$. Тогда координаты точки p:

$$\begin{aligned} x &= a(\cos\theta + \cos\varphi) \\ y &= a\left(\cos\left(\theta - \frac{\pi}{2}\right) + \cos\left(\varphi - \frac{\pi}{2}\right)\right). \end{aligned}$$

Подставляя эти выражения в уравнение кривой, и применяя формулу $\cos\alpha\cos\beta = \frac{1}{2}\left[\cos(\alpha-\beta)+\cos(\alpha+\beta)\right]$, Кемпе приходит к уравнению вида

$$f(x,y) = \sum_{r,s} B_{rs}\cos(r\varphi + s\theta + \chi_{rs}) = C, \tag{1}$$

где r, s — целые не равные нулю одновременно, $B_{rs} > 0$, C — постоянная, зависящая от A_{kl}, a, а χ_{rs}— постоянный угол.

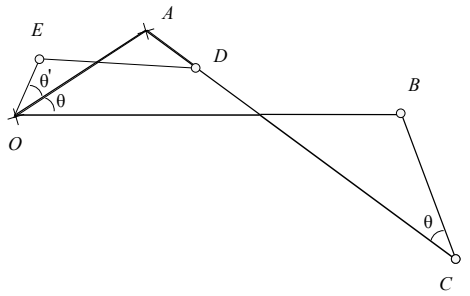


Рис. 2:

Далее дело сводится к последовательному сложению векторов длин B_{rs}, образующих с осью OX углы $r\varphi+s\theta+\chi_{rs}$ для чего используются механизмы умножителя и накопителя углов, и переносчика векторов [1, 7]. На рис. 2 изображён удвоитель угла, в его состав входят два антипараллелограмма, то есть самопересекающихся четырёхугольника с равными противоположными сторонами. Переносчик состоит из двух параллелограммов с общей стороной. Таким образом, строится цепочка рычагов с начальным шарниром p_j в точке

p и конечным шарниром p_K. Если совместить этот конечный шарнир p_K с шарниром прямолинейно-направляющего механизма Поселье, движущимся по вертикали $x = C$, то мы получим требуемый механизм Кемпе.

Результаты современных работ. Алгебраическим множеством называем множество общих нулей совокупности многочленов относительно переменных — декартовых координат точки в R^k. *Аналитический изоморфизм* подмножеств евклидовых пространств есть гомеоморфизм, осуществляемый сужениями аналитических (т.е. представимых покоординатно локально сходящимися степенными рядами) отображений.

Теорема (Kapovich, Millson)**.** *Для любого компактного алгебраического множества $X \subset R^k$ найдётся КШС, конфигурационное пространство которой аналитически изоморфно конечному набору непересекающихся копий множества X.*

В отличии от результата Кемпе эта теорема имеет характер результата «в целом». Её доказательство опирается на видоизменённый метод Кемпе построения нужного механизма из простейших.

Получен и следующий результат. Рассмотрим кусок K полиномиально параметризованной кривой $f : [a, b] \to R^2$.

Теорема (Kapovich, Millson)**.** *Кривая K может быть прочерчена шарниром подходящим образом выбранного плоского шарнирного механизма, а именно, закон движения этого шарнира есть $f(t), a \leq t \leq b$.*

Поскольку любую непрерывную на отрезке $[a, b]$ функцию можно сколь угодно точно приближать многочленом, то утверждение Тёрстона в случае подписи, рисуемой без отрыва ручки от листа бумаги, сводится к этой теореме.

Анализ претензий к Кемпе. Попытаемся формализовать результат Кемпе. Пусть K — конфигурационное пространство КШС $\mathbf{d}$, а K_i — конфигурационное пространство плоского шарнирного механизма, отвечающего этой КШС, то есть неодноточечная компонента связности K. И пусть K_i^j — множество положений j-го шарнира механизма K_i. Иными словами, K_i^j есть проекция конфигурационного пространства K_i механизма на плоскость R_j^2 положений j-го шарнира.

Теорема, которую проще всего было бы сформулировать на основе работы Кемпе, звучит так.

Теорема. *Для произвольной плоской алгебраической кривой A, и точки $p \in A$ найдутся окрестность U точки p и механизм с*

шарниром p_j, *для которого* $K_i^j \cap U = A \cap U$.

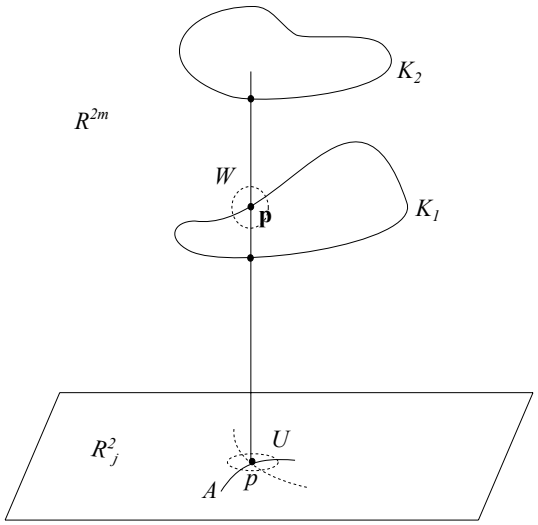


Рис. 3: На рисунке положению j-го шарнира p отвечают два положения шарнирного механизма K_1 и одно положение механизма K_2.

Главное затруднение заключается в том, что в точку p могут проектироваться (рис. 3) различные точки конфигурационного пространства механизма K_i, а также точки конфигурационных пространств других механизмов с этой же кинематической схемой. Естественно, может оказаться $K_i^j \cap U \supset A \cap U$, и тем более $K^j \cap U \supset A \cap U$, где K^j — проекция K на плоскость положений j-го шарнира. И тогда эта теорема окажется неверной.

С последней возможностью вынуждены бороться те, кто принимает точку зрения на конфигурационное пространство шарнирного механизма, внедряемую абстрактными математиками. Такое пони-

мание конфигурационного пространства механизма игнорирует его кинематическую природу. Если мы чертим кривую A шарниром p_j механизма K_i, нас совершенно не волнует, попадёт ли шарнир p_j другого механизма с той же кинематической схемой в начальную точку p кривой A. Ведь мы же не сможем перейти к другому механизму непрерывно двигая механизм K_i! Возможность $K_i^j \cap U \supset A \cap U$, однако, остаётся.

Наиболее естественной теоремой, учитывающей кинематическую природу задачи, является следующая. Пусть наш механизм имеет m свободных шарниров, а значит $K \subset R^{2m}$, и пусть шарнирник $\mathbf{p} \in F^{-1}(\mathbf{d})$.

Теорема. *Для произвольной плоской алгебраической кривой A, и точки $p \in A$ найдётся механизм с шарниром p_j и такая окрестность $U \subset \mathbb{R}^2$ точки p, а также окрестность $W \subset R^{2m}$ шарнирника $\mathbf{p}$, что $\pi(K_i \cap W) = A \cap U$, где π — проекция на плоскость положений шарнира p_j.*

Из этой теоремы следует, что в случае связности $A \cap U$ каждая точка из $A \cap U$ достигается шарниром p_j при непрерывном и небольшом движении механизма, а именно движении, не выводящем его из окрестности W.

Такая формулировка отметает основную претензию к рассуждениям Кемпе, заключающуюся в том, что антипараллелограммы могут вытягиваться и распрямляясь переходить в параллелограммы. И наоборот, шарнирный параллелограмм распрямляясь переходит в антипараллелограмм (рис. 4). Что может привести к появлению положений чертящего шарнира, не лежащих на алгебраической кривой, которую мы взялись чертить. Чтобы избежать таких паразитных положений современные авторы добавляют укрепляющие рычаги, препятствующие переходам параллелограмм - антипараллелограмм. Последнее особенно существенно при доказательстве теорем о конфигурационном пространстве в целом. Например, параллелограмм можно укрепить, добавив к нему рычаг, соединяющий шарниры, расположенные в серединах его противоположных сторон (рис. 4).

Вторая претензия относится к справедливости рассуждений Кемпе в особых точках алгебраической кривой. Она высказана в [2] без каких-либо разъяснений. В этих точках кривая может ветвиться, что, например, не имеет места для движения чертящего шарнира в теореме о подписи. На мой взгляд, эта претензия не обоснована. Действительно, в точке p ветвления алгебраической кривой, которую мы чертим методом Кемпе, наблюдается интересное кинематическое явление. Движение от чертящего шарнира p_j механизма к его шар-

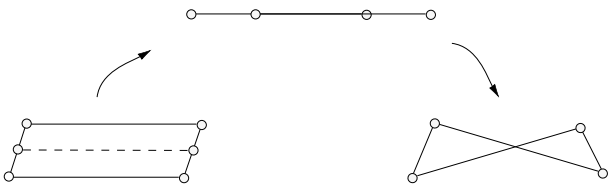


Рис. 4: Рычаг, обозначенный пунктиром, предотвращает переход параллелограмма в антипараллелограмм.

ниру p_K (см. доказательство Кемпе), принадлежащему инверсору Поселье и перемещающемуся по отрезку прямой, передаётся с однозначной определённостью. В то время, как движение в обратном направлении от p_K к p_j передаётся неоднозначно, с точностью до выбора ветви кривой в точке $p \in R^2$. Но это не означает, что в точке ветвления p рассуждения Кемпе не справедливы.

Приведём пример. Возьмём шарнирный ромб со стороной единичной длины, и вершиной в начале координат (рис. 5). Будем строить

методом Кемпе на этом ромбе механизм, шарнир p_j которого, совпадающий с вершиной ромба, чертит кривую $x(y-1)=0$. Пусть $\angle XOA=\theta$, $\angle XOB=\varphi$.

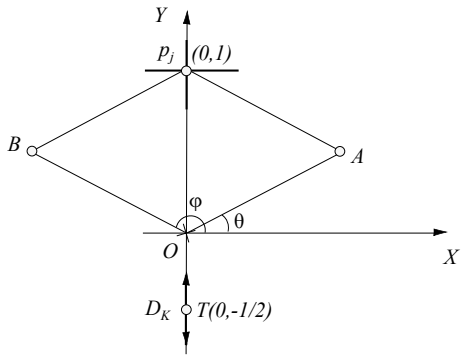


Рис. 5:

Подставляя выражения координат шарнира p_j через углы в уравнение $x(y-1)=0$, придём к уравнению

$$\frac{1}{2}\cos\left(2\varphi-\frac{\pi}{2}\right)+\frac{1}{2}\cos\left(2\theta-\frac{\pi}{2}\right)+\cos\left(\varphi+\theta-\frac{\pi}{2}\right)+$$
$$+\cos(\varphi+\pi)+\cos(\theta+\pi)=0.$$

Когда шарнир p_j, отвечающего этому уравнению механизма Кемпе, находится в точке $(0,1)$, шарнир p_K лежит в точке $T=\left(0,-\frac{1}{2}\right)$. Если сдвигать шарнир p_j по оси OY, то шарнир p_K будет перемещаться вверх от точки T. На рис. 6а сплошной линией показано изменение ординаты шарнира p_K в зависимости от смещения шарнира p_j. Если сдвигать шарнир p_j по прямой $y=1$, то шарнир p_K

будет смещаться вниз от точки T. Зависимость смещения p_K от такого смещения шарнира p_j показана сплошной линией на рис. 6b. Пунктиром на обоих рисунках показано постоянное нулевое значение абсциссы шарнира p_K. Итак, при ненулевой скорости движения шарнира p_j, в точке T скорость шарнира p_K равна нулю. Движение механизма из положения $\mathbf{p}$, в котором шарнир p_K лежит в точке T, существенно неоднозначно. Если шарнир p_K двигать из положения $\mathbf{p}$ вверх, то шарнир p_j движется по вертикали. Если шарнир p_K двигать из положения $\mathbf{p}$ вниз, то шарнир p_j движется по горизонтали. Однако, например, при движении p_K из положения $\mathbf{p}$ вниз шарнир p_j может начать двигаться как влево, так и вправо. И если механизм находился в покое в положении $\mathbf{p}$, то совершенно неясно, — в какую сторону он начнёт двигаться? Заметим ещё, что при приближении шарнира p_K к точке T двигать этот шарнир будет всё труднее, ибо постоянной ненулевой скорости его движения должна отвечать неограниченно возрастающая скорость движения шарнира p_j.

Имеется ещё третья претензия [9] к рассуждениям Кемпе, состоящая в том, что его построения выполнялись для острых углов. Она легко преодолима. Достаточно начало координат в доказательстве теоремы Кемпе взять так далеко от точки p, а ромб настолько вытянутым, чтобы углы φ, θ были так малы, что все их кратные в уравнении (1) лежали, скажем, в интервале $\left(-\frac{\pi}{4}, \frac{\pi}{4}\right)$. Максимальная кратность углов φ, θ в уравнении (1) равна степени N многочлена, задающего кривую. Если в теореме Кемпе ограничиться малыми движениями, то появление распрямлённых параллелограммов становится невозможным. А распрямление антипараллелограммов возможно лишь для механизма накопителя при сложении углов, величины которых случайно совпали. Чтобы избежать этого, достаточно взять угол θ много меньшим угла φ, например, $\varphi > 2N\theta$. Чего можно добиться поворотом системы координат. Беря теперь такую окрестность $U \subset R^2$ точки p, чтобы для ромба с вершиной в произвольной точке $p' \in U$ выполнялись условия $N(\varphi + \theta) < \frac{\pi}{3}$ и $\varphi > N\theta$, мы можем быть уверены, что все антипараллелограммы механизмов-кирпичиков механизма Кемпе не распрямляются при движении шарнира p_j внутри U.

С этими уточнениями первоначальные рассуждения Кемпе представляют собой полное доказательство его теоремы. Или простыми словами того, что произвольную ограниченную и связную часть алгебраической кривой можно без лишних точек вычертить шарнирным механизмом при его непрерывном движении.

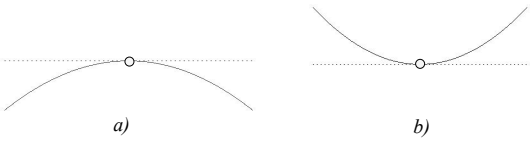


Рис. 6: Кружочком обозначено положение шарнира p_K, в котором он совпадает с точкой T.

Геометрические вопросы теории шарнирных конструкций. Вопросы, связанные с теоремой Кемпе, отнюдь не исчерпывают интересные геометрические вопросы относительно шарнирных конструкций. В настоящее время здесь остаётся открытым ряд фундаментальных вопросов. Перечислим некоторые из них.

ВОПРОС 1. В общем случае, если мы не сосредоточиваемся на изучении шарнирного механизма, на ШСС шарнирной конструкции не накладывается условие 4, также ШСС может не содержать закреплённых шарниров. В этом случае говорят о реализациях связного графа в плоскости. Пусть $F : R^{2m} \to \mathcal{R}^r$ — рычажное отображение, отвечающее этому графу (ШСС в плоскости без закреплённых шарниров). Если для какого-либо шарнирника $\mathbf{p} \in R^{2m}$ строки мат-

рицы $dF(\mathbf{p})$ дифференциала рычажного отображения, отвечающие некоторому набору рёбер (рычагов), линейно независимы, то этот набор рёбер (рычагов) будем называть независимым в плоских реализациях графа (ШСС).

Теорема (Поллячек-Гейрингер, Ламан)**.** *Рёбра графа G в R^2 независимы тогда и только тогда, когда G удовлетворяет условию: для любой непустой совокупности E рёбер графа G, с числом рёбер в ней $|E|$, число $|V|$ инцидентных им вершин удовлетворяет неравенству $|E| \leq 2|V| - 3$.*

Вопрос нахождения подобного структурного критерия независимости рёбер для графа (ШСС) в трёхмерном пространстве до сих пор остаётся открытым. Теорема аналогичная вышеприведённой не имеет места [10, 11].

ВОПРОС 2. Рассматриваем ЗШС в R^2, и отвечающее ей рычажное отображение F. Пусть ранг дифференциала $dF(\mathbf{p})$ равен l на множестве $M_l \subset R^{2m}$. В известных примерах множество M_l в случае положительной размерности является неограниченным [12]. Всегда ли это так?

ВОПРОС 3. Рассматриваем ЗШС в плоскости и отвечающее ей рычажное отображение $F : R^{2m} \to \mathcal{R}^r$. Допустим, что размерность $\dim F(R^{2m}) = r$. Возможна ли однократная точка отображения F внутри его образа $F(R^{2m})$? То есть, такая внутренняя точка $\mathbf{d} \in F(R^{2m})$, что $F^{-1}(\mathbf{d})$ состоит лишь из одной точки $\mathbf{p} \in R^{2m}$. Иными словами, существует ли геометрически устойчивая КШС $\mathbf{d}$, которой бы отвечала единственная шарнирная ферма? Под геометрической устойчивостью КШС я понимаю [11, 13] существование шарнирника, отвечающего произвольной достаточно мало изменённой по отношению к исходной КШС. В противном случае КШС называется геометрически неустойчивой.

ВОПРОС 4. Плоский шарнирник $\mathbf{p}$ называем *геометрически устойчивым* [11, 13], если для любой его ε-окрестности $O(\mathbf{p}, \varepsilon) \subset R^{2m}$ найдется δ-окрестность $O(\mathbf{d}, \delta) \subset \mathcal{R}^r$ точки $\mathbf{d} = F(\mathbf{p})$, целиком лежащая в образе $F(O(\mathbf{p}, \varepsilon))$. Если достаточно мало изменить длины рычагов геометрически устойчивого шарнирника, то шарнирник с измененными длинами рычагов можно будет собрать таким образом, что все его шарниры окажутся близки к соответствующим шарнирам исходного шарнирника. Из неустойчивости КШС $\mathbf{d}$, очевидно, следует неустойчивость любого шарнирника $\mathbf{p} \in F^{-1}(\mathbf{d})$. Открыт следующий естественный вопрос. Возможна ли устойчивая КШС $\mathbf{d}$, для которой каждый шарнирник $\mathbf{p} \in F^{-1}(\mathbf{d})$ неустойчив?

Список литературы

1. Kempe A. B. On a general method of describing plane curves of the n^{th} degree by Linkwork // Proc. of the London Math. Soc. — 1876. — V. 7, no. 102. — C. 213–216.

2. Kapovich M., Millson J. J. Universality theorems for configurations of planar linkages // Topology. — 2002 — V. 41, no. 6. — P. 1051–1107.

3. King Henry C. Planar Linkages and Algebraic Sets // arXiv.org:math/9807023.

4. King Henry C. Semiconfiguration spaces of planar linkages // arXiv.org:math/9810130.

5. King Henry C. Configuration Spaces of Linkages in R^n // arXiv.org:math/9811138.

6. Demaine E., O'Rourke J. Geometric Folding Algorithms: Linkages, Origami, Polyhedra. — Cambridge University Press, 2007.

7. Ошемков А. А., Попеленский Ф. Ю., Тужилин А. А., Фоменко А. Т., Шафаревич А. И. Курс наглядной геометрии и топологии. — М.: ЛЕНАНД, 2015.

8. Гильберт Д., Кон-Фоссен С. Наглядная геометрия. — М.: Наука, 1981.

9. Power S. Elementary proofs of Kempe universality // arXiv.org: 1511.09002v2.

10. Graver J., Servatius B., Servatius H. Combinatorial Rigidity. — American Mathematical Society, Providence, 1993.

11. Ковалёв М. Д. Геометрическая теория шарнирных устройств // Известия РАН Серия математ. — 1994. — Т. 58, № 1. — С. 45–70.

12. Ковалёв М. Д. Некоторые свойства рычажных отображений // Фундаментальная и прикладная математика. — 2006. — Т. 12, № 1. — С. 1–14.

13. Ковалёв М. Д. Вопросы геометрии шарнирных устройств и схем // Вестник МГТУ, Серия Машиностроение. — 2001. — № 4. — С. 33–51.

БУЛЕВЫ ПРЕОБРАЗОВАНИЯ БЕРНУЛЛИЕВСКИХ СЛУЧАЙНЫХ ВЕЛИЧИН

А. Д. Яшунский (Москва)

Задача получения одних дискретных случайных величин из других посредством некоторого класса преобразований, которые можно условно считать «алгебраическими», рассматривается в математической кибернетике уже давно: первые работы в подобной постановке относятся к концу 50-х — началу 60-х годов XX века. Достаточно рано в качестве отдельной задачи обособились исследования комбинационных преобразований случайных величин, которые в отличие от, например, модельных устройств, рассматривавшихся в работах Дж. фон Неймана [1] и А. Гилла [2], оперировали не с потенциально бесконечной последовательностью случайных величин, а с набором случайных аргументов фиксированной длины, и вычисляли от этого набора функцию из некоторого класса. Одним из первых подобные преобразования систематически исследовал Р. Л. Схиртладзе [3]. В его работах, а также в дальнейших исследованиях особое внимание уделялось случаю, когда преобразуемые случайные величины — бернуллиевские, принимающие значения 0 и 1, а преобразующие функции — булевы из некоторого класса.

Примечательно, что первым модельным объектом, осуществляющим преобразования бернуллиевских случайных величин, были не непосредственно булевы функции, а так называемые *вероятностные сети*: двухполюсные сети, в которых каждое ребро проводит сигнал с некоторой вероятностью, значение которой принадлежит заданному множеству начальных распределений. Несложно заметить, что если каждому ребру сети приписать свою булеву переменную, то вероятность обращения в 1 функции проводимости при подстановке вместо ее переменных случайных величин будет в точности равна вероятности проводимости сети. Наиболее простым для анализа подмножеством вероятностных сетей являются параллельно-последовательные сети. Эквивалентный им класс преобразующих булевых функций состоит из всех функций, бесповторно выразимых с помощью операций конъюнкции и дизъюнкции.

При исследовании подобных задач естественным образом возникает соответствие между булевыми функциями и функциями, преобразующими бернуллиевские распределения. Каждое такое распределение — вектор $(1-p, p)$ с неотрицательными компонентами. Его вторая компонента однозначно определяет первую, поэтому далее говоря о бернуллиевских распределениях можем отождествлять их с числами из отрезка $[0; 1]$. При подстановке в булеву функцию

$f(x_1, \ldots, x_n)\colon \{0,1\}^n \to \{0,1\}$ независимых в совокупности бернуллиевских случайных величин с распределениями $p_1, \ldots, p_n \in [0;1]$ вероятность обращения результата в 1 равна

$$\widehat{f}(p_1, \ldots, p_n) = \sum_{f(\sigma_1,\ldots,\sigma_n)=1} \pi(p_1, \sigma_1) \cdots \pi(p_n, \sigma_n),$$

где $\pi(p,0) = 1-p$, $\pi(p,1) = p$. Функцию $\widehat{f}(p_1, \ldots, p_n)\colon [0;1]^n \to [0;1]$ будем называть *индуцированной* функцией. Несложно заметить, что индуцированная функция полилинейно (т. е. линейно по каждому аргументу при фиксировании остальных) доопределяет функцию f с вершин n-мерного единичного куба на его внутренность.

Отождествление переменных превращает индуцированную функцию $\widehat{f}(p_1, \ldots, p_n)$ в многочлен $h_f(p)$, который часто называют *характеристическим* для функции f. Он выражает вероятность получения единичного значения при подстановке в функцию f независимых одинаково распределенных случайных величин, обращающихся в 1 с вероятностью p. Такие многочлены также возникают в задачах построения надежных управляющих систем из ненадежных элементов, см., в частности, работу Э. Ф. Мура и К. Э. Шеннона [4]. Качественно отличаясь от задач преобразования случайных величин, эти задачи, тем не менее, иногда имеют с ними общие элементы не только на уровне определений.

В задачах о преобразованиях случайных величин весьма естественно возникает понятие *алгебры распределений*: множества распределений, замкнутого относительно преобразований некоторым набором индуцированных функций. По-видимому, впервые в этих терминах задачу описания преобразований случайных величин рассмотрел Ф. И. Салимов в [5]. Если задано множество булевых функций B и некоторое начальное множество распределений $G \subseteq [0;1]$, то наименьшая по включению алгебра, замкнутая относительно индуцированных функций $\widehat{B} = \{\widehat{f} \mid f \in B\}$ и содержащая G, есть в точности то множество распределений, которое может быть получено из G с помощью функций из B. Будем обозначать это множество $V_B(G)$. В простейших случаях оно может быть описано явно. Так, в частности, $V_{\{\oplus\}}(\{p\}) = \{\frac{1}{2}(1-(1-2p)^n)\}_{n\in\mathbb{N}}$.

Помимо множеств распределений, которые могут быть получены точно, можно также рассматривать множества распределений, которые могут быть приближены с любой наперед заданной точностью комбинациями случайных величин с распределениями из G, подставленными в булевы функции из B. Такие распределения образуют

аппроксимационную алгебру, будем обозначать ее $W_B(G)$. Она получается из алгебры $V_B(G)$ путем топологического замыкания (т. е. добавления всех предельных точек). В силу непрерывности индуцированных функций аппроксимационные алгебры также замкнуты относительно операций из $\widehat{B}$.

Для фиксированного множества преобразующих функций B всевозможные алгебры распределений при их частичном упорядочении по отношению включения образуют решетку. Наибольшим элементом в такой решетке для любой системы операций B будет множество всех распределений — отрезок $[0;1]$. При этом аппроксимационные алгебры будут подрешеткой в решетке всех алгебр. Естественно, что полное описание решетки алгебр для любого заданного множества B позволило бы отвечать на вопросы о возможности точного получения или аппроксимации распределений при любом множестве начальных распределений. Несмотря на то, что бернуллиевский случай, по-видимому, самый простой в классе задач о преобразованиях случайных величин на конечных множествах, исследования решеток алгебр бернуллиевских распределений далеки от завершения. Тем не менее, получен ряд результатов, существенно расширяющих наши представления об устройстве этих решеток алгебр.

Для различных систем преобразующих функций решетки алгебр распределений оказываются взаимосвязаны. В частности, если $B' \subseteq B''$, то любое множество, замкнутое относительно $\widehat{B''}$, будет также замкнутым относительно $\widehat{B'}$. Оказывается (по-видимому, первым это отметил Ф. И. Салимов, см., например, [6]), что для любой системы B решетка алгебр в точности совпадает с решеткой алгебр, соответствующей системе $[B]_0$ — бесповторному замыканию B, т. е. множеству функций, которые выразимы бесповторными формулами над системой $B \cup \{x\}$, где x — тождественная функция. Таким образом, всевозможные системы, у которых бесповторные замыкания совпадают, оказываются эквивалентными с точки зрения задач преобразования и приближения случайных величин.

Системы булевых функций можно частично упорядочить по отношению включения их бесповторных замыканий. Элементами этого частичного порядка будут, в частности, все замкнутые классы булевых функций, содержащие тождественную функцию (клоны). При этом, естественно, любая решетка алгебр для более сильной (т. е. большей в смысле построенного частичного порядка) системы булевых функций будет частью решетки алгебр для любой более слабой системы. Наиболее слабой системой является множество монотонных функций существенно зависящих от одной переменной, для

которого решетка алгебр состоит из произвольных подмножеств отрезка $[0;1]$.

Для дальнейшего изложения введем следующие обозначения классов булевых функций (через $[B]$ обозначаем замыкание системы B по суперпозиции, $d_n(x_1,\ldots,x_n) = \bigvee\limits_{1\leqslant i<j\leqslant n} x_ix_j$, d_n^* — двойственная к d_n функция): $MU = [\{x\}]$ — монотонные функции, существенно зависящие от одной переменной; $U = [\{\overline{x},1\}]$ — функции, существенно зависящие от одной переменной; $K = [\{\&,0,1\}]$ — конъюнкции; $D = [\{\vee,0,1\}]$ — дизъюнкции; $L = [\{\oplus,1\}]$ — линейные функции; $O^\infty = [\{\to\}]$; $O^\mu = [\{\to,d_{\mu+1}\}]$; $I^\infty = [\{\overline{x_1}x_2\}]$; $I^\mu = [\overline{x_1}x_2, d^*_{\mu+1}]$; $SM = [\{d_3\}]$ — самодвойственные монотонные функции; $S = [\{d_3,\overline{x}\}]$ — самодвойственные функции; $T_0 = [\{\&,\oplus\}]$ — функции, сохраняющие 0; $T_1 = [\{\vee,\sim\}]$ — функции, сохраняющие 1; $P_2 = [\{\&,\overline{x}\}]$ — множество всех булевых функций.

По-видимому, наиболее изученной является подрешетка алгебр рациональных распределений, т. е. подмножеств множества $[0;1]\cap\mathbb{Q}$. Пусть $\mathcal{P}$ — множество всех простых чисел. Для $R\subseteq\mathcal{P}$ через $\Gamma[R]$ обозначим множество всех несократимых дробей, у которых в разложении знаменателя на простые множители встречаются только числа из R. Из определения индуцированных функций легко видеть, что для любого $R\subseteq\mathcal{P}$ множество $\Gamma[R]$ замкнуто относительно преобразований любыми индуцированными функциями.

Ф. И. Салимов в 1988 г. показал [6], что для системы $B = \{0,1,x_1x_2\vee\overline{x_1}x_3\}$ (и, следовательно, для любой более сильной системы) верхняя часть подрешетки алгебр рациональных распределений состоит только из множеств $\Gamma[R]$.

В случае $B = P_2$ этот результат был доведен до окончательного Р. М. Колпаковым. Для описания нижней части подрешетки рациональных распределений определим дополнительно следующие множества. Пусть $R\subseteq\mathcal{P}$ и $T\subset\mathbb{N}$, причем каждый элемент $t\in T$ взаимно прост со всеми элементами $r\in R$. Положим

$$\Gamma[R;T] = \left\{ \frac{m}{n}\in\Gamma[R] \;\middle|\; \begin{array}{l} \exists T'\subseteq T\colon \tau_1 = \prod\limits_{t\in T'} t,\ \tau_2 = \prod\limits_{t\in T\setminus T'} t, \\ m\equiv 0\,(\mathrm{mod}\ \tau)_1,\ m\equiv n\,(\mathrm{mod}\ \tau)_2 \end{array} \right\},$$

где допускаются пустые произведения, которые по определению считаются равными единице. В 2001 г. Р. М. Колпаков показал [7], что при преобразованиях случайных величин произвольными булевыми функциями рациональными подалгебрами бернуллиевских распределений являются всевозможные множества $\Gamma[R;T]$ и только они.

Для произвольных (не обязательно рациональных) распределений имеющиеся результаты касаются преимущественно аппроксимационных алгебр. Одним из исключений можно считать полученную А. Д. Яшунским в 2018 г. следующую характеризацию конечных алгебр распределений [8]:

Теорема. *Если* $V_B(G) = G$ *и* $|G| < \infty$, *то имеет по крайней мере одно из следующих утверждений*: (1) $G \subseteq \{0,1\}$; (2) $B \subseteq U$; (3) $G = \{p\}$, *где* $p \in [0;1]$ — *алгебраическое число*; (4) $G \subseteq \{0, \frac{1}{2}, 1\}$ *и* $B \subseteq L$.

Аппроксимационные алгебры устроены несколько проще, чем произвольные алгебры распределений. Еще в 1966 г. Р. Л. Схиртладзе установил [9], что существуют системы, в которых любое начальное распределение $p \neq 0, 1$ позволяет приблизить любое другое распределение.

Теорема. *Для* $p \neq 0, 1$ *выполнено* $W_{\{\&,\vee,\overline{x}\}}(\{p\}) = [0;1]$.

Это утверждение было усилено в 2006 г. А. Д. Яшунским [10] и в 2012 г. независимо Дж. Браком с соавторами [11], которые показали, что для $p \neq 0, 1$ выполнено $W_{\{\&,\vee\}}(\{p\}) = [0;1]$. Таким образом, как минимум для всех систем, содержащих $[\{\&, \vee\}]_0$, решетка аппроксимационных алгебр содержит выше алгебры $\{0,1\}$ только алгебру всех распределений $[0;1]$. Такие системы будем называть *аппроксимационно полными*.

В работе [10] было также установлено, что если $B \not\subseteq K, D, L$, то для аппроксимационной полноты системы B необходимо и достаточно выполнения условия $W_B(\{p\}) \ni 0, 1$ при всех $p \neq 0, 1$. В то же время несложно проверить, что $W_K(\{p\}) = \{p^n\}_{n\in\mathbb{N}} \cup \{0,1\}$, $W_D(\{p\}) = \{1-(1-p)^n\}_{n\in\mathbb{N}} \cup \{0,1\}$, $W_L(\{p\}) = \{\frac{1}{2}(1-(-1)^c(1-2p)^n)\}_{n\in\mathbb{N},c\in\{0,1\}}$, откуда вытекает, что никакие подсистемы систем K, D или L не могут быть аппроксимационно полными. Таким образом по своей аппроксимирующей силе системы функций делятся на заведомо слабые, и те, где аппроксимационная полнота зависит от возможности приближения 0 и 1.

В работах [12, 13] А. Д. Яшунским было получено полное описание решеток алгебр распределений для всех классов булевых функций, не содержащихся в классах K, D, L. Отметим, что ряд вспомогательных утверждений в этих работах перекликается с вспомогательными утверждениями из работы С. Г. Гиндикина и А. А. Мучника [14], посвященной построению надежных схем из ненадежных функциональных элементов. Хотя доказательство соответствующего утверждения и нетривиально, описание решеток ал-

гебр распределений для замкнутых классов булевых функций оказывается устроено достаточно просто.

Теорема. *Пусть* $B = [B]$ *и* $B \not\subseteq K, D, L$. *Если* $W_B(G) = G$ *и* $G \neq \varnothing$, *то* G *может быть только одним из следующих множеств*: (1) $\{0,1\}$ *или* $[0;1]$; (2) $\{0\}$, *если* $B \subseteq T_0$, $\{1\}$, *если* $B \subseteq T_1$; (3) $\{\frac{1}{2}\}$, *если* $B \subseteq S$; (4) $[0;p]$, *если* $p \leqslant 1 - \frac{1}{\mu}$ *и* $B \subseteq I^\mu$, $[p;1]$, *если* $p \geqslant \frac{1}{\mu}$ *и* $B \subseteq O^\mu$.

Примечательно, что все перечисленные в теореме алгебры оказываются выпуклыми. Их рассмотрение показывает, что, по-видимому, имеет смысл несколько расширить определение аппроксимационно полных систем. В частности, таковыми, вероятно, также следует считать все системы, которые содержат класс S (а точнее даже содержат множество $[\{d_3, \overline{x}\}]_0$), поскольку от аппроксимационно полных систем они отличаются только наличием дополнительной подалгебры $\{\frac{1}{2}\}$. Кроме того, может быть оправдано выделение какого-то класса *слабо аппроксимационно полных* систем, в которых аппроксимация произвольного распределения возможна при достаточно общих условиях на множество начальных распределений. Одним из вариантов может быть выделение таких систем B, для которых существует конечное множество G, удовлетворяющее равенству $W_B(G) = [0;1]$.

Если бесповторное замыкание системы B содержит один из классов I^∞, SM, O^∞, то описанная выше структура алгебр для замкнутых классов дает достаточно много информации об устройстве алгебр для системы B, хотя и не позволяет полностью их описать. Основные не решенные к настоящему моменту проблемы, касающиеся аппроксимационных алгебр, относятся к системам, лежащим между классами K, L, D с одной стороны и I^∞, SM, O^∞ с другой стороны. В отношении подсистем классов K, D и L при этом понятно, что все конечно порожденные алгебры могут быть относительно просто описаны, а бесконечно порожденные алгебры могут иметь весьма замысловатую структуру. Одним из путей дальнейших исследований, на котором получено некоторое продвижение, является рассмотрение нижней части решеток аппроксимационных алгебр для различных систем. Здесь оказывается полезным изучение множеств предельных точек алгебр распределений.

Напомним, что точка q называется *предельной* для множества $G \subseteq [0;1]$, если для любого $\varepsilon > 0$ найдется элемент $g \in G$, удовлетворяющий условиям $0 < |q - g| < \varepsilon$. Будем обозначать множество предельных точек множества G через $\lambda(G)$.

Очевидно, что в нижней части решетки расположены алгебры с малым числом предельных точек. В частности, приведенная выше

характеризация конечных алгебр распределений может также рассматриваться как описание алгебр, у которых число предельных точек равно нулю. Следующим естественным шагом является рассмотрение алгебр с единственной предельной точкой. А. Д. Яшунским в 2018 г. показано [15], что такие алгебры должны удовлетворять весьма жестким условиям.

Теорема. *Если* $W_B(G) = G$ *и* $\lambda(G) = \{q\}$*, то выполнено одно из следующих утверждений:* (1) $B \subseteq MU$; (2) $q = 0$ *и* $B \subseteq K$; (3) $q = 1$ *и* $B \subseteq D$; (4) $q = \frac{1}{2}$ *и* $B \subseteq L$.

Эта теорема, кроме прочего показывает, что среди всех систем булевых функций, только подсистемы K, D или L приводят к некоторому подобию «закона больших чисел», при котором результат многократного применения операций из системы B к случайным величинам с начальными распределениями из произвольного конечного множества приближается к некоторому стационарному распределению. При этом предельное распределение оказывается непосредственно связанным с тем, какие операции используются.

Основное следствие теоремы о единственности предельной точки для классификации аппроксимирующих свойств систем булевых функций заключается в том, что во всех достаточно сильных системах алгебры с единственной предельной точкой невозможны. Естественно задаться вопросом о наличии алгебр с каким-то другим конечным числом предельных точек. Ответ на этот вопрос дает следующая теорема, доказанная А. Д. Яшунским в [16].

Теорема. *Если* $W_B(G) = G$ *и* $|\lambda(G)| < \infty$*, то либо* $B \subseteq U$*, либо* $|\lambda(G)| < 2$.

Следовательно, никакие системы функций, за исключением весьма тривиальных, не могут иметь алгебр распределений с двумя, тремя и т. д. предельными точками. Для всех систем, которые не содержатся в K, D или L любая алгебра либо конечна, либо имеет не менее чем счетное множество предельных точек. Примеры континуальных множеств предельных точек в изобилии предоставляются алгебрами, индуцированными замкнутыми классами. Вместе с тем, примеры алгебр, у которых множество предельных точек в точности счетно, также имеются: таковыми, например являются алгебры $W_{\{d_3\}}(\{p\})$ при $p \neq 0, \frac{1}{2}, 1$.

Результаты исследований на настоящий момент позволяют выделить ряд вопросов и проблем, рассмотрение которых представляет интерес с точки зрения развития общей теории алгебр бернуллиевских распределений. Перечислим некоторые из них.

1. Для систем $B \neq P_2$ и начальных распределений $G \subseteq [0;1] \cap \mathbb{Q}$ описать алгебры, отличные от $V_{P_2}(G) \cap W_B(G)$ (на примере си-

стемы $B = \{\&, \vee\}$ можно показать, что такие алгебры существуют).

2. Описать одноэлементные алгебры распределений: по-видимому, далеко не любое алгебраическое число из отрезка $[0; 1]$ может образовывать одноэлементную алгебру.
3. Найти условия (необходимые, достаточные) для выполнения включения $0, 1 \in W_B(G)$.
4. Описать решетки аппроксимационных алгебр для систем функций, содержащих один из классов I^∞, SM, O^∞.

Список литературы

1. von Neumann J. Various techniques used in connection with random digits // Natl. Bur. Stand. Appl. Math. Ser. V. 12. Monte Carlo method. — 1951. — P. 36–38.

2. Gill A. Synthesis of probability transformers // J. Franklin Inst. — 1962. — V. 274, N 1. — P. 1–19 [Имеется перевод: Кибернетический сборник. Вып. 8. — М.: Мир, 1964. — С. 91–114].

3. Схиртладзе Р. Л. О синтезе p-схемы из контактов со случайными дискретными состояниями // Сообщ. АН ГрузССР. — 1961. — Т. 26, № 2. — С. 181–186.

4. Moore E. F., Shannon C. E. Reliable circuits using less reliable relays // J. Franklin Inst. — 1956. — V. 262, N 3. — P. 191–208; N 4. — P. 281–297 [Имеется перевод: Кибернетический сборник. Вып. 1. — М., ИЛ, 1960. — С. 109–148].

5. Салимов Ф. И. Об одной системе образующих для алгебр над случайными величинами // Изв. вузов. Математика. — 1981. — № 5. — С. 78–82.

6. Салимов Ф. И. Об одном семействе алгебр распределений // Изв. вузов. Математика. — 1988. — № 7. — С. 64–72.

7. Колпаков Р. М. Замкнутые классы булевых случайных величин с рациональнозначными распределениями // Математические вопросы кибернетики. Вып. 10. — М.: Физматлит, 2001. — С. 215–224.

8. Яшунский А. Д. Конечные алгебры бернуллиевских распределений // Дискретная математика. — 2018. — Т. 30, № 2. — С. 148–161.

9. Схиртладзе Р. Л. О методе построения булевой величины с заданным распределением вероятностей // Дискретный анализ. Вып. 7. — Новосибирск: ИМ СО АН СССР, 1966. — С. 71–80.

10. Яшунский А. Д. О преобразованиях вероятности бесповторными булевыми формулами // Материалы XVI Международной школы-семинара «Синтез и сложность управляющих си-

стем» (Санкт-Петербург, 26–30 июня 2006 г.) — М.: Механико-математический ф-т МГУ им. М. В. Ломоносова, 2006. — С. 150–155.

11. Zhou H., Loh P.-L., Bruck J. The synthesis and analysis of stochastic switching circuits. arXiv: 1209.0715v1 [cs.IT] (2012).

12. Яшунский А. Д. Преобразования бернуллиевских распределений булевыми функциями из замкнутых классов // Препринты ИПМ им. М. В. Келдыша. — 2016. — № 38.

13. Yashunsky A. D. Clone-induced approximation algebras of Bernoulli distributions // Algebra universalis. — 2019. — V. 80, N 5. — P. 1–16.

14. Гиндикин С. Г., Мучник А. А. Решение проблемы полноты для систем функций алгебры логики с ненадежной реализацией // Проблемы кибернетики. Вып. 15. — М.: Наука, 1965. — С. 65–84.

15. Яшунский А. Д. Алгебры бернуллиевских распределений с единственной предельной точкой // Препринты ИПМ им. М. В. Келдыша. — 2018. — № 135.

16. Яшунский А. Д. О предельных точках алгебр бернуллиевских распределений // Препринты ИПМ им. М. В. Келдыша. — 2018. — № 270.

СИНТЕЗ, СЛОЖНОСТЬ И НАДЕЖНОСТЬ УПРАВЛЯЮЩИХ СИСТЕМ

О СВОЙСТВЕ КОЛЛИЗИЯ УСТОЙЧИВОСТИ КВАНТОВОЙ ФУНКЦИИ

М. Ф. Аблаев (Казань)

Используемые определения, обозначения и результаты о квантовой хеш-функции приведены в работах [1, 2].

В данной работе дается формализация понятия коллизия ϵ-усойчивости квантовой хеш-функции. В рамках такой формализации формулируется теорема, в которой доказывается верхняя оценка вероятности коллизии ϵ-устойчивой квантовой функции. Свойство коллизия устойчивости является одним из центральных (наряду с однонаправленностью) свойств хеш-функций.

Напомним, что криптографическая хеш-функция — это словарная сжимающая функция (в алфавите Σ слова длины k отображаются в короткие слова длины m)

$$h : \Sigma^k \to \Sigma^m, \quad (k > m).$$

Функция h должна удовлетворять (как минимум) следующим требованиям.

- Хеш-функция h должна быть однонаправленной (точнее «условно однонаправленной» на сегодняшний день).
- Хеш-функция h должна быть стойкой к коллизиям первого рода: для заданного сообщения w должно быть «вычислительно сложно» подобрать другое сообщение v, для которого $h(w) = h(v)$.
- Хеш-функция h должна быть стойкой к коллизиям второго рода: должно быть «вычислительно сложно» подобрать пару сообщений (w, v) такую, что $h(w) = h(v)$.
- Функция h должна удовлетворять лавинному эффекту (avalanche effect): изменение одного символа аргумента должно вызывать изменение в среднем половины выходных символов (лавинное изменение).

Для множества $(\mathcal{H}^2)^{\otimes s}$ квантовых s кубитных состояний функцию

$$\psi : \Sigma^k \to (\mathcal{H}^2)^{\otimes s}$$

будем называть классически-квантовой (сокращенно просто квантовой) функцией.

В [1, 2] квантовая хеш-функция определяется как квантовая функция, обладающая свойствами, подобными свойствам классическим криптографическим хеш-функций. А именно, определяются понятия однонапрвленности (one-way) и коллизия устойчивости квантовой хеш-функции. В частности, свойство коллизия устойчивости формулируется так:

Определение. Для $0 \leq \epsilon \leq 1$ квантовую функцию ψ будем называть коллизия ϵ-устойчивой (ϵ-resistant), если для каждой пары w, w' различных элементов из Σ^k скалярное произведение состояний $|\psi(w)\rangle, |\psi(w')\rangle$ удовлетворяет неравенству

$$|\langle\psi(w)|\psi(w')\rangle| \leq \epsilon.$$

Состояния $|\psi(w)\rangle$ и $|\psi(w')\rangle$ будем называть ϵ-ортогональными.

В основе решениия проблем коллизия устойчивости классических хеш-функций лежат, в частности, следующие факты. Коллизии реально существуют и имеются (многократные) возможности сравнения значений функции.

В определении квантовой коллизия ϵ-устойчивости требуется, чтобы различные элементы $w, w' \in \Sigma^k$ порождали ϵ-ортогональные состояния. Это означает, что коллизий в квантовом случае в общепринятом смысле не существует. А именно, разные элементы $w, w' \in \Sigma^k$ порождают различные квантовые состояния (образы) $|\psi(w)\rangle$ и $|\psi(w')\rangle$. Однако, коллизия возникает, если по элементу $w \in \Sigma^k$ порождено квантовое состояние $|\psi(w)\rangle$, а при анализе состояния $|\psi(w)\rangle$ оно воспринимается наблюдателем как квантовое состояние $|\psi(w')\rangle$, порожденное другим элементом w'. Этот факт можно интерпретировать, как появление коллизии.

Мы предлагаем следующую формализацию описанного выше.

- Определим событие $Collision_\psi(w, w')$ как следующее событие. По элементу $w \in \Sigma^k$ функцией ψ порождено квантовое состояние $|\psi(w)\rangle$, а при анализе состояния $|\psi(w)\rangle$ оно воспринимается как состояние $|\psi(w')\rangle$, порожденное элементом $w' \in \Sigma^k$.
- Обозначим $Pr(Collision_\psi(w, w'))$ вероятность такого события $Collision_\psi(w, w')$.

В рамках такой формализации справедлива следующая

Теорема. *Для $0 \leq \epsilon \leq 1$, для коллизия ϵ-устойчивой квантовой функции ψ, для каждой пары w, w' различных элементов из $\mathbb{X}$ выполняется*

$$Pr(Collision_{\psi}(w, w')) \leq \epsilon^2.$$

Идея доказательства. В доказательстве теоремы используется следующее. Вероятность $Pr(Collision_{\psi}(w, w'))$ такой коллизии рассчитается на основе закона Борна. Закон Борна — один из ключевых принципов квантовой механики — рассчитывает вероятность того, что измерение квантовой системы позволит получить какой-либо результат. Закон Борна в формулировке книги [3] (раздел 9.2) формулируется так. Вероятность обнаружить систему в состоянии $|\phi\rangle$ при условии, что она была приготовлена в состоянии $|\psi\rangle$, задаётся квадратом модуля скалярного произведения этих состояний.

$$F(\phi, \psi) = |\langle\phi|\psi\rangle|^2.$$

Эту величину называют фиделити (fidelity). В работе показывается, что вероятность $Pr(Collision_{\psi}(w, w'))$ коллизии оценивается величиной $F(\phi, \psi)$ фиделити.

Обсуждение. В силу теоремы имеем, что для для коллизия ϵ-устойчивой квантовой функции ψ верно следующее.

- Вероятности обнаружения коллизий первого и второго рода ограничены величиной ϵ^2.
- Функция ψ удовлетворяет лавинному эффекту в следующем смысле. Изменение одного символа слова $w \in \Sigma^k$ дает другое слово $w' \in \Sigma^k$. При этом квантовые состояния $|\psi(w)\rangle$ и $|\psi(w')\rangle$ являются ϵ-ортогональными, т.е. “сильно отличимы” в соответствии с теоремой. Это можно интерпретировать как факт того, что изменение одного символа аргумента ведет к значительному («лавинному») изменению значения функции.
- На основе теоремы формулируются процедуры, которые применяются в протоколе квантовой аутентификации

Список литературы

1. Аблаев Ф. М., Аблаев М. Ф. Квантовое криптографическое хеширование // Материалы XII Международного семинара «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (20-25 июня 2016 г.). — М.: Изд-во механико-математического факультета МГУ, 2016. — С. 58–63.

2. Аблаев М. Ф. О построении квантовых хеш-функций // Труды IX Международной конференции «Дискретные модели в теории

управляющих систем» МГУ, (20-22 мая 2015 г). — МГУ, 2016. — С. 8–9.

3. Mark M. Wilde. Quantum Information Theory. — Cambridge University Press, 2 edition, 2017.

НИЖНЯЯ ОЦЕНКА БИЛИНЕЙНОЙ СЛОЖНОСТИ УМНОЖЕНИЯ МАТРИЦ РАЗМЕРОВ 2×2 И $2 \times m$ НАД КОНЕЧНЫМИ ПОЛЯМИ

В. Б. Алексеев, А. А. Назаров (Москва)

Поскольку с конца 1980-х годов не удается существенно улучшить оценку $O\left(n^{2.38}\right)$ для сложности умножения матриц порядка n, большой интерес вызывает исследование различных вопросов, связанных с алгоритмами умножения матриц.

Билинейный алгоритм для задачи умножения матрицы $||a_{ij}||$ размера $p \times n$ на матрицу $||b_{kl}||$ размера $n \times m$ над полем F состоит в вычислении d выражений вида (здесь t — индекс, а не степень):

$$(\sum_{i=1}^{p}\sum_{j=1}^{n}\alpha_{ij}^{t}a_{ij})(\sum_{k=1}^{n}\sum_{l=1}^{m}\beta_{kl}^{t}b_{kl}), t = \overline{1,d},$$

таких, чтобы из них линейными комбинациями можно было получить все билинейные формы

$$\sum_{j=1}^{n} a_{ij}b_{jl}, i = \overline{1,p}, l = \overline{1,m}$$

(все коэффициенты берутся из F). Число d называется *сложностью* этого алгоритма, а минимально возможное d по всем билинейным алгоритмам для этой задачи называется ее *билинейной сложностью*.

Данная работа посвящена получению нижних оценок билинейной сложности умножения матриц. Этот вопрос активно исследовался в работах [1–7].

У обычного алгоритма умножения матрицы размера 2×2 на матрицу размера $2 \times m$ билинейная сложность равна, очевидно, $4m$. Из

алгоритма Штрассена [8] известно, что билинейная сложность умножения матрицы 2×2 на матрицу 2×2 не больше 7. Следовательно, разбивая матрицу $2 \times m$ на блоки 2×2 (при нечетном m останется еще один блок 1×2) и, перемножая поблочно, мы получим сложность $\frac{7}{2}m$ при четном m и $\frac{7}{2}(m-1)+4 = \frac{7}{2}m+\frac{1}{2}$ при нечетном m. Это верхняя оценка билинейной сложности данной задачи. В [1] доказано, что для поля из 2 элементов верхняя оценка дает точное значение при любом натуральном m. Для произвольных полей в [2, 3, 5] доказано, что эта верхняя оценка дает точное значение при $m \leq 4$.

Для $m \geq 5$ в [6] получена нижняя оценка над произвольным полем: $3m + 2$. Основным результатом данной работы является следующая теорема.

Теорема. *Билинейная сложность умножения матрицы размера 2×2 на матрицу размера $2 \times m$ над конечным полем с K элементами не меньше, чем $\left(3 + \frac{3}{K^2+2}\right) \cdot m$.*

Доказательство вытекает из следующих утверждений. Пусть F — конечное поле с K элементами. Пусть L — множество всех матриц размера 2×2 с элементами из F, на котором рассматриваются операции сложения матриц в поле F и умножение матриц на элементы из F. Тогда L — линейное пространство над F (размерности 4).

Пусть L_1 — 2-мерное линейное подпространство в L, порожденное матрицами $\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}$ и $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$, а L_2 — 2-мерное линейное подпространство в L, порожденное матрицами $\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}$ и $\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$. Пусть P и Q — любые матрицы ранга 2 из L. Положим $PL_1Q = \{PAQ | A \in L_1\}$ и $PL_2Q = \{PAQ | A \in L_2\}$. Будем называть 2-мерное линейное подпространство L' в L подпространством типа 1 (соответственно, типа 2), если существуют матрицы P и Q ранга 2 такие, что $L' = PL_1Q$ (соответственно, $L' = PL_2Q$).

Лемма. *Пусть имеется d_1 матриц ранга 1 и d_2 матриц ранга 2 из L. Тогда найдется подпространство типа 1, которому принадлежат не менее $\frac{d_1}{(K+1)^2} + \frac{d_2}{K^2-1}$ из этих матриц, и подпространство типа 2, которому принадлежат не менее $\frac{d_1}{K+1}$ из этих матриц.*

Пусть задан некоторый билинейный алгоритм сложности d для умножения матрицы размера 2×2 на матрицу размера $2 \times m$ над полем F. Тогда коэффициенты α_{ij}^t (см. определение билинейного алгоритма) можно рассматривать как d матриц размера 2×2 над полем

F, то есть d матриц из пространства L.

Лемма. *Если в билинейном алгоритме сложности d для умножения матрицы размера 2×2 на матрицу размера $2 \times m$ среди первых линейных форм имеются k таких, что их матрицы принадлежат одному подпространству типа 1, то $d \geq 3m + k$, а если среди первых линейных форм имеются k таких, что их матрицы принадлежат одному подпространству типа 2, то $d \geq 3m + \frac{k}{2}$.*

Рассмотрим некоторый билинейный алгоритм сложности d для умножения матрицы размера 2×2 на матрицу размера $2 \times m$ над полем F. Пусть в нем среди первых линейных форм имеются pd таких, что их матрицы имеют ранг 1, и $(1-p)d$ таких, что их матрицы имеют ранг 2. Тогда из двух предыдущих лемм получаем: $d \geq 3m + \frac{pd}{(K+1)^2} + \frac{(1-p)d}{K^2-1}$ и $d \geq 3m + \frac{pd}{2(K+1)}$. Отсюда $\frac{3m}{d} \leq \min\{1 - \frac{1}{K^2-1} + \frac{2p}{(K+1)^2(K-1)}, 1 - \frac{p}{2(K+1)}\}$. С ростом p первая функция под минимумом возрастает, а вторая убывает, и их графики пересекаются при $p = \frac{2K+2}{K^2+3}$. В этой точке правая часть неравенства достигает максимума, равного $\frac{K^2+2}{K^2+3}$. Поэтому при любом p имеем: $\frac{3m}{d} \leq \frac{K^2+2}{K^2+3}$ и $d \geq \left(3 + \frac{3}{K^2+2}\right) \cdot m$.

Эта оценка улучшает оценку $d \geq 3m + 2$ при $m \geq \frac{2K^2+4}{3}$.

Работа первого автора выполнена при поддержке РФФИ (проект 17-01-00782-а).

Список литературы

1. Hopcroft J. E., Kerr L. R. On minimazing the number of multiplications necessary for matrix multiplication // Technical report No. 69-44. — September 1969. — Department of Computer Science, Cornell University, Ithaca, New York.

2. Winograd S. On multiplication of 2×2 matrices // Linear Algebra and Appl. — 1971. — V. 4. — P. 381–388.

3. Alekseyev V. B. On the comlexity of some algorithms of matrix multiplication // Journal of Algorithms. —1985. — V. 6, no. 1. — P. 71–85.

4. Blaser M., On the complexity of the multiplication of matrices of small formats // J. Complexity. — 2003. — V. 19, no. 1. — P. 43–60.

5. Алексеев В. Б., Смирнов А. В. О точной и приближенной билинейных сложностях умножения матриц размеров 4×2 и 2×2 // Современные проблемы математики. — 2013. — Вып. 17. — С. 135–152.

6. Алексеев В. Б. О билинейной сложности умножения матриц

$m \times 2$ и 2×2 // Чебышевский сборник. — 2015. — Т. 16, вып. 4. — С. 11–27.

7. Landsberg J. M. New lower bounds for the rank of matrix multiplication // SIAM J. Comput. — 2014. — V. 43, no. 1. — P. 144–149.

8. Strassen V. Gaussian elimination is not optimal // Numer. Math. — 1969. — V. 13. — P. 354–356. [Имеется перевод: Штрассен В. Алгоритм Гаусса не оптимален // Кибернетический сборник, вып. 7. М.: Мир, 1970. С. 67–70].

О НАДЕЖНОСТИ СХЕМ В БАЗИСЕ, СОДЕРЖАЩЕМ СУЩЕСТВЕННУЮ ЛИНЕЙНУЮ ФУНКЦИЮ

М. А. Алехина, О. Ю. Барсукова, Т. А. Шорникова (Пенза)

Рассмотрим реализацию булевых функций схемами из ненадежных функциональных элементов в полном конечном базисе B, содержащем линейную функцию $l(x_1, ..., x_k)$ $(k \geq 2)$, существенно зависящую не менее чем от двух переменных. Считаем, что схема реализует булеву функцию $f(x_1, x_2, \ldots, x_n)$ $(n \in \mathbf{N})$, если при поступлении на входы схемы двоичного набора $\tilde{a}^n = (a_1, a_2, ..., a_n)$ при отсутствии неисправностей на выходе схемы появляется значение $f(\tilde{a}^n)$. Допустим, что все элементы схемы независимо друг от друга с вероятностью ε $(0 < \varepsilon < 1/2)$ переходят в неисправные состояния типа 0 на выходах. Эти неисправности характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию, а в неисправном – константу 0.

Пусть $P_{\bar{f}(\tilde{a}^n)}(S, \tilde{a}^n)$ – вероятность появления $\bar{f}(\tilde{a}^n)$ на выходе схемы S, реализующей булеву функцию $f(\tilde{x}^n)$, при входном наборе $\tilde{a}^n$. Ненадежность $P(S)$ схемы S определяется как максимальное из чисел $P_{\bar{f}(\tilde{a}^n)}(S, \tilde{a}^n)$ при всевозможных входных наборах $\tilde{a}^n$. Надежность схемы S равна $1 - P(S)$.

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

Замечание. При неисправностях типа 0 на выходах элементов любая схема, содержащая хотя бы один функциональный элемент и реализующая отличную от константы 0 функцию, имеет ненадежность, не меньше ε при всех $\varepsilon \in (0, 1/2)$ [1].

Известно [2], что если полный конечный базис содержит обобщенную конъюнкцию $x_1^a \& x_2^b$ $(a, b \in \{0, 1\})$ и линейную функцию, существенно зависящую не менее чем от двух переменных, то в этом базисе любую булеву функцию можно реализовать схемой, ненадежность которой не больше $\varepsilon + 100\varepsilon^2$ при $\varepsilon \in (0, 1/960]$. Этот результат удалось обобщить. Справедлива следующая теорема.

Теорема. *Пусть полный конечный базис B содержит линейную функцию $l(x_1, ..., x_k)$ $(k \geq 2)$, существенно зависящую не менее чем от двух переменных. Тогда в этом базисе любую булеву функцию f можно реализовать такой схемой S, что $P(S) \leq \varepsilon + 100\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.*

Из теоремы и замечания получаем следующий результат: в рассматриваемом базисе B почти любую булеву функцию можно реализовать асимптотически оптимальной по надежности схемой, которая функционируют с ненадежностью, асимптотически равной ε при $\varepsilon \to 0$.

Этот результат в два раза лучше ранее известного результата [3] для инверсных неисправностей на выходах элементов в соответствующем базисе B.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проект 17-01-00451.

Список литературы

1. Алехина М. А. О надежности схем в произвольном полном конечном базисе при однотипных константных неисправностях на выходах элементов // Дискретная математика. — 2012. — Т. 24. — С. 17–24.

2. Алехина М. А., Клянчина Д. М. Об асимптотически оптимальных по надежности схемах в базисах, содержащих существенную линейную функцию и функцию вида $x_1^a \& x_2^b$ // Материалы XVI Международной конференции «Проблемы теоретической кибернетики» — С. 33–37.

3. Васин А. В. Асимптотически оптимальные по надежности схемы в полных базисах из трехвходовых элементов // Дис. ... канд. физ.-мат. наук. — Пенза. — 2010. — 100 с.

ОБ АСИМПТОТИЧЕСКИ ОПТИМАЛЬНЫХ ПО НАДЕЖНОСТИ СХЕМАХ, ПРИ НЕИСПРАВНОСТЯХ ТИПА 0 НА ВЫХОДАХ ЭЛЕМЕНТОВ

М. А. Алехина, С. М. Грабовская, Ю. С. Гусынина (Пенза)

Рассмотрим реализацию булевых функций схемами из ненадежных функциональных элементов в полном конечном базисе B. Считаем, что схема реализует булеву функцию $f(x_1, x_2, \ldots, x_n)$ $(n \in \mathbf{N})$, если при поступлении на входы схемы двоичного набора $\tilde{a}^n = (a_1, a_2, ..., a_n)$ при отсутствии неисправностей на выходе схемы появляется значение $f(\tilde{a}^n)$. Допустим, что все элементы схемы независимо друг от друга с вероятностью ε $(0 < \varepsilon < 1/2)$ переходят в неисправные состояния типа 0 на выходах. Эти неисправности характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию, а в неисправном — константу 0.

Пусть $P_{\bar{f}(\tilde{a}^n)}(S, \tilde{a}^n)$ — вероятность появления $\bar{f}(\tilde{a}^n)$ на выходе схемы S, реализующей булеву функцию $f(\tilde{x}^n)$, при входном наборе $\tilde{a}^n$. Ненадежность $P(S)$ схемы S определяется как максимальное из чисел $P_{\bar{f}(\tilde{a}^n)}(S, \tilde{a}^n)$ при всевозможных входных наборах $\tilde{a}^n$. Надежность схемы S равна $1 - P(S)$.

Пусть $P_\varepsilon(f) = \inf P(S)$, где S — схема, реализующая $f(\tilde{x}^n)$. Схему A, реализующую f, назовем *асимптотически оптимальной по надежности*, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \to 0$, т. е. $\lim\limits_{\varepsilon \to 0} \dfrac{P_\varepsilon(f)}{P(A)} = 1$.

Замечание. При неисправностях типа 0 на выходах элементов любая схема, содержащая хотя бы один функциональный элемент и реализующая отличную от константы 0 функцию, имеет ненадежность, не меньше ε при всех $\varepsilon \in (0, 1/2)$ [1].

Булевы функции f_1 и f_2 назовем конгруэнтными, если одна из них может быть получена из другой заменой переменных (без отождествления).

Пусть $X \subseteq P_2$. Обозначим $Congr(X)$ множество всех функций, каждая из которых конгруэнтна некоторой функции множества X.

$M_1 = Congr\{x_1^{\sigma_1} x_2^{\sigma_2} \vee x_1^{\bar{\sigma}_1} x_2^{\bar{\sigma}_2} x_3^{\sigma_3} | \sigma_i \in \{0,1\},\ i \in \{1,2,3\}\}$,

$M_2 = Congr\{x_1^{\sigma_1} x_2^{\sigma_2} x_3^{\sigma_3} \vee x_1^{\sigma_1} x_2^{\bar{\sigma}_2} x_3^{\bar{\sigma}_3} \vee x_1^{\bar{\sigma}_1} x_2^{\sigma_2} x_3^{\bar{\sigma}_3} | \sigma_i \in \{0,1\},\ i \in \{1,2,3\}\}$,

$$M_3 = Congr\{\bar{x}_1(x_2^{\sigma_2} \vee x_3^{\sigma_3}) | \sigma_i \in \{0,1\},\ i \in \{1,2,3\}\},$$

$$M_4 = Congr\{x_1^{\sigma_1} x_2^{\sigma_2} x_3^{\sigma_3} \vee x_1^{\bar{\sigma}_1} x_2^{\bar{\sigma}_2} x_3^{\bar{\sigma}_3} | \sigma_i \in \{0,1\},\ i \in \{1,2,3\}\},$$

а также M_1^*, M_2^*, M_3^*, M_4^* – множества функций, двойственных соответственно функциям из множеств M_1, M_2, M_3, M_4.

Обозначим $M = \bigcup_{i=1}^{4} (M_i \cup M_i^*)$.

Ранее при инверсных неисправностях на выходах элементов доказано [2], что если полный конечный базис B содержит функцию из множества M, то любую булеву функцию можно реализовать схемой, ненадежность которой не больше $2\varepsilon + 109\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$. Следовательно, в базисе B любую булеву функцию можно реализовать схемой, функционирующей с ненадежностью, асимптотически не больше 2ε при $\varepsilon \to 0$.

При неисправностях типа 0 на выходах элементов справедлива теорема.

Теорема. *Пусть полный конечный базис B содержит функцию из множества M. Тогда в этом базисе любую булеву функцию f можно реализовать такой схемой S, что $P(S) \leq \varepsilon + 100\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.*

Из теоремы и замечания следует, что в базисе B, $B \cap M \neq \emptyset$, почти любую функцию можно реализовать асимптотически оптимальной по надежности схемой, функционирующей с ненадежностью, асимптотически равной ε при $\varepsilon \to 0$.

Отметим, что для базисов, содержащих некоторые из функций множества M эта теорема была доказана ранее [3, 4]. При доказательстве утверждения теоремы в других базисах пришлось искать новые методы построения надежных схем.

Таким образом, 1) полученный результат асимптотически в два раза лучше ранее известного результата [1] для инверсных неисправностей на выходах элементов в соответствующем базисе B;

2) значительно расширено ранее известное множество булевых функций, наличие которых в базисе обеспечивает реализацию почти любой функции асимптотически оптимальной по надежности схемой, функционирующей (асимптотически) с тривиальной оценкой ненадежности.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проект 17-01-00451-а.

Список литературы

1. Алехина М. А. Синтез асимптотически оптимальных по надежности схем. Пенза: ИИЦ ПГУ, 2006. — 156 с.

2. Васин А. В. Асимптотически оптимальные по надежности схемы в полных базисах из трехвходовых элементов // Дис. ... канд. физ.-мат. наук. — Пенза. — 2010. — 100 с.

3. Алехина М. А., Клянчина Д. М. Достаточные условия реализации булевых функций асимптотически оптимальными схемами с тривиальной оценкой ненадежности // Международный симпозиум «Надежность и качество, 2010» (г. Пенза, 24–31 мая 2010 г.). Пенза: ИИЦ ПГУ, 2010. — Т. 1. С. 229–232.

4. Алехина М. А., Клянчина Д. М. Об асимптотически оптимальных по надежности схемах в некоторых специальных базисах // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2010. — № 4 (16). — С. 3–13.

ФУНКЦИИ БУЛЕВОЙ И МНОГОЗНАЧНОЙ ЛОГИКИ НА ЯЗЫКЕ КВАНТОВОЙ ИНФОРМАТИКИ

Ю. И. Богданов, Н. А. Богданова, Д. В. Фастовец, В. Ф. Лукичев (Москва)

В настоящей работе рассматривается фундаментальная взаимосвязь между квантовыми информационными технологиями и дискретной математикой. Описан метод представления функций многозначной логики в виде унитарных преобразований, играющий важную роль при построении квантовых схем [1]. Рассмотрен вопрос о связи полиномов Жегалкина, определяющих алгебраическую нормальную форму булевой функции, с квантовыми схемами [2]. Показано, что квантово-информационный язык предоставляет простой алгоритм построения полинома Жегалкина на основе таблицы истинности. Предложенный подход справедлив не только для булевых функций но и для произвольных функций многозначной (k-значной)

логики, когда k — простое число. Разработанные методы и алгоритмы обобщены на случай произвольной функции с многомерной областью определения и многомерным множеством значений. Разработанный подход имеет существенное значение для реализации квантовых компьютерных технологий и является основой для перехода от классической машинной логики к квантовому аппаратному обеспечению [3].

Согласно квантовой информатике [1], квантовая реализация булевой функции $f(x)$ состоит в том, что двухчастичное состояние $|x, y\rangle$ преобразуется в состояние $|x, y \oplus f(x)\rangle$, т.е.

$$|x, y\rangle \xrightarrow{f} |x, y \oplus f(x)\rangle$$

На основе приведенного определения легко вывести правило получения блочной матрицы U_f квантового преобразования — аналога булевой функции $f(x)$. Нулю в таблице истинности функции $f(x)$ соответствует единичная матрица $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ на главной диагонали, а единице — матрица $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Тот же принцип построения сохраняется и для многокубитовых булевых функций.

Область определения x однобитовой функции будем представлять в виде вектора-столбца $x = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Этот вектор будем рассматривать в качестве базисного вектора e_1 двумерного векторного пространства. В качестве второго базисного вектора рассмотрим вектор-столбец: $e_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Рассмотрим двухбитовые булевы функции. Двухбитовые базисные векторы задаются тензорными произведениями однобитовых векторов:

$$e_{ij} = e_i \otimes e_j, \quad i, j = 0, 1.$$

С другой стороны, можно использовать альтернативное представление базисных векторов: $e_0 = x \oplus 1$, $e_1 = x$ и сразу получить полином Жегалкина. На примере вектора e_{01} получим:

$$e_{01} = e_0 \otimes e_1 = (x_1 \oplus 1)x_2 = x_1x_2 + x_2.$$

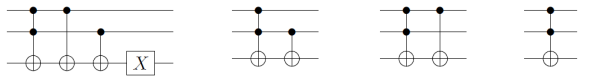
Введем столбцы коэффициентов базисных векторов e_0 и e_1: $p_0 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $p_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Используя эти векторы коэффициентов, мы сразу

получим столбец коэффициентов полинома Жегалкина:

$$e_{01} \to p_{01} = p_0 \otimes p_1 = (0,1,0,1)^T.$$

Данный вектор является столбцом коэффициентов для полинома $x_1x_2 + x_2$ в лексикографическом порядке по показателям степени $(00, 01, 10, 11)$.

Каждому полиному Жегалкина можно поставить в соответствие квантовую схему. Например, двухбитовой булевой функции соответствует трехкубитовая квантовая схема. Два верхних кубита отвечают области определения функции, третий кубит - множеству значений. Слагаемому x_1x_2 отвечает гейт $CCNOT$ (условное преобразование NOT, когда два верхних кубита управляют нижним); слагаемому x_1 отвечает гейт $CNOT$, в котором верхний кубит управляет нижним; слагаемому x_2 отвечает гейт $CNOT$, в котором средний кубит управляет нижним; наконец слагаемому 1 отвечает однокубитовый гейт X, который символизирует безусловное преобразование NOT и действует на нижний кубит. На рисунке 1 представлены квантовые схемы, соответствующие полиномам Жегалкина базисных векторов e_{00}, e_{01}, e_{10} и e_{11}.



$e_{00} = x_1x_2 \oplus x_1 \oplus x_2 \oplus 1$ $e_{01} = x_1x_2 \oplus x_2$ $e_{10} = x_1x_2 \oplus x_1$ $e_{11} = x_1x_2$

Рис. 1: Квантовые схемы для двухкубитовых базисных функций

Разработанный подход можно обобщить на случай многозначной (k-значной) логики. Для формирования базисных функций следует рассмотреть степени вектора-столбца x от 0 до $k-1$. Соответствующий набор будет полным в том и только том случае, когда k - простое число [4]. На основе степеней вектора x строится матрица из k столбцов $Q = [x^0, x^1, ..., x^{k-1}]$. Для матрицы Q строится обратная к ней матрица P. Таким образом, при вычислениях по модулю k, справедливо тождество: $QP = PQ = I$. При нахождении коэффициентов полинома Жегалкина ключевую роль играют столбцы матрицы P: $P = [p_0, p_1, ..., p_{k-1}]$. Обозначим столбец коэффициентов полинома Жегалкина как a. Тогда матрица P обеспечивает переход от функции f к коэффициентам полинома Жегалкина: $a = P * f$, а матрица Q от столбца коэффициентов a к исходной функции: $f = Q * a$.

Таким образом, представленные в работе методы наглядно демонстрируют глубокую связь между классической дискретной мате-

матикой и квантовой информатикой. Разработанные нами алгоритмы позволяют рассмотреть унитарные квантовые представления для произвольных булевых функции с многобитовыми областями определения/значений. Подробно описана связь полиномов Жегалкина и схем квантовой логики. Выполнено обобщение разработанной теории на случай многозначных (k-значных) логик, когда k - простое число. Данное обобщение позволяет эффективно находить аналоги полиномов Жегалкина для функций многозначной логики.

На наш взгляд, рассматраваемый подход имеет существенное значение для реализации методов квантовой обработки информации, а также для решения задач классической и квантовой криптографии.

Работа выполнена в рамках Государственного задания ФТИАН им. К.А. Валиева РАН Минобрнауки РФ по теме №0066-2019-0005.

Список литературы

1. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. — М.: Мир, 2006.

2. Bogdanov Yu. I., Bogdanova N. A., Fastovets D. V., Lukichev V. F. Representation of Boolean functions in terms of quantum computation // Proc. SPIE 11022, International Conference on Micro- and Nano-Electronics 2018, 110222R (15 March 2019) — 2019. [arXiv:1906.06374].

3. Валиев К. А., Кокин А. А. Квантовые компьютеры: надежда и реальность. — Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001.

4. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.

ЛЕГКОТЕСТИРУЕМЫЕ СХЕМЫ В БАЗИСЕ ЖЕГАЛКИНА ПРИ КОНСТАНТНЫХ НЕИСПРАВНОСТЯХ ТИПА «1» НА ВЫХОДАХ ЭЛЕМЕНТОВ

Ю. В. Бородина (Москва)

Будем рассматривать схемы из функциональных элементов в некотором конечном базисе B. В качестве неисправностей предполагаем константные неисправности типа «1» на выходах элементов (при переходе в неисправное состояние элемент выдает значение 1 независимо от входных данных).

Пусть S — некоторая схема из функциональных элементов, реализующая булеву функцию $f(\tilde{x})$, $\tilde{x} = (x_1, x_2, \ldots, x_n)$, в базисе B.

Функция, реализуемая на выходе схемы при наличии в последней неисправного элемента, называется *функцией неисправности*. Всякое множество T входных наборов схемы S называется *полным проверяющим тестом* для этой схемы, если для любой функции неисправности $g(\tilde{x})$, не равной тождественно $f(\tilde{x})$, в T найдется хотя бы один такой набор $\tilde{\sigma}$, что $f(\tilde{\sigma}) \neq g(\tilde{\sigma})$ [1, 2]. Число наборов, составляющих этот тест, называется *длиной* теста.

Введем обозначения [1, 2]: $D(T)$ — длина теста T; $D(S) = \min D(T)$, где минимум берется по всем полным проверяющим тестам T для схемы S; $D(f, B) = \min D(S)$, где минимум берется по всем схемам S в данном базисе B, реализующим функцию f; $D(n, B) = \max D(f, B)$, где максимум берется по всем булевым функциям f от n переменных. Функция $D(n) = D(n, B)$ называется *функцией Шеннона* длины полного проверяющего теста для базиса B.

Пусть $B = \{\oplus, \&, 0, 1\}$ — базис Жегалкина. Считаем, что константы 0 и 1 при реализации функций схемами в этом базисе подаются на входы схемы, сами же они функциональными элементами не являются и в неисправное состояние перейти не могут.

В работе [3] была доказана

Теорема 1. *Любую булеву функцию можно реализовать схемой из функциональных элементов в базисе B, допускающей в случае константных неисправностей типа «0» на выходах элементов полный проверяющий тест длины* 1.

Следующее утверждение показывает, что в случае константных неисправностей типа «1» такого рода результат невозможен.

Теорема 2. *Функция $f(\tilde{x})$, отличная от констант, может быть реализована схемой, допускающей полный проверяющий тест длины* 1*, тогда и только тогда, когда все ее существенные переменные можно разбить на такие два непересекающихся множества Z и Y, что функция f представима в виде*

$$f(x) = (\ldots((M \oplus \bigoplus_{A_0} z_k)y_1 \oplus \bigoplus_{A_1} z_k)y_2 \oplus \ldots)y_s \oplus \bigoplus_{A_s} z_k,$$

где $s \leq n$, $A_0, A_1, \ldots, A_s \subset Z$, а выражение M имеет один из следующих 4 *типов:*
(I) $y_{-1} \oplus y_0$, и тогда $Y = \{y_{-1}, y_0, y_1, \ldots, y_s\}$;
(II) $y_0 \oplus 1$, и тогда $Y = \{y_0, y_1, \ldots, y_s\}$;
(III) $z_p z_q$, где $z_p, z_q \in Z, p \neq q$, и тогда $Y = \{y_1, \ldots, y_s\}$;

(IV) 0, *и тогда* $Y = \{y_1, \ldots, y_s\}$,
причем если $M = 0$, *то* $A_0 \neq \emptyset$.

Количество описанных в условии теоремы функций при $n \geq 5$ меньше числа всех булевых функций от n переменных, откуда $D(n) \geq 2$ при $n \geq 5$.

Список литературы

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

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

3. Бородина Ю. В., Бородин П. А. Синтез легкотестируемых схем в базисе Жегалкина при константных неисправностях типа «0» на выходах элементов // Дискретная математика. — 2010. — Т. 22, вып. 3. — С. 127–133.

О ПРИМЕНЕНИИ SAT-РЕШАТЕЛЕЙ ДЛЯ ПРОВЕРКИ ПРИНАДЛЕЖНОСТИ БУЛЕВЫХ ФУНКЦИЙ, ЗАДАННЫХ ПОЛИНОМАМИ, ОДНОМУ ЗАМКНУТОМУ КЛАССУ

А. В. Бухман (Москва)

Булевой функцией от n переменных назовём любое отображение вида $f : E_2^n \to E_2$, где $E_2 = \{0, 1\}$.

Одним из способов задания булевой функции является её представление в виде *полинома Жегалкина. Мономом* от переменных $x_1, \ldots, x_n$ назовём любое выражение вида $x_{i_1} \cdot \ldots \cdot x_{i_k}$, где $i_1, \ldots, i_n \in \{1, \ldots, n\}$ — различные числа, или просто 1. Равенство мономов рассматривается с точностью до перестановки переменных. *Полиномом Жегалкина* назовём сумму по модулю два конечного числа различных мономов или 0. Равенство полиномов рассматриваем с точностью до перестановки слагаемых. Известно, что любая булева функция представима в виде полинома Жегалкина, причём единственным способом.

На практике часто возникают задачи проверки свойств булевых функций. Например, для исследования системы функций на полноту важно уметь проверять свойства сохранения констант, самодвойственность, монотонность, линейность. Сложность алгоритма при этом зависит от способа представления функции. Для случая представления функции в виде полинома полиномиальный алгоритм проверки этих свойств был построен С. Н. Селезневой в работе [1]. Также С. Н. Селезневой были предложены полиномиальные алгоритмы для проверки принадлежности функции всем замкнутым классам кроме классов семейства O^m.

В настоящий момент нет данных о том, является ли эта задача полиномиальной или NP-трудной. Поэтому актуальным остаётся вопрос о быстром её решении. В данной статье предложен подход на основе использования SAT-решателей. Далее будет показано, как полиномиально свести задачу о принадлежности O^2 функции, заданной полиномом, к выполнимости КНФ, которую в свою очередь можно подать на вход SAT-решателя и получить ответ.

Класс O^2 — множество булевых функций таких, что для любых двух наборов, на которых функция принимает нулевое значение, найдётся переменная, также принимающая нулевое значение.

Пусть задана функция f, тогда для проверки того, что она не принадлежит O^2, нужно найти два набора α, β таких, что $f(\alpha) = 0, f(\beta) = 0, \alpha \vee \beta = 1$. Это равносильно тому, что следующая система уравнений совместна:

$$\begin{cases} f(x_1, \ldots, x_n) &= 0 \\ f(y_1, \ldots, y_n) &= 0 \\ \bar{x}_1 \bar{y}_1 &= 0 \\ \cdots & \\ \bar{x}_n \bar{y}_n &= 0 \end{cases} \tag{1}$$

Задачу решения системы булевых уравнений в форме полиномов можно свести к задаче выполнимости КНФ следующим образом. Пусть есть уравнение

$$K_1 \oplus \cdots \oplus K_l = 0, \tag{2}$$

где $K_1, \ldots, K_n$ — мономы. Введём вспомогательные переменные $u_1, \ldots, u_{l-2}$. Тогда уравнение можно переписать в виде:

$$\begin{cases} K_1 \oplus K_2 \oplus u_1 &= 0 \\ u_1 \oplus K_3 \oplus u_2 &= 0 \\ u_2 \oplus K_4 \oplus u_3 &= 0 \\ \cdots & \\ u_{l-2} \oplus K_l &= 0 \end{cases} \tag{3}$$

Теорема. *Система* (3) *имеет решение тогда и только тогда, когда имеет решение исходное уравнение.*

Проделав эту процедуру для каждого уравнения, получим большую систему полиномиальных уравнений, эта система будет совместна тогда и только тогда, когда совместна исходная, и в полученной системе каждое уравнение будет иметь не более трёх слагаемых в правой части. Полином содержащий не более трёх слагаемых можно представить в виде ДНФ, содержащей не более 8 конъюнкций. Далее строим дизъюнкцию всех ДНФ. От ДНФ перейдём к КНФ, сделав отрицание. Получим задачу выполнимости КНФ. Причём справедливо, что если на вход подавался полином длины l, то полученная КНФ будет иметь длину $O(l)$. Подаём КНФ на вход SAT-решателя, получаем ответ: если SAT-решатель находит ответ, значит функция не принадлежит O^2, иначе принадлежит.

Работа выполнена при поддержке РФФИ, грант 17-01-00782-а.

Список литературы

1. Селезнева С. Н. О сложности распознавания полноты множеств булевых функций, реализованных полиномами Жегалкина // Дискретная математика. — 1997. — Т. 9, вып. 4. — С. 24–31.

СЛОЖНОСТЬ И СЛОЖНЫЕ ФУНКЦИИ В КЛАССАХ ПОЛИНОМИАЛЬНЫХ ФОРМ БУЛЕВЫХ ФУНКЦИЙ

С. Ф. Винокуров, А. С. Францева (Иркутск)

В работе приведен обзор результатов по сложным функциям в различных классах полиномиальных нормальных форм. Для этого используется операторный подход, при котором булева функция $f(x_1, \ldots, x_n)$ представляется как сумма по модулю два операторных образов некоторой (называемой базисной) функции $g(x_1, \ldots, x_n)$ от базисного пучка операторов. Если в качестве базисной функции g взять функцию $x_1 \cdot \ldots \cdot x_n$, то классы операторных форм редуцируются до классов полиномиальных нормальных форм (ПНФ). На рисунке 1 изображена часть диаграммы классов операторных форм. Классы расположены по включению снизу-вверх. На схеме на нижнем уровне показаны базисные операторные пучки `A`; среди них есть,

например, пучки соответствующие СПНФ и полиному Жегалкина. Далее представлены:

- классы двупорожденных операторных пучков вида $H_{\mathfrak{b}}$, где $\mathfrak{b}$ — оператор длины n, имеет вид последовательности $\mathfrak{b}_1 \dots \mathfrak{b}_n$, $\mathfrak{b}_i \in \{d, e, p\}$ (классу $H_{d\dots d}$ соответствует класс Zh поляризованных полиномов Жегалкина), операторы подробно изложены в [3];
- классы $E_{\mathfrak{A}}$ — расширений двупорожденных операторных пучков;
- класс H всех двупорожденных операторных пучков (Kro — класс кронекеровых форм);
- классы $EH_{\mathfrak{b}}$, EH расширенных двупорожденных операторных форм ($EH_{d\dots d}$ — класс расширенных поляризованных полиномов Жегалкина, $KroE$ — класс расширенных кронекеровых форм);
- класс MH смешанных двупорожденных операторных форм ($PKro$ — класс псевдокронекеровых форм);
- класс OP всех операторных форм (ему соответствует класс ПНФ всех полиномиальных нормальных форм).

Пусть K — класс операторных форм, B_n — класс всех булевых функций. Тогда функция Шеннона $L_K(n)$ сложности представлений всех булевых функций в классе K равна:

$$L_K(n) = \max_{f \in B_n}\{\min_{OF(f)}\{l(f)\}\},$$

по всем операторным формам $OF(f)$ функции f, построенным по пучкам класса K; $l(f)$ — число операторных образов функции g в операторном представлении $OF(f)$.

Значение нижней границы функции Шеннона в указанных классах (за исключением класса ПНФ) найдено через построение последовательности множеств сложных функций. Пусть далее через f_n обозначена функция $f(x_1, \dots, x_n)$.

Функция Шеннона сложности представлений класса B_n в классах $H_{\mathfrak{b}}, H, MH$:

$$L_{H_{\mathfrak{b}}}(n) = L_H(n) = \left\lfloor \tfrac{2}{3} 2^n \right\rfloor \text{ [2, 3, 4]}; \quad L_{MH}(n) = \tfrac{1}{2} 2^n \text{ [1]}.$$

Множества функций, имеющие соответствующую сложность в классах $H_{\mathfrak{b}}, H, MH$:

$p_0 = 0,\ q_0 = 1,\ t_0 = 1,$

$p_n = x_n q_{n-1} \oplus \bar{x}_n t_{n-1},\ q_n = x_n t_{n-1} \oplus \bar{x}_n p_{n-1},$

$t_n = x_n p_{n-1} \oplus \bar{x}_n q_{n-1}$ [3, 4].

Функция Шеннона сложности представлений класса B_n в классах операторных форм:

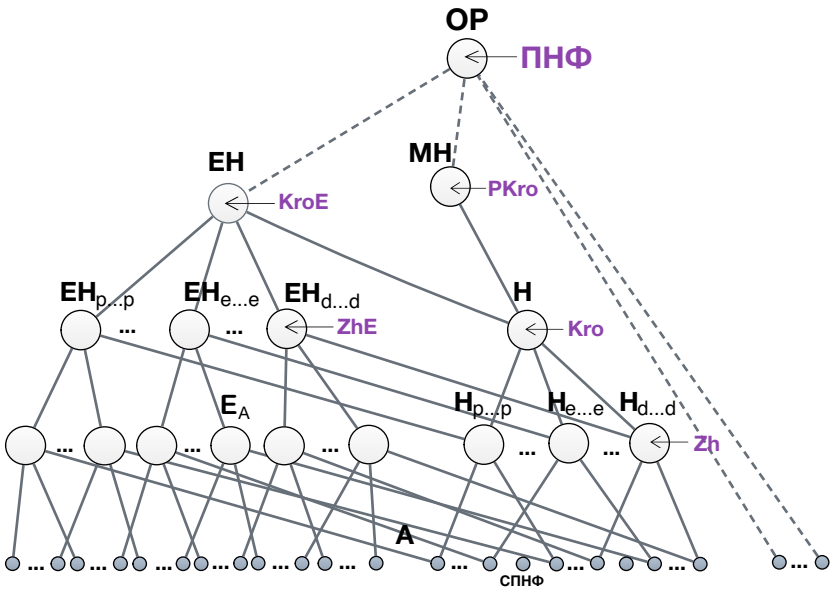


Рис. 1: Диаграмма классов операторных форм булевых функций

$\frac{1}{2}2^n - 1 \leq L_{EH_\text{ь}}(n) \leq \frac{1}{2}2^n$ [3, 5].

Множества функций, имеющие соответствующую сложность в классах $EH_{b_1\ldots b_{n-3}pep}$, $EH_{b_1\ldots b_{n-3}pde}$, $EH_{b_1\ldots b_{n-3}epe}$, $EH_{b_1\ldots b_{n-3}eed}$, $EH_{b_1\ldots b_{n-3}dpp}$, $EH_{b_1\ldots b_{n-3}ddd}$:

$p_3^1 = (00011011)$, $q_3^1 = (11010001)$, $t_3^1 = (11001010)$;

в классах $EH_{b_1\ldots b_{n-3}ppe}$, $EH_{b_1\ldots b_{n-3}ped}$, $EH_{b_1\ldots b_{n-3}epp}$, $EH_{b_1\ldots b_{n-3}edd}$, $EH_{b_1\ldots b_{n-3}dep}$, $EH_{b_1\ldots b_{n-3}dde}$:

$p_3^2 = (10100001)$, $q_3^2 = (11001101)$, $t_3^2 = (01101100)$;

в классах $EH_{b_1\ldots b_{n-3}ppd}$, $EH_{b_1\ldots b_{n-3}edp}$, $EH_{b_1\ldots b_{n-3}dee}$:

$p_3^3 = (01010011)$, $q_3^3 = (10001011)$, $t_3^3 = (11011000)$;

в классах $EH_{b_1\ldots b_{n-3}pdp}$, $EH_{b_1\ldots b_{n-3}eee}$, $EH_{b_1\ldots b_{n-3}dpd}$:

$p_3^4 = (01011101)$, $q_3^4 = (01100101)$, $t_3^4 = (00111000)$;

в классах $EH_{b_1\ldots b_{n-3}ppp}$, $EH_{b_1\ldots b_{n-3}pdd}$, $EH_{b_1\ldots b_{n-3}eep}$, $EH_{b_1\ldots b_{n-3}ede}$, $EH_{b_1\ldots b_{n-3}dpe}$, $EH_{b_1\ldots b_{n-3}ded}$:

$p_3^5 = (10111010)$, $q_3^5 = (00011100)$, $t_3^5 = (10100110)$;

в классах $EH_{b_1\ldots b_{n-3}pee}$, $EH_{b_1\ldots b_{n-3}epd}$, $EH_{b_1\ldots b_{n-3}ddp}$:

$p_3^6 = (01000110),\ q_3^6 = (10110100),\ t_3^6 = (11110010)$;
при $n > 3$, по всем $j \in \{1, 2, \ldots, 6\}$
$p_n^j = x_n q_{n-1}^j \oplus \bar{x}_n p_{n-1}^j, q_n^j = x_n t_{n-1}^j \oplus \bar{x}_n q_{n-1}^j, t_n^j = x_n p_{n-1}^j \oplus \bar{x}_n t_{n-1}^j$[5].

Функция Шеннона сложности представлений класса B_n в классе EH:

$$\left\lfloor \tfrac{5}{12} 2^n \right\rfloor \leq L_{EH}(n) \leq \tfrac{1}{2} 2^n \text{ [3, 5]}.$$

Множества функций, имеющие соответствующую сложность в классе EH: $p_4 = (0001011001101001), q_4 = (1110100010000001)$,

$t_4 = (1111111011101000)$;
$p_n = x_n q_{n-1} \oplus \bar{x}_n p_{n-1}, q_n = x_n t_{n-1} \oplus \bar{x}_n q_{n-1}, t_n = x_n p_{n-1} \oplus \bar{x}_n t_{n-1}$[5].

Список литературы

1. Балюк А. С., Винокуров С. Ф. Функция Шеннона для некоторых классов операторных полиномиальных форм // Оптимизация, управление, интеллект. — 2000. — Вып 5. — С. 167–180.

2. Винокуров С. Ф. Смешанные операторы в булевых функциях и их свойства // Иркутский университет. Серия: Дискретная математики и информатика. — 2000. — Вып. 12. — 36 с.

3. Избранные вопросы теории булевых функций / под ред. С. Ф. Винокурова и Н. А. Перязева. — М.: Физматлит, 2001. — 192 с.

4. Перязев Н. А. Сложность булевых функций в классе полиномиальных поляризованных форм // Алгебра и логика. — 1995. — Т. 34, № 3. — С. 323–326.

5. Францева А. С. Сложность представлений булевых функций в классах расширенных двупорожденных операторных форм // Сибирские Электронные Математические Известия. — 2019. — Т. 16. — С. 523–541.

БЫСТРЫЕ АЛГОРИТМЫ РЕШЕНИЯ УРАВНЕНИЙ СТЕПЕНИ НЕ ВЫШЕ 4 В НЕКОТОРЫХ КОНЕЧНЫХ ПОЛЯХ

С. Б. Гашков (Москва)

Пусть $M(n)$ — сложность умножения многочленов степени n над полем характеристики 3. В качестве $M(n)$ можно взять $n(\log_2 n)\psi(n)$ где $\psi(n)$ растет медленнее любой итерации логарифма.

Теорема. *Решение уравнений степени не выше четырех в поле* $GF(p^s)$, *где* $p > 3$, $s = 2^k r$, $k \to \infty$, $r = \pm 1 \bmod 6$, $p, r = O(1)$, *при использовании подходящего базиса можно найти с битовой сложностью*

$$O_r(M(2^k)kM(r)M(\log_2 p)) = O_{r,p}(M(s)\log_2 s).$$

В полях $GF(3^s)$, *где* $s = \pm 1 \bmod 6$, *при использовании нормального базиса решения можно найти с битовой сложностью* $O(M(GF(3^s))\log_2 s)$. *В полях* $GF(2^s)$, *где* $s = 2r$, $r \neq 0 \bmod 3$, *при использовании нормального базиса решения можно найти с битовой сложностью* $O(M(GF(2^s))\log_2 s)$.

Пример решения уравнения $x^4 - \omega_1 x^3 - (\omega_1+1)x^2 - \omega_1 x + \omega_1 = 0$ **с коэффициентами в поле** $GF(3^2)$, $\omega_1^2 + \omega_1 = 1$.

После замены $y = x - \omega_1$ получим уравнение $y^4 - y^2(\omega_1 + 1) + y\omega_1 + \omega_1 - 1 = 0$. Представим его левую часть в виде

$$(y^2 + a)^2 + y^2(-(\omega_1 + 1) + a) + y\omega_1 + \omega_1 - 1 - a^2.$$

Выберем $a \in GF(3^4)$ так, чтобы дискриминант

$$D = \omega_1^2 - (-(\omega_1 + 1) + a)(\omega_1 - 1 - a^2) = 0.$$

Получим резольвенту Феррари $-\omega_1^2 - 1 + a(1-\omega_1) - (\omega_1+1)a^2 + a^3 = 0$. Сделаем замену $u = a - b, 2(\omega_1 + 1)b = 1 - \omega_1, b = 1 + \omega_1$ и получим уравнение

$$-\omega_1^2 - 1 + (u+\omega_1+1)(1-\omega_1) - (\omega_1+1)(u+\omega_1+1)^2 + (u+\omega_1+1)^3 = 0 \Leftrightarrow$$

$$\Leftrightarrow u^3 - (\omega_1 + 1)u^2 + 1 - \omega_1 = 0.$$

После замены $u = 1/v$ оно принимает вид

$$1/v^3 - (\omega_1 + 1)/v^2 + 1 - \omega_1 = 0 \Leftrightarrow \omega_1 - 1 + \omega_1 v + v^3 = 0.$$

Извлекая квадратный корень, найдем $d \in GF(3^4)$ из условия $d^2 = \omega_1, d = \omega_2$, и, выполнив замену $v = wd = \omega_2 w$, приведем полученное уравнение к виду $\omega_1 - 1 + \omega_1\omega_2 w + \omega_1\omega_2 w^3 = 0 \Leftrightarrow w^3 + w = (1 - \omega_1)/\omega_1\omega_2 = \omega_2$ Решаем его заменой $w = x + y\omega_2, x, y \in GF(3^2)$:

$$(x + y\omega_2)^3 + x + y\omega_2 = x^3 + x + (y^3\omega_1 + y)\omega_2 = \omega_2 \Leftrightarrow$$

$$\Leftrightarrow x^3 + x = 0, y^3\omega_1 + y = 1.$$

Уравнение $x^3 + x = 0$ имеет корни $x = 0, \pm\imath = \pm(1 - \omega_1)$. Решаем уравнение $y^3\omega_1 + y = 1$ аналогичной заменой

$$y^3\omega_1 + y = 1 \Leftrightarrow (y_1 + y_2\omega_1)^3\omega_1 + y_1 + y_2\omega_1 = 1 \Leftrightarrow$$

$$\Leftrightarrow -1 + y_1 - y_2^3 + \omega_1(y_1^3 + y_2) = 0 \Leftrightarrow -1 + y_1 - y_2^3 = 0; y_1^3 + y_2 = 0 \Leftrightarrow$$

$$\Leftrightarrow -1 + y_1 + y_1^9 = 0, -1 + y_1 + y_1^3 = 0 \Leftrightarrow$$

$$\Leftrightarrow y_1 = -1, y_2 = 1, y = -1 + \omega_1.$$

Поэтому уравнение $w^3 + w = \omega_2$ имеет корни

$$w_{1,2,3} = (-1 + \omega_1)\omega_2, \pm(1 - \omega_1) + (-1 + \omega_1)\omega_2,$$

тогда

$$v = w_1 d = \omega_2 w_1 = (-1 + \omega_1)\omega_2^2 = (-1 + \omega_1)\omega_1 = \omega_1 + 1,\ u = 1/v = \omega_1,$$

$$a = u + b = \omega_1 + 1 + \omega_1 = 1 - \omega_1,$$

и левая часть исходного уравнения принимает вид

$$(y^2 + a)^2 + y^2(-(\omega_1 + 1) + a) + y\omega_1 + \omega_1 - 1 - a^2 = (y^2 + 1 - \omega_1)^2 + y^2\omega_1 +$$

$$+ y\omega_1 + \omega_1 = (y^2 + 1 - \omega_1)^2 + \omega_1(y^2 + y + 1) = (y^2 + 1 - \omega_1)^2 + \omega_1(y - 1)^2.$$

Извлекаем квадратный корень из $-\omega_1$ в поле $GF(3^4)$:

$$-\omega_1 = (\omega_2)^2\omega_1^4,\ \sqrt{-\omega_1} = \omega_2\omega_1^2 = \omega_2(1 - \omega_1).$$

Получаем, что левая часть исходного уравнение разлагается на квадратные множители над полем $GF(3^4)$

$$(y^2 + 1 - \omega_1)^2 + \omega_1(y - 1)^2 = (y^2 + 1 - \omega_1)^2 - (((1 - \omega_1)\omega_2)^2(y - 1))^2 =$$

$$= (y^2 + (1 - \omega_1)\omega_2 y + (1 - \omega_1)(1 - \omega_2))(y^2 - (1 - \omega_1)\omega_2 y + (1 - \omega_1)(1 + \omega_2)).$$

Решаем первое квадратное уравнение:

$$y^2 + (1 - \omega_1)\omega_2 y + (1 - \omega_1)(1 - \omega_2) =$$

$$= (y - (1 - \omega_1)\omega_2)^2 + (1 - \omega_1)(1 - \omega_2) - (1 - \omega_1)^2\omega_1 =$$

$= (y-(1-\omega_1)\omega_2)^2+(1-\omega_1)(1-\omega_2)+\omega_1 = (y-(1-\omega_1)\omega_2)^2+1+\omega_2(1-\omega_1)$,
находим квадратный корень

$$\sqrt{\omega_2(\omega_1-1)-1} = x_1 + x_2\omega_3 \Leftrightarrow$$

$$\Leftrightarrow x_1^2 + x_2^2\omega_2 - x_1x_2\omega_3 = \omega_2(\omega_1-1)-1 \Leftrightarrow$$

$\Leftrightarrow x_1x_2 = 0; x_1^2+x_2^2\omega_2 = \omega_2(\omega_1-1)-1 \Leftrightarrow x_1 = 0; x_2^2\omega_2 = \omega_2(\omega_1-1)-1 \Leftrightarrow$

$\Leftrightarrow x_2^2 = \omega_1-1-\omega_2/\omega_1 = \omega_1-1-\omega_2(\omega_1+1) \Leftrightarrow x_2 = \sqrt{\omega_1-1-\omega_2(\omega_1+1)}$,
еще раз вычисляем квадратный корень

$$\sqrt{\omega_1-1-\omega_2(\omega_1+1)} = x_3 + x_4\omega_2 \Leftrightarrow$$

$$\Leftrightarrow x_3^2 + x_4^2\omega_1 - x_3x_4\omega_2 = \omega_1-1-\omega_2(\omega_1+1) \Leftrightarrow$$

$$\Leftrightarrow x_3^2 + x_4^2\omega_1 = \omega_1-1; x_3x_4 = \omega_1+1 \Leftrightarrow$$

$$\Leftrightarrow x_4 = (\omega_1+1)/x_3; \omega_1(\omega_1+1)^2/(x_3)^2 + x_3^2 = \omega_1-1 \Leftrightarrow$$

$$\Leftrightarrow \omega_1+1+x_3^4 = (\omega_1-1)x_3^2 \Leftrightarrow$$

$$\Leftrightarrow x_5 = x_3^2, 0 = \omega_1+1+x_5^2-(\omega_1-1)x_5;$$

$$x_5 = (\omega_1-1) \pm \sqrt{(\omega_1-1)^2-\omega_1-1} =$$

$$= (\omega_1-1) \pm \sqrt{(\omega_1)^2} = (\omega_1-1) \pm \omega_1 = -1, -1-\omega_1;$$

далее находим $x_3 = \sqrt{1} = \pm 1, x_4 = \pm(\omega_1+1), x_2 = \pm(1+(\omega_1+1)\omega_2), x_1 = 0$, значит

$$\sqrt{\omega_2(\omega_1-1)-1} = x_1 + x_2\omega_3 = \pm(1+(\omega_1+1)\omega_2)\omega_3,$$

и корни первого уравнения

$$y_{1,2} = (1-\omega_1)\omega_2 \pm \sqrt{\omega_2(\omega_1-1)-1} = (1-\omega_1)\omega_2 \pm (1+(\omega_1+1)\omega_2)\omega_3 =$$

$$= (1-\omega_3^4)\omega_3^2 \pm (1+(\omega_3^4+1)\omega_3^2)\omega_3,\ \omega_3 \in GF(3^8),\ \omega_3^8+\omega_3^4 = 1.$$

Второе уравнение решается аналогично.

Работа выполнена при финансовой поддержке РФФИ, проект № 18–01–00337

ВЕРХНЯЯ ОЦЕНКА ЭНЕРГОПОТРЕБЛЕНИЯ ОБЪЕМНЫХ СХЕМ В КЛАССЕ БУЛЕВЫХ ОПЕРАТОРОВ

А. А. Ефимов (Москва)

В ряде работ исследовалась сложность схем из функциональных элементов, реализующих функции алгебры логики от n аргументов. Однако, зачастую в них рассматривались схемы, в которых не накладывалось никаких ограничений на размещение элементов схемы, способ соединения и т.п. На самом деле в любой схеме, когда она располагается в пространстве, функциональные элементы имеют определенную длину, ширину и соединяются проводниками, размеры которых следует учитывать.

Данная работа посвящена объемным схемам, которые определяются аналогично плоским схемам, но в пространстве. Впервые понятие плоской схемы было введено С.С. Кравцовым в 1967 году [1]. Н.А. Шкаликова в работе [3] установила, что если оператор реализуется трёхмерной схемой с объемом V, то его можно реализовать плоской схемой с площадью $\mathcal{O}(V^{3/2})$, причём порядок оценки нельзя понизить. Подобные схемы впервые начал рассматривать Коршунов [2]. Им была получена оценка сложности схем из объемных функциональных элементов (l-схем), удовлетворяющим некоторым ограничениям.

Развитие теории плоских схем было связано с развитием технологии производства и укладки реальных микросхем. Идея о том, что схемы можно укладывать друг на друга в пространстве была также известна давно, но не находила широкого применения вплоть до недавнего времени. Лишь несколько лет назад подобная технология начала использоваться, так как у инженеров закончились способы выжать лучшие характеристики из чипов прежнего размера. В частности, речь идёт о том, чтобы в будущем использовать многослойные чипы.

Основной целью данной работы является обобщение результатов Калачева [4, 5] на объёмные схемы. Как и в его работах, автор использует такое понятие сложности схемы, как максимальный потенциал. Он равен максимальному значению количества единиц на всех внутренних узлах схемы, взятому по всем входным наборам. Неформально говоря, потенциал показывает количество «энергии» схемы, необходимой для её функционирования. В работе [6] была получена верхняя оценка потенциала для класса булевых функций, а в данной работе — для класса булевых операторов.

Определение. *Объёмная схема* — это схема из функциональ-

ных элементов, уложенная на трёхмерную целочисленную решетку в пространстве так, что каждому входу и выходу соответствует некоторое ребро решётки.

Определение. *Длиной* схемы K будем называть длину наименьшего прямоугольного параллелепипеда, содержащего все непустые элементы схемы K, обозначается $l(K)$.

Определение. *Шириной* схемы K будем называть ширину наименьшего прямоугольного параллелепипеда, содержащего все непустые элементы схемы K, обозначается $w(K)$.

Определение. *Высотой* схемы K будем называть высоту наименьшего прямоугольного параллелепипеда, содержащего все непустые элементы схемы K, обозначается $h(K)$.

Определение. *Объемом* схемы K будем называть число элементов в схеме, обозначается $|K|$.

Для каждой схемы K зафиксируем некоторую нумерацию её узлов. На i-м узле реализуется некоторая функция g_i от входных переменных схемы K (на входах схемы считаем, что реализуются тождественные функции).

Везде далее будем считать, что схема K имеет n входов, m выходов и l узлов.

Определение. *Состоянием* схемы K на входном наборе x назовём вектор

$$s_K(x) := (g_1(x), ..., g_l(x)).$$

Если $v = (v_1, ..., v_q) \in \{0,1\}^q$, обозначим $|v| := v_1 + v_2 + ... + v_q$.

Определение. *Потенциалом* схемы K на входном наборе $x \in \{0,1\}^n$ назовём величину $u_K(x) := |s_K(x)|$.

Определение. *Максимальным потенциалом* схемы K назовём величину

$$\hat{U}(K) := \max_{x \in \{0,1\}^n} u_K(x).$$

Пусть $f : \{0,1\}^n \to \{0,1\}^m$ – булев оператор. Тогда

$$\hat{U}(f) := \min_{K \in Impl(f)} \hat{U}(K).$$

Если $Impl(f)$ пусто, то формально полагаем $\hat{U}(f) = \infty$.

Теорема. *Пусть дан булев оператор $f : \{0,1\}^n \to \{0,1\}^m$. Тогда существует объемная схема W_f со входами $x_1, x_2, \ldots, x_n$ на m выходах которой реализуется оператор f, причём схема W_f обладает следующими характеристиками:*

1. *Если $m \leq n$:*

   (a) $l(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $w(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $h(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$.
   (b) $|W_f| = \mathcal{O}(m \cdot 2^n)$.
   (c) $\hat{U}(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$.
2. *Если* $m > n$*:*
   (a) $l(W_f) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$, $w(W_f) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$, $h(W_f) = \mathcal{O}(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3})$.
   (b) $|W_f| = \mathcal{O}(m \cdot 2^n)$.
   (c) $\hat{U}(W_f) = \mathcal{O}(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3})$.

Заметим, что результат работы [6] является частным случаем при $m = 1$. Отметим также, что при $\log_2(m) = o(2^n)$ объем схемы $|W_f|$ является оптимальным по порядку, что легко получить по аналогии с [3, утв. 1] или нижней оценкой в [2].

Список литературы

1. Кравцов С. С. О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов. // Проблемы кибернетики. Вып. 19. — М.: Наука, 1967. — С. 285–293.

2. Коршунов А. Д. Об оценках сложности из объемных функциональных элементов и объемных схем из функциональных элементов. // Проблемы кибернетики. Вып. 19. — М.: Наука, 1967. — С. 275–283.

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

4. Калачёв Г. В. Порядок мощности плоских схем, реализующих булевы функции // Дискретная математика. — 2014. — Т. 26, № 1. — С. 49–74.

5. Калачёв Г. В. Об одновременной минимизации площади, мощности и глубины плоских схем, реализующих частичные булевы операторы // Интеллектуальные системы. Теория и приложения. — 2016. — Т. 20, № 2. — С. 203–266.

6. Ефимов А. А. Верхняя оценка энергопотребления в классе объемных схем. // Интеллектуальные системы. Теория и приложения. — 2019. — Т. 23, № 1. — С. 117–132.

ТЕСТИРОВАНИЕ ПОЛЯРИЗУЕМЫХ ФУНКЦИЙ

Д. В. Кафтан, А. А. Вороненко (Москва)

Базовые понятия настоящей работы можно найти в учебнике [1] и пионерских работах [2, 3].

В. А. Стеценко [2] получил все слабоповторные функции в элементарном базисе $B_0 = \{\&, \vee, \neg\}$. С точностью до преобразований обобщенной однотипности они образуют пять семейств, нас интересуют три из них:

$$f_m^s = x_1(x_2 \vee \cdots \vee x_s) \vee x_2 x_3 \ldots x_s, \quad s \geq 3,$$
$$f_4 = x_1(x_2 \vee x_3) \vee x_3 x_4,$$
$$f_5 = x_1(x_2 \vee x_3 x_4) \vee x_5(x_2 x_3 \vee x_4).$$

Далее все рассматриваемые базисы будем считать состоящими из B_0 и функций из этих трех семейств.

В работе [2] была поставлена задача тестирования относительно бесповторной альтернативы. В работе [4] доказана линейность теста относительно бесповторной альтернативы в базисе B_0. Обозначим B_l^{mon} базис, состоящий из $\{\vee, \&\}$ и функций из множества $\{f_4, f_5, f_m^s\}$, B_l^{pol} – базис, состоящий из B_0 и функций из множества $\{f_4, f_5, f_m^s\}$, где l – максимальная размерность слабоповторной функции в базисе. Также обозначим $T_{mon}(n)$ и $T_{pol}(n)$ функции Шеннона [5] длины теста относительно бесповторной альтернативы в этих базисах

Пусть f — произвольная слабоповторная поляризуемая функция n переменных. Обозначим $t(f)$ минимальное количество наборов, на которых f отличается от всех других поляризуемых функций n переменных. Обозначим $t(n)$ функцию Шеннона количества наборов, на которых произвольная поляризуемая слабоповторная функция n переменных отличается от всех поляризуемых функций n переменных. Функция $t(n)$ монотонно не убывает при $n \geq 3$.

Утверждение. *Произвольная поляризуемая функция f с вектором поляризации $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$ отличается от всех поляризуемых функций на множестве M, если по нему однозначно определяется вектор поляризации функции и для каждого набора $(\alpha_1, \ldots, \alpha_n)$ из множества верхних нулей и нижних единиц обобщенно-однотипной с f монотонной функции $f(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n})$ набор $(\alpha_1^{\sigma_1}, \ldots, \alpha_n^{\sigma_n})$ лежит в M.*

Обозначим $\mathbf{e}_i$ набор с одной единицей в i-м разряде.

Таблица 1:

№	Функция	Наборы
1	f_4	$M_1 = \{(0,1,1,0),(0,0,1,1),(0,1,0,1),(1,0,1,0),(1,1,0,0),$ $(1,0,0,1),(1,0,0,0)\}$
2	f_5	$M_2 = \{(0,1,1,1,0),(0,1,0,0,1),(0,1,1,0,1),(0,0,0,1,1),$ $(1,1,0,0,0),(1,0,0,1,0),(1,0,1,1,0),(1,0,1,0,1),$ $(1,0,0,1,1)\}$
3	f_m^s	$M_3 = \{\mathbf{0}\oplus\mathbf{e}_1, \mathbf{0}\oplus\mathbf{e}_1\oplus\mathbf{e}_2,\ldots,\mathbf{0}\oplus\mathbf{e}_1\oplus\mathbf{e}_s,$ $\mathbf{1}\oplus\mathbf{e}_1, \mathbf{1}\oplus\mathbf{e}_1\oplus\mathbf{e}_2,\ldots,\mathbf{1}\oplus\mathbf{e}_1\oplus\mathbf{e}_s\}$

Лемма. $t(f_4) \le 7,\ t(f_5) \le 9,\ t(f_m^s) \le 2s.$

Доказательство. Примеры тестов, на которых слабоповторные поляризуемые функции отличаются от всех поляризуемых функций того же числа переменных, приведены в таблице 1. □

Добавив не более $2n$ наборов для доказательства ветора поляризации, получим утверждение.

Лемма. $T_{pol}(n) \le 2n + T_{mon}(n)$.

В работе [6] показано, что любая булева функция имеет две существенных переменных, для которых существуют константы, подстановка которых сохраняет существенность остальных переменных. Переименовав переменные, можно построить последовательность функций, существенно зависящих от всех переменнных

$$f(x_1,\alpha_2,\ldots,\alpha_n),$$
$$f(x_1,x_2,\alpha_3,\ldots,\alpha_n),$$
$$\ldots$$
$$f(x_1,\ldots,x_n).$$

Описание теста. На s-ом шаге индукции мы будем к уже существующему тесту добавлять t_s наборов. Для $s = 1$ в качестве теста возьмем весь оба набора.

Тест для функции $f(x_1,\ldots,x_s,\alpha_{s+1},\ldots,\alpha_n)$ позволяет отличить функцию $f(x_1,\ldots,x_s,x_{s+1},\alpha_{s+2},\ldots,\alpha_n)$ от любой бесповторной функции, различающейся с ней на подкубе $x_{s+1} = \alpha_{s+1}$. Если добавить к тесту t_s наборов, на которых $f(x_1,\ldots,x_s,x_{s+1},\alpha_{s+2},\ldots,\alpha_n)$ отличается от любой функции, совпадающей с ней на подкубе $x_{s+1} = \alpha_{s+1}$, то получим тест для $f(x_1,\ldots,x_s,x_{s+1},\alpha_{s+2},\ldots,\alpha_n)$.

Длина теста складывается из длин множеств M_n и равна $\sum\limits_{i=1}^{n} t_i$.

Теорема. *Длина теста равна* $\sum_{s=1}^{n} t_s$*.Если* t_s *ограничены константой, то* $T_{mon}(n) = \Theta(n), T_{pol}(n) = \Theta(n)$.

Список литературы

1. Алексеев А. Б. Лекции по дискретной математике. — М.: ИНФРА-М, 2012. — 90 с.

2. Стеценко В. А. О предплохих базисах в P_2 // Математические вопросы кибернетики. Вып. 4. —М.: Физматлит, 1992. — С. 139–177.

3. Вороненко А. А. О проверяющих тестах для бесповторных функций // Математические вопросы кибернетики. Вып. 11. — 2002. — С. 165–176

4. Вороненко А. А. О длине проверяющего теста для бесповторных функций в базисе $\{0, 1, \&, \vee, \neg\}$ // Дискретная математика. — 2005. — 17. — С. 139–143

5. Shannon C. E. A symbolic analysis of relay and switching circuits // Trans. AIEE. —1938. — 57. — P. 713–723.

6. Chimev K. Structural properties of the functions // 7-th International Conference on Discrete Mathematics and Applications. — 2004, June 17-20. — P. 3–4.

НИЖНЯЯ ОЦЕНКА СЛОЖНОСТИ ЛИНЕЙНОЙ ФУНКЦИИ В ОДНОМ БЕСКОНЕЧНОМ БАЗИСЕ

Ю. А. Комбаров (Москва)

В работе исследуется сложность реализации схемами из функциональных элементов линейной булевой функции $l_n(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n$. Сложность функции l_n известна для многих базисов, состоящих из двухвходовых элементов. Приведем некоторые работы, посвященные этому вопросу: в [1] доказано, что сложность l_n в базисе $\{x\&y, x \vee y, \overline{x}\}$ составляет $4n - 4$, в [2] аналогичный результат доказан для базиса $\{\overline{x\&y}\}$, а в [3] — для базиса $\{x \to y, \overline{x}\}$.

Мы будем рассматривать схемы из функциональных элементов в базисе U_∞, состоящего из всех булевых функций, имеющих вид $x_1^{\sigma_1}\& \ldots \& x_s^{\sigma_s}$ или $x_1^{\sigma_1} \vee \ldots \vee x_s^{\sigma_s}$ (здесь $s \in \mathbb{N}$, $(\sigma_1, \ldots, \sigma_s) \in \{0, 1\}^s$).

Другими словами, базис U_∞ состоит из конъюнкторов и дизъюнкторов с произвольным количеством входов, любой вход которых может быть инвертирован. Сложность схемы в базисе U_∞ определяется как количество элементов в ней. Сложность булевой функции f в базисе U_∞ определяется как наименьшая сложность схемы, реализующей эту функцию, и обозначается через $L(f)$.

В работе [4] для сложности линейной функции в базисе U_∞ получены следующие оценки: $2n + \Theta(1) \leq L(l_n) \leq 2\frac{1}{2}n + \Theta(1)$. В [5] улучшена верхняя оценка: $L(l_n) \leq 2\frac{1}{3}n + \Theta(1)$. Для ее доказательства построена схема наименьшей сложности (среди известных схем), реализующая линейную функцию.

В данной работе улучшается нижняя оценка. А именно, доказана

Теорема. $L(l_n) \geq 2\frac{1}{9}n + \Theta(1)$.

Доказательство теоремы использует метод забивающих констант, примененный в работах [1–4], а также в многих других доказательствах нижних оценок схемной сложности.

Существенную роль в доказательстве играет идея о выборе вспомогательной меры сложности при помощи решения задачи линейного программирования. Этот подход был предложен в работе [6].

Работа выполнена при финансовой поддержке РФФИ, проект № 18–01–00337.

Список литературы

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

2. Редькин Н. П. О минимальной реализации линейной функции схемой из функциональных элементов // Кибернетика. — 1971. — 6. — С. 31–38.

3. Шкребела И. С. О сложности реализации линейных булевых функций схемами из функциональных элементов в базисе $\{x \to y, \overline{x}\}$ // Дискрет. матем. — 2003. — 15, 4. — С. 100–112.

4. Wegener I., The complexity of the parity function in unbounded fan-in, unbounded depth circuits // Theoretical Computer Science. — 1991. — 85. — P. 155–170.

5. Комбаров Ю. А. Верхняя оценка сложности реализации линейных функций схемами в одном базисе из многовходовых элементов // Вестник Московского университета. Серия 1. — 2015. — 5. — С. 47—50.

6. Find M. G., Golovnev A., Hirsch E. A., Kulikov A. S. A better-than-3n lower bound for the circuit complexity of an explicit function //

2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS) — 2016. — P. 89–98.

О СЛОЖНОСТИ РЕАЛИЗАЦИИ СИСТЕМЫ ИЗ ДВУХ МОНОМОВ СХЕМАМИ КОМПОЗИЦИИ

С. А. Корнеев (Москва)

Мономом над множеством переменных $X = \{x_1, x_2, \ldots, x_q\}$ будем называть выражение вида ${x_1}^{a_1} {x_2}^{a_2} \ldots {x_q}^{a_q}$, где $a_1, a_2, \ldots, a_q$ — целые неотрицательные числа, причём $a_1 + a_2 + \ldots + a_q > 0$. Если $a_1 + a_2 + \ldots + a_q = 0$, то такое выражение будем называть *нулевым мономом*.

Следуя [1] и [2] введём понятие композиции мономов. Пусть $U = {x_1}^{a_{11}} {x_2}^{a_{12}} \ldots {x_q}^{a_{1q}}$, $V = {x_1}^{a_{21}} {x_2}^{a_{22}} \ldots {x_q}^{a_{2q}}$ — мономы, $R = {x_1}^{a_{31}} {x_2}^{a_{32}} \ldots {x_q}^{a_{3q}}$ — моном (возможно, нулевой), и для всех $k = 1, \ldots, q$ выполнены условия $a_{3k} \le a_{1k}$ и $a_{3k} \le a_{2k}$. Тогда моном

$$(U, V)_R = \frac{UV}{R} = {x_1}^{a_{11}+a_{21}-a_{31}} {x_2}^{a_{12}+a_{22}-a_{32}} \ldots {x_q}^{a_{1q}+a_{2q}-a_{3q}}$$

называется *композицией мономов U и V относительно монома R*.

Схемой композиции над системой мономов $M = \{U_1, \ldots, U_r\}$ будем называть такую последовательность мономов

$$(U_1, \ldots, U_r, U_{r+1}, \ldots, U_{r+n}), \tag{1}$$

что для любого $k = r+1, \ldots, r+n$ найдутся такие натуральные числа s и t и такой моном R_k (возможно, нулевой), что $s < k$, $t < k$ и

$$U_k = (U_s, U_t)_{R_k}.$$

Схему композиции над системой мономов $X = \{x_1, x_2, \ldots, x_q\}$ будем называть *схемой композиции над множеством переменных X* или просто *схемой композиции*. Если S — схема композиции вида (1), то под *сложностью $l_{sh}(S)$ схемы композиции S* будем понимать число n. Будем говорить, что *схема композиции S реализует моном U*, если $U \in S$. Аналогично, *схема композиции S реализует систему мономов M*, если для каждого $U \in M$ выполнено условие $U \in S$.

Пусть M и M_0 — системы мономов. Следуя [3], положим $l_{sh}(M) = \min l_{sh}(S)$, где минимум берётся по всем схемам, реализующим систему M над множеством переменных $\{x_1, \ldots, x_q\}$. Величину $l_{sh}(M)$ будем называть *сложностью реализации системы мономов* M. Аналогично, величину $l_{sh}(M/M_0)$, определяемую равенством $l_{sh}(M/M_0) = \min l_{sh}(S)$, где минимум берётся по всем схемам, реализующим систему мономов M над системой мономов M_0, будем называть *сложностью реализации системы мономов* M *над системой мономов* M_0.

Величину $l_{sh}(M/M_0)$ также можно интерпретировать как минимально возможную сложность схемы из функциональных элементов (см., например, [4]), на входы которой подаются мономы системы M_0, на выходах вычисляются мономы системы M, а сама схема состоит из двухвходовых элементов, реализующих композицию мономов относительно некоторого монома R (вообще говоря, своего для каждого функционального элемента).

Заметим, что любой матрице из целых неотрицательных чисел размера $p \times q$ можно поставить в соответствие систему из p мономов от q переменных. С помощью этого соответствия можно ввести функции $l_{sh}(A)$ сложности реализации матрицы и $l_{sh}(A/M_0)$ сложности реализации матрицы над системой мономов.

Для произвольной матрицы A введём обозначение

$$\delta(A) = \begin{cases} 1, \text{ если в матрице A нет столбцов без нулей;} \\ 0, \text{ иначе.} \end{cases}$$

Леммы 1 и 2 позволяют свести общую задачу о сложности реализации системы из двух мономов над системой переменных $\{x_1, \ldots, x_q\}$ к задаче о сложности реализации системы из двух мономов без нулевых степеней над мономом $x_1 \ldots x_q$.

Лемма 1. *Пусть A — матрица размера $2 \times q$ без нулевых строк и столбцов, состоящая из целых неотрицательных чисел, B — матрица, полученная из матрицы A заменой всех нулей на единицы. Тогда*

$$l_{sh}(B) = l_{sh}(A) + \delta(A).$$

Лемма 2. *Пусть $x_1, x_2, \ldots, x_r$ — все общие переменные мономов U_1 и U_2. Тогда*

$$l_{sh}(\{U_1, U_2\}) = l_{sh}(\{U_1, U_2\}/\{x_1 x_2 \ldots x_r, x_{r+1}, \ldots, x_q\}) + r - 1.$$

Лемма 3 доставляет нижнюю оценку для матрицы произвольного размера $p \times q$, которая для матрицы размера $2 \times q$ оказывается оптимальной.

Лемма 3. *Пусть в матрице*

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1q} \\ a_{21} & a_{22} & \dots & a_{2q} \\ \dots & \dots & \dots & \dots \\ a_{p1} & a_{p2} & \dots & a_{pq} \end{pmatrix}$$

все элементы — натуральные числа. Тогда

$$l_{sh}(A/x_1x_2\dots x_q) \geq \max_{(i_1\dots i_p)\in S_p} \sum_{k=1}^{p} \left\lceil \log \max \left(\max_{1\leq j\leq q} \left(\frac{a_{i_k j}}{\max\limits_{l<k} a_{i_l j}} \right), 1 \right) \right\rceil,$$

где S_p обозначает группу перестановок множества $\{1, 2, \dots, p\}$.

Заключительная теорема устанавливает точное значение сложности реализации системы из двух мономов.

Теорема. *Пусть в матрице*

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1q} \\ a_{21} & a_{22} & \dots & a_{2q} \end{pmatrix}$$

все элементы — целые неотрицательные числа. Тогда:

$$1)\ l_{sh}(A) = \max(t_1 + t_{21}, t_2 + t_{12}) + q - 1 + \delta(A),$$

$$2)\ l_{sh}(A) = \max_{1\leq k,l\leq q} l_{sh} \begin{pmatrix} b_{1k} & b_{1l} \\ b_{2k} & b_{2l} \end{pmatrix} + q - 2 + \delta(A),$$

где

$$b_{ij} = \max(a_{ij}, 1), \quad i = 1, 2, \quad j = 1, \dots, q,$$

$$t_1 = \left\lceil \log \max_{1\leq k\leq q} b_{1k} \right\rceil, t_2 = \left\lceil \log \max_{1\leq k\leq q} b_{2k} \right\rceil,$$

$$t_{12} = \left\lceil \log \max_{1\leq k\leq q} \frac{b_{1k}}{b_{2k}} \right\rceil, t_{21} = \left\lceil \log \max_{1\leq k\leq q} \frac{b_{2k}}{b_{1k}} \right\rceil.$$

Список литературы

1. Ширшов А. И. Некоторые алгоритмические проблемы для алгебр Ли // Сиб. матем. журнал. — 1962. — Т. 3. — С. 292–296.

2. Мерекин Ю. В. О порождении слов с использованием операции композиции // Дискретн. анализ и исслед. опер. — 2003. — Т. 10, № 4. — С. 70–78.

3. Трусевич Е. Н. О сложности некоторых систем одночленов схемами композиции // Вестник московского университета. Сер. 1. Математика. Механика. — 2014. — № 5. — С. 18–22.

4. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во Моск. ун-та, 1984. — 138 с.

ДИСКРЕТНАЯ ПОСТАНОВКА ЗАДАЧИ О СЛОЖНОСТИ ВЫЧИСЛЕНИЯ РАССТОЯНИЯ МЕЖДУ ХАУСДОРФОВЫМИ ПРОСТРАНСТВАМИ

Н. Н. Косовский, Т. М. Косовская
(Санкт-Петербург)

В геометрии широко используется расстояние по Громову–Хаусдорфу между компактными метрическими пространствами. Для метрических пространств X и Y рассматриваются всевозможные изометрические (то есть сохраняющие расстояния) их вложения f в третье пространство Z. Тогда

$$d_{GH}(X,Y) = \inf_f\{d_H(f(X), g(Y))\},$$

где d_H — расстояние по Хаусдорфу между подмножествами метрических пространств

$$d_H(A,B) = \max\{\sup_{a\in A}\{d(a,B)\}, \sup_{b\in B}\{d(b,A)\}\}.$$

Если X и Y — метрические пространства, и $R \subset X \times Y$ — "многозначное сюръективное отображение" (далее — *соответствие*) между ними, то его *искажением* называется

$$\operatorname{dis} R = sup_{x_1,x_2\in X; y_1,y_2\in Y}\{|d_X(x_1,x_2) - d_Y(y_1,y_2)|\},$$

Расстояние по Громову–Хаусдорфу можно задать [1, теорема 7.3.25] через инфимум искажений соответствий между пространствами. А именно,

$$d_{GH}(X,Y) = \frac{1}{2}\inf_R\{\operatorname{dis} R\}.$$

Для того, чтобы оценить расстояние между двумя компактными пространствами, можно рассмотреть расстояние между их конечными ε-сетями. Действительно, расстояние между пространством и его ε-сетью не превосходит ε, а значит расстояние между пространствами и их ε-сетями отличается не больше, чем на 2ε.

Конечной ε-сети можно сопоставить взвешенный полный псевдограф, в каждой вершине которого есть петля, $G = (V, E, W)$, а вес ребра — расстояние между соответствующими точками в метрическом пространстве.

В дальнейшем будет оцениваться удвоенное расстояние по Громову–Хаусдорфу между конечными пространствами. Для упрощения ситуации будем считать все расстояния рациональными числами. Таким образом, мы имеем

— два взвешенных псевдографа $G_1 = (V_1, E_1, W_1)$ и $G_2 = (V_2, E_2, W_2)$, где W_k – веса рёбер $w_{ij}^k \in Q_+$ при $i = 1, \ldots, n_k$, $j = 1, \ldots, n_k$, каждый из которых представляет собой полный взвешенный граф с n_k $(k = 1, 2)$ вершинами. В каждой вершине v^k графа G_k $(k = 1, 2)$ имеется петля $\{v^k, v^k\}$ веса 0;

— отношение $R \subset V_1 \times V_2$, проекции которого на V_1 и на V_2 совпадают с V_1 и V_2 соответственно.

Определение. Если $(v_{i_1}^1, v_{i_2}^2) \in R$ и $(v_{j_1}^1, v_{j_2}^2) \in R$, то расстоянием между рёбрами $e_{l_1}^1 = \{v_{i_1}^1, v_{j_1}^1\}$ и $e_{l_2}^2 = \{v_{i_2}^2, v_{j_2}^2\}$ при отношении R называется абсолютная величина разности весов этих рёбер

$$\rho_R(e_{l_1}^1, e_{l_2}^2) = |w_{i_1 j_1}^1 - w_{i_2 j_2}^2|$$

.

Определение. Расстоянием $\rho_R(G_1, G_2)$ между графами G_1 и G_1 при отношении R называется максимум по всем рёбрам графа G_1 расстояний до всех рёбер в графе G_2, находящихся с ними в отношении R

$$\rho_R(G_1, G_2) = \max_{e_{l_1}^1 \in E_1,\ e_{l_2}^2 \in f(e_{l_1}^1)} \rho_R(e_{l_1}^1,\ e_{l_2}^2).$$

Определение. Расстоянием $\rho(G_1, G_2)$ между графами G_1 и G_2 называется минимум по всем отношениям $R \subseteq V_1 \times V_2$, проекции которых R_{V_1} и R_{V_2} на V_1 и на V_2 совпадают с V_1 и V_2 соответственно, расстояний между графами G_1 и G_2 при отношении R

$$\rho(G_1, G_2) = \min_{R: R_{V_1} = V_1\ \&\ R_{V_2} = V_2} \rho_R(G_1, G_2).$$

По определению это удвоенное расстояние по Громову–Хаусдорфу между конечными метрическими пространствами, если графы произошли из метрических пространств.

В результате имеем следующую задачу.

Расстояние между графами по Громову–Хаусдорфу (РГГХ).

Дано. Два взвешенных псевдографа $G_1 = (V_1, E_1, W_1)$ и $G_2 = (V_2, E_2, W_2)$, где W_k – веса рёбер $w_{ij}^k \in Q_+$ при $i = 1, \ldots, n_k$, $j = 1, \ldots, n_k$, каждый из которых представляет собой полный взвешенный граф с n_k $(k = 1, 2)$ вершинами. В каждой вершине v^k графа G_k $(k = 1, 2)$ имеется петля $\{v^k, v^k\}$ веса 0.

$B \in Q_+$. (Вместо Q_+ может быть взято любое конструктивное множество положительных чисел.)

Вопрос. Верно ли, что $\rho(G_1, G_2) \leq B$.

Утверждение. *Задача* **РГГХ** *принадлежит классу* **NP**.

Рассмотрим задачу **Изоморфизм графов (ИГ)** [2].

Каждому из графов H_k $(k = 1, 2)$ поставим в соответствие полный взвешеный граф с петлями на каждой вершине G_k, веса в котором определены следующим образом. Если ребро e является ребром в H_k, то его вес равен 1, если ребро e является ребром в дополнении к H_k, то его вес равен 2, петли (т.е. рёбра вида $\{v, v\}$) имеют вес 0.

Расстояние по Громову–Хаусдорфу между соответсвующими метрическими пространствами равно нулю тогда и только тогда, когда метрические прострaства изометричны ([1], Теорема 7.3.30), а в данном случае это означает, что графы изоморфны. То есть графы H_1 и H_2 изоморфны тогда и только тогда, когда расстояние между G_1 и G_2 равно нулю.

Вопрос в задаче **ИГ** можно переформулировать так: верно ли, что расстояние по Громову–Хаусдорфу между построенными выше графами G_1 и G_2 не превосходит нуля.

Утверждение. *Задача* **ИГ** *является сужением задачи* **РГГХ** *при* $B = 0$ *и взвешенными псевдографами* G_1 *и* G_1*, полученными из* H_1 *и* H_2 *описанным выше способом.*

По псевдографам G_1 и G_1 можно построить граф G, "вершинами"которого являются рёбра G_1 и G_1, а "ребрами— те пары рёбер G_1 и G_1, расстояния между которыми меньше B.

Утверждение. *Задача* **РГГХ** *является подзадачей задачи* **Индуцированный подграф со свойством** П [2, *стр.* 243, ТГ21]*, в*

которой в качестве свойства Π *взято следующее отношение*

$$\begin{array}{l}\{v^1,u^1:\exists v^2u^2(\{\{v^1,u^1\},\{v^2,u^2\}\}\in E)\}=V_1\ \&\\ \{v^2,u^2:\exists v^1u^1(\{\{v^1,u^1\},\{v^2,u^2\}\}\in E)\}=V_2\end{array}\quad .$$

.

Список литературы

1. Бураго Д. Ю., Бураго Ю. Д., Иванов С. В. Курс метрической геометрии. — Ижевск: РХД, 2004.

2. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи: путеводитель по NP-полноте. — М.: Мир, 1982.

О СЛОЖНОСТИ СИСТЕМ ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ В ДВУХ БЕСКОНЕЧНЫХ БАЗИСАХ

В. В. Кочергин, А. В. Михайлович (Москва)

В работе исследуется сложность реализации систем функций k-значной ($k \geq 2$) логики схемами из функциональных элементов в бесконечных базисах B_P и B_L, состоящих из всех монотонных (относительно порядка $0 < 1 < \ldots < k-1$) функций k-значной логики, к которым добавляется одна немонотонная функция: для базиса B_P такой функцией является отрицание Поста, т. е. функция $N_P(x) = x + 1 \pmod k$, а для базиса B_L — отрицание Лукасевича, т. е. функция $N_L(x) = k - 1 - x$. Эти две задачи тесно связаны с задачей о немонотонной сложности (характеризующей число только немонотонных элементов в схеме — см., например, [1]) функций k-значной логики в базисах B_P и B_L, которая, в свою очередь, является обобщением классической задачи [2, 3] об инверсионной сложности булевых функций.

Дадим необходимые определения.

Пусть P_k ($k \geq 2$) — множество всех функций k-значной логики, M — класс всех функций из P_k, монотонных относительно порядка $0 < 1 < \ldots < k-1$.

Обозначим $E_k = \{0, 1, \ldots, k-1\}$. Последовательность $\tilde{\alpha}_1, \tilde{\alpha}_2, \ldots, \tilde{\alpha}_r$ наборов из множества E_k^n назовем *цепью относительно порядка*

$0 < 1 < \ldots < k-1$, если все наборы $\tilde{\alpha}_i = (\alpha_{i1}, \ldots, \alpha_{in})$ различны и выполняются неравенства $\alpha_{ij} \leq \alpha_{i+1,j}$, $i = 1, \ldots, r-1$, $j = 1, \ldots, n$.

Пусть $f(x_1, \ldots, x_n) \in P_k$. Упорядоченную пару наборов $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_n)$, $\tilde{\alpha}, \tilde{\beta} \in E_k^n$, будем называть *обрывом для функции* f, если $\alpha_j \leq \beta_j$ для всех $j = 1, \ldots, n$, но при этом $f(\tilde{\alpha}) > f(\tilde{\beta})$.

Обрывом для системы функций будем называть любую пару наборов, являющуюся обрывом хотя бы для одной функции системы.

Под *падением* $d_C(F)$ *системы* $F \subset P_k$ *на цепи* C будем понимать число обрывов для системы F на парах соседних наборов цепи C.

Спад $d(F)$ системы F определим равенством $d(F) = \max d_C(F)$, где максимум берется по всем цепям C.

Для произвольной системы функций $F \subset P_k$ и полного в P_k базиса B обозначим через $L_B(F)$ и $I_B(F)$ обычную сложность и немонотонную сложность системы F в базисе B, т. е. минимальное число всех элементов и, соответственно, немонотонных элементов в схемах, реализующих систему F в базисе B.

А. А. Марковым для случая реализации системы булевых функций в базисе $B_0 = M \cup \{\overline{x}\}$ установлено [2, 3] точное значение инверсионной сложности:

$$I_{B_0}(F) = \lceil \log_2(d(F) + 1) \rceil .$$

В работе [1] этот результат обобщен на случай реализации произвольной системы функций k-значной логики в базисах B_P и B_L:

$$I_{B_P}(F) = \lceil \log_2(d(F) + 1) \rceil , \quad I_{B_L}(F) = \lceil \log_k(d(F) + 1) \rceil .$$

Для меры сложности, соответствующей общему числу всех элементов в схеме, для случая реализация одной функции k-значной логики в базисах B_P и B_L в работах [4, 5] получены нижние и верхние оценки, отличающиеся для базиса B_P не более чем на 1, а для базиса B_L — не более чем на 2. Точные формулировки требуют введения дополнительных обозначений, поэтому сформулируем их в упрощенном виде: для любой функции $f \in P_k$ при $k \geq 3$ выполняется равенство

$$L_{B_P}(f) = 3 \log_3(d(f) + 1) + O(1) \quad (\text{при } k \geq 3),$$
$$L_{B_L}(f) = 2 \log_k(d(f) + 1) + O(1) \quad (\text{при } k \geq 2).$$

Теперь сформулируем полученные для этой меры результаты о сложности реализации систем функций k-значной логики в базисах B_P и B_L.

Теорема 1. *Для любой системы функций* $F = \{f_1, f_2, \ldots, f_m\} \subset P_k$, $k \geq 3$, *выполняются неравенства*

$$3\left(\lceil \log_3(d(F)+1)\rceil - 1\right) + \tau(d(F)+1) - 1 \leq L_{B_P}(F) \leq \\ \leq 3\left(\lceil \log_3(d(F)+1)\rceil - 1\right) + \tau(d(F)+1) + m,$$

где

$$\tau(n) = \begin{cases} 1, & \text{если } 3^r < n \leq 4 \times 3^{r-1} \text{ для некоторого целого } r; \\ 2, & \text{если } 4 \times 3^{r-1} < n \leq 2 \times 3^r \text{ для некоторого целого } r; \\ 3, & \text{если } 2 \times 3^r < n \leq 3 \times 3^r \text{ для некоторого целого } r. \end{cases}$$

Теорема 2. *Для любой системы функций* $F = \{f_1, f_2, \ldots, f_m\} \subset P_k$, $k \geq 2$, *выполняются неравенства*

$$2\lceil \log_k(d(F)+1)\rceil - 1 \leq L_{B_P}(F) \leq 2\lceil \log_k(d(F)+1)\rceil + m.$$

Работа первого автора выполнена при частичной финансовой поддержке РФФИ, проект № 18–01–00337.

Список литературы

1. Кочергин В. В., Михайлович А. В. О минимальном числе отрицаний при реализации систем функций k-значной логики // Дискретная математика. — 2016. — Т. 28, вып. 4. — С. 80–90.

2. Марков А. А. Об инверсионной сложности систем функций // ДАН СССР. — 1957. — Т. 116, № 6. — С. 917–919.

3. Марков А. А. Об инверсионной сложности систем булевых функций // ДАН СССР. — 1963. — Т. 150, № 3. — С. 477–479.

4. Кочергин В. В., Михайлович А. В. О сложности функций многозначной логики в одном бесконечном базисе // Дискретный анализ и исследование операций. — 2018. — Т. 25, № 1. — С. 42–74.

5. Кочергин В. В., Михайлович А. В. О схемной сложности функций k-значной логики в одном бесконечном базисе // Прикладная математика и информатика. — 2018. — № 58. — С. 21–34.

СИНТЕЗ И ОПТИМИЗАЦИЯ УПРАВЛЯЮЩЕЙ СИСТЕМЫ ОБСЛУЖИВАНИЯ НЕОДНОРОДНЫХ ТРЕБОВАНИЙ

Е. В. Кудрявцев, М. А. Федоткин
(Нижний Новгород)

В работе рассматривается система E адаптивного управления конфликтными потоками Π_1 и Π_2 разнотипных требований, вероятностная модель которой представляется в виде упорядоченной тройки $(\Omega, \mathfrak{F}, \mathbf{P}(\cdot))$. Здесь Ω — множество описаний ω элементарных исходов управляющей системы, $\mathfrak{F}$ — сигма-алгебра исходов $A \subset \Omega$ и $\mathbf{P}(\cdot)$ — вероятность на $\mathfrak{F}$. Для построения вероятностной модели $(\Omega, \mathfrak{F}, \mathbf{P}(\cdot))$ был использован кибернетический подход Ляпунова–Яблонского. Кибернетический подход подразумевает наблюдение за системой в дискретные моменты времени $\tau_i(\omega), i = 0, 1, \ldots$, и представление управляющей системы в виде схемы с определенными блоками, выделение информации, координат и функций. Схема управляющей системы отражает ее структурное строение и позволяет выделить связи между ее блоками. Схема системы включает следующие структурные блоки: входные полюса, внешнюю память, блок по переработке внешней памяти, внутреннюю память, блок по переработке внутренней памяти и выходные полюса. Перейдем к математическому описанию структурных блоков.

При $j = 1, 2$ обозначим через $\eta_{j,i}$ случайное число заявок потока Π_j, которые поступили в систему на интервале $[\tau_i; \tau_{i+1})$, и $\eta_i = (\eta_{1,i}, \eta_{2,i})$. Тогда последовательность $\{\eta_i;\, i \geq 0\}$ является математическим описанием входного полюса первого типа. Пусть $\xi_{j,i}$ — максимально возможное число заявок потока Π_j, которые система может обслужить на интервале $[\tau_i, \tau_{i+1})$, и $\xi_i = (\xi_{1,i}, \xi_{2,i})$. Тогда последовательность $\{\xi_i;\, i \geq 0\}$ является математическим описанием входного полюса второго типа.

Внешней памятью являются неограниченные накопители очередей O_1 и O_2 по входным потокам Π_1 и Π_2. Если через случайные величины $\kappa_{1,i}$ и $\kappa_{2,i}$ обозначить количество требований в накопителях O_1 и O_2 в момент τ_i и принять $\kappa_i = (\kappa_{1,i}, \kappa_{2,i})$, то последовательность $\{\kappa_i;\, i \geq 0\}$ будет являться математическим описанием блока внешней памяти.

Внутренней памятью является обслуживающее устройство с 8 состояниями $\Gamma = \{\Gamma^{(1)}, \Gamma^{(2)}, \ldots, \Gamma^{(8)}\}$. Состоянием внутренней памяти на интервале $[\tau_i, \tau_{i+1})$ обозначим через $\Gamma_i(\omega) \in \Gamma$. Математическим

описанием блока внутренней памяти является последовательность $\{\Gamma_i;\, i \geq 0\}$.

Блок по переработке внешней памяти задается следующими рекуррентными соотношениями

$$\kappa_{j,i+1} = \begin{cases} \max\{0, \kappa_{j,i} + \eta_{j,i} - \xi_{j,i}\}, & \text{если } \Gamma_i \in \Gamma \backslash \{\Gamma^{(3)}, \Gamma^{(6)}\}; \\ \eta_{j,i} + \max\{0, \kappa_{j,i} - \xi_{j,i}\}, & \text{если } \Gamma_i \in \{\Gamma^{(3)}, \Gamma^{(6)}\}. \end{cases}$$

Блок по переработке внутренней памяти задается рекуррентными функциональными соотношениями

$$\Gamma_{i+1} = u(\Gamma_i, \kappa_i, \eta'_i) =$$
$$= \begin{cases} \Gamma^{(3j-2)}, & \left\{\left[\Gamma_i = \Gamma^{(3s)}\right] \& \left[(\kappa_{j,i} > 0) \vee (\kappa_{s,i} \geq K_s) \vee (\eta'_i = y_j)\right]\right\} \vee \\ & \vee \left\{\left[\Gamma_i = \Gamma^{(3j)}\right] \&[\kappa_{s,i} = 0] \&[\kappa_{j,i} \leq K_j] \&[\eta'_i = y_j]\right\}, \\ \Gamma^{(3j-1)}, & \left\{\Gamma_i = \Gamma^{(3j-2)}\right\} \vee \left\{\left[\Gamma_i = \Gamma^{(6+j)}\right] \&[\eta'_i = y_j]\right\}, \\ \Gamma^{(3j)}, & \left\{\Gamma_i = \Gamma^{(3j-1)}\right\} \vee \left\{\left[\Gamma_i = \Gamma^{(6+j)}\right] \&[\eta'_i \neq y_j]\right\}, \\ \Gamma^{(6+j)}, & \left[\Gamma_i = \Gamma^{(3s)}\right] \&[\kappa_{j,i} = 0] \&[\kappa_{s,i} < K_s] \&[\eta'_i = y_0]. \end{cases}$$

Здесь случайная величина η'_i определяется очередностью поступления заявок по потокам и принимает значения $y_0 = (0,0)$, $y_1 = (1,0)$, $y_2 = (0,1)$. Константы K_1 и K_2 определяют некоторые пороговые длины очередей по потокам Π_1 и Π_2.

Обозначим через $\overline{\xi}_{j,i}$ случайное число заявок потока Π_j, которые реально покинут систему на интервале $[\tau_i, \tau_{i+1})$, и $\overline{\xi}_i = (\overline{\xi}_{1,i}, \overline{\xi}_{2,i})$. Тогда последовательность $\{\overline{\xi}_i; i \geq 0\}$ определяет выходной полюс, где

$$\overline{\xi}_{j,i} = \begin{cases} \min\{\kappa_{j,i} + \eta_{j,i}; \xi_{j,i}\}, & \text{если } \Gamma_i \in \Gamma \backslash \{\Gamma^{(3)}, \Gamma^{(6)}\}; \\ \min\{\kappa_{j,i}; \xi_{j,i}\}, & \text{если } \Gamma_i \in \{\Gamma^{(3)}, \Gamma^{(6)}\}. \end{cases}$$

Состояние системы на i-м такте времени $[\tau_i, \tau_{i+1})$ описывается случайным элементом $(\Gamma_i(\omega), \kappa_i(\omega))$ [1]. Математическими моделями системы управления конфликтными потоками разнотипных требований в классе адаптивных алгоритмов являются векторные последовательности $\{(\Gamma_i, \kappa_i);\, i = 0, 1, \ldots\}$ и $\left\{(\Gamma_i, \kappa_i, \overline{\xi}_i);\, i = 0, 1, \ldots\right\}$.

Для данных последовательностей доказаны теоремы марковости и проведены классификации их состояний. В частности для $\{(\Gamma_i, \kappa_i);\, i = 0, 1, \ldots\}$ имеют место следующие утверждения.

Лемма. *Случайная последовательность* $\{(\Gamma_i, \kappa_i); i = 0, 1, \ldots\}$ *с заданным начальным распределением вектора* $\{(\Gamma_0, \kappa_0)\}$ *является марковской.*

Теорема. *Пусть* j, $s = 1, 2$, $j \neq s$, $x = (x_1, x_2) \in X^2$, (X — *множество целых неотрицательных чисел*) *и пусть*

$$G = \{(\Gamma^{(h)}, x) \colon \Gamma^{(h)} \in \Gamma,\, x \in X^2\},$$

$$G^{(3j-2)} = \{(\Gamma^{(3j-2)}, x_s y_s) \colon x_s < K_s - l_{3s}\},$$

$$G^{(3j-1)} = \{(\Gamma^{(3j-1)}, x_s y_s) \colon x_s < K_s - l_{3s}\},$$

$$G^{(6+j)} = \{(\Gamma^{(6+j)}, x) \colon x_j > 0\} \cup \{(\Gamma^{(6+j)}, x) \colon x_s \geq K_s - l_{3s}\},$$

$$G_j = \begin{cases} G^{(6+j)} \cup G^{(3j-2)}, \; l_{3j-2} > 0, \\ G^{(6+j)} \cup G^{(3j-2)} \cup G^{(3j-1)}, \; l_{3j-2} = 0, \end{cases}$$

где l_{3j}, l_{3j-1}, l_{3j-2} — *некоторые параметры системы. Тогда состояния из* G_j *являются несущественными и класс* $G_0 = G \backslash (G_1 \cup G_2)$ *является неразложимым апериодическим классом существенных состояний.*

К сожалению, не удается аналитически найти такие важные характеристики, как среднее время пребывания произвольного требования в системе и средние длины очередей по потокам. Необходимо изучить указанные характеристики системы в стационарном режиме. Поэтому важной задачей является определение времени достижения стационарного режима и изучение переходного процесса.

Для решения поставленных вопросов реализована имитационная модель системы адаптивного управления конфликтными потоками неоднородных требований в виде программы, написанной на языке C++. Имитационная модель позволяет не только изучить процесс управления и обслуживания неоднородных требований, но и получить реализации векторной последовательности $\{(\Gamma_i, \kappa_i);\, i \geq 0\}$. В работе предлагается метод определения момента достижения стационарного режима и метод вычисления оценок среднего времени пребывания произвольного требования в системе. На основе этого предлагается способ нахождения квазиоптимальных значений для параметров T_k, $k = 1, \ldots, 6$, K_1, K_2, n_1 и n_2.

Список литературы

1. M. Fedotkin, E. Kudryavtsev Necessary conditions for stationary distribution existence in the adaptive control system of conflict flows // Analytical and Computational Methods in Probability Theory. ACMPT 2017. Lecture Notes in Computer Science. — 2017. — 10684. — P. 83–96.

КВАНТОВОЕ УЛУЧШЕНИЕ АЛГОРИТМА ПОСТРОЕНИЯ ДЕРЕВЬЕВ РЕШЕНИЙ C5.0 ДЛЯ ЗАДАЧ КЛАССИФИКАЦИИ

И. М. Маннапов, Л. И. Сафина, К. Р. Хадиев (Казань)

Машинное обучение и квантовые вычисления — передовые направления в области теоретической кибернетики и математики. Медицина, образование, экономические и финансовые структуры, энергетические отрасли и многие другие активно используют возможности машинного обучения для решения своих задач. Квантовые вычисления позволяют ускорить алгоритмы машинного обучения.

Одной из основных задач машинного обучения является задача классификации [1]. Формальная постановка задачи следующая: даны два множества — X и Y. $X = \{x_1, \ldots, x_N\}$ — множество объектов, $x_i = \{x_1^i, \ldots, x_j^i, \ldots, x_d^i\}$ $x_j^i \in \mathbb{R}$, $Y = \{y_1, y_2, \ldots, y_N\}$ — номера существующих классов, $y_i \in [1, M]$ — номер класса, к которому принадлежит объект x_i. Необходимо построить такую классифицирующую модель, которая для нового x_{new} определит соответсвующий класс $y_{new} \in [1, M]$.

Для реализации классификатора часто используются алгоритмы Дж. Квинлана, которые строятся с помощью деревьев решений, а именно: алгоритмы Id3, C4.5 [2], C5.0, последний из которых является более усовершенствованным.

Мы предлагаем модификацию алгоритма C5.0, использующую известные квантовые алгоритмы, благодаря которым мы получили ускорение. Асимптотическая сложность C5.0 составила $O(hd(NM + N \log N))$. Предложенный квантовый алгоритм QC5.0, работающий за $O(h \log d\sqrt{d}(NM + N \log N))$.

Реализацией алгоритма приведена в [3].

Пусть d — количество атрибутов (признаков) для каждого $x_i \in X$. h — заданная глубина дерева. N — размерность X, а M — количество классов. Обозначим через D множество атрибутов. X — обучающая выборка, $X_i \in X$ — выборка, достигшая i-ого узла.

Для создания узла дерева необходимо выбрать атрибут и значение порога, по которым выборка будет распределяться по дочерним узлам. Атрибуты могут быть как числовыми значениями, так и дискретными (категории, множества, перечисления). Для числовых значений в узле хранится предикат, а для других — категориальная функция. В листьях дерева будут храниться номера классов, к которым будут принадлежать объекты, подаваемые классификатору.

Критерий выбора атрибута — соотношение прироста информации. При построении каждого нового узла необходимо найти признак, для значения которого достигается максимум функции $GR(X;B)$, вычисляется по формуле:

$$B_p = \arg\max_{p:\, p \in D} \Big(GR(X;B) \Big),$$

где $GR(X;B) = \frac{G(X;B)}{P(X;B)}$, $P(X,B) = -\sum_{i=1}^{t} \frac{|X_i|}{|X|} \log\left(\frac{|X_i|}{|X|}\right)$ — количество потенциальной информации от разбиения на тесте B. $G(X,B) = I(X) - \sum_{i=1}^{t} \frac{|X_i|}{|X|} I\left(X_i\right)$. $I(X) = -\sum_{j=1}^{M} RF\left(C_j, X\right) \log\left(RF\left(C_j, X\right)\right)$ — количество информации, необходимое для определения класса объекта из множества. $C_j = \{i : i \in \{1,\ldots,N\}, y_i = j\}$ — набор объектов из исходного множества X, которые относятся к классу $j \in \{1,\ldots,M\}$. $RF(j;X) = \frac{|C_j|}{|X|} = \frac{|C_j|}{N}$ — относительная частота тренировочных векторов из X.

Процесс построения дерева продолжится пока не будет достигнута определенная высота h либо все объекты не будут распределены по классам.

Временная сложность построения дерева составляет $O(hd(NM + N\log N))$.

Для квантового алгоритма C5.0 (QC5.0) можно ускорить поиск оптимального значения атрибута и его порогов для разбиения с помощью таких квантовых алгоритмов, как алгоритм поиска Гровера [6] и алгоритм Dürr и Høyer [5]. Алгоритм Dürr и Høyer позволяет найти максимальное (или минимальное) значение в некоторой последовательности за $O(\sqrt{K})$ операций, где K — это размер последовательности. Вероятность нахождение корректного значения в алгоритме Dürr и Høyer не менее $\frac{1}{2}$.

Ускорение достигается за счет применения алгоритма нахождения максимума и модифицированного алгоритма Гровера в нахождении признака, который максимизирует функцию $GR(X;B)$.

Вычислим вероятность успешного построения дерева. Пусть k — количество узлов в дереве без листьев. Применяя квантовые алгоритмы Гровера [4] и алгоритм Dürr и Høyer [5] для создания узла, получим вероятность не менее $\frac{1}{2}$. Каждый узел строится независимо, поэтому вероятность успешного построения дерева составит не менее $\frac{1}{2^k}$. Полученная вероятность стремится к 0. Для увеличения вероят-

ность успеха поиск $B_p = \arg\max_{p:p\in D}\left(GR(X;B)\right)$ достаточно запустить $\log d$ раз в каждом узле. Тогда вероятность успеха составит не менее $\left(1-\frac{1}{d}\right)^k$.

Подведем итоги. Классический алгоритм C5.0 работает за время $O(hd(NM + N\log N))$. Время работы квантового алгоритма QC5.0 составляет $O(h\log d\sqrt{d}(NM+N\log N))$. Вероятность корректной работы квантового алгоритма больше или равна $\left(1-\frac{1}{d}\right)^k$. При больших значениях d вероятность стремится к 1.

Список литературы

1. Quinlan J. R. Induction of decision trees // Machine learning. — 1986. — 1 (1). — P. 81–106.

2. Quinlan J. R. C4.5: Programs for Machine Learning. — Morgan Kaufmann Publishers, 1993.

3. Реализация C5.0. — `https://rulequest.com/download.html`

4. Grover L. K. A fast quantum mechanical algorithm for database search // arXiv preprint quant-ph/9605043. — 1996.

5. Dürr C., Høyer P. A quantum algorithm for finding the minimum // arXiv preprint quant-ph/9607014. — 1996.

О ПРОВЕРЯЮЩИХ И ДИАГНОСТИЧЕСКИХ ТЕСТАХ ДЛЯ КОНТАКТНЫХ СХЕМ

К. А. Попков (Москва)

Рассматривается задача синтеза легкотестируемых двухполюсных контактных схем [1], реализующих заданные булевы функции. (Слово «двухполюсная» в дальнейшем будем опускать.) Представим, что имеется контактная схема S, реализующая булеву функцию $f(\tilde{x}^n)$, где $\tilde{x}^n = (x_1, \ldots, x_n)$. Под воздействием некоторого источника неисправностей один или несколько контактов схемы S могут перейти в неисправное состояние. В качестве неисправностей контактов обычно рассматриваются их обрывы и замыкания. При обрыве контакта проводимость между его концами становится тождественно нулевой, а при замыкании — тождественно единичной. В результате

схема S вместо исходной функции $f(\tilde{x}^n)$ будет реализовывать некоторую булеву функцию $g(\tilde{x}^n)$, вообще говоря, отличную от f. Все такие функции $g(\tilde{x}^n)$ называются *функциями неисправности* данной схемы.

Введём следующие определения [2–4]. *Проверяющим тестом* для схемы S называется такое множество T наборов значений переменных $x_1, \ldots, x_n$, что для любой отличной от $f(\tilde{x}^n)$ функции неисправности $g(\tilde{x}^n)$ схемы S в T найдётся набор $\tilde{\sigma}$, на котором $f(\tilde{\sigma}) \neq g(\tilde{\sigma})$. *Диагностическим тестом* для схемы S называется такое множество T наборов значений переменных $x_1, \ldots, x_n$, что T является проверяющим тестом и, кроме того, для любых двух различных функций неисправности $g_1(\tilde{x}^n)$ и $g_2(\tilde{x}^n)$ схемы S в T найдётся набор $\tilde{\sigma}$, на котором $g_1(\tilde{\sigma}) \neq g_2(\tilde{\sigma})$. Число наборов в T называется *длиной* теста. В качестве тривиального диагностического (и проверяющего) теста длины 2^n для схемы S всегда можно взять множество, состоящее из всех двоичных наборов длины n.

Назовём проверяющий (диагностический) тест *k-проверяющим* (*k-диагностическим*), если в схеме могут быть неисправны не более k контактов, где $k \in \mathbb{N}$. Будем рассматривать такие тесты только для *k-неизбыточных схем*, в которых любая допустимая неисправность не менее одного и не более k контактов приводит к функции неисправности, отличной от исходной функции, реализуемой схемой.

Пусть зафиксирован вид неисправностей контактов и множество T является k-проверяющим тестом для некоторой контактной схемы S. Введём следующие обозначения: $D_{k\text{-П}}(T)$ — длина теста T; $D_{k\text{-П}}(S) = \min D_{k\text{-П}}(T)$, где минимум берётся по всем k-проверяющим тестам T для контактной схемы S; $D_{k\text{-П}}(f) = \min D_{k\text{-П}}(S)$, где минимум берётся по всем k-неизбыточным контактным схемам S, реализующим функцию f; $D_{k\text{-П}}(n) = \max D_{k\text{-П}}(f)$, где максимум берётся по всем булевым функциям f от n переменных. По аналогии с функциями $D_{k\text{-П}}$ можно ввести функции $D_{k\text{-Д}}$ для k-диагностического теста, зависящие от T, от S, от f и от n. Функции $D_{k\text{-П}}(n)$ и $D_{k\text{-Д}}(n)$ называются *функциями Шеннона* длины k-проверяющего и k-диагностического теста соответственно.

Для удобства над буквой D будем ставить символы «$0, 1$» или «1» в случаях, когда в схемах допускаются соответственно обрывы и замыкания контактов или только их замыкания. В данной работе рассматриваются именно эти два случая.

Будем говорить, что некоторое свойство выполняется *для почти всех булевых функций от n переменных*, если отношение числа булевых функций от n переменных, для которых это свойство не выпол-

няется, к числу всех булевых функций от n переменных (т. е. к 2^{2^n}) стремится к нулю при $n \to \infty$.

Х. А. Мадатян в [5] доказал соотношение $D^{0,1}_{1\text{-П}}(n) = O\left(\frac{2^n}{n\sqrt{n}}\right)$. В [4, с. 113, теорема 9] с использованием идей С. В. Яблонского установлено, что функция $D^{0,1}_{1\text{-Д}}(n)$ асимптотически не превосходит $\frac{2^{n+1}}{n}$; аналогично можно показать, что $D^1_{1\text{-Д}}(n) \lesssim \frac{2^n}{n}$. Н. П. Редькиным в [6] получена оценка $D^1_{1\text{-П}}(n) \lesssim 2^{\frac{n}{1+\frac{1}{2\log_2 n}}+\frac{5}{2}}$. В [7] для почти всех булевых функций f от n переменных доказаны неравенства $D^1_{1\text{-П}}(f) \leqslant 4$ и $D^1_{1\text{-Д}}(f) \leqslant 8$.

Несложно показать, что для любой булевой функции $f(\tilde{x}^n)$ и любого $k \in \mathbb{N}$ справедливо равенство $D^1_{k\text{-П}}(f) = D^1_{1\text{-П}}(f)$. Отсюда следует, что в неравенствах $D^1_{1\text{-П}}(n) \lesssim 2^{\frac{n}{1+\frac{1}{2\log_2 n}}+\frac{5}{2}}$, $D^1_{1\text{-П}}(f) \leqslant 4$ из [6, 7] нижний индекс 1 у буквы D можно заменить на k.

Получены следующие новые результаты.

Теорема. *Для почти всех булевых функций f от n переменных выполняется равенство $D^1_{k\text{-П}}(f) = 2$ для любого $k \in \mathbb{N}$.*

Теорема. *При условии $k = k(n) \leqslant 2^{n-4}$ для почти всех булевых функций f от n переменных выполняется соотношение $D^1_{k\text{-Д}}(f) \leqslant 2k + 2$.*

Данные две теоремы при $k = 1$ улучшают упомянутые оценки из [7].

Назовём булеву функцию $f_2(\tilde{x}^n)$ *родственной* булевой функции $f_1(\tilde{x}^n)$, если существуют такие попарно различные индексы $i_1, \ldots, i_n$ от 1 до n и такие булевы константы $\sigma_1, \ldots, \sigma_n$, что $f_2(\tilde{x}^n) = f_1(x_{i_1}^{\sigma_1}, \ldots, x_{i_n}^{\sigma_n})$.

Теорема. *Пусть $f(\tilde{x}^n)$ — булева функция. Справедливо равенство*

$$D^{0,1}_{1\text{-П}}(f) = \begin{cases} 0, & \text{если } f \equiv 0 \text{ или } f \equiv 1, \\ 2, & \text{если } f \text{ родственна функции } x_1, \\ 3, & \text{если } f \text{ родственна одной из функций } x_1x_2,\ x_1 \vee x_2. \end{cases}$$

В остальных случаях $D^{0,1}_{1\text{-П}}(f) \geqslant 4$.

Теорема. *Для почти всех булевых функций f от n переменных выполняется равенство $D^{0,1}_{1\text{-П}}(f) = 4$.*

Теорема. *Для почти всех булевых функций f от n переменных выполняется неравенство $D^{0,1}_{1\text{-Д}}(f) \leqslant 8$.*

Список литературы

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

2. Яблонский С. В. Надёжность и контроль управляющих систем // Материалы Всесоюзного семинара по дискретной математике и ее приложениям (Москва, 31 января–2 февраля 1984 г.). — М.: Изд-во МГУ. — 1986. — С. 7–12.

3. Яблонский С. В. Некоторые вопросы надёжности и контроля управляющих систем // Математические вопросы кибернетики. Вып. 1. — М.: Наука, 1988. — С. 5–25.

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

5. Мадатян Х. А. Построение единичных тестов для контактных схем — Сборник работ по математической кибернетике. — М.: ВЦ АН СССР, 1981. — С. 77–86.

6. Редькин Н. П. О проверяющих тестах замыкания и размыкания // Методы дискретного анализа в оптимизации управляющих систем. — Вып. 40. — Новосибирск: Институт математики СО АН СССР, 1983. — С. 87–99.

7. Попков К. А. О тестах замыкания для контактных схем // Дискретная математика. — 2016. — Т. 28, вып. 1. — С. 87–100.

О СЛОЖНОСТИ МОНОТОННЫХ СХЕМ ДЛЯ СИММЕТРИЧЕСКИХ ПОРОГОВЫХ ФУНКЦИЙ

И. С. Сергеев (Москва)

В работе рассматривается сложность реализации пороговых симметрических булевых функций схемами из функциональных элементов над базисом $\{\vee, \wedge\}$. Сложность функции f над указанным базисом далее обозначается через $C(f)$. Подробное изложение используемых понятий можно найти в [1].

Через T_n^k обозначается пороговая симметрическая функция n переменных с порогом k. По определению,

$$T_n^k(x_1, \ldots, x_n) = (x_1 + \ldots + x_n \geq k).$$

Через S_n^k обозначим булев (k,n)-оператор, составленный из первых k пороговых функций: $S_n^k = (T_n^1, T_n^2, \ldots, T_n^k)$.

Известно, что $C(S_n^n) = \Theta(n \log n)$: нижняя оценка доказана в [2], а верхняя — в [3]. При постоянном k из работы Яо [4] вытекает оценка

$$C(S_n^k) \le 2(p+1)n + O\left(\log^r n\right), \tag{1}$$

где $p = \lfloor \log_2 k \rfloor$ и $r = \lceil \log_2((k+1)/3) \rceil$. При $k \le 5$ лучшие оценки

$$C(S_n^k) \le kn + O(n^{1-1/k}) \tag{2}$$

дает конструкция Адлемана (см., например, [5]).

Метод [4] ориентирован на построение схем компараторов. При адаптации его к монотонным схемам получается следующий результат.

Теорема 1. *При постоянном k справедливы оценки:*
(i) $C(S_n^k) \le 2pn + O(\sqrt{n})$, *если* $2^p \le k < 3 \cdot 2^{p-1}$;
(ii) $C(S_n^k) \le (2p+1)n + O\left(\log^p n\right)$, *если* $3 \cdot 2^{p-1} \le k < 2^{p+1}$.

Оценки теоремы уточняют (1) и превосходят (2) при всех $k \ge 3$.

Известно, что сложность функции T_n^2 не меньше $2n-3$ даже в полном базисе из всех двуместных булевых функций [6]. Для монотонного базиса получена чуть лучшая оценка $C(T_n^2) \ge 2n + \log_2 n - 4$ (см. [5]). На самом деле, можно показать, что при $k = 2$ остаточный член в (2) точен по порядку. Справедлива

Теорема 2. $C(T_n^2) \ge 2n + \sqrt{2n/3} - O(1)$.

Известные конструкции схем, доставляющие верхнюю оценку (2), имеют глубину 3: все конъюнкторы в них расположены на одном уровне. В классе таких схем оценка сложности (обозначим соответствующий функционал через C_3) может быть установлена с более высокой точностью. Имеет место

Теорема 3. $C_3(T_n^2) = 2n + 2\sqrt{n} + O(\sqrt[4]{n}) - O(1)$.

Для следующей пороговой функции T_n^3 П. Дунн получил нижнюю оценку $C(T_n^3) \ge 2.5n - 5.5$ в [7]. Доказанная им в [8] более общая оценка при $3 \le k \le n/2$ имеет вид

$$C(T_n^k) \ge \max\{2n + 3k,\ 2.5n + 1.5k\} - O(1) \tag{3}$$

и принимает максимальное значение $3.5n - O(1)$ для функции голосования $T_n^{n/2}$. Первая оценка может быть усилена.

Теорема 4. *Если* $n \ge 4$, *то* $C(T_n^3) \ge 3n - 5$.

Как следствие теорем 1 и 4, $C(T_n^3) = 3n + O(\log n) - O(1)$.

Кроме того, теорема 4 позволяет упростить вид общей оценки (3) до $C(T_n^k) \geq 3n + k - O(1)$ при $3 \leq k \leq n/2$ (см. также [5]).

Работа выполнена при поддержке РФФИ, проект № 19–01–00294а.

Список литературы

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

2. Lamagna E. A., Savage J. E. Combinational complexity of some monotone functions // Proc. 15th IEEE Symp. on Switching and Automata Theory. — New Orleans: IEEE, 1974. — P. 140–144.

3. Ajtai M., Komlós J., Szemerédi E. Sorting in $c \log n$ parallel steps // Combinatorica. — 1983. — V. 3, no. 1. — P. 1–19.

4. Yao A. C. Bounds on selection networks // SIAM J. on Computing. — 1980. — V. 9, no. 3. — P. 566–582.

5. Wegener I. The complexity of Boolean functions — Stuttgart: Wiley–Teubner, 1987.

6. Клосс Б. М., Малышев В. А. Оценки сложности некоторых классов функций // Вестник Моск. унив. Серия 1. Матем. Мех. — 1965. — 4. — С. 44–51.

7. Dunne P. E. A $2.5n$ lower bound on the monotone network complexity of T_3^n // Acta Inf. — 1985. — V. 22. — P. 229–240.

8. Dunne P. E. Lower bounds on the monotone network complexity of threshold functions // Proc. 22nd Allerton Conf. on Communication, Control and Computing. — 1984. — P. 911–920.

СЛОЖНОСТЬ СИНТЕЗА МНОГОСЛОЙНЫХ СХЕМ

Т. Р. Сытдыков (Ташкент), Г. В. Калачев (Москва)

Задача синтеза схем из функциональных элементов, обладающих оптимальной или субоптимальной сложностью, интенсивно исследовалась с середины XX века в связи с развитием вычислительной техники. Асимптотическая оценка функции Шеннона сложности СФЭ была получена Лупановым [1]. В более поздних работах исследовалась сложность схем, структура которых учитывает различные практические ограничения — расположение в пространстве или на плоскости, разводку проводов и др. Коршунов в [2] получил

оценки сложности для СФЭ, размещенных в трехмерном пространстве с ограничениями на расстояния между элементами и проводами, а также на длины проводов. Кравцов в [3] исследовал плоские схемы, элементы которых размещены в клетках прямоугольной решетки. Клеточные схемы изучались и в ряде более поздних работ (например, в [4, 5]).

Поскольку оценки сложности, полученные для плоских и объемных схем, превосходят по порядку оценку Лупанова $\frac{2^n}{n}$, возникает задача обобщения модели плоских либо пространственных схем так, чтобы уменьшить порядок функции Шеннона и в тоже время оставить модель в некотором смысле естественной, приближенной к реально существующих схемам. В данной работе рассматривается подобное обобщение — многослойные схемы.

В качестве базиса СФЭ будем рассматривать все булевы функции от не более чем двух переменных.

Носителем будем называть произвольный непустой граф с конечным или счетным числом вершин.

Для СФЭ S через $G(S)$ обозначим граф, полученный из S удалением разметки вершин и ребер.

Укладкой СФЭ S на носитель T будем называть произвольный гомоморфизм $h\colon G(S) \to T$.

Схемой с носителем T будем называть пару $K = (S, h)$, где S — схема из функциональных элементов, а h — ее укладка на T.

Обычно в задачах синтеза схем имеются те или иные ограничения на укладку. Более формально, ограничение на укладку представляет собой функцию U, которая паре (S, T) ставит в соответствие некоторое множество $U(S, T) \subseteq Hom(G(S), T)$ допустимых укладок S в T, где S — СФЭ, T — носитель.

Важным классом ограничений являются технологические (локальные) ограничения. Ограничение на укладку будем называть *локальным*, если оно может быть описано в терминах ограничения на прообраз вершин и ребер носителя.

Моделью схем будем называть пару $M = (T, U)$, где T — носитель, U — ограничение на укладку. Далее в качестве U будем рассматривать следующее локальное ограничение:

- В каждую вершину носителя может быть отображено не более одного функционального элемента, реализующего нетождественную булеву функцию;
- В каждое ребро носителя может быть отображено не более k ребер СФЭ.

Можно рассматривать схемы с таким локальным ограничением как

k-слойные схемы, в которых только один слой может содержать функциональные элементы. Остальные слои служат для разводки проводов.

Для краткости будем называть схемы с описанным выше ограничением многослойными схемами.

Под *сложностью* схемы с носителем будем понимать количество вершин носителя, в которые отобразился хотя бы один функциональный элемент исходной СФЭ. Для фиксированной модели схем M естественным образом определяется сложность синтеза произвольной булевой функции $L(M, f)$ и функция Шеннона сложности $L(M, n)$.

В данной работе получены оценки функции Шеннона сложности для многослойных схем с некоторыми типами носителей. Ясно, что функция Шеннона будет зависеть от числа слоев k и носителя T. В общем случае будем использовать обозначение $L(M_k^T, n)$, заменяя при необходимости параметр T на другой, более удобный параметр, или опуская его вовсе.

Теорема. *Если в качестве носителя выступает граф целочисленной двумерной решетки $\mathbb{Z}^2$, то асимптотика функции Шеннона имеет вид*

$$L(M_k, n) \sim \frac{2^n}{\min(n, 2\log k)} \quad \textit{при} \quad k \to \infty,\ n \to \infty.$$

Верхняя и нижняя оценки функции Шеннона из приведенной выше теоремы доказываются для более общих классов носителей.

Теорема. *Если в качестве носителя выступает граф d-мерной целочисленной решетки $\mathbb{Z}^d$, то*

$$L(M_k^d, n) \lesssim \frac{2^n}{\min(n, d\log k)} \quad \textit{при} \quad d \geq 2,\ k \to \infty,\ n \to \infty.$$

Теорема. *Если в качестве носителя выступает произвольный планарный граф T с ограниченной степенью вершин, то*

$$L(M_k^T, n) \gtrsim \frac{2^n}{\min(n, 2\log k)} \quad \textit{при} \quad k \to \infty,\ n \to \infty.$$

Условие ограниченности степени вершин носителя является существенным. Доказано, что в отсутствии данного ограничения асимптотика функции Шеннона для схем с не менее чем тремя слоями совпадает с полученной Лупановым асимптотикой для СФЭ.

Утверждение. *Если в качестве носителя выступает произвольный граф T с ограниченной степенью вершин, то*

$$L(M_k^T, n) \sim \frac{2^n}{n} \quad при \quad k \geq 3,\ n \to \infty.$$

Список литературы

1. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. — 1963. — Т. 10. — С. 63–97.

2. Коршунов А. Д. Об оценках сложности схем из объемных функциональных элементов и объемных схем из функциональных элементов // Проблемы кибернетики. — 1967. — Т. 19. — С. 275–283.

3. Кравцов С. С. О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов // Проблемы кибернетики. — 1967. — Т. 19. — С. 285–293.

4. Жуков Д. А. О вычислении частичных булевых функций клеточными схемами // Дискретный анализ и исследование операций. — 2004. — Т. 1, вып. 11, № 2. — С. 32–40.

5. Калачев Г. В. Об одновременной минимизации площади, мощности и глубины плоских схем, реализующих частичные булевы операторы // Интеллектуальные системы. — 2016. — Т. 20, вып. 2. — С. 203–266.

АЛГЕБРАИЧЕСКИЙ СИНТЕЗ ГИПЕРКОНТАКТНЫХ И КОНТАКТНО-ТРАНСФОРМАТОРНЫХ СХЕМ

Ю. Г. Таразевич (Минск)

В классах $\mathrm{PM}_F^{(n)}$ *расширенных матриц над кольцами полиномов с идемпотентными переменными* [1] определяются подклассы (*гиперконтактных схем*): $\mathrm{ГС}_F^{(n)}$ (над произвольным полем F) и $\mathrm{ГС}_Z^{(n)}$ (над кольцом Z целых чисел), — алгебраически расширяющие класс матриц инциденций *контактных схем* [2] ($\mathrm{КС}^{(n)}$) и реализующие произвольные *булевы функции* (БФ), зависящие от n переменных, со сложностью менее $3\sqrt{2}\cdot 2^{n/2}$ контактов. Для матриц класса $\mathrm{ГС}_Z^{(n)}$ предлагается физическая интерпретация в виде матриц инциденций-зацеплений *контактно-трансформаторных схем* ($\mathrm{ТКС}^{(n)}$).

1. *Гиперконтактные схемы.* Обозначим: F — произвольное поле;

$F[X^{(n)}]$ — *кольцо полиномов с идемпотентными переменными* [1], $X^{(n)}=\{x_1,\dots,x_n\}$; $\ominus$ и $*$ — вычитание и умножение в $F[X^{(n)}]$.

Из элементов поля F построим произвольную $k\times(l+1)$-матрицу

$$\boxed{A_1}\boxed{A_2}\boxed{\cdots}\boxed{A_l}\boxed{B} \qquad (1)$$

с одним выделенным столбцом B (k и $l+1$ — произвольные натуральные числа). При $l>0$ каждый столбец A_j умножим на какой-нибудь полином $p_j\in\{x_1,1\ominus x_1,x_2,1\ominus x_2,\dots,x_n,1\ominus x_n,1\}\subset F[X^{(n)}]$. В результате получим $\mathrm{PM}_F^{(n)}$-*матрицу* [1] следующего специального вида:

$$\begin{array}{|c|c|c|c|c|}\hline p_1*A_1 & p_2*A_2 & \cdots & p_l*A_l & B\\ \hline\end{array}\ =\ \begin{array}{|c|c|c|c|c|}\hline A_1 & A_2 & \cdots & A_l & B\\ \hline\end{array}\,, \qquad \begin{array}{ccccc} & & & & f\\ p_1 & p_2 & \dots & p_l & \end{array} \qquad (2)$$

реализующую (в соответствии с [1]) на выделенном столбце B некоторую булеву функцию (БФ) $f(x_1,\dots,x_n)$. Справа в (2) матрица записана в «удобном» для нее — *окаймленном* — виде, т. е. с метками-множителями p_j над константными столбцами A_j и «нейтральной» (т. е. не являющейся множителем) меткой f выделенного столбца.

Определение. Любую $\mathrm{PM}_F^{(n)}$-матрицу вида (2) будем называть $\mathrm{ГС}_F^{(n)}$-*матрицей* или, иначе, *гиперконтактной схемой над полем* F, ее выделенный столбец B — *источником*, столбцы $1*A_j$ — *проводниками*, столбцы x_i*A_j или $(1\ominus x_i)*A_j$ — *контактами*, константную матрицу (1) — *топологической матрицей* гиперконтактной схемы (2).

Замечание. Для любого поля F через $\mathrm{КС}_F^{(n)}$ обозначим множество всех $\mathrm{ГС}_F^{(n)}$-матриц, в каждом ненулевом столбце топологической матрицы которых ровно два ненулевых элемента — единица и минус единица поля F. Любая $\mathrm{КС}_F^{(n)}$-матрица M, записанная в окаймленном виде (см. (2)), естественным образом, независимо от поля F, рассматривается как *матрица инциденций* [3] двухполюсной *контактной схемы* [2] S_M, дополненной *источниковым ребром* [1], соединяющим полюсы, и содержащей обычные (неориентированные) замыкающие (x_i) и размыкающие ($\bar{x}_i=1\ominus x_i$) контакты, проводники (с меткой 1) и «свободные» петли (инцидентные произвольным вершинам), соответствующие нулевым (или пустым) столбцам $\mathrm{КС}_F^{(n)}$-матрицы M.

Утверждение. *Для любого поля* F *любая* $\mathrm{КС}_F^{(n)}$-*матрица* M *реализует ту же булеву функцию, что и соответствующая контактная схема* S_M (*см. замечание* 1).

Таким образом, класс $\mathrm{КС}^{(n)}=\mathrm{КС}_F^{(n)}$ «инвариантен» относительно произвольного выбора поля F ($\forall F$: $\mathrm{КС}^{(n)}\subset\mathrm{ГС}_F^{(n)}\subseteq\mathrm{PM}_F^{(n)}$).

2. *Контактно-трансформаторные схемы.* Обозначим: Q — поле рациональных чисел; $\mathrm{ГС}_Z^{(n)}$ — множество всех $\mathrm{ГС}_Q^{(n)}$-матриц с целочисленными топологическими матрицами. Существует физическая интерпретация произвольных $\mathrm{ГС}_Z^{(n)}$-матриц, при которой множество строк исходной $\mathrm{ГС}_Z^{(n)}$-матрицы разбивается на две подматрицы: «верхнюю» V и «нижнюю» T (одна из подматриц может оказаться

пустой). При этом «верхняя» подматрица V является $\text{КС}^{(n)}_Q$-матрицей и рассматривается как матрица инциденций контактной схемы S_V (см. замечание 1), а «нижняя» (в общем случае произвольная) подматрица T рассматривается как матрица целочисленных *коэффициентов зацеплений* (определяемых соответствующими *индексами пересечений* [3]) между электропроводящими одномерными элементами (контактами, проводниками и источником) «верхней» схемы S_V и магнитопроводящими окружностями-сердечниками, соответствующими строкам «нижней» подматрицы. В результате получается *матрица инциденций-зацеплений* некоторой (в общем случае произвольной) *контактно-трансформаторной схемы* ($\text{ТКС}^{(n)}$-*схемы*) построенной из идеальных элементов: контактов, проводников, кольцевых многообмоточных трансформаторов [4] и источника переменного (или импульсного) тока, — физическое функционирование которой (холостой ход или нагрузка) соответствует алгебраическому функционированию (ноль или единица) исходной $\text{ГС}^{(n)}_Z$-матрицы.

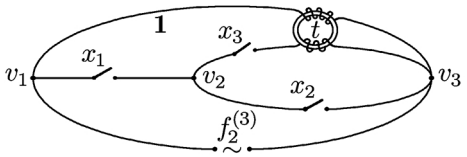
Замечание. Существует простая «локальная» процедура, позволяющая (с помощью определенных в [1] элементарных преобразований расширенных матриц) произвольную $\text{ГС}^{(n)}_Z$-матрицу «монотонно» преобразовать в эквивалентную $\text{ТКС}^{(n)}$-схему, построенную из источника переменного тока, контактов, проводников и одинаковых *двухобмоточных* трансформаторов (с произвольно заданным коэффициентом трансформации). При этом сохраняется число контактов (добавляются только строки-сердечники и столбцы-проводники).

3. *Алгебраический синтез.* Обозначим: K — произвольное поле или кольцо Z целых чисел; K_∞ — произвольное бесконечное поле или кольцо Z; F_q — произвольное конечное (q-элементное) поле; $L^K(f)$ — минимальное число контактов $\text{ГС}^{(n)}_K$-матрицы, реализующей БФ f; $L^K(n)=\max\{L^K(f)\}$, где максимум берется по всем БФ f, зависящим от n переменных; $f^{(n)}_r$ — монотонная симметрическая БФ с произвольным порогом r, существенно зависящая от n переменных [5]; $\oplus$ — знак сложения по модулю два; $l^{(n)}=x_1\oplus\ldots\oplus x_n$ — линейная БФ [2]; $\gtrsim$ — знак асимптотического неравенства [2].

Теорема. $L^K(n)\leqslant 3\sqrt{2}\cdot 2^{n/2}-4$; $L^{F_q}(n)\gtrsim\frac{2^{\frac{n}{2}+1}}{\sqrt{\log_2 q}}$;
$L^{K_\infty}\bigl(f^{(n)}_r\bigr)=n$; $L^{F_q}\bigl(f^{(n)}_r\bigr)\leqslant n\lceil\log_q(n+1)\rceil$; $L^K\bigl(l^{(n)}\bigr)=2n$.

Из предыдущего, в частности, следует, что любая монотонная симметрическая БФ $f^{(n)}_r$ физически реализуется (безрелейной, однотактной) n-контактной $\text{ТКС}^{(n)}$-схемой. Ниже приводится (в окаймленном виде) матрица инциденций-зацеплений $\text{ТКС}^{(3)}$-схемы, реализующей БФ $f^{(3)}_2$ ($\mathbf{1}$, x_1, x_2, x_3 — метки-множители проводника и контактов; $f^{(3)}_2$, v_1, v_2, v_3 и t — «нейтральные» метки источника, узлов и сердечника; k и l — произвольные целые положительные числа). Ниже приводится (в окаймленном виде) «троичная» $\text{ГС}^{(n)}_F$-матрица (3),

	$\mathbf{1}$	x_1	x_2	x_3	$f_2^{(3)}$
v_1	-1	-1	0	0	-1
v_2	0	1	-1	-1	0
v_3	1	0	1	1	1
t	k	0	0	$-l$	0



реализующая (при любых F и четных $n \geqslant 2$) БФ $l^{(n)}$ и представленная (с использованием «нейтральных» меток v_i для узлов и t_j для сердечников) в виде матрицы инциденций-зацеплений ТКС$^{(n)}$-схемы, построенной из источника (с «нейтральной» меткой $l^{(n)}$), $2n$ контактов $(x_1, \bar{x}_1, \ldots, x_n, \bar{x}_n)$, $\frac{n}{2}+2$ узлов и $\frac{n}{2}-1$ одинаковых четырехобмоточных трансформаторов (с «коэффициентом трансформации» 1:1:1:1).

		x_1	x_2	$x_3 \ldots x_{n-1}$	x_n	$\bar{x}_1$	$\bar{x}_2$	$\bar{x}_3 \ldots \bar{x}_{n-1}$	$\bar{x}_n$	$l^{(n)}$
узлы	v_1	-1	-1	$-1 \cdots -1$	-1	0	0	$0 \cdots 0$	0	-1
	v_2	0	0	$0 \cdots 0$	0	1	1	$1 \cdots 1$	1	1
	v_3	1	1			-1	-1			0
чередующиеся сердечники и узлы	t_1		1	$1 \ddots 1$			1	$1 \ddots 1$		0
	v_4									$\vdots$
	$\vdots$		0				0			
	$t_{\frac{n}{2}-1}$			$1 \ddots 1$				$-1 \ddots -1$		0
	$v_{\frac{n}{2}+2}$				1				-1	0

(3)

Список литературы

1. Таразевич Ю. Г. Расширенные полиномиальные матрицы и алгебраизация контактных схем // Журн. Белорус. гос. ун-та. Математика. Информатика. — 2017. — № 3. — С. 85–93.

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

3. Зейферт Г., Трельфалль В. Топология, Изд. 2-е. — М., Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001.

4. Касаткин А. С., Немцов М. В. Электротехника, Учебник для вузов, изд. 7-е, стер. — М.: Высшая школа, 2002.

5. Коршунов А. Д. Монотонные булевы функции // Успехи матем. наук. — 2003. — Т. 58, № 5. — С. 5–108.

О ПОВЕДЕНИИ ФУНКЦИИ ШЕННОНА ДЛЯ ГЛУБИНЫ ФУНКЦИЙ АЛГЕБРЫ ЛОГИКИ В СТАНДАРТНОМ БАЗИСЕ

В. А. Титов, С. А. Ложкин (Москва)

В работе рассматривается задача синтеза оптимальных по глубине формул в стандартном базисе $\{\vee, \&, \neg\}$ с единичной глубиной всех элементов.

Введем ряд вспомогательных определений и обозначений, а также напомним полученные ранее результаты. Те понятия, которые здесь не определяются, могут быть найдены, например, в [2, 3].

Глубиной формулы Σ называется максимальное число элементов цепи, соединяющей вход и выход данной формулы. Глубиной функции алгебры логики (ФАЛ) f в классе формул называется величина $D(f)$ равная минимальному значению глубины формул, реализующих ФАЛ f. Функция Шеннона $D(n)$ равна максимальной глубине ФАЛ f, $f \in P_2(n)$, где $P_2(n)$ — множество ФАЛ от переменных из множества $X(n) = \{x_1, \ldots, x_n\}$.

Из результатов, полученных С. Б. Гашковым [1], вытекает неравенство:

$$D(n) \leq \lceil n - \log_2 \log_2(n) + \overline{o}(1) \rceil + 2.$$

В работе [4] указанная оценка улучшается следующим образом:

$$D(n) \leq \lceil n - \log_2 \log_2(n) + \frac{7 * \log_2(e) * \log_2 \log_2(n)}{\log_2(n)} + O(\frac{1}{\log_2(n)}) \rceil.$$

Будем называть *буквой* выражение вида x^σ, где $x \in X(n)$, а $\sigma \in B = \{0, 1\}$, значение которого равно x, если $\sigma = 1$ и равно $\overline{x}$, если $\sigma = 0$.

Следуя [2], будем говорить, что $\delta \subseteq B^n$ — m-регулярное множество наборов единичного n-мерного куба B^n, если, $m < n, |\delta| = 2^m$ и все префиксы длины m наборов из δ различны. Разбиение Δ множества B^n, состоящее из 2^{n-m} m-регулярных компонент, будем называть m-регулярным разбиением.

Заметим, что m-регулярному множеству $\delta \subseteq B^n$ можно взаимно однозначно сопоставить систему ФАЛ $\psi = (\psi_1, \ldots, \psi_{n-m}) \subseteq P_2^{n-m}(n)$ так, что набор $\alpha = (\beta, \gamma)$, где $\beta \in B^m$ и $\gamma \in B^{n-m}$, принадлежит δ тогда и только тогда, когда $\psi(\beta) = \gamma$.

Важно отметить, что любая ФАЛ $g \in P_2(n)$ совпадает на m-регулярном множестве δ с некоторой ФАЛ из $P_2(m)$, если рассматривать $P_2(m)$ как подмножество $P_2(n)$ с несущественными БП $x_{m+1}, \ldots, x_n$. При этом любая ФАЛ из связанной с δ системы функций совпадает на данном множестве наборов с соответствующей БП куба B^n.

Будем говорить, что m-регулярное разбиение $\Delta = (\delta_1, \ldots, \delta_{2^{n-m}})$ куба B^n, моделирует систему ФАЛ $G \subseteq P_2(m)$ с помощью БП или их отрицаний, если для любой компоненты разбиения δ_i, $i \in [1, 2^{n-m}]$ любая ФАЛ $g \in G$ совпадает на ней с некоторой буквой x_j^σ, где $j \in [1, n]$. При этом компонента δ_i считается «хорошей» (относительно множества G), если указанное совпадение имеет место при $\sigma = 1$ для всех $g \in G$. Иначе, компонента считается «плохой».

Для доказательства основного результата данной работы используется следующее утверждение (см., например, [5]).

Лемма. *Пусть $G \subseteq P_2(m), |G| = \lambda$ и $q \geq m + \lambda$. Тогда существует m-регулярное разбиение куба B^q, которое моделирует ФАЛ из G с помощью БП или их отрицаний и имеет при этом $C_{q-m}^0 + \cdots + C_{q-m}^{\lambda-1}$ «плохих» компонент.*

Теорема. *Функция Шеннона $D(n)$ для глубины ФАЛ от n переменных удовлетворяет неравенству:*

$$D(n) \leq \lceil n - \log_2 \log_2(n) + \frac{4 * \log_2(e) * \log_2 \log_2(n)}{\log_2(n)} + O(\frac{1}{\log_2(n)}) \rceil.$$

Опишем кратко идею доказательства.

Рассмотрим произвольную ФАЛ $f \in P_2(n)$ и разделим множество ее переменных $X(n)$ на четыре группы, последняя из которых состоит из d переменных, где $d = m + 3 * k$ и $k = 2^m$. Построим m-регулярное разбиение Δ булева куба B^d на 2^{d-k} компонент δ_i, используя лемму, где в качестве системы функций G возьмем все элементарные конъюнкции ранга m, от первых m булевых переменных последней группы.

Именно это разбиение будем использовать для разложения ФАЛ f вместо разбиения на «растянутые» единичные сферы, применявшегося в [4].

Заметим, что нижняя оценка функции Шеннона $D(n)$, получаемая на основе мощностных соображений, имеет вид:

$$D(n) \geq \lceil n - \log_2 \log_2(n) - \log_2(1 + \frac{1}{\log_2(n)}) \rceil.$$

Сопоставляя доказанную в теореме верхнюю оценку функции Шеннона или аналогичную верхнюю оценку [4] с нижней оценкой, можно прийти к выводу о существовании функции $\phi(k)$ натурального аргумента $k = 1, 2, \ldots$ такой, что $\phi(k) = \overline{o}(2^{2^{k+1}})$, для которой при любом n, удовлетворяющем неравенствам

$$2^{2^k} + \phi(k) \leq n \leq 2^{2^{k+1}} - \phi(k),$$

имеет место равенство

$$D(n) = n - k + 1.$$

Таким образом, в результате полученного уточнения верхней оценки функции Шеннона $D(n)$ расширено (по сравнению с результатом [4]) множество тех значений n, для которых известно точное значение рассматриваемой функции Шеннона.

Полученный результат является частью магистерской диссертации [6]. Работа выполнена при финансовой поддержке РФФИ, грант № 18–01–00800.

Список литературы

1. Гашков С. Б. О глубине булевых функций // Проблемы кибернетики, вып. 34. — Наука, 1978. — С. 265–268.

2. Ложкин С. А. Дополнительные главы кибернетики [Электронный курс]. — URL: `http://mk.cs.msu.ru/images/3/39/Лекции_ДГКТУС_Часть_1-2.pdf`

3. Ложкин С. А. Основы кибернетики — М.: Изд. отдел факультета ВМК МГУ им. М.В. Ломоносова, 2004.

4. Ложкин С. А. О глубине функции алгебры логики в некоторых базисах // ANNALES Budapest Univ. Sectio Computatorica — 1983. — IV. — P. 113–125.

5. Ложкин С. А., Коноводов В. А. О синтезе и сложности формул с ограниченной глубиной альтернирования // Вестн. Моск. ун-та, Сер. 15. Вычисл. матем. и киберн. — 2012. — 2. — С. 28–36.

6. Титов В.А. О глубине мультиплексорных функций и поведении функции Шеннона для глубины в некоторых базисах. — Магистерская диссертация, МГУ им. М.В. Ломоносова, факультет ВМК, 2019.

О СЛОЖНОСТИ РЕАЛИЗАЦИИ СТАНДАРТНЫХ МУЛЬТИПЛЕКСОРНЫХ ФУНКЦИЙ В НЕКОТОРЫХ КЛАССАХ КОНТАКТНЫХ СХЕМ

Д. Э. Хзмалян, С. А. Ложкин (Москва)

Рассматриваемая задача относится к теории синтеза управляющих систем, которая является одним из основных разделов дискретной математики и математической кибернетики. Необходимость проектирования и логического описания дискретных вычислительных устройств различного типа привела к возникновению данной теории. Клод Шеннон в работах [1, 2] дал строгую математическую постановку задачи синтеза управляющих систем, положив тем самым начало соответствующей теории, исследования в которой ведутся с тех пор непрерывно.

В теории синтеза управляющих систем изучаются модели различных дискретных преобразователей сигналов, их сложность, надежность и другие характеристики. Интерес к этой области знания обусловлен, прежде всего, возможностью применения полученных результатов при проектировании оптимальных или близких к оптимальным по определённым характеристикам схем, при изучении их поведения и надёжности, при тестировании схем и т.д.

Задача синтеза ставится для определенного класса управляющих систем, при этом, количество таких классов довольно велико, что оправдано потребностью в изучении различных моделей и характеристик реальных схем. Для каждого класса определяется структура его схем и их функционирование в виде системы функций алгебры логики (ФАЛ). Также для каждого класса предполагается наличие функционала сложности, который каждой схеме ставит в соответствие положительное число, отражающее некоторую числовую характеристику для схем из рассматриваемого класса (например, в классе схем из функциональных элементов функционалом сложности может являться число элементов в схеме).

Задача синтеза в общем виде состоит в построении для заданной системы ФАЛ такой реализующей её схемы из заданного класса, на которой достигается минимальное значение исследуемого функционала сложности. Указанное значение считается сложностью данной системы ФАЛ в рассматриваемом классе схем относительно изучаемого функционала. В теории синтеза выделяют при этом два основных направления: «массового» и «индивидуального» синтеза.

Напомним некоторые определения, а также введем обозначения, связанные с реализацией ФАЛ в классе контактных схем. Те понятия, которые в данной работе не определяются, могут быть найдены,

например, в [3, 4].

Пусть $B = \{0, 1\}$, а $B^n = \underbrace{B \times ... \times B}_{n \text{ раз}}$ — единичный куб размерности n.

Будем говорить, что ФАЛ $f(x_1, ..., x_n)$ представляет собой отображение $B^n \xrightarrow{f} B$.

Сеть Σ с входом a' и выходом a'', в которой все ребра помечены переменными $x_1, ..., x_n$ или их отрицаниями $\overline{x}_1, ..., \overline{x}_n$, называется $(1, 1)$-контактной схемой (КС) от булевых переменных (БП) $x_1, ..., x_n$. При этом ребро с пометкой x_i ($\overline{x}_i$) называется замыкающим (соответственно размыкающим) контактом БП x_i.

Указанная КС Σ реализует, как обычно, ФАЛ $f(x_1, ..., x_n)$, которая является ФАЛ проводимости от a' к a''.

В данной работе рассматривается задача индивидуального синтеза в классе КС для стандартной мультиплексорной ФАЛ порядка n, то есть для функции μ_n от $n + 2^n$ БП, где первые n БП называются «адресными» БП, а оставшиеся 2^n — «информационными» БП. При этом значение функции μ_n равно значению той ее информационной переменной, номер которой поступил на ее адресные входы, то есть $\mu_n(x_1, x_2, ..., x_n, y_0, y_1, ..., y_{2^n-1}) = \bigvee\limits_{\tilde{\sigma}=(\sigma_1,\sigma_2,...,\sigma_n)\in B^n} x_1^{\sigma_1} x_2^{\sigma_2} ... x_n^{\sigma_n} y_{\nu(\tilde{\sigma})}$, где $\nu(\tilde{\sigma})$ это число, двоичная запись которого совпадает с $\tilde{\sigma}$.

Сложностью $L(\Sigma)$ контактной схемы Σ будем называть количество контактов в ней.

Определение. Будем говорить, что контактная схема Σ от адресных БП $x_1, ..., x_n$ и информационных БП $y_1, ..., y_{2^n-1}$ *корректна*, если выполнены следующие два условия:

1. в схеме Σ нет нулевых цепей, содержащих противоположные контакты одной и той же информационной переменной,
2. для любой проводящей цепи в схеме Σ верно, что если она содержит вершину, инцидентную некоторому контакту информационной переменной, то она содержит также один из контактов информационных переменных инцидентных данной вершине.

Теорема. *Для любой корректной контактной схемы Σ, реализующей мультиплексорную ФАЛ $\mu_n, n \geq 2$, справедливо следующее неравенство:*

$$L(\Sigma) \geq 2^{n+1} + \frac{2^n}{4n} - 4.$$

Основная идея доказательства данной теоремы состоит в разделении контактной схемы на связные компоненты информационных БП.

Из работы [5], известно, что для сложности $L^{\pi}(\mu_n)$ мультиплек-

сорной ФАЛ μ_n в классе параллельно-последовательных схем (π-схем) выполняется соотношение

$$L^{\pi}(\mu_n) = 2^{n+1} + \frac{2^n}{n} \pm O\Big(\frac{2^n}{n \log n}\Big).$$

Верхняя оценка этой работы достигается построением π-схемы, которая является корректной контактной схемой и реализует мультиплексорную ФАЛ.

Таким образом, для любой минимальной корректной контактной схемы Σ, реализующей мультиплексорную ФАЛ $\mu_n, n \geq 2$, выполняются неравенства:

$$2^{n+1} + \frac{2^n}{4n} - 4 \leq L(\Sigma) \leq 2^{n+1} + \frac{2^n}{n} + O\Big(\frac{2^n}{n \log n}\Big).$$

Работа выполнена при финансовой поддержке РФФИ, грант № 18–01–00800.

Список литературы

1. Shannon C. E. A symbolic analysis of relay and switching circuits // Trans. AIEE. — 1938. — 57. — P. 713–723.

2. Shannon C. E. The synthesis of two-terminal switching circuits // Bell Syst. Techn. J. — 1949. — 28. — P. 59–98.

3. Ложкин С. А. Лекции по основам кибернетики. — М.: Изд. отдел фак. ВМиК МГУ, 2004. — 256 с.

4. Алексеев В. Б., Ложкин С. А. Элементы теории графов, схем и автоматов. — М.: Изд. отдел фак. ВМиК МГУ, 2000. — 58 с.

5. Ложкин С. А., Власов Н. В., О сложности мультиплексорной функции в классе π-схем // Физико-математические науки, Учен. зап. Казан. гос. ун-та. Сер. Физ.-матем. науки. — 2009. — 151, № 2. — С. 98—106.

О СЛОЖНОСТИ ЧАСТИЧНЫХ БУЛЕВЫХ ФУНКЦИЙ

А. В. Чашкин (Москва)

Рассматривается сложность реализации частичных булевых функций формулами в базисе из всех двухместных булевых функций. Далее $L(f)$ обозначает сложность частичной функции f, N — размер области определения рассматриваемой функции. Известно

[1, 2], что при $n \to \infty$ сложность любой частичной n-местной булевой функции f асимптотически не превосходит величины $\frac{N}{\log_2 n}$ в случае, когда $\log_2 N \sim n$. Этот результат легко достигается методом Э. И. Нечипорука из [1], при помощи которого также можно показать, что при $\log_2 N > n/2$ для сложности частичной функции справедливо неравенство

$$L(f) = O\left(\frac{N}{\log_2 n}\right). \tag{1}$$

Основной результат настоящей работы состоит в распространении последнего неравенства на функции с меньшей областью определения.

Теорема. *Пусть $n \to \infty$, $\log_2 N = \Theta(n)$. Для любой частичной n-местной булевой функции f, определенной на области размера N,*

$$L(f) = O\left(\frac{N}{\log_2 n}\right).$$

Доказательство теоремы основано на доказательстве Л. А. Шоломова оценки сложности частичных булевых функций при их реализации схемами из [3], следует, в основном, доказательству, приведенному в [4], и состоит в следующем. Сначала доказывается существование линейного оператора $\mathcal{L}(x)$ инъективного почти на всей области определения D реализуемой функции f, за исключением не более чем $O\left(N/n^3\right)$ наборов, число компонент которого меньше $2\log_2 N$. Затем на образе $\mathcal{L}(D)$ определяется частичная функция

$$g(y) = \begin{cases} 0, \text{ если } \exists\ x \text{ такой, что } y = \mathcal{L}(x) \text{ и } f(x) = 0, \\ 1, \text{ в противном случае,} \end{cases}$$

а на D — частичная функция $h(x) = f(x) \oplus g(\mathcal{L}(x))$. Наконец, функция $f(x)$ реализуется по формуле $f(x) = h(x) \oplus g(\mathcal{L}(x))$, в которой сложность h очевидно не превосходит $O\left(\frac{N}{n^2}\right)$, для g справедливо неравенство (1), а для композиции $g(\mathcal{L}(x))$ — неравенство $O\left(l \cdot \frac{N}{\log_2 n}\right)$, где l — сложность самой сложной компоненты $\mathcal{L}$. Покажем, что существует оператор, для которого $l = O(1)$. Сделаем это, сведя задачу построения оператора к задаче о покрытии булевой таблицы ее строками. Существование покрытия установим при помощи градиентного метода.

Составим таблицу из не более чем $\binom{N}{2}$ столбцов, соответствующих суммам $x \oplus y$ элементов из D, и $\binom{n}{k}$ строк, соответствующих n-местным линейным булевым функциям с k существенными аргументами. На пересечении столбца и строки поставим значение соответствующей функции на соответствующей сумме. Нетрудно видеть, что, если при $n \to \infty$ для некоторой постоянной k найдутся $m < 2\log_2 N$ строк покрывающих все столбцы, за исключением не более чем $O\left(N/n^3\right)$ столбцов, то линейный оператор, компонентами которого являются функции, соответствующие этим строкам, будет требуемым оператором.

Прежде всего отметим, что из равенства $\log_2 N = \Theta(n)$ следует, что найдется такая постоянная α, что почти все наборы, соответствующие столбцам таблицы, содержат не менее αn единиц. Оставим в таблице только такие столбцы. В каждом столбце новой таблицы содержится не менее $\Sigma\binom{\alpha n}{i}\binom{(1-\alpha)n}{k-i}$ единиц, где суммирование ведется по всем нечетным i. Так как при $n \to \infty$

$$\binom{\alpha n}{i}\binom{(1-\alpha)n}{k-i} \Big/ \binom{n}{k} \sim \binom{k}{i}\alpha^i(1-\alpha)^{k-i},$$

то доля единиц в столбце не превосходит величины

$$A = \sum_{\text{все нечетные } i} \binom{k}{i}\alpha^i(1-\alpha)^{k-i},$$

а доля нулей — величины

$$B = \sum_{\text{все четные } i} \binom{k}{i}\alpha^i(1-\alpha)^{k-i}.$$

Так как $A + B = 1$ и $B - A = (1-2\alpha)^k$, то $A = \frac{1}{2}\left(1 - (1-2\alpha)^k\right)$. Очевидно, что в таблице найдется строка, в которой доля единиц не меньше A. Возьмем такую строку в качестве первого элемента покрытия. После этого в таблице останется не более

$$\binom{N}{2}(1-A) = \binom{N}{2}\frac{1}{2}\left(1 + (1-2\alpha)^k\right)$$

непокрытых столбцов. После m подобных итераций число непокрытых столбцов не превысит

$$\binom{N}{2}\left(\frac{1}{2}\left(1 + (1-2\alpha)^k\right)\right)^m.$$

Нетрудно показать, что

$$\left(\frac{1}{2}\left(1+(1-2\alpha)^k\right)\right)^m \le 2^{-m\left(1-2\cdot 2^{-2\alpha k}\right)}.$$

Из последнего неравенства видно, что для любой положительной постоянной δ константу k можно выбрать так, что число непокрытых столбцов после m итераций не превысит

$$\binom{N}{2}2^{-m(1-\delta)}.$$

При $m = \lceil (1+3\delta)\log_2 N\rceil$ последняя величина есть $O\left(N^{1-\delta}\right)$.

Таким образом, существует набор из $m = \lceil (1+3\delta)\log_2 N\rceil$ строк, покрывающий в исходной таблице (с учетом выброшенных столбцов, соответствующих наборам с малым числом единиц) почти все столбцы, за исключением не более чем $O\left(N/n^3\right)$ столбцов.

Работа выполнена при финансовой поддержке РФФИ, проект № 18–01–00337

Список литературы

1. Нечипорук Э. И. О синтезе вентильных схем // Проблемы кибернетики. Вып. 9. — М.: Наука, 1963, С. 37–44.

2. Чашкин А. В. О сложности реализации булевых функций формулами // Дискретн. анализ и исслед. опер. сер. 1. — 2005 — Т. 12, вып. 2. — С. 56–72.

3. Шоломов Л. А. О реализации недоопределенных булевых функций схемами из функциональных элементов // Проблемы кибернетики. Вып. 21. — М.: Наука, 1969. — С. 215–226.

4. Чашкин А. В. Дискретная математика. — М.: Академия, 2012.

МИНИМИЗАЦИЯ БУЛЕВЫХ ФУНКЦИЙ ДЛЯ МЕР СЛОЖНОСТИ ПОЛИНОМИАЛЬНОГО ПОРЯДКА РОСТА

И. П. Чухров (Москва)

Задача о минимизации булевых функций для аддитивных мер сложности в геометрической интерпретации является специальным видом комбинаторной постановки взвешенной задачи о минимальном покрытии множества. Мерой сложности комплексов граней (ДНФ) называется функционал $\mathcal{L}$, который определен на множестве всех комплексов граней и удовлетворяет аксиомам неотрицательности, монотонности относительно умножения, выпуклости относительно сложения и инвариантности относительно изоморфизма. Мера сложности называется аддитивной, если сложность любого комплекса граней равна сумме сложностей граней. Множество аддитивных мер сложности обозначим через Λ_+.

Отметим, что булевы функции n переменных имеют не более $\binom{n}{2}$ подмножеств максимальных граней различной сложности.

Используемые понятия и обозначения можно найти в [1, 2].

Обозначим через $\tilde{P}_n \subset P_n$ множество булевых функций, которое содержит почти все функции n переменных, имеющие определенные свойства максимальных граней, а для минимальных и кратчайших комплексов граней асимптотически равны длины и сложности: $l_L(f) \sim l(f) \sim \bar{l}_n$ и $L(f) \sim n\, l(f)$, где $\bar{l}_n \sim \bar{c}_n 2^n / (\log n \cdot \log\log n)$ — среднее значение длины кратчайшего комплекса граней и $1 \le \bar{c}_n$ (см. [1]), а верхняя оценка $\bar{c}_n$ колеблется между $1.38826\ldots$ и $1.54169\ldots$ в зависимости от дробной части $\log\log n + \log\log\log n$ [3].

Множество функций $\varphi : Z_0^+ \times Z_0^+ \to R_0^+$, удовлетворяющие условиям неотрицательности и монотонности: $\varphi(i,j) \ge 0$, $\varphi(i+1,j) \ge \varphi(i,j)$ и $\varphi(i,j+1) \ge \varphi(i,j)$, обозначим через Φ. Для $\varphi \in \Phi$ максимальное значение $\varphi(i,j)$ при $0 \le i+j \le n$ обозначим через $\varphi(n)$.

Лемма 1. *Мера сложности $\mathcal{L}$ принадлежит Λ_+ тогда и только тогда, когда есть функция $\varphi_{\mathcal{L}} \in \Phi$ такая, что для любой грани g выполняется $\mathcal{L}(g) = \varphi_{\mathcal{L}}(L_0(g), L_1(g))$.*

Значения $\varphi(n) = \max\{\varphi(i,j), 0 \le i+j \le n\}$ и $\partial\varphi(n) = \varphi(n,n) - \varphi(n-1,n-1)$ будем называть порядком и скоростью роста функции $\varphi \in \Phi$. Отметим, что максимальная сложность грани куба B^n достигается на грани ранга n, т. е. $\varphi(n) = \max\{\varphi(i,n-i), 0 \le i \le n\}$. Подмножество функций Φ, для которых $\varphi(n) \le n^{\Theta(1)}$ и $\varphi(n) \to \infty$ при $n \to \infty$, т.е. полиномиальный порядок роста, обозначим через

Φ^p. Так как $\varphi(n) \le \varphi(n,n) \le \varphi(2n)$, то $\varphi(n) \le n^{\Theta(1)}$ и $\varphi(n) \to \infty$ эквивалентно выполнению таких же условий для $\varphi(n,n)$.

Множество последовательностей $\{x_n \mid 0 \le x_n \le x_{n+1}, n = 1, \ldots\}$ обозначим через Q.

Множество функций, которые определены для $r \ge 1$ неотрицательных переменных и являются неотрицательными и неубывающими, обозначим через M. Подмножество функций $\xi(t_1, \ldots, t_r) \in M$ таких, что для любых последовательностей $\left\{x_n^{(k)}\right\}, \left\{a_n^{(k)}\right\} \in Q$ и $x_n^{(k)} \sim a_n^{(k)}$, где $k = 1, \ldots, r$ и $r \ge 1$, выполняется $\xi\left(x_n^{(1)}, \ldots, x_n^{(r)}\right) \sim \xi\left(a_n^{(1)}, \ldots, a_n^{(r)}\right)$ при $n \to \infty$, обозначим через M^*.

Множество последовательностей $\{h_n\} \in Q$, для которых $0 < h_n < \frac{n}{2}$ при $n = 1, \ldots$, обозначим через Q_h.

Для $\{a_n\} \in Q$ и $\{h_n\} \in Q_h$ множество функций $\varphi \in \Phi$, для которых выполняется условие: если $\frac{n}{2} - h_n \le i_n, j_n \le \frac{n}{2} + h_n$ для $n = 1, \ldots$, то $\varphi(i_n, j_n) \sim a_n$ при $n \to \infty$, обозначим через $\Phi(a_n, h_n)$.

Множество функций $\varphi \in \Phi$ таких, что для последовательности $\{h_n\} \in Q_h$ есть $\{a_n\} \in Q$, для которой выполняется $\varphi \in \Phi(a_n, h_n)$, обозначим через $\tilde{\Phi}(h_n)$.

Для функции $\xi(t_1, \ldots, t_r) \in M$ и набора $\tilde{\sigma} \in B^r$, определим меру сложности $\mathcal{L}_{\xi,\tilde{\sigma}} \in \Lambda_+$ соотношением $\mathcal{L}_{\xi,\tilde{\sigma}}(g) = \xi(L_{\sigma_1}(g), \ldots, L_{\sigma_r}(g))$ для любой грани g, где $L_\sigma(g)$ — число направлений грани равные σ для $\sigma = 0, 1$. Сложности $\mathcal{L}_{\xi,\tilde{\sigma}}$ соответствует функция $\varphi_{\xi,\tilde{\sigma}} \in \Phi$, которая получается из функции ξ заменой переменной t_k на переменную i, если $\sigma_k = 0$, и на переменную j, если $\sigma_k = 1$, где $k = 1, \ldots, r$.

Подмножество функций Φ, которое для функции $\xi(t_1, \ldots, t_r) \in M$ содержит функции $\varphi_{\xi,\tilde{\sigma}}(i,j)$ для любого $\tilde{\sigma} \in B^r$, обозначим Φ_ξ.

Для подмножества $Z \subseteq M$ замыкание относительно операции суперпозиция и множество функций $\bigcup_{\xi \in Z} \Phi_\xi \subseteq \Phi$ обозначим через $[Z]$ и $\Phi(Z)$ соответственно.

Определим подмножество функций $M_0 \subset M$:

$M_0 = \{t + c, \max(0, t - c), ct, \max(0, \ln t), t^c\} \cup$

$\cup \{t_1 + t_2, t_1 t_2, \max(t_1, t_2), t_1(1 - 1/\max(1, t_2))\}$, где $c > 0$.

Лемма 2. *Справедливы следующие соотношения.*

(i) $[M_0] \subset M^* = [M^*]$ *и если функция* ξ *лежит в* M^*, *то для функции* $\varphi \in \Phi_\xi$ *выполняется* $\varphi \in \tilde{\Phi}(h_n)$ *при* $h_n = o(n)$ *и* $n \to \infty$.

(ii) Если функция φ *лежит в* $\Phi([M_0])$, *то* $\varphi(n,n) \to \infty$, $\varphi(n,n) \le n^{\Theta(1)}$ *и* $\partial\varphi(n,n) \le \varphi(n,n)\,\Theta\left(n^{-1}\right)$ *при* $n \to \infty$, *т. е.*

$\Phi([M_0]) \subset \Phi^p$.

Теорема 1. *Если функция f лежит в $\tilde{P}_n$, мера сложности $\mathcal{L}$ принадлежит Λ_+, $\varphi_{\mathcal{L}}(n) \le e^{n^c}$ и $\varphi_{\mathcal{L}} \in \tilde{\Phi}(h_n)$, где $h_n = \lceil n^{2/3}\log^{-1} n \rceil$ и $0 < c < \frac{1}{3}$, то $l_{\mathcal{L}}(f) \sim l(f) \sim \bar{l}_n$ и $\mathcal{L}(f) \sim l(f)\,\varphi_{\mathcal{L}}\left(\left\lfloor \frac{n}{2} \right\rfloor, \left\lfloor \frac{n}{2} \right\rfloor\right)$ при $n \to \infty$.*

Теорема 2. *Если функция f лежит в $\tilde{P}_n$, мера сложности $\mathcal{L}$ принадлежит Λ_+ и $\varphi_{\mathcal{L}} \in \Phi([M_0])$, то $l_{\mathcal{L}}(f) \sim l(f) \sim \bar{l}_n$ и $\mathcal{L}(f) \sim l(f)\,\varphi_{\mathcal{L}}\left(\left\lfloor \frac{n}{2} \right\rfloor, \left\lfloor \frac{n}{2} \right\rfloor\right)$ при $n \to \infty$.*

Для меры сложности $\mathcal{L}$, функции $f \in P_n$ и подмножества $A \subset B^n$ минимальную сложность граней, которые пересекаются с множеством A и содержатся в одном минимальном комплексе функции f обозначим через $\mathcal{L}_\cap(f, A)$. Полученные в теореме 1 результаты для функций $f \in \tilde{P}_n$ основаны на выполнении соотношений $\mathcal{L}(f) \sim \mathcal{L}_\cap\left(f, H^n_{h_n}\right)$ и $\mathcal{L}_\cap\left(f, B^n \setminus H^n_{h_n}\right) = o(\mathcal{L}(f))$ при $n \to \infty$, где H^n_h — пояс куба, который содержит слои куба B^n_i для $0 \le \frac{n}{2} - h \le i \le \frac{n}{2} + h \le n$. В случае $\varphi_{\mathcal{L}}(n) = e^{\Theta(n^c)}$, где $c > 1$, асимптотика сложности минимальных комплексов для почти всех булевых функций может определяться сложностью покрытия малой доли вершин функции.

Замечание. Пусть функция $\xi_{T,V}(t)$ определяется последовательностями чисел T и непрерывных функций V:
$T = \left\{t_n \in R^+_0 \mid t_0 = 0, t_{n-1} < t_n, n = 1, \ldots\right\}$, $t_n \to \infty$ при $n \to \infty$;
$V = \{v_n(t) \mid v_n(t) \in M, n = 1, \ldots\}$ и $v_1(0) = 0$;
$\xi_{T,V}(0) = 0$; $\xi_{T,V}(t) = \xi_{T,V}(t_{n-1}) + v_n(t) - v_n(t_{n-1})$ для $t_{n-1} \le t \le t_n$ и, следовательно, $\xi_{T,V}(t_n) = \sum_{i=1}^n v_i(t_i)$ для $n = 1, \ldots$.

Очевидно, что функция $\xi_{T,V}(t) \in M$ и является непрерывной. При этом возникают вопросы об определении свойств функции $\xi_{T,V}$:
— принадлежность $\xi_{T,V}$ множеству M^*, если $V \subset M^*$ или имеют одинаковый порядок и асимптотически различную скорость роста;
— порядок роста $\xi_{T,V}$, если функции из множества V могут иметь различный (полиномиальный, экспоненциальный) порядок роста.

Список литературы

1. Сапоженко А. А, Чухров И. П. Минимизация булевых функций в классе дизъюнктивных нормальных форм // Итоги науки и техники. Серия Теория вероятностей. Математическая статистика. Теоретическая кибернетика. — 1987. — Т. 25. — С. 68–116.

2. Чухров И. П. О мерах сложности комплексов граней в единичном кубе // Дискретный анализ и исследование операций. — 2013. — Т. 20, Вып. 6. — С. 77–94.

3. Pippenger N. The shortest disjunctive normal form of a random

boolean function // Random Structures & Algorithms. — 2003. — V. 22, no. 2. — P. 161–186.

ПРЕДСТАВЛЕНИЕ МНОЖЕСТВ СТОХАСТИЧЕСКИХ МАТРИЦ С ЗАДАННЫМИ СВОЙСТВАМИ НА ОСНОВЕ АВТОНОМНОГО ВЕРОЯТНОСТНОГО АВТОМАТА

С. В. Шалагин, Б. Ф. Эминов (Казань)

Разработан алгоритм представления множеств стохастических матриц (СМ) с рациональными элементами, с заданной структурой на основе автономного вероятностного автомата (АВА). Получение разнообразия множеств СМ достигается изменением в автомате функции переходов и случайного входа. Представлены оценки мощности множеств получаемых СМ с рациональными элементами в зависимости от их размерности. В [1–5] показано, что задача построения множеств СМ возникает при анализе вероятностных моделей, построении укрупненных СМ и других приложениях. Рассмотрим следующий АВА [6, 7].

$$\text{АВА} = \left(S,\ \hat{X},\ \Delta(x,\ s) = s,\ \overline{\pi_0}\right), \tag{1}$$

где $S = \{s_i\}$, $i = \overline{0,\ n-1}$, — множество состояний; $\hat{X}$ — дискретная случайная величина $\hat{X} = \begin{pmatrix} x_0 & x_1 & \ldots & x_{l-1} \\ p_0 & p_1 & \ldots & p_{l-1} \end{pmatrix}$, $0 < p_i < 1$, $\sum_{i=0}^{l-1} p_i = 1$; $\Delta\,(x,\ s)$ — функция переходов АВА (1), задаваемая автоматной таблицей размера $n \times l$, как произвольно, так и по алгоритмам [8–10] на основе разложения заданной СМ (обозначим P_S) размера $n \times n$. Параметры n и l определяют размерность автоматной модели. P_S представим как разложение вида [8, 9]

$$P_S = \sum\nolimits_{k=0}^{l-1} p_k M\,(x_k), \tag{2}$$

где p_k, $k = \overline{0,\ l-1}$ — элементы $\overline{P}$, $M\left(x_k\right)$, $k = \overline{0,\ l-1}$ — простая матрица размера $n \times n$, соответствующая символу x_k; l удовлетворяет соотношению [8, 9]

$$l \leq n^2 - n + 1. \tag{3}$$

Замечание. Оценка мощности множества автоматных таблиц размера $n \times l$ для задания функций $\Delta\left(x,\ s\right)$ определена на основе функции, задающей число перестановок множества S с повторениями:

$$L_1 = \sum\nolimits_{\sum_{j=1}^{n} i_j = n \cdot l} \frac{k!}{i_1! \cdot i_2! \cdot \ldots \cdot i_n!}, \tag{4}$$

где $i_1,\ i_2,\ \ldots,\ i_n$ — натуральные числа такие, что $\sum_{j=1}^{n} i_j = n \cdot l = k$.

Закон (СМ P_S размера $n \times n$) цепи Маркова, получаемой в автомате (1) можно однозначно вычислить в виде (2) в соответствии с [11] по заданным элементам (1): $\hat{X}$ и $\Delta(x,\ s)$.

Алгоритм вычисления множества СМ вида P_S (далее Алгоритм) на основе соотношений (2) и (3) можно представить в виде следующих трех этапов.

1. Определение по заданной $\Delta\left(x,\ s\right)$ простых матриц $M\left(x_k\right)$, $k = \overline{0,\ l-1}$.
2. Перемножение полученных $M\left(x_k\right)$ на соответствующие элементы p_k, $k = \overline{0,\ l-1}$, заданного вектора $\overline{P}$.
3. Вычисление P_S в соответствии с (2).

Задавая для (1) различные $\Delta\left(x,\ s\right)$ в виде соответствующих автоматных таблиц при фиксированном стохастическом векторе $\overline{P}$, можно получить по Алгоритму различные множества (подклассы) СМ P_S с отличающейся структурой (эргодические квазитреугольные, эргодические блочные и др. [1, 3]).

Меняя в (1) стохастический вектор $\overline{P}$ при фиксированной $\Delta\left(x,\ s\right)$ получим множество СМ P_S из фиксированного подкласса, определяемого функцией $\Delta\left(x,\ s\right)$. Оценим общее число возможного разнообразия построенных СМ на основе модели (1) по рассмотренному Алгоритму. Введем ограничения. Пусть для вектора вида $\overline{P}$ элементы вычисляются согласно формуле:

$$p_i = a_i / N, \quad \sum\nolimits_{i=0}^{l-1} a_i = N, \tag{5}$$

где a_i целые неотрицательные числа и N кратно l. Тогда $\overline{P}$ относится к классу распределений вероятностей, мощность которого оценивается величиной [7].

$$L_2 = C_{l+N-1}^{N-1}. \tag{6}$$

Величина L_2 определяет мощность множества СМ, получаемых изменением $\overline{P}$. Решение задачи построения множества этих векторов с мощностью (6) можно выполнить в соответствии с [7]. Справедливо

Утверждение. *Если мощность множества автоматных таблиц для задания* $\Delta(x,\ s)$ *в автомате* (1) *определяется величиной* (4), *то мощность множества стохастических матриц* P_S, *получаемых на автоматной модели* (1) *и удовлетворяющих условиям* (5), (6), *оценивается произведением* $L_1 \cdot L_2$.

Работа выполнена при финансовой поддержке гранта РФФИ № 18–01–00120 «Специализированные устройства для генерирования и обработки массивов данных в архитектуре программируемых логических интегральных схем класса FPGA».

Список литературы

1. Захаров В. М., Нурмеев Н. Н., Салимов Ф.И., Шалагин С. В. Классификация стохастических эргодических матриц методами кластерного и дискриминантного анализа // Исследования по информатике. Казань: Отечество, 2000. — С.91–106.

2. Захаров В. М., Нурмеев Н. Н., Салимов Ф. И., Соколов С. Ю., Шалагин С. В. К задаче дискриминантного анализа автоматных марковских моделей // Вестник КГТУ им. А.Н.Туполева — 2001. — 3. — С. 37–39.

3. Шалагин С. В., Нурутдинова А. Р. Многопараметрическая классификация автоматных марковских моделей на основе генерируемых ими последовательностей состояний // Прикладная дискретная математика. — 2010. — 4(10). — С. 41–54.

4. Zakharov V. M., Eminov B. F., Shalagin S. V. Representing lumped Markov chains by minimal polynomials over field F(q) // International conference information technologies in business and industry 2018, Tomsk. Journal of Physics: Conference series. — 2018. — Vol. 2015. — P. 1–6.

5. Zakharov V. M. , Shalagin S. V., Eminov B. F. Representation of Markov Functions by Minimal Polynomials over a Finite Field // Journal of Physics: Conference Series. — 2018. — Vol. 1015. — P. 032–033.

6. Бухараев Р. Г. Основы теории вероятностных автоматов. — М.: Наука, 1985. — 287 с.

7. Бухараев Р. Г., Захаров В. М. Управляемые генераторы случайных кодов. — Казань: КГУ, 1978. — 160 с.

8. Поспелов Д. А. Вероятностные автоматы. — М: Энергия, 1970. — 88 с.

9. Ченцов В. М. Об одном методе синтеза автономного стохастического автомата // Кибернетика. — 1968. — 3. — С. 32–35.

10. Эминов Б. Ф., Захаров В. М. Анализ алгоритмов разложения двоично-рациональных стохастических матриц на комбинацию булевых матриц // Информационные технологии, №3. — М.: Изд-во Новые технологии, 2008. — С. 54–59.

11. Левин Б. Р., Шварц В. Вероятностные модели и методы в системах связи и управления. — М.: Радио и связь, 1985. — 312 с.

ПРИМЕНЕНИЕ МОДИФИЦИРОВАННОГО АЛГОРИТМА «ПРЯМОГО-ОБРАТНОГО ХОДА» ДЛЯ ИДЕНТИФИКАЦИИ ЦЕПЕЙ МАРКОВА

С. В. Шалагин, А. Р. Нурутдинова (Казань)

Предложено применение модификации метода Л. Рабинера для решения задачи идентификации цепей Маркова (ЦМ) на предмет принадлежности с заданной вероятностью к определенному подклассу автоматной марковской модели (АММ). Модели, заданной на основе стохастических матриц класса эргодических, которые и определяют подкласс АММ. Особенность ЦМ — наличие подмножеств допустимых реализаций в множестве состояний в каждый момент времени.

Показана возможность развития модифицированного согласно [1] алгоритма «прямого-обратного хода» [2] на задачу идентификации ЦМ, для которых в заданный момент времени существует подмножество состояний, наблюдаемых с равной вероятностью. Задача идентификации рассматривается для АММ [3], определенных на основе эргодических стохастических матриц (ЭСМ) [4]. АММ определена как автономный вероятностный автомат без выхода вида [5]

$$(S,\ \varphi(s'/\ s))\,, \tag{1}$$

где $S = \{s_i\}$, $i = \overline{0, n-1}$ — множество состояний ЦМ, s, $s' \in S$, $\varphi(s',\ s)$ — функция переходов, заданная ЭСМ P_s, $P_s = (p_{ij})$ размерности $n \times n$, $i, j = \overline{0, n-1}$.

Если задавать различные $\varphi(s',\ s)$, то для АММ можно получить конечное множество из c различных подклассов АММ, определяемых ЭСМ P: $\{Q_k\}$, $P \in Q_k$, $k = \overline{1,\ c}$, и решать задачу распознавания АММ по реализациям ЦМ, получаемых на основе заданных подклассов АММ. Подклассы АММ выделены в зависимости от структуры ЭСМ P и определяются расположением положительных элементов в заданных ее позициях (элементах). В частности, в [6, 7] выделены такие подклассы ЭСМ как треугольные верхние, треугольные нижние, блочные правые и блочные левые.

Введем следующие определения.

Определение. $\hat{S}(N) = u_1, u_2, \ldots, u_N$ — множество допустимых реализаций цепи Маркова, заданной АММ вида (1), в моменты времени t, где u_t — подмножество состояний ЦМ из множества S, допустимых в момент времени t, $t = \overline{1, N}$, с равной вероятностью q^{-1}, $u_t \subset S$, $|u_t| = q \in [1,\ n]$.

Определение. Частный случай $\hat{S}(N) = u_1, u_2, \ldots, u_N$ — полностью наблюдаемая цепь Маркова: $|u_t| = 1$, $t = \overline{1, N}$.

Определение. Для элемента $\hat{S}(N)$ допустимо полное множество реализаций S в момент времени t с равной вероятностью n^{-1}, $u_t = S$ $|u_t| = n$, что соответствует полностью ненаблюдаемому состоянию ЦМ.

Требуется определить $P(\hat{S}(N)|(P))$ − вероятность того, что множество $\hat{S}(N)$ сгенерировано на основе (P), где ЭСМ P принадлежит заданному подклассу Q_k.

В общем случае, для идентификации множества $\hat{S}(N) = u_1, u_2, \ldots, u_N$ развитие алгоритма «прямого-обратного хода» выглядит следующим образом.

Этап 1. Инициализация:

$$\alpha_1(i) = \pi_0(i) \cdot z_i(1),$$

$$z_i(1) = \begin{cases} q_1^{-1}: & s_i \in u_1 \\ 0: & \text{иначе} \end{cases},$$

$$q_1 = |u_1|,\ i = \overline{1, n}.$$

Этап 2. Индукция:

$$\alpha_{t+1}(j) = \left(\sum_{i=1}^{n} \alpha_t(i) \cdot p_{ij} \right) \cdot z'_j(t+1),$$

$$z'_j(t+1) = \begin{cases} n^{-1} : & |u_{t+1}| = n \\ z_j(t+1) : & \text{иначе} \end{cases},$$

$$z_j(t+1) = \begin{cases} q_{t+1}^{-1} : & s_j \in u_{t+1} \\ 0 : & \text{иначе} \end{cases}, q_{t+1} = |u_{t+1}|, j = \overline{1,\ n}, t = \overline{1, N-1}.$$

Этап 3. Находим $P\left(\hat{S}_k(N)|(P)\right) = \sum_{i=1}^{n} \alpha_N(i)$.

Пусть $d_t = \begin{cases} q_t : & q_t > 1 \\ 0 : & \text{иначе} \end{cases}$, $t = \overline{1,\ N}$. Для предложенного алгоритма справедливо

Утверждение. *Вычислительная сложность предложенного алгоритма по количеству операций умножения, сложения и умножения на константу составляет:* $(N-1)\,n^2$, $(n-1)(n\,(N-1)+1)$ *и* $d_1 + n\sum_{t=1}^{N-1} d_{t+1}$, *соответственно.*

Согласно утверждению, вычислительная сложность предложенного алгоритма имеет порядок $O(N \cdot n^2)$ как по количеству операций умножения так и по количеству операций сложения. В зависимости от вида идентифицируемого множества $\hat{S}(N)$ сложность алгоритма отличается только по количеству операций умножения на константу. Количество данных операций определяется мощностью подмножеств $q_{t+1} = |u_{t+1}| \leq n$.

Таким образом, предложенный модифицированный алгоритм «прямого-обратного хода» является достаточно эффективными по оценкам вычислительной сложности. Кроме того, метод позволяет решать задачу распознавания для последовательностей как со скрытыми, так и с частично идентифицированными элементами.

Работа выполнена при финансовой поддержке гранта РФФИ № 18–01–00120 «Специализированные устройства для генерирования и обработки массивов данных в архитектуре программируемых логических интегральных схем класса FPGA».

Список литературы

1. Нурутдинова А. Р. Идентификация автоматных марковских моделей с использованием модифицированного алгоритма «прямого-обратного хода» // Системы управления и информационные технологии. — 2018. — № 2. — С. 36–41.

2. Рабинер Л. Р. Скрытые марковкие модели и их применение в избранных приложениях при распознавании речи: обзор // ТИИЭР. — 1989. — Т. 77, № 2. — С. 257–286.

3. Нурутдинова А. Р., Шалагин С. В. Методика идентификации автоматных марковских моделей на основе порождаемых ими последовательностей // Вестник КГТУ им. А.Н. Туполева. — 2010. — № 1. — С. 94–99.

4. Кемени Дж., Снелл Дж. Конечные цепи Маркова. — М.: Наука, 1970. — 272 с.

5. Бухараев Р. Г. Вероятностные автоматы // Казань: Изд-во КГУ. — 1970. — 188 с.

6. Нурутдинова А. Р., Шалагин С. В Многопараметрическая классификация автоматных марковских моделей на основе генерируемых ими последовательностей состояний // Прикладная дискретная математика. — 2010. — № 4. — С. 41–54.

7. Захаров В. М., Нурмеев Н. Н., Салимов Ф. И., Шалагин С. В. Анализ стохастических матриц методами многомерной классификации // Дискретная математика и ее приложения: мат-лы 7-го Междунар. семинара — М.: Изд-во мех.-мат. ф-та МГУ, 2001. — С. 156–159.

Секция «Функциональные системы»

О НЕКОТОРЫХ ИНТЕРВАЛАХ РЕШЕТКИ ЗАМКНУТЫХ КЛАССОВ В ЧАСТИЧНОЙ k-ЗНАЧНОЙ ЛОГИКЕ

В. Б. Алексеев (Москва)

Пусть $E_k = \{0, 1, \ldots, k-1\}$, $E_k^n = \{(a_1, a_2, \ldots, a_n) |\ a_i \in E_k\}$ и $*$ трактуется как неопределенность. Множество всех функций $f : E_k^n \to E_k$ ($f : E_k^n \to E_k \cup \{*\}$), ($n = 1, 2, \ldots$) с операцией суперпозиции называют k-значной логикой P_k (соответственно, частичной k-значной логикой P_k^*). Под суперпозицией понимается возможность многократно произвольно переименовывать переменные, добавлять и изымать фиктивные переменные, а также подставлять функции друг в друга вместо переменных.

Важную роль в P_k и P_k^* играют классы функций, замкнутые относительно операции суперпозиции, множество которых счетно в P_2, но континуально в P_k при $k \geq 3$ и в P_k^* при $k \geq 2$. Любой замкнутый класс из P_k является замкнутым классом в P_k^*.

В [1] начато изучение связей между решетками замкнутых классов в P_k и P_k^*. А именно: для каждого предполного класса в P_2 изучалась мощность семейства замкнутых классов в P_k^*, содержащих этот класс. Было установлено, что для предполного класса линейных булевых функций эта мощность континуальна, а для остальных предполных классов конечна. Несколько изменив задачу, D. Lau предложила [2] для замкнутого класса $A \subseteq P_k$ рассматривать интервал $I(A)$ в решетке замкнутых классов в P_k^*, состоящий из тех классов, в которых множество всюду определенных функций совпадает с A. Задача определения мощности семейства $I(A)$ для различных замкнутых классов A («проблема Лау») активно изучалась многими зарубежными математиками. Однако только в 2017 году мощность $I(A)$ установлена для всех замкнутых классов A из P_2 [2, 3].

В P_k^* при $k \geq 3$ мощность интервала $I(A)$ установлена для всех предполных классов из P_k, кроме некоторых классов монотонных функций. Для предполных классов монотонных функций найдены необходимые и достаточные условия, при которых интервал $I(A)$ бес-

конечен [4–6], однако пока неизвестна точная мощность этих интервалов.

Пусть A — замкнутый класс в P_k. Через $Str(A)$ в [2] обозначено множество всех функций из P_k^*, которые можно доопределить (заменой $*$ на другие значения) до некоторой функции из A. Для любого замкнутого класса A класс $Str(A)$ замкнут и $A \subseteq Str(A)$. Очевидно, что множество всюду определенных функций в $Str(A)$ совпадает с A и значит $Str(A)$ содержится в интервале $I(A)$. Обозначим через $Int(A)$ множество всех замкнутых классов B в P_k^*, таких, что $A \subseteq B \subseteq Str(A)$. Тогда $Int(A) \subseteq I(A)$. Интересной задачей является определение мощности семейства $Int(A)$ для различных замкнутых классов A. Например, для класса L булевских линейных функций мощность $I(L)$ континуальна, а про $Int(L)$ доказано только, что это семейство бесконечно [1], но точная мощность его неизвестна. Если A — предполный класс монотонных k-значных функций, то семейство $I(A)$ может быть и конечным и бесконечным, но семейство $Int(A)$ всегда конечно и состоит из 6 замкнутых классов.

При изучении интервала $Int(A)$ возникает интересная связь с множествами предикатов на E_k. Пусть $Pr(k)$ — множество всех предикатов на E_k (то есть функций, принимающих только значения 0 и 1) от любого числа переменных. Пусть A — замкнутый (относительно суперпозиции) класс из P_k. Пусть O_A — множество следующих операций над предикатами из $Pr(k)$: произвольное переименование переменных, добавление и изъятие фиктивных переменных, подстановка в предикат функций из A вместо переменных и дизъюнкция предикатов. Обозначим через $Z(A)$ семейство всех подмножеств в $Pr(k)$, замкнутых относительно этих операций.

Теорема. *Для любого замкнутого класса A из P_k интервал $Int(A)$ с отношением включения и семейство $Z(A)$ с отношением включения изоморфны.*

Если A и B — замкнутые классы из P_k и $A \subseteq B$, то все операции из O_A содержатся среди операций из O_B. Поэтому любой класс предикатов, замкнутый относительно операций из O_B, замкнут и относительно операций из O_A. Структура $Z(B)$ (с отношением включения) получается из структуры $Z(A)$ «прореживанием» (возможно, структуры совпадают). Таким образом, при переходе к более широкому замкнутому классу мощность $Z(A)$, а значит и $Int(A)$, не может увеличиваться (при этом, так как в P_k^* счетное число функций, то мощность $Int(A)$ при любом A не превосходит континуума).

Обычно рассматривают только те замкнутые классы (клоны), ко-

торые содержат все селекторные функции (равные просто переменной). Самым маленьким из них является класс I всех селекторов.

Теорема. *Интервал $Int(I)$ для любого $k \geq 2$ содержит континуум замкнутых классов.*

Для доказательства этой теоремы рассматриваются предикаты $Maj_n = Maj(x_1, x_2, \ldots, x_n)$, $n = 1, 2, \ldots$ на E_k, которые принимают значение 1, если и только если вес набора (обычная сумма координат) больше половины от максимального веса, то есть от $n \cdot (k-1)$. Доказывается следующее утверждение.

Лемма. *При любом $k \geq 2$ в множестве предикатов $\{Maj_{2n}, n = 2, 3, 5, \ldots\}$, где n пробегает множество простых чисел, ни один предикат не выражается через остальные с помощью операций из O_I.*

Из леммы вытекает , что замыкания разных подмножеств из $\{Maj_4, Maj_6, Maj_{10}, \ldots\}$ относительно операций из O_I дают разные классы из $Z(I)$. Получаем, что мощность семейства $Z(I)$ равна континууму, и справедливость второй теоремы вытекает из первой.

Интересно определить мощность интервала $Int(A)$ для других замкнутых классов A из P_k, в частности, для всех замкнутых классов A из P_2. В [3] показано, что мощность интервала $I(A)$ для любого замкнутого класса A из P_2 либо конечна, либо равна континууму. Для последних классов интересно выяснить, сохранится ли континуальность при переходе к интервалу $Int(A)$ и бывают ли классы, для которых эта мощность становится счетной.

Работа выполнена при поддержке РФФИ (проект №17–01–00782а).

Список литературы

1. Алексеев В. Б., Вороненко А. А. О некоторых замкнутых классах в частичной двузначной логике // Дискретная математика. — 1994. — Т. 6, вып. 4. — С. 58–79.

2. Lau D. Function algebras on finite sets: a basic course on many-valued logic and clone theory. — Berlin.: Springer, 2006.

3. Couceiro M., Haddad L., Schölzel K., Waldhauser T. A solution to a problem of D. Lau: Complete classification of intervals in the lattice of partial Boolean clones // J. Mult.-Valued Logic Soft Comput. — 2017. — V. 28. — P. 47–58.

4. Дудакова О. С. О классах частичных монотонных функций шестизначной логики // Проблемы теоретической кибернетики: XVIII международная конференция (Пенза, 19–23 июня 2017 г.): Материалы: Под редакцией Ю. И. Журавлева. —М.: МАКС Пресс, 2017. — С. 78–81.

5. Алексеев В. Б. О замкнутых классах в частичной k-значной

логике, содержащих класс монотонных функций // Дискретная математика. — 2018. — Т. 30, вып. 2. — С. 3–13.

6. Дудакова О. С. Построение бесконечного семейства классов частичных монотонных функций многозначной логики // Вестник Московского университета. Серия 1: Математика. Механика. — 2019. — № 1. — С. 3–7.

О РЕШЕТКЕ ЗАМКНУТЫХ КЛАССОВ АВТОМАТОВ С ОПЕРАЦИЕЙ СУПЕРПОЗИЦИИ.

Бабин Д. Н.

Известно, что в классе автоматов с операцией суперпозиции любая полная система бесконечна [1, 2], имеется континуум предполных классов [3], и полна система двухместных автоматов [4].

Пусть $E_2 = \{0, 1\}$, P_2 — множество булевых функций вида $g : E_2^n \to E_2$, E_2^∞ — множество всех сверхслов из нулей и единиц. Функция вида

$$f : (E_2^\infty)^n \to (E_2^\infty)^m$$

называется *автоматной функцией (a-функцией)*, которая задается известными рекуррентными соотношениями [1]. Булеву функцию мы будем ассоциировать с автоматной, выдающей в каждый момент значение булевой функции от входных аргументов в этот момент. Класс всех a-функций обозначим через P. В этом классе обычным образом введем операции суперпозиции автоматных функций.

Автоматная функция T_0, задаваемая уравнениями

$$\begin{cases} (q_1(1), q_2(1)) = (0, 0), \\ (q_1(t+1), q_2(t+1)) = (a_1(t), a_2(t)); \text{при } (a_1(t), a_2(t)) = (0, 0) \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{и } (a_1(t), a_2(t)) = (1, 1), \\ (q_1(t+1), q_2(t+1)) = (q_1(t), q_2(t)); \text{ при } (a_1(t), a_2(t)) = (0, 1), \\ (q_1(t+1), q_2(t+1)) = (q_2(t), q_1(t)); \text{ при } (a_1(t), a_2(t)) = (1, 0), \\ (b_1(t), b_2(t)) = (q_1(t), q_2(t)) \end{cases}$$

называется автоматной функцией «триггер». Здесь $(a_1(t), a_2(t))$, $(q_1(t), q_2(t))$, $(b_1(t), b_2(t)) \in (E_2)^2$.

Константной автоматной функцией назовем автоматную функцию, выдающую одно и тоже периодическое выходное сверхслово на всех входных сверхсловах. Класс константных автоматных функций обозначим через K.

Имеют место

Теорема 1 ([5])**.** *В P не существует предполного класса автоматных функций содержащего замкнутый класс $[K \cup P_2 \cup \{T_0\}]$.*

Теорема 2. *Пусть замкнутые классы μ, X таковы что $[P_2 \cup \{T_0\}] \subseteq \mu \subset X$, $\mu \nsubseteq K$, $K \subset X$. Тогда класс μ расширяется до предполного класса в X.*

Следствие 1. *Всякий конечно-порожденный замкнутый класс μ в замкнутом классе автоматных функций $X \supseteq [K \cup P_2 \cup \{T_0\}]$ расширяется до предполного.*

Следствие 2. *Всякий конечно-порожденный замкнутый класс μ в P расширяется до предполного.*

Получается итоговая

Теорема 3. *Замкнутый класс $\mu \supseteq [P_2 \cup \{T_0\}]$ расширяется до предполного класса точно тогда, когда $\mu \not\supseteq K$*

Все полученные результаты верны также для автоматных функций над $E_k = \{0, 1, \dots k-1\}$.

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М:. Наука, 1985

2. Алешин С. В. Алгебраические системы автоматов. — М:. МАКС Пресс, 2016

3. Кудрявцев В. Б. О мощностях множеств предполных классов некоторых функциональных систем, связанных с автоматами // ДАН СССР[— 1963. — Т. 151. —С. 493–496.

4. Бабин Д. Н. О полноте двухместных автоматных функций относительно суперпозиции // Дискретная математика. — 1989. — Т.1, вып. 4. — С. 86-92.

5. Бабин Д. Н. Класс автоматов с суперпозициями, не расширяющийся до предполного // Интеллектауальные системы. Теория и приложения. — 2016. — Т 20, вып. 4. — С. 162-173

О КЛАССАХ ЧАСТИЧНЫХ МОНОТОННЫХ ФУНКЦИЙ ТРЕХЗНАЧНОЙ ЛОГИКИ

О. С. Дудакова (Москва)

В работе исследуются замкнутые классы частично определенных функций многозначной логики [1]. Рассматривается задача описания классов частичных функций, содержащих замкнутый класс всюду определенных монотонных функций. Известно [2, 3], что если на E_k задан частичный порядок с наименьшим и наибольшим элементами, то семейство классов частичных функций, монотонных на своей области определения, содержащих класс всех всюду определенных монотонных функций, имеет конечную мощность тогда и только тогда, когда частичный порядок является решеткой. В данной работе получены некоторые аналогичные результаты для частичных порядков без наименьшего и наибольшего элементов.

Пусть $E_3 = \{0, \alpha, \alpha'\}$. Через P_3^* обозначается семейство всех частичных функций на E_3, то есть множество всевозможных отображений $f : E_3^n \to \{E_3 \cup \{*\}\}$ для всех $n \geq 1$. Обозначим через $\mathcal{E}$ частично упорядоченное множество $(E_3, \leq)$, такое что $0 \leq \alpha,\ 0 \leq \alpha'$, элементы α и α' несравнимы. Обозначим через M, $\widehat{M}^*$ и M^* классы всех всюду определенных монотонных функций на $\mathcal{E}$, всех частичных функций, монотонных на своей области определения, и всех частичных функций из $\widehat{M}^*$, доопределяемых до функций из M соответственно.

Пусть F_1 и F_2 — замкнутые классы в P_3^*. Положим

$$\mathcal{I}(F_1, F_2) = \{G \subseteq P_3^* \mid [G] = G, F_1 \subseteq G \subseteq F_2\}.$$

В настоящей работе исследуется интервал $\mathcal{I}(M^*, \widehat{M}^*)$.

Пусть $f(x_1, \ldots, x_n) \in P_3^*$. Тройку наборов $\widetilde{a}, \widetilde{a}', \widetilde{z} \in \mathcal{E}^n$ назовем *полуквадратом* для f в $\mathcal{E}^n$, если выполняются следующие условия: 1) $\widetilde{a}, \widetilde{a}' < \widetilde{z}$; 2) $f(\widetilde{a}) = \alpha, f(\widetilde{a}') = \alpha', f(\widetilde{z}) = *$ (определение полуквадрата соответствует определению квадрата из работы [2]). Нетрудно показать, что произвольная функция $f(x_1, \ldots, x_n)$ из $\widehat{M}^*$ принадлежит M^* тогда и только тогда, когда в $\mathcal{E}^n$ нет полуквадратов для f.

Пусть $f \in \widehat{M}^*,\ \widetilde{a}, \widetilde{a}', \widetilde{z}$ — полуквадрат для f. Последовательность наборов $\widetilde{a}_1, \ldots, \widetilde{a}_k,\ k \geq 3$, назовем *путем в полуквадрате*, если выполняются следующие условия: $\widetilde{a}_1 = \widetilde{a},\ \widetilde{a}_k = \widetilde{a}'$; $\widetilde{a}_i$ и $\widetilde{a}_{i+1}$ сравнимы для всех $i = 1, \ldots, k-1$; $f(\widetilde{a}_i) \neq *$ для всех $i = 2, \ldots, k-1$. Число $k-2$ будем называть *длиной пути*.

Определим следующие множества функций (см также [2]):

F_∞**:** множество всех функций $f \in \widehat{M}^*$, таких что для f нет полуквадрата, в котором есть путь.

F_k**:** множество всех функций $f \in \widehat{M}^*$, таких что для f нет полуквадрата, в котором есть путь длины меньшей, чем k, $k \geq 1$.

Заметим, что в этих обозначениях $F_1 = \widehat{M}^*$.

Теорема 1. *Все множества $F_2, F_3, \ldots, F_\infty$ являются замкнутыми классами и выполняются включения*

$$M^* \subset F_\infty \subset \ldots \subset F_{k+1} \subset F_k \subset \ldots \subset F_2 \subset F_1 = \widehat{M}^*.$$

Теорема 2. *Справедливы следующие утверждения*:

1. *Пусть $f \in \widehat{M}^* \setminus F_2$. Тогда $[\{f\} \cup M^*] = \widehat{M}^*$.*
2. *F_2 — единственный предполный в $\widehat{M}^*$ класс, содержащийся в интервале $\mathcal{I}(M^*, \widehat{M}^*)$.*
3. *Пусть $f \in \widehat{M}^* \setminus M^*$. Тогда в замыкании $[\{f\} \cup M^*]$ найдется функция $g \in F_\infty \setminus M^*$.*
4. *Пусть $g \in F_\infty \setminus M^*$. Тогда $[\{f\} \cup M^*] = F_\infty$.*
5. *M^* — предполный класс в F_∞; любой замкнутый класс из интервала $\mathcal{I}(M^*, \widehat{M}^*)$, отличный от M^*, содержит класс F_∞.*

Пусть $f \in \widehat{M}^*$, $\widetilde{a}, \widetilde{a}', \widetilde{z}$ — полуквадрат для f и $\widetilde{a}_1, \ldots, \widetilde{a}_k$ — путь в полуквадрате, $k \geq 3$. Будем говорить, что путь *идет вниз*, если $\widetilde{a}_2 < \widetilde{a}_1$, и *идет вверх*, если $\widetilde{a}_2 > \widetilde{a}_1$. Далее, для каждого $k = 2, 3, \ldots$ обозначим через $F_k^\sharp$ множество всех функций из F_k, для которых не существует полуквадрата, в котором есть одновременно путь длины k, идущий вверх, и путь длины k, идущий вниз.

Теорема 3. *Все множества $F_k^\sharp$, $k = 2, 3, \ldots$, являются замкнутыми классами и выполняются включения $F_{k+1} \subset F_k^\sharp \subset F_k$.*

Обозначим через G множество всех функций f из $F_2 \setminus F_2^\sharp$, обладающих следующим свойством: пусть $\widetilde{a}, \widetilde{a}', \widetilde{z}$ — полуквадрат для f, $\widetilde{a}, \widetilde{b}_1, \widetilde{b}_2, \widetilde{a}'$ — путь длины 2 в этом полуквадрате, идущий вниз, $\widetilde{a}, \widetilde{c}_1, \widetilde{c}_2, \widetilde{a}'$ — путь длины 2 в этом полуквадрате, идущий вверх. Тогда не существует такого набора $\widetilde{d}$, для которого выполняются неравенства $\widetilde{b}_1, \widetilde{c}_2 < \widetilde{d} < \widetilde{b}_2, \widetilde{c}_1$ и $f(\widetilde{d}) \neq *$. Обозначим через $F_2^{\sharp\sharp}$ множество $F_2^\sharp \cup G$. Нетрудно показать, что $F_2^\sharp \subset F_2^{\sharp\sharp} \subset F_2$.

Теорема 4. *Множество $F_2^{\sharp\sharp}$ является замкнутым классом, причем это единственный предполный в F_2 класс, содержащийся в интервале $\mathcal{I}(M^*, \widehat{M}^*)$.*

Заметим, что утверждения теорем 1 и 3 справедливы для произвольного частично упорядоченного множества $\mathcal{P} = (E_k, \leq)$, в котором есть хотя бы одна пара элементов, не имеющих верхней грани. В этом случае полуквадрат для функции $f(x_1, \ldots, x_n)$ будет определяться как тройка наборов $\widetilde{a}, \widetilde{a}', \widetilde{z} \in \mathcal{P}^n$, для которых выполняются условия: 1) $\widetilde{a}, \widetilde{a}' < \widetilde{z}$; 2) $f(\widetilde{a}) = p_1, f(\widetilde{a}') = p_2, f(\widetilde{z}) = *$, где p_1 и p_2 — пара элементов $\mathcal{P}$, не имеющих верхней грани; понятие пути в полуквадрате, а также семейства функций $F_k, F_k^\sharp$ и F_∞ определяются аналогичным образом. Кроме того, заметим, что аналогичные результаты можно получить для частично упорядоченных множеств, содержащих пару элементов, не имеющих нижней грани.

Работа выполнена при поддержке РФФИ (проект № 18–01–00337 «Проблемы синтеза, сложности и надежности в теории управляющих систем»).

Список литературы

1. Lau D. Function algebras on finite sets: a basic course on many-valued logic and clone theory. — Springer Monographs in Mathematics. — Berlin. — Springer, 2006.

2. Дудакова О. С. Построение бесконечного семейства классов частичных монотонных функций многозначной логики // Вестник Московского университета. Серия 1: Математика. Механика. — 2019. — № 1. — С. 3–7.

3. Алексеев В. Б. О замкнутых классах в частичной k-значной логике, содержащих класс монотонных функций // Дискретная математика. — 2018. — 30, вып. 2. — С. 3–13.

НА ПУТИ К ПОЛНОЙ КЛАССИФИКАЦИИ НЕЛИНЕЙНЫХ ПО МОДУЛЮ k ФУНКЦИЙ P_k

Д. Г. Мещанинов (Москва)

Пусть $k \geq 2$, $E_k = \{0, 1, \ldots, k-1\}$, $P_k = \{f : E_k^n \to E_k,\ n = 0, 1, 2 \ldots\}$ — класс всех функций k-значной логики. Мы рассматриваем замкнутые относительно суперпозиции классы в P_k, содержащие все линейные по модулю k функции, и решетку таких классов как

важную часть континуальной при $k \geq 3$ решетки $\mathcal{L}_k$. Анализируемые классы описываются каноническими представлениями своих элементов в виде аддитивных формул (сумм) [1, 2], слагаемые которых определены однозначно. В каждой такой сумме одно слагаемое является линейной функцией. Мы укажем семейства таких классов, их полные системы, канонические формулы и место классов в решетке $\mathcal{L}_k$.

Введем следующие определения и обозначения.

Пусть $d|k$. Функция $f(\tilde{x}) = f(x_1, \ldots, x_n)$ из P_k, удовлетворяющая условию

$$\tilde{a} \equiv \tilde{b} \pmod{d} \;\Rightarrow\; f(\tilde{a}) \equiv f(\tilde{b}) \pmod{d},$$

называется *d-периодической.*

Будем применять обозначения:
$G_d(\tilde{x})$ — для d-периодической функции;
$dF(\tilde{x})$ — для функции, все значения которой кратны d;
$l(\tilde{x})$ — для линейной функции;
$A(M)$ — для системы функций, полной в замкнутом классе M;
$p, p_1, \ldots, p_s, q$ — для простых чисел.

Введем функции:

$$g_d(\tilde{x}) = \begin{cases} 1, & \text{если } \tilde{x} \equiv \tilde{0} \pmod{d}, \\ 0, & \text{иначе,} \end{cases} \qquad j(\tilde{x}) = \begin{cases} 1, & \text{если } \tilde{x} = \tilde{0}, \\ 0, & \text{иначе,} \end{cases},$$

$$\chi_{d,\,i}(\tilde{x}) = x_i g_d(\tilde{x}),\ i = 1, \ldots, n; \qquad \delta_d(x) = d\lfloor x/d \rfloor.$$

Рассмотрим следующие семейства классов (всюду $d|k$).

1. Классы $C(d) = \{f(\tilde{x}) = l(\tilde{x}) + G_d(\tilde{x}) + dF(\tilde{x})\}$ порождаются системами $\{1, x + y,\ g_d(x, y),\ dj(x, y)\}$. Если $d \neq 1$ и $d \neq k$, то класс $C(d)$ является предполным в P_k [3].

2. Классы $C_1(d) = \{f(\tilde{x}) = l(\tilde{x}) + dF(\tilde{x})\}$ порождаются системами $\{1, x + y,\ dj(x, y)\}$. Класс $C_1(d)$ является предполным в классе $C(d)$ в точности при $k = pd$ [4].

3. Классы $R(d) = \{f(\tilde{x}) = l(\tilde{x}) + G_d(\tilde{x}) + dF(\tilde{x})\}$, где

$$\begin{aligned} dF(\tilde{x}) = \sum_{\tilde{a} \,\in\, E_d^n} \sum_{i=1}^{n} c_1(\tilde{a},\ i)\chi_{d,\,i}(\tilde{x} - \tilde{a}) + \\ + \sum_{i=1}^{n} \delta_d(x_i), \quad c_1(\tilde{a}, i), c_2(i) \in E_k, \end{aligned} \tag{1}$$

порождаются системами $\{1, x+y,\ \chi_{d,\,1}(x),\ dj(x,y)\}$. Класс $R(d)$ является предполным в классе $C(d)$ в точности при $k = pd$ [5].

4. Классы $L(d) = \{f(\tilde{x}) = l(\tilde{x}) + G_d(\tilde{x}) + \sum_{i=1}^{n} \delta_d(x_i)\}$ порождаются системами $\{1, x+y,\ g_d(x,y)\}$. Класс $L(d)$ является предполным в классе $R(d)$ в точности при $k = pd$ [6].

5. Классы $S(d) = \{f(\tilde{x}) = l(\tilde{x}) + dG_d(\tilde{x}) + dF(\tilde{x})\}$, где $dF(\tilde{x})$ имеет вид (1), порождаются системами

$$\{1, x+y,\ \chi_{d,\,1}(\tilde{x}),\ \delta_d(x)\} \cup \bigcup_{n=1}^{\infty} \{dg_d(x_1, \ldots, x_n)\}.$$

При $k = p^2$ и $k = pq$ класс $S(p)$ конечно-порожден и является предполным в $R(p)$ [4].

6. Классы $K(d) = \{f(\tilde{x}) = l(\tilde{x}) + dG_d(\tilde{x})\}$ порождаются системами

$$\{1, x+y\} \cup \bigcup_{n=1}^{\infty} \{dg_d(x_1, \ldots, x_n))\}.$$

Теорема 1 ([7]). *При $k = pq$ класс $K(p)$ конечно-порожден и является предполным в классе $L(p)$, а класс L является предполным в $K(p)$ и $K(q)$.*

Следствие. *При $k = pq$ имеются следующие неуплотняемые цепи замкнутых классов*:

$$L \subset K(d) \subset L(d) \subset R(d) \subset C(d) \subset P_k, \quad d = p, q.$$

Эти классы содержат, в частности, функции, не представимые полиномами по модулю pq.

Для сравнения приведем следующий результат, имеющий место при $k = p^2$.

Теорема 2 ([8]). *При $k = p^2$ класс всех полиномов по модулю k есть $R(p)$. Решетка всех классов полиномов, содержащих L, бесконечна. Класс $K(p)$ бесконечно-порожден, не имеет базиса и является пределом возрастающей цепи своих подклассов.*

Для классов полиномов, содержащих L, справедлива

Теорема 3 ([6]). *При $k = p_1 \cdots p_s$ все классы полиномов, содержащие L, образуют решетку, изоморфную s-мерному кубу.*

Список литературы

1. Мещанинов Д. Г. Семейства замкнутых классов в P_k, определяемые аддитивными и полиномиальными представлениями функций // Материалы XII Международного семинара «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (20–25

июня 2016 г.). — М.: Изд-во механико-математического факультета МГУ, 2016. — С. 96–106.

2. Мещанинов Д. Г. Функции, обобщающие полиномы по модулю k // Труды X Международной конференции "Дискретные модели в теории управляющих систем" (Москва и Подмосковье, 23–25 мая 2018 г.) — М.: МАКС-Пресс, 2018. — С. 198–200.

3. Яблонский С. В. Функциональные построения в k-значной логике // Труды МИАН СССР. — 1958. — Т. 51. — С. 5–142.

4. Мещанинов Д. Г. Некоторые замкнутые классы в P_k и их гомоморфизмы в P_d при $d|k$ // Труды XVIII Международной конференции «Проблемы теоретичской кибернетики» (Пенза, 19–23 июня 2017 г.). — М.: МАКС-Пресс, 2017. — С. 161–163.

5. Мещанинов Д. Г. О первых d-разностях функций k-значной логики // Математические вопросы кибернетики. Вып. 7. — М.: Наука, 1998. — С. 265–280.

6. Мещанинов Д. Г. О замкнутых классах k-значных функций, сохраняющих первые d-разности // Математические вопросы кибернетики. Вып. 8. — М.: Наука, 1999. — С. 219–230.

7. Мещанинов Д. Г. Об одном семействе замкнутых классов в k-значной логике // Вестник Московского университета. Сер. 15. Вычислительная математика и кибернетика. — 2019. — № 1. — С. 26–32.

8. Мещанинов Д. Г. Замкнутые классы полиномов по модулю p^2 // Дискретная математика. — 2017. — Т. 29, вып. 3. — С. 54–69.

АРИФМЕТИЗАЦИЯ РЕГИСТРОВЫХ МАШИН СО СЧЁТЧИКАМИ

И. В. Савицкий (Москва)

Рассматривается задача построения базиса по суперпозиции в классе $\mathcal{E}^2$ иерархии Гжегорчика. Приводится новый базис в этом классе, полученный при помощи арифметизации RC-машин.

Пусть $x \dot{-} y = \max(x - y, 0)$; $\lfloor x/y \rfloor$ — целая часть от деления x на y; $\mathrm{rm}(x, y)$ — остаток от деления x на y.

Класс $\mathcal{E}^2$ — это наименьший класс функций, содержащий функции 0, $x+1$, $x \cdot y$ и замкнутый относительно операции суперпозиции и операции ограниченной примитивной рекурсии, позволяющей получить функцию f из функций g, h, j согласно соотношениям

$$\begin{cases} f(\tilde{x}^n, 0) = g(\tilde{x}^n), \\ f(\tilde{x}^n, y+1) = h(\tilde{x}^n, y, f(\tilde{x}^n, y)), \\ f(\tilde{x}^n, y) \leqslant j(\tilde{x}^n, y). \end{cases}$$

В работе [1] С. А. Волков при помощи арифметизации машин Минского получил следующий базис по суперпозиции в классе $\mathcal{E}^2$:

$$x+1,\ xy,\ x \dot{-} y,\ \lfloor x/y \rfloor,\ \min(2^x, y),\ \lfloor \log_2 x \rfloor,\ Q(x, p_1, p_2, c_1, c_2, t),$$

где функция Q получается по схеме

$$\begin{cases} Q(x, p_1, p_2, c_1, c_2, 0) = x, \\ Q(x, p_1, p_2, c_1, c_2, t+1) = Q(x, p_1, p_2, c_1, c_2, t) + R(p_2, c_2 t), \\ \qquad\qquad\qquad\qquad \text{если } Q(x, p_1, p_2, c_1, c_2, t) \wedge R(p_1, c_1 t) = 0, \\ Q(x, p_1, p_2, c_1, c_2, t+1) = Q(x, p_1, p_2, c_1, c_2, t) \ \text{ иначе}, \end{cases}$$

при этом $x \wedge y$ — поразрядная конъюнкция двоичных представлений чисел x и y, а $R(x, y)$ — циклический сдвиг двоичного представления числа x на y разрядов вправо.

Мы применим схожий метод арифметизации к регистровым машинам со счётчиками (RC-машины) [2].

RC-машина $\mathcal{M}$ состоит из входных регистров $x_1, \ldots, x_n$, счётчиков $t_1, \ldots, t_m$, регистров r и 0 и набора программ $P_1, \ldots, P_s$. Вычисление на RC-машине $\mathcal{M}$ на входе $\tilde{x}^n$ со значением ёмкости счётчиков t производится следующим образом. Входные регистры содержат значения входа, а нулевой регистр — число 0. В начальный момент счётчики и регистр r содержат 0, и активна программа P_1. На каждом такте активная программа в зависимости от соотношений $=$, $<$, $>$ между всеми парами регистров и счётчиков выбирает регистр или счётчик, значение которого заносится в r, или любую программу (кроме P_1), которая будет активирована на следующем такте (при этом в любом вычислении каждая программа может быть активирована не более одного раза). Затем счётчики меняются по принципу прибавления единицы к числу

$$t_1 + t_2 \cdot t + \ldots + t_{m-1} \cdot t^{m-2} + t_m \cdot t^{m-1}$$

в позиционной системе счисления с основанием t, после чего происходит переход к следующему такту. Вычисление заканчивается через t^m тактов. Результат вычисления $\mathcal{M}(\tilde{x}^n;\ t)$ содержится в r.

Пусть $T(\tilde{x}^n)$ — функция натурального аргумента. Функция $f(\tilde{x}^n)$ *вычислима* на RC-машине $\mathcal{M}$ с ёмкостью счётчиков $T(\tilde{x}^n)$, если $f(\tilde{x}^n) = \mathcal{M}(\tilde{x}^n;\ T(\tilde{x}^n))$. Всюду определённая функция $f(\tilde{x}^n)$ *строго вычислима* на RC-машине $\mathcal{M}$ с ёмкостью счётчиков $T(\tilde{x}^n)$, если она вычислима на $\mathcal{M}$ с любой ёмкостью счётчиков $T'(\tilde{x}^n) \geqslant T(\tilde{x}^n)$.

В [2] с помощью RC-машин были промоделированы вычисления на машинах SRM [3] и получен следующий результат.

Теорема 1. *Любая функция из класса $\mathcal{E}^2$ строго вычислима на подходящей* RC*-машине с полиномиальной ёмкостью счётчиков.*

Пусть $\varphi_1(\tilde{x}^n, t), \ldots, \varphi_k(\tilde{x}^n, t)$ — функции натурального аргумента. RC-машина с константами $\varphi_1, \ldots, \varphi_k$ получается из RC-машины добавлением регистров $T_1, \ldots, T_k$, которые во время вычисления на входе $\tilde{x}^n$ со значением ёмкости счётчиков t постоянно содержат значения $\varphi_1(\tilde{x}^n, t), \ldots, \varphi_k(\tilde{x}^n, t)$. Соотношения $=, <, >$ с участием этих регистров учитываются при выборе команды, и значения этих регистров могут быть записаны в r. Как показано в [4], использование констант позволяет обходиться RC-машинами с одной программой.

Теорема 2. *Любая функция из класса $\mathcal{E}^2$ строго вычислима на подходящей* RC*-машине с одной программой, константами вида $c_1 \cdot \lfloor t/c_2 \rfloor$ и полиномиальной ёмкостью счётчиков.*

Будем называть RC-машинами без неравенств RC-машины, программы которых при выборе команды позволяют лишь проверять, равны ли значения регистров/счётчиков в каждой паре, не различая, какое из значений в паре больше, а какое меньше.

Теорема 3. *Любая функция из класса $\mathcal{E}^2$ строго вычислима на подходящей* RC*-машине без неравенств с одной программой, константами вида $c_1 \cdot \lfloor t/c_2 \rfloor + c_3$ и полиномиальной ёмкостью счётчиков.*

Рассмотрим ещё одну модификацию RC-машин. RC-машина $\mathcal{M}$ с ограниченным числом сравнений устроена аналогично RC-машинам с константами, но вместо программ она имеет набор команд $(g_1, \ldots, g_s)$. Каждая команда g_j имеет вид $r = a_j,\ b_j = c_j \to d_j$, где a_j, b_j, c_j, d_j — любые регистры/счётчики $\mathcal{M}$, кроме регистра r.

Во время вычисления машина $\mathcal{M}$ на такте i всегда выполняет команду g_j, где $j = \mathrm{rm}(i, s) + 1$. При этом, если $r = a_j$ и $b_j = c_j$, то в регистр r заносится d_j. Иначе значение регистра r не меняется.

Теорема 4. *Любая функция из класса $\mathcal{E}^2$ строго вычислима на*

RC-*машине с ограниченным числом сравнений, константами вида* $c_1 \cdot \lfloor t/c_2 \rfloor + c_3$ *и полиномиальной ёмкостью счётчиков.*

Представляя значения регистров и счётчиков и номера регистров в программе цифрами числа в позиционной системе счисления, можно арифметизировать вычисления на RC-машинах с ограниченным числом сравнений. Пусть функция $Q(x,T,t)$ задаётся схемой

$$\begin{cases} Q(x,T,0) = 0, \\ Q(x,T,t+1) = (x+t)[x\{4t+3\}_T]_T, \\ \qquad\qquad\qquad \text{если } Q(x,T,t) = (x+t)[x\{4t+2\}_T]_T \\ \qquad\qquad\qquad \text{и } \ (x+t)[x\{4t\}_T]_T = (x+t)[x\{4t+1\}_T]_T, \\ Q(x,T,t+1) = Q(x,T,t) \ \text{ иначе.} \end{cases}$$

Здесь $x[y]_T$ — y-я по старшинству цифра (0 соответствует младшей цифре) числа x в позиционной системе счисления с основанием T; а $x\{y\}_T = x[\mathrm{rm}(y, N_T(x))]_T$, где $N_T(x)$ — число цифр в числе x в системе счисления с основанием T.

Теорема 5. *Система функций*

$$x+1, \ x+y, \ xy, \ Q(x,T,t)$$

является базисом по суперпозиции в классе $\mathcal{E}^2$.

Список литературы

1. Волков С. А. Пример простой квазиуниверсальной функции в классе $\mathcal{E}^2$ иерархии Гжегорчика // Дискретная математика. — 2006. — Т. 18, вып. 4. — С. 31–44.

2. Савицкий И. В. Вычисления на регистровых машинах со счетчиками // Дискретная математика. — 2017. — Т. 29, вып. 1. — С. 95–113.

3. Бельтюков А. П. Машинное описание и иерархия начальных классов Гжегорчика // Записки научных семинаров Ленинградского отделения Математического института им. В. А. Стеклова АН СССР. — 1979. — Т. 88. — С. 30–46.

4. Марченков С. С., Савицкий И. В. Машины в теории вычислимых функций. — М.: МАКС Пресс, 2018.

О КЛАССАХ САМОДВОЙСТВЕННЫХ ФУНКЦИЙ НЕЯВНО ПРЕДПОЛНЫХ В P_k

М. В. Старостин (Москва)

Понятие неявной выразимости введено А. В. Кузнецовым как одно из обобщений выразимости по суперпозиции [1].

Пусть Σ — произвольная система функций k-значной логики P_k. Следуя [2], обозначим через $E(\Sigma)$ множество $[\Sigma \cup \{x\}]$, которое будем называть *явным замыканием* Σ. Говорят, что функция $f(x_1, x_2, \ldots, x_n) \in P_k$ *неявно выразима* над системой функций Σ, если существуют такие функции $A_i(x_1, x_2, \ldots, x_n, z)$ и $B_i(x_1, x_2, \ldots, x_n, z)$, где $i = 1 \leq i \leq m$, принадлежащие $E(\Sigma)$, что система неявных уравнений

$$\begin{cases} A_1(x_1, \ldots, x_n, z) = B_1(x_1, \ldots, x_n, z), \\ A_2(x_1, \ldots, x_n, z) = B_2(x_1, \ldots, x_n, z), \\ \qquad\qquad \ldots \\ A_m(x_1, \ldots, x_n, z) = B_m(x_1, \ldots, x_n, z), \end{cases}$$

эквивалентна единственному уравнению $z = f(x_1, x_2, \ldots, x_n)$.

Множество всех функций, неявно выразимых над системой Σ называется *неявным расширением* Σ и обозначается через $I(\Sigma)$. Нетрудно заметить, что неявное расширение любой системы функций содержит в себе ее замыкание по суперпозиции. Говорят, что система функций Σ является *неявно полной* в P_k, если ее неявное расширение совпадает с P_k.

Выделим несколько основных подходов к установлению неявной полноты систем функций. Первый из них использует критерий неявной полноты в P_k, доказанный О. М. Касим-Заде в [3]. Этот критерий позоляет установить неявную полноту системы по множеству функций от трех переменных, содержащихся в ее явном замыкании. А именно, система функций $\Sigma \in P_k$ неявно полна тогда и только тогда, когда для любого набора $\tilde{\alpha} \in E_k^3$ в $E(\Sigma)$ найдется такая пара функций f и g, зависящих от трех переменных, что их значения различаются только на наборе $\tilde{\alpha}$.

Второй подход использует понятие минимальных по включению неявно полных замкнутых по суперпозиции классов. Он основан на том, что каждый неявно полный класс содержит в своем явном замыкании один из минимальных полных классов. В [3] доказано, что при любом $k \geq 2$ минимальных неявно полных классов конечное число. Списки всех минимальных неявно полных классов в P_2 и P_3 приведены в работе [4].

Третий подход использует понятие неявно предполных классов. Класс функций F называется *неявно предполным* в P_k, если он не является неявно полным, но становится таковым при добавлении к нему любой функции не из F. Известно, что их число также конечно при любом $k \geq 2$ [3]. Отметим, что из соотношений между неявной выразимостью и выразимостью по суперпозиции следует, что любой предполный по суперпозиции класс является либо неявно полным, либо неявно предполным. Касим-Заде в [5] установил, что в P_2 имеется ровно 6 неявно предполных классов: T_0, T_1, S, L, K, D. Описание всех неявно предполных классов в P_3 получено автором в [6]. В частности, неявно предполными оказались классы сохранения констант, а также класс самодвойственных функций.

Обозначим группу подстановок на множестве E_k через $\mathfrak{S}_k$. Говорят, что функция $f(x_1, \ldots, x_n) \in P_k$ является самодвойственной относительно подстановки $\sigma \in \mathfrak{S}_k$, если $\sigma f(x_1, \ldots, x_n) = f(\sigma(x_1), \ldots, \sigma(x_n))$. Множество всех самодвойственных относительно подстановки σ функций является замкнутым по суперпозиции классом и обозначается через S_σ. Известно, что класс S_σ является предполным по суперпозиции тогда и только тогда, когда σ разлагается в произведение циклов одинаковой простой длины [7].

Будем говорить, что элемент $a \in E_k$ является *неподвижной точкой* подстановки σ, если $\sigma a = a$. Наименьшее из целых положительных чисел m, для которых σ^m равно тождественной подстановке, называется *порядком* подстановки σ [8].

Используя приведенные выше определения, можно переформулировать условие предполноты по суперпозиции для классов самодвойственных функций: класс S_σ является предполным по суперпозиции тогда и только тогда, когда σ имеет простой порядок и не имеет неподвижных точек.

Основным результатом настоящей работы является следующая

Теорема. *Пусть σ — подстановка на множестве E_k. Тогда класс S_σ неявно предполон в P_k тогда и только тогда, когда σ имеет простой порядок, и число ее неподвижных точек отлично от единицы.*

Работа выполнена при поддержке гранта РФФИ № 18–01–00337 «Проблемы синтеза, сложности и надежности в теории управляющих систем».

Список литературы

1. Кузнецов А. В. О средствах для обнаружения невыводимости или невыразимости // Логический вывод. — М.: Наука, 1979. — С. 5–33.

2. Касим-Заде О. М. О неявной выразимости булевых функций //

Вестник Московского университета. Серия 1. Математика. Механика. — 1995. — № 2. — С. 44–49.

3. Касим-Заде О. М. О неявной полноте в k-значной логике // Вестник Московского университета. Серия 1. Математика. Механика. — 2007. — № 3. — С. 9–13.

4. Орехова Е. А. Об одном критерии неявной полноты в трехзначной логике // Математические вопросы кибернетики. — М.: Физматлит, 2003. — Вып. 12. — С. 27–74.

5 Касим-Заде О. М. О неявной выразимости в двузначной логике и криптоизоморфизмах двухэлементных алгебр — Доклады РАН. — 1996. — Т. 348, № 3. — С. 299–301.

6. Старостин М. В. Неявно предполные классы и критерий неявной полноты в трехзначной логике // Вестник Московского университета. Серия 1. Математика. Механика. — 2018. — № 2. — С. 56–59.

7. Яблонский С. В. Функциональные построения в k-значной логике // Сборник статей по математической логике и ее приложениям к некоторым вопросам кибернетики. — М.: Изд-во АН СССР, 1958.

8. Ван-дер-Варден Б. Л. Алгебра. — М.: Мир, 1976.

КВАЗИУНИВЕРСАЛЬНЫЙ ИНИЦИАЛЬНЫЙ БУЛЕВ АВТОМАТ С 4 КОНСТАНТНЫМИ СОСТОЯНИЯМИ

Л. Н. Сысоева (Москва)

Пусть $P_2(n)$ — множество всех булевых функций, зависящих от фиксированных переменных $x_1, x_2, \ldots, x_n$, $n \geq 1$. Под *булевым автоматом* будем понимать автомат $V = (\{0,1\}, \{0,1\}, Q, F, G)$ с произвольным числом входов, входным алфавитом $\{0,1\}$, выходным алфавитом $\{0,1\}$, алфавитом состояний Q, функцией перехода G и функцией выхода F. Определения автомата и инициального автомата можно найти в [1, 2]. Пусть n — число входов автомата V. Без ограничения общности будем полагать, что входы автомата V занумерованы от 1 до n и на i-й вход автомата V подается значение булевой переменной x_i. Тем самым можно считать, что в каждый момент времени на входы автомата V подается некоторый двоичный набор значений переменных $x_1, x_2, \ldots, x_n$ и для любого состояния $q \in Q$ функция выхода $F(q, x_1, x_2, \ldots, x_n)$ является булевой

функцией от переменных $x_1, x_2, \ldots, x_n$. Булев автомат V будем называть *булевым автоматом с константными состояниями*, если для любого $q \in Q$ функция $F(q, x_1, x_2, \ldots, x_n)$ является константной булевой функцией 0 или 1.

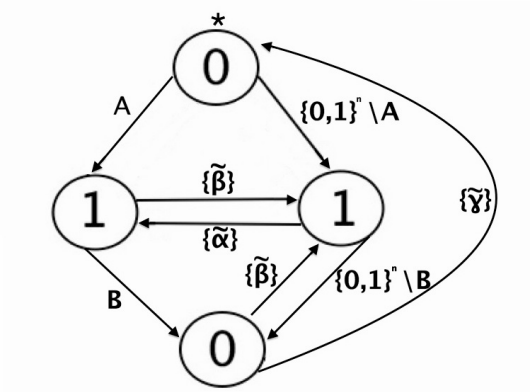
Пусть $V_{q_1} = (\{0,1\}, \{0,1\}, Q, F, G, q_1)$ — инициальный булев автомат с начальным состоянием q_1 и n входами. Пусть $C = (\widetilde{\beta}_1, \widetilde{\beta}_2, \ldots, \widetilde{\beta}_{2^n})$ — упорядоченная последовательность всех двоичных наборов длины n, $n \geq 1$. Будем говорить, что *автомат V_{q_1} с последовательностью C реализует булеву функцию* $f(x_1, x_2, \ldots, x_n)$, если при последовательной подаче на входы автомата V_{q_1} наборов из C в каждый момент $t = 1, 2, \ldots, 2^n$ на выходе автомата V_{q_1} выдается значение $f(\widetilde{\beta}_t)$. Будем также говорить, что *функция f реализуется автоматом V_{q_1}*, если для некоторой последовательности наборов C автомат V_{q_1} с последовательностью C реализует f.

Множество всех инициальных булевых автоматов с k константными состояниями и n входами обозначим через $\mathfrak{V}_k(n)$. Обозначим через $p_k(n)$ максимальную мощность множества булевых функций из $P_2(n)$, реализуемых автоматом из $\mathfrak{V}_k(n)$. Автоматы из $\mathfrak{V}_k(n)$, реализующие $p_k(n)$ функций, называются квазиуниверсальными. В работах [3, 4] автором были получены точные значения $p_2(n) = \frac{5}{8} \cdot 2^{2^n}$, при $n \geq 1$, и $p_3(n) = 2^{2^n} - 2^n$, при $n \geq 6$, и описаны все квазиуниверсальные инициальные булевы автоматы с 2 и 3 константными состояниями при $n > 9$. В работе [5], была получена верхняя оценка на $p_k(n)$ для произвольного k и доказано, что она достигается при $k = 2^n + 2$, где $n \geq 1$.

В данной работе описан инициальный булев автомат с минимальным количеством константных состояний, реализующий максимально возможное число различных булевых функций. А именно, построен инициальный булев автомат с 4 константными состояниями, реализующий все булевы функции из $P_2(n)$ кроме констант.

Пусть A — множество всех булевых наборов длины n с первым нулевым элементом, B — множество всех булевых наборов длины n со вторым нулевым элементом, $\widetilde{\alpha}, \widetilde{\beta}, \widetilde{\gamma}$ — различные наборы, такие, что $\widetilde{\alpha} \in A$, $\widetilde{\beta}, \widetilde{\gamma} \in \{0,1\}^n \backslash A$, $\widetilde{\alpha}, \widetilde{\gamma} \in B$, $\widetilde{\beta} \in \{0,1\}^n \backslash B$. Через V_4 обозначим инициальный булев автомат с четырьмя константными состояниями и диаграммой переходов, изображенной на рисунке, где $A, B, \{\widetilde{\alpha}\}, \{\widetilde{\beta}\}, \{\widetilde{\gamma}\} \subseteq \{0,1\}^n$, $n \geq 3$. В кружочках, обозначающих состояния, написаны символы, соответствующие функции выхода в этом состоянии, а на стрелках — множества всех наборов, при подаче

которых на вход автомата автомат из состояния, из которого идет стрелка, переходит в состояние, на которое указывает стрелка. Если подается набор, не указанный на диаграмме, то автомат остается в том же состоянии, в котором он находился в предыдущий момент времени. Звездочкой помечено начальное состояние автомата.



Теорема. *Для любого $n \geq 3$ инициальный булев автомат V_4 может реализовать любую булеву функцию от n переменных отличную от константы.*

Для доказательства теоремы рассматриваются всевозможные значения, которые функция f из $P_2(n)$ может принимать на наборах $\widetilde{\alpha}, \widetilde{\beta}$ и $\widetilde{\gamma}$. Для каждой функции f из $P_2(n)$, кроме констант, строится последовательность C всех двоичных наборов длины n, такая, что автомат V_4 с последовательностью C реализует f.

Автор выражает искреннюю признательность Р. М. Колпакову и О. С. Дудаковой за постановку задачи и обсуждение результатов работы.

На момент написания данных тезисов автор является сотрудником национального исследовательского университета «Высшая школа экономики».

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2006.

2. Конспект лекций О. Б. Лупанова по курсу «Введение в математическую логику» // Отв. ред. А. Б. Угольников. — М.: Изд-во ЦПИ при механико-математическом факультете МГУ имени М. В. Ломоносова, 2007.

3. Сысоева Л. Н. Максимальное число булевых функций, реализуемых инициальным булевым автоматом с двумя константными состояниями // Вестник Московского университета. Сер. 1. Математика. Механика. — 2016. — вып. 4. — С. 12–17.

4. Сысоева Л. Н. Оценки числа булевых функций, реализуемых инициальным булевым автоматом с тремя константными состояниями // Вестник Московского университета. Сер. 1. Математика. Механика. — 2017. — вып. 2. — С. 19–28.

5. Сысоева Л. Н. Квазиуниверсальные инициальные булевы автоматы с константными состояниями // Материалы XII Международного семинара "Дискретная математика и её приложения"имени академика О. Б. Лупанова (20–25 июня 2016 г.) — М.: Изд-во механико-математического факультета МГУ, 2016. — С. 229-232.

ГРУППА АВТОТОПИЙ СИЛЬНО ЗАВИСИМЫХ n-АРНЫХ ПОЛУГРУПП

А. В. Черемушкин (Москва)

Напомним, что *моноидом* называется бинарная полугруппа с единицей. При $n = 2$ каждая бинарная полугруппа $(X, *)$ с сильно зависимой операцией $*$ является моноидом ([1], стр. 57). При $n \geq 3$ непустое конечное множество X с заданной на нем n-арной операцией f, называется n-арной *полугруппой* (n-*полугруппой*), если при всех $1 \leq i < j \leq n$ выполняются тождества $\{i, j\}$-ассоциативности

$$f(x_1, \ldots, x_{i-1}, f(x_i, \ldots, x_{i+n-1}), x_{i+n}, \ldots, x_{2n-1}) = \\ = f(x_1, \ldots, x_{j-1}, f(x_j, \ldots, x_{j+n-1}), x_{j+n}, \ldots, x_{2n-1}),$$

$x_1, \ldots, x_n \in X$. Если при этом n-полугруппа является n-квазигруппой, то она называется n-*группой*. Строение произвольной n-группы впервые описано в Э. Постом в терминах т. н. обертывающей группы. В случае сильно зависимых n-арных полугрупп можно получить аналогичное описание.

Определение. Назовем моноид $G = (\hat{X}, \circ)$ *обертывающим* для n-арной полугруппы (X, f) с сильно зависимой операцией f, если $X \subset \hat{X}$, множество X порождает моноид G, а n-арная операция f связана с бинарой операцией в моноиде G равенством:

$$f(x_1, x_2, \ldots, x_n) = x_1 \circ x_2 \circ \ldots \circ x_n, \quad x_1, x_2, \ldots, x_n \in X.$$

Теорема 1. *Пусть $n \geq 3$. Для конечной n-арной полугруппы (X, f) с сильно зависимой операцией f найдется обертывающий моноид $G = (\hat{X}, \circ)$ такой, что при некотором обратимом элементе $a \in X$ множеству $X_0 = X \circ a^{-1}$ соответствует подмоноид $H = (X_0, \circ)$, удовлетворяющий условиям $G =< X >$, $a \circ X_0 \circ a^{-1} = X_0$ и $|\hat{X}| \mid |X_0| \cdot (n-1)$.*

Другой способ описания строения таких полугрупп, аналогичный теореме Л. М. Глускина и М. Хоссу, получен в [2].

Теорема 2. *Если f — асоциативная сильно зависимая n-арная операция на конечном множестве X, то для некоторого моноида $(X, *)$, обратимого элемента a и автоморфизма θ этого моноида таких, что $\theta^{n-1}(x) = a * x * a^{-1}$, $\theta(a) = a$, $x_i \in X$, $i = 1, \ldots, n$, справедливо тождество*

$$f(x_1, \ldots, x_n) = x_1 * \theta(x_2) * \theta^2(x_3) * \ldots * \theta^{n-1}(x_n) * a.$$

Из этих теорем и общего описания групп автотопий бесповторной суперпозиции сильно зависимых функций из [3, 4] вытекает описание строения их групп автотопий. Для случая n-арных квазигрупп оно было получено в работе [5].

Пусть $G = (X, *)$ — моноид, $b \in G^*$ и $\theta \in \mathrm{Aut}(*)$. Рассмотрим операции $f_*(x_1, \ldots, x_n) = x_1 * \cdots * x_n$ и

$$f_{\theta,*}(x_1, \ldots, x_n) = x_1 * \theta(x_2) * \theta^2(x_3) * \ldots * \theta^{n-1}(x_n),$$
$$f_{\theta,*,b}(x_1, \ldots, x_n) = x_1 * \theta(x_2) * \theta^2(x_3) * \ldots * \theta^{n-1}(x_n) * b.$$

Если рассматривать правое действие $\alpha\beta(x) = x^{\alpha\beta} = \beta(\alpha(x))$, то $f_*(x) = f^T_{\theta,*}(x) = f_{\theta,*}(x^{T^{-1}})$, где $T = (id, \theta, \theta^2, \ldots, \theta^{n-1}, id)$ — главная автотопия, и поэтому $\mathrm{Atp}(f_{\theta,*}) = T\mathrm{Atp}(f_*)T^{-1}$.

Группа автотопий операции $f_*(x_1, \ldots, x_n)$ описана в [3]:

Лемма. *Пусть $G = (\Omega, *)$ — моноид и $f_*(x_1, \ldots, x_n) = x_1 * \cdots * x_n$. Тогда* а) *если операция $*$ — неабелева, то группа $\mathrm{Atp}\,(f)$ имеет порядок $|G^*|^{n+1}\,|\mathrm{Aut}\,(G)|$ и состоит из преобразований вида $(\alpha_1, \ldots, \alpha_n, \alpha_{n+1})$, где $\alpha_i(x) = a_i^{-1} * \xi(x) * a_{i+1}$, $i = \overline{1,n}$, $\alpha_{n+1}(x) = a_1^{-1} * \xi(x) * a_{n+1}$, при некоторых $a_1, \ldots, a_{n+1} \in G^*$, $\xi \in \mathrm{Aut}\,(G)$;*

б) *если операция* $*$ *— абелева; то группа* $\mathrm{Atp}\,(f)$ *имеет порядок* $|G^*|^n\,|\mathrm{Aut}\,(G)|$ *и состоит из преобразований вида* $(\alpha_1,\ldots,\alpha_n,\alpha_{n+1})$, *где* $\alpha_i(x)=\xi(x)*a_i$, $i=\overline{1,n}$, $\alpha_{n+1}(x)=\xi(x)*a_1*\cdots*a_n$, *при некоторых* $a_1,\ldots,a_n\in G^*$, $\xi\in\mathrm{Aut}\,(G)$.

Теорема. *Пусть* $*$ *— моноид и* $\theta\in\mathrm{Aut}(*)$.

1. *Если операция* $*$ *неабелева, то группа автотопий операции* $f_{\theta.*}(x_1,\ldots,x_n)=x_1*\theta(x_2)*\theta^2(x_3)*\ldots*\theta^{n-1}(x_n)$ *состоит из таких наборов подстановок* $(\alpha_1,\alpha_2,\ldots,\alpha_n,\alpha_{n+1})$, *что при некоторых обратимых относительно* $*$ *элементов* $a_1,a_2,\ldots,a_{n+1}\in X$ *и* $\xi\in\mathrm{Aut}(*)$ *выполнены равенства*

$$\begin{cases} \alpha_1(x_1)= & a_1^{-1}*\xi(x_1)*a_2,\\ \alpha_2(x_2)= & \theta^{-1}(a_2^{-1}*\xi(\theta(x_2))*a_3),\\ \alpha_3(x_3)= & \theta^{-2}(a_3^{-1}*\xi(\theta^2(x_3)*a_4),\\ \ldots\quad\ldots & \ldots\\ \alpha_{n-1}(x_{n-1})= & \theta^{2-n}(a_{n-1}^{-1}*\xi(\theta^{n-2}(x_{n-1}))*a_n),\\ \alpha_n(x_n)= & \theta^{1-n}(a_n^{-1}*\xi(\theta^{n-1}(x_n))*a_{n+1}),\\ \alpha_{n+1}(y)= & a_1^{-1}*\xi(y)*a_{n+1}. \end{cases}$$

При этом всякий набор подстановок $(\alpha_1,\ldots,\alpha_n,\alpha_{n+1})$ *при произвольных обратимых* $a_1,\ldots,a_{n+1}\in G^*$ *и* $\xi\in\mathrm{Aut}\,(G)$, *удовлетворяющий этим равенствам, является автотопией операции* $f_{\theta.*}$.

2. *Если операция* $*$ *абелева, то группа автотопий операции* $f_{\theta.*}(x_1,\ldots,x_n)$ *состоит из таких наборов подстановок* $(\alpha_1,\alpha_2,\ldots,\alpha_n,\alpha_{n+1})$, *что при некоторых обратимых относительно* $*$ *элементов* $a_1,a_2,\ldots,a_n\in X$ *и* $\xi\in\mathrm{Aut}(*)$ *выполнены равенства*

$$\begin{cases} \alpha_1(x_1)= & a_1^{-1}*\xi(x_1)*a_1,\\ \alpha_2(x_2)= & \theta^{-1}(\xi(\theta(x_2))*a_2),\\ \alpha_3(x_3)= & \theta^{-2}(\xi(\theta^2(x_3)*a_3),\\ \ldots\quad\ldots & \ldots\\ \alpha_{n-1}(x_{n-1})= & \theta^{2-n}(\xi(\theta^{n-2}(x_{n-1}))*a_{n-1}),\\ \alpha_n(x_n)= & \theta^{1-n}(\xi(\theta^{n-1}(x_n))*a_n),\\ \alpha_{n+1}(y)= & \xi(y)*a_1\ldots*a_n. \end{cases}$$

При этом всякий набор подстановок $(\alpha_1,\ldots,\alpha_n)$ *при произвольных обратимых* $a_1,\ldots,a_n\in G^*$ *и* $\xi\in\mathrm{Aut}\,(G)$, *удовлетворяющий этим равенствам, является автотопией операции* $f_{\theta.*}$.

Группы автотопий операции $f_{\theta,*,b}$ описывается с учетом равенства равенства $f_{\theta,*,b}=f^S_{\theta,*}$, где $S=(id,\ldots,id,R_b)$, откуда вытекает

соотношение $\mathrm{Atp}(f_{\theta,*,b}) = S^{-1}\mathrm{Atp}(f_{\theta,*})S$. Поэтому описание группы автотопий функции $f_{\theta,*,b}$ отличается тем, что в приведенной выше теореме надо заменить приведенное там значение подстановки $\alpha_{n+1}(y)$ на $R_b^{-1}\alpha_{n+1}R_b(y) = \alpha_{n+1}(y * b^{-1}) * b$.

Список литературы

1. Bruck R. H. A survey of binary systems. — Berlin – Heidelberg – New York: Springer, 1958.

2. Черемушкин А. В. Аналоги теорем Глускина–Хоссу и Малышева для сильно зависимых n-арных операций // Дискретная математика. — 2018. — Т. 30, вып. 2. — С. 15–24.

3. Черемушкин А. В. Бесповторная декомпозиия сильно зависимых функций. // Дискретная математика. — 2004. — Т. 16, вып. 3. — С. 3–42.

4. Черемушкин А. В. Декомпозиия и классификация дискретных функций: монография. — М.: Курс, 2018.

5. Khodabandeh H., Shahryari M. On the automorphisms and representations of polyadic groups. // Communications in Algebra. — 2012. — v. 40, no. 6. — P. 2199–2212.

ЕДИНСТВЕННОСТЬ ПРЕДЕЛЬНОЙ ТОЧКИ В АЛГЕБРАХ БЕРНУЛЛИЕВСКИХ РАСПРЕДЕЛЕНИЙ

А. Д. Яшунский (Москва)

При исследовании преобразований случайных величин дискретными функциями достаточно естественно возникает понятие алгебры вероятностных распределений — множества распределений, замкнутого относительно преобразований, заключающихся в подстановке случайных величин с соответствующими распределениями в функции из некоторого заданного класса. По-видимому, одним из первых такие алгебры стал рассматривать Ф. И. Салимов [1].

Различные результаты о строении алгебр распределений получены Ф. И. Салимовым и Р. М. Колпаковым, который, в частности, для всех k описал всевозможные алгебры рациональных распределений

на k-элементном множестве, замкнутые относительно преобразования произвольными функциями k-значной логики [2]. Настоящая работа посвящена исследованию некоторых свойств алгебр бернуллиевских распределений с произвольной системой преобразующих булевых операций.

Будем рассматривать бернуллиевские случайные величины, принимающие значения 0 и 1. Распределение такой случайной величины — вектор $(1-p, p)$, где $p \in [0,1]$. Этот вектор однозначно задается компонентой p, поэтому далее, говоря о распределениях бернуллиевских случайных величин, будем отождествлять их с числами из отрезка $[0,1]$.

Пусть $X_1, \ldots, X_n$ — независимые в совокупности бернуллиевские случайные величины с распределениями $p_1, \ldots, p_n$ соответственно, а $f(x_1, \ldots, x_n)$ — булева функция. Тогда $f(X_1, \ldots, X_n)$ — также бернуллиевская случайная величина, и ее распределение может быть выражено как функция $\widehat{f}(p_1, \ldots, p_n)$:

$$\widehat{f}(p_1, \ldots, p_n) = \sum_{\substack{\sigma_1,\ldots,\sigma_n \in \{0,1\} \\ f(\sigma_1,\ldots,\sigma_n)=1}} \pi(p_1, \sigma_1) \cdots \pi(p_n, \sigma_n),$$

где $\pi(p,0) = 1-p$ и $\pi(p,1) = p$. Таким образом каждой булевой функции f сопоставлена функция $\widehat{f}\colon [0,1]^n \to [0,1]$. Если B — множество булевых функций, то положим $\widehat{B} = \{\widehat{f} \mid f \in B\}$. Подмножество $G \subseteq [0,1]$, замкнутое относительно операций из множества $\widehat{B}$, образует *алгебру бернуллиевских распределений* $\langle G, \widehat{B}\rangle$.

Точку $q \in [0,1]$ будем называть *предельной точкой* множества $G \subseteq [0,1]$, если для любого $\varepsilon > 0$ найдется такая точка $g \in G$, что $0 < |g - q| < \varepsilon$. Совокупность предельных точек множества G обозначим через $\lambda(G)$. Отметим, что $\lambda(G)$ не обязательно содержится в множестве G.

Напомним, что переменная x_i булевой функции $f(x_1, \ldots, x_n)$ *несущественная*, если для любых $\alpha_1, \ldots, \alpha_{n-1} \in \{0,1\}$ выполнено $f(\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_i, \ldots, \alpha_{n-1}) = f(\alpha_1, \ldots, \alpha_{i-1}, 1, \alpha_i, \ldots, \alpha_{n-1})$. Введем обозначения для некоторых классов булевых функций, полагая, что вместе с каждой функцией в класс входят все функции, получающиеся в результате переименования переменных или добавления

несущественных переменных. Положим:

$$\begin{aligned} MU &= \{0, 1, x\}, \\ \mathcal{A}(0) &= \{\min(x_1, \ldots, x_n)\}_{n\in\mathbb{N}} \cup \{0, 1\}, \\ \mathcal{A}\left(\tfrac{1}{2}\right) &= \{x_1 + \cdots + x_n + c \bmod 2\}_{c\in\{0,1\}, n\geqslant 0}, \\ \mathcal{A}(1) &= \{\max(x_1, \ldots, x_n)\}_{n\in\mathbb{N}} \cup \{0, 1\}. \end{aligned}$$

Имеет место следующая теорема.

Теорема. *Пусть для алгебры бернуллиевских распределений* $\langle G, \widehat{B}\rangle$ *выполнено* $\lambda(G) = \{q\}$. *Тогда либо* $B \subseteq MU$, *либо* $q \in \left\{0, \frac{1}{2}, 1\right\}$ *и* $B \subseteq \mathcal{A}(q)$.

Таким образом, показано, что возникновение алгебр с единственной предельной точкой (отметим, что именно подобные системы часто составляют объект исследований классической теории вероятностей), ограничено узким набором классов преобразующих функций, достаточно «слабых» с точки зрения своих выразительных возможностей. Полученные результаты дополняют полученную автором ранее характеризацию конечных алгебр бернуллиевских распределений [3].

Список литературы

1. Салимов Ф. И. Об одной системе образующих для алгебр над случайными величинами // Известия вузов. Математика. — 1981. — № 5. — С. 78–82.

2. Колпаков Р. М. Замкнутые классы конечных распределений рациональных вероятностей // Дискретный анализ и исследование операций. Сер. 1. — 2004. — Т. 11, № 3. — С. 16–31.

3. Яшунский А. Д. Конечные алгебры бернуллиевских распределений // Дискретная математика. — 2018. — Т. 30, вып. 2. — С. 148–161.