МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
им. М. В. ЛОМОНОСОВА
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
МАТЕМАТИКИ И МЕХАНИКИ им. акад. В. И. СМИРНОВА

МАТЕРИАЛЫ XVI МЕЖДУНАРОДНОЙ ШКОЛЫ-СЕМИНАРА

«СИНТЕЗ И СЛОЖНОСТЬ УПРАВЛЯЮЩИХ СИСТЕМ»

(Санкт-Петербург, 26–30 июня 2006 г.)

Издательство механико-математического факультета МГУ

Москва 2006

М34
УДК 519.7

Издание осуществлено при поддержке Российского фонда фундаментальных исследований по проекту 06–01–10068

М34 Материалы XVI Международной школы-семинара «Синтез и сложность управляющих систем» (Санкт-Петербург, 26–30 июня 2006 г.) / Под редакцией О. Б. Лупанова. — М.: Изд-во механико-математического факультета МГУ, 2006. — 159 с.

Сборник содержит материалы XVI Международной школы-семинара «Синтез и сложность управляющих систем», проходившей в Санкт-Петербурге с 26 по 30 июня 2006 г. при поддержке Российского фонда фундаментальных исследований (проект 06–01–10068). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание

МАТЕРИАЛЫ
XVI МЕЖДУНАРОДНОЙ ШКОЛЫ-СЕМИНАРА
«СИНТЕЗ И СЛОЖНОСТЬ УПРАВЛЯЮЩИХ СИСТЕМ»
(Санкт-Петербург, 26–30 июня 2006 г.)

Под общей редакцией О. Б. Лупанова

Редакционная группа:
О. М. Касим-Заде, Т. М. Косовская, Н. К. Косовский, В. В. Кочергин, А. В. Чашкин

Ответственный за выпуск *В. В. Кочергин*

Н/К
ИД №04059 от 20.02.2001 Подписано к печати 28.07.2006. Формат 60 × 90/16.
Бумага типогр. №1. Печать РИЗО. Печ. л. 10. Тираж 100 экз.
Издательство механико-математического факультета МГУ. 119992, Москва, Ленинские горы, МГУ.
Отпечатано с оригинал-макета в типографии ООО «Объектив», Москва

СОДЕРЖАНИЕ

С. И. Аксенов О надежности схем над произвольной полной системой при инверсных неисправностях на выходах элементов 5
М. А. Алехина О функциях и схемах, корректирующих ошибки 8
А. С. Балюк, С. В. Балюк Вычислительная реализация алгоритмов минимизации термальных представлений булевых функций небольшой размерности в бинарных и тернарных базисах 12
Л. Н. Бондаренко Применение «метода вронскианов» для решения комбинаторных задач 17
Я. В. Вегнер Сложность вычисления экспоненты методом Карацубы 22
С. Ф. Винокуров Об операторной классификации булевых функций 27
А. С. Герасимов Программная реализация поиска доказательств в бесконечнозначной предикатной логике, основанной на линейных неравенствах 30
О. С. Дудакова О конечной порожденности некоторых семейств предполных классов монотонных функций k-значной логики 35
Р. Н. Забалуев О средней глубине монотонных функций 38
М. А. Иорданский Индуктивное описание класса планарных графов 41
А. С. Казимиров Число классов булевых функций, порожденных операторными отображениями 44
Н. К. Косовский Нижняя оценка длины записи интерпретатора n-программ 48
Н. К. Косовский, Фам Тхань Лам Оценка памяти, необходимой для исключения бесконечного зацикливания в Паскаль-программах, выполняемых на компьютере 53
В. В. Кочергин О сложности совместного вычисления двух элементов свободной абелевой группы 54
С. Г. Курносова Решение задачи нахождения всех T-неприводимых расширений для симметричных ориентаций цепей 59
Ю. М. Лифшиц Обработка сжатых текстов 64
С. А. Ложкин, О. Б. Седелев О реализации функций алгебры логики BDD, вложенными в единичный куб 68
С. А. Ложкин, М. С. Шуплецов Асимптотические оценки высокой степени точности для сложности предикатных схем из одного класса 72
Ю. В. Мерекин Об одной форме представления рекуррентных схем порождения слов и их аддитивная сложность 77
Е. В. Михайлец О ранге неявных представлений функций k-значной логики над классом монотонных функций 78
Е. А. Окольнишникова Об одном классе схем 83

Т. Г. Петросян Размер максимального множества, свободного от произведений в группах порядка pq 85
В. Н. Потапов О полностью коммутативно разделимых n-квазигруппах 88
Д. С. Романов, А. Е. Казачёк Об оценках функций Шеннона длин локальных тестов относительно слипаний 91
В. С. Рублев, Д. В. Чехранов Алгебра объектных операций системы управления данными DIM 97
И. С. Сергеев О реализации некоторых операций конечных полей характеристики 2 схемами логарифмической глубины 101
С. В. Сидоров О подобии матриц третьего порядка над кольцом целых чисел 103
Р. В. Хелемендик О единой формальной записи всех допустимых ходов в любой шахматной позиции 108
А. В. Чашкин О вложении графов в решетки ограниченной высоты 113
А. Н. Черепов Оценки сложности приближения непрерывных функций некоторых классов детерминированными функциями с задержкой 118
В. В. Чугунова Об асимптотически наилучших по надежности схемах в базисах $\{\to, \oplus\}$ и $\{\not\to, \sim\}$ при инверсных неисправностях на входах элементов 122
В. В. Чумаков, В. Н. Шевченко Вершины целочисленных многогранников и решение крамеровских систем 127
В. И. Шевченко О сложности тестирования перепутываний в схемах 131
В. Н. Шевченко Триангуляции выпуклых многранников и их булевы функции 135
Л. А. Шоломов О последовательной реализации частичных булевых функций 142
В. Л. Щербина, В. А. Захаров О сложности распознавания эквивалентности машин Тьюринга без записи на ленту 147
А. Д. Яшунский О преобразованиях вероятности бесповторными булевыми формулами 150
Информация 156

О НАДЕЖНОСТИ СХЕМ НАД ПРОИЗВОЛЬНОЙ ПОЛНОЙ СИСТЕМОЙ ПРИ ИНВЕРСНЫХ НЕИСПРАВНОСТЯХ НА ВЫХОДАХ ЭЛЕМЕНТОВ

С. И. Аксенов (Пенза)

Впервые задачу синтеза надежных схем из ненадежных элементов рассматривал Дж. фон Нейман [1]. Он предполагал, что все элементы схемы независимо друг от друга подвержены с вероятностью ε инверсным неисправностям, когда функциональный элемент (ф. э.) с приписанной ему булевой функцией φ в неисправном состоянии реализует функцию $\bar{\varphi}$. Дж. фон Нейман предложил итерационный метод, позволяющий при $\varepsilon < 1/6$ произвольную булеву функцию реализовать схемой, вероятность ошибки на выходе которой при любом входном наборе значений переменных асимптотически не превосходит ε при условии, что в рассматриваемом базисе содержится медиана $m(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$.

Как и Дж. фон Нейман предполагаем, что все элементы схемы независимо друг от друга с вероятностью ε подвержены инверсным неисправностям на выходах элементов. Пусть схема S реализует булеву функцию $f(\tilde{x})$ ($\tilde{x} = (x_1, \ldots, x_n)$) при отсутствии неисправностей в схеме. Обозначим $P_{\overline{f}(\tilde{a})}(S, \tilde{a})$ — вероятность того, что схема S при $\tilde{x} = \tilde{a}$ выдает значение $\overline{f}(\tilde{a})$. Будем считать, что схема S реализует функцию $f(\tilde{a})$ с ненадежностью $P(S)$, если $P(S) = \max\limits_{\tilde{a}} P_{\overline{f}(\tilde{a})}(S, \tilde{a})$, где максимум берется по всем входным наборам $\tilde{a}$. Надежность схемы S равна $1 - P(S)$. Определим сложность схемы $L(S)$ как количество ф. э. в ней.

С. И. Ортюков [2] и Д. Улиг [3] получили следующий результат: при $\varepsilon \le \varepsilon_0$ для любых p, $p > q(\varepsilon)L_m$, где $q(\varepsilon) = \varepsilon + 3\varepsilon^2 + o(\varepsilon^2)$, L_m — минимальное число элементов, необходимое для реализации медианы в рассматриваемом базисе, любую булеву функцию f можно реализовать схемой S с ненадежностью $P(S) \le p$. Если выбрать $p \sim L_m\varepsilon$, то $P(S) \lesssim L_m\varepsilon$.

М. А. Алехина [4] рассмотрела базис $\{x|y\}$ (штрих Шеффера). Для "почти всех" функций построены асимптотически наилучшие по надежности схемы, которые функционируют с ненадежностью $P(S) \sim 3\varepsilon$.

Будем рассматривать реализацию булевых функций надежными схемами над произвольной полной в P_2 системой функций, в которой может и не содержаться медиана. Справедлива следующая теорема [5].

Теорема 1. *Пусть Ω — полная в P_2 система функций, тогда существуют константы ε_0 и c такие, что при $\varepsilon \le \varepsilon_0$ любую функцию $f \in P_2$ можно реализовать схемой S над Ω, для котор ой верно $P(S) \le 5\varepsilon + c\varepsilon^2$.*

То есть по сравнению с результатом С. И. Ортюкова и Д. Улига $P(S) \lesssim L_m\varepsilon$ получена более определенная оценка: $P(S) \lesssim 5\varepsilon$. Полное доказательство этой теоремы приведено в [5]. Ниже сформулируем без доказательства леммы 1-6, на которые опирается доказательство теоремы.

Введем классы функций G_1, G_2 и G_3:

$$G_1 = \{g_1 \in P_2 : g_1(x_1, x_2, x_3) = x_1^{\sigma_1}x_2^{\sigma_2} \vee x_1^{\sigma_1}x_3^{\sigma_3} \vee x_2^{\sigma_2}x_3^{\sigma_3}\},$$

$$G_2 = \{g_2 \in P_2 : g_2(x_1, x_2, x_3, x_4) = x_1^{\sigma_1}x_2^{\sigma_2} \vee x_3^{\sigma_3}x_4^{\sigma_4}\},$$

$$G_3 = \{g_3 \in P_2 : g_3(x_1, x_2, x_3, x_4) = (x_1^{\sigma_1} \vee x_2^{\sigma_2}) \cdot (x_3^{\sigma_3} \vee x_4^{\sigma_4})\},$$

где $\sigma_i \in \{0, 1\}$, $i = 1, 2, 3, 4$. Объединение этих классов обозначим G, т. е. $G = G_1 \cup G_2 \cup G_3$. Класс G_1 содержит 8 функций, G_2 и G_3 — по 16 функций, G — 40 функций.

Лемма 1. *Пусть функции f и $\bar{f}$ реализованы схемами из ф. э. над некоторой полной в P_2 системой функций Ω с ненадежностью не более p; пусть $g \in G$, а S_g — схема над Ω, ее реализующая с числом элементов $L(S_g)$, тогда существует схема S, реализующая функцию f над Ω с ненадежностью $P(S) \le L(S_g) \cdot \varepsilon + 6p^2$.*

Обозначим, как и в [6], T_0 — класс функций, сохраняющих константу 0; T_1 — класс функций, сохраняющих константу 1; L — класс линейных функций; M — класс монотонных функций.

Леммы 2–4 касаются некоторых свойств функций из классов T_0, T_1, L и M.

Лемма 2. *Пусть $f_0(x_1, \ldots, x_k) \notin T_0$, $f_1(x_1, \ldots, x_m) \notin T_1$. Тогда либо $\bar{x} \in \{\varphi_0(x), \varphi_1(x)\}$, либо $\varphi_0(x) \equiv 1$, $\varphi_1(x) \equiv 0$.*

Лемма 3. *Из любой нелинейной функции $f_l(x_1, \ldots, x_n)$ путем подстановки переменных можно получить нелинейную функцию $\varphi_l(x_1, x_2, x_3)$, имеющая вид либо*

$$\varphi_l(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_0,$$

либо

$$\varphi_l(x_1, x_2, x_3) = x_1x_2 \oplus a_1x_1 \oplus a_2x_2 \oplus a_0,$$

если x_3 фиктивна.

Лемма 4. *Из любой немонотонной функции $f_m(x_1, \ldots, x_n)$ путем подстановки переменных можно получить немонотонную*

функцию $\varphi_m(x_1, x_2, x_3)$, где переменные x_2, x_3 могут быть фиктивны.

Основной вспомогательный результат сформулирован в лемме 5.

Лемма 5. *Пусть Ω — полная в P_2 система функций, тогда существует схема S, $L(S) \le 5$, реализующая функцию из класса G над Ω.*

При доказательстве леммы 5 использовался тот факт, что в силу полноты Ω в ней содержится функции $f_0 \notin T_0$, $f_1 \notin T_1$, $f_l \notin L$, $f_m \notin M$. Из функций f_0, f_1, f_l, f_m получаем, соответственно, функции $\varphi_0(x)$, $\varphi_1(x)$, $\varphi_l(x_1, x_2, x_3)$ и $\varphi_m(x_1, x_2, x_3)$ (см. леммы 2-4). Далее для каждого возможного варианта четверки функций φ_0, φ_1, φ_l, φ_m строим схему S_g, реализующую функцию $g \in G$. В результате получаем, что во всех перебираемых случаях $L(S_g) \le 5$.

Лемма 6. *Пусть Ω — полная в P_2 система функций, тогда функцию $x|y$ (штрих Шеффера) можно реализовать схемой S над Ω, причем $L(S) \le 6$.*

Замечание 1. В [7] доказано, что для $\varepsilon \le \varepsilon_0$, где $\varepsilon_0 = 1/(600k)$, любую булеву функцию можно реализовать схемой S с ненадежностью $P(S) \le 7k\varepsilon$, где k — минимальное количество ф. э., необходимое для реализации функции штрих Шеффера $x|y$ над рассматриваемой полной системой. Из леммы 6 следует, что $k \le 6$, т. е. $\varepsilon_0 = 1/3600$, $P(S) \le 42\varepsilon$.

Доказательство теоремы 1. Из лемм 1, 6 и замечания 1 следует, что $\varepsilon_0 = 1/3600$, $c = 6 \cdot 42^2$, а, учитывая лемму 5, окончательно получаем утверждение теоремы 1.

Список литературы

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

2. Ортюков С. И. Об избыточности реализации булевых функций схемами из ненадежных элементов // Труды семинара по дискретной математике и ее приложениям (Москва, 27–29 января 1987 г.). — М.: МГУ, 1989. — С. 166–168.

3. Uhlig D. Reliable networks from unreliable gates with almost minimal complexity // Lecture Notes in Comput. Sci. (Fundamentals of computation theory. Intern. conf. FCT'87. Proc.) — Berlin: Springer-Verl., 1987. — V. 278. — P. 462–469.

4. Алехина М. А. О надежности и сложности схем в базисе $\{x|y\}$ при инверсных неисправностях элементов // Дискретный анализ и исслед. операций. Сер. 1. — 2005. — Т. 12, № 2. — С. 3–11.

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

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

7. Алехина М. А. Синтез и сложность надежных систем из ненадежных элементов // Мат. вопросы кибернетики. — М.: Физматлит, 2002. — Вып. 11. — С. 193–218.

О ФУНКЦИЯХ И СХЕМАХ, КОРРЕКТИРУЮЩИХ ОШИБКИ

М. А. Алехина (Пенза)

Впервые задачу синтеза надежных схем из ненадежных элементов рассматривал Дж. фон Нейман [1]. Он предполагал, что все элементы схемы независимо друг от друга с вероятностью ε ($\varepsilon < 1/2$) подвержены инверсным неисправностям на выходах, когда функциональный элемент с приписанной ему булевой функцией $e(\tilde{x})$ в неисправном состоянии реализует $\bar{e}(\tilde{x})$. Для повышения надежности схем Дж. фон Нейман использовал схему, реализующую функцию голосования (медиану) $g_1(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$. Позднее задача реализации булевых функций надежными схемами при однотипных константных неисправностях элементов решалась автором, а для повышения надежности применялись схемы, реализующие как медиану $g_1(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$, так и функции $g_2(x_1, x_2, x_3, x_4) = x_1x_2 \vee x_3x_4$ и $g_3(x_1, x_2, x_3) = (x_1 \vee x_2)\&(x_3 \vee x_4)$. Аксенов [2] расширил множество функций, корректирующих ошибки. Он ввел три класса функций $G_1 = \{x_1^{a_1}x_2^{a_2} \vee x_1^{a_1}x_3^{a_3} \vee x_2^{a_2}x_3^{a_3}\}$, $G_2 = \{x_1^{a_1}x_2^{a_2} \vee x_3^{a_3}x_4^{a_4}\}$, $G_3 = \{(x_1^{a_1} \vee x_2^{a_2})\&(x_3^{a_3} \vee x_4^{a_4})\}$ ($a_i \in \{0, 1\}$, $i = 1, 2, 3, 4$) и показал, что при инверсных неисправностях на выходах элементов наличие любой из функций множества $G = G_1 \cup G_2 \cup G_3$ ($|G| = 40$) в заданном полном множестве $Б$ гарантирует реализацию произвольной булевой функции схемой, функционирующей с вероятностью ошибки не больше $\varepsilon + c\varepsilon^2$, где $\varepsilon \le d$, c, d – некоторые положительные константы.

Оказалось, что наличие и некоторых других функций в базисе дает такой же результат. Опишим эти функции.

1. О функциях, корректирующих ошибки

Пусть булева функция $m(x_1,...,x_k)$ существенно зависит от k ($k \geq 3$) переменных и обладает свойством: найдется такой набор $(b_1,...,b_k)$, что на нем и всех соседних с ним наборах функция m принимает значение 0, а на наборе $(\bar{b}_1,...,\bar{b}_k)$ и всех соседних с ним наборах — значение 1. Наборы $(b_1,...,b_k)$ и $(\bar{b}_1,...,\bar{b}_k)$ будем называть характеристическими наборами функции $m(x_1,...,x_k)$. Обозначим M_k — множество всех функций $m(x_1,...,x_k)$ с названным свойством.

Нетрудно проверить, что $2^{2^k-2k-1} \leq |M_k| \leq 2^{2^k-k-2}$. Заметим также, что:

1) множество M_3 есть множество G_1, рассмотренное Аксеновым;

2) множество M_4 содержит множество $G_2 \cup G_3$ и $|M_4| = 992$;

3) $|M_3 \cup M_4| = 1000$.

Рассмотрим реализацию булевых функций схемами из ненадежных элементов над полным множеством *Б* [3]. Схема из ненадежных функциональных элементов реализует булеву функцию $f(x_1,\ldots,x_n)$, если при поступлении на входы схемы двоичного набора $\tilde{a} = (a_1,\ldots,a_n)$ при отсутствии неисправностей на выходе схемы появляется значение $f(\tilde{a})$. Предполагается, что все элементы схемы независимо друг от друга переходят в неисправные состояния.

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

Теорема 1. *Пусть $f(x_1,...,x_n)$ — произвольная булева функция, а S — схема, ее реализующая с ненадежностью $P(S) \leq p$. Пусть схема S_m реализует функцию $m(x_1,...,x_k) \in M_k$ и $P(S_m) \leq p$. Обозначим v^1 и v^0 — вероятности ошибок схемы S_m на характеристических наборах. Тогда функцию f можно реализовать такой схемой A, что $P(A) \leq \max\{v^0, v^1\} + cp^2$, где положительная константа $c \leq kC_k^{[k/2]}$.*

Доказательство. Пусть $(b_1,...,b_k)$ — характеристический набор функции $m(x_1,...,x_k)$ такой, что $m(b_1,...,b_k) = 0$. Пусть в этом наборе компоненты $b_{i_1},...,b_{i_t}$ равны нулю, а остальные — единице. Возьмем t экземпляров схемы S и $k-t$ экземпляров S', реализующей функцию $\bar{f}$ с ненадежностью $P(S') \leq p$. Соединим i_1-ый,...,i_t-ый входы схемы S_m с выходами схем S, а остальные $k-t$ входов — с

выходами схем S'. Построенная таким образом схема D реализует функцию f. Вычислим вероятности ошибок на выходе схемы D.

Пусть входной набор $\tilde{a}$ схемы S является нулевым для функции f, т. е. $f(\tilde{a}) = 0$. Вероятность ошибки $P_1(D,\tilde{a})$ на выходе схемы D в этом случае удовлетворяет неравенству $P_1(D,\tilde{a}) \leq v^1 + kpP(S_m) + (k-1)C_k^{[k/2]}p^2$. Но $P(S_m) \leq p$, поэтому $P_1(D,\tilde{a}) \leq v^1 + kp^2 + (k-1)C_k^{[k/2]}p^2 \leq v^1 + kC_k^{[k/2]}p^2$.

Пусть входной набор $\tilde{a}$ схемы S является единичным для функции f, т. е. $f(\tilde{a}) = 1$. Вероятность ошибки $P_0(D,\tilde{a})$ на выходе схемы D в этом случае удовлетворяет неравенству $P_0(D,\tilde{a}) \leq v^0 + kpP(S_m) + (k-1)C_k^{[k/2]}p^2$. Но $P(S_m) \leq p$, поэтому $P_0(D,\tilde{a}) \leq v^0 + kp^2 + (k-1)C_k^{[k/2]}p^2 \leq v^0 + kC_k^{[k/2]}p^2$.

Следовательно, $P(D,\tilde{a}) \leq \max\{v^0, v^1\} + cp^2$, где $c = kC_k^{[k/2]}$. Схема D — искомая.

Теорема 1 доказана.

Следствие 1. *Пусть полное множество Б содержит функцию $m(x_1,...,x_k) \in M_k$, а функциональные элементы с вероятностью ε подвержены инверсным неисправностям на выходах. Пусть f — произвольная булева функция, а S — схема, ее реализующая с ненадежностью $P(S) \leq s\varepsilon$ (s — положительная константа). Тогда функцию f можно реализовать такой схемой A над Б, что $P(A) \leq \varepsilon + c\varepsilon^2$ (положительная константа $c \leq kC_k^{[k/2]}s^2$).*

Доказательство следует из равенств $v^1 = v^0 = \varepsilon$ и теоремы 1.

2. О надежности схем при однотипных константных неисправностях на выходах элементов

В этом разделе будем считать, что все элементы схемы независимо друг от друга подвержены неисправностям типа 0 на выходах. Эти неисправности характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию, а в неисправном, в которое переходит с вероятностью γ ($\gamma < 1/2$), — константу 0.

Теорема 2. *Пусть полное множество Б содержит функцию $m(x_1,...,x_k) \in M_k$. Тогда найдутся такие положительные константы d и r, что при $\gamma \leq d$ любую булеву функцию можно реализовать схемой A над Б с ненадежностью $P(A) \leq \gamma + r\gamma^2$.*

Доказательство. Пусть S_h — схема над *Б*, которая реализует функцию штрих Шеффера $x/y = \bar{x} \vee \bar{y}$ с ненадежностью μ. Тогда [4] любую булеву функцию можно реализовать такой схемой S, что $P(S) \leq 4\mu$. Предположим, что схема S_h содержит l ($l \geq 1$) элементов,

тогда $\mu \le l\gamma$. Следовательно, при $l\gamma \le 1/160$ (т.е. $\gamma \le 1/160l = d$) произвольную булеву функцию можно реализовать схемой S с ненадежностью $P(S) \le 4\mu \le 4l\gamma$. При неисправностях типа 0 на выходах элементов $v^1 = 0$, $v^0 = \gamma$. Из теоремы 1 следует возможность построения схемы A, реализующей f с ненадежностью $P(A) \le \gamma + c(4l\gamma)^2$, т.е. $r = 16l^2kC_k^{[k/2]}$.

Теорема 2 доказана.

Обозначим $P(f) = \inf P(S)$, где S — схема из ненадежных элементов, реализующая булеву функцию $f(x_1, ..., x_n)$.

Схему A из ненадежных элементов, реализующую булеву функцию $f(x_1, ..., x_n)$, назовем асимптотически оптимальной по надежности, если $P(A) \sim P(f)$ при $\gamma \to 0$, т. е.

$$\lim_{\gamma \to 0} \frac{P(A)}{P(f)} = 1.$$

Обозначим $K(n)$ — множество булевых функций $f(x_1, ..., x_n)$, отличных от функций $x_1, ..., x_n$ и константы 0.

Теорема 3. *Пусть Б — полное множество. Для любой схемы S над Б, реализующей функцию $f \in K(n)$, при $\gamma < 1/2$ верно неравенство $P(S) \ge \gamma$.*

Для доказательства достаточно выделить подсхему из выходного элемента и вычислить вероятность ошибки на любом единичном входном наборе функции f.

Из теоремы 3 следует, что функции из класса $K(n)$ при $\gamma < 1/2$ нельзя реализовать схемами с ненадежностью, меньше γ. Поэтому любая схема, удовлетворяющая условиям теоремы 2 и реализующая булеву функцию $f \in K(n)$, является асимптотически оптимальной по надежности и функционирует с ненадежностью, асимптотически равной γ при $\gamma \to 0$. Число функций $f \in K(n)$ равно $2^{2^n} - n - 1$.

Однако ненадежность схемы, реализующей произвольную функцию, может быть асимптотически равна γ и тогда, когда полное множество $Б$ не содержит функцию из M_k. Т.е. наличие функции из M_k во множестве $Б$ является достаточным условием, по крайней мере, в случае однотипных константных неисправностей на выходах элементов. Об этом свидетельствует теорема 4.

Теорема 4. *Пусть полное множество Б содержит функции $x_1 \& x_2$, $x_1 \oplus x_2$. Тогда найдутся такие положительные константы c и d, что при $\gamma \le d$ любую булеву функцию можно реализовать схемой A над Б с ненадежностью $P(A) \le \gamma + c\gamma^2$.*

Для доказательства достаточно предъявить схему S_m, реализующую медиану $m(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$ с подходящими

вероятностями ошибок. Например, схема S_m из четырех элементов, построенная по формуле $x_2 \oplus (x_1 \oplus x_2)\&(x_2 \oplus x_3)$ имеет вероятности ошибок на выходе: $P_1(000) = 0$, $P_1(001) = 0$, $P_1(010) \le 3\gamma$, $P_0(011) = \gamma$, $P_1(100) = 0$, $P_0(101) \le 4\gamma$, $P_0(110) = \gamma$, $P_0(111) = \gamma$. Следовательно, $v^1 = 0$, $v^0 = \gamma$. Применяя теорему 2, получим утверждение теоремы 5.

Список литературы

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

2. Аксенов С. И. О надежности схем над произвольной полной системой функций при инверсных неисправностях на выходах элементов // Известия высших учебных заведений. Поволжский регион. Естественные науки. — 2005. — №6 (21). — С. 42–55.

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

4. Алехина М. А. О надежности схем из ненадежных элементов x/y // Материалы XI Межгосударственной школы-семинара "Синтез и сложность управляющих систем" (Нижний Новгород, 20–25 ноября 2000 г.). Ч. 1. — М.: Изд-во центра прикл. исслед. при мех.-мат. ф-те МГУ, 2001. — С. 9–14.

ВЫЧИСЛИТЕЛЬНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМОВ МИНИМИЗАЦИИ ТЕРМАЛЬНЫХ ПРЕДСТАВЛЕНИЙ БУЛЕВЫХ ФУНКЦИЙ НЕБОЛЬШОЙ РАЗМЕРНОСТИ В БИНАРНЫХ И ТЕРНАРНЫХ БАЗИСАХ

А. С. Балюк, С. В. Балюк (Иркутск)

Определения и обозначения. *Булевой функцией* (или просто *функцией*) размерности n называется отображение $f : \{0,1\}^n \to \{0,1\}$.

Терм над множеством булевых функций B определяется следующим образом:

1) переменные $x_1, \ldots, x_i, \ldots$ являются термами;

2) если $0 \in B$, то 0 — терм, если $1 \in B$, то 1 — терм;

3) если $\Phi_1, \ldots, \Phi_m$ — термы, и g — имя m-местной функции из B, то выражение $g(\Phi_1, \ldots, \Phi_m)$ является термом.

Для упрощения, вхождения в термы двухместных функций будем записывать в инфиксной нотации, например, $x_1 \vee x_2$ вместо $\vee(x_1, x_2)$.

Множество всех термов над B будем обозначать $\varphi(B)$. Множество переменных, входящих в терм Φ, будем обозначать $\chi(\Phi)$.

Пусть $\chi(\Phi) \subseteq \{x_1, \ldots, x_n\}$. Тогда значение терма Φ на наборе $\tilde{\sigma} = (\sigma_1, \ldots, \sigma_n)$, $\tilde{\sigma} \in \{0,1\}^n$, обозначается $\Phi(\tilde{\sigma})$ и вычисляется следующим образом:
1) если $\Phi \equiv x_i$, то $\Phi(\tilde{\sigma}) = \sigma_i$;
2) если Φ — имя нульместной функции, то $\Phi(\tilde{\sigma})$ — ее значение;
3) если $\Phi \equiv g(\Phi_1, \ldots, \Phi_m)$, то $\Phi(\tilde{\sigma})$ — это значение функции g на наборе $(\Phi_1(\tilde{\sigma}), \ldots, \Phi_m(\tilde{\sigma}))$.

Будем говорить, что терм Φ *представляет* n-местную функцию f, если $\chi(\Phi) \subseteq \{x_1, \ldots, x_n\}$ и на всех наборах $\tilde{\sigma} \in \{0,1\}^n$ выполняется равенство $\Phi(\tilde{\sigma}) = f(\tilde{\sigma})$. В дальнейшем, запись $f \approx \Phi$ означает, что терм Φ представляет функцию f. Множество термов над B, представляющих функцию f будем обозначать $\varphi_f(B)$.

Сложностью терма Φ будем называть величину $L(\Phi)$, равную числу вхождений переменных в терм Φ. *Сложностью функции* f над множеством функций B называется величина $L_B(f)$, которая определяется как

$$L_B(f) = \begin{cases} \infty, & \text{если } \varphi_f(B) = \emptyset; \\ \min\{L(\Phi) \mid \Phi \in \varphi_f(B)\}, & \text{иначе.} \end{cases}$$

Функция g размерности n называется *остаточной подфункцией* функции f размерности $n+1$, если найдется $i \in \{1, \ldots, n\}$, и $\tau \in \{0,1\}$, такие что для любого $\tilde{\sigma} \in \{0,1\}^n$ выполняется равенство

$$g(\sigma_1, \ldots, \sigma_n) = f(\sigma_1, \ldots, \sigma_{i-1}, \tau, \sigma_i, \ldots, \sigma_n).$$

Две n-местные функции f и g называются *обобщенно однотипными*, если существует перестановка $(i_1, \ldots, i_n)$ и набор $\tilde{\tau} \in \{0,1\}^{n+1}$, такие что для любого набора $\tilde{\sigma} \in \{0,1\}^n$ выполняется равенство

$$f(\sigma_1, \ldots, \sigma_n) = \tau_{n+1} \oplus g(\sigma_{i_1} \oplus \tau_1, \ldots, \sigma_{i_n} \oplus \tau_n).$$

Множество функций B называется *полным* (или *базисом*), если любую булеву функцию можно представить термом над B. Базис B называется *приведенным*, если выполняются следующие условия:
1) B содержит все остаточные подфункции для каждой ненульместной функции из B;

2) B содержит все обобщенно однотипные функции для каждой функции из B.

Любому множеству функций B, содержащих хотя бы одну существенную нелинейную функцию размерности не меньше двух, можно поставить в соответствие единственный приведенный базис, замкнув B по отношению обобщенной однотипности и получению остаточных подфункций. Такой базис будем обозначать $B^\star$.

Класс всех приведенных базисов, не содержащих двухместную линейную функцию $x_1 \oplus x_2$, обозначим NL. Класс NL_k является подклассом NL, каждый базис которого не содержит функций размерности выше k. Очевидно, что $NL_2 \subset NL_3 \subset \cdots \subset NL$.

Из работ Стеценко [1] и Черухина [2] следует, что NL_3 состоит из восьми базисов:

$$\begin{array}{llll} B_{000} = \{\vee\}^\star, & B_{001} = \{d\}^\star, & B_{010} = \{p\}^\star, & B_{011} = \{d, p\}^\star, \\ B_{100} = \{z\}^\star & B_{101} = \{d, z\}^\star, & B_{110} = \{p, z\}^\star, & B_{111} = \{d, p, z\}^\star, \end{array}$$

где $d \approx x_1x_2 \vee x_1x_3 \vee x_2x_3$, $p \approx x_1x_2x_3 \vee \bar{x}_1\bar{x}_2\bar{x}_3$, $z \approx x_1x_2 \vee \bar{x}_1x_3$.

Постановка задачи. Задача минимизации ставится следующим образом: для заданного полного множества B и заданной булевой функции f построить над B терм Φ, представляющий f, так чтобы число вхождений переменных в Φ было наименьшим, то есть чтобы выполнялось равенство $L(\Phi) = L_B(f)$.

В данной работе рассматривается минимизация 5-местных функций в любом базисе из NL_3. Заметим, что поскольку каждый базис из NL_3 полный, величина $L_B(f)$ конечна для любой функции f и любого $B \in NL_3$. Кроме того, отношение обобщенной однотипности сохраняет сложность функций, так как все базисы в NL_3 приведенные.

Подход к решению. Для задачи в данной постановке существует алгоритм решения, относящийся к классу алгоритмов “полного перебора”. Как показывает практика, алгоритмы этого класса обычно не пригодны для практического использования. В то же время для этой задачи до сих пор не разработан алгоритм, который не относился бы к классу алгоритмов “полного перебора”. Более того, есть гипотеза, что таких алгоритмов не существует [3].

В данной работе предлагается подход, который позволяет решать задачу за разумное время для булевых функций размерности не более пяти. Подход состоит в следующем:
1) строится база данных, в которой для одной функции из каждого класса эквивалентности по отношению обобщенной однотипности строится минимальный терм;

2) затем, для того чтобы найти минимальный терм для произвольной функции f, в базе данных ищется функция из того же класса эквивалентности, что и f, и представляющий ее терм преобразуется таким образом, чтобы представлять функцию f.

Основное преимущество данного подхода состоит в том, что база данных строится только один раз. Вторая часть данного подхода может быть выполнена за время $P + Q + R$, где P — это время, необходимое для построения представителя класса эквивалетности, Q — это время поиска этого представителя в базе данных и R — время трансформации формулы. Существенным параметром является также размер базы данных S.

Размер базы данных S — это количество классов эквивалентности, которое с точностью до мультипликативной константы можно найти поделив число всех функций на максимальное число функций в одном классе ($2^{n+1} \cdot n!$); значение P получается при применении поиска в неупорядоченном массиве размером $O(2^{n+1} \cdot n!)$; значение Q получается при применении двоичного поиска в базе данных размером S; значение R есть линейная функция от сложности $L_B(f)$, которая есть $O\left(\frac{2^n}{\ln n}\right)$ [4]. Таким образом,

$$P = O(2^{n+1} \cdot n!), \quad Q = O\left(\ln \frac{2^{2^n-1}}{2^n \cdot n!}\right), \quad R = O\left(\frac{2^n}{\ln n}\right).$$

Поскольку рассматриваются пятиместные булевы функции, то $n = 5$ и, например, $2^{n+1} \cdot n! = 7680$. Кроме того, коэффициенты, "спрятанные" в обозначении $O(\cdot)$ не велики, и поэтому на современных компьютерах вычисления могут быть выполнены практически мгновенно.

Построение базы данных. Таким образом, самой трудоемкой частью решения является построение базы данных. Построение базы осуществляется последовательно от термов меньшей сложности к термам большей сложности на основании следующей леммы.

Лемма. *Пусть минимальный терм Φ над приведенным базисом B, представляющий функцию f имеет вид $g(\Phi_1, \ldots, \Phi_m)$, пусть функции $f_1, \ldots, f_n$ такие, что $f_1 \approx \Phi_1, \ldots, f_m \approx \Phi_m$, и пусть f_1° — произвольная обобщенно однотипная с f_1. Тогда найдутся функции $g^\circ, f_2^\circ, \ldots, f_m^\circ$ обобщенно однотипные с функциями $g, f_2, \ldots, f_m$ соответственно, такие что выражение $g^\circ(\Psi_1, \ldots, \Psi_m)$, в котором $\Psi_1, \ldots, \Psi_m$ — минимальные термы над B, представляющие $f_1^\circ, f_2^\circ, \ldots, f_m^\circ$ соответственно, является минимальным термом над B, представляющим функцию f°, обобщенно однотипную с f.*

Эта лемма позволяет ограничить перебор, выбирая в качестве первого аргумента в базисных функциях минимальные термы только представителей классов по отношению обобщенной однотипности.

Другая оптимизация состоит в том, что функции $f_1, \ldots, f_m$, встречающиеся в формулировке леммы, выбираются таким образом, чтобы выполнялась цепочка неравенств $L_B(f_1) \geq \cdots \geq L_B(f_m)$.

Результаты. По описанному методу были проведены вычисления на базе вычислительного сервера Иркутского государственного педагогического университета.

В качестве результатов приведем в таблице оценки длины минимальных термов для самых сложных пятиместных функций и, где возможно, представителей классов, функции из которых имеют наибольшую сложность. В таблице для булевых функций используется векторное задание в шестнадцатеричном виде и обозначения: B — базис из класса NL_3; $L_B(5) = \max\{L_B(f) \mid f : \{0,1\}^5 \to \{0,1\}\}$; $\mu(B)$ — множество представителей всех классов эквивалентности по отношению обобщенной однотипности, со сложностью $L_B(5)$.

B	$L_B(5)$	$\mu(B)$
B_{000}	29	1669E996 16686997 16696997
B_{001}	≥ 26	
B_{010}	21	16696997
B_{100}	≥ 24	
B_{011}	21	16696997

B	$L_B(5)$	$\mu(B)$
B_{101}	24	16686BD6 16686881
	≥ 24	69969669
B_{110}	20	16696997 16686BD6
B_{111}	20	16696997 16686BD6

Минимальные термы для любых функций размерности не более пяти, можно получить на сайте `http://isttu.irk.ru/mbf/`.

Заключение. В работе рассмотрен случай минимизации в базисах из класса NL_3. Представляется интересным рассмотреть приведенные тернарные базисы, содержащие двухместную линейную функцию.

Другим открытым вопросом является вопрос нахождения минимальных термов для частично заданных булевых функций.

Работа выполнена при частичной финансовой поддержке РФФИ (проект 04-07-90178-в).

Список литературы

1. Стеценко В. А. О предплохих базисах в P_2 // Математические вопросы кибернетики. Вып. 4. — М.: Наука, 1992. — С. 139–177.

2. Черухин Д. Ю. Алгоритмический критерий сравнения булевых базисов // Математические вопросы кибернетики. Вып. 8. — М.: Наука, 1999. — С. 77–122.

3. Яблонский С. В. О невозможности элиминации перебора всех функций из P_2 при решении некоторых задач теории схем // Докл. АН СССР. — 1959. — Т. 124, № 1. — С. 44–47.

4. Лупанов О. Б. О сложности реализаций функций алгебры логики формулами // Проблемы кибернетики. Вып. 3. — М.: Физматгиз, 1960. — С. 61–80.

ПРИМЕНЕНИЕ «МЕТОДА ВРОНСКИАНОВ» ДЛЯ РЕШЕНИЯ КОМБИНАТОРНЫХ ЗАДАЧ

Л. Н. Бондаренко (Пенза)

Использование комбинаторных методов решения ряда перечислительных задач приводит к линейным двухиндексным рекуррентным соотношениям, простым примером которых является выражение

$$a_{0,k} = \delta_{0,|k|},\ a_{m,k} = \alpha a_{m-1,k} + \beta a_{m-1,k-1},\ m \in \mathrm{N}, k \in \mathrm{Z}, \qquad (1)$$

где $\delta_{0,|k|}$ — символ Кронекера, а функции $\alpha{=}\alpha(m,k)$ и $\beta{=}\beta(m,k)$ с целочисленными коэффициентами линейны относительно m и k.

Один из мощнейших методов решения одноиндексных рекуррентных уравнений основан на нахождении для искомой последовательности производящей функции одного переменного. Но уже для решения (1) часто не удается найти соответствующую производящую функцию двух переменных. Поэтому в [1, 2] отмечается важность рассмотрения общих подходов для исследования таких соотношений.

Введем многочлен $u_m(t){=}\sum_k a_{m,k} t^{r(m,k)}$ комплексного переменного t, для которого функция $r(m,k)$ с целочисленными коэффициентами линейна по m и k, и предположим, что при заданных α и β в выражении (1) существует линейный дифференциальный оператор $H{=}H(D,t)$, $D{=}d/dt$, обладающий следующим свойством:

$$u_{m+1}(t) = Hu_m(t),\ m \ge m_0 \ge 0, \qquad (2)$$

Определитель $W(\varphi_0(t),...,\varphi_{m-1}(t)){=}\det(D^i\varphi_j(t))_{i,j=0}^{m-1}$ для системы функций $\{\varphi_j(t)\}_0^{m-1}$ называется *определителем Вронского* или *вронскианом* и обладает следующими свойствами:

Лемма. *Пусть* $\Phi{=}\{D(\varphi_j(t)/\varphi_0(t))\}_1^{m-1}$. *Тогда*

a) $W(\varphi_0(t),...,\varphi_{m-1}(t)){=}(\varphi_0(t))^m W(\Phi)$;

b) если $\{\varphi_j(t)\}_0^{m-1}$ *— фундаментальная система решений линейного дифференциального уравнения* $Lu{=}0$, *где* $Lu \equiv \sum_{i=0}^m p_i(t)D^i u$ *и* $u{=}u(t)$, *то* $Lu{=}\varphi_0(t)p_m(t)W(\Phi, D(u(t)/\varphi_0(t))/W(\Phi)$.

Доказательство. Прямое вычисление $D(\varphi_j(t)/\varphi_0(t))$ и применение простейших свойств определителей приводит к тождеству a), а b) несложно получить из рассмотрения однородной системы уравнений $\{\sum_{i=0}^m p_i(t)D^i\varphi_j(t){=}0\}_{j=0}^{m-1}$, $\sum_{i=0}^m p_i(t)D^i u{-}Lu{=}0$ и использования тождества a).

При введенных ограничениях многочлены $u_m(t)$ можно выразить через соответствующие вронскианы.

Теорема 1. *Пусть характеристическое уравнение* $(H-z)U{=}0$, *где* z *— комплексное переменное, имеет соответствующее формальное решение* $U(t,z){=}\sum_{j=0}^\infty b_j\varphi_j(t)z^j$. *Тогда многочлен*

$$u_m(t) = \varphi_0(t)p_{m-m_0}(t)W(\Phi, D(u_{m_0}(t)/\varphi_0(t))/W(\Phi), \qquad (3)$$

где $\Phi{=}\{D(\varphi_j(t)/\varphi_0(t))\}_1^{m-m_0-1}$, $\{\varphi_j(t)\}_0^{m-m_0}$ *— фундаментальная система решений уравнения* $H^{m-m_0}u{=}0$, *а* $p_{m-m_0}(t)$ *— коэффициент при старшей производной в последнем уравнении.*

Доказательство. Из (2) имеем $u_m(t){=}H^{m-m_0}u_{m_0}(t)$. Для формального ряда $U(t,z){=}\sum_{m=0}^\infty u_{m+m_0}(t)/z^m$ также из (2) получается формальное уравнение $(H{-}z)U{=}{-}u_{m_0}(t)z$, решение которого $U(t,z){=}{-}(H{-}z)^{-1}u_{m_0}(t)z$. Поэтому справедливо следующее тождество $(H{-}z)^{-1}{=}{-}\sum_{m=0}^\infty H_m/z^{m+1}$ и остается применить лемму.

В отличие от аналитической теории дифференциальных уравнений при доказательстве теоремы 1 применен формальный ряд, а полученные результаты нетрудно модифицировать для решения более сложных двухиндексных рекуррентных соотношений.

Рассмотрим примеры использования метода вронскианов.

1. Числа Стирлинга второго рода $S_{m,k}$ определяются выражением (1) при $\alpha{=}k$, $\beta{=}1$. Для них имеем $u_m(t){=}\sum_{k=0}^m S_{m,k}t^k$, $u_0(t){=}1$, $H{=}t(D{+}1)$, $p_m(t){=}t^m$, $\varphi_0(t){=}e^{-t}$, $\Phi{=}\{D\ln^j t\}_1^{m-1}$.

2. Числа Лаха без знака $L_{m,k}{=}\frac{m!}{k!}\binom{m-1}{k-1}$ определяются формулой (1) при $\alpha{=}m{+}k{-}1$, $\beta{=}1$. В этом случае $u_m(t){=}\sum_{k=0}^m L_{m,k}t^{m+k}$,

$u_0(t)=1$, $H=t^2(D+1)$, $p_m(t)=t^{2m}$, $\varphi_0(t)=e^{-t}$, $\Phi=\{Dt^{-j}\}_1^{m-1}$.

3. Числа $[m!/k!]$, где $[\cdot]$ означает целую часть, задаются выражением (1) при $\alpha=m-k$, $\beta=1$. В этом случае $u_m(t)=\sum_{k=0}^{m-1}[m!/k!]t^{m-k}$, $u_1(t)=t$, $H=t^2D+1$, $p_{m-1}(t)=t^{2(m-1)}$, $\varphi_0(t)=e^{1/t}$, $\Phi=\{Dt^{-j}\}_1^{m-2}$.

4. Числа Моргана $\Delta^k 0^m=k!S_{m,k}$ задаются соотношением (1) при $\alpha=\beta=k$. В этом случае $u_m(t)=\sum_{k=0}^{m}k!S_{m,k}t^k$, $u_0(t)=1$, $H=tD(t+1)$, $p_m(t)=(t^2+t)^m$, $\varphi_0(t)=(t+1)^{-1}$, $\Phi=\{D\ln^j(t/(t+1))\}_1^{m-1}$.

5. Числа Йордана без знака $J_{m,k}$ определяются выражением (1) при $\alpha=\beta=2m-k-1$. В этом случае получим $u_m(t)=\sum_{k=0}^{m}J_{m,k}t^{2m-k}$, $u_0(t)=1$, $H=t^2D(t+1)$, $p_m(t)=(t^3+t^2)^m$, $\varphi_0(t)=(t+1)^{-1}$, а система функций $\Phi=\{D(1/t+\ln(t/(t+1))^j\}_1^{m-1}$.

Приведенные примеры могут быть продолжены на целые отрицательные значения индекса m. Отметим, что $S_{-k,-m}$ совпадают с числами Стирлинга $s_{m,k}$ первого рода без знака, а $L_{m,k}=L_{-k,-m}$.

Поставим следующую задачу на векторные разбиения. Пусть каждая компонента k – мерного вектора $(n,\dots,n)$, где $n=6m+1$, разложена на три целых положительных слагаемых $x<y<z$, $x+y+z=n$ так, что все слагаемые различны. Пусть $q_{m,k}$ — число различных наборов троек (x,y,z) при произвольном их упорядочивании.

При фиксированном m построим прямоугольную таблицу, строки которой x пронумерованы числами $1,2,\dots,2m-1$, а столбцы y — числами $2,3,\dots,3m-1$. Каждая тройка (x,y,z) описывается клеткой этой таблицы, в которую записано число $2m+2\le z\le 6m-2$, причем $x<y<z$, $x+y+z=n$.

Для этой таблицы $q_{m,k}$ совпадает с числом различных наборов из k клеток (x,y,z), а при замене z в клетке (x,y,z) символом " $*$ " обозначим через $Q_{m,k}$ число различных наборов из k клеток $(x,y,*)$. Количество заполненных клеток (x,y,z) рассматриваемой таблицы равно $q_{m,1}=Q_{m,1}$ и совпадает с числом $m(3m-2)$. Также можно получить формулы: $q_{2r,2}=r(3r-1)(24r^2-32r+11)$, $q_{2r+1,2}=r^2(72r^2+24r-7)$ и $Q_{m,2}=m(m-1)(9m^2-17m+7)/2$.

В связи с задачами, поставленными в [3], представляет интерес оценка числа $q_{m,m}$, причем вычислением получены значения: $q_{1,1}=1$; $q_{2,2}=6$; $q_{3,3}=65$; $q_{4,4}=1013$; $q_{5,5}=20973$; $q_{6,6}=543505$. Для нахождения требуемой оценки применяется

Теорема 2. *При начальных условиях $q_{0,k}=Q_{0,k}=\delta_{0,|k|}$ справедливы следующие рекуррентные соотношения:*

$$q_{m,k}=q_{m-1,k}+q'_{m,k}+q''_{m,k},\ m\in\mathrm{N},k\in\mathrm{Z}, \qquad (4)$$

где $q'_{m,k}$ — число различных наборов из k клеток (x,y,z) таблицы, в которых ровно одна имеет номер строки 1 или 2; $q''_{m,k}$ — число различных наборов из k клеток (x,y,z) таблицы, в которых имеется ровно одна с номером строки 1 и ровно одна с номером строки 2;

$$Q_{m,k}=Q_{m-1,k}+\alpha Q_{m-1,k-1}+\beta Q_{m-1,k-2},\ m\in\mathrm{N},k\in\mathrm{Z}, \qquad (5)$$

где $\alpha=6m-4k-1$, $\beta=(3m-2k)(3m-2k+1)$.

Доказательство. Преобразование клеток (x,y,z) таблицы при фиксированном m в клетки вида $(x-2,y-2,z-2)$ приводит к рассмотрению таблицы для случая $m-1$. При этом наборы из k различных клеток (x,y,z) таблицы разделяются на три класса: первый содержит ровно $q_{m-1,k}$, второй — $q'_{m,k}$, а третий — $q''_{m,k}$ таких наборов. Поэтому справедливо выражение (4). Для клеток вида $(x,y,*)$ дополнительно находится число α, равное количеству различных клеток $(x,y,*)$ в первых двух строках таблицы, не совпадающих с различными выбранными $k-1$ клетками $(x,y,*)$ из остальных строк таблицы. Затем определяется число β, равное количеству различных пар клеток $(x,y,*)$ в первых двух строках таблицы, не совпадающих с различными выбранными $k-2$ клетками $(x,y,*)$ из остальных строк таблицы. В результате получается выражение (5).

В частности, из (4), (5) находим $q_{m,0}=Q_{m,0}=1$ при $m\ge 0$, а из (5) получим $Q_{2r+1,3r+1}=2^{-r}(2r+1)!^2/r!$, $Q_{2r,3r-1}=2^{-r-1}(2r+1)!^2/r!$.

С помощью рекуррентного соотношения (5) определим многочлен $u_m(t)=\sum_{k=0}^{[(3m-1)/2]}Q_{m,k}t^{3m-2k}$, причем $u_0(t)=1$, для которого справедливо равенство (2) с оператором $H=t(D^2+2tD+t^2+1)$.

Распространение действия теоремы 1 на этот оператор приводит к следующим результатам: $p_m(t)=t^m$, $\varphi_0(t)=e^{-t^2/2}$, а систему $\Phi=\{\{Dt^j\}_1^m,\{D(t^j\ln t)\}_1^{m-1}\}$ составляет $2m-1$ функция.

Система функций Φ находится с помощью решения характеристического уравнения $(H-z)U=0$, которое выражается через комбинацию модифицированных функций Бесселя первого порядка и имеет вид: $U=\sqrt{t}e^{-t^2/2}(C_1I_1(2\sqrt{tz})+C_2K_1(2\sqrt{tz}))$, а разложение по степеням z этого выражения и позволяет найти фундаментальную систему решений, соответствующую оператору H^m.

Запись $u_m(t)$ в форме (3) приводит к следующему утверждению:

Теорема 3. *Перечисляющий числа $Q_{m,k}$ многочлен имеет вид:*

$$u_m(t) = \sum_{k=1}^{m} (-i)^{m+k} L_{m,k} He_{m+k}(it) t^k, \qquad (6)$$

где $L_{m,k}$ — числа Лаха без знака, $He_n(t)$ — многочлен Эрмита [4], *$i{=}\sqrt{-1}$. Также справедливо равенство*

$$Q_{m,m} = (m+1)(m-1)! \sum_{k=1}^{m} \binom{m}{k}^2 \binom{m+k}{m+1} 2^{-k}. \qquad (7)$$

Доказательство. Так как по известной формуле Родрига $He_n(t){=}(-1)^n e^{t^2/2} D^n e^{-t^2/2}$, то сравнение форм (3) для многочленов, описывающих числа Лаха без знака, и для рассматриваемых многочленов $u_m(t)$, а также применение простейших свойств определителей приводит к выражению (6). При подстановке явных выражений для чисел $L_{m,k}$ и многочленов Эрмита $He_n(t)$ в формулу (6) определение коэффициента при t^m позволяет найти выражение для $Q_{m,m}$ в форме соотношения (7).

Из полученных результатов следует

Теорема 4. *a) $Q_{m,m}{=}O(C^m(m-1)!)$, где число C определяется равенством $C{=}(1{+}\mu)(1{-}\mu)^{-2}{\approx}7,41375$, а μ является действительным корнем уравнения $x^3{+}x^2{+}x{-}1{=}0$ и $\mu{\approx}0,543689$.*

b) $q_{m,m}{=}O(c^m(m-1)!)$, где $1{<}c{<}C$.

Доказательство. В выражении (7) отношение $(k+1)$–го и k–го членов суммы равно $2^{-1}k^{-1}(k{+}1)^{-2}(m{+}k{+}1)(m{-}k)^2$. Обозначая $\mu{=}k/m$ и устремляя m и k к ∞, находим с помощью стандартной методики исследования асимптотики сумм с положительными членами [2] оценку в a). Для получения оценки в b) применяются формулы (4) и (5), из которых следует, что $q_{m,m}{>}(m{-}1)q_{m-1,m-1}$. Также учитываем неравенство $q_{m,k}{\le}Q_{m,k}$, непосредственно вытекающее из определения рассматриваемых чисел.

Теорема 4 и вычисленные значения $q_{m,m}$ позволяют высказать следующую гипотезу: $q_{m,m}{\le}\prod_{k=1}^{m}(5m{-}4){=}5^m\Gamma(m{+}1/5)/\Gamma(1/5)$, где $\Gamma(x)$ означает гамма функцию.

Список литературы

1. Грэхем Р., Кнут Д., Паташник О. Конкретная математика. Основание информатики. — М.: Мир, 1998.

2. Бендер Э. А. Асимптотические методы в теории перечислений // Перечислительные задачи комбинаторного анализа. — М.: Мир, 1979. — С. 266–310.

3. Бондаренко Л. Н. Аддитивная задача перечисления перестановок // Проблемы теоретической кибернетики. Тезисы докладов XIV Международной конференции (Пенза, 23–28 мая 2005 г.). — М.: Изд-во механико-математического факультета МГУ, 2005. — С. 21.

4. Справочник по специальным функциям / Под ред. М. Абрамовица, И. Стиган. — М.: Наука, 1979.

СЛОЖНОСТЬ ВЫЧИСЛЕНИЯ ЭКСПОНЕНТЫ МЕТОДОМ КАРАЦУБЫ

Я. В. Вегнер (Москва)

Рассматривается метод Е. Карацубы вычисления трансцендентных функций [1], позволяющий вычислять функцию e^x со сложностью $O(n\log^3 n\log\log n)$. Приводится уточненная оценка сложности этого метода с явно выписанными константами.

Используются оценки сложности из [2]: сложность $(3,2)$-компрессора не превосходит $5n$, сложность сложения двух чисел длины n не превосходит $11n$. Пусть $M(n)$ — функция, оценивающая сверху сложность умножения двух n-значных чисел, удовлетворяющая неравенству $2M(n) \le M(2n)$.

Далее излагается метод Карацубы [1] вместе с уточненными оценками сложности каждого шага. Исследуется сложность вычисления функции e^x на отрезке $[0,1/4]$ с погрешностью 2^{-n}, где $n > 8$. Вводятся обозначения $k = \lceil \log n \rceil$ и $p = 2^{k+1}$.

Вычисление функции в точке x_0 заменяется вычислением в точке x_p, имеющей вид $x_p = 0{,}00\alpha_3\alpha_4\ldots\alpha_p$ и приближающей точку x_0 с погрешностью $|x_0 - x_p| \le 2^{-p}$. Возникающая погрешность не превосходит $e^{3/8}2^{-p}$.

Число x_p представляется в виде

$$x_p = \frac{\beta_2}{2^4} + \frac{\beta_3}{2^8} + \ldots + \frac{\beta_{k+1}}{2^{2^{k+1}}},$$

где

$$\beta_2 = \alpha_3\alpha_4, \quad \beta_3 = \alpha_5\alpha_6\alpha_7\alpha_8, \quad \ldots, \quad \beta_{k+1} = \alpha_{p-2^k+1}\ldots\alpha_p$$

и β_ν, $2 \le \nu \le k+1$ — целое $2^{\nu-1}$-значное число.

Тогда число e^{x_p} переписывается в виде произведения

$$e^{x_p} = \prod_{\nu=2}^{k+1} e^{\beta_\nu 2^{-2^\nu}}.$$

Каждый множитель произведения раскладывается в ряд Тэйлора

$$e^{\beta_\nu 2^{-2^\nu}} = e^{\alpha/2^m} = 1 + \frac{\alpha}{1!2^m} + \frac{\alpha^2}{2!2^{2m}} + \ldots + \frac{\alpha^r}{r!2^{rm}} + R_\nu(r),$$

где $m = 2^\nu, \alpha = \beta_\nu, r = p\ 2^{-\nu+1} = 2^{k-\nu+2}$.

R_ν — остаточный член, не превосходящий 2^{-p}. Таким образом,

$$e^{\beta_\nu 2^{-2^\nu}} = \xi_\nu + \theta_\nu(r)2^{-p},$$

где

$$\xi_\nu = 1 + \frac{\alpha}{1!2^m} + \frac{\alpha^2}{2!2^{2m}} + \ldots + \frac{\alpha^r}{r!2^{rm}}, \quad 0 < \theta_\nu(r) < 1.$$

Число ξ_ν представляется в виде дроби

$$\xi_\nu = a_\nu/c_\nu, \quad c_\nu = r!2^{rm}, \quad a_\nu = \xi_\nu c_\nu.$$

Пусть η_ν — p-значное приближение к ξ_ν, то есть

$$\xi_\nu = a_\nu/c_\nu = \eta_\nu + \theta'_\nu 2^{-p}, \quad |\theta'_\nu| < 1.$$

Тогда

$$e^{x_p} = \prod_{\nu=2}^{k+1} (\eta_\nu + 2\theta_\nu 2^{-p}), \quad |\theta_\nu| \le 1.$$

Это произведение можно дополнить до 2^l множителей, где $l = \lceil \log k \rceil$, положив $\eta_\nu = 1, \theta_\nu = 0$ при $\nu > k$. Произведение

$$e^{x_p} = \prod_{\nu=2}^{2^l+1} (\eta_\nu + 2\theta_\nu 2^{-p})$$

можно вычислить с погрешностью 2^{-n} за l шагов следующего процесса.

На первом шаге перемножаются последовательно попарно множители этого произведения, то есть члены вида $(\eta_\nu + 2\theta_\nu 2^{-p})$ и $(\eta_{\nu+1} + 2\theta_{\nu+1}2^{-p})$. Умножение $\eta_\nu\eta_{\nu+1}$ проводится с точностью 2^{-p}. На втором шаге перемножаются последовательно попарные произведения, полученные на предыдущем шаге. Продолжая этот процесс, получим в конце произведение всех сомножителей.

Таким образом, вычисление e^{x_0} сводится к четырем этапам:

1) поиск числителей a_ν, $2 \le \nu \le k+1$;

2) поиск знаменателей $c_\nu = r!2^{rm}$, $2 \le \nu \le k+1$;

3) деление a_ν на c_ν с точностью 2^{-p}, дающее η_ν;

4) умножение с помощью указанного процесса всех η_ν.

Вычисление a_ν проводится с помощью группировки и выделения общего множителя соседних слагаемых в сумме

$$a_\nu = 2^{rm}r! + 2^{(r-1)m}\frac{r!}{1!}\alpha + 2^{(r-2)m}\frac{r!}{2!}\alpha^2 + \ldots + 2^0\frac{r!}{r!}\alpha^r,$$

затем группировки пар слагаемых в четверки, и так далее, пока не получится одно число. В соответствии с этим построением вычисляется набор коэффициентов $\beta_{r_i-j}(i)$, $i = 1, \ldots, k-\nu+2$, $j = 0, \ldots, \frac{r_i}{2} - 1$, где $r_i = \frac{2r}{2^i}$. Сначала вычисляются самые короткие коэффициенты. Вычисление одного коэффициента $\beta_{r_i-j}(i)$ имеет сложность

$$\begin{aligned} L \quad \le \quad & \left(2 + \left\lceil \frac{\log r}{m} \right\rceil\right) M(2^i m) + \left(2 + \left\lceil \frac{m}{\log r} \right\rceil\right) M(2^i \log r) + \\ & + M(2^i \log r) + 21(i + 2^i(2m + 2\log r)), \end{aligned}$$

а сложность вычисления всех a_ν не превосходит

$$\begin{aligned} L \quad \le \quad & M(2^{k+2}(k+1)) + 4kM(2^{k+1}k) + 4kM(2^k k) + \\ & + M(2^{k+2})(4.5k^2 + 4k) + 82k2^{k+2} + 7k(k+1)(2k+1) + \\ & + 8k(k+1) + 84k. \end{aligned}$$

Поскольку для деления на c_ν потребуется их нормализовать, мы будем вычислять c_ν вместе с их длинами. По определению,

$$c_\nu = r!2^{rm} = (2^{k-\nu+2})!2^{2^{k+2}}, \quad 2 \le \nu \le k+1.$$

Это означает, что все c_ν можно вычислять совместно, посчитав $(2^j)!$, $j = 1, \ldots, k$, и приписав к ним нужное число нулей.

Вместо обычной операции умножения чисел при подсчете c_ν будем использовать операцию над парами чисел, сопоставляющую числам a, b и их длинам l_a, l_b произведение ab и длину произведения l_{ab}:

$$(a, l_a) \times (b, l_b) \to (ab, l_{ab}).$$

Если длины l_a и l_b заданы, то произведение ab может иметь длину либо $l_a + l_b$, либо $l_a + l_b - 1$ ($a \neq 0, b \neq 0$). Выбрать правильную длину можно, анализируя $(l_a + l_b - 1)$-й бит произведения. Сложность этой подсхемы не превосходит

$$L(S_n) \leq M(n) + 3n + 27\lceil \log n \rceil + 16,$$

где $l_a \leq n, l_b \leq n$.

Вычисление организуем так: выпишем числа $1, 1, 2, 3, 4, \ldots, 2^k - 1$, чьи длины не превосходят k. На первом шаге умножаем их последовательно попарно. Получится 2^{k-1} чисел с длиной не больше $2k$. Результаты первого шага перемножим последовательно попарно, получим 2^{k-2} чисел длины $4k$. Продолжим этот процесс, пока не получим одно число, равное $(2^k - 1)!$. Сложность вычисления всех c_ν вместе с их длинами составляет

$$\begin{aligned} L \quad \leq \quad & kM(2^{k-1}k) + 3k^2 2^{k-1} + 27 \cdot 2^k \lceil \log k \rceil + 43 \cdot 2^k + \\ & + 11 \left(\frac{k(k+1)}{2} + k2^{k+2} + 2k + (k-2)2^{k+1} + 4 \right). \end{aligned}$$

Деление реализуем с помощью итерации Ньютона: найдем обратную величину к c_ν, и умножим a_ν на c_ν^{-1}. Используем итерацию

$$s_{2n} = z s_n^2 - 2 s_n,$$

где $\frac{1}{2} \leq z < 1$ — нормализованное значение c_ν, $z = c_\nu 2^{-l_{c_\nu}}$, s_n — приближение к z^{-1} с погрешностью 2^{-n}. Достаточно $(k+2)$ шагов итерации, чтобы получить z^{-1} с требуемой точностью. По окончании итерации необходимо будет провести денормализацию, то есть умножить s_n на $2^{-l_{c_\nu}}$.

Сложность деления a_ν на c_ν составляет

$$\begin{aligned} L \quad \leq \quad & 4(2^{k+2} + (k - \nu + 1)2^{k-\nu+2} + 1) \times \\ & \times \log(2^{k+2} + (k - \nu + 1)2^{k-\nu+2} + 1) + \\ & + M(2^{k+2}) + M(2^{k+3}) + M(2^{k+4}) + 16 \cdot 2^{k+4}. \end{aligned}$$

Суммируя по всем ν, $2 \leq \nu \leq k+1$, получим

$$\begin{aligned} L \quad \leq \quad & 8k(k+1)2^{k+2} + 8k(k+1) + (k-1)(k+1)2^{k+2} + 4k + 4 + \\ & + M(2^{k+3}) + M(2^{k+4}) + M(2^{k+5}) + 128 \cdot 2^{k+2}. \end{aligned}$$

Поскольку умножение производится с точностью 2^{-p}, то для вычисления произведения $\prod \eta_\nu$ требуется

$$M(p)(2^{l-1} + 2^{l-2} + \ldots + 1) = (2^l - 1)M(p) < 2kM(p)$$

операций.

Складывая оценки для сложности и глубины всех этапов, получаем окончательную оценку сложности вычисления e^x на отрезке $[0, 1/4]$ с погрешностью 2^{-n}:

$$\begin{aligned} L \quad \leq \quad & M(2^{k+2}) + 4kM(2^{k+1}k) + 4kM(2^k k) + kM(2^{k-1}k) + \\ & + 2kM(2^{k+1}) + M(2^{k+2})(5k^2 + 4k) + \\ & + M(2^{k+3}) + M(2^{k+4}) + M(2^{k+5}) + \\ & + 2^{k+2}(10k^2 + 107k + 7\log k + 134) + \\ & + k(k+1)(14k + 29) + 110k + 48, \end{aligned}$$

где $k = \lceil \log n \rceil$. Полученная оценка равна по порядку исходной оценка Карацубы $O(n \log^3 n \log\log n)$, однако позволяет вычислять сложность схемы для конкретных n.

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

Список литературы

1. Карацуба Е. А. Быстрые вычисления трансцендентных функций // Проблемы передачи информации. — 1991. — Т. 27, вып. 4.

2. Wegener I. The complexity of boolean functions // Stuttgart: Wiley, 1987.

ОБ ОПЕРАТОРНОЙ КЛАССИФИКАЦИИ БУЛЕВЫХ ФУНКЦИЙ

С. Ф. Винокуров (Иркутск)

В работе рассматривается классификация булевых функций, построенная по группе операторных преобразований. Важность рассмотрения таких преобразований связана с задачей представления булевых функций минимальными полиномиальными формами и их обобщениями — операторными формами.

Пусть $\tilde{x}$ — сокращение для набора $x_1, \ldots, x_n$. Оператор $\mathbf{t}$ представляется последовательностью $\mathbf{t}_1 \ldots \mathbf{t}_n$, где $\mathbf{t}_i \in \{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$, n — размерность оператора. Действие оператора $\mathbf{t}$ на функцию $g(\tilde{x})$ определяется по правилу $\mathbf{t}g(\tilde{x}) = g_n(\tilde{x})$, где $g_0(\tilde{x}) = g(\tilde{x})$ и

$$g_i(\tilde{x}) = \begin{cases} g_{i-1}(\tilde{x}), & \text{если } \mathbf{t}_i = \mathbf{e}; \\ g_{i-1}(x_1, ..., x_{i-1}, \bar{x}_i, x_{i+1}, ..., x_n), & \text{если } \mathbf{t}_i = \mathbf{p}; \\ g_{i-1}(\tilde{x}) \oplus g_{i-1}(x_1, ..., x_{i-1}, \bar{x}_i, x_{i+1}, ..., x_n), & \text{если } \mathbf{t}_i = \mathbf{d}. \end{cases}$$

Под операторной формой понимается представление булевой функции f в следующем виде:

$$f(\tilde{x}) = \mathbf{a}_1(g(\tilde{x})) \oplus \cdots \oplus \mathbf{a}_t(g(\tilde{x})), \qquad (*)$$

где $\mathbf{a}_1, ..., \mathbf{a}_t$ — операторы, $g(\tilde{x})$ — функция, называемая базисной. Подробно операторы и операторные формы описаны в [1]. В дальнейшем изложении можно считать, что $g(\tilde{x}) = x_1 \cdot \cdots \cdot x_n$

На операторах можно определить отображение. Пусть P — полная группа подстановок на множестве $\{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$. Пусть φ — последовательность $\varphi_1\varphi_2 \ldots \varphi_n$, где $\varphi_i \in P$. Тогда φ действует на оператор $\mathbf{a}_1 \ldots \mathbf{a}_n$ так: $\varphi(\mathbf{a}_1 \ldots \mathbf{a}_n) = \varphi_1(\mathbf{a}_1) \ldots \varphi_n(\mathbf{a}_n)$.

Отображение φ операторов продолжается на функции: $\varphi(f) = \varphi(\mathbf{b}_1)(g) \oplus \cdots \oplus \varphi(\mathbf{b}_t)(g)$.

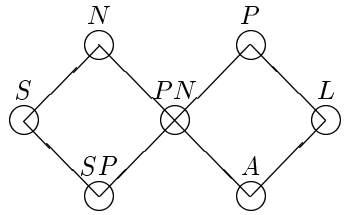
Такие преобразования функций будем называть S-преобразованиями.

Определение. SP-преобразованиями функций назовем композицию S-преобразований и преобразований, задаваемых перестановками переменных.

Легко показать, что SP-преобразования образуют группу, в которую входит подгруппа S-преобразований.

Определение. Функции f и g называются $SP(S)$-эквивалентными, если существует $SP(S)$-преобразование φ, что $g = \varphi(f)$.

На диаграмме приведено сравнение по включению S- и SP-эквивалентностей с известными эквивалентностями (включение снизу-вверх).



Символами обозначены следующие группы преобразований: P — группа перестановок переменных, задает преобразование $g(\tilde{x}) = f(x_{i_1}, ..., x_{i_n})$; N — группа инвертирования переменных, задает преобразование $g(\tilde{x}) = f(x^{\alpha_1}, ..., x^{\alpha_n})$, $\alpha_i \in \{0, 1\}$, $x^1 = x$, $x^0 = \bar{x}$; PN — группа Джевонса, задает преобразование $g(\tilde{x}) = f(x_{i_1}^{\alpha_1}, ..., x_{i_n}^{\alpha_n})$; L — группа линейных преобразований $g(\tilde{x}) = f(\oplus_i a_{1i}x_i, ..., \oplus_i a_{ni}x_i)$, $a_{ij} \in \{0, 1\}$, $\det(a_{ij}) \neq 0$; A — группа аффинных преобразований $g(\tilde{x}) = f(\oplus_i a_{1i}x_i \oplus b_1, ..., \oplus_i a_{ni}x_i \oplus b_n)$, $\det(a_{ij}) \neq 0$, $b_j \in \{0, 1\}$.

Можно заметить, что преобразования P, N, PN, L и A сохраняют количество единиц в векторном представлении функции. Более точно, эти преобразования являются перестановками, действующими на вектор функции (подробнее см. [2]).

Преобразования P, N, PN, S и SP сохраняют сложность операторной формы, в частности — сложность полиномиального представления. Все функции, попадающие в один класс эквивалентности относительно любой из этих групп, имеют одинаковую сложность (сложность как число слагаемых в операторной форме) [1]. Однако преобразования S и SP не только не являются перестановками вектора функции, но даже не сохраняют число единиц функции.

Классификация булевых функций естественно связана с нахождением как числа классов эквивалентности булевых функций, так и непосредственно представителей этих классов. Для S- и SP-преобразований важность нахождения представителей связана с их непосредственным использованием в алгоритмах минимизации [3].

Для получения представителей классов эквивалентности обычно пользуются понятием инварианта группы преобразований.

В свою очередь решение задачи нахождения инвариантов для группы SP-преобразований может быть связано с представлением булевой функции специальной операторной формой.

Для булевой функции $f(\tilde{x})$ специальная операторная форма строится следующим образом. Известно [1], что для любого оператора $\mathbf{a}$ найдутся 2^n операторов $\mathbf{b}_1, ..., \mathbf{b}_{2^n}$, что для любой функции $g(\tilde{x})$ имеет место равенство

$$\mathbf{a}(g(\tilde{x})) = \bigoplus_i \mathbf{b}_i(g(\tilde{x})). \qquad (**)$$

В операторной форме $(*)$ каждый оператор $\mathbf{a}_i$ заменяется соответствующей суммой $(**)$, затем производится сокращение пар одинаковых слагаемых. Полученное представление и называется специальной операторной формой (СОФ)[4].

Количество слагаемых (длина) СОФ является инвариантом SP-преобразований. При $n = 3$ неэквивалентные функции имеют разную длину СОФ.

Операторы представляются последовательностями, в которых элемент с индексом i действует на функцию по переменной x_i. По СОФ строится таблица размерами $3 \times n$ частот операторных символов — по каждой переменной подсчитывается количество появлений символов **d**, **e** или **p**. Таблица частот также является инвариантом. При $n = 4$ неэквивалентные функции имеют различные таблицы частот.

При $n = 5$ указанные инварианты не образуют полную систему. Однако для этого случая также найден полный инвариант. Аналогично таблице частот строится таблица размерами $3n \times 3n$, состоящая из $n \times n$ квадратов размерами 3×3. Квадрат ij соответствует паре $x_i x_j$, столбцы и строки квадрата помечены символами {**d**, **e**, **p**}. Элемент квадрата, например с индексом **de**, равен количеству пар вхождений символов **d** и символов **e** в СОФ по переменным x_i и x_j, соответственно. Такая таблица также является инвариантом SP-преобразований, причем для $n = 5$ это полный инвариант.

В качестве простого примера рассмотрим функцию $f = (00010110)$. Ее специальная операторная форма выглядит так (указаны только операторы, базисная функция $g(x_1, x_2, x_3) = x_1 \cdot x_2 \cdot x_3$): СОФ($f$)=**epp** $\oplus$ **epd** $\oplus$ **edp** $\oplus$ **edd** $\oplus$ **pep** $\oplus$ **ped** $\oplus$ **ppe** $\oplus$ **ppd** $\oplus$ **pde** $\oplus$ **pdp** $\oplus$ **dep** $\oplus$ **ded** $\oplus$ **dpe** $\oplus$ **dpp** $\oplus$ **dde** $\oplus$ **ddd**.

Таблица частот:

	x_1	x_2	x_3
d	6	6	6
e	4	4	4
p	6	6	6

Таблица пар частот:

	d	**e**	**p**	**d**	**e**	**p**	**d**	**e**	**p**
d	6	0	0	2	2	2	2	2	2
e	0	4	0	2	0	2	2	0	2
p	0	0	6	2	2	2	2	2	2
d	2	2	2	6	0	0	2	2	2
e	2	0	2	0	4	0	2	0	2
p	2	2	2	0	0	6	2	2	2
d	2	2	2	2	2	2	6	0	0
e	2	0	2	2	0	2	0	4	0
p	2	2	2	2	2	2	0	0	6

Работа выполнена при финансовой поддержке РФФИ, проект 04-07-90178в.

Список литературы

1. Избранные вопросы теории булевых функций / Под ред. Винокурова С. Ф. и Перязева Н. А. — М.: ФИЗМАТЛИТ, 2001.

2. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии — М.: МЦНМО, 2004.

3. Gaidukov A. Algorithm to derive minimum ESOP for 6-variable function // 5th International Workshop on Boolean Problems. — Freiberg, 2002.— P. 141–148.

4. Винокуров С. Ф. Специальная операторная форма булевых функций и некоторые ее приложения // Международная школа-семинар "Синтез и сложность управляющих систем".— Новосибирск: изд-во ИМ СО РАН.— 2004.— С. 26–29.

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ ПОИСКА ДОКАЗАТЕЛЬСТВ В БЕСКОНЕЧНОЗНАЧНОЙ ПРЕДИКАТНОЙ ЛОГИКЕ, ОСНОВАННОЙ НА ЛИНЕЙНЫХ НЕРАВЕНСТВАХ

А. С. Герасимов (Санкт-Петербург)

В данной работе описывается алгоритм поиска вывода в секвенциальном исчислении для бесконечнозначной предикатной логики Lq более выразительной, чем логика Лукасевича. (Логика Lq кратко описана в [1] и более подробно, вместе с секвенциальным исчислением и его свойствами, — в [2].) Также в данной работе приводятся основные особенности интерфейса прикладного программирования (ИПП) для поиска вывода в рассматриваемом исчислении. Главными

принципами ИПП являются модульность и возможность его адаптации к другим секвенциальным исчислениям. ИПП может служить ядром дедуктивной системы, основанной на логике Lq.

1. Обзор синтаксиса логики и исчисления. Термом является предметная переменная и предметная константа. Атомарной формулой является любое рациональное число и предикатный символ, за которым следует заключенный в скобки список термов.

Атомарная формула является формулой логики Lq. Если A и B — формулы, q — рациональное число, x — предметная переменная, то $(A\&B)$, $(A \vee B)$, $\forall xA$, $\exists xA$, $(A \prec B)$, $q \cdot A$ являются формулами.

Логическая связка $\prec$ называется нечетким неравенством, а связка $q\cdot$ (где q — рациональное число) — модератором.

В безантецедентном обратимом секвенциальном исчислении LqS связки $\&$, $\vee$ и кванторы могут вводиться в главную формулу заключения как (а) логические символы самого верхнего уровня, (б) логические символы второго уровня, когда модератор является логическим символом самого верхнего уровня, (в) логические символы более низких уровней, когда нечеткие неравенства находятся в главной формуле на нескольких верхних уровнях, на следующем уровне, возможно, находится модератор, и уже на последующем уровне находится введенный логический символ. При этом различаются случаи неотрицательных и отрицательных модераторов и случаи так называемых положительных и отрицательных вхождений $\prec$ в формулу. Кванторные правила вывода имеют стандартные ограничения для вывода чистых секвенций. Приведем несколько правил вывода:

$$\frac{\Delta, q_n \cdot A}{\Delta, q_n \cdot B} \ (q_n\vee), \qquad \frac{\Delta, F_1(A \prec_+ q_p \cdot B(y|x))F_2}{\Delta, F_1(A \prec_+ q_p \cdot \forall xB)F_2} \ (\prec_+ q_p\forall),$$

$$\frac{\Delta, F_1(A \prec_- q_p \cdot B(t|x))F_2, F_1(A \prec_- q_p \cdot \forall xB)F_2}{\Delta, F_1(A \prec_- q_p \cdot \forall xB)F_2} \ (\prec_- q_p\forall).$$

В этих правилах Δ — список формул, q_n — отрицательное рациональное число, q_p — неотрицательное рациональное число, A, B — формулы, $\prec_+$ — положительное вхождение $\prec$, $\prec_-$ — отрицательное вхождение $\prec$, x и y — предметные переменные, $B(t|x)$ — результат подстановки терма t на место всех свободных вхождений предметной переменной x, F_1 и F_2 — части соответствующей формулы. Правила, содержащие F_1 и F_2, вводят логический символ под несколькими нечеткими неравенствами и модератором (см. (в) выше).

Вопрос о том, является ли секвенция аксиомой, сводится к построению соответствующей данной секвенции системы линейных неравенств с рациональнозначными переменными (так, как это описано в [2]) и проверке несовместности этой системы.

Основной проблемой при обратном поиске вывода (начиная с исходной формулы, для которой требуется построить вывод) в исчислении LqS является нахождение термов для подстановки при контрприменениях (от заключений к посылкам) минус-правил (т.е. правил, содержащих неопределенный терм, обозначенный t). Таких термов для подстановки бесконечно много. В [2] также описано минус-нормальное исчисление $LqSn$, равнообъемное исчислению LqS. Исчисление $LqSn$ отличается от LqS только наличием дополнительного ограничения на минус-правила: терм t может быть только одним из термов, которые входят в заключение правила и которые не являются связанными в заключении правила; если таких термов нет, то терм t является какой угодно предметной переменной, не входящей в заключение правила.

2. Алгоритм поиска вывода. Поиск вывода секвенции S_0 осуществляется в секвенциальном исчислении $LqSn$, дополненном специальным видом предметных переменных — метапеременными. При поиске вывода строится заготовка дерева вывода, ее построение описывается ниже. Изначально заготовка дерева вывода состоит из одного узла-корня, в котором находится секвенция S_0. Алгоритм осуществляет повторение следующих действий.

Выбираются (а) правило вывода R, (б) секвенция S, находящаяся в одном из листовых узлов заготовки дерева вывода, (в) главная формула F_M секвенции S и (г) вхождение F_s подформулы главной формулы, причем эта подформула является минимальной подформулой, содержащей логический символ, который правило R вводит. (Например, для вышеприведенных правил вывода выбранные подформулы будут иметь вид $(A \vee B)$, $\forall xB$ и $\forall xB$ соответственно.) При таком выборе предпочтение отдается, во-первых, однопосылочным правилам, отличным от минус-правил, во-вторых, двухпосылочным правилам и, в-третьих, минус-правилам, причем при выборе минус-правил предпочтение отдается тому вхождению подформулы, к которому минус-правило применялось меньшее число раз.

Далее производится контрприменение правила R к секвенции S в соответствии с выбранными F_M и F_s. Заготовка дерева вывода достраивается так, что непосредственными потомками узла, содержащего секвенцию S, становятся узлы, содержащие секвенции-посылки правила R.

Если применяется кванторное правило, не являющееся минус-правилом, то генерируется уникальная предметная переменная (отличная от каждой из встречающихся в текущей заготовке дерева вывода переменной), которая используется в посылке правила. Уникальность переменной обеспечивает выполнение ограничения на такое кванторное правило.

Если применяется минус-правило, то вместо терма t подставляется уникальная метапеременная, для которой указывается множество подстановок — конечное множество термов, которые могут быть подставлены вместо этой метапеременной (эти термы выбираются из секвенции S согласно ограничению на минус-правила, упомянутому в конце раздела 1). При любой замене метапеременной на терм из множества подстановки этой метапеременной ограничения на кванторное правило, очевидно, выполняются.

В момент, когда никакие правила вывода не применимы, производится преобразование каждой секвенции, находящейся в листовом узле заготовки дерева вывода (далее — листовой секвенции), к системе линейных неравенств и проверка несовместности этой системы. Если все системы, соответствующие листовым секвенциям, оказались несовместны, то алгоритм заканчивает работу с ответом "секвенция выводима", иначе — с ответом "секвенция невыводима".

В момент, когда применимы только минус-правила, и ко всем вхождениям подформул, к которым какое-либо минус-правило применимо, минус-правила применялись одинаковое число раз, производится унификация, т. е. подбор значений метапеременных так, чтобы все листовые секвенции превратились в аксиомы. В процессе унификации осуществляется (конечный) перебор термов из множеств подстановок всех метапеременных, входящих в заготовку дерева вывода, подстановка термов вместо метапеременных, преобразование каждой листовой секвенции к системе линейных неравенств и проверка несовместности этой системы. Если при некоторой подстановке термов вместо метапеременных все системы, соответствующие листовым секвенциям, оказались несовместны, то алгоритм заканчивает работу с ответом "секвенция выводима".

В силу обратимости всех правил вывода и выполнения ограничений на кванторные правила описанный алгоритм выдает ответ "секвенция невыводима", если исходная секвенция выводима в исчислении $LqSn$, и если алгоритм выдает ответ "секвенция невыводима", то исходная секвенция невыводима.

3. ИПП для поиска вывода. ИПП реализован на объектно-ориентированном языке программирования Java.

Формула представляется в виде синтаксического дерева. Абстрактный класс `Formula` является вершиной иерархии классов, которые представляют формулы, являющиеся предикатными символами с аргументами (класс `PredicateSymbol`), начинающиеся с квантора (класс `QuantifierFormula`) и др. От абстрактного класса `Term`, представляющего терм, наследуют классы `IndividualConstant`, `BoundIndividualVariable`, `FreeIndividualVariable` и `Metavariable`. Для создания экземпляров различных типов формул и переменных

служит класс-фабрика `LogicalFactory`. Такой подход позволяет не создавать каждый раз новые объекты, а использовать разделяемые объекты.

Секвенция как список формул представлена классом `Sequent`. Класс `DerivationSkeleton` представляет заготовку дерева вывода, узел которой представлен классом `DerivationSkeleton.Node`. Абстрактный класс `InferenceRule` (его наследниками являются классы, представляющие правила вывода) имеет метод `applyBackward (DerivationSkeleton.Node node, Formula mainFormula, Formula subformula)`, который выполняет контрприменение правила. Таким образом, правила вывода могут быть легко изменены.

Интерфейс `Tactics` задает так называемую тактику поиска вывода. Тактика выбирает для контрприменения правило вывода, секвенцию, главную формулу и подформулу (см. раздел 2), а также указывает те моменты, когда следует попытаться закрыть заготовку дерева вывода (исследовав листовые секвенции на аксиоматичность). Реализующий этот интерфейс класс `DefaultTactics` делает выбор так, как описано в разделе 2. Такая архитектура (см. паттерн проектирования Стратегия [3]) позволяет экспериментировать с порядком применения правил вывода, не затрагивая остальные части алгоритма поиска вывода.

В классе `Prover` закодирован алгоритм поиска вывода, построенный на основе упомянутых абстракций.

Каждая система линейных неравенств, получаемая при распознавании аксиом, проверяется на несовместность вспомогательным алгоритмом [4], если все неравенства системы двучленные, иначе — функцией `FindInstance` системы компьютерной алгебры Mathematica (посредством J/Link-инструментария, связывающего программу на Java с Mathematica).

Список литературы

1. Герасимов А. С. Бесконечнозначная предикатная логика со связкой для усиления утверждений // Современная логика: проблемы теории, истории и применения в науке. Материалы IX Общероссийской научной конференции (Санкт-Петербург, 22–24 июня 2006 г.) — СПб: Изд-во СПбГУ, 2006. — С. 348–350.

2. Герасимов А. С. Предикатная логика на основе секвенциального исчисления, предназначенная для моделирования непрерывных шкал // Труды Десятой национальной конференции по искусственному интеллекту с международным участием КИИ-06. В печати.

3. Гамма Э., Хелм Р., Джонсон Р., Влиссидес Дж. Приемы объектно-ориентированного проектирования. Паттерны проектирования — СПб: Питер, 2001.

4. Герасимов А. С., Косовский Н. К. Истинно полиномиальный алгоритм определения совместности систем линейных двучленных неравенств // Устойчивость и процессы управления. Труды международной конференции (Санкт-Петербург, 29 июня – 1 июля 2005 г.). Т. 2. — СПб: СПбГУ, НИИ ВМ и ПУ, ООО ВММ, 2005. — С. 779–785.

О КОНЕЧНОЙ ПОРОЖДЕННОСТИ НЕКОТОРЫХ СЕМЕЙСТВ ПРЕДПОЛНЫХ КЛАССОВ МОНОТОННЫХ ФУНКЦИЙ K-ЗНАЧНОЙ ЛОГИКИ

О. С. Дудакова (Москва)

В работе исследуются предполные классы монотонных функций k-значной логики [1, 2]. Известно [3, 4], что при $k \leq 7$ все предполные классы в P_k являются конечно порожденными. При $k \geq 8$ в общем случае это неверно: в [5] приведен пример частично упорядоченного множества из восьми элементов, такого, что предполный класс всех функций, монотонных на этом множестве, не имеет конечного базиса. Полного описания всех конечно порожденных предполных классов монотонных функций к настящему времени не получено, известны лишь некоторые достаточные условия конечной порожденности предполных классов монотонных функций, (см., например, [6, 7]). В данной работе приводятся два семейства частично упорядоченных множеств, для которых найдены необходимые и достаточные условия конечной порожденности соответствующих предполных классов монотонных функций (см. также [8, 9]).

Пусть $\mathcal{P}$ — некоторое частично упорядоченное множество с отношением порядка $\leq$. Пусть $a_1, a_2 \in \mathcal{P}$, элементы a_1 и a_2 несравнимы. Назовем $b \in \mathcal{P}$ верхней гранью элементов a_1, a_2, если выполняются неравенства $b \geq a_1$ и $b \geq a_2$. Верхнюю грань b элементов a_1, a_2 назовем минимальной верхней гранью этих элементов, если ни для какой другой верхней грани x этих элементов не выполняется неравенство $b > x$. Будем говорить, что элементы $a_1, a_2, b_1, b_2, c_1, c_2 \in \mathcal{P}$ обладают p-свойством, если элементы a_1, a_2 несравнимы, b_1, b_2 — минимальные верхние грани элементов a_1, a_2, а элементы c_1, c_2 — минимальные верхние грани элементов b_1, b_2.

Пусть $\mathcal{P}$ — частично упорядоченное множество. Положим $w_{\mathcal{P}} = \max |J|$, где максимум берется по всем антицепям J из $\mathcal{P}$, величина $w_{\mathcal{P}}$ называется шириной множества $\mathcal{P}$.

Обозначим через $\mathbb{A}_0$ семейство всех частично упорядоченных множеств с наименьшим и наибольшим элементами. Пусть $\mathcal{M}_{\mathcal{P}}$ — класс всех функций, монотонных на множестве $\mathcal{P}$. Известно [1], что для любого множества $\mathcal{P} \in \mathbb{A}_0$ класс $\mathcal{M}_{\mathcal{P}}$ является предполным. Обозначим через $\mathbb{P}_0$ семейство всех таких частично упорядоченных множеств $\mathcal{P}$ с наименьшим и наибольшим элементами, для которых выполняется неравенство $w_{\mathcal{P}} \leq 2$. Отметим, что семейству $\mathbb{P}_0$ принадлежит множество, приведенное в работе [5].

Теорема 1 [8, 9]. *Пусть $\mathcal{P} \in \mathbb{P}_0$. Класс $\mathcal{M}_{\mathcal{P}}$ является конечно порожденным тогда и только тогда, когда множество $\mathcal{P}$ не содержит шестерку элементов, обладающих p-свойством.*

Обозначим через через $\mathbb{A}_1$ семейство всех множеств $\mathcal{P}$ из $\mathbb{A}_0$ следующего вида: $\mathcal{P} = P_1 \cup \ldots \cup P_m$, $m \geq 2$, $|P_1| = |P_m| = 1$, для каждого $i = 2, \ldots, m-1$ выполняется неравенство $|P_i| \geq 2$, и любые два элемента $a, b \in P_i$ несравнимы, а для любых i, j, $1 \leq i < j \leq m$, и для любых элементов $a \in P_i$ и $b \in P_j$ выполняется неравенство $a < b$.

Определим две операции над множествами с наименьшим и наибольшим элементами. Пусть $\mathcal{R}_1$ и $\mathcal{R}_2 \in \mathbb{A}_0$. Наименьший и наибольший элементы множества $\mathcal{R}_i$, обозначим через 0_i и 1_i соответственно, положим $\mathcal{R}_i' = \mathcal{R}_i \setminus \{0_i, 1_i\}$.

(1) Будем говорить, что множество $\mathcal{R}$ получено в результате последовательного соединения множеств $\mathcal{R}_1$ и $\mathcal{R}_2$, если $\mathcal{R} = \{0\} \cup \mathcal{R}_1' \cup \{\varepsilon\} \cup \mathcal{R}_2' \cup \{1\}$, и для любых элементов $a \in \mathcal{R}_1'$ и $b \in \mathcal{R}_2'$ выполняются неравенства $0 < a < \varepsilon < b < 1$.

(2) Будем говорить, что множество $\mathcal{R}$ получено в результате параллельного соединения множеств $\mathcal{R}_1$ и $\mathcal{R}_2$, если $\mathcal{R} = \{0\} \cup \mathcal{R}_1' \cup \mathcal{R}_2' \cup \{1\}$, любые два элемента $a \in \mathcal{R}_1'$ и $b \in \mathcal{R}_2'$ несравнимы, и выполняются неравенства $0 < a, b < 1$.

Определим семейство $\mathbb{A}_2$ конечных частично упорядоченных множеств следующим образом: $\mathbb{A}_1 \subset \mathbb{A}_2$, и если $\mathcal{R}_1, \mathcal{R}_2 \in \mathbb{A}_2$, и если множество $\mathcal{R}$ получено в результате применения операций (1) или (2) к множествам $\mathcal{R}_1$ и $\mathcal{R}_2$, то $\mathcal{R} \in \mathbb{A}_2$.

Теорема 2. *Пусть $\mathcal{P} \in \mathbb{A}_2$. Класс $\mathcal{M}_{\mathcal{P}}$ является конечно порожденным тогда и только тогда, когда множество $\mathcal{P}$ не содержит шестерку элементов, обладающих p-свойством.*

При доказательстве необходимости обобщается медод из [5]. Для доказательства достаточности показывается, что если $\mathcal{P} \in \mathbb{A}_2$, и если в множестве $\mathcal{P}$ нет шестерки элементов, обладающих p-свойством, то в классе $\mathcal{M}_{\mathcal{P}}$ содержится мажоритарная функция, откуда следует (см. [7]), что класс $\mathcal{M}_{\mathcal{P}}$ является конечно порожденным.

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

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

Список литературы

1. Rosenberg I. G. Über die funktionale Vollständigkeit in den mehrwertigen Logiken // Rozpr. ČSAV. MPV. — 1970. — V. 80. — P. 3–93.

2. Яблонский С. В., Гаврилов Г. П., Набебин А. А. Предполные классы в многозначных логиках. — М.: Изд-во МЭИ, 1997.

3. Lau D. Bestimmung der Ordnung maximaler Klassen von Funktionen der k-wertigen Logik // Z. math Log. und Grundl. Math. — 1978. — 24. — P. 79–96.

4. Lau D. Über partielle Funktionenalgebren // Rostok. math. Kolloq. — 1988. — 33. — 23–48.

5. Tardos G. A not finitely generated maximal clone of monotone operations // Order. — 1986. — V. 3. — P. 211–218.

6. Demetrovics J., Hannák L., Rónyai L. On algebraic properties of monotone clones // Order. — 1986. — V. 3. — P. 219–225.

7. Baker K., Pixley A. Polynomial interpolation and the Chinese remainder theorem for algebraic systems // Math. Z. — 1975. — V. 143. — P. 165–174.

8. Дудакова О. С. Об одном семействе предполных классов функций k-значной логики, не имеющих конечного базиса // Вестн. Моск. ун-та. Серия 1. Математика. Механика. — 2006. — № 2. — С. 29–33.

9. Дудакова О. С. О свойствах предполных классов монотонных функций k-значной логики // Труды VII Международной конференции "Дискретные модели в теории управляющих систем" (Покровское, 4–6 марта 2006 г.). — М.: МАКС Пресс. — 2006. — С. 107–113.

О СРЕДНЕЙ ГЛУБИНЕ МОНОТОННЫХ ФУНКЦИЙ

Р. Н. Забалуев (Москва)

В работе рассматривается средняя глубина деревьев решений, реализующих монотонные функции. Пусть E_2^n — множество всех двоичных наборов длины n. Множество двоичных наборов длины n, содержащих ровно t единиц, обозначим через $E_2^{n,t}$. *Деревом решений*, реализующим булеву функцию n переменных, называется ориентированное корневое дерево с конечным числом вершин, где

а) каждой внутренней вершине приписан символ одной из переменных $\{x_1, \ldots, x_n\}$;

б) каждая внутренняя вершина имеет ровно два исходящих ребра, помеченных числами из E_2 (в процессе решения двигаемся по тому ребру, значение которого совпадает со значением переменной, приписанной вершине);

в) каждой висячей (концевой) вершине приписано число из E_2 (значение функции).

Пусть Γ — дерево решений, реализующее булеву функцию f от n переменных. Нетрудно видеть, что для каждого набора $\tilde{\delta}$ из n переменных существует единственный путь в Γ, где выполняются вычисления для набора $\tilde{\delta}$. Будем говорить, что дерево решений *вычисляет* булеву функцию f, если для каждого набора $\tilde{\delta}$ из E_2^n концевой вершине пути, который соответствует набору $\tilde{\delta}$, приписано значение $f(\tilde{\delta})$. Обозначим через $l(\tilde{\delta})$ длину пути, соответствующего набору $\tilde{\delta}$. *Глубиной* и *средней глубиной* дерева решений Γ называются соответственно величины:

$$g(\Gamma) = \max_{\tilde{\delta} \in E_2^n} l(\tilde{\delta}) \quad \text{и} \quad h(\Gamma) = \frac{1}{2^n} \sum_{\tilde{\delta} \in E_2^n} l(\tilde{\delta}).$$

Для булевой функции f через $g(f)$ и $h(f)$ обозначим соответственно *минимальную глубину* и *минимальную среднюю глубину* дерева решений, реализующего f.

Пусть B — множество булевых функций. Рассмотрим функции

$$G_B(n) = \max\{g(f) : f \in B, \quad \dim f \le n\},$$

$$H_B(n) = \max\{h(f) : f \in B, \quad \dim f \le n\},$$

где $\dim f$ — это число аргументов функции f. Функции характеризуют худший случай роста минимальной глубины и минимальной

средней глубины деревьев решений, реализующих функции из B, при росте числа аргументов. Заметим, что $H_B(n) \le G_B(n)$.

В работе Чикалова [1] для класса монотонных функций M получены следующие оценки средней глубины

$$n+1-\sqrt{n+1} \le H_M(n) \le n - \lfloor n/2 \rfloor 2^{-n/2}.$$

В данной работе получено улучшение верхней оценки для величины $H_M(n)$. Показано, что средняя глубина каждой монотонной функции существенно меньше, т. е. отличается на бесконечно растущую по числу аргументов величину, чем $G_M(n) = n$.

Отметим, что подобный эффект наблюдается [2] для класса монотонных функций при оценке средней сложности: средняя сложность каждой монотонной функции при растущем числе аргументов гораздо меньше чем сложность реализации схемами из функциональных элементов самой сложной монотонной функции.

Также в данной работе показано, что верхняя оценка средней глубины для почти каждой монотонной функции совпадает с нижней оценкой $H_M(n)$ с точностью до порядка второго члена при растущем числе аргументов.

Теорема 1. *Для почти каждой функции $f(x_1, \dots, x_n) \in M$ при $n \to \infty$ выполнено*

$$h(f) \le n - \sqrt{\frac{2n}{\pi}} + o(\sqrt{n}).$$

Через $f_{i_1}^{\delta_1} \dots {}_{i_k}^{\delta_k}$ обозначим функцию $n-k$ переменных, получающуюся из функции $f(x_1, \dots, x_n)$ подстановкой двоичных значений $\delta_1, \dots, \delta_k$ вместо переменных $x_{i_1}, \dots, x_{i_k}$ соответственно, при этом нумерация переменных, в которые значения подставлены не были, не меняется.

Лемма 1. *Пусть $f(x_1, \dots, x_n) \in M$. Тогда существуют такие числа $i_1, \dots, i_k$ $(2 \le k \le n)$, что количество наборов, на которых функции $f_{i_1}^1 \dots {}_{i_k}^1$ и $f_{i_1}^0 \dots {}_{i_k}^0$ не совпадают, не превосходит величины*

$$\frac{n+1}{2n}\binom{n}{\lceil n/2 \rceil}.$$

Доказательство этой леммы аналогично доказательству леммы из [3] для $k = 2$.

Теорема 2. *Для каждой функции $f(x_1, \dots, x_n) \in M$ при достаточно больших n выполнено*

$$h(f) \le n - \frac{1}{2} \cdot \log_2 n + 3 \log_2 \log_2 n.$$

Доказательство. Будем строить дерево решений для функции $f \in M$, используя лемму 1. Пусть k — целочисленный параметр, который мы выберем позже. Пусть $i_1, \dots, i_k$ — числа, найденные по лемме 1. Можно считать, что $i_1 = n-k+1, \dots, i_k = n$. Через R обозначим множетсво наборов длины $n-k$, найденных по лемме 1, на которых функции $f_{n-k+1}^1 \dots {}_n^1$ и $f_{n-k+1}^0 \dots {}_n^0$ не совпадают. Тогда

$$|R| \le \frac{n+1}{2n}\binom{n}{\lceil n/2 \rceil}.$$

Допустим Γ — произвольное дерево решений для f. Пусть $\tilde{\delta} = (\delta_1, \dots, \delta_n) \in E_n \setminus R$. Дерево Γ преобразуем к дереву Γ'следующим образом: вершину, которая соединяется путем, соответствующим набору длины $n-k+1$ $(\delta_1, \dots, \delta_{n-k}, 1)$, заменим на висячую вершину и припишем ей значение $f(\delta_1, \dots, \delta_{n-k}, 1, \dots, 1)$; вершину, которая соединяется путем соответствующим набору $(\delta_1, \dots, \delta_{n-k}, 0)$, заменим на висячую вершину и припишем ей значение $f(\delta_1, \dots, \delta_{n-k}, 0, \dots, 0)$. Поскольку

$$f(\delta_1, \dots, \delta_{n-k}, 0, \dots, 0) = f(\delta_1, \dots, \delta_{n-k}, 1, \dots, 1),$$

то дерево Γ' также реализует функцию f. Теперь оценим среднюю глубину дерева Γ':

$$h(\Gamma') = \frac{1}{2^n}\left(\sum_{\tilde{\delta} \in E_n \setminus R} (n-k) + \sum_{\tilde{\delta} \in R} n\right) \le$$

$$\le \frac{1}{2^n}\left((n-k)\left(2^n - \frac{n+1}{2n}\binom{n}{\lceil n/2 \rceil} \cdot 2^k\right) + n \cdot \frac{n+1}{2n}\binom{n}{\lceil n/2 \rceil} \cdot 2^k\right) \le$$

$$\le \frac{1}{2^n}\left((n-k)2^n + k \cdot \frac{n+1}{2n}\binom{n}{\lceil n/2 \rceil} \cdot 2^k\right).$$

Положим $k = \lfloor \frac{1}{2}\log_2 n - 2\log_2 \log_2 n \rfloor$. Тогда при достаточно больших n выполнено

$$h(\Gamma') \le n - \frac{1}{2} \cdot \log_2 n + 3 \log_2 \log_2 n.$$

Теорема доказана.

Следствие. *При достаточно больших n выполнено*

$$H_M(n) \le n - \frac{1}{2} \cdot \log_2 n + 3 \log_2 \log_2 n.$$

Работа выполнена при финансовой поддержке РФФИ (проект № 05-01-00994), программ «Ведущие научные школы РФ» (проект НШ-1807.2003.1) и «Университеты России» (проект УР.04.02.528) и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики» (проект «Оптимальный синтез управляющих систем»).

Список литературы

1. Chikalov I. On the average depth of DT implementing Boolean functions // Fundamenta Informaticae. — 2000. — V. 50. — P. 265–284.

2. Забалуев Р. Н. О средней сложности монотонных функций // Дискретная математика. — 2006. — Т. 18, вып. 2. — С. 71–83.

3. Чашкин А. В. О сложности реализации булевых функций формулами // Дискрет. анализ и исслед. операций. Серия 1. — 2005. — Т. 12, № 2. — С. 75–91.

ИНДУКТИВНОЕ ОПИСАНИЕ КЛАССА ПЛАНАРНЫХ ГРАФОВ

М. А. Иорданский (Нижний Новгород)

Рассматриваются связные планарные графы. Используются следующие обозначения: K_n — n-вершинный полный обыкновенный граф; $K_{n,m}$ — полный двудольный граф, доли которого содержат n и m вершин; C_1 — петля. *Оболочкой* подграфа $G' \subset G$ называется подграф, порожденный ребрами множества $E(G) \backslash E(G')$.

Используется конструктивный подход к представлению графов, основывающийся на построении одних графов из других с помощью бинарных операций склейки, отождествляющих изоморфные подграфы графов-операндов [1]. Для графа G, полученного в результате склейки графов G_1 и G_2 по подграфам, изоморфным графу $\tilde{G}$, используется обозначение $G \Leftarrow (G_1 \circ G_2)\tilde{G}$. Граф G реализуем Q-суперпозицией графов из P, если его можно получить из графов множества P путем последовательного применения операций склейки по графам $\tilde{G} \in Q$.

Пусть G_Γ — подграф планарного графа G, образующий границу связной грани Γ в некоторой плоской укладке графа G. Каждый планарный граф G допускает плоскую укладку, в которой все вершины грани Γ можно расположить на окружности, вписанной в эту грань, в порядке кругового обхода грани [1]. В этой же работе было показано, что для сохранения свойства планарности при выполнении операций склейки достаточно чтобы отождествляемые вершины принадлежали подграфам G_Γ в графах-операндах и пары отождествляемых вершин выбирались в соответствии с круговыми обходами окружностей, вписанных в грани, соответствующие подграфам G_Γ. В последующих работах удалось избавиться от указанных геометрических представлений. Было предложено теоретико-множественное описание подграфов G_Γ [2] и введена процедура *db*-поиска в глубину [3], отличающаяся от стандартной использованием следующих ограничений:

1) если есть другие возможности, не выбирать ребер, являющихся мостами в непройденном подграфе исходного графа;

2) среди ребер, являющихся мостами, не выбирать тех, которые принадлежат двусвязным компонентам исходного графа, если есть другие возможности.

В [4] было установлено, что каждый планарный граф G допускает плоскую укладку, в которой все вершины подграфа G_Γ расположены на окружности, вписанной в Γ, в порядке их перечисления при произвольном *db*-поиске в глубину на G_Γ.

В данной работе на основе этих результатов доказана

Теорема. *Планарными графами являются:*

1. *Графы K_1, C_1 и K_2.*

2. *Все графы $G \Leftarrow (G_1 \circ G_2)\tilde{G}$, если*

a) G_1 и G_2 — планарные графы;

b) отождествляемые вершины принадлежат подграфам $G'_1 \subseteq G_1$ и $G'_2 \subseteq G_2$, обладающим следующими свойствами:

i) G'_1 и G'_2 реализуемы $\{K_1\}$-суперпозициями простых циклов и максимальных (по включению) деревьев;

ii) оболочки подграфов G'_1 и G'_2 не содержат цепей, соединяющих вершины, принадлежащие разным циклам или вершины, принадлежащие циклам, с вершинами, не принадлежащими циклам, а также не содержат цепей, соединяющих вершины максимальных деревьев, использовавшихся при построении G'_1 или G'_2;

iii) G_1 *и* G_2 *не содержат подграфа, гомеоморфного* $K_{2,3}$*, большую долю в котором образуют вершины, принадлежащие одному циклу в* G'_1 *или* G'_2

iiii) G_1 *и* G_2 *не содержат подграфа, гомеоморфного* K_4*, в котором все вершины степени три принадлежат одному циклу из* G'_1 *или* G'_2;

c) пары отождествляемых вершин выбираются в соответствии с порядком их перечисления при произвольном db-поиске в глубину на подграфах G'_1 *и* G'_2;

d) пары отождествляемых ребер выбираются из множества кратных ребер, образующихся в результате отождествления вершин.

Других планарных графов нет.

Работа выполнена при финансовой поддержке РФФИ (проект 04-01-00374).

Список литературы

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

2. Иорданский М. А. Теоретико-множественное описание подграфов граней планарных графов // Проблемы теоретической кибернетики. Тезисы докладов XIV Международной конференции (Пенза, 23–28 мая 2005 г.). — М.: Изд-во механико-математического факультета МГУ, 2005. — С. 56.

3. Иорданский М. А. Поиск в глубину и одностраничные укладки графов // Проблемы теоретической кибернетики. Тезисы докладов XIII Международной конференции (Казань, 27–31 мая 2002 г.). Часть I. — М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2002. — С. 76.

4. Иорданский М. А. Свойства плоских укладок планарных графов // Дискретные модели в теории управляющих систем: VII Международная конференция, Покровское, 4–6 марта 2006 г.: Труды. — М.: МАКС Пресс, 2006. — С. 136–138.

ЧИСЛО КЛАССОВ БУЛЕВЫХ ФУНКЦИЙ, ПОРОЖДЕННЫХ ОПЕРАТОРНЫМИ ОТОБРАЖЕНИЯМИ

А. С. Казимиров (Иркутск)

Одной из задач построения классификаций является задача перечисления, то есть определения числа классов, порождаемых той или иной группой отображений.

Задача перечисления обычно решается с помощью теории перечисления Пойа и не требует нахождения самих представителей. В частности, теорема Пойа применяется для получения числа классов по N-, P-, PN-, линейным и аффинным отображениям [1]. Она дает формулу для числа классов через цикловые индексы групп отображений.

Но данную теорему не удается применить к S-отображениям, так как они не являются подстановками на множестве наборов, что является одним из условий теоремы Пойа.

Для подсчета числа S-классов можно использовать лемму Бернсайда, которая является отправной точкой теоремы Пойа и которая не требует, чтобы отображения представляли собой подстановки на множестве наборов.

Определение [2]. Под *оператором* a на множестве булевых функций n переменных будем понимать последовательность $a_1 \dots a_n$, в которой $a_i \in \{d, e, p\}$. Действие оператора a на функцию $f(x_1, \dots, x_n)$ определяется по правилу: $a(f(x_1, \dots, x_n)) = f_n(x_1, \dots, x_n)$, где $f_0(x_1, \dots, x_n) = f(x_1, \dots, x_n)$ и

$$f_i(x_1, \dots, x_n) = \begin{cases} f_{i-1}(x_1, \dots, x_n), & \text{если } a_i = e; \\ f_{i-1}(x_1, \dots, x_{i-1}, \bar{x}_i, x_{i+1}, \dots, x_n), & \text{если } a_i = p; \\ (f_{i-1}(x_1, \dots, x_n))'_{x_i}, & \text{если } a_i = d. \end{cases}$$

Здесь через $f'_{x_i}(x_1, \dots, x_n)$ обозначается производная функции $f(x_1, \dots, x_n)$ по переменной x_i.

Пусть имеется представление функции $f(x_1, \dots, x_n)$ в виде полиномиальной нормальной формы:

$$f(x_1, \dots, x_n) = \sum_{i=1}^{s} K_i, \qquad (1)$$

в которую в качестве слагаемых входят элементарные конъюнкции — произведения $K_i = z_1 \cdot \dots \cdot z_{k_i}$, где $z_j = x_t$ или $z_j = \overline{x}_t$ для некоторой переменной x_t, причем переменная может входить в

произведение не более одного раза. В сумму может входить слагаемое K_i, не содержащее ни одной переменной. Такое K_i считается равным 1.

Поскольку любая элементарная конъюнкция является образом некоторого оператора от $x_1 \cdot \dots \cdot x_n$, то представление (1) может быть записано в виде операторной формы:

$$f(x_1, \dots, x_n) = \sum_{i=1}^{s} a^i(x_1 \cdot \dots \cdot x_n),$$

где a^i — соответствующие операторы.

Пусть S — полная группа подстановок на множестве $\{d, e, p\}$:

$$S = \left\{ \begin{pmatrix} dep \\ dep \end{pmatrix}, \begin{pmatrix} dep \\ dpe \end{pmatrix}, \begin{pmatrix} dep \\ ped \end{pmatrix}, \begin{pmatrix} dep \\ edp \end{pmatrix}, \begin{pmatrix} dep \\ epd \end{pmatrix}, \begin{pmatrix} dep \\ pde \end{pmatrix} \right\}.$$

Введем следующие обозначения для элементов группы S:

$$\iota = \begin{pmatrix} dep \\ dep \end{pmatrix}, \delta = \begin{pmatrix} dep \\ dpe \end{pmatrix}, \varepsilon = \begin{pmatrix} dep \\ ped \end{pmatrix}, \pi = \begin{pmatrix} dep \\ edp \end{pmatrix}, \mu = \begin{pmatrix} dep \\ epd \end{pmatrix}, \nu = \begin{pmatrix} dep \\ pde \end{pmatrix}$$

Определим отображение φ операторов размерности n в виде последовательности $\varphi_1 \dots \varphi_n$, где $\varphi_i \in S$. Тогда φ действует на оператор $a = a_1 \dots a_n$ следующим образом: $\varphi(a) = \varphi_1(a_1) \dots \varphi_n(a_n)$. Таким образом построенное отображение φ назовем S-отображением.

Действие S-отображений распространяется на множество функций следующим образом. Пусть $f(x_1, \dots, x_n) = \sum_{i=1}^{s} a^i(x_1 \cdot \dots \cdot x_n)$ — некоторая операторная форма функции. Тогда $\varphi(f) = \sum_{i=1}^{s} \varphi(a^i)(x_1 \cdot \dots \cdot x_n)$.

Множество S-отображений n-местных функций является группой. Обозначим группу S-отображений n-местных функций через G_n. Порядок группы G_n равен 6^n.

Определение. Две функции $f(x_1, \dots, x_n)$ и $g(x_1, \dots, x_n)$ называются *S-эквивалентными*, если существует $\varphi \in G_n$, что $\varphi(f) = g$.

Все функции n переменных разбиваются на классы S-эквивалентных функций, называемые S-классами. S-отображения интересны тем, что сохраняют сложность полиномиальной формы (по числу слагаемых).

Действие любого S-отображения φ на функцию f эквивалентно умножению вектора функции на матрицу, соответствующую этому отображению [3]. Обозначим матрицу отображения φ через $A(\varphi)$.

Одноместным S-отображениям будут соответствовать следующие матрицы:

$$I = A(\iota) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, D = A(\delta) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$E = A(\varepsilon) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, P = A(\pi) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$M = A(\mu) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, N = A(\nu) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix};$$

n-местные S-отображения получаются из этих матриц с помощью кронекерова произведения ($\otimes$).

Например, отображению $\delta\pi$ будет соответствовать матрица

$$D \otimes P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \left(\begin{array}{c|c} O & P \\ \hline P & O \end{array}\right) = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Матрицы S-отображений являются невырожденными.

Введем следующее обозначение для кронекеровой степени матрицы A:

$$\underbrace{A \otimes A \otimes \dots \otimes A}_{n} = A^{\otimes n}$$

Определение. Функция f называется *инвариантной* по отображению φ, если $\varphi(f) = f$.

Обозначим через $st(\varphi)$ количество функций, инвариантных по n-местному отображению φ. Пусть отображение φ представимо матрицей A, тогда имеет место следующее утверждение.

Утверждение 1. *$st(\varphi) = 2^{2^n - rank(A \oplus I^{\otimes n})}$, где $rank(A)$ — ранг матрицы A.*

Доказательство этого утверждения следует из того факта, что уравнение $\varphi(f) = f$ эквивалентно уравнению $Af = I^{\otimes n} f$, поскольку матрица $I^{\otimes n}$ является единичной матрицей размерности 2^n.

Утверждение 2. *$st(\varphi_1 \varphi_2 \dots \varphi_n) = st(\varphi_{i_1} \varphi_{i_2} \dots \varphi_{i_n})$, где $\{i_1, i_2, \dots, i_n\}$ — некоторая перестановка чисел $\{1, 2, \dots, n\}$.*

Данное равенство имеет место, поскольку между множествами инвариантных функций по каждому из указанных в условии отображений можно установить взаимно однозначное соответствие: если функция $f(x_1, \dots, x_n)$ инвариантна по отображению $\varphi_1 \varphi_2 \dots \varphi_n$, то функция $f(x_{i_1}, \dots, x_{i_n})$ инвариантна по отображению $\varphi_{i_1} \varphi_{i_2} \dots \varphi_{i_n}$.

Все подстановки из группы S можно разбить на 3 типа — тождественная $\{\iota\}$, транспозиции $\{\delta, \varepsilon, \pi\}$ и циклы $\{\mu, \nu\}$.

Утверждение 3. *$st(\varphi_1\varphi_2\dots\varphi_n) = st(r(\varphi_1\varphi_2\dots\varphi_n)$, где $r(\varphi_1\varphi_2\dots\varphi_n) = r(\varphi_1)r(\varphi_2)\dots r(\varphi_n)$ и*

$$r(\varphi_i) = \begin{cases} \iota, & \text{если } \varphi_i = \iota; \\ \delta, & \text{если } \varphi_i \in \{\delta, \varepsilon, \pi\}; \\ \mu, & \text{если } \varphi_i \in \{\mu, \nu\}. \end{cases}$$

Легко проверяется, что матрицы $A(\varphi) \oplus I^{\otimes n}$ и $A(r(\varphi)) \oplus I^{\otimes n}$ сводятся одна к другой линейными преобразованиями строк и столбов.

Поэтому в дальнейшем можно рассматривать только S-отображения вида $\iota\dots\iota\delta\dots\delta\mu\dots\mu$.

Число инвариантных функций для отображений такого вида можно найти с использованием следующих утверждений.

Утверждение 4. $rank(M^{\otimes n} \oplus I^{\otimes n}) = \frac{2}{3}(2^n + (-1)^{n+1})$.

Утверждение 5. $rank((D \otimes M^{\otimes n}) \oplus I^{\otimes n+1}) = \frac{1}{3}(5\cdot 2^n + 2\cdot(-1)^{n+1})$.

Утверждение 6. $rank((D^{\otimes 2} \otimes A) \oplus I^{\otimes n}) = 2 \cdot rank((D \otimes A) \oplus I^{\otimes n-1})$, *где A — матрица некоторого отображения из G_{n-2}.*

Утверждение 7. $rank((I \otimes A) \oplus I^{\otimes n}) = 2 \cdot rank(A \oplus I^{\otimes n-1})$, *где A — матрица некоторого отображения из G_{n-1}.*

Существенную часть теории Пойа составляет следующее утверждение, называемое леммой Бернсайда. Данная лемма, в отличие от теоремы Пойа, не требует, чтобы отображения являлись подстановками на множестве наборов.

Лемма Бернсайда [4]. *Для числа классов $K(G)$, порожденных группой G, выполняется соотношение:*

$$K(G) = \frac{1}{|G|} \sum_{\varphi \in G} st(\varphi).$$

Из этой леммы и утверждений 1–7 вытекает следующая теорема.

Теорема. *Число S-классов K_n булевых функций n переменных выражается формулой*

$$K_n = \frac{1}{6^n} \sum_{i=0}^{n} C_n^i 2^i \left((4^{n-i} - 1) \cdot 2^{2^{n-i}(2^i + 2(-1)^i)/6} + 2^{2^{n-i}(2^i + 2(-1)^i)/3} \right).$$

Для K_n справедлива асимптотическая оценка $K_n \sim 2^{2^n}/6^n$.

Работа выполнена при финансовой поддержке РФФИ, проект 04-07-90178в.

Список литературы

1. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004.

2. Избранные вопросы теории булевых функций / Под ред. Винокурова С. Ф. и Перязева Н. А. — М.: ФИЗМАТЛИТ, 2001.

3. Казимиров А. С. Оценка числа классов LP-эквивалентности булевых функций // Вестник Бурятского университета: Математика и информатика. Серия 13. — Улан-Удэ: Бурятский государственный ун-т, 2005. — Вып. 2. — С. 17–22.

4. ДеБрейн Н. Дж. Теория перечислений Пойа // Прикладная комбинаторная математика / Сб. статей под ред. Беккенбаха Э. — М.: Мир, 1968. — С. 61–106.

НИЖНЯЯ ОЦЕНКА ДЛИНЫ ЗАПИСИ ИНТЕРПРЕТАТОРА n-ПРОГРАММ

Н. К. Косовский (Санкт-Петербург)

Доказывается, что любая процедура языка Паскаль,которая может быть реализована на памяти, ограниченной константой, может быть доопределена до всюду применимой процедуры на языке Паскаль, что находится в оппозиции с аналогичным утверждением в теории алгоритмов. Это позволяет надеяться на создание математической теории программ, существенно отличающейся от теории алгоритмов и имеющей большее практическое значение.

Кто-то из классиков утверждал, что в каждой науке столько науки, сколько в ней математики. Возможно, в настоящее время можно было бы сказать "математического моделирования" вместо "математики".

Развивая указанную идею классика можно утверждать, что сейчас у каждой математической модели столько массового использования, сколько для нее "запускается" компьютерных программ.

В последнее время активно начали исследоваться способы безопасного функционирования различных программ. Первая теорема этой работы касается безопасности программы от бесконечного зацикливания.

Под программой ниже понимается программа, написанная на языке Паскаль и использующая при своей работе память, ограниченную возможностями компьютера.

Исходную программу необходимо преобразовать следующим образом: во всех процедурах вводится дополнительный параметр,

позволяющий занумеровать все конструкции возможного бесконечного зацикливания программы, в которых вводится вызов процедуры *counter*, которая подсчитывает в массивах x1, ..., xp число обращений к ней.

Предлагается математическое моделирование процедур-операторов, написанных на используемых фрагментах языка Паскаль.

Имеется несколько способов математического моделирования программ:

1) понятие алгоритма некоторого класса [1],

2) понятие схемы программ.

Ниже предлагается понятие n-программы (процедуры) при любом положительном целом n, которое более адекватно общепринятому термину "программа", у которого, как правило, содержание меняется от версии к версии транслятора с языка Паскаль.

Доказан ряд теорем о свойствах n-программ и n-интерпретатора n-программ с двумя аргументами.

Вводится математическое понятие целочисленной n-программы на языке Паскаль [2] как программы, длина записи которой не превосходит nK, где $K = 1024$, и работа которой осуществляется для аргументов и результатов, длины записи которых не превосходят nK. Это математическое понятие является более адекватной формализацией понятия программы, нежели математическое понятие алгоритма, даже специально приближенное к компьютеру (ср., например, с [3]).

Следует отметить, что учебные программы являются, как правило, 1-программами. Программы, написанные в качестве курсовых работ могут быть 2-программами. В дипломных работах могут разрабатываться 3-программы и 4-программы и т. д.

Для вводимого понятия n-программы доказывается теоретическая возможность его доопределения до всюду применимой m-программы, где m больше, чем n.

Ниже доказана линейная относительно n нижняя оценка длины записи всюду применимого n-интерпретатора для фрагментов языка Паскаль, использующих заранее заданный объем памяти.

Здесь речь идет об интерпретаторах программ, написанных на фрагменте языка Паскаль и реализованной средствами этого же фрагмента языка Паскаль. Такие интерпретаторы разрабатываются при использовании метода "раскрутки" для создания интерпретатора, написанного в результате на языке ассемблер или на языке стековой машины.

Известно, что интерпретаторы оказываются достаточно длинными программами.

Доказанная ниже теорема 2 дает нижнюю оценку длины записи интерпретатора, тем самым обеспечивая теоретический фундамент

последнему утверждению-наблюдению.

Программы, являясь,вообще говоря, математическими объектами, отличаются от алгоритмов не столько тем, что они пишутся на конкретных языках программирования, сколько тем, что они могут использовать лишь заранее ограниченный объем исходных данных, записанный, например, на диске.

Для программы, написанной на языке Паскаль, перечень имен процедур и (или) функций называется совместно рекурсивным, если каждое из описаний их тела содержит хотя бы один вызов процедур и (или) функций из этого перечня. Перечень, состоящий из одного имени, естественно называть рекурсивным.

Определение. Назовем *n-программой* (*n-процедурой, n-оператором*) такую программу (процедуру, оператор), которая использует только память в виде массивов с элементами типа *integer*, суммарное количество элементов которых не превосходит nK. Каждый аргумент и результат работы программы имеет такую же верхнюю границу числа элементов (напомним, что $K = 1024$).

Теорема 1. *Каковы бы ни были целое положительное число n и n-программа, существуют целое положительное число m ($m > n$) и m-программа (с теми же аргументами) такие, что для любых значений аргументов применима m-программа. При этом если исходная n-программа применима к этим исходным данным, то результаты работы обеих программ совпадают.*

Доказательство. Пусть $|P|_0$ означает количество в программе P точек всех вариантов возможного бесконечного зацикливания.

Выполнение программы, записанной в строку, может рассматриваться как продвижение некоторого указателя ее выполнения от одной конструкции к другой, как правило слева направо, а также справа налево для организации возвращений по тексту программы, включая обращение к процедурам и функциям.

Программа зацикливается, если в процессе ее работы в какой-либо точке ее выполнения дважды появляется одинаковое содержимое памяти компьютера (включая память, отводимую для входного файла).

Пусть новая программа останавливается при превышении количества посещений точек всех вариантов возможного бесконечного зацикливания больше $|P|_0$, умноженной на число всех различных вариантов содержимого памяти компьютера. Поэтому в начале программы описываем переменную b типа int, и переменные $x1, \ldots, xp$: $array\ [-2^{15}..2^{15}-1]\ of\ int$.

Пусть $exit$ — оператор выхода из цикла.

Определим следующую программу.

```
procedure counter (var x1, ..., xp: array of int);
begin
b := 0;
for i := -2^15 to 2^15 - 1 do
  begin if x1[i] <> 2^15 - 1 then begin x1[i] := x1[i] + 1; b :=
1; exit end
        else x1[i] := 0;
  end;
if b = 0 then
     for i := -2^15 to 2^15 - 1 do
       begin if x2[i] <> 2^15 - 1 then begin x2[i] := x2[i] + 1; b :=
1; exit end
             else x2[i] := 0;
     end;
.....
if b = 0 then
     for i := -2^15 to 2^15 - 1 do
       begin if xp[i] <> 2^15 - 1then begin xp[i] := xp[i] + 1; b :=
1; exit end
             else xp[i] := 0;
     end; if b = 0 then stop end
```

Более точно, обращение к процедуре *counter* следует вставить сразу перед *end* в блоке, являющемся телом цикла типа *while* (если тело цикла на является блоком, то заключить его в операторные скобки *begin* - *end*) сразу перед *until*, *goto* назад, в начале тела рекурсивной или совместно рекурсивной процедуры и функции. Теорема доказана.

Под записью программы будем понимать массив ASCII-кодов букв, причем последней дополнительной буквой (литерой) записи программы является точка.

Пусть $\mathbf{P_n}$ – множество n-программ, написанных на некотором фрагменте языка Паскаль и имеющих не более трех аргументов – массивов с элементами типа *integer*. При этом длина записи программы из $\mathbf{P_n}$, длина записи исходных данных, дополнительная память и длина записи результата суммарно не превосходят nK.

Определение. Назовем *n-интерпретатором* процедуру-оператор INT от трех параметров, если для любой программы $P \in \mathbf{P_n}$, и исходных данных x, таких, что длина записи программы P не превосходит nK, длина записи x не превосходит nK и длина записи результата $P(x)$ не превосходит nK выполняется свойство

$$!P(x) \Rightarrow\ !INT(\text{"}P\text{"}, x, result),$$

где символ ! заменяет слова "заканчивает работу", а "P" означает запись в ASCII-кодах программы с именем P. Кроме того, при любом y с тем же свойством

$$!P(y) \Rightarrow\ (INT(\text{"}P\text{"}, y, result)\{result = P(y)\}).$$

Все это при условии, что в процессе работы программы P с данными y не требуется ни на каком шаге дополнительная память, превосходящая nK по суммарному числу элементов массивов целочисленных переменных.

(Заключение импликации означает, что если указанное обращение к процедуре INT заканчивает свою работу, то после ее завершения имеет место равенство $result = P(x)$.)

Рассмотрим фрагмент всюду применимых процедур языка Паскаль, который содержит по крайней мере составной оператор ";", обращение к процедуре и оператор добавления к элементу массива константы. Пусть $|INT|$ обозначает длину записи процедуры INT, то есть количество символов в записи текста процедуры.

Для любого фрагмента языка Паскаль, расширяющего описанный фрагмент, приведенная ниже теорема 2 превращается в нижнюю оценку длины записи всюду применимого n-интерпретатора этого фрагмента, написанного на этом же фрагменте языка Паскаль.

Теорема 2. *Для всякого целого положительного числа n n-интерпретатор INT описанного фрагмента языка Паскаль, написанный на этом же фрагменте, не может быть всюду применимой n-процедурой, если $nK \geq |INT| + K$.*

Работа частично выполнена в лаборатории СПбГУ СПРИНТ, созданной при поддержке фирмы INTEL.

Список литературы

1. Косовский Н. К. Основы теории элементарных алгоритмов. — Л.: ЛГУ, 1987.

2. Абрамов В. Г., Трифонов Н. П., Трифонова Г. Н. Введение в язык Паскаль. — М.: "Наука", 1988.

3. Косовский Н. К. Элементы математической логики и ее приложения к теории субрекурсивных алгоритмов. — Л.: ЛГУ, 1981.

ОЦЕНКА ПАМЯТИ, НЕОБХОДИМОЙ ДЛЯ ИСКЛЮЧЕНИЯ БЕСКОНЕЧНОГО ЗАЦИКЛИВАНИЯ В ПАСКАЛЬ-ПРОГРАММАХ, ВЫПОЛНЯЕМЫХ НА КОМПЬЮТЕРЕ

Н. К. Косовский, Фам Тхань Лам (Санкт-Петербург)

Производится оценка дополнительной памяти, достаточной для безопасности от бесконечного зацикливания любых Паскаль-программ [1]. Доказывается теорема о доопределении любых Паскаль-программ, выполняемых на компьютере, до всегда заканчивающих свою работу.

Введем понятие точки вариантов возможного незавершения какой-либо конструкции языка Паскаль в записи программы P_n и обозначаем их число $|P_n|_0$. Таких точек достаточно, следующих:

- Перед каждым оператором goto назад.
- Перед каждым телом цикла типа repeat.
- Перед каждым do в цикле типа while.
- В начале каждого тела функции и(или) процедуры, которые совместно рекурсивно вычисляются.(определяются совместной рекурсией или рекурсивным образом.)

Теорема. *Пусть P_n — программа на языке Паскаль, во время выполнения которой отведена память для переменных объемом nK чисел, при этом разница между наибольшим и наименьшим числом не больше 2^M. Здесь $K = 1024$. При $mK \geq \lceil \frac{1}{M} \log_2 (|P_n|_0) \rceil + nK + 1$ построена программа P_m, которая всюду применима. Если исходная программа применима к этим исходым данным, то результаты обеих программ совпадают. Таким образом P_m — расширение P_n.*

Доказательство. Достаточно рассмотреть случай когда P_n зацикливается. Тогда $|P_n|_0 \geq 1$. Известно, что в каждый момент процесса работы P_n определяются такие параметры:

- Положение указателя на начало тела выполняемой конструкции программы.
- Содержание памяти компьютера.

P_n зацикливается, если в процессе ее работы в какой-нибудь точке её выполнение дважды появляется одинаковое содержание памяти компьютера. Посчитаем сколько различных возможных содержаний памяти. Внутреннюю память представим как множество массивов

типа integer. Пусть арифметические операции осуществляются по модулю 2^M (обычно M=16). Всего 2^{MnK} состояний.

Ясно по приципу Дирихле, что если количество посещений точек вариантов возможного незавершения в программе превосходит $2^{MnK}|P_n|_0$, то программа P_n зацикливается бесконечным образом.

Преобразуем P_n так, что в процессе ее работы подсчитывалось количество посещений точек вариантов возможного незавершения в программе. Добавим массив (возможно несколько массивов, поскольку каждый массив не может содержать больше чем 2^M элементов), предзначенный для подсчета количества посещений точек вариантов возможного незавершения в программе.

Количество элементов массива может быть равно $\lceil \frac{1}{M} \log_2 (|P_n|_0) \rceil + nK + 1$.

Полученная программа с этим дополнением станет всюду применимой программой, если программа будет останавливаться при превышении количества посещений точек вариантов возможного незавершения указанной выше величины. Теорема доказана.

Из доказательства теоремы следует, что она имеет место для многих языков программирования, выполняемых на компьютере и имеющих механизм отведения используемой памяти, например, копилка в Рефал-2 [2], Рефал-5 [3].

Работа частично выполнена в лаборатории СПБГУ СПРИНТ, созданной при поддержке фирмы Intel.

Список литературы

1. Borland Pascal. Руководство пользователя. — `http://www.cit-forum.ru/programming/bp70-ug/`

2. Алешин А. Ю., Красовский А. Г., Роменко С. А., Шерстнев В. Ю. Рефал-2. Руководство пользователя. — М , 1991. — `htttp://www.refal.net.`

3. Турчин В. Ф. Руководство по программированию Рефал-5. — `http://www.refal.org/rf5_frm.htm.`

О СЛОЖНОСТИ СОВМЕСТНОГО ВЫЧИСЛЕНИЯ ДВУХ ЭЛЕМЕНТОВ СВОБОДНОЙ АБЕЛЕВОЙ ГРУППЫ

В. В. Кочергин (Москва)

Пусть свободная абелева группа (групповую операцию будем называть умножением) задана конечным или бесконечным множеством свободных образующих $\{x_i \mid i \in I\}$.

Для произвольной системы элементов этой группы $g_1 = x_1^{a_{11}} x_2^{a_{12}} \dots x_q^{a_{1q}}$, $g_2 = x_1^{a_{21}} x_2^{a_{22}} \dots x_q^{a_{2q}}, \dots,$ $g_p = x_1^{a_{p1}} x_2^{a_{p2}} \dots x_q^{a_{pq}}$, заданной целочисленной матрицей $A = (a_{ij})$, обозначим через $l_F(g_1, g_2, \dots, g_p)$ (будем также использовать обозначение $l_F(A)$) *сложность совместного вычисления элементов* $g_1, g_2, \dots, g_p$, т. е. минимальное число операций умножения, достаточное для вычисления элементов $g_1, g_2, \dots, g_p$ по множеству $\{x_i, x_i^{-1} \mid i \in I\}$, состоящему из образующих и обратных к ним элементов, при этом разрешается многократное использование промежуточных результатов вычислений.

Величину $l_F(A)$ можно также интерпретировать как минимально возможную сложность схемы из функциональных элементов [1], на входы которой подаются функции $\{x_1, x_2, \dots, x_q, x_1^{-1}, x_2^{-1}, \dots, x_q^{-1}\}$, на выходах схемы вычисляются функции $x_1^{a_{11}} x_2^{a_{12}} \dots x_q^{a_{1q}}$, $x_1^{a_{21}} x_2^{a_{22}} \dots x_q^{a_{2q}}, \dots,$ $x_1^{a_{p1}} x_2^{a_{p2}} \dots x_q^{a_{pq}}$, задаваемые целочисленной матрицей наборов показателей степеней A размера $p \times q$, а сама схема состоит из двухвходовых элементов, реализующих произведение функций, подаваемых на входы элемента. Введенная мера сложности l_F близка мерам сложности l и l_2, рассматривавшимся в работах [2–4], но в отличии от них не обладает свойством двойственности [5].

В общем виде задача нахождения асимптотики роста величины $l_F(A)$ (с ростом, например, максимума абсолютных значений элементов матрицы) представляется довольно сложной.

Для случая $p = 1$, используя результаты работы [6], получаем, что для почти всех матриц $(a_1, a_2, \dots, a_q)$ (все a_i больше 1 и различны) при $\prod a_i \to \infty$ справедливо соотношение (здесь и далее все логарифмы берутся по основанию 2):

$$l_F(x_1^{a_1} x_2^{a_2} \dots x_q^{a_q}) \sim \log(\max a_i) + \frac{\log \prod a_i}{\log\log \prod a_i} + c(a_1, a_2, \dots, a_q) q,$$

где $c(a_1, a_2, \dots, a_q)$ — некоторая функция, удовлетворяющая неравенствам $0 \le c(a_1, a_2, \dots, a_q) < 1$.

В данной работе изучается случай $p = 2$. По целочисленной матрице A размера $2 \times q$ определим целочисленную матрицу M_A с неотрицательными элементами, последовательно преобразуя столбцы исходной матрицы следующим образом: 1) если в столбце $\begin{pmatrix} a_{1i} \\ a_{2i} \end{pmatrix}$ элементы имеют один знак, т. е. $a_{1i} a_{2i} \ge 0$, то включаем в матрицу M_A вместо этого столбца столбец $\begin{pmatrix} |a_{1i}| \\ |a_{2i}| \end{pmatrix}$; 2) если в столбце $\begin{pmatrix} a_{1i} \\ a_{2i} \end{pmatrix}$ элементы имеют разные знаки, т. е. $a_{1i} a_{2i} < 0$, то включаем в матрицу M_A вместо этого столбца матрицу $\begin{pmatrix} |a_{1i}| & 0 \\ 0 & |a_{2i}| \end{pmatrix}$. Таким образом, M_A — целочисленная матрица с неотрицательными элементами размера $2 \times r$, где r удовлетворяет условию $q \le r \le 2q$.

Аналогично [2] для матрицы $M_A = (m_{ij})$ $(i = 1, 2,\ j = 1, 2, \dots, r)$ положим $D(M_A) = \max\{\max m_{ij},\ \max |m_{1i} m_{2j} - m_{1i} m_{2j}|\}$, т. е. $D(M_A)$ — это максимум абсолютных величин миноров матрицы M_A, где максимум берется по всем минорам.

Теорема. *Для произвольной последовательности целочисленных матриц $A(n) = (a_{ij}(n))$ размера $2 \times q(n)$, удовлетворяющей условию $\max a_{ij}(n) \to \infty$ при $n \to \infty$, справедливы соотношения*

$$\log D(M_A) \le l_F(A) \le \log D(M_A) + O\left(q \frac{\log \max |a_{ij}|}{\log\log \max |a_{ij}|}\right).$$

Доказательство. Верхняя оценка. В силу определения матрицы M_A имеем: $l_F(A) = l_F(x_1^{a_{11}} x_2^{a_{12}} \dots x_q^{a_{1q}},\ x_1^{a_{21}} x_2^{a_{22}} \dots x_q^{a_{2q}}) \le l(z_1^{m_{11}} z_2^{m_{12}} \dots z_r^{m_{1r}},\ z_1^{m_{21}} z_2^{m_{22}} \dots z_r^{m_{2r}})$. Далее, применяя следствие к теореме 2 из [4], получаем: $l(z_1^{m_{11}} z_2^{m_{12}} \dots z_r^{m_{1r}},\ z_1^{m_{21}} z_2^{m_{22}} \dots z_r^{m_{2r}}) \le \log D(M_A) + O\left(r \frac{\log \max m_{ij}}{\log\log \max m_{ij}}\right) = \log D(M_A) + O\left(q \frac{\log \max |a_{ij}|}{\log\log \max |a_{ij}|}\right)$. Верхняя оценка доказана.

Прежде чем перейти к непосредственному доказательству нижней оценки установим два вспомогательных утверждения.

Лемма 1. *Пусть элементы g_1 и g_2 свободной абелевой группы с образующими x_1 и x_2 представляются в виде $g_1 = x_1^{a_{11}} x_2^{a_{12}}$, $g_2 = x_1^{a_{21}} x_2^{a_{22}}$, где a_{ij} — целые $(i = 1, 2,\ j = 1, 2)$. Тогда выполняется неравенство $|a_{11} a_{22} - a_{12} a_{21}| \le 2^{l_F(g_1, g_2)}$.*

Доказательство. Утверждение леммы устанавливается аналогично [7] (см. также доказательство леммы 1 из [2]) индукцией по числу операций умножения.

Лемма 2. *Пусть элементы g_1 и g_2 свободной абелевой группы с образующими $x_1, x_2, \dots, x_q$ представляются в виде $g_1 = x_1^{a_{11}} x_2^{a_{12}} \dots x_q^{a_{1q}}$, $g_2 = x_1^{a_{21}} x_3^{a_{22}} \dots x_q^{a_{2q}}$, где a_{ij} — целые $(i = 1, 2,\ j = 1, \dots, q)$. Тогда:*

1) *если $a_{11} a_{21} < 0$, то $l_F(g_1, g_2) \ge \log |a_{11} a_{21}|$;*

2) *если $a_{11} a_{21} < 0$ и $a_{12} a_{22} < 0$, то $l_F(g_1, g_2) \ge \log |a_{11} a_{22}|$.*

Доказательство. Рассмотрим схему из функциональных элементов S со входами $\{x_1, x_1^{-1}, x_2, x_2^{-1}, \dots x_q, x_q^{-1}\}$, реализующую систему $\{g_1, g_2\}$ со сложностью $l_F(g_1, g_2)$. Для каждой вершины v схемы

S определим величины $\partial(x_j, v)$ и $\partial(x_j^{-1}, v)$, $j = 1, 2$, следующим образом. Пусть в вершине v вычисляется элемент g_v группы, представляющийся через образующие так: $g_v = x_1^{b_1} x_2^{b_2} \dots x_q^{b_q}$. Положим

$$\partial(x_i, v) = \begin{cases} b_i, & \text{если } b_i \geq 0, \\ 0, & \text{если } b_i < 0, \end{cases} \qquad \partial(x_i^{-1}, v) = \begin{cases} 0, & \text{если } b_i \geq 0, \\ b_i, & \text{если } b_i < 0. \end{cases}$$

Зафиксируем две различные литеры y и z из множества $\{x_1, x_1^{-1}, x_2, x_2^{-1}\}$. Для произвольной подсхемы S' схемы S положим

$$\varphi(S', y, z) = \max_{v \in S'} \{\partial(y, v) - \partial(z, v)\} \max_{v \in S'} \{\partial(z, v) - \partial(y, v)\}.$$

Для подсхемы S_0, состоящей только из входовых вершин, выполняется равенство $\varphi(S', y, z) = 1$. Операция добавления к уже имеющейся подсхеме еще одного элемента умножения не может привести к увеличению значения φ более, чем в два раза, так как каждый из множителей $\max\limits_{v \in S'} \{\partial(y, v) - \partial(z, v)\}$ и $\max\limits_{v \in S'} \{\partial(z, v) - \partial(y, v)\}$ не может увеличиться более, чем в два раза, причем одновременно оба множителя увеличиться не могут. Поэтому для любых двух различных y и z из множества $\{x_1, x_1^{-1}, x_2, x_2^{-1}\}$ верно соотношение $\varphi(S, y, z) \leq 2^{l_F(g_1, g_2)}$.

С другой стороны, если выполняется неравенство $a_{11}a_{21} < 0$, то справедливо соотношение $\varphi(S, x_1, x_1^{-1}) \geq |a_{11}a_{21}|$. Следовательно, $l_F(g_1, g_2) \geq \log |a_{11}a_{21}|$.

Если же выполняется еще и неравенство $a_{12}a_{22} < 0$, то, полагая $y = x_1^{a_{11}/|a_{11}|}$ и $z = x_2^{a_{22}/|a_{22}|}$, получаем: $\varphi(S, y, z) \geq \log |a_{11}a_{22}|$. Поэтому $l_F(g_1, g_2) \geq \log |a_{11}a_{22}|$. Лемма 2 доказана.

Нижняя оценка. Если найдутся такие индексы i и j, $1 \leq i \leq 2$, $1 \leq j \leq r$, что выполняется равенство $D(M_A) = m_{ij}$, то найдется и такой индекс s, $1 \leq s \leq q$, что выполняется равенство $D(M_A) = |a_{is}|$. Тогда $l_F(A) = l_F(x_1^{a_{11}} x_2^{a_{12}} \dots x_q^{a_{1q}},\ x_1^{a_{21}} x_2^{a_{22}} \dots x_q^{a_{2q}}) \geq l_F(x_s^{a_{is}}) \geq \log |a_{is}| = \log D(M_A)$. Поэтому далее считаем, что найдутся такие индексы i и j, $1 \leq i, j \leq r$, что выполняется равенство $D(M_A) = |m_{1i}m_{2j} - m_{1j}m_{2i}|$.

Пусть при построении матрицы M_A по матрице A i-й и j-й столбцы матрицы M_A получаются путем замещения, соответственно, s-го и t-го столбца матрицы A (отметим, что, вообще говоря, s и t могут совпадать). Отдельно рассмотрим разные случаи в зависимости от того, на сколько столбцов — один или два — заменяются s-й и t-й столбцы матрицы A.

Случай 1. Пусть и s-й, и t-й столбец заменяются на один столбец.

Тогда $s \neq t$, и в силу построения матрицы M_A выполняются соотношения: $|a_{1s}| = m_{1i}$, $|a_{2s}| = m_{2i}$, $|a_{1t}| = m_{1j}$, $|a_{1t}| = m_{1j}$, $a_{1s}a_{2s} \geq 0$, $a_{1t}a_{2t} \geq 0$.

С использованием леммы 1 имеем: $l_F\left(x_s^{a_{1s}} x_t^{a_{1t}},\ x_s^{a_{2s}} x_t^{a_{2t}}\right) \geq \log |a_{1s}a_{2t} - a_{1t}a_{2s}| = \log |m_{1i}m_{2j} - m_{1j}m_{2i}| = \log D(M_A)$. Поэтому

$$l_F(A) = l_F(x_1^{a_{11}} x_2^{a_{12}} \dots x_q^{a_{1q}},\ x_1^{a_{21}} x_2^{a_{22}} \dots x_q^{a_{2q}}) \geq$$
$$\geq l_F\left(x_s^{a_{1s}} x_t^{a_{1t}},\ x_s^{a_{2s}} x_t^{a_{2t}}\right) \geq \log D(M_A).$$

Случай 2. Пусть один из столбцов с номерами s и t замещается одним столбцом, а другой — двумя.

Без ограничения общности будем считать, что s-й столбец замещается одним столбцом, а t-й — двумя. Тогда $s \neq t$, и в силу построения матрицы M_A выполняются соотношения: $|a_{1s}| = m_{1i}$, $|a_{2s}| = m_{2i}$, $a_{1s}a_{2s} \geq 0$, $a_{1t}a_{2t} < 0$, $m_{1j}m_{2j} = 0$. Опять-таки без ограничения общности будем считать, что $m_{1j} = 0$. Тогда справедливо равенство $m_{2j} = |a_{2t}|$. Поэтому, применяя лемму 1, получаем:

$$l_F\left(x_s^{a_{1s}} x_t^{a_{1t}}, x_s^{a_{2s}} x_t^{a_{2t}}\right) \geq \log |a_{1s}a_{2t} - a_{1t}a_{2s}| = \log |a_{1s}||a_{2t}| + |a_{1t}||a_{2s}| \geq$$
$$\geq \log |a_{1s}||a_{2t}| = \log(m_{1i}m_{2j}) = \log |m_{1i}m_{2j} - m_{1j}m_{2i}| = \log D(M_A).$$

Следовательно, $l_F(A) = l_F(x_1^{a_{11}} x_2^{a_{12}} \dots x_q^{a_{1q}},\ x_1^{a_{21}} x_2^{a_{22}} \dots x_q^{a_{2q}}) \geq l_F\left(x_s^{a_{1s}} x_t^{a_{1t}},\ x_s^{a_{2s}} x_t^{a_{2t}}\right) \geq l_2\left(x_s^{a_{1s}} x_t^{a_{1t}},\ x_s^{a_{2s}} x_t^{a_{2t}}\right) - 2 \geq \log D(M_A) - 2$.

Случай 3. Пусть и s-й, и t-й столбец замещаются двумя столбцами.

Тогда в силу построения матрицы M_A выполняются соотношения: $a_{1s}a_{2s} < 0$, $a_{1t}a_{2t} < 0$, $m_{1i}m_{2i} = 0$, $m_{1j}m_{2j} = 0$. При этом одно из произведений $m_{1i}m_{2j}$ и $m_{1j}m_{1i}$ отлично от нуля, так как $|m_{1i}m_{2j} - m_{1j}m_{2i}| = D(M_A) > 0$. Пусть, без ограничения общности, $m_{1i}m_{2j} \neq 0$.

Если $s = t$ (при этом $j = i + 1$), то $|a_{1s}| = m_{1i}$, $|a_{2s}| = m_{2j}$, и, применяя первую часть леммы 2, получаем оценку:

$$l_F(A) = l_F(x_1^{a_{11}} x_2^{a_{12}} \dots x_q^{a_{1q}}, x_1^{a_{21}} x_2^{a_{22}} \dots x_q^{a_{2q}}) \geq \log |a_{1s}a_{2s}| = \log m_{1i}m_{2j}.$$

Если же $s \neq t$, то $|a_{1s}| = m_{1i}$, $|a_{2t}| = m_{2j}$, и применяя вторую часть леммы 2, получаем такую же оценку:

$$l_F(A) = l_F(x_1^{a_{11}} x_2^{a_{12}} \dots x_q^{a_{1q}},\ x_1^{a_{21}} x_2^{a_{22}} \dots x_q^{a_{2q}}) \geq \log |a_{1s}a_{2t}| =$$
$$= \log m_{1i}m_{2j} = \log |m_{1i}m_{2j} - m_{1j}m_{2i}| = \log D(M_A).$$

Окончательно имеем:

$$l_F(A) \geq \log m_{1i}m_{2j} = \log |m_{1i}m_{2j} - m_{1j}m_{2i}| = \log D(M_A).$$

Теорема доказана.

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

Список литературы

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

2. Кочергин В. В. Об асимптотике сложности аддитивных вычислений систем целочисленных линейных форм // Дискретный анализ и исследование операций. Серия 1. — 2006. — Т. 13, № 2. — С. 38–58.

3. Кочергин В. В. О сложности вычисления пары одночленов от двух переменных // Дискретная математика. — 2005. — Т. 17, вып. 4. — С. 116–142.

4. Кочергин В. В. О сложности вычисления систем одночленов от двух переменных // Труды VII Международной конференции «Дискретные модели в теории управляющих систем» (Покровское, 4–6 марта 2006 г.). — М.: МАКС Пресс, 2006. — С. 185–190.

5. Гашков С. Б., Кочергин В. В. Об аддитивных цепочках векторов, вентильных схемах и сложности вычисления степеней // Методы дискретного анализа в теории графов и сложности. — Новосибирск, 1992. — Вып. 52. — С. 22–40.

6. Кочергин В. В. О двух обобщениях задачи об аддитивных цепочках // *Труды* IV Международной конференции "Дискретные модели в теории управляющих систем" (19–25 июня 2000 г.). — Москва, "МАКС Пресс", 2000. — С. 55–59.

7. Morgenstern J. Note on a lower bound of the linear complexity of the fast Fourier transform // J. Assoc. Comput. Mach. — 1973. — V. 20. — P. 305–306.

РЕШЕНИЕ ЗАДАЧИ НАХОЖДЕНИЯ ВСЕХ Т-НЕПРИВОДИМЫХ РАСШИРЕНИЙ ДЛЯ СИММЕТРИЧНЫХ ОРИЕНТАЦИЙ ЦЕПЕЙ

С. Г. Курносова (Саратов)

Одной из оптимизационных задач в теории дискретных систем является построение отказоустойчивых реализаций системы. Формализованное понятие отказоустойчивости, предложенное Авиженисом, Хейз [1] сформулировал в терминах теории графов. При этом понятием, эквивалентным понятию отказоустойчивой реализации дискретной системы, допускающей графовое представление, стала конструкция расширения графа. Расширением n-вершинного графа G называется граф H с $n+1$ вершинами такой, что G вкладывается в каждый максимальный подграф графа H. Для произвольного графа G его множество расширений не пусто, так как существует хотя бы одно расширение — тривиальное, которое является соединением исходного графа G с одновершинным графом. Руководствуясь различными критериями, из всего множества расширений выделяют подмножества оптимальных расширений. Первую такую конструкцию рассмотрел Хейз. Он предлагал среди всех расширений графа выбирать расширения с минимальным количеством ребер (изначально все критерии были сформулированы для неориентированных графов). Задача нахождения минимального расширения для произвольного графа остается не решенной и представляется очень сложной. Были получены только некоторые частные результаты в этом направлении. Второй критерий оптимальности предложил В. Н. Салий [2]. Эта конструкция называется Т-неприводимым расширением (ТНР), и получаются такие расширения удалением максимального числа ребер из тривиального расширения графа без нарушения свойства расширения. Аналогично минимальным расширениям здесь тоже пока не найдено эффективного алгоритма для описания все ТНР произвольного графа, рассматривались отдельные классы графов, для которых удалось решить эту задачу.

Как уже отмечалось выше, все расширения рассматривались в основном для неориентированных графов. В работе [3] конструкция ТНР естественным образом обобщена на ориентированные графы (орграфы). При этом возникает аналогичная задача отыскания всех ТНР для произвольного орграфа. Решить ее в общей постановке пока не представляется возможным, и поэтому был выбран один частный случай — класс ориентаций цепей — и для него рассматривалась эта проблема. Ориентацией цепи (далее: ориентацией) называется орграф, полученный из неориентированной цепи $P_n : u_1u_2 \dots u_n$ приданием произвольной ориентации каждому ребру. При этом любую ориентацию можно задать вектором $(r_2, \dots, r_n)$, где $r_i = 0$, если в ориентации есть дуга (u_i, u_{i-1}), и $r_i = 1$ в противном случае. Но даже эту частную задачу решить пока не удалось, и был выделен еще более узкий подкласс — симметричные ориентации. Ориентацию $(r_2, \dots, r_n)$, где $n > 2$ и нечетное, назовем симметричной ориентацией (СО), если выполнено равенство $(r_2, \dots, r_n) = (\bar{r}_n, \dots, \bar{r}_2)$, где $\bar{}$ есть операция дополнения. В этом подклассе сначала было найдено одно ТНР для произвольной СО, а затем для СО с некоторым

дополнительным свойством было указано еще два ТНР, не изоморфных ранее найденному (статьи с этими результатами — в печати). В настоящей работе показывается, что только эти три конструкции и будут ТНР для СО.

Таким образом, задача нахождения всех Т-неприводимых расширений для симмеиричных ориентаций цепей решена полностью.

Рассмотрим свойство СО, которое будет необходимо для доказательств:

$$(\exists i)(\ r_i = r_{i+1}\ \&\ (r_2, \ldots, r_i) \text{ есть СО}). \qquad (*)$$

Теорема 1. *Если для вектора $(r_2, \ldots, r_n)$ n-вершинной СО G с $n > 5$ не выполнено свойство $(*)$, то единственным ТНР для G будет орграф H, который получается из G добавлением новой вершины v и следующих дуг*:

1) *дуг (v, u_1) и (v, u_n), если $r_2 = 0$, или дуг (u_1, v) и (u_n, v), если $r_2 = 1$*;

2) *дуг (v, u_2) и (v, u_{n-1}), если $r_3 = 0$, или дуг (u_2, v) и (u_{n-1}, v), если $r_3 = 1$*;

3) *вершина u_i, где $i = \overline{3, n-2}$, соединяется с вершиной v одним из следующих способов*:

а) *дугой (u_i, v), если $r_i = \bar{r}_{i+1} = 0$ и $(r_2, \ldots, r_i)$ или $(r_{i+1}, \ldots, r_n)$ — не СО*;

б) *дугой (v, u_i), если $r_i = \bar{r}_{i+1} = 1$ и $(r_2, \ldots, r_i)$ или $(r_{i+1}, \ldots, r_n)$ — не СО*;

в) *дугами (v, u_i) и (u_i, v), если $r_i = r_{i+1}$*;

г) *вершина u_i не соединяется дугой с v, если $r_i = \bar{r}_{i+1}$ и $(r_2, \ldots, r_i)$ и $(r_{i+1}, \ldots, r_n)$ — СО.*

Доказательство. По ранее доказанному, орграф H является ТНР для G. Покажем, что он будет единственным ТНР для G при нарушении условия (*). Предположим, что у орграфа G есть еще одно ТНР — орграф H', не изоморфный H. По критерию Т-неприводимости в H' есть вершина v, такая что $H' - v$ изоморфно G. Занумеруем вершины в $H' - v$, как в орграфе G. Тогда в H' должны быть следующие дуги:

— дуги (v, u_1) и (v, u_n), если $r_2 = 0$, либо дуги (u_1, v) и (u_n, v), если $r_2 = 1$;

— дуги (v, u_2) и (v, u_{n-1}), если $r_3 = 0$, либо дуги (u_2, v) и (u_{n-1}, v), если $r_3 = 1$;

— дуги (u_i, v) при $3 \le i \le n-2$, $r_i = \bar{r}_{i+1} = 0$ и $(r_2, \ldots, r_i)$ или $(r_{i+1}, \ldots, r_n)$ — не СО, либо дуги (v, u_i) при $3 \le i \le n-2$, $r_i = \bar{r}_{i+1} = 1$ и $(r_2, \ldots, r_i)$ или $(r_{i+1}, \ldots, r_n)$ — не СО.

В силу неприводимости орграфов H и H' их множества дуг, инцидентных вершине v, должны быть несравнимыми. Значит, в G существует вершина u_i, где $3 \le i \le n-2$, такая, что $r_i = r_{i+1}$ и в H' не будет дуги (u_i, v) или дуги (v, u_i), так как все остальные дуги, которые есть в H (по построению), присутствуют и в H'. Предположим, что в H' нет дуги (v, u_i) при $r_i = r_{i+1}$ и $3 \le i \le n-2$. Рассмотрим сначала случай, когда $r_i = r_{i+1} = 1$. Тогда в орграфе $H' - u_{i-1}$ вершина u_i будет источником и вложения G в $H' - u_{i-1}$ будет невозможно в силу нарушения условия (*). Аналогично орграф G не будет вкладываться в $H' - u_{i+1}$, если в H' нет дуги (v, u_i) при $r_i = r_{i+1} = 0$ и $3 \le i \le n-2$. Значит, в H' должны быть дуги (v, u_i) и (u_i, v), где $r_i = r_{i+1}$ и $3 \le i \le n-2$. Из этого следует, что в орграфе H' присутствуют все дуги орграфа H, а значит, эти орграфы совпадают или H' не является неприводимым. Оба эти вывода приводят к противоречию и, следовательно, при нарушении условия (*) у орграфа G единственным ТНР будет орграф H.

Теорема 2. *Если для вектора $(r_2, \ldots, r_n)$ n-вершинной СО G с $n > 5$ выполнено условие $(*)$, то у такой СО будет только три ТНР*: *орграф H (описание которого дано в Теореме 1), орграфы H_1 и H_2. Орграф H_1 получаем из G добавлением новой вершины v и следующих дуг*:

1) *дуг (v, u_1), (v, u_n), (u_1, v), (u_n, v)*;

2) *дуг (v, u_2) и (v, u_{n-1}), если $r_3 = 0$, или дуг (u_2, v) и (u_{n-1}, v), если $r_3 = 1$*;

3) *вершина u_i, где $i = \overline{3, n-2}$, соединяется с вершиной v одним из следующих способов*:

а) *дугой (u_i, v), если $r_i = \bar{r}_{i+1} = 0$ и $(r_2, \ldots, r_i)$ или $(r_{i+1}, \ldots, r_n)$ — не СО, или $r_i = r_{i+1}$ и $r_2 = 1$ и $(r_2, \ldots, r_i)$ или $(r_{i+1}, \ldots, r_n)$ — СО*;

б) *дугой (v, u_i), если $r_i = \bar{r}_{i+1} = 1$ и $(r_2, \ldots, r_i)$ или $(r_{i+1}, \ldots, r_n)$ — не СО, или $r_i = r_{i+1}$ и $r_2 = 0$ и $(r_2, \ldots, r_i)$ или $(r_{i+1}, \ldots, r_n)$ — СО*;

в) *дугами (v, u_i) и (u_i, v), если $r_i = r_{i+1}$ и $(r_2, \ldots, r_i)$ и $(r_{i+1}, \ldots, r_n)$ — не СО*;

г) *вершина u_i не соединяется дугами с v, если $r_i = \bar{r}_{i+1}$ и $(r_2, \ldots, r_i)$ и $(r_{i+1}, \ldots, r_n)$ — СО.*

Орграф H_2 получаем из G добавлением новой вершины v и следующих дуг:

1) *дуг (v, u_1), (u_1, v) и дуги (u_n, v), если $r_2 = 1$, либо дуги (v, u_n), если $r_2 = 0$*;

2) *дуг* (v, u_2) *и* (v, u_{n-1}), *если* $r_3 = 0$, *или дуг* (u_2, v) *и* (u_{n-1}, v), *если* $r_3 = 1$;

3) *вершина* u_i, *где* $i = \overline{3, n-2}$, *соединяется с вершиной* v *одним из следующих способов*:

а) *дугой* (u_i, v), *если* $r_i = \bar{r}_{i+1} = 0$ *и* $(r_2, \ldots, r_i)$ *или* $(r_{i+1}, \ldots, r_n)$ *— не СО, или* $r_i = r_{i+1}$ *и* $r_2 = 1$ *и* $(r_2, \ldots, r_i)$ *является СО*;

б) *дугой* (v, u_i), *если* $r_i = \bar{r}_{i+1} = 1$ *и* $(r_2, \ldots, r_i)$ *или* $(r_{i+1}, \ldots, r_n)$ *— не СО, или* $r_i = r_{i+1}$ *и* $r_2 = 0$ *и* $(r_2, \ldots, r_i)$ *является СО*;

в) *дугами* (v, u_i) *и* (u_i, v), *если* $r_i = r_{i+1}$ *и* $(r_2, \ldots, r_i)$ *не СО*;

г) *вершина* u_i *не соединяется дугами с* v, *если* $r_i = \bar{r}_{i+1}$ *и* $(r_2, \ldots, r_i)$ *и* $(r_{i+1}, \ldots, r_n)$ *— СО*.

Доказательство. Согласно ранее доказанному, орграфы H, H_1 и H_2 являются ТНР для G. Покажем, что других ТНР у G нет. Предположим, что нашелся орграф H', являющийся ТНР для G и не изоморфный ни H, ни H_1, ни H_2. По критерию Т-неприводимости в H' есть вершина v, такая что $H' - v$ изоморфно G. Занумеруем вершины в $H' - v$, как в орграфе G. Тогда в H' должны быть следующие дуги:

— дуги (v, u_1) и (v, u_n), если $r_2 = 0$, либо дуги (u_1, v) и (u_n, v), если $r_2 = 1$;

— дуги (v, u_2) и (v, u_{n-1}), если $r_3 = 0$, либо дуги (u_2, v) и (u_{n-1}, v), если $r_3 = 1$;

— дуги (u_i, v), если $3 \le i \le n-2$, $r_i = \bar{r}_{i+1} = 0$ и $(r_2, \ldots, r_i)$ или $(r_{i+1}, \ldots, r_n)$ — не СО, либо дуги (v, u_i) если $3 \le i \le n-2$, $r_i = \bar{r}_{i+1} = 1$ и $(r_2, \ldots, r_i)$ или $(r_{i+1}, \ldots, r_n)$ — не СО.

Возможны следующие четыре случая.

1. В H' вершины v и u_1 соединены только одной дугой и вершины v и u_n соединены только одной дугой.

2. В H' вершины v и u_1 соединены двумя дугами, а вершины v и u_n соединены только одной дугой.

3. В H' вершины v и u_1 соединены только одной дугой, а вершины v и u_n соединены двумя дугами.

4. В H' присутствуют все четыре дуги (u_1, v), (v, u_1), (u_n, v) и (v, u_n).

Непосредственная проверка показывает, что во всех четырех случаях получается противоречие с предположением о неприводимости орграфа H'. Это означает, что не существует орграфа, который был бы отличен от H, H_1 и H_2 и был бы ТНР для G.

Работа выполнена при финансовой поддержке гранта РФФИ (проект 05-08-18082).

Список литературы

1. Hayes P. A graph model for fault-tolerant computing system // IEEE Trans. Comput. — 1976. — V. C-25, № 9. — P. 875–884.

2. Салий В. Н. Доказательства с нулевым разглашением в задачах о расширениях графов // Вестник Томского государственного университета. Приложение N 6. — Томск: ТГУ, 2003. — С. 63–65.

3. Курносова С. Г. Т-неприводимые расширения для ориентаций цепей с числом вершин не более 8.— Саратов: СГУ, 2005. — 22 с. — Деп. в ВИНИТИ 11.05.05, № 677—В2005.

ОБРАБОТКА СЖАТЫХ ТЕКСТОВ

Ю. М. Лифшиц (Санкт-Петербург)

1. Введение. В связи со стремительным ростом объемов информации все большее внимание уделяется алгоритмам обработки сжатых объектов *без разархивирования*. Изучается обработка сжатых изображений, деревьев, схем. В последнее десятилетие активные исследования связаны с операциями над сжатыми текстами.

Отметим, что алгоритмы обработки сжатых текстов не только необходимы для непосредственного применения на практике, но и используются для решения других вычислительных задач. Так, недавно найдены (см. [1]) приложения алгоритмов обработки сжатых текстов для анализа диаграмм последовательностей сообщений (message sequence charts). Прорывом стал алгоритм Пландовского для решения уравнений в словах [2], основанный на сжатом представлении строк.

В этой работе мы рассмотрим все самые существенные результаты по обработки сжатых текстов. Это алгоритмы и теоремы о трудности для вычислительных задач на сжатых текстах. В качестве обзора по обработке сжатых текстов можно также порекомендовать [3]. По сравнению с этой работой мы включили ряд совсем новых результатов и открытых проблем.

1.1. Что такое сжатый текст? Мы рассматриваем конечный алфавит Σ, текстом (строкой, словом) называется любая конечная последовательность его букв.

Центральным понятием нашей работы является сжатие строки (слова). В девяностые годы для построения алгоритмов стали использовать модель, основанную на грамматиках — *прямолинейные программы* (Straight-Line Programs). Этой последней моделью мы и

будем пользоваться. Неформально, прямолинейная программа — это контекстно-свободная грамматика, порождающая только одно слово.

Определение. Прямолинейной программой называется контекстно-свободная грамматика $\mathcal{P}$, в которой нетерминальные символы $X_1, \ldots, X_m$ упорядочены (X_m — стартовый символ), и где у каждого нетерминального символа есть только одно правило: $X_i \to a$, где a — терминал, или $X_i \to X_j X_k$ для некоторых $j, k < i$.

Важно отметить, что прямолинейные программы являются моделью *декомпрессора*, то есть моделируют лишь получение исходного текста из сжатого представления. В данной работе мы совершенно не заботимся о том, как были получены сжатые тексты.

Трудность обработки сжатых текстов связана с тем, что соотношение между размером прямолинейной программы и длиной порождаемого текста может быть экспоненциальным. Таким образом, мы не можем себе позволить восстанавливать оригинальный текст.

Так как архивы полученные большинством используемых практических методов могут быть преобразованы в прямолинейные программы примерно того же размера [4], то все исследования мы ведем только для нашей абстрактной модели.

2. Алгоритмы для решения задач на сжатых текстах. Перечислим основные задачи, которые изучаются для сжатых текстов:

Эквивалентность представлений: дано два сжатых текста, требуется определить, совпадают они или нет.

Поиск подстроки в сжатом тексте: дан шаблон и сжатый текст, требуется определить, является ли шаблон подстрокой текста, и при положительном ответе найти первое вхождение.

Поиск сжатой подстроки в сжатом тексте: дан сжатый шаблон и сжатый текст, требуется определить, является ли шаблон подстрокой текста, и при положительном ответе найти первое вхождение.

Принадлежность языку: зафиксирован некоторый язык. Требуется по данной сжатой строке определить, принадлежит она языку или нет.

Вычислительная сложность этих задач рассматривалась в целом ряде работ [5–7]. Первые три задачи имеют полиномиальную сложность. Особо выделим работу [5], где был построен полиномиальный алгоритм для поиска сжатой подстроки в сжатом тексте. Вопрос о принадлежности регулярному языку также решается за полиномиальное время.

Еще одним важным результатом является эффективное приближенное построение в [4] по данному тексту минимальной прямолинейной программы (ПП), порождающей этот текст. Более формально, построен алгоритм, работающий за время $O(n \cdot \log|\Sigma|)$, который по тексту длины n строит $O(\log n)$-приближение минимальной ПП, порождающей этот текст. Это означает, что поиск адекватного (близкого к максимально возможному) сжатия в модели прямолинейных программ может быть выполнен эффективно.

В работе [8] были ускорены алгоритмы для поиска сжатого шаблона в сжатом тексте и для нахождения минимального периода сжатого текста. Также были построены полинамиальные алгоритмы для нахождения минимального накрывающего шаблона (cover) и построения таблицы отпечатков сжатого текста.

3. Трудные задачи на сжатых текстах. Поиск сжатого шаблона в сжатом тексте можно осуществить за полиномиальное время. Однако ряд очень близких задач (поиск сжатого шаблона, входящего *как подпоследовательность* в сжатый текст, вычисление расстояния Хэмминга) оказались NP-трудны [8, 9].

Маркус Лори показал, что задача о принадлежности контекстно-свободному языку оказывается PSPACE-полной [6]. В работе [10] задачи поиска подстрок обобщены на двумерные тексты. Как оказалось, при этом резко возрастает вычислительная сложность. Поиск явно заданного шаблона в сжатом двумерном тексте является NP-полным, а поиск сжатого шаблона в сжатом двумерном тексте является Σ_2^P-полным.

Как известно, строки являются элементами свободного конечно-порожденного моноида. В работе [6] изучается обработка сжатых элементов различных классов конечно-порожденных моноидов. В зависимости от ограничений на моноид были получены доказательства полноты задачи эквивалентности сжатых представлений для классов P, coNP, PSPACE и EXPSPACE.

Также оказалось что некоторые задачи — принадлежность регулярному языку [11], чтение одного символа [9] — являются P-полными (то есть плохо поддается распараллеливанию).

4. Направления для будущих исследований. В области построения новых алгоритмов:

1. Найти более эффективный чем в [8] алгоритм для поиска сжатой подстроки в сжатом тексте. *Гипотеза:* задачу можно решить за время $O(nm \log|T|)$.

2. Построить более быстрый алгоритм и/или использующий меньше памяти для задачи об ограниченных подпоследовательностях в сжатых текстах. Напомним, что эта задача была решена в работе [12] за время и память $O(nk^2 \log k)$. *Гипотеза:* Достаточно $O(nk)$ памяти.

3. Построить $O(nm)$ алгоритм для (взвешенного) редакторского расстояния, где n длина текста T_1, а m размер ПП, порождающей текст T_2. Такой алгоритм привел бы к ускорению классической задачи для любого "сверх-логарифмического" сжатия, так как только $O(\frac{n^2}{\log n})$ классический алгоритм известен для этой задачи.

Изучение сложности задач на сжатых текстах:

1. Принадлежность сжатой строки к языку, описанному расширенным регулярным выражением является NP-трудной задачей. С другой стороны, эта задача лежит в PSPACE. Интересно найти точную сложность задачи.

2. Задача о вхождении одного сжатого текста в виде подпоследовательности в другой сжатый текст является Θ_2-трудной [9]. С другой стороны, эта задача лежит в классе PSPACE. Интересно найти точную сложность задачи.

3. Задача о нахождении расстояния Хемминга между сжатыми текстами является в NP-трудной и coNP-трудной тоже лежит в PSPACE. Какова ее сложность?

В заключение, перечислим основные направления для развития теории обработки сжатых текстов. Во-первых, следует рассмотреть классические строковые задачи, которые еще не были рассмотрены на сжатых текстах. Далее, интересно изучить более сильные модели порождения и архивирования строк (например, метод Берроуза — Вилера). Интересно также провести глубокое экспериментальное исследование построенных алгоритмов. Наконец, было бы замечательно найти принципиально отличные от динамического программирования техники обработки сжатых текстов.

Работа выполнена при поддержке грантов INTAS 04-77-7173 и НШ-8464.2006.1

Список литературы

1. Genest B., Muscholl A. Pattern matching and membership for hierarchical message Sequence Charts // Lecture Notes in Comput. Sci. (Proceedings of the 5th Latin American Symposium on Theoretical Informatics, LATIN-2002). — Springer-Verlag, 2002. — V. 2286 — P. 326–340.

2. Plandowski W. Satisfiability of word equations with constants is in PSPACE // J. ACM. — 2004. — V. 51, № 3. — P. 483–496.

3. Rytter W. Grammar compression, LZ-encodings, and string algorithms with implicit input // Lecture Notes in Comput. Sci. (Proceedings of the 31st International Colloquium on Automata, Languages and Programming, ICALP-2004). — Springer-Verlag, 2004. — V. 3142 — P. 14–27.

4. Rytter W. Application of Lempel-Ziv factorization to the approximation of grammar-based compression // Theoretical Computer Science. — 2003. — V. 302, №№ 1–3. — P. 211–222.

5. Gasieniec L., Karpinski M., Plandowski W., Rytter W. Efficient algorithms for Lempel — Ziv encoding (extended abstract) // Lecture Notes in Comput. Sci. (Proceedings of the 5th Scandinavian Workshop on Algorithm Theory, SWAT-1996). — Springer-Verlag, 1996. — V. 1097. — P. 392–403.

6. Lorhey M. Word problems on compressed word // Lecture Notes in Comput. Sci. (ICALP 2004). — Springer-Verlag, 2004. — V. 3142 — P. 906–918.

7. Plandowski W., Rytter W. Complexity of language recognition problems for compressed words // Jewels are Forever. Contributions on Theoretical Computer Science in Honor of Arto Salomaa. — Springer-Verlag, 1990. — P. 262–272.

8. Lifshits Yu. Solving classical string problems on compressed texts // Preprint arxiv: cs.DS/0604058, 2006.

9. Lifshits Yu., Lohrey M. Querying and embedding compressed texts // To appear in MFCS'06.

10. Berman P., Karpinski M., Larmore L. L., Plandowski W., Rytter W. On the complexity of pattern matching for highly compressed two-dimensional texts // Journal of Computer and Systems Science. — 2002. — V. 65, № 2. — P. 332–350.

11. Markey N., Schnoebelen Ph. A PTIME-complete matching problem for SLP-compressed words // Information Processing Letters. — 2004. — V. 90, № 1. — P. 3–6.

12. Cégielski P., Guessarian I., Lifshits Yu., Matiyasevich Yu. Window subsequence problems for compressed texts // Lecture Notes in Comput. Sci. (CSR'06). — Springer-Verlag, 2006. — V. 3967. — 127–136.

О РЕАЛИЗАЦИИ ФУНКЦИЙ АЛГЕБРЫ ЛОГИКИ BDD, ВЛОЖЕННЫМИ В ЕДИНИЧНЫЙ КУБ

С. А. Ложкин, О. Б. Седелев (Москва)

В настоящее время достаточно распространённой моделью реализации функций алгебры логики, наряду со схемами из функциональных элементов, являются двоичные решающие диаграммы

(BDD). Напомним, что BDD представляют собой, по существу, специальный частный случай контактных схем и были введены в рассмотрение в 1959 г. Lee C. Y. Им же были получены следующие оценки для функции Шеннона $L(n)$, которая равна сложности самой "сложной" ФАЛ от n булевских переменных при их реализации в классе BDD:

$$\frac{2^n}{2n} \le L(n) \le 4\frac{2^n}{n} - 1.$$

Позднее Кузьмин В. А. установил, что:

$$L(n) = \frac{2^n}{n}(1 \pm \bar{o}(1)),$$

а Ложкин С. А. [1] получил для функции Шеннона $L(n)$ асимптотические оценки высокой степени точности:

$$L(n) = \frac{2^n}{n}\left(1 \pm \bar{o}\left(\frac{\log(n)}{n}\right)\right).$$

Во многих случаях для дальнейшего использования построенной схемы необходима её геометрическая реализация, т. е. вложение определенного вида в ту или иную заданную геометрическую структуру. В качестве такой структуры часто выступают плоские прямоугольные решётки или, иначе, клеточные схемы, а в последнее время — единичный n-мерный куб. При этом рассматриваются различные типы вложений и, в частности, гомеоморфные [2] вложения.

В данной работе рассматривается геометрическая реализация BDD, связанная с их гомеоморфными вложениями в единичные кубы, при которых вершины BDD переходят в вершины единичного куба, а рёбра — в рёбра или так называемые транзитные цепи единичного куба, не имеющие общих внутренних вершин. При этом критерием "сложности" BDD считается минимальная размерность единичного куба, в который возможно её вложение указанного вида. Обычным образом определяется значение рассматриваемого функционала сложности для произвольной ФАЛ f, а затем вводится соответствующая функция Шеннона $R(n)$, которая равна минимальной размерности единичного куба, допускающего для любой ФАЛ $f(x_1, \ldots, x_n)$ гомеоморфное вложение реализующей её BDD.

Основной результат работы заключается в установлении следующих оценок:

$$n - \lfloor \log\log(n) - \log 3 + o(1) \rfloor \le R(n) \le n - \lfloor \log\log(n) + 3 + o(1) \rfloor, \quad (*)$$

которые усиливают аналогичные оценки из [3].

Доказательство нижней оценки проводится на основе мощностных соображений. Для этого доказывается верхняя оценка вида:

$$A(n, r) \le ((n+4)r(r-1))^{2^r},$$

где $A(n, r)$ — число различных BDD от n булевых переменных (БП) $x_1, \ldots, x_n$, которые можно вложить в единичный куб B^r размерности r.

Действительно, при вложении BDD от n БП в B^r каждой вершине куба может быть поставлен в соответствие один из следующих символов: $x_1, \ldots, x_n$, 0, 1, либо вершина может быть транзитной или не использованной. Далее, для любой вершины, которой сопоставлена вершина BDD, существует не более чем $r(r-1)$ вариантов выбора её выходных рёбер и присвоения им пометок 0 или 1, после чего вложение полностью определено.

Требуемая нижняя оценка (*) получается из решения обычного мощностного неравенства:

$$(n+4)R(n)(R(n)-1))^{2^{R(n)}} \ge 2^{2^n}.$$

Доказательство верхней оценки состоит из двух этапов.

На первом этапе осуществляется реализация заданной (произвольной) ФАЛ $f(x_1, \ldots, x_n)$ в виде специальным образом построенной BDD Σ_f.

Для построения BDD Σ_f используем метод, основанный на работах [1, 2].

Пусть q — число, представимое в виде $q = 2^{2^m} + m$, где $m = 0, 1, 2, \ldots$ построим разбиение единичного куба B^q от БП $x_1, \ldots, x_q$ на множества A_i, $i = 1, \ldots, 2^{q-m}$ такое, что:

1) каждое из множеств A_i состоит из 2^m наборов;

2) для каждого из множеств A_i любая ФАЛ от переменных $x_1, \ldots, x_q$ совпадает с одной из переменных $x_{m+1}, \ldots, x_q$ или её отрицанием.

Пусть X_i — характеристическая функция множества A_i. Тогда любая ФАЛ от q переменных $f(x_1, \ldots, x_q)$ может быть представлена в виде:

$$f(x_1, \ldots, x_q) = X_1 x_{j_1}^{\sigma_1} \vee \ldots \vee X_{2^{q-m}} x_{j_{2^{q-m}}}^{\sigma^{2^{q-m}}},$$

где $\sigma_i \in \{0, 1\}$.

Для любой ФАЛ $f(x_1,\dots,x_n)$ искомая BDD Σ_f строится на основе представления:

$$f(x) = \bigvee_{(\sigma_{q+1},\dots,\sigma_n)} x_{q+1}^{\sigma_{q+1}} \dots x_n^{\sigma_n} f(x_1,\dots,x_q,\sigma_{q+1},\dots,\sigma_n) =$$

$$= \bigvee_{(\sigma_{q+1},\dots,\sigma_n)} x_{q+1}^{\sigma_{q+1}} \dots x_n^{\sigma_n} \left(\bigvee_{i=1}^{2^{q-m}} X_i x_{j_i}^{\sigma_i} \right) =$$

$$= \bigvee_{i=1}^{2^{q-m}} X_i \left(\bigvee_{(\sigma_{q+1},\dots,\sigma_n)} x_{q+1}^{\sigma_{q+1}} \dots x_n^{\sigma_n} x_{j_i}^{\sigma_i} \right).$$

При этом BDD Σ_f включает в себя следующие подграфы:

1) D' — дерево из q ярусов, реализующее все конъюнкции от переменных $x_1,\dots,x_q$ (в корне дерева расположена вершина x_1, на втором ярусе вершины x_2 и т. д.);

2) D — граф, состоящий из дерева D', листья которого объединены в группы по 2^m в каждой, так, что D реализует характеристические функции $X_1,\dots,X_{2^{q-m}}$;

3) каждое дерево D_i, $i=1,\dots,2^{q-m}$, состоит из дерева, реализующего все конъюнкции от переменных $x_{q+1},\dots,x_n$ (при этом в корне дерева расположена вершина x_{q+1}, на втором ярусе вершины x_{q+2} и т. д.), к листьям которого присоединены деревья (из одного яруса), реализующие переменные $x_{j_i}^{\sigma_i}$.

На втором этапе BDD Σ_f, необходимо вложить в единичный куб как можно меньшей размерности.

Единичный куб размерности $n-m+1$ делится на непересекающиеся подкубы размерности $n-q+1$, а все их вершины, принадлежащие соседним подкубам соединяются рёбрами. К данной системе рёбер подсоединяются все деревья $D_1,\dots,D_{2^{q-m}}$ и дерево D'. При этом используется следующий факт: в кубе B^p любые p вершин могут быть соединены непересекающимися путями без петель с одной произвольной вершиной (доказательство проводится по индукции). При вложении деревьев $D_1,\dots,D_{2^{q-m}}$ и дерева D' учитывается, что k-ярусное дерево можно вложит в единичный куб размерности $k+1$.

В итоге вложение оказывается возможным для куба размерности $n-\log\log n+3+o(1)$.

Тем самым, получено совпадение нижней и верхней оценок с точностью до константы.

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

Список литературы

1. Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. Вып. 6. — М.: Наука, 1996. — С. 189–214.

2. Ложкин С. А. О сложности реализации функций алгебры логики схемами и формулами, построенными из функциональных элементов с прямыми и итеративными входами // Труды III Международной конференции "Дискретные модели в теории управляющих систем" (Красновидово, 22–27 июня 1998.). — М.: Диалог-МГУ, 1998. — С. 72–73.

3. Седелев О. Б. Верхняя и нижняя оценки сложности реализации функций алгебры логики BDD, вложенными в n-мерный куб // Тезисы XIV Международной школы-семинара "Синтез и сложность управляющих систем" (Нижний Новгород, 27 октября – 1 ноября 2003 г.).

АСИМПТОТИЧЕСКИЕ ОЦЕНКИ ВЫСОКОЙ СТЕПЕНИ ТОЧНОСТИ ДЛЯ СЛОЖНОСТИ ПРЕДИКАТНЫХ СХЕМ ИЗ ОДНОГО КЛАССА

С. А. Ложкин, М. С. Шуплецов (Москва)

Рассмотрим множество (базис) из булевских предикатов $\mathfrak{D} = \{\pi_1,\dots,\pi_s\}$, где предикат π_i, $i=1,\dots,s$, зависит от k_i булевских переменных (БП) и пусть $\mathcal{X}(\mathcal{Y})$ — счетный упорядоченный алфавит внешних (внутренних) переменных.

Предикатной схемой Σ в базисе $\mathfrak{D}$ назовем двудольный граф, в котором все различные вершины первой доли помечены различными символами из $\mathcal{X}\cup\mathcal{Y}$, а все вершины второй доли — символами из множества $\mathfrak{D}$. При этом каждая вершина второй доли с пометкой $\pi_i, i=1,\dots,s$, соединена k_i ребрами, помеченными числами $1,\dots,k_i$, с вершинами $v_1,\dots,v_{k_i}$ из первой доли соответственно и связана с предикатом $\pi_i(u_1,\dots,u_{k_i})$, где u_j, $j=1,\dots,k_i$, — БП из $\mathcal{X}\cup\mathcal{Y}$, являющаяся пометкой вершины v_j.

Схема Σ указанного вида от внешних БП $x = (x_{i_1}, \ldots, x_{i_n})$ и внутренних БП $y = (y_{j_1}, \ldots, y_{j_m})$ реализует предикат $\pi(x)$, для которого набор α значений БП x допустим, то есть $\pi(\alpha)$ истинно, тогда и только тогда, когда существует набор β значений БП y такой, что компоненты наборов α и β задают допустимые наборы для всех базисных предикатов, связанных с вершинами второй доли Σ.

Суперпозицией предикатных схем по переменным x_i и x_j назовем схему, которая представляет собой объединение исходных схем, причем вершины указанных переменных отождествляются в одну вершину, помеченную новым символом внутренней или внешней переменной. Частными случаями суперпозиции являются переименование переменных, введение и удаление фиктивных переменных, отождествление переменных, а также объединение схем [1]. Естественным образом вводится понятие полноты класса предикатных схем, относительно операции суперпозиции. Основные вопросы полноты схем из предикатов k-значной логики ($k \geqslant 2$) были решены в [1, 2]. Пусть Π_2 — множество всех булевских предикатов от конечного числа переменных из $\mathcal{X}$. В [5] получено прямое доказательство критерия полноты предикатных схем в Π_2.

В данной работе рассматривается базис из двух булевских предикатов Б $= \{\sigma_2^1, \kappa\}$, где предикат σ_2^1 — естественная реализация инвертора, а предикат κ — замыкающего контакта в классе предикатных схем. Данные предикаты можно представить в виде матриц [1, 2]), столбцы которых состоят из допустимых наборов, следующим образом:

$$\sigma_2^1(x_1,\, x_2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \kappa(x_1,\, x_2,\, x_3) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Полюс предиката κ соответсвующий переменной x_1 будем называть затвором. В [5] было установлено, что система Б является полной в Π_2. Пусть $\mathcal{U}^{\mathrm{P}}$ — класс предикатных схем, построенных в базисе Б, а $\Pi_2(n)$ — множество всех булевских предикатов от n переменных $x_1, \ldots, x_n$. Под сложностью $L(\Sigma)$ предикатной схемы Σ, $\Sigma \in \mathcal{U}^{\mathrm{P}}$, понимается число её предикатов, а под сложностью $L^{\mathrm{P}}(\phi)$ предиката ϕ — минимальная из сложностей реализующих его схем. Введем обычным образом функцию Шеннона

$$L^{\mathrm{P}}(n) = \max_{\phi \in \Pi_2(n)} L^{\mathrm{P}}(\phi)$$

для класса $\mathcal{U}^{\mathrm{P}}$ относительно сложности L в базисе Б.

Основным результатом работы является следующее утверждение.

Теорема. *Для функции Шеннона $L^{\mathrm{P}}(n)$ справедливо равенство*

$$L^{\mathrm{P}}(n) = \frac{2^{n-1}}{n}\left(1 + \frac{2{,}5\log n \pm O(1)}{n}\right).$$

Рассмотрим специальные предикатные конструкции обобщающие разложение булевской функции по части её переменных [4]. Предикат $Q_n(x_1, \ldots, x_n,\ y_0, \ldots, y_{2^n-1})$ будем называть предикатным мультиплексором, если для него допустимыми являются только наборы вида $(\sigma_1, \ldots, \sigma_n,\ \delta_0, \ldots, \delta_{2^n-1})$, где $\delta_i = 1$, если $i = \nu(\sigma_1, \ldots, \sigma_n)$, то есть набор $(\sigma_1, \ldots, \sigma_n)$ является двоичной записью числа i и δ_i произвольно в остальных случаях. Предикатный мультиплексор можно реализовать на основе контактного дерева, используя предикатный контакт, при этом сложность построенного таким образом мультиплекосра не будет превосходить $2^{n+1}+n+1$. Рассмотрим разложение предиката $\phi(x_1, \ldots, x_n)$ по части его переменных

$$\phi(x', x'') = \bigvee_{\sigma'' = (\sigma_{r+1}, \ldots, \sigma_n)} x_{r+1}^{\sigma_{r+1}} \ldots x_n^{\sigma_n} \cdot \phi_{\sigma''}(x'), \qquad (1)$$

где $x' = (x_1, \ldots, x_r)$, $x'' = (x_{r+1}, \ldots, x_n)$ и для всех σ'', $\sigma'' \in B^{n-r}$, $\phi_{\sigma''}(x') = \phi(x', \sigma'')$ — так называемые остаточные предикаты. Разложение (1) можно реализовать при помощи предикатного мультиплексора и специальной моделирующей схемы для остаточных предикатов от БП $x', z_0, \ldots, z_{2^{n-r}-1}$, где с каждым предикатом $\phi_{\sigma''}$ ассоциируется полюс $z_{\nu(\sigma'')}$, который принимает истинное значение тогда и только тогда, когда на полюсах соответствующих переменным из x' формируется набор σ', а на полюсах, соответствующих другим остаточным предикатам, формируется значение 0, если данный предикат принимает ложное значение на σ', и принимает либо значение 1, либо произвольное значение, если данный предикат примет истинное значение на σ'.

Лемма 1. *Для любого предиката ϕ, $\phi \in \Pi_2(n)$, существует реализующая его предикатная схема Σ_ϕ, $\Sigma_\phi \in \mathcal{U}^{\mathrm{P}}$, такая, что*

$$L^{\mathrm{P}}(\Sigma_\phi) \leqslant \frac{2^{n-1}}{n}\left(1 + \frac{2{,}5\log n + O(1)}{n}\right).$$

Доказательство. Построим схему Σ_ϕ, которая реализует произвольный предикат $\phi(x_1, \ldots, x_n)$ на основе разложения (1). Рассмотрим разбиение $\Delta = \{\delta_1, \ldots, \delta_{2p}\}$ единичного куба B^r, такое что

$|\delta_i| = s_i$, $i = 1, \ldots, 2p$. Будем предполагать, что $s' \leqslant 2^r$, $s'' \leqslant 2^r$, $p = \lceil \frac{2^r}{s'+s''} \rceil$, $s_1 = \cdots = s_p = s'$, $s_{p+1} = \cdots = s_{2p-1} = s''$, $s_{2p} = 2^r - ps' - (p-1)s'' \leqslant s''$. Рассмотрим первые p компонент разбиения Δ и пусть $G^{(i)}$ множество всевозможных предикатов π, $\pi \in \Pi_2(r)$, которые принимают ложное значение на всех наборах всех компонент разбиения, кроме δ_i и δ_{p+i}, причем на δ_{p+i} они принимают только истинное значение. Для компонент разбиения $\delta_{p+1}, \ldots, \delta_{2p}$ определим $G^{(p+1)}$ как множество всех тех предикатов π, $\pi \in \Pi_2(r)$, которые принимают ложное значение на всех наборах первых p компонент разбиения Δ и одинаковые значения на наборах компонент разбиения $\delta_{p+1}, \ldots, \delta_{2p}$, которые имеют одинаковое "смещение" относительно первого элемента компоненты. Пусть $G^* = G^{(1)} \cup \ldots \cup G^{(p+1)}$, тогда для каждого предиката из этого множества можно построить предикат, который будет моделировать исходный предикат значением специально выделенного полюса (1 — исходный предикат истенен на наборе, 0 — в противном случае). Обобщая метод каскадов [3], предикаты этого множества можно реализовать со сложностью не превосходящей $6|G^*|$.

Используя предикатные контакты, построим предикат κ_p, который является суперпозицией p контактов по одной из вершин не являющейся затвором. При этом вершину, по которой производилась суперпозиция, назовем обобщенной вершиной, а вершины, отличные от затворов контактов и не участвовавшие в суперпозиции, назовем свободными. Используя предикаты, моделирующие предикаты из G^* и предикат κ_p, можно построить моделирующую схему G. Сначала реализуем все предикаты моделирующие предикаты из множества G^*, обьединяя полюса, соответствующие переменным моделируемых предикатов. Далее для каждого остаточного предиката $\phi_{\sigma''}$ соединим свободные вершины и контакты κ_p следующим образом: i-й, $i = 1, \ldots, p$, затвор соединяется с полюсом моделирующего предиката из $G^{(i)}$ так, что этот предикат на наборах из δ_i моделирует предикат, который поучается из $\phi_{\sigma''}$ инвертированием значений состояний предиката, а j-ая, $j = p+1, \ldots, 2p$, свободная вершина соединяется с полюсом моделирующего предиката из $G^{(p+1)}$ так, что этот предикат на наборах из δ_j моделирует предикат $\phi_{\sigma''}$. Обобщенный полюс пометим $z_{\nu(\sigma'')}$. Проделывая аналогичную операцию для всех отстаточных предикатов, получим предикат G. Обьединяя полюса предикатного дешифратора с соответствующими полюсами предиката G, получим искомый предикат ϕ. При этом аналогичным образом построенная предикатная схема будет иметь сложность, которая удовлетворяет следующим неравенствам

$L^{\mathrm{P}}(\Sigma_\phi) \leqslant 2^{n-r}(p+2) + 6\left(p \cdot 2^{s'} + 2^{s''}\right) + O(n)$. При $s' = \lceil n - 3\log n \rceil$, $s'' = \lceil n - 2\log n \rceil$ и $r = \lceil 2\log n \rceil$ справедливы неравенства

$$L^{\mathrm{P}}(\Sigma_\phi) \leqslant \frac{2^{n-1}}{n - 2{,}5\log n} + O\left(\frac{2^n}{n^2}\right) = \frac{2^{n-1}}{n}\left(1 + \frac{2{,}5\log n + O(1)}{n}\right).$$

Лемма доказана.

Для получения нижней оценки воспользуемся мощностными соображениями. При это будем использовать более удобное для подсчета представление предикатных схем в рассматриваемом базисе аналогичное представлению итеративных контактных схем из [4]. Пусть $\|\mathcal{U}^{\mathrm{P}}(L,n)\|$ — число попарно неэквивалентных схем из класса $\mathcal{U}^{\mathrm{P}}$ сложности не более L от n переменных $x_1, \ldots, x_n$. Тогда, используя технику, приведенную в [3], число неэквивалентных преобразованных схем можно оценить сверху следующим неравенством, справедливым для произвольных натуральных значений L и n:

$$\|\mathcal{U}^{\mathrm{P}}(L,n)\| \leqslant 2L^3 32^L \left(\left(\frac{c(L+n)^2}{(\log(L+n))^3}\right)^{L+n} + (bL+n)^L\right), \qquad (2)$$

где c и b — некоторые константы.

Из оценки (2) и мощностного равенства $\|\mathcal{U}^{\mathrm{P}}(L,n)\| = 2^{2^n}$ стандартными методами получения нижних мощностных оценок устанавливается справедливость следующего утверждения

Лемма 2. Для функции Шеннона справедлива следующая оценка

$$L^{\mathrm{P}}(n) \geqslant \frac{2^{n-1}}{n}\left(1 + \frac{2{,}5\log n - O(1)}{n}\right).$$

Из лемм 1 и 2 вытекает справедливость основной теоремы данной работы.

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

Список литературы

1. Боднарчук В. Г., Калужнин Л. А., Котов В. Н., Ромов Б. А. Теория Галуа для алгебр Поста. I // Кибернетика. — 1969. —№ 3. — С. 1–10.

2. Боднарчук В. Г., Калужнин Л. А., Котов В. Н., Ромов Б. А. Теория Галуа для алгебр Поста. II // Кибернетика. 1969. —№ 5. — С. 1–10.

3. Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. Вып. 6. — М.: Наука. Физматлит, 1996. — С. 189–214.

4. Ложкин С. А. Лекции по основам кибернетики. — М.: Издательский отдел факультета ВМиК МГУ им. М. В. Ломоносова, 2004.

5. Шуплецов М. С. О реализации булевых предикатов в одном классе логических сетей // Курсовая работа (кафедра математической кибернетики факультета ВМиК). — МГУ, 2005.

ОБ ОДНОЙ ФОРМЕ ПРЕДСТАВЛЕНИЯ РЕКУРРЕНТНЫХ СХЕМ ПОРОЖДЕНИЯ СЛОВ И ИХ АДДИТИВНАЯ СЛОЖНОСТЬ

Ю. В. Мерекин (Новосибирск)

Аддитивной сложностью $L(w)$ слова w называется длина кратчайшей схемы порождения этого слова с помощью аддитивной операции.

Определим рекуррентную схему на основе построения «словарной» матрицы. Пусть $h(x,y)$ и $l(x,y)$, $1 \le x \le y$, такие целочисленные функции, что $0 \le l(x,y) \le h(x,y) < x$. Рассмотрим бесконечную верхне-треугольную матрицу $(w_{i,j}) = (w(h,l)_{i,j})$, в которой:

a) отличные от нуля элементы являются словами в алфавите $\Sigma = \langle w_{1,1}, \ldots, w_{1,q} \rangle$, $q \ge 1$;

b) элементы первой строки $w_{1,1}, \ldots, w_{1,j}, \ldots$, где $w_{1,j} = w_{1,j+q}$, $j \ge 1$, есть символы алфавита;

c) элементы второй строки $w_{2,2}, \ldots, w_{2,j}, \ldots$, $j \ge 2$, есть $w_{2,j} = w_{1,j-1} w_{1,j}$;

d) элементы i-й строки $w_{i,i}, \ldots, w_{i,j}, \ldots$, $3 \le i \le j$, есть $w_{i,j} = w_{i-1,j-1} w_{i-h(i,j),j-l(i,j)}$.

Из построения матрицы следует, что для слов главной диагонали выполняются условия $w_{1,1} \subset w_{2,2} \subset w_{3,3} \ldots$, которые определяют бесконечное слово $w_\infty = \lim_{i \to \infty} w_{i,i}$. Тем самым определён класс слов, которые назовём *словами типа Туэ — Морса*. Получены неравенства $i - 1 \le L(w_{i,i}) \le (i^2 - i)/2$, определяющие границы значений аддитивной сложности слов типа Туэ — Морса, и для обобщенной последовательности Туэ — Морса доказана

Теорема. *При любом $i \ge q$ для всякого слова $w_{i,i}$ матрицы $(w(1,0)_{i,j})$ в конечном алфавите $\Sigma = \langle w_{1,1}, \ldots, w_{1,q} \rangle$, $q \ge 2$, справедливо равенство*

$$L(w_{i,i}) = q(i-q) + \left(\begin{array}{c} q \\ 2 \end{array} \right).$$

Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 05-01-00364)

О РАНГЕ НЕЯВНЫХ ПРЕДСТАВЛЕНИЙ ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ НАД КЛАССОМ МОНОТОННЫХ ФУНКЦИЙ

Е. В. Михайлец (Москва)

Понятие неявной выразимости функций k-значной логики введено А. В. Кузнецовым как одно из обобщений понятия выразимости функций суперпозициями [1].

Пусть A — произвольная система функций k-значной логики, $A \subseteq P_k$. *Системой неявных уравнений* над системой функций A будем называть всякую систему уравнений вида

$$\left\{ \begin{array}{l} \Phi_1(x_1, \ldots, x_n, y) = \Psi_1(x_1, \ldots, x_n, y), \\ \qquad \ldots \\ \Phi_q(x_1, \ldots, x_n, y) = \Psi_q(x_1, \ldots, x_n, y), \end{array} \right. \qquad (1)$$

где $\Phi_1, \ldots, \Phi_q$, $\Psi_1, \ldots, \Psi_q$ — некоторые формулы над системой функций A.

Говорят, что функция $f(x_1, \ldots, x_n)$ k-значной логики *неявно выразима* над системой функций A, если существует система неявных уравнений над A вида (1), имеющая при любых фиксированных значениях $x_1, \ldots, x_n$ единственное решение $y = f(x_1, \ldots, x_n)$. При этом соответствующую систему уравнений называют *неявным представлением* функции $f(x_1, \ldots, x_n)$ над A.

Множество всех функций f, $f \in P_k$, неявно выразимых над системой функций A, принято называть *неявным расширением* системы A и обозначать через $I(A)$. Благодаря очевидному соотношению

$I(A) = I([A])$, при исследовании неявных расширений можно ограничиться рассмотрением только замкнутых относительно суперпозиции классов функций k-значной логики.

Рассмотрим произвольную функцию f из неявного расширения некоторой системы A функций k-значной логики, $f \in I(A)$. Назовем *рангом* функции f над системой A и будем обозначать через $m_A^k(f)$ наименьшее число уравнений, достаточное для построения неявного представления f над A.

Как обычно, вводится функция Шеннона $m_A^k(n) = \max m_A^k(f)$, называемая *ранговой функцией* системы A (максимум берется по всем функциям k-значной логики, принадлежащим неявному расширению системы A и существенно зависящим не более чем от n переменных).

О. М. Касим-Заде в работе [2] исследовал поведение ранговой функции $m_A^2(n)$ для всех замкнутых классов булевых функций. Для классов D_2 и F_i^μ, где $i = 2, 3, 6, 7$ и $\mu = 2, 3, \ldots, \infty$, в работе [2] получены порядки роста величины $m_A^2(n)$, а для всех остальных замкнутых классов найден точный вид ранговой функции. В частности, для класса монотонных функций О. М. Касим-Заде доказал следующую теорему.

Теорема 1 [2]. *При всех натуральных n для ранговой функции $m_A^2(n)$, где A — класс монотонных функций в P_2, имеет место равенство*

$$m_A^2(n) = \left\lceil \frac{n+2}{2} \right\rceil.$$

В настоящей работе получено точное выражение для ранговой функции класса монотонных функций в P_k. Оказывается, ранговая функция дла данного класса не зависит от k и при любых натуральных $k \geq 2$ определяется формулой из теоремы 1.

Определение 1. Назовем функцию $f(x_1, \ldots, x_n)$ k-значной логики *монотонной*, если для любых наборов $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_n)$, таких что $\tilde{\alpha} \leq \tilde{\beta}$, выполняется неравенство $f(\tilde{\alpha}) \leq f(\tilde{\beta})$.

Определение 2. Будем называть *l-м слоем* в E_k^n множество всех n-мерных наборов $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n) \in E_k^n$, для которых $\sum\limits_{i=1}^{n} \alpha_i = l$.

Легко видеть, что $0 \leq l \leq n(k-1)$.

Определение 3. *Весом* набора $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n) \in E_k^n$ будем называть сумму его компонент и обозначать через $|\tilde{\alpha}|$, $|\tilde{\alpha}| = \sum\limits_{i=1}^{n} \alpha_i$.

Очевидно, что вес набора совпадает с номером слоя, которому принадлежит набор.

Отметим, что класс A всех монотонных функций в P_k является неявно полным, то есть его неявное расширение совпадает с P_k, $I(A) = P_k$.

Теорема 2. *При всех натуральных $k \geq 2$ и натуральных n для ранговой функции $m_A^k(n)$, где A — класс монотонных функций в P_k, имеет место равенство*

$$m_A^k(n) = \left\lceil \frac{n+2}{2} \right\rceil.$$

Доказательство. Доказательство теоремы разбивается на две части: получение верхней и нижней оценки для ранговой функции. Выведем нижнюю оценку.

Зафиксируем натуральное число n. Возьмем некоторую максимальную цепь Ω_n в кубе E_n^k вида $\tilde{0} = \tilde{\alpha}^0 \leq \tilde{\alpha}^1 \leq \cdots \leq \tilde{\alpha}^{n(k-1)} = \widetilde{(k-1)}$. Она имеет длину $n(k-1)$, т. е. состоит из $n(k-1)+1$ различных наборов. Рассмотрим функцию $f(x_1, \ldots, x_n)$ k-значной логики, заданную следующим образом. На цепи Ω_n она принимает значения: $f(\tilde{\alpha}^0) = 1$, $f(\tilde{\alpha}^1) = 2$, $\ldots$, $f(\tilde{\alpha}^{k-2}) = k-1$, $f(\tilde{\alpha}^{k-1}) = k-2$, далее $f(\tilde{\alpha}^{k+i}) = k-1$ при четных значениях i, $f(\tilde{\alpha}^{k+i}) = k-2$ при нечетных значениях i, где $0 \leq i \leq n(k-1) - k$.

Пусть $0 \leq l \leq n(k-1)$. Для любого набора $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ на l-ом слое куба E_k^n положим $f(\tilde{\alpha}) = f(\tilde{\alpha}^l)$, где $\tilde{\alpha}^l$ — набор цепи Ω_n, принадлежащий l-му слою.

На основе цепи Ω_n построим максимальную цепь Ω'_{n+1} в E_k^{n+1}, состоящую из расширенных наборов: $(\tilde{\alpha}^0, 0) \leq (\tilde{\alpha}^0, 1) \leq (\tilde{\alpha}^1, 1) \leq (\tilde{\alpha}^1, 2) \leq \cdots \leq (\tilde{\alpha}^{k-2}, k-2) \leq (\tilde{\alpha}^{k-2}, k-1) \leq (\tilde{\alpha}^{k-1}, k-1) \leq (\tilde{\alpha}^k, k-1) \leq \cdots \leq (\tilde{\alpha}^{n(k-1)}, k-1)$. Легко видеть, что цепь Ω'_{n+1} имеет длину $(n+1)(k-1)$ (т. е. содержит $(n+1)(k-1)+1$ наборов). Для удобства обозначим наборы цепи Ω'_{n+1} следующим образом: $\tilde{\beta}^0 = (\tilde{\alpha}^0, 0), \tilde{\beta}^1 = (\tilde{\alpha}^0, 1), \ldots, \tilde{\beta}^{(n+1)(k-1)} = (\tilde{\alpha}^{n(k-1)}, k-1)$.

Заметим, что каждый набор $\tilde{\beta}^i$ цепи Ω'_{n+1} с нечетным номером i является точкой графика функции f, а каждый набор $\tilde{\beta}^i$ с четным номером i не является точкой графика функции f, $0 \leq i \leq (n+1)(k-1)$.

Рассмотрим произвольное неявное представление $E(f)$ функции $f(x_1, \ldots, x_n)$ над классом A монотонных функций в P_k, пусть оно

содержит m уравнений:

$$\begin{cases} \varphi_1(x_1,\dots,x_n,y) = \psi_1(x_1,\dots,x_n,y), \\ \dots \\ \varphi_m(x_1,\dots,x_n,y) = \psi_m(x_1,\dots,x_n,y). \end{cases}$$

Введем вектор-функции $\Phi(\tilde{x},y) = (\varphi_1(\tilde{x},y),\dots,\varphi_m(\tilde{x},y))$, $\Psi(\tilde{x},y) = (\psi_1(\tilde{x},y),\dots,\psi_m(\tilde{x},y))$, где $\tilde{x} = (x_1,\dots,x_n)$. Непосредственно из определения неявного представления вытекает, что в точках $(\tilde{\alpha},f(\tilde{\alpha})) \in E_k^{n+1}$ графика функции $f(\tilde{x})$ верно равенство $\Phi(\tilde{\alpha},f(\tilde{\alpha})) = \Psi(\tilde{\alpha},f(\tilde{\alpha}))$, в остальных точках $(\tilde{\alpha},\delta) \in E_k^{n+1}$, $\delta \neq f(\tilde{\alpha})$, — неравенство $\Phi(\tilde{\alpha},\delta) \neq \Psi(\tilde{\alpha},\delta)$.

Кроме того, вектор-функции $\Phi(\tilde{x},y)$ и $\Psi(\tilde{x},y)$ монотонны в следующем смысле: если $(\tilde{\alpha},\delta) \le (\tilde{\gamma},\tau)$, где $(\tilde{\alpha},\delta),(\tilde{\gamma},\tau) \in E_k^{n+1}$, то для каждого i, $1 \le i \le m$, выполняются соотношения $\varphi_i(\tilde{\alpha},\delta) \le \varphi_i(\tilde{\gamma},\tau)$ и $\psi_i(\tilde{\alpha},\delta) \le \psi_i(\tilde{\gamma},\tau)$.

Таким образом, на цепи Ω'_{n+1} вектор-функции $\Phi(\tilde{x},y)$ и $\Psi(\tilde{x},y)$ монотонно не убывают, при этом на наборах $\tilde{\beta}^i$ с четными номерами $\Phi(\tilde{\beta}^i) \neq \Psi(\tilde{\beta}^i)$, на наборах $\tilde{\beta}^i$ цепи Ω'_{n+1} с нечетными номерами $\Phi(\tilde{\beta}^i) = \Psi(\tilde{\beta}^i)$ при всех i, $0 \le i \le (n+1)(k-1)$. Отсюда вытекает, что при всех нечетных значениях i из промежутка $1 \le i \le (n+1)(k-1)-2$ справедливы неравенства $|\Phi(\tilde{\beta}^{i+2})| \ge |\Phi(\tilde{\beta}^i)|+1$, $|\Psi(\tilde{\beta}^{i+2})| \ge |\Psi(\tilde{\beta}^i)|+1$.

Пусть число $(n+1)(k-1)$ нечетно. Тогда набор $\tilde{\beta}^{(n+1)(k-1)} = \widetilde{(k-1)}$ — точка графика функции f. В этом случае получаем

$$\begin{cases} |\Phi(\tilde{\beta}^{(n+1)(k-1)})| \ge |\Phi(\tilde{\beta}^1)| + ((n+1)(k-1)-1)/2, \\ |\Psi(\tilde{\beta}^{(n+1)(k-1)})| \ge |\Psi(\tilde{\beta}^1)| + ((n+1)(k-1)-1)/2. \end{cases} \qquad (2)$$

Пусть $(n+1)(k-1)$ четно. Тогда, аналогично,

$$\begin{cases} |\Phi(\tilde{\beta}^{(n+1)(k-1)-1})| \ge |\Phi(\tilde{\beta}^1)| + ((n+1)(k-1)-2)/2, \\ |\Psi(\tilde{\beta}^{(n+1)(k-1)-1})| \ge |\Psi(\tilde{\beta}^1)| + ((n+1)(k-1)-2)/2. \end{cases}$$

Так как в четном случае набор $\tilde{\beta}^{(n+1)(k-1)} = \widetilde{(k-1)}$ не является точкой графика, то на нем $\Phi(\tilde{\beta}^{(n+1)(k-1)}) \neq \Psi(\tilde{\beta}^{(n+1)(k-1)})$, в то время как $\Phi(\tilde{\beta}^{(n+1)(k-1)-1}) = \Psi(\tilde{\beta}^{(n+1)(k-1)-1})$. Не нарушая общности, будем считать, что $\Phi(\tilde{\beta}^{(n+1)(k-1)}) \ge \Psi(\tilde{\beta}^{(n+1)(k-1)})$ и, следовательно,

$|\Phi(\tilde{\beta}^{(n+1)(k-1)})| \ge |\Phi(\tilde{\beta}^{(n+1)(k-1)-1})| + 1$. Таким образом,

$$|\Phi(\tilde{\beta}^{(n+1)(k-1)})| \ge |\Phi(\tilde{\beta}^1)| + (n+1)(k-1)/2, \qquad (3)$$

Так как набор $\tilde{\beta}^0 = \tilde{0}$ — не точка графика, то $\Phi(\tilde{\beta}^0) \neq \Psi(\tilde{\beta}^0)$, при этом $\Phi(\tilde{\beta}^1) = \Psi(\tilde{\beta}^1)$. В силу монотонности вектор-функций $\Phi(\tilde{x},y)$ и $\Psi(\tilde{x},y)$ заключаем, что $|\Phi(\tilde{\beta}^1)| \ge 1$ и $|\Psi(\tilde{\beta}^1)| \ge 1$. Учитывая этот факт и объединяя (2) и (3), в конечном итоге получаем

$$|\Phi(\widetilde{k-1})| \ge \left\lceil \frac{(n+1)(k-1)+1}{2} \right\rceil.$$

С другой стороны, $|\Phi(\widetilde{k-1})| \le m(k-1)$, следовательно,

$$m \ge \left\lceil \frac{(n+1)(k-1)+1}{2(k-1)} \right\rceil. \qquad (4)$$

Итак, для каждого натурального n в P_k найдется функция $f(x_1,\dots,x_n)$, неявное представление которой над классом A всех монотонных функций содержит m уравнений, где m удовлетворяет неравенству (4). Это означает, что

$$m_A^k(n) \ge \left\lceil \frac{(n+1)(k-1)+1}{2(k-1)} \right\rceil. \qquad (5)$$

Верхняя оценка

$$m_A^k(n) \le \left\lceil \frac{(n+1)(k-1)+1}{2(k-1)} \right\rceil \qquad (6)$$

в данной статье приводится без доказательства.

Легко видеть, что при $k \ge 2$ верно $\left\lceil \frac{(n+1)(k-1)+1}{2(k-1)} \right\rceil = \left\lceil \frac{n+2}{2} \right\rceil$. Следовательно, из соотношений (5) и (6) вытекает равенство

$$m_A^k(n) = \left\lceil \frac{n+2}{2} \right\rceil,$$

что завершает доказательство теоремы 2.

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

и Программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики» (проект «Синтез и сложность управляющих систем»).

Список литературы

1. Кузнецов А. В. О средствах для обнаружения невыводимости или невыразимости // Логический вывод. — М.: Наука, 1979. — С. 5–33.

2. Касим-Заде О. М. Об одной метрической характеристике неявных и параметрических представлений булевых функций // Математические вопросы кибернетики. Вып. 6. — М.: Наука. Физматлит, 1996. — С. 133–188.

ОБ ОДНОМ КЛАССЕ СХЕМ

Е. А. Окольнишникова (Новосибирск)

В данной работе вводится класс схем, моделирующих работу параллельных машин. Одним из простейших классов схем, моделирующих работу вычислительных параллельных машин с общим доступом к памяти являются схемы ограниченной ширины. Для моделирования работы параллельных машин с распределенной памятью [1, 2] предлагаются распределенные схемы. Распределенная схема (схема из функциональных элементов или ветвящаяся программа) состоит из m процессоров (схем), при этом каждый процессор работает самостоятельно, но разрешается определенное число раз за время работы схем использовать результаты вычислений, полученных на предыдущем уровне любым из остальных процессоров. Схема ограниченной ширины является частным случаем распределенной схемы, когда возможно использование результатов вычислений, полученных любым процессором на всех предыдущих уровнях.

Напомним определение ветвящейся программы ограниченной ширины. Говорят, что детерминированная ветвящаяся программа имеет ширину d, если она разбита на уровни и на каждом уровне имеется не более d вершин. При этом дуги ориентированы из вершин меньшого уровня в вершины большего уровня. Для сложности вычисления булевых функций схемами с этим ограничением был получен ряд интересных результатов. В частности, для программ ширины d Л. Бабаи, П. Пудлак, Р. Редл и М. Семереди [3] получили нижние оценки сложности вычисления полностью определенных симметрических булевых функций $\Omega(n \log n)$ (в том числе функции голосования MAJ_n). В [4] были получены оценки $\Omega(n \log\log n)$ для сложности вычисления неконстантных пороговых функций программами ограниченной ширины.

Скажем, что схема из функциональных элементов имеет ширину d, если множество ее элементов разбито на уровни и на каждом уровне имеется не более d элементов. При этом выход элементов меньшего уровня направлен на входы элементов большего уровня. Напомним, что входы схемы, переменные, не являются элементами.

Введем определение распределенных ветвящихся программ и распределенной схемы из функциональных элементов. Распределенная ветвящаяся программа от переменных $x_1, \ldots, x_n$ — система, состоящая из m ветвящихся программ (процессоров) от переменных $x_1, \ldots, x_n$. Вершины каждой ветвящейся программы занумерованы. Пусть уровни $i_1, i_2, \ldots, i_l$, где $i_1 < i_2 < \ldots < i_l$, определены как уровни, на которых возможен обмен информацией. Положим $i_0 = 0$. Тогда дуги из вершины с номером i', $i_p \le i' < i_{p+1}$, принадлежащей j'-й ветвящейся программы, могут идти как в вершины с номерами i, $i > i'$, той же ветвящейся программы, так и в вершины с номерами i, где $i \ge i_{p+1}$, остальных программ. Распределенная ветвящаяся программа вычисляет систему булевых функций $\{0,1\}^n \to \{0,1\}^m$. Под временем вычисления T распределенной ветвящейся программы понимается максимальное число вершин в программах, входящих в систему. Можно ввести определение сложности $\widetilde{T}$ распределенной ветвящейся программы, в котором учитывается объем информации, полученной каждым из процессоров в ходе обмена информацией.

Аналогичным образом определяется распределенная схема из функциональных элементов. Распределенная схема из функциональных элементов от переменных $x_1, \ldots, x_n$ — система, состоящая из m схем из функциональных элементов (процессоров) от переменных $x_1, \ldots, x_n$. Элементы каждой схемы занумерованы. Пусть уровни $i_1, i_2, \ldots, i_l$, где $i_1 < i_2 < \ldots < i_l$, определены как уровни, на которых возможен обмен информацией. Положим $i_0 = 0$. Тогда дуги из элемента с номером i', $i_p \le i' < i_{p+1}$, принадлежащей j'-й схеме из функциональных элементов, могут идти как на входы элементов i, $i > i'$, той же схемы, так и на входы элементов с номерами i, где $i \ge i_{p+1}$, остальных схем. Распределенная схема из функциональных элементов вычисляет систему булевых функций $\{0,1\}^n \to \{0,1\}^m$. Под временем вычисления T распределенной схемы из функциональных элементов понимается максимальное число вершин в схемах, входящих в систему. Можно ввести определение сложности $\widetilde{T}$ рас-

пределенной схемы, в котором учитывается объем информации, полученной каждым из процессоров в ходе обмена информацией.

Предложены последовательности систем булевых функций из $\{0,1\}^n$ в $\{0,1\}^{m(n)}$, где $m(n) \to \infty$ при $n \to \infty$, для которых разрешение однократного обмена информацией позволяет существенно уменьшить время работы системы как для меры сложности T, так и для меры сложности $\widetilde{T}$. Данное упрощение возможно как в классе ветвящихся программ, так и в классе схем из функциональных элементов.

Работа выполнена при финансовой поддержке программы фундаментальных исследований ОМН РАН.

Список литературы

1. Параллельная машина // Энциклопедия "Дискретная математика". — М.: Большая Российская энциклопедия, 2004. — С. 193–194.

2. Параллельных вычислений теория // Энциклопедия "Дискретная математика". — М.: Большая Российская энциклопедия, 2004. — С. 194–196.

3. Babai L., Pudlák P., Rödl V., Szemerédi M. Lower bounds to the complexity of symmetric Boolean functions // Theoret. Comput. Sci. — 1990. — V. 74. — P. 313–324.

4. Barrington D. A. M., Straubing H. Superlinear lower bounds for bounded-width branching programs // J. Computer and System Sci. — 1995. — V. 50, № 3. — P. 374–381.

РАЗМЕР МАКСИМАЛЬНОГО МНОЖЕСТВА, СВОБОДНОГО ОТ ПРОИЗВЕДЕНИЙ В ГРУППАХ ПОРЯДКА pq

Т. Г. Петросян (Москва)

В работе получено точное значение размера максимального множества, свободного от произведений, в группах порядка pq (везде далее предполагается, что p и q — простые числа), $p \equiv 2 \pmod 3$.

Будем называть M *множеством, свободным от произведений* (МСП), если уравнение $xy = z$ не имеет решений в множестве M. Обозначим семейство всех МСП группы G через $PF(G)$. Множество M, свободное от произведений, называется *максимальным*, если $|M| \geq |T|$ для любого $T \in PF(G)$. Обозначим через $\lambda(G)$ размер максимального МСП в группе G. Пусть $\mu(G) = \lambda(G)/|G|$.

В классе абелевых групп задача нахождения размера максимального МСП окончательно решена в статье [1].

Разобьем класс конечных абелевых групп на три подкласса и определим на этих подклассах функцию $\nu(G)$:

1) класс 1: n делится на простое $p \equiv 2 \pmod 3$, $\nu(G) = \frac{1}{3} + \frac{1}{3p}$, где p – наименьшее такое простое число;

2) класс 2: n не делится ни на какое простое $p \equiv 2 \pmod 3$, но $3|n$, $\nu(G) = \frac{1}{3}$;

3) класс 3: n делится только на простые $p \equiv 1 \pmod 3$, $\nu(G) = \frac{1}{3} - \frac{1}{3m}$, где m – является экспонентой G.

Теорема 1 (Грин — Ружа, [1]). *Для любой абелевой группы G выполняется $\mu(G) = \nu(G)$.*

По данной проблеме практически нет работ в классе произвольных конечных групп. Первый результат, по-видимому, получен в [2].

Теорема 2 (Диананда — Яп, [2]). *Пусть $|G| = 3q$, где q — простое число, сравнимое с 1 (mod 3). Тогда $\mu(G) = 1/3$.*

В [3] изучена структура максимальных МСП в группах порядка $3p$, $p \equiv 1 \pmod 3$. Получен следующий результат.

Теорема 3 (Яп, [3]). *Пусть G произвольная группа порядка $3p$, где p — простое число, и $p \equiv 1 \pmod 3$. Если S — максимальное МСП в G, то тогда оно является смежным классом по некоторой подгруппе H порядка p группы G.*

В данной работе получено обобщение теоремы 2.

Теорема 4. *Пусть G группа порядка pq и $p \neq 3k+1$ при любом $k \in \mathbb{N}$. Тогда*

$$\lambda(G) = q, \tag{1}$$

если $p = 3$, и

$$\lambda(G) = \frac{q(p+1)}{3},$$

если $p \equiv 2 \pmod 3$.

В работе используются следующие теоремы.

Теорема 5 (Олсон, [4]). *Пусть A и B являются конечными непустыми подмножествами группы G, тогда существует подмножество S множества AB и подгруппа H группы G, такие, что $|S| \geq |A| + |B| - |H|$, и либо $SH = S$, либо $HS = S$.*

Теорема 6 (Яп, [5]). *Пусть* $S \in MPF(\mathbb{Z}_p)$, $p = 3k+2$. *Тогда* $-S = S$ *и любое максимальное МСС при некотором автоморфизме группы* $\mathbb{Z}_p$ *имеет вид* $\{k+1,\ k+2, \ldots, 2k+1\}$.

Доказательство теоремы 4. Известно, что группы порядка pq, где p и q — простые числа, $p < q$, изоморфны полупрямому произведению циклических групп порядков q и p, соответственно. Пусть $p = 3$. В [2] было доказанно, что при $q \equiv 1 (\mathrm{mod}\ 3)$ выполняется (1). Если $q \equiv 2 (\mathrm{mod}\ 3)$, тогда, поскольку $q-1$ не делится на три, группа G изоморфна прямому произведению циклических групп. Откуда следует (1).

Пусть теперь $p \geq 5$, $p \equiv 2 \pmod 3$, и M — некоторое максимальное МСП. Из теоремы 5 следует, что

$$|MM| \geq 2|M| - |H|, \tag{2}$$

где H — подгруппа группы G, причем множество MM содержит некоторый смежный класс по этой подгруппе. Отсюда следует, что $H \neq G$. Поскольку $MM \cap M = \emptyset$, то из (2) получаем

$$3|M| - |H| \leq |MM| + |M| \leq |G|.$$

Таким образом,

$$|M| \leq \frac{|G| + |H|}{3}.$$

В группе G есть только собственные подгруппы порядков 1, p и q. Поэтому

$$|M| \leq \frac{q(p+1)}{3}.$$

Поскольку $p \neq 3$, то из условия следует, что $p \equiv 2 \pmod 3$. Рассмотрим фактор-группу G/G_q, где G_q — силовская q-подгруппа группы G. Из теоремы 6 следует существование МСП порядка $\frac{p+1}{3}$ в группе G/G_q. Очевидно, что полный прообраз этого множества при каноническом гомоморфизме из G на G/G_q будет МСП. Его мощность равна $\frac{q(p+1)}{3}$.

Список литературы

1. Green B., Ruzsa I. Z. Sum-free sets in abelian groups // Israel J. Math. — 2005. — V. 147. — P. 157–189.

2. Diananda P. H., Yap H. P. Maximal Sum-Free Sets of Elements of Finite Groups // Proc. Japan Acad. — 1969. — V. 45, № 1. — P. 1–5.

3. Yap H. P. Structure of maximal sum-free sets in groups of order $3p$ // Proc. Japan Acad. — 1970. — V. 46. — P. 758–762.

4. Olson J. E. On the sum of two sets in a group // Journal of Number Theory. — 1984. — V. 18. — P. 110–120.

5. Yap H. P. The number of maximal sum-free sets in C_p // Nanta Math. — 1968. — V. 2, №. 1. — P. 68–71.

О ПОЛНОСТЬЮ КОММУТАТИВНО РАЗДЕЛИМЫХ n-КВАЗИГРУППАХ

В. Н. Потапов (Новосибирск)

Алгебраическая система, состоящая из множества A мощности $|A| = k$ и n-арной операции $f : A^n \to A$, однозначно обратимой по каждой своей переменной, называется *n-квазигруппой порядка k*. Принято (см. [1]) называть n-квазигруппой порядка k также и соответствующую функцию f. Таблица значений n-квазигруппы порядка k называется латинским n-кубом измерения k (если $n = 2$, то латинским квадратом).

Введём обозначение $[n] = \{1, \ldots, n\}$. Пусть $\tau : [n] \to [n]$ — перестановка, т. е. $\tau \in S_n$, $\overline{\sigma} = (\sigma_1, \ldots, \sigma_n)$ — набор перестановок $\sigma_i : A \to A$, т. е. $\overline{\sigma} \in S_k^n$. Для набора переменных $\overline{x} = (x_1, \ldots, x_n) \in A^n$ определим $\overline{x}_\tau = (x_{\tau(1)}, \ldots, x_{\tau(n)})$ и $\overline{\sigma x} = (\sigma_1(x_1), \ldots, \sigma_n(x_n))$.

n-Квазигруппа f называется *разделимой*, если найдутся: целое число m, $2 \leq m < n$, $(n-m+1)$-квазигруппа h, m-квазигруппа g и перестановка $\tau \in S_n$, – такие что

$$f(\overline{x}_\tau) \equiv h(g(x_1, \ldots, x_m), x_{m+1}, \ldots, x_n).$$

n-Квазигруппы f и g называются *эквивалентными*, перестановки $\sigma_0 \in S_k$, $\overline{\sigma} \in S_k^n$, $\tau \in S_n$, – такие что

$$f(\overline{x}_\tau) \equiv \sigma_0 g(\overline{\sigma x}).$$

n-Квазигруппы f и g называются *главно изотопными*, если они эквивалентны, причём перестановки $\sigma_0 \in S_k$, $\tau \in S_n$ — тождественные.

Разделимую n-квазигруппу будем называть *полностью коммутативно разделимой*, если она не содержит в качестве подфункций

неразделимых подквазигрупп (размерности более 2) и все её подквазигруппы размерности 2 эквивалентны коммутативным группам.

n-Квазигруппа будем называть *приведённой*, если $f(\overline{0}) = 0$. Приведённую n-квазигруппу будем называть *трансляционно транзитивной*, если для любого набора $\overline{a} \in A^n$ найдутся перестановки $\overline{\sigma} \in S_k^n$ и $\sigma_0 \in S_k$, для которых справедливы равенства $\overline{\sigma}(\overline{0}) = \overline{a}$, $\sigma_0(0) = f(\overline{a})$, $f(\overline{\sigma x}) \equiv \sigma_0(f(\overline{x}))$.

В работе показано, что если n-квазигруппа ($n \geq 6$) порядка 4 не содержит неразделимых подквазигрупп, то она является полностью коммутативно разделимой. Кроме того, построено множество трансляционно транзитивных n-квазигрупп порядка 4 с экспоненциально растущей (относительно n) мощностью.

Утверждение 1. *Пусть $*$ — коммутативная групповая операция, тогда n-квазигруппа $f(x_1, x_2, \ldots, x_n) = x_1 * x_2 * \cdots * x_n$ является трансляционно транзитивной.*

Доказательство. Пусть $a_1 * a_2 * \cdots * a_n = a_0$. Определим $\sigma_i(y) = y * a_i$ для всех $i = 0 \ldots n$. Из ассоциативности и коммутативности операции $*$ имеем равенство

$$f(\overline{\sigma x}) = (x_1 * a_1) * (x_2 * a_2) * \cdots * (x_n * a_n) = x_1 * x_2 * \cdots * x_n * a_0 = \sigma_0(f(\overline{x})).$$

В множестве A зафиксируем нулевой элемент $0 \in A$ и рассмотрим множество $\mathcal{G}$ коммутативных групповых операций на A с этим нулём. Нетрудно видеть, что операции из $\mathcal{G}$ попарно не являются главно изотопными.

В статье [2] было доказано существование и единственность канонического представления разделимых n-квазигрупп. Для полностью коммутативно разделимой n-квазигруппы f оно будет иметь следующий вид

$$f(x_1, x_2, \ldots, x_n) = C_1(u_1) * C_2(u_2) * \cdots * C_k(u_k) * d, \qquad (1)$$

где $k \geq 2$, $* \in \mathcal{G}$, $C_i(u_i) \neq B_1(v_1) * B_2(v_2)$. Здесь и далее C_i, B_j — приведённые квазигруппы различной размерности, u_i, v_j — некоторые непересекающиеся наборы из переменных $x_1, x_2, \ldots, x_n$, упорядоченные по возрастанию номеров.

Нетрудно показать, что другие представления n-квазигруппы f получаются из канонического сложением некоторых наборов слагаемых.

Обозначим через $\pi_i^a[f]$ подфункцию f, полученную подстановкой в f константы $a \in A$ вместо переменной x_i. Используя существование канонических представлений вида (1) для подфункций, можно доказать следующее утверждение.

Утверждение 2. *Пусть f — n-квазигруппа ($n \geq 6$) и для всех $a \in A$ и $i \in [n]$ подфункции $\pi_i^a[f]$ полностью коммутативно разделимы. Тогда для каждого $i \in [n]$ найдётся независимое от a разбиение переменных $\{u_1^i, \ldots u_k^i\}$, такое что для всех $a \in A$ имеем*

$$\pi_i^a[f](u_1^i, u_2^i, \ldots, u_k^i) = C_1^{a,i}(u_1^i) *_{a,i} C_2^{a,i}(u_2^i) *_{a,i} \cdots *_{a,i} C_k^{a,i}(u_k^i) *_{a,i} d_{a,i}.$$

Заметим, что это представление не всегда является каноническим для $\pi_i^a[f]$.

Утверждение 3. *Пусть для n-квазигруппы f найдутся функции $g(u)$ и $h^a(v)$, такие что $\pi_1^a[f](u, v) = g(u) * h^a(v)$ для всех $a \in A$. Тогда f — разделимая.*

Доказательство. Из условия следует, что $f(a, \bar{0}, v) = h^a(v) * g(\bar{0})$. Тогда $f(x_1, u, v) = g(u) * f(x_1, \bar{0}, v) * (g(\bar{0}))^{-1}$.

Используя утверждения 2 и 3, можно доказать следующее.

Теорема 1. *Пусть f — n-квазигруппа ($n \geq 6$) и для всех $a \in A$ и $i \in [n]$ подфункции $\pi_i^a[f]$ полностью коммутативно разделимы. Тогда f — полностью коммутативно разделима.*

Далее рассмотрим случай $|A| = 4$. Нетрудно проверить

Утверждение 4. *Любая 2-квазигруппа порядка 4 эквивалентна коммутативной группе $Z_2 \times Z_2$ или коммутативной группе Z_4.*

Тогда из теоремы 1 вытекает

Следствие. *Пусть n-квазигруппа порядка 4 ($n \geq 6$) не содержит неразделимых подфункций. Тогда она является полностью коммутативно разделимой.*

Обозначим операцию в группе $Z_2 \times Z_2$ через $\oplus$. Нетрудно видеть, что для любой перестановки $\sigma \in S_4$, если $\sigma(0) = 0$, то равенство $\sigma(a) \oplus \sigma(b) = \sigma(a \oplus b)$ справедливо для всех $a, b \in A$. Из этого свойства нетрудно получить

Утверждение 5. *Пусть f — трансляционно транзитивная n-квазигруппа порядка 4. Тогда $(n+m)$-квазигруппа*

$$f(x_1, \ldots, x_{i-1}, x_i \oplus x_{i+1} \oplus x_{i+m}, x_{i+m+1}, \ldots, x_{n+m})$$

является трансляционно транзитивной.

Пусть $p(n)$ — число различных представлений в виде суммы натуральных слагаемых числа n. Известно (см, например, [3]), что $p(n) = \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}}$ при $n \to \infty$.

Теорема 2. *Количество классов эквивалентности трансляционно транзитивных n-квазигрупп порядка 4 не менее $p(n)$.*

Доказательство. Рассмотрим разбиение $J = \{u_1, u_2, \ldots, u_k\}$ множество переменных. Спектром разбиения назовём вектор $Sp(J) = (|u_{i1}|, |u_{i2}|, \ldots, |u_{ik}|)$, где $|u_{i1}| \le |u_{i2}| \le \cdots \le |u_{ik}|$. Определим функции

$$h_i(u_i) = x_{j_1} \oplus \cdots \oplus x_{j_{m(i)}},$$

где $u_i = \{x_{j_1}, \ldots, x_{j_{m(i)}}\}$ и функцию

$$g_J(\overline{x}) = h_1(u_1) * h_2(u_2) * \cdots * h_k(u_k),$$

где $*$ — некоторая коммутативная групповая операция на A, неэквивалентная $\oplus$. Трансляционная транзитивность n-квазигруппы g_J следует из утверждений 1 и 5. Число различных спектров очевидно равняется $p(n)$. Если $Sp(J) \ne Sp(I)$, то неэквивалентность n-квазигрупп g_J и g_I следует из неэквивалентности операций $*$ и $\oplus$.

Асимптотика числа и некоторые другие свойства n-квазигрупп порядка 4 доказаны в [4].

Работа выполнена при финансовой поддержке РФФИ (проект 05-01-00364).

Список литературы

1. Белоусов В. Д. n-Арные квазигруппы — Кишинёв: "Штиинца", 1972.

2. Черёмушкин А. В. Каноническое разложение n-арных квазигрупп // Мат. исследования. —Кишинёв: "Штиинца", 1988. — Вып. 102. — С. 97–105.

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

4. Потапов В. Н., Кротов Д. С. Асимптотика числа n-квазигрупп порядка 4 // Сибирский математический журнал. – В печати.

ОБ ОЦЕНКАХ ФУНКЦИЙ ШЕННОНА ДЛИН ЛОКАЛЬНЫХ ТЕСТОВ ОТНОСИТЕЛЬНО СЛИПАНИЙ

Д. С. Романов, А. Е. Казачёк (Москва)

Пусть n, k, t — натуральные числа $(1 \le k \le n)$, $f(x_1, x_2, \ldots, x_n) = f(\tilde{x}^n)$ — булева функция, и $\Phi_t(\tilde{y}^k) = \{\varphi_i(\tilde{y}^k) \mid i = \overline{1;t}\}$ — система попарно неравных булевых функций k переменных. Обозначим через $\Psi = \Psi_{n,k,t,f,\Phi_t}(\tilde{x}^n)$ систему функций, в которую входит функция $f(\tilde{x}^n)$ и всевозможные функции $\psi(\tilde{x}^n)$ вида $\psi(\tilde{x}^n) = f(x_1, \ldots, x_{j-1},$

$\underbrace{\varphi_i(x_j, x_{j+1}, \ldots, x_{j+k-1}), \ldots, \varphi_i(x_j, x_{j+1}, \ldots, x_{j+k-1})}_{k \text{ раз}}, x_{j+k}, \ldots, x_n)$, где $1 \le j \le n-k+1$, $i \in \{1, \ldots, t\}$. Каждую из функций $\psi(\tilde{x}^n)$, назовем *Ψ-неисправной*. Ясно, что $|\Psi| = t(n-k+1)+1$. Множество T наборов значений переменных $x_1, \ldots, x_n$ называется *локальным диагностическим тестом относительно слипаний переменных булевой функции $f(\tilde{x}^n)$, порожденных системой $\Phi_t(\tilde{y}^k)$*, тогда и только тогда, когда любые две не равные друг другу функции из Ψ различаются на множестве T. Если $t = 2$ и $\Phi_t(\tilde{y}^k) = \{0(\tilde{y}^k), 1(\tilde{y}^k)\}$ $(0(\tilde{y}^k) \equiv 0$, $1(\tilde{y}^k) \equiv 1)$, то локальный тест относительно слипаний переменных, порожденных системой $\Phi_t(\tilde{y}^k)$, будем называть *локальным тестом относительно k-кратных константных слипаний. Тестом для таблицы M* с различными столбцами называется всякое такое множество строк T этой таблицы, что в таблице, составленной из строк этого множества, все столбцы попарно различны. Число наборов (строк) в тесте T называется его *длиной* и обозначается $l(T)$. Тест минимальной длины называется *минимальным*. Длину минимального локального диагностического теста относительно слипаний переменных булевой функции $f(\tilde{x}^n)$, порожденных системой $\Phi_t(\tilde{y}^k)$, будем обозначать через $L_{k,t,\Phi_t}(f(\tilde{x}^n))$. Введем *функцию Шеннона длины минимальных локальных диагностических тестов относительно слипаний переменных булевой функции, порожденных системой* $\Phi_t(\tilde{y}^k)$: $L_{k,t,\Phi_t}(n) = \max\limits_{f(\tilde{x}^n)} l_{k,t,\Phi_t}(f(\tilde{x}^n))$.

В работе [1] изучено поведение функции Шеннона длины проверяющего теста относительно дизъюнктивных нелокальных слипаний, а в работе [2] — поведение функции Шеннона длины единичного диагностического теста относительно константных неисправностей (этот случай совпадает с однократными константными слипаниями) — получено, что $L_{1,2,\{0,1\}}(n) = 2n$.

Легко видеть, что слипания переменных $x_j, x_{j+1}, \ldots, x_{j+k-1}$ функции $f(\tilde{x}^n)$, порожденные функцией $\varphi(\tilde{y}^k)$, у которой $\varphi(\tilde{0}^k) = \varphi(\tilde{1}^k) = \delta$ $(\delta \in \{0,1\})$, неотличимы от слипаний тех же переменных, порожденных тождественной константой $\delta(\tilde{y}^k)$, поэтому везде в дальнейшем будет предполагаться, что система функций $\Phi_t(\tilde{y}^k)$ не содержит отличных от констант функций $\varphi(\tilde{y}^k)$, у которых $\varphi(\tilde{0}^k) = \varphi(\tilde{1}^k)$.

Составим из столбцов значений всех функций $\varphi_i(\tilde{y}^k) \in \Phi_t(\tilde{y}^k)$ $(i = \overline{1;t})$ таблицу $M(\Phi_t)$ и обозначим через $l(\Phi_t)$ длину минималь-

ного теста этой таблицы. В дальнейшем будем для записи булевых наборов использовать символику записи слов в алфавите $\{0,1\}$, считая, что набор $(\alpha_1,\alpha_2,\dots,\alpha_n)$ может быть записан как слово $(\alpha_1\alpha_2\dots\alpha_n)$. При этом через $[s]^p$ будет записываться слово $\underbrace{ss\dots s}_{p\text{ раз}}$ (если слово s состоит из одного символа, квадратные скобки будут опускаться). Если же от слова $[s]^p$ берутся лишь первые r символов, это будет записано как $[s]^p|_r$.

Теорема 1. *Пусть $n\in N$, $2\le k\le\frac{n-2}{2}$, $t\in\{1,2,\dots,2^{2^k}\}$. Тогда для всех достаточно больших n: 1) при $t\ge 2$ имеет место неравенство $L_{k,t,\Phi_t}(n)\ge(l(\Phi_t)-1)\cdot(n-k+1)$, а если, кроме того, ни в какой тест минимальной длины для таблицы $M(\Phi_t)$ не входит набор $\tilde 0^k$ (или набор $\tilde 1^k$), то $L_{k,t,\Phi_t}(n)\ge l(\Phi_t)\cdot(n-k+1)$; 2) при $t=1$ имеет место неравенство $n-k\le L_{k,t,\Phi_t}(n)\le n-k+1$.*

Доказательство. Рассмотрим функцию $h(\tilde x^n)$, обращающуюся в нуль в точности на следующем множестве наборов

$$N_{\bar h}=\Big\{\beta_1=\Big([0^k1]^{\lceil\frac{n}{k+1}\rceil}\Big|_n\Big),\ \beta_2=\Big(1\,[0^k1]^{\lceil\frac{n-1}{k+1}\rceil}\Big|_{n-1}\Big),$$

$$\beta_3=\Big(01\,[0^k1]^{\lceil\frac{n-2}{k+1}\rceil}\Big|_{n-2}\Big),\ \beta_4=\Big(001\,[0^k1]^{\lceil\frac{n-3}{k+1}\rceil}\Big|_{n-3}\Big),\dots,$$

$$\beta_k=\Big(0^{k-2}1\,[0^k1]^{\lceil\frac{n-k+1}{k+1}\rceil}\Big|_{n-k+1}\Big),\ \beta_{k+1}=\Big(0^{k-1}1\,[0^k1]^{\lceil\frac{n-k}{k+1}\rceil}\Big|_{n-k}\Big)\Big\}.$$

Пусть $\alpha=(\alpha_1,\dots,\alpha_k)$ — произвольный набор, отличный от $\tilde 0^k$, а $\beta=(\beta_1,\dots,\beta_k)$ — произвольный набор, отличный от $\tilde 1^k$. Тогда таблица неисправностей, построенная при действии на $h(\tilde x^n)$ произвольных локальных слипаний кратности k, порожденных системой $\Phi_t(\tilde y^k)$, устроена следующим образом: $(h^i_j=h(x_1,\dots,x_{j-1},\underbrace{\varphi_i(x_j,x_{j+1},\dots,x_{j+k-1}),\dots,\varphi_i(x_j,x_{j+1},\dots,x_{j+k-1})}_{k\text{ раз}},x_{j+k},\dots,x_n)$, где $1\le j\le n-k+1$, $i\in\{1,\dots,t\}$, $\gamma_i=\varphi_i(\tilde 0^k)$, $\eta_i=\varphi_i(\alpha)$; в таблице указаны значения переменных $x_1,x_2,\dots,x_k,x_{k+1},x_{k+2},x_{k+3},\dots,x_{2k+1}$,

$x_{2k+2},x_{2k+3},\dots$):

$\tilde x^n$	h	h^i_1	h^i_2	h^i_3	…	h^i_{k+1}	h^i_{k+2}	h^i_{k+3}	…
00…0100…010…	0	γ_i	1	1	…	1	γ_i	1	…
10…0010…001…	0	1	γ_i	1	…	1	1	γ_i	…
01…0001…000…	0	1	1	γ_i	…	1	1	1	…
…	…	…	…	…	…	…	…	…	…
00…1000…100…	0	1	1	1	…	γ_i	1	1	…
$\alpha_1\alpha_2\dots\alpha_k$100…010…	1	η_i	1	1	…	1	1	1	…
$1\alpha_1\dots\alpha_{k-1}\alpha_k$10…001…	1	1	η_i	1	…	1	1	1	…
$01\dots\alpha_{k-2}\alpha_{k-1}\alpha_k$1…000…	1	1	1	η_i	…	1	1	1	…
…	…	…	…	…	…	…	…	…	…
00…1$\alpha_1\alpha_2\alpha_3$…100…	1	1	1	1	…	η_i	1	1	…
00…01$\alpha_1\alpha_2\dots\alpha_k$10…	1	1	1	1	…	1	η_i	1	…
10…001$\alpha_1\dots\alpha_{k-1}\alpha_k$1…	1	1	1	1	…	1	1	η_i	…
…	…	…	…	…	…	…	…	…	…

(из наборов других типов подстановками нулей на k подряд идущих разрядов нельзя получить набор из $N_{\bar h}$, и все функции h, h^i_j на таких наборах равны 1).

Если через R_d обозначить матрицу $(k+1)\times t$, d-я строка которой имеет вид $\gamma_1\gamma_2\dots\gamma_t$, а остальные строки состоят из единиц, через $\hat M$ — матрицу $(2^k-1)\times t$, полученную из $M(\Phi_t)$ удалением первой строки $\gamma_1\gamma_2\dots\gamma_t$, а через $J_{p,t}$ — матрицу $p\times t$, все строки состоят из единиц, то при выбрасывании из матрицы $D(h(\tilde x^n),\Phi_t(\tilde y^k))$ столбцов значений функций системы $\Psi_{n,k,t,h,\Phi_t}(\tilde x^n)\setminus\{h\}$ всех строк, порожденных наборами, из которых под действием локальных слипаний нельзя получить наборы из $N_{\bar h}$, и перестановке строк и столбцов, матрица $D(h(\tilde x^n),\Phi_t(\tilde y^k))$ приведется к виду

$$\underbrace{\begin{pmatrix} R_{(1)'} & R_{(2)'} & \dots & R_{(k+1)'} & R_{(k+2)'} & R_{(k+3)'} & \dots & R_{(n-k+1)'}\\ \hat M & J_{2^k-1,t} & \dots & J_{2^k-1,t} & J_{2^k-1,t} & J_{2^k-1,t} & \dots & J_{2^k-1,t}\\ J_{2^k-1,t} & \hat M & \dots & J_{2^k-1,t} & J_{2^k-1,t} & J_{2^k-1,t} & \dots & J_{2^k-1,t}\\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots\\ J_{2^k-1,t} & J_{2^k-1,t} & \dots & \hat M & J_{2^k-1,t} & J_{2^k-1,t} & \dots & J_{2^k-1,t}\\ J_{2^k-1,t} & J_{2^k-1,t} & \dots & J_{2^k-1,t} & \hat M & J_{2^k-1,t} & \dots & J_{2^k-1,t}\\ J_{2^k-1,t} & J_{2^k-1,t} & \dots & J_{2^k-1,t} & J_{2^k-1,t} & \hat M & \dots & J_{2^k-1,t}\\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots\\ J_{2^k-1,t} & J_{2^k-1,t} & \dots & J_{2^k-1,t} & J_{2^k-1,t} & J_{2^k-1,t} & \dots & \hat M \end{pmatrix}}_{n-k+1}$$

(здесь и далее $(p)'$ означает число из множества $\{1,2,\dots,k+1\}$, сравнимое с p по модулю $k+1$). В последней матрице порядок столбцов такой: h^1_1, $h^2_1,\dots,h^t_1$, h^1_2, $h^2_2,\dots,h^t_2,\dots,h^1_{n-k+1}$, $h^2_{n-k+1},\dots,h^t_{n-k+1}$,

а порядок строк такой: строки $k+1$ наборов из $N_{\bar{h}}$ (далее все строки наборов не из $N_{\bar{h}}$), затем в лексикографическом порядке строки 2^k-1 наборов, из которых можно подстановками нулей на k подряд идущих разрядов, начиная с 1-го, получить набор $\beta_{(1)'}$, затем в лексикографическом порядке строки 2^k-1 наборов, из которых можно подстановками нулей на k подряд идущих разрядов, начиная со 2-го, получить набор $\beta_{(2)'}$, и т. д., затем в лексикографическом порядке строки 2^k-1 наборов, из которых можно подстановками нулей на k подряд идущих разрядов, начиная с $(n-k+1)$-го, получить набор $\beta_{(n-k+1)'}$. Ясно, что в условиях теоремы все эти наборы попарно различны.

Теперь утверждение первой части теоремы с очевидностью следует из того, что для различения слипаний, действующих на переменные начиная с x_{j_1}, требуется по крайней мере $l(M(\Phi_t))$ наборов, среди которых лишь один может быть из $N_{\bar{h}}$, и лишь он может участвовать в различении слипаний, действующих на переменные начиная с x_{j_2} $(j_2 \neq j_1)$, — следует учесть лишь то, что $L_{k,t,\Phi_t}(h(\tilde{x}^n)) \leq L_{k,t,\Phi_t}(n)$.

Для доказательства второй части теоремы рассмотрим сначала случай $\varphi_1 \not\equiv 1$ (в $M(\Phi_t)$ есть строка, единственный элемент которой есть нуль). Тогда q $(q \in N_0)$ входящих в минимальный тест для h наборов из $N_{\bar{h}}$ разбивают $\Psi_{n,k,t,h,\Phi_t}(\tilde{x}^n)\setminus\{h\}$ на $q+1$ классов эквивалентности $Q_1, Q_2, \ldots, Q_{q+1}$, для полного различения которых в этот тест должно войти наборов не менее $q+\sum\limits_{u=1}^{q+1}(|Q_u|-1) = n-k$. Значит, $n-k \leq L_{k,t,\Phi_t}(h(\tilde{x}^n)) \leq L_{k,t,\Phi_t}(n)$. Верхняя оценка функции Шеннона тривиальна. Для случая $\varphi_1 \equiv 1$ следует применить двойственные рассуждения. Теорема доказана.

Теорема 2. *Пусть $n \in N$, $n \to \infty$, $2 \leq k \leq \frac{n-2}{2}$, $t \in \{2, \ldots, 2^{2^k}\}$, $t \to \infty$. Тогда можно для каждого натурального t указать Φ_t, для которого $L_{k,t,\Phi_t}(n) \sim t(n-k)$.*

Доказательство. Верхняя оценка функции Шеннона тривиальна и связана с числом столбцов таблицы неисправностей. Утверждение теоремы вытекает из части 1б теоремы 1, если в качестве системы Φ_t взять систему, матрица которой $M(\Phi_t)$ имеет вид $(E_t = \mathrm{diag}(\underbrace{1,1,\ldots,1}_{t}))$: $M(\Phi_t) = \begin{pmatrix} \tilde{0}^t \\ E_t \\ J_{2^k-k-1,t} \end{pmatrix}$.

Теорема 3. *Пусть $n \in N$, $2 \leq k \leq \frac{n-2}{2}$, $t = 2$, $\Phi_t(\tilde{y}^k) = \{0(\tilde{y}^k), 1(\tilde{y}^k)\}$. Тогда $2(n-k+1)-1 \leq L_{k,t,\Phi_t}(n) \leq 2(n-k+1)$.*

Доказательство. Верхняя оценка функции Шеннона тривиальна. Нижняя получается в полной аналогии с доказательством части 2) теоремы 1, если вместо h использовать функцию $g(\tilde{x}^n)$, обращающуюся в нуль в точности на следующем множестве наборов $N_{\bar{g}} = \Big\{\xi_1 = \Big([0^k1^k]^{\lceil\frac{n}{2k}\rceil}\Big|_n\Big)$, $\xi_2 = \Big(1\,[0^k1^k]^{\lceil\frac{n-1}{2k}\rceil}\Big|_{n-1}\Big)$, $\xi_3 = \Big(11\,[0^k1^k]^{\lceil\frac{n-2}{2k}\rceil}\Big|_{n-2}\Big)$, $\xi_4 = \Big(111\,[0^k1^k]^{\lceil\frac{n-3}{2k}\rceil}\Big|_{n-3}\Big), \ldots,$ $\xi_k = \Big(1^{k-1}\,[0^k1^k]^{\lceil\frac{n-k+1}{2k}\rceil}\Big|_{n-k+1}\Big)$, $\xi_{k+1} = \Big(1^k\,[0^k1^k]^{\lceil\frac{n-k}{2k}\rceil}\Big|_{n-k}\Big)$, $\xi_{k+2} = \Big(01^k\,[0^k1^k]^{\lceil\frac{n-k-1}{2k}\rceil}\Big|_{n-k-1}\Big)$, $\xi_{k+3} = \Big(001^k\,[0^k1^k]^{\lceil\frac{n-k-2}{2k}\rceil}\Big|_{n-k-2}\Big), \ldots,$ $\xi_{2k-1} = \Big(0^{k-2}1^k\,[0^k1^k]^{\lceil\frac{n-2k+2}{2k}\rceil}\Big|_{n-2k+2}\Big)$, $\xi_{2k} = \Big(0^{k-1}1^k\,[0^k1^k]^{\lceil\frac{n-2k+1}{2k}\rceil}\Big|_{n-2k+1}\Big)\Big\}$.

Нетрудно видеть, что нулевые значения могут приниматься одной из функций из $\Psi_{n,k,t,g,\Phi_t}(\tilde{x}^n)$ лишь на наборах из $N_{\bar{g}}$, а также на наборах, из которых можно получить набор из $N_{\bar{g}}$ подстановкой одинаковых констант на k последовательных разрядов. На остальных наборах все функции из $\Psi_{n,k,t,g,\Phi_t}(\tilde{x}^n)$ обращаются в единицу, и эти наборы далее рассматриваться не будут. Далее, рассмотрим любые два различных набора $\chi_1, \chi_2 \notin N_{\bar{g}}$, из которых можно получить один и тот же набор из $N_{\bar{g}}$ подстановкой одинаковых констант на k последовательных разрядов, начиная с j_0-го ($j_0 \in \{1, \ldots, n-k+1\}$). Ясно, что $g(\chi_1) = g(\chi_2) = 1$, $g^i_j(\chi_1) = g^i_j(\chi_2) = 1$ ($j \in \{1, \ldots, n-k+1\}$, $i \in \{1,2\}$). Поэтому из всего множества наборов, из которых можно получить один и тот же набор из $N_{\bar{g}}$ подстановкой одинаковых констант на k последовательных разрядов, начиная с j_0-го, достаточно рассмотреть в таблице неисправностей лишь один набор.

Опишем теперь структуру таблицы неисправностей функции g при действии на входные переменные константных локальных слипаний кратности k. Транспонирование будем обозначать верхним индексом T. Через $\bar{E}_p$ обозначим квадратную матрицу порядка p, у которой на главной диагонали нули, а остальные элементы — единицы. Через $\bar{e}^u_p$ обозначим столбец из p элементов, у которого u-й элемент есть нуль, а остальные элементы — единицы. Через $\hat{\bar{E}}_{2k}$ обозначим квадратную матрицу порядка $2k$ следующего вида: $\hat{\bar{E}}_{2k} = (\bar{e}^1_{2k}\bar{e}^{k+1}_{2k}\bar{e}^2_{2k}\bar{e}^{k+2}_{2k}\ldots\bar{e}^k_{2k}\bar{e}^{2k}_{2k})$. Тогда функциональ-

ная часть упомянутой таблицы неисправностей будет иметь вид:

$$\left(\begin{array}{c|c} (\tilde{0}^{2k})^{\mathrm{T}} & \hat{\hat{E}}_{2k}\hat{\hat{E}}_{2k}\ldots\hat{\hat{E}}_{2k}\hat{\hat{E}}'_{2k} \\ \hline (\tilde{1}^{2(n-k+1)})^{\mathrm{T}} & \tilde{E}_{2(n-k+1)} \end{array}\right)$$

(в матрице $\hat{\hat{E}}'_{2k}$ по сравнению с $\hat{\hat{E}}_{2k}$ может отсутствовать часть последних столбцов). Порядок столбцов и строк здесь схож с порядком в аналогичной таблице из теоремы 1. Дальнейшее доказательство аналогично финальным рассуждениям второй части теоремы 1.

Работа выполнена при поддержке грантов РФФИ № 06-01-00745 и № 04-01-00359.

Список литературы

1. Погосян Г. Р. О проверяющих тестах для логических схем. — М.: ВЦ АН СССР, 1982.

2. Носков В. Н. О длинах минимальных единичных диагностических тестов, контролирующих работу входов логических схем // Методы дискретного анализа в синтезе управляющих систем. — Новосибирск: ИМ СО АН СССР, 1978. — № 32. — С. 40–51.

АЛГЕБРА ОБЪЕКТНЫХ ОПЕРАЦИЙ СИСТЕМЫ УПРАВЛЕНИЯ ДАННЫМИ DIM

В. С. Рублев, Д. В. Чехранов (Ярославль)

Рассматривается проблема построения СУБД, которая имеет гибкий и удобный механизм, учитывающий динамику свойств предметной области. Традиционные объектные технологии построения систем управления данными (объектно-реляционная и объектно-ориентированная) практически непригодны для описания динамических систем, в которых тип данных может меняться. В [1, 2] предложена новая модель данных — динамическая информационная модель DIM, основанная на реляционной технологии, которая позволяет структурировать данные и методы их обработки (является объектной), динамически изменять тип и методы обработки данных, сохраняя при этом их «историю», включает в себя механизм наследования в цепочке изменения типов.

Для манипулирования данными определение типа объекта DIM [1, 2] приводит к очень сложным конструкциям SQL-запросов, и потому необходим язык объектных операций, который бы позволил снять эту сложность. Введению объектных операций и рассмотрению свойств алгебры этих операций (*объектной алгебры*) и посвящена данная работа.

Пусть $\mathbb{C}$ — множество всех классов объектной модели DIM, $\mathbb{O}$ — множество всех объектов этой модели, $\mathbb{S}$ — множество свойств всех ее объектов.

Строчными буквами мы будем обозначать объекты или классы (например, o — объект, c — класс), а прописными буквами — множества объектов или классов (например, O — множество объектов, C — множество классов). Ввиду того, что класс является как прототипом нового объекта, так и множеством всех своих объектов, то $\forall o \in \mathbb{O}\ \forall c \in \mathbb{C}$ либо $o \in c$, либо $o \notin c$.

1. *Операции для множеств классов и объектов*: *c(o)* — класс объекта o; *C(O)* — множество классов объектов множества O: $C(O) = \cup_{o\in O} c(o)$; $|O|$, $|C|$ — число элементов во множестве. Для множества объектов одного класса $|C(O)| = 1$.

2. *Операции алгебры множеств.* Операции объединения и пересечения множеств для объектов и для классов вводятся обычным образом: $O_1 \cup O_2 = \{o \in \mathbb{O} \mid o \in O_1 \vee o \in O_2\}$, $O_1 \cap O_2 = \{o \in \mathbb{O} \mid o \in O_1 \wedge o \in O_2\}$.

Для множеств классов указанные операции аналогичны.

Также вводятся 2 варианта операции дополнения:

Если множество объектов O состоит из объектов одного класса ($|C(O)| = 1$), то *простым* дополнением назовем множество объектов $\widetilde{O} = \{o \in c \mid o \notin O\}$, т. е. это объекты класса c, не принадлежащие множеству O. Для пустого множества положим $\widetilde{\emptyset} \equiv \mathbb{O}$. Для классов эта операция не имеет смысла.

Общим дополнением для множества объектов O назовем множество $\overline{O} = \{o \in \mathbb{O} \mid o \notin O\}$, т. е. это множество ВСЕХ объектов, не принадлежащих O.

Для классов эта операция аналогична: $\overline{C} = \{c \in \mathbb{C} \mid c \notin C\}$.

Дополнения обладают следующими свойствами.

Пусть $c \in \mathbb{C}$, $O_1 \subseteq \mathbb{O}(c)$, $O_2 \subseteq \mathbb{O}(c)$. Тогда выполнены законы де Моргана:

$\widetilde{\widetilde{O_1}} = O_1$, $\widetilde{O_1 \cup O_2} = \widetilde{O_1} \cap \widetilde{O_2}$, $\widetilde{O_1 \cap O_2} = \widetilde{O_1} \cup \widetilde{O_2}$, $\overline{\overline{O_1} \cup \overline{O_2}} = O_1 \cup O_2$, $\overline{\overline{O_1} \cap \overline{O_2}} = O_1 \cap O_2$.

В общем случае, когда множества содержат объекты разных классов ($O_1 \subseteq c_1$, $O_2 \subseteq c_2$, $c_1 \neq c_2$), то свойства простого дополнения изменяются:

$\widetilde{O_1 \cup O_2} = \widetilde{O_1} \cup \widetilde{O_2}$, $\widetilde{O_1 \cap O_2} = \mathbb{O}$, $\widetilde{\widetilde{O_1 \cup O_2}} = O_1 \cup O_2$, $\widetilde{\widetilde{O_1 \cap O_2}} = O_1 \cap O_2 = \emptyset$.

Свойства общего дополнения:

$\overline{O_1 \cup O_2} = \overline{O_1} \cap \overline{O_2}$, $\overline{O_1 \cap O_2} = \overline{O_1} \cup \overline{O_2}$.

3. *Выбор*: $\Sigma_\Theta(O)$ — подмножество объектов множества O, удовлетворяющих ограничению Θ. Здесь Θ — ДНФ ограничений на свойства (конъюнкция обозначается ","). Каждое ограничение записывается в виде <свойство> <операция сравнения> <значения>. Здесь <свойство> — это тройка (s, t, l), где $s \in \mathbb{S}$ — имя свойства, t — его тип, l — ограничения на тип свойства, <операция сравнения> — это одна из операций сравнения (=, <>, >, <, >=, <=), а <значения> — это либо значение свойства, либо список значений (через знак "|"), либо диапазон значений (через ".."), либо их совокупность. Отдельно отметим ограничение "c =<список классов>" или "c <> <список классов>". Это ограничение на класс объектов множества O. Формат записи тот же, но в качестве значений используются имена классов.

Таким образом, $\Sigma_{c=c_0}(O)$ — подмножество объектов O, принадлежащие классу c_0. Если $C = \{c_1, \ldots, c_n\}$, то $\Sigma_{c=c_1|c_2 \ldots |c_n}(O) = \Sigma_{c \in C}(O)$ — подмножество объектов O, где класс каждого объекта принадлежит множеству C: $\Sigma_{c=c_1|c_2 \ldots |c_n}(O) = \cup_{c_i \in C}\ \Sigma_{c=c_i}(O)$. Пример: $\Sigma_{c=c_1|c_2, Model='YA1'}(O)$.

4. *Набор значений свойств*: $S(c)$ — множество свойств класса c; $S(o) = S(c(o))$ — множество свойств объекта o; Результат операции S — это множество троек вида "(<имя свойства>, <тип свойства>, <список значений>)"

Для получения значений свойств используется проекция: $\Pi_A(o)$ — множество пар вида (<имя свойства>, <значение>), $A \subseteq S$ (возвращает кортеж значений свойств из множества A в объекте o); $\Pi_A(O)$ — множество пар вида (<имя свойства>, <значение>), $A \subseteq S$ (возвращает кортежи значений свойств из множества A объектов множества O).

Аналогично вводятся операции для классов (поскольку класс — это множество объектов).

5. *Наследование.* Для любого объекта $o \in \mathbb{O}$: $P(o)$ — множество объектов, являющихся родителями объекта o; $\widehat{P}(o)$ — множество объектов, являющихся наследниками объекта o.

Для любого множества объектов $O \subseteq \mathbb{O}$: $P(O)$ — множество родителей объектов множества O: $P(O) = \bigcup_{o \in O} P(o)$; $\widehat{P}(O)$ — множество наследников объектов множества O: $\widehat{P}(O) = \bigcup_{o \in O} \widehat{P}(o)$.

Операции для классов вводятся аналогично.

6. *Включение.* Для любого объекта $o \in \mathbb{O}$: $I(o)$ — множество объектов, в которые включен объект o (в том числе и по наследованию); $\widehat{I}(o)$ — множество объектов, которые включены в объект o (в том числе и по наследованию).

Для любого множества объектов $O \subseteq \mathbb{O}$: $I(O)$ — множество объектов, в каждый из которых включен объект множества O: $I(O) = \bigcup_{o \in O} I(o)$; $\widehat{I}(O)$ — множество объектов, каждый из которых включен в объект множества O: $\widehat{I}(O) = \bigcup_{o \in O} I(o)$.

Операции для классов вводятся аналогично.

7. *Отношение функционального включения*: $H(c)$ — множество классов связей для класса c (рассматриваются также и классы, включенные в родителей); $H(o, o_j)$ — множество объектов связей при включении объекта $o_j \in I(o)$ в объект $o \in \mathbb{O}$.

8. *История*: $T(O)$ — множество объектов-последователей для каждого из объектов множества O; $\widehat{T}(O)$ — множество объектов-предшественников для каждого из объектов множества O.

9. *Результат работы.* Введенная совокупность операций (исключая операции получения свойств и их значений):

а) является замкнутой, т. е. применение любой последовательности операций над множеством объектов дает множество объектов;

б) позволяет определять ограничения целостности (ограничения выбора, определенности, однозначности). Например, ограничение выбора в приведенных операциях выражается так:

$\forall o \in \mathbb{O}$, $\forall o_j \in \widehat{I}(o)$, $\forall c_0 \in C(H(o, o_j))$: $|\Sigma_{c=c_0}(H(o, o_j))| \leq 1$;

в) за счет алгебраических преобразований позволяет проводить оптимизацию выделения множества объектов.

Список литературы

1. Рублев В. С., Юсупов А. Р. Концепции объектной динамической информационной модели. — Депонирована в ВИНИТИ РАН 30.05.05 771-В 2005. — Ярославль: ЯрГУ, 2005. — 38 с.

2. Рублев В. С., Юсупов А. Р. Концепции объектной динамической информационной модели DIM // Математика в Ярославском университете: Сб. обзорных статей. К 30-летию математического факультета. — Ярославль: ЯрГУ, 2006. — С. 355–394.

О РЕАЛИЗАЦИИ НЕКОТОРЫХ ОПЕРАЦИЙ КОНЕЧНЫХ ПОЛЕЙ ХАРАКТЕРИСТИКИ 2 СХЕМАМИ ЛОГАРИФМИЧЕСКОЙ ГЛУБИНЫ

И. С. Сергеев (Москва)

В настоящей работе рассматривается реализация некоторых операций в конечном поле $GF(2^n)$ схемами в базисе всех двуместных булевых функций с глубиной $O(\log n)$ (глубина обсуждаемых далее схем не будет специально оговариваться). Введение в алгоритмическую теорию конечных полей содержится в [1], а понятия сложности и глубины схем изложены в [2].

При реализации арифметики в конечных полях наиболее употребительной является интерпретация конечного поля как векторного пространства (в частности, поле $GF(2^n)$ является двоичным векторным пространством размерности n с операцией умножения векторов).

Реализация операций в конечном поле зависит от выбора базиса. При этом очевидно, что сложение в любом базисе поля $GF(2^n)$ выполняется со сложностью n и глубиной 1. Чаще всего используется *стандартный* (или полиномиальный) базис $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, генератором которого является элемент α — корень некоторого неприводимого многочлена $m(x)$ степени n над $GF(2)$. Элементы поля в указанном базисе представляются многочленами степени не выше $n-1$, операции над которыми производятся по модулю многочлена $m(x)$.

В последнее время активно применяются *нормальные* базисы, имеющие вид $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$. Генератор нормального базиса α также должен быть корнем некоторого неприводимого многочлена степени n, т.е. генератором некоторого стандартного базиса. Обратное неверно, т.е. не для каждого стандартного базиса существует нормальный с тем же генератором. Однако известно, что нормальные базисы существуют во всех полях. Интерес к нормальным базисам объясняется тем, что операция Фробениуса (возведение в степень вида 2^k) осуществляется в них циклическим сдвигом координат, т.е. с нулевой схемной сложностью.

Известно [3], что умножение в стандартном базисе поля $GF(2^n)$ выполняется схемой сложности $O(n \log n \log\log n)$. Также известно, что операцию Фробениуса в стандартном базисе можно реализовать со сложностью $O(n^{1.67})$ (см. [1]). (В приводимых здесь и далее оценках используются экспоненты матричных умножений, которые взяты из [4].) Вместо операции деления можно рассматривать операцию инвертирования, т.к. деление сводится к умножению и инвертированию. Из работ [5, 6] следует, что инвертирование может быть реализовано схемой полиномиальной сложности.

Используя метод А. Брауэра (см. [1]), можно построить схему инвертирования сложности $O(n^{1.67})$, однако глубины $O(\log^2 n)$. На самом деле, оценку сложности $O(n^{1.67})$ можно получить и для схемы логарифмической глубины.

Разработанные специально для нормальных базисов методы умножения и инвертирования имеют достаточно высокую сложность (по крайней мере, $O(n^2)$) и порядок глубины не менее $O(\log^2 n)$. Для ускорения реализации операций в указанных базисах (как по сложности, так и по глубине) можно использовать идею перехода к стандартному базису (см. [1]). Под переходом понимается соответствующее преобразование координат элемента поля.

Для перехода между нормальным и стандартным базисами можно построить схему сложности $O(n^{1.81})$ (этот результат частично получен в [7]), что приводит к аналогичной оценке сложности умножения и инвертирования в нормальных базисах.

Эта же идея может применяться и для ускорения некоторых операций в стандартных базисах. В качестве примера приведем иногда встречающуюся в приложениях задачу проверки базисности нормальной системы: задан элемент $\beta \in GF(2^n)$ — требуется проверить, порождает ли он нормальный базис. В нормальном базисе для решения этой задачи можно построить схему сложности $O(n^{1.67})$, откуда следует оценка $O(n^{1.81})$ для реализации в стандартном базисе.

В прилагаемой таблице содержатся сведения о сложности реализации обсуждавшихся операций схемами логарифмической глубины (выделены результаты, которые, по-видимому, являются новыми).

Операция	СБ	НБ
Умножение	$n \log n \log\log n$	$n^{\mathbf{1.81}}$
Операция Фробениуса	$n^{1.67}$	0
Инвертирование	$n^{\mathbf{1.67}}$	$n^{\mathbf{1.81}}$
Переход к НБ	$n^{\mathbf{1.81}}$	$n \log n \log\log n$
Переход к СБ	$n^{1.67}$	$n^{1.81}$
Тест генератора НБ	$n^{\mathbf{1.81}}$	$n^{1.67}$

Автор признателен научному руководителю С. Б. Гашкову за постановку задачи и внимание к работе.

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

Список литературы

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

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

3. Schönhage A. Schnelle multiplikation von polynomen über körpern der charakteristik 2 // Acta Inf. — 1977. — V. 7. — P. 395–398.

4. Huang X., Pan V. Fast rectangular matrix multiplication and applications // J. Complexity. — 1998. — V. 14. — P. 257–299.

5. Litow B., Davida G. $O(\log n)$ parallel time finite field inversion // Lecture Notes in Computer Science (Proc. Aegean Workshop on Computing). — Berlin, 1988. — V. 319. — P. 74–80.

6. von zur Gathen J. Inversion in finite fields using logarithmic depth // J. Symb. Comput. — 1990. — V. 9. — P. 175–183.

7. Kaltofen E., Shoup V. Subquadratic-time factoring of polynomials over finite fields // Math. Comput. — 1998. — V. 67, № 223. — P. 1179–1197.

О ПОДОБИИ МАТРИЦ ТРЕТЬЕГО ПОРЯДКА НАД КОЛЬЦОМ ЦЕЛЫХ ЧИСЕЛ

С. В. Сидоров (Нижний Новгород)

Квадратные матрицы A и B с коэффициентами из поля $\mathbf{F}$ называются подобными над $\mathbf{F}$, если существует невырожденная матрица S с коэффициентами из $\mathbf{F}$ такая, что $AS = SB$. Задача о подобии матриц над полем $\mathbf{F}$ является классической задачей линейной алгебры (см., например, [1]). В работе рассматривается задача подобия 3×3 матриц над кольцом целых чисел. Случай матриц второго порядка рассматривался в [2].

Определение. Будем говорить, что матрица $B\in\mathbf{Z}^{n\times n}$ *подобна* матрице $A\in\mathbf{Z}^{n\times n}$ над кольцом $\mathbf{Z}$, если существует $S\in\mathbf{Z}^{n\times n}$ такая, что $AS = SB$ и $\det S \in \{1,-1\}$ и обозначать это $A\sim B$. Матрица S называется *трансформирующей* B в A матрицей.

Подобие матриц A и B над полем $\mathbf{Q}$ будем обозначать $A \approx B$. Очевидно, что из подобия над $\mathbf{Z}$ следует подобие над $\mathbf{Q}$. Обратное неверно (см. пример в [2]). Если матрицы подобны (над $\mathbf{Z}$ или над $\mathbf{Q}$), то у них совпадают характеристические многочлены. Далее будем считать, что $n = 3$. Пусть матрица $A\in\mathbf{Z}^{3\times3}$ имеет приводимый над $\mathbf{Z}$ характеристический многочлен $d(\lambda)$. Возможны следующие варианты: 1) все корни $d(\lambda)$ лежат в $\mathbf{Z}$; 2) $d(\lambda) = (\lambda-\alpha)(\lambda^2+u\lambda+v)$, причем $\lambda^2+u\lambda+v$ неприводим над $\mathbf{Z}$.

В первом случае A подобна над $\mathbf{Q}$ одной из жордановых матриц:
a) если $d(\lambda) = (\lambda-\alpha)^3$, то A подобна над $\mathbf{Q}$ одной из матриц $J_1(\alpha) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$, $J_2(\alpha) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & \alpha \end{pmatrix}$, $J_3(\alpha) = \begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & \alpha \end{pmatrix}$. Пусть $K(J_i(\alpha)) = \{A \in \mathbf{Z}^{3\times3} | A \approx J_i(\alpha)\}$, $i = 1,2,3$.
b) если $d(\lambda) = (\lambda-\alpha)(\lambda-\beta)^2$, то A подобна над $\mathbf{Q}$ либо $J_1(\alpha,\beta) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \beta \end{pmatrix}$, либо $J_2(\alpha,\beta) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 1 \\ 0 & 0 & \beta \end{pmatrix}$. Пусть $K(J_i(\alpha,\beta)) = \{A \in \mathbf{Z}^{3\times3} | A \approx J_i(\alpha,\beta)\}$, $i = 1,2$.
c) если $d(\lambda) = (\lambda-\alpha)(\lambda-\beta)(\lambda-\gamma)$, то A подобна над $\mathbf{Q}$ матрице $J(\alpha,\beta,\gamma) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$. Пусть $K(J(\alpha,\beta,\gamma)) = \{A \in \mathbf{Z}^{3\times3} | A \approx J(\alpha,\beta,\gamma)\}$.

Во втором случае A подобна над $\mathbf{Q}$ матрице Фробениуса $F = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & -u & -v \\ 0 & 1 & 0 \end{pmatrix}$. Обозначим $K(F) = \{A \in \mathbf{Z}^{3\times3} | A \approx F\}$.

Каждый из вышеперечисленных классов матриц, подобных над $\mathbf{Q}$, вообще говоря, не является классом подобных над $\mathbf{Z}$ матриц. Поэтому возникает задача о классификации матриц по отношению подобия над $\mathbf{Z}$ или о разбиении каждого из этих классов на подклассы матриц, подобных над $\mathbf{Z}$. Следующие теоремы показывают такое разбиение.

Теорема 1. *Пусть* $d(\lambda) = (\lambda-\alpha)^3, \alpha \in \mathbf{Z}$. *Тогда:*
1. $K(J_1(\alpha)) = Y_\alpha = \{A \in \mathbf{Z}^{3\times3} | A \sim J_1(\alpha)\} = \{J_1(\alpha)\}$.
2. $K(J_2(\alpha)) = \bigcup Y_\alpha(d)$, $Y_\alpha(d) = \{A \in \mathbf{Z}^{3\times3} | A \sim R_\alpha(d)\}$,

$R_\alpha(d) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & d \\ 0 & 0 & \alpha \end{pmatrix}$, $d \geq 1$.

3. $K(J_3(\alpha)) = \bigcup Y_\alpha(a,b,r)$, $Y_\alpha(a,b,r) = \{A \in \mathbf{Z}^{3\times 3} | A \sim R_\alpha(a,b,r)\}$,

$R_\alpha(a,b,r) = \begin{pmatrix} \alpha & a & r \\ 0 & \alpha & b \\ 0 & 0 & \alpha \end{pmatrix}$, $a, b \geq 1$, $0 \leq r < НОД(a,b)$.

Теорема 2. *Пусть* $d(\lambda) = (\lambda-\alpha)(\lambda-\beta)^2, \alpha, \beta \in \mathbf{Z}$. *Тогда:*

1. $K(J_1(\alpha,\beta)) = \bigcup Y_{\alpha,\beta}(d)$, $Y_{\alpha,\beta}(d) = \{A \in \mathbf{Z}^{3\times 3} | A \sim R_{\alpha,\beta}(d)\}$,

$R_{\alpha,\beta}(d) = \begin{pmatrix} \alpha & d & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \beta \end{pmatrix}$, $d = 0$ *или* d — *положительный делитель* $|\beta-\alpha|$ (*не равный* $|\beta-\alpha|$).

2. $K(J_2(\alpha,\beta)) = \bigcup Y_{\alpha,\beta}(a_1,a_2,a_3)$, $Y_{\alpha,\beta}(a_1,a_2,a_3) = \{A \in \mathbf{Z}^{3\times 3} | A \sim R_{\alpha,\beta}(a_1,a_2,a_3)\}$,

$R_{\alpha,\beta}(a_1,a_2,a_3) = \begin{pmatrix} \alpha & a_1 & a_2 \\ 0 & \beta & a_3 \\ 0 & 0 & \beta \end{pmatrix}$, *где* a_1, a_2, a_3 *удовлетворяют условиям:*

I) $a_3 \geq 1$, $0 \leq a_2 \leq \lfloor \frac{|\beta-\alpha|}{2} \rfloor$, $a_1 = 0$;

II*a*) *если* $|\beta-\alpha|$ — *нечетное, то*

$a_3 \geq 1$, $1 \leq a_1 \leq \lfloor \frac{|\beta-\alpha|}{2} \rfloor$, $0 \leq a_2 < d$, *где* $d =$*НОД*$(|\beta-\alpha|, a_1)$;

II*b*) *если* $|\beta-\alpha|$ — *четное, то:*

1) $1 \leq a_1 \leq \frac{|\beta-\alpha|}{2} - 1$, $a_3 \geq 1$, $0 \leq a_2 < d$;

2) $a_1 = \frac{|\beta-\alpha|}{2}$, $a_3 \geq 1$, $0 \leq a_2 \leq \lfloor \frac{r}{2} \rfloor$ *и* $1 + r \leq a_2 \leq \lfloor \frac{a_1+r}{2} \rfloor$, *где* r — *остаток от деления* a_3 *на* a_1.

Теорема 3. *Пусть* $d(\lambda) = (\lambda-\alpha)(\lambda-\beta)(\lambda-\gamma), \alpha, \beta, \gamma \in \mathbf{Z}, \alpha < \beta < \gamma$. *Тогда* $K(J(\alpha,\beta,\gamma)) = \bigcup Y_{\alpha,\beta,\gamma}(a_1,a_2,a_3)$,

$Y_{\alpha,\beta,\gamma}(a_1,a_2,a_3) = \{A \in \mathbf{Z}^{3\times 3} | A \sim R_{\alpha,\beta,\gamma}(a_1,a_2,a_3)\}$,

$$R_{\alpha,\beta,\gamma}(a_1,a_2,a_3) = \begin{pmatrix} \alpha & a_1 & a_2 \\ 0 & \beta & a_3 \\ 0 & 0 & \gamma \end{pmatrix},$$

где a_1, a_2, a_3 *удовлетворяют условиям:*

I) $a_1 = 0$, $0 \leq a_2 \leq \lfloor \frac{\gamma-\alpha}{2} \rfloor$, $0 \leq a_3 \leq \lfloor \frac{\gamma-\beta}{2} \rfloor$;

II*a*) *если* $\gamma-\beta$ — *нечетное, то* $1 \leq a_1 \leq \lfloor \frac{\beta-\alpha}{2} \rfloor$, $0 \leq a_2 < \gamma-\alpha$, $0 \leq a_3 \leq \lfloor \frac{\gamma-\beta}{2} \rfloor$;

II*b*) *если* $\gamma-\beta$ — *четное, то:*

1) $1 \leq a_1 \leq \lfloor \frac{\beta-\alpha}{2} \rfloor$, $0 \leq a_2 < \gamma-\alpha$, $0 \leq a_3 \leq \frac{\gamma-\beta}{2} - 1$;

2) $1 \leq a_1 \leq \lfloor \frac{\beta-\alpha}{2} \rfloor$, $0 \leq a_2 \leq \lfloor \frac{\gamma-\alpha-a_1}{2} \rfloor$, $\gamma-\alpha-a_1+1 \leq a_2 \leq \lfloor \frac{2(\gamma-\alpha)-a_1}{2} \rfloor$, $a_3 = \frac{\gamma-\beta}{2}$.

Таким образом, классы $K(J_1(\alpha)), K(J_1(\alpha,\beta)), K(J(\alpha,\beta,\gamma))$ разбиваются на *конечное* число классов подобных над $\mathbf{Z}$ матриц, а остальные — на *счетное* число.

Нам осталось рассмотреть случай, когда $d(\lambda) = (\lambda-\alpha)(\lambda^2+u\lambda+v)$ и $\lambda^2+u\lambda+v$ неприводим над $\mathbf{Z}$. Матрица, имеющая такой характеристический многочлен, подобна над $\mathbf{Z}$ блочной матрице $C = \left(\begin{array}{c|c} \alpha & a \\ \hline 0 & A' \end{array}\right)$, где $a^T \in \mathbf{Z}^2$, $A' \in \mathbf{Z}^{2\times 2}$, причем характеристический многочлен матрицы A' равен $\chi(\lambda) = \lambda^2+u\lambda+v$.

Утверждение 1. *Матрица* $A_1 = \left(\begin{array}{c|c} \alpha & a \\ \hline 0 & A' \end{array}\right)$ *подобна над* $\mathbf{Z}$ *матрице* $A_2 = \left(\begin{array}{c|c} \alpha & r \\ \hline 0 & A' \end{array}\right)$, *где* $a = (a_1, a_2)$, $r = (r_1, r_2)$, r_i — *остаток от деления* a_i *на* $|\chi(\alpha)|$, $i = 1, 2$, $\chi(\alpha) = \det(A' - \alpha E)$.

Доказательство. Положим $S = \left(\begin{array}{c|c} 1 & q \\ \hline 0 & E \end{array}\right)$, где вектор $q \in \mathbf{Z}^2$ является решением системы линейных уравнений $a - r = q(A' - \alpha E)$. Тогда $A_1 S = S A_2$, $\det S = 1$. Утверждение доказано.

Выясним, при каких условиях две матрицы вида

$$A = \left(\begin{array}{c|c} \alpha & a \\ \hline 0 & A' \end{array}\right), B = \left(\begin{array}{c|c} \alpha & b \\ \hline 0 & B' \end{array}\right), \quad (1)$$

где $0 \leq a_i < |\chi(\alpha)|$, $0 \leq b_i < |\chi(\alpha)|$, $i = 1, 2$, подобны над $\mathbf{Z}$. Если они подобны, то найдется такая унимодулярная матрица $S = \left(\begin{array}{c|c} t & u \\ \hline v & S' \end{array}\right)$, что $AS = SB$. Так как

$$AS = \left(\begin{array}{c|c} \alpha t + av & \alpha u + aS' \\ \hline A'v & A'S' \end{array}\right) = \left(\begin{array}{c|c} \alpha t & tb + uB' \\ \hline \alpha v & vb + S'B' \end{array}\right) = SB, \quad (2)$$

то $A'v = \alpha v$. Отсюда $v = 0$, ибо в противном случае α было бы собственным числом матрицы A', что невозможно, так как ее характеристический многочлен неприводим. Следовательно, $t, \det S' \in \{\pm 1\}$. Итак, $S = \left(\begin{array}{c|c} \pm 1 & u \\ \hline 0 & S' \end{array}\right)$. Из (2) также следует, что $A'S' = S'B'$, $u(B' - \alpha E) = aS' \pm b$. Приходим к следующему утверждению.

Утверждение 2. *Матрицы вида* (1) *подобны над* $\mathbf{Z}$ *тогда и только тогда, когда:* 1) A' *и* B' *подобны над* $\mathbf{Z}$; 2) *существует такая матрица* S' (*трансформирующая* B' *в* A'), *что вектор* u,

определяемый из условия $u(B' - \alpha E) = aS' \pm b$, *является целочисленным.*

Для проверки первого условия Утверждения 2 можно применить алгоритм из [2]. Выясним, как проверить второе условие. Обозначим $\Lambda_{A',B'} = \{S \in \mathbf{Z}^{2\times 2} | A'S = SB'\}$ — подмодуль в $\mathbf{Z}^{2\times 2}$. Пусть T_1 и T_2 – базис $\Lambda_{A',B'}$, тогда любую матрицу из $\Lambda_{A',B'}$ можно представить в виде $xT_1 + yT_2$ для некоторых x и y из $\mathbf{Z}$. Для подобия нужно, чтобы существовали целые x и y такие, что $f(x,y) = \det(xT_1 + yT_2) = a'x^2 + b'xy + c'y^2 = \pm 1$. Пусть $D = b'^2 - 4a'c'$ — дискриминант квадратичной формы $f(x,y)$. Возможны два случая: 1) $f(x,y)$ определенная ($D < 0$); 2) $f(x,y)$ неопределенная ($D > 0$). В первом случае уравнение $f(x,y) = \pm 1$ имеет конечное число решений, следовательно, число матриц, трансформирующих B' в A', конечно. Поэтому проверку второго условия Утверждения 2 можно осуществить перебором. Во втором же случае это уравнение либо не имеет решений, либо имеет счетное множество решений (x_n, y_n). При этом любое решение уравнения $f(x,y) = \pm 1$ можно получить, зная его минимальное решение (x_0, y_0) и (x', y') — минимальное решение уравнения Пелля $x^2 - Dy^2 = \pm 1$ (см. [3]). Обозначив через $Q = \begin{pmatrix} x' - b'y' & -2c'y' \\ 2a'y' & x' + b'y' \end{pmatrix}$, имеем $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = Q^n \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$, $n \in \mathbf{Z}$, $\det Q \in \{\pm 1\}$. Таким образом, любая матрица, трансформирующая B' в A', имеет вид

$$S_n = x_n T_1 + y_n T_2, \ n \in \mathbf{Z} \tag{3}$$

Нужно проверить, существует ли такое n, что $u = (aS_n \pm b)(B' - \alpha E)^{-1} \in \mathbf{Z}^2$. Это равносильно системе сравнений $(aS_n \pm b)(B' - \alpha E)^* \equiv 0 (mod \Delta)$, где $\Delta = |det(B' - \alpha E)|$. Заметим, что достаточно рассматривать $0 \le n \le \Delta^2 - 1$. Действительно, рассмотрим множество матриц $\{Q^n | n \in \mathbf{Z}\}$ по модулю Δ. Это циклическая группа, содержащая не более Δ^2 элементов, так как любая степень матрицы Q представима в виде $t_1 Q + t_2 E$. Взяв это представление по модулю Δ, имеем не более Δ^2 различных матриц. В итоге условие 2) Утверждения 2 можно проверить за конечное число шагов (не более Δ^2).

Теорема 4. *Матрицы вида* (1) *подобны над* $\mathbf{Z}$ *тогда и только тогда, когда:*
1) A' *и* B' *подобны над* $\mathbf{Z}$; 2) *существует матрица* S_n *вида* (3), $0 \le n \le \Delta^2 - 1$, *что вектор* u, *определяемый из условия* $u(B' - \alpha E) = aS_n \pm b$, *является целочисленным.*

Так как число классов подобия 2×2 матриц, имеющих неприводимый характеристический многочлен, конечно [2], то число классов подобия 3×3 матриц, имеющих характеристический многочлен $d(\lambda) = (\lambda - \alpha)(\lambda^2 + u\lambda + v)$, также *конечно.*

Вопрос о подобии 3×3 матриц, имеющих неприводимый характеристический многочлен, остается открытым.

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

Список литературы

1. Гантмахер Ф. Р. Теория матриц. 4-е изд. — М.: Наука, 1988.
2. Шевченко В. Н., Сидоров С. В. О подобии матриц второго порядка над кольцом целых чисел // Известия вузов. Математика. — 2006. — № 4. — С. 57–64.
3. Касселс Дж. Рациональные квадратичные формы. — М.: Мир, 1982.

О ЕДИНОЙ ФОРМАЛЬНОЙ ЗАПИСИ ВСЕХ ДОПУСТИМЫХ ХОДОВ В ЛЮБОЙ ШАХМАТНОЙ ПОЗИЦИИ

Р. В. Хелемендик (Москва)

В настоящей работе для любой легальной шахматной позиции записано множество всех допустимых правилами ходов. В этой записи использованы конечнозначные функции, формулы логики предикатов, а также операция объединения конечных множеств. Для случаев шаха, мата и пата определены соответствующие им формулы. Такая полная запись шахматных ходов существенно упрощает применение логики ветвящегося времени и игровых программ к решению шахматных задач (см. [1, 2]).

Шахматную позицию будем считать *легальной* при выполнении следующих условий: у белых и чёрных по одному королю, при ходе белых (чёрных) чёрный (белый) король не находится под шахом, каждая белая (чёрная) пешка не находится ни на первой, ни на последней горизонталях. Таким образом, всякая позиция, полученная при соблюдении шахматных правил из позиции, с которой начинается обычная шахматная партия, является легальной. Следуя определению шахматных правил (см. [3]), все возможные ходы разделим на шесть групп, соответствующих шахматным фигурам: ходы короля,

ферзя, ладьи, слона, коня и пешки. При этом рокировку будем рассматривать как разновидность хода короля, а взятие на проходе и превращение пешки (в ферзя, ладью, слона или коня) — как ход пешки. Если после выполненного по шахматным правилам (см. [3]) хода белой (чёрной) фигуры белый (чёрный) король не находится под шахом — т. е. поле, на котором он стоит не будет атаковать ни одна из чёрных (белых) фигур, — то такой ход называется *допустимым* (по правилам).

Каждую шахматную позицию будем записывать набором $\bar{y} = < y_0, y_1, \ldots, y_{68} >$. В данном наборе переменная y_0 принимает значение 0, если в позиции ход белых, и значение 1, если в позиции ход чёрных. Переменные $y_1, \ldots, y_{64}$ соответствуют полям шахматной доски, а их значения — виду фигур на этих полях. Любая такая переменная принимает значение 0 (если поле пусто), либо число от 1 до 12, соответствующее виду белой или чёрной фигуры. Переменная y_{65} (y_{66}) принимает значение 0, если своим последним ходом белые (чёрные) не ходили пешкой на два поля; в противном случае переменная y_{65} (y_{66}) есть число от 1 до 8, соответствующее номеру вертикали, по которой ходила данная пешка. Переменная y_{67} (y_{68}) принимает значение от 0 до 3, которое соответствует возможности рокировки белых (чёрных) в длинную и/или короткую стороны, либо невозможности рокировки вообще. Таким образом, значение набора $\bar{y}$ однозначно определяет ту из сторон, чья очередь ходить, а также всю информацию, необходимую для нахождения множества всех допустимых ходов этой стороны в легальной позиции. Наряду с набором $\bar{y}$ будем задавать шахматную позицию также набором $\bar{z} =< z_0, z_1, \ldots, z_{68} >$, в котором переменные имеют тот же смысл, что и в наборе $\bar{y}$. Нетрудно проверить, что если в легальной позиции, заданной набором $\bar{y}$, сделан ход β (записанный на языке шахматной нотации), то полученная после этого хода позиция задаётся набором $\bar{z}$ однозначно, что будем обозначать $g(\bar{y}, \beta) = \bar{z}$.

Пусть задана произвольная легальная позиция $\bar{y}$, в которой ход белых, т. е. $y_0 = 0$. Определим для этой позиции множество всех допустимых ходов белых. Это множество будет состоять из объединения шести конечных множеств, дающих допустимые ходы для каждой из фигур.

Определим множество $WhiteBishop(\bar{y})$, дающее все допустимые ходы слона.

$WhiteBishop(\bar{y}) = \cup_{1 \le i \le 64, y_i = 4} \cup_{1 \le l \le 4} WhiteBishopMoves(\bar{y}, i, l)$.

Множество $WhiteBishopMoves(\bar{y}, i, l)$ для поля i, на котором стоит слон и одного из направлений одной из диагоналей задаёт все ходы слона по этой диагонали следующим образом:

$WhiteBishopMoves(\bar{y}, i, l) = \cup_{k \in BI(i,l)} WhiteBishopMove(\bar{y}, i, l, k)$.

Используемое в этой формуле множество $BI(i, l)$ задаёт передвижения слона в направлении l по диагонали. Функции $x_g(i)$ и $x_v(i)$ дают соответственно горизонталь и вертикаль, на которой находится поле с номером i, где $1 \le i \le 64$.

$BI(i, l) = \{k | PBI(i, l, k)\}$,
$PBI(i, 1, k) \rightleftharpoons ((1 \le k \le 8 - x_v(i)) \wedge (x_g(i) + k \le 8))$,
$PBI(i, 2, k) \rightleftharpoons ((1 \le k \le 8 - x_v(i)) \wedge (x_g(i) - k \ge 1))$,
$PBI(i, 3, k) \rightleftharpoons ((1 \le k < x_v(i)) \wedge (x_g(i) + k \le 8))$,
$PBI(i, 4, k) \rightleftharpoons ((1 \le k < x_v(i)) \wedge (x_g(i) - k \ge 1))$.
$x_g(i) = \lfloor (i-1)/8 \rfloor + 1$, $x_v(i) = i - 8 \cdot (x_g(i) - 1)$.

Определяемое ниже множество $WhiteBishopMove(\bar{y}, i, l, k)$ состоит из не более чем одной позиции $\bar{z}$, получаемой после хода слона с поля i в направлении l на k-ю клетку, если этот ход правилами допускается. Если же такой ход невозможен, то $WhiteBishopMove(\bar{y}, i, l, k) = \emptyset$.

$WhiteBishopMove(\bar{y}, i, l, k) = \{\bar{z} | PB(i, l, k), j = fB(i, l, k), ((8 \le y_j \le 12) \vee (y_j = 0)), \forall t(((0 \le t \le 68) \wedge (t \notin \{0, i, j, 65, 68\})) \rightarrow z_t = y_t), z_i = 0, z_j = 4, z_{65} = 0, z_{68} = fKBO(j, y_{68}), z_0 = 1, SafeWKing(\bar{z})\}$.

Формула $PB(i, l, k)$ “проверяет”, чтобы в случае хода слона с поля i в направлении l на k-ю летку, где $k > 1$, каждая k'-я клетка, где $k' < k$, была бы пустой. Функция $fB(i, l, k)$ выдает поле слона после данного сделанного хода.

$PB(i, 1, k) \rightleftharpoons \forall h((1 \le h < k) \rightarrow y_{i+h+8 \cdot h} = 0)$,
$PB(i, 2, k) \rightleftharpoons \forall h((1 \le h < k) \rightarrow y_{i+h-8 \cdot h} = 0)$,
$PB(i, 3, k) \rightleftharpoons \forall h((1 \le h < k) \rightarrow y_{i-h+8 \cdot h} = 0)$,
$PB(i, 4, k) \rightleftharpoons \forall h((1 \le h < k) \rightarrow y_{i-h-8 \cdot h} = 0)$,
$fB(i, 1, k) \rightleftharpoons i + k + 8 \cdot k$, $fB(i, 2, k) \rightleftharpoons i + k - 8 \cdot k$,
$fB(i, 3, k) \rightleftharpoons i - k + 8 \cdot k$, $fB(i, 4, k) \rightleftharpoons i - k - 8 \cdot k$.

Функция $fKBO(j, y_{68})$ фиксирует потерю возможности рокировки чёрными в длинную или короткую стороны в случае занятия белой фигурой или пешкой соответствующего углового поля.

$$fKBO(j, y_{68}) \rightleftharpoons \begin{cases} j = 57, & 2 \cdot \lfloor y_{68}/2 \rfloor \\ j = 64, & y_{68} - 2 \cdot \lfloor y_{68}/2 \rfloor \\ j \notin \{57, 64\}, & y_{68} \end{cases}.$$

Формула $SafeWKing(\bar{z})$ ($SafeBKing(\bar{z})$), определяемая ниже, истинна тогда и только тогда, когда в позиции $\bar{z}$ поле, на котором стоит белый (чёрный) король, не будет находиться под атакой никакой фигуры чёрных (белых).

Ходы белой ладьи определяются аналогично ходам слона с заменой диагоналей на горизонтали и вертикали, а также добавлением возможного изменения значения переменной z_{67} (т. е. возможной потерей рокировки в одну из сторон) в случае хода белой ладьи с поля $a1$ или $h1$. Ходы ферзя определяются с использованием ходов ладьи и слона. Ходы коня определяются аналогично ходам слона с заменой диагоналей и передвижений по ним на восемь фиксированных перемещений, которые задаются табличным способом. Ходы короля являются объединением обычных ходов короля, определённых по той же схеме, что и ходы коня, и двух возможных рокировок. При определении ходов-рокировок с использованием формулы $SafeWKing(\bar{y})$ выполняется проверка шаха белому королю и прохождения короля через битое поле. Ходы пешек являются объединением следующих четырёх видов ходов: обычный ход пешки на одно поле или обычное взятие; ход пешки на два поля; ход, являющийся взятием на проходе; ход пешки на одно поле или взятие, при котором она превращается в другую фигуру. Для легальной позиции $\bar{y}$, в которой очередь хода за чёрными, ходы чёрных фигур определяются аналогично ходам белых фигур. Объединение множеств ходов всех белых (чёрных) фигур в позиции $\bar{y}$, в которой ход белых (чёрных), обозначим через $WM(\bar{y})$ ($BM(\bar{y})$).

Формулу $SafeWKing(\bar{y})$ определим следующим образом:

$SafeWKing(\bar{y}) \rightleftharpoons \exists i((1 \le i \le 64) \wedge (y_i = 1) \wedge SafeWKingN(\bar{y}, i) \wedge$
$\wedge SafeWKingP(\bar{y}, i) \wedge SafeWKingK(\bar{y}, i) \wedge$
$\wedge SafeWKingRQ(\bar{y}, i) \wedge SafeWKingBQ(\bar{y}, i))$.

В этой формуле подформула

$SafeWKingK(\bar{y}, i)$ ($SafeWKingN(\bar{y}, i)$, $SafeWKingP(\bar{y}, i)$)

проверяет, чтобы поле с номером i не атаковал чёрный король (ни один из чёрных коней, ни одна из чёрных пешек), а подформула $SafeWKingBQ(\bar{y}, i)$ ($SafeWKingRQ(\bar{y}, i)$) проверяет, чтобы поле с номером i не атаковал ни один из чёрных слонов и ни один из черных ферзей по диагонали (ни одна из чёрных ладей и ни один из черных ферзей по вертикали или горизонтали). Определим формулу $SafeWKingBQ(\bar{y}, i)$. Остальные четыре формулы определяются аналогичным образом с использованием формул и функций для ходов соответствующих фигур.

$SafeWKingBQ(\bar{y}, i) \rightleftharpoons \bigwedge_{1 \le l \le 4} SafeWKingBQMoves(\bar{y}, i, l)$,
$SafeWKingBQMoves(\bar{y}, i, l) \rightleftharpoons \bigwedge_{1 \le k \le 7} SafeWKingBQMove(\bar{y}, i, l, k)$,
$SafeWKingBQMove(\bar{y}, i, l, k) \rightleftharpoons$
$\neg(PBI(i, l, k) \wedge PB(i, l, k) \wedge ((y_{fB(i,l,k)} = 8) \vee (y_{fB(i,l,k)} = 10)))$.

Формула $SafeBKing(\bar{y})$ определяется аналогично формуле $SafeWKing(\bar{y})$.

Следующие три формулы соответствуют ситуациям, в которых белым шах, мат или пат. Аналогичные формулы для чёрных определяются тем же способом.

$WCheck(\bar{y}) \rightleftharpoons ((y_i = 0) \wedge \neg SafeWKing(\bar{y}))$,

$WCheckMate(\bar{y}) \rightleftharpoons (WCheck(\bar{y}) \wedge (WM(\bar{y}) = \emptyset))$,

$WStaleMate(\bar{y}) \rightleftharpoons ((y_i = 0) \wedge SafeWKing(\bar{y}) \wedge (WM(\bar{y}) = \emptyset))$.

Теорема 1 (о корректности). *Если в легальной позиции $\bar{y}$ $y_0 = 0$ и $\bar{z} \in WM(\bar{y})$, то в этой позиции существует такой допустимый ход белых β, что $g(\bar{y}, \beta) = \bar{z}$.*

Теорема 2 (о полноте). *Если в легальной позиции $\bar{y}$ очередь хода за белыми, ход белых β является допустимым и $g(\bar{y}, \beta) = \bar{z}$, то $\bar{z} \in WM(\bar{y})$.*

Теорема 3. *В легальной позиции $\bar{y}$ формула $WCheck(\bar{y})$ ($WCheckMate(\bar{y})$, $WStaleMate(\bar{y})$) истинна тогда и только тогда, когда в этой позиции белым шах (мат, пат).*

Аналогичные теоремы имеют место и для чёрных.

Работа выполнена при финансовой поддержке программы фундаментальных исследований Отделения математических наук РАН “Алгебраические и комбинаторные методы математической кибернетики” (проект “Оптимальный синтез управляющих систем”).

Список литературы

1. Хелемендик Р. В. О методе решения шахматных задач с помощью формул логики ветвящегося времени // Алгебра, логика и кибернетика. Материалы Международной конференции. — Иркутск: изд-во ГОУ ВПО ”ИГПУ”, 2004. — С. 215–216.

2. Хелемендик Р. В. Об одном алгоритме решения задачи синтеза игровых программ // Дискретные модели в теории управляющих систем. Труды VI Международной конференции (Москва, 7–11 декабря 2004 г.). — М.: Издательский отдел факультета ВМиК МГУ им. М. В. Ломоносова, 2004. — С. 150–153.

3. Капабланка Х. Р. Учебник шахматной игры (пер. с англ.). Изд. 2-е. — М.: Физкультура и спорт, 1975.

О ВЛОЖЕНИИ ГРАФОВ В РЕШЕТКИ ОГРАНИЧЕННОЙ ВЫСОТЫ

А. В. Чашкин (Москва)

В работе рассматриваются два вопроса о сложности реализации графов в трехмерном пространстве. В качестве меры сложности используется минимально возможный объем выпуклой области ограниченной высоты, внутри которой можно поместить реализуемый граф. Дадим необходимые определения. Множество

$$H_{k,m,n} = \{v = (v_1, v_2, v_3)\},$$

где $v_1 \in \{0, 1, \ldots, k-1\}$, $v_2 \in \{0, 1, \ldots, m-1\}$ и $v_3 \in \{0, 1, \ldots, n-1\}$ назовем целочисленной решеткой ширины k, длины m и высоты n. Объемом решетки $H_{k,m,n}$ назовем произведение $V(H_{k,m,n}) = kmn$. Элементы решетки будем называть вершинами. Значением вершины $v = (v_1, v_2, v_3)$ назовем величину $||v|| = v_1 \cdot nm + v_2 \cdot n + v_3$. Пару вершин (v, u), где $v = (v_1, v_2, v_3)$, $u = (u_1, u_2, u_3)$, назовем простым ребром i-го направления, если $|v_i - u_i| = 1$ и $v_j = u_j$ при $j \neq i$. Последовательность простых ребер (v_1, v_2), (v_2, v_3), $\ldots$, (v_{k-1}, v_k) назовем составным ребром (v_1, v_k) и будем говорить, что это ребро связывает вершины v_1 и v_k, которые будем называть концевыми вершинами ребра. Пусть G — граф с множеством вершин V и множеством ребер W. Будем говорить, что граф G вложен в решетку $H_{k,m,n}$, если каждой вершине v и каждому ребру (v, u) графа G поставлены в соответствие вершина $h(v)$ и составное ребро $h(v, u) = (h(v), h(u))$ решетки $H_{k,m,n}$ так, что разным вершинам графа соответствуют разные вершины решетки, которые находятся на ее границе, и любые два ребра решетки могут пересекаются только в общей концевой вершине. Сложностью вложения графа G в решетку высоты d назовем величину $V_d(G) = \min V(H_{k,m,d})$, где минимум берется по всем решеткам $H_{k,m,d}$ высоты d, в которые можно вложить граф G. Через $G_3(q)$ обозначим множество связанных неориентированных графов без кратных ребер и петель с q вершинами, у которых степень каждой вершины не превосходит трех. Следующая теорема является распространением основного результата работы [1] на случай, когда графы размещаются в пространстве ограниченной высоты.

Теорема 1. *При $q \to \infty$ и $2 \le d = O(\sqrt{q})$:*

1) *любой граф G из $G_3(q)$ может быть вложен в решетку высоты d так, что $V_d(G) = O\left(q^2/d\right)$;*

2) *для почти каждого графа G из $G_3(q)$ справедливо равенство $V_d(G) = \Omega\left(q^2/d\right)$.*

Доказательство верхней оценки теоремы аналогично доказательству из [1] и отличается от него только иным выбором значений параметров. Нижняя оценка доказывается ниже в леммах 1–3.

Пусть G — граф с вершинами $v_1, \ldots, v_n$, π — нумерация вершин G. Через $d_\pi(j)$ обозначим число вершин с номерами от 1 до j, связанных ребрами с остальными вершинами. Шириной графа G назовем величину

$$d(G) = \min_{\pi} \max_{1 \le j \le n} d_\pi(j), \tag{1}$$

где минимум берется по всем возможным нумерациям вершин.

Через $N(p, q, d)$ обозначим число связанных неориентированных графов ширины d без кратных ребер и петель с q вершинами и p ребрами.

Лемма 1. *При некоторых постоянных c_1 и c_2 справедливо неравенство*

$$N(p, q, d) \le c_1^p (c_2 d)^{p-q+1}.$$

Доказательство. Пусть G — связанный граф ширины d с q вершинами и p ребрами, π — нумерация его вершин, на которой в (1) достигается минимум. Вершины графа G разобъем на $\lceil \frac{n}{d} \rceil$ подмножеств V_j, каждое из которых, кроме может быть последнего, состоит из d вершин с последовательными номерами. Граф G преобразуем в граф G' следующим образом. Если вершина $v_i \in V_j$ связана ребрами с вершинами $v_{i_k} \in V_{j_k}$, где $j_k \ge j + 2$, то: 1) в V_{j+1} добавим вершину v'_i; 2) свяжем эту вершину ребрами с вершиной v_i и с вершинами v_{i_k}; 3) удалим ребра, связывающие v_i с вершинами v_{i_k}. Будем выполнять описанную операцию до тех пор, пока это возможно. В результате, в графе G' для каждого V'_j любая вершина из этого множества будет связана ребрами только с вершинами из V'_{j-1}, V'_j и V'_{j+1}. Нетрудно видеть, что каждое множество V'_j графа G' состоит не более чем из $2d$ вершин. Поэтому число вершин q' в графе G' не больше чем $2q$. Также легко видеть, что разность числа ребер p' и вершин q' графа G' равна $p - q$.

В графе G выделим остовное дерево с корнем, лежащим в V_1. На ребрах дерева введем ориентацию, полагая, что все ребра ориентированы от корня. Каждое ребро (u, v) пометим меткой $\mu((u, v))$ так, что

$$\mu((u, v)) = \begin{cases} 1, & \text{если } u \in V_j,\ v \in V_{j+1}; \\ 0, & \text{если } u \in V_j,\ v \in V_j; \\ -1, & \text{если } u \in V_j,\ v \in V_{j-1}. \end{cases}$$

Из [2] легко следует, что для числа N таких размеченных остовных деревьев справедлива оценка

$$N \le 12^{2q}, \qquad (2)$$

которая получается перемножением величины 2^{4q}, являющейся верхней оценкой корневых деревьев с $2q$ вершинами из [2], и числа 3^{2q-1}, равного числу последовательностей, составленных из меток ребер. В [2] деревья с $2q$ вершинами кодируются двухсимвольными последовательностями длины $4q$ так, что можно однозначно указать пару символов, соответствующих каждой вершине. Поэтому в оценке (2) учитывается некоторый линейный порядок на множестве вершин дерева, т. е. можно считать, что вершины остовного дерева перенумерованы. Более того, разметка ребер позволяет установить нумерацию вершин внутри каждого множества V'_j. Номер вершины $v \in V'_j$ среди вершин этого множества обозначим через $\eta(v)$. Очевидно, что для каждой вершины v справедливо неравенство $\eta(v) \le 2d$. Нетрудно показать, что оставшиеся ребра, а их не более $p-q+1$, можно расположить в графе не более чем

$$2^{p+2q-1}(6d)^{p-q+1} \qquad (3)$$

способами. Число (3) получается следующим образом. На оставшихся ребрах произвольным образом введем ориентацию. Каждое ребро зададим, указав вершину, из которой это ребро выходит, и вершину, в которую оно входит. Все вершины, из которых ребра выходят, зададим набором из нулей и единиц длины не более $p+2q-1$. В этом наборе число единиц, находящихся между i-м и $(i+1)$-м нулями, равно числу ребер, выходящих из $(i+1)$-й вершины графа. Все вершины, в которые ребра входят, зададим набором длины не более $(p-q+1)$, в которой j-й элемент соответствует j-у ребру и является парой (x,y). Здесь $x=1$, если ребро направлено из вершины множества V'_i в вершину множества V'_{i+1}; $x=-1$, если ребро направлено в вершину множества V'_{i-1}; $x=0$, если ребро направлено в вершину множества V'_i. Число y равно номеру $\eta(v)$ той вершины v, в которую ребро входит.

Объединяя (2) и (3), видим, что число различных размеченных графов G' не превосходит величины $12^{2q}2^{p+2q-1}(6d)^{p-q+1}$. Наконец заметим, что для восстановления графа G из графа G' достаточно удалить вершины, добавленные при построении графа G'. Эти вершины можно выделить не более чем 2^{2q} способами. Умножая $12^{2q}2^{p+2q-1}(6d)^{p-q+1}$ на 2^{2q} и учитывая, что число ребер в связанном графе не меньше числа вершин без единицы, получаем требуемую оценку для числа рассматриваемых графов. Лемма доказана.

Через $N_3(q)$ обозначим число связанных неориентированных графов без кратных ребер и петель с q вершинами, у которых степень каждой вершины не превосходит трех, т. е. $N_3(q) = |G_3(q)|$.

Лемма 2. *При некоторой постоянной c_3 справедливо неравенство*

$$N_3(q) \ge (c_3 q)^{q/2}.$$

Доказательство. Без ограничения общности будем полагать, что число вершин q четное и равно $2k$. Занумеруем вершины числами от 1 до $2k$. Проведем ребра между вершинами с номерами i и $i+1$ для $i=1,\dots,2k-1$ и между вершинами с номерами 1 и $2k$, направив их от вершин с меньшими номерами к вершинам с большими номерами. Отметим, что ориентированная цепь, связывающая все вершины графа, однозначно определяет исходную нумерацию вершин. Затем из каждой вершины с номером от 1 до k проведем по одному ребру в вершину с номером от $k+1$ до $2k$ так, чтобы не было кратных ребер и степень каждой вершины была равна трем. Нетрудно видеть, что это можно сделать $k! - 2(k-1)! + (k-2)!$ различными способами. Таким образом существует не менее чем $k! - 2(k-1)! + (k-2)!$ различных связанных ориентированных графов на $2k$ вершинах, степени которых не превосходят трех. Так как ориентацию ребер можно задать 2^{3k} способами, то найдется не менее $(k! - 2(k-1)! + (k-2)!)2^{-3k} \ge (c_3 q)^{q/2}$ различных связанных неориентированных графов на $2k$ вершинах, степени которых не превосходят трех. Лемма доказана.

Лемма 3. *Существует такая постоянная c_4, что при $q \to \infty$ и $2 \le d = O(\sqrt{q})$ для почти каждого графа G из $G_3(q)$ справедливо неравенство $V_d(G)) \ge c_4 q^2/d$.*

Доказательство. Допустим, что найдется такая постоянная c, что граф G из $G_3(q)$ может быть вложен в целочисленную решетку H, высота которой равна d, а объем не превосходит $(cq)^2/d$. В этом случае без ограничения общности будем полагать, что длина H не больше чем cq/d. Вершины графа G перенумеруем числами от 1 до p так, что если для произвольных вершин v_i и v_j справедливо неравенство $||h(v_i)|| < ||h(v_j)||$, то номер вершины v_i меньше номера вершины v_j. Пусть v — произвольная вершина графа G и $h(v) = (v_1, v_2, v_3)$ — реализация этой вершины в решетке H. Множество вершин G разобъем на два подмножества V_1 и V_2, первое из которых состоит из вершины v и всех вершин с меньшими номерами, а второе — из всех остальных вершин. Нетрудно видеть, что реализация любого ребра, связывающего вершины из V_1 и V_2, обязательно пересекает плоскость проходящую через вершины, у ко-

торых первая координата равна v_1. Следовательно, число вершин из V_1, связанных с вершинами из V_2, не превосходит количества точек решетки H, первая координата которых равна v_1, т. е. не превосходит величины $d \cdot cq/d = cq$. Таким образом, ширина графа G не больше, чем cq. В силу леммы 1 число таких графов не превосходит $c_1^q (c_2 cq)^{q/2+1} \le (c_1 c_2 cq)^{q/2+1}$. С другой стороны, в силу леммы 2, $N_3(q) \ge (c_3 q)^{q/2}$. Поэтому, при $c < c_3/4c_1c_2$ цепочка неравенств

$$(c_1 c_2 cq)^{q/2+1} \le (2c_1 c_2 cq)^{q/2} \le (c_3 q/2)^{q/2} = o(N_3(q))$$

приводит к противоречию. Лемма доказана.

Следующую теорему приведем без доказательства. Эта теорема является обобщением леммы 11 из [3], в которой рассматривается перестройка булевой схемы, вложенной в трехмерную кубическую решетку, в плоскую схему [4]. Заметим, что метод перестройки схемы, использованный в [3], существенным образом опирается на равенство ширины, длины и высоты исходной схемы и поэтому не может быть использован для доказательства теоремы 2.

Теорема 2. *Граф, вложенный в решетку ширины n, длины m и высоты dk, можно вложить в решетку высоты $O(d)$ так, что ширина и длина этой решетки по порядку величины не превосходят соответственно kn и km.*

Из теоремы 1 легко следует, что утверждение теоремы 2 является точным, с точностью до постоянного множителя.

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

Список литературы

1. Колмогоров А. Н., Барздинь Я. М. О реализации сетей в трехмерном пространстве // Проблемы кибернетики. — 1967. — Вып. 19. — С. 261–268.

2. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. — 1963. — Вып. 10. — С. 63–97.

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

4. Кравцов С. С. О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов // Проблемы кибернетики. — 1967. — Вып. 19. — С. 285–292.

ОЦЕНКИ СЛОЖНОСТИ ПРИБЛИЖЕНИЯ НЕПРЕРЫВНЫХ ФУНКЦИЙ НЕКОТОРЫХ КЛАССОВ ДЕТЕРМИНИРОВАННЫМИ ФУНКЦИЯМИ С ЗАДЕРЖКОЙ

А. Н. Черепов (Смоленск)

Задача об оценке сложности реализации непрерывных функций и классов таких функций, была поставлена А. Н. Колмогоровым в начале 60-х годов 20 века. При этом, в качестве множества приближающих функций A бралось множество дискретных функций, близких к автоматным [1]. Несколько иной подход был рассмотрен С. Б. Гашковым [2], множество A при этом совпадает с множеством функций, реализуемых схемами в непрерывных базисах. В предлагаемой работе, в качестве множества приближающих функций рассматривается класс дискретных детерминированных функций с задержкой. Этот класс появляется при естественном обобщении понятия детерминированной функции. В этом смысле, задача приближения детерминированными функциями с задержкой является более близкой к колмогоровской постановке, чем подход, реализованный С. Б. Гашковым. Использовать детерминированные функции с задержкой для приближения непрерывных функций предложил В. А. Буевич. Первые результаты о приближении непрерывных функций функциями с задержкой были получены Н. Ф. Тюленевым [3].

Рассмотрим множество всех бесконечных двоичных последовательностей E. Множество всех функций вида $f : E^n \to E$ обозначим P. Предположим, что $a_1, a_2, \ldots, a_n$ последовательности из E, а $\tilde{a} = (a_1, a_2, \ldots, a_n)$ — набор таких последовательностей. Пусть $a_1|k, a_2|k, \ldots, a_n|k$ первые k членов последовательностей $a_1, a_2, \ldots, a_n$ соответственно, тогда $\tilde{a}|k = (a_1|k, a_2|k, , a_n|k)$.

Назовем функцию f *детерминированной*, если для всех $k = 1, 2, \ldots$ выполнено:

$$\forall \tilde{a}, \tilde{b} : \tilde{a}|k = \tilde{b}|k \Rightarrow f(\tilde{a})|k = f(\tilde{b})|k.$$

Класс всех детерминированных функций обозначим P_d, все остальные функции из P будем называть недетерминированными.

Определение 1 [3]. Говорим, что функция f является *детерминированной функцией с задержкой* τ, где τ — произвольное неотрицательное целое число, если для любого $k = 1, 2, 3, \ldots$ и любых $\tilde{a}, \tilde{b}$ выполнено:

$$\tilde{a}|k + \tau = \tilde{b}|k + \tau \Rightarrow f(\tilde{a})|k = f(\tilde{b})|k.$$

Множество всех функций с задержкой τ обозначим P_d^τ. Заметим, что $P_d^0 = P_d$. Множество P_d^τ можно определить и следующим образом

Определение 2. Говорим, что функция f является *детерминированной функцией с задержкой* τ, где τ — произвольное неотрицательное целое число, если существует такая детерминированная функция g, что для любого $\tilde{a}$ и $b = g(\tilde{a})$, $b = b(1)b(2)b(3)\ldots$ значение функции f на наборе $\tilde{a}$ равно $f(\tilde{a}) = b(\tau+1)b(\tau+2)b(\tau+3)\ldots$.

Утверждение 1 [4]. *Определения* 1 *и* 2 *эквивалентны.*

Перейдем к функциям вида $f : [0,1]^n \to [0,1]$. При этом будем считать, что числа отрезка $[0,1]$ представлены в двоичной системе счисления и для чисел, допускающих два представления, выберем представление с бесконечным "хвостом" из нулей.

Определение 3. Пусть $\alpha = 0,\alpha_1\alpha_2\ldots, \beta = 0,\beta_1\beta_2\ldots$ — действительные числа отрезка $[0,1]$, и k — натуральное число. Тогда будем считать, что $\alpha|k = \beta|k$, если у чисел α, β совпадают первые k двоичных разряда. Для точек $\tilde{a}, \tilde{b} \in [0,1]^n$ имеем, что $\tilde{a}|k = \tilde{b}|k$, если в каждой координате выполнено равенство $a_i|k = b_i|k$. Действительную функцию f назовем детерминированной, если для любого $k = 1,2,3\ldots$ из $\tilde{a}|k = \tilde{b}|k$ следует, что $f(\tilde{a})|k = f(\tilde{b})|k$. Класс всех детерминированных функций обозначим D_d. В множество D_d^τ действительных детерминированных функций с задержкой τ включим все функции, удовлетворяющие свойству: для любого $k = 1,2,3,\ldots$ из $\tilde{a}|k+\tau = \tilde{b}|k+\tau$ следует $f(\tilde{a})|k = f(\tilde{b})|k$.

Класс D_d^∞ определим как объединение всех множеств D_d^τ. Множества D_d^τ и D_d^∞ могут быть построены по соответствующим им классам дискретных функций, при потере части информации о значениях дискретных функций на последовательностях вида $a(1)a(2)\ldots a(i)0111\ldots$.

Определение 4. Пусть $\varepsilon > 0$, будем говорить, что функция $d(\tilde{x})$ ε-равна функции $f(\tilde{x})$ на единичном кубе $[0,1]^n$, если при любом $\tilde{x} \in [0,1]^n$ имеем, что $\mid f(\tilde{x} - d(\tilde{x}) \mid < \varepsilon$. Будем также говорить, что $d(\tilde{x})$ ε-приближает $f(\tilde{x})$.

Пусть $C[0,1]^n$ — множество непрерывных на единичном кубе $[0,1]^n$ функций, принимающих значения из отрезка $[0,1]$. Для любых точек $\tilde{x}, \tilde{y} \in [0,1]^n$ будем считать, что $\|\tilde{x} - \tilde{y}\| = \max \mid x_i - y_i \mid$, где максимум берется по всем координатам.

Оказывается, что не всякую функцию множества $C[0,1]^n$ можно ε-приблизить детерминированными функциями класса D_d. Но функций класса D_d^∞ уже достаточно для решения этой задачи. В работе [3] следующее утверждение было доказано для функций несколько

более широкого чем D_d^∞ класса.

Теорема. *Для любого* $\varepsilon > 0$ *и любой функции* $f(\tilde{x}) \in C[0,1]^n$ *существует число* $\tau \geq 0$ *и функция* $d(\tilde{x}) \in D_d^\tau$ *такие, что* $d(\tilde{x})$ ε*-рав на* $f(\tilde{x})$.

Определение 5. Для любой непрерывной функции f и любого ε назовем сложностью реализации в классе автоматно-реализуемых с задержкой τ функций, наименьшее τ такое, что существует функция $d(\tilde{x})$ класса D_d^τ, ε-равная f. Сложность реализации функции f будем обозначать $L(f,\varepsilon)$. Пусть задан подкласс H класса непрерывных на множестве $[0,1]^n$ функций, принимающих значения из отрезка $[0,1]$. Положим $L(H,\varepsilon) = \sup[L(f,\varepsilon) : f \in H]$.

Укажем оценки величины $L(H,\varepsilon)$ для некоторых известных классов непрерывных функций, для которых найдены оценки числа 2ε-различимых функций [5].

Введем следующие обозначения [6]. Будем считать, что,

$$f(n) = O(g(n)) \Leftrightarrow |f(n)| \leq |Cg(n)|,$$

для некоторой константы $C > 0$. Аналогично,

$$f(n) = \Omega(g(n)) \Leftrightarrow |f(n)| \geq |Cg(n)|,$$

если существует такая константа $C > 0$. Кроме того, если $f(n) = \Omega(g(n))$ и $f(n) = O(g(n))$, то $f(n) = \Theta(g(n))$.

Рассмотрим некоторые из известных классов непрерывных функций. Напомним, что функция $f(\tilde{x})$ удовлетворяет условию Гельдера с показателем α и константой L, если для любых выполнено:

$$\mid f(\tilde{x}) - f(\tilde{y}) \mid \leq L \| \tilde{x} - \tilde{y} \|^\alpha,$$

где в качестве нормы рассматривается максимум модуля разности координат. В дальнейшем будем предполагать $L = 1$, что не ограничивает общность рассмотрения и именно такую норму. Обозначим класс функций не более чем от n аргументов, удовлетворяющих условию Гельдера с показателем α и константой $L = 1$, через $G_n(\alpha)$.

Утверждение 2. $L(G_1(1),\varepsilon) = \Theta(\log(1/\varepsilon)))$.

Класс функций от n аргументов, удовлетворяющих условию Гельдера [5]. Рассмотрим множество $F_r G_n(\alpha)$ действительных функций n переменных, определенных на $[0,1]^n$, все частные производные порядка не выше r, удовлетворяют условию Гельдера с показателем $0 < \alpha \leq 1$ и константой $L = 1$, кроме того, эти производные в начале координат не больше 1.

Утверждение 3. *Справедлива верхняя оценка* $L(F_rG_n(\alpha),\varepsilon) = O(1/\alpha(\log(1/\varepsilon)))$.

Утверждение 4. *Справедлива нижняя оценка* $L(F_rG_n(\alpha),\varepsilon) = \Omega(1/s\log 1/\varepsilon)$, *где* $s = r+\alpha$.

Следствие. *Справедлива оценка* $L(G_1(\alpha),\varepsilon) = \Theta(1/\alpha(\log 1/\varepsilon))$.

Класс F_r [1, 5]. Класс F_r определяется как класс непрерывных на отрезке $[0,1]$ функций, имеющих r производных. Функции $f \in F_r$ и их производные удовлетворяют неравенствам

$$\max \mid f^{(i)}(x) \mid < 1, i = 1,2,\ldots,r,$$

$$f^{(i)}(0) = 0, i = 1,2,\ldots,r-1.$$

Утверждение 5. *Для функций класса* F_r *справедлива верхняя оценка* $L(F_r,\varepsilon) = O(\log 1/\varepsilon)$.

Утверждение 6. *Для функций класса* F_r *справедлива нижняя оценка* $L(F_r,\varepsilon) = \Omega(1/r(\log 1/\varepsilon))$.

Класс F_A аналитических функций [5]. Класс F_A определяется как класс аналитических в некоторой области функций, производные которых удовлетворяют неравенствам:

$$\max|f^{(i)}(x)/i!| \le (1/2)^i, i = 1,2,\ldots.$$

Поскольку функции этого класса удовлетворяют условию Липшица, то справедливо утверждение.

Утверждение 7. *Для функций класса* F_A *выполнена следующая верхняя оценка* $L(F_A,\varepsilon) = O(\log 1/\varepsilon)$.

Утверждение 8. *Для функций класса* F_A *выполнена нижняя оценка* $L(F_A,\varepsilon) = \Omega(\log(\log 1/\varepsilon))$.

Автор выражают свою признательность В. А. Буевичу за постановку задачи и существенную помощь, оказанную при окончательном оформлении результатов.

Список литературы

1. Офман Ю. О. приближенной реализации непрерывных функций на автоматах // ДАН СССР. — 1963. — Т. 152, № 4. — С. 823–825.

2. Гашков С. Б. О сложности приближенной реализации непрерывных функций схемами и формулами в полиномиальных и некоторых других базисах // Математические вопросы кибернетики. Вып. 5. — М.: Физматлит, 1994.Ё— С. 144–207.

3. Тюленев Н. Ф. Приближение непрерывных функций дискретными // Труды семинара по дискр. матем. и ее применениям. — М.: Изд-во мех-мат ф-та МГУ, 1997. — С. 148–151.

4. Черепов А. Н., Черепов И. А. О классификации недетерминированных функций // Материалы VIII Международного семинара «Дискретная математика и ее приложения». — М.: Изд-во механико-математического факультета МГУ, 2004. — С. 163–166.

5. Витушкин А. Г. Оценка сложности задачи табуляции. — М.: Физматгиз, 1959.

6. Грехем Р., Кнут Д., Паташник О. Конкретная математика. — М.: Мир, 1998.

ОБ АСИМПТОТИЧЕСКИ НАИЛУЧШИХ ПО НАДЕЖНОСТИ СХЕМАХ В БАЗИСАХ $\{\to,\oplus\}$ И $\{\not\to,\sim\}$ ПРИ ИНВЕРСНЫХ НЕИСПРАВНОСТЯХ НА ВХОДАХ ЭЛЕМЕНТОВ

В. В. Чугунова (Пенза)

Рассматривается реализация булевых функций схемами из ненадежных функциональных элементов в базисах $\{\to,\oplus\}$ и $\{\not\to,\sim\}$. Схема реализует функцию $f(x_1, x_2, ..., x_n)$, если при поступлении на входы схемы набора $\tilde{a} = (a_1, a_2, ..., a_n)$ при отсутствии неисправностей на выходе схемы появляется значение $f(\tilde{a})$ [1]. Предполагается, что все элементы схемы независимо друг от друга с вероятностью ε ($\varepsilon < 1/2$) подвержены инверсным неисправностям на входах. Эти неисправности характеризуются тем, что поступающее на вход элемента значение a, ($a \in \{0,1\}$) с вероятностью ε может превратиться в значение $\bar{a}$.

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

Обозначим $P(f) = \inf P(S)$, где S — схема из ненадежных элементов, реализующая булеву функцию $f(x_1, x_2, ..., x_n)$. Схему A из ненадежных элементов, реализующую булеву функцию $f(x_1, x_2, ..., x_n)$, назовем асимптотически наилучшей по надежности, если $P(A) \sim P(f)$ при $\varepsilon \to 0$.

1. Базис $\{\to, \oplus\}$.

Построим асимптотически наилучшие по надежности схемы из ненадежных элементов в базисе $\{\to, \oplus\}$.

Теорема 1. *При $\varepsilon < 1/2$ функцию $x|y$ в базисе $\{\to, \oplus\}$ можно реализовать такой схемой S_h, ненадежность которой $P(S_h) \le 4\varepsilon$.*

Доказательство. Построим схему S, реализующую функцию $x|y$, моделируя формулу $(x \to y) \oplus y$. Схема S содердит два ненадежных элемента. Ненадежность каждого элемента не больше 2ε. Поэтому ненадежность схемы S не больше 4ε.

Схема S является искомой схемой S_h. Теорема 1 доказана.

Верхняя оценка ненадежности схем получена в теореме 2.

Теорема 2. *При $\varepsilon \le 1/200$ любую булеву функцию f в базисе $\{\to, \oplus\}$ можно реализовать схемой S с ненадежностью $P(S) \le 2\varepsilon + 66\varepsilon^2$.*

Для доказательства теоремы 2 используем теоремы 3 и 4.

Пусть схема S_h реализует функцию $x|y$ с ненадежностью μ.

Теорема 3 [2]. *Если $\mu \le 1/50$, то любую функцию f можно реализовать схемой S, ненадежность которой $P(S) \le 4\mu$.*

Теорема 4 [3]. *Пусть f — произвольная функция, S — схема, реализующая функцию f с ненадежностью $P(S)$, S' — схема, реализующая функцию $\bar{f}$ с ненадежностью $P(S')$. Тогда по схемам S и S' можно построить схему $\varphi(S, S')$, реализующую функцию f, для которой $P(\varphi(S, S')) \le 2\varepsilon + 7\varepsilon^2 + 18\varepsilon\hat{P}(S) + 3\hat{P}^2(S)$, где $\hat{P}(S) = \max\{P(S), P(S')\}$, при $\varepsilon < 1/2$.*

Доказательство. Пусть f — произвольная булева функция. По теореме 3 при $\varepsilon \le 1/200$ ее можно реализовать схемой S с ненадежностью $P(S) \le 16\varepsilon$. Для повышения надежности схемы S будем использовать схему D, реализующую функцию $g(x, y, z) = \overline{xy \vee x\bar{z} \vee y\bar{z}}$. Нетрудно проверить, что $\overline{xy \vee x\bar{z} \vee y\bar{z}} = ((x \oplus y) \to (y \oplus z)) \oplus y$. Моделируя формулу в правой части последнего равенства, построим схему D из четырех элементов. Вероятности ошибок на выходе этой схемы таковы: $P_0(000) \le 5\varepsilon$, $P_0(001) \le 2\varepsilon + 7\varepsilon^2$, $P_1(010) \le 5\varepsilon$, $P_0(011) \le 8\varepsilon$, $P_1(100) \le 8\varepsilon$, $P_0(101) \le 5\varepsilon$, $P_1(110) \le 2\varepsilon + 7\varepsilon^2$, $P_1(111) \le 5\varepsilon$.

Возьмем два экземпляра схемы S, реализующей функцию f, один экземпляр схемы S', реализующей функцию $\bar{f}$, и соединим их выходы с входами схемы D. Построенную таким образом схему обозначим $\varphi(S, S')$. Вычислим вероятности ошибок на выходе этой схемы.

Пусть входной набор $\tilde{a}$ схемы S является нулевым для функции

f ($f(\tilde{a}) = 0$) и единичным для функции $\bar{f}$ ($\bar{f}(\tilde{a}) = 1$). Вероятность ошибки $P_0(\varphi(S, S'), \tilde{a})$ на выходе схемы $\varphi(S, S')$ удовлетворяет неравенству: $P_0(\varphi(S, S'), \tilde{a}) \le (1-P_1(S, \tilde{a}))^2 P_0(S', \tilde{a})5\varepsilon + (1-P_1(S, \tilde{a}))^2(1-P_0(S', \tilde{a}))(2\varepsilon + 7\varepsilon^2) + (1 - P_1(S, \tilde{a}))P_1(S, \tilde{a})P_0(S', \tilde{a})(1 - 5\varepsilon) + (1 - P_1(S, \tilde{a}))P_1(S, \tilde{a})(1 - P_0(S', \tilde{a}))8\varepsilon + P_1(S, \tilde{a})(1 - P_1(S, \tilde{a}))P_0(S', \tilde{a})(1 - 8\varepsilon) + P_1(S, \tilde{a})(1 - P_1(S, \tilde{a}))(1 - P_0(S', \tilde{a}))5\varepsilon + P_1^2(S, \tilde{a})P_0(S', \tilde{a})(1 - 2\varepsilon - 7\varepsilon^2) + P_1^2(S, \tilde{a})(1 - P_0(S', \tilde{a}))(1 - 5\varepsilon) \le 2\varepsilon + 7\varepsilon^2 + 5P_0(S', \tilde{a})\varepsilon + 13P_1(S, \tilde{a})\varepsilon + 2P_0(S', \tilde{a})P_1(S, \tilde{a})$. Следовательно,

$$P_0(\varphi(S, S'), \tilde{a}) \le$$
$$\le 2\varepsilon + 7\varepsilon^2 + 5P_0(S', \tilde{a})\varepsilon + 13P_1(S, \tilde{a})\varepsilon + 2P_0(S', \tilde{a})P_1(S, \tilde{a}). \qquad (1)$$

Пусть входной набор $\tilde{a}$ схемы S является единичным для функции f ($f(\tilde{a}) = 1$) и нулевым для функции $\bar{f}$ ($\bar{f}(\tilde{a}) = 0$). Вероятность ошибки $P_1(\varphi(S, S'), \tilde{a})$ на выходе схемы $\varphi(S, S')$ в этом случае удовлетворяет неравенству: $P_1(\varphi(S, S'), \tilde{a}) \le P_0^2(S, \tilde{a})(1 - P_1(S', \tilde{a}))(1 - 5\varepsilon) + P_0^2(S, \tilde{a})P_1(S', \tilde{a})(1 - 2\varepsilon - 7\varepsilon^2) + P_0(S, \tilde{a})(1 - P_0(S, \tilde{a}))(1 - P_1(S', \tilde{a}))5\varepsilon + P_0(S, \tilde{a})(1 - P_0(S, \tilde{a}))P_1(S', \tilde{a})(1 - 8\varepsilon) + (1 - P_0(S, \tilde{a}))P_0(S, \tilde{a})(1 - P_1(S', \tilde{a}))8\varepsilon + (1 - P_0(S, \tilde{a}))P_0(S, \tilde{a})P_1(S', \tilde{a})(1 - 5\varepsilon) + (1 - P_0(S, \tilde{a}))^2(1 - P_1(S', \tilde{a}))(2\varepsilon + 7\varepsilon^2) + (1 - P_0(S, \tilde{a}))^2 P_1(S', \tilde{a})5\varepsilon \le 2\varepsilon + 7\varepsilon^2 + 5P_1(S', \tilde{a})\varepsilon + 13P_0(S, \tilde{a})\varepsilon + 2P_1(S', \tilde{a})P_0(S, \tilde{a})$. Следовательно,

$$P_1(\varphi(S, S'), \tilde{a}) \le$$
$$\le 2\varepsilon + 7\varepsilon^2 + 5P_1(S', \tilde{a})\varepsilon + 13P_0(S, \tilde{a})\varepsilon + 2P_1(S', \tilde{a})P_0(S, \tilde{a}) \qquad (2)$$

Таким образом, при $\varepsilon < 1/2$ из (1) и (2), считая $\hat{P}(S) = \max\{P(S), P(S')\}$, получим: $P(\varphi(S, S')) \le 2\varepsilon + 7\varepsilon^2 + 18\varepsilon\hat{P}(S) + 3\hat{P}^2(S)$.

Теорема 4 доказана.

Доказательство теоремы 2. Пусть схема S_h реализует функцию $x|y$ с вероятностью ошибки на выходе $P(S_h) \le 4\varepsilon$ (см. теорему 1). Тогда $\mu \le 4\varepsilon$ и $\varepsilon \le 1/200$. По теореме 3 при $\varepsilon \le 1/200$ любую булеву функцию можно реализовать схемой $\tilde{S}$ с ненадежностью $P(\tilde{S}) \le 16\varepsilon$. Применяя теорему 4, по схеме $\tilde{S}$ построим схему $\varphi(\tilde{S}, \tilde{S}')$, ненадежность которой $P(\varphi(\tilde{S}, \tilde{S}')) \le 2\varepsilon + 1063\varepsilon^2 + 4096\varepsilon^3 \le 7\varepsilon + 83\varepsilon^2$ при $\varepsilon \le 1/200$. Применяя теорему 4 еще раз, получим схему $\varphi^2(\tilde{S}, \tilde{S}')$, для которой $P(\varphi^2(\tilde{S}, \tilde{S}')) \le 2\varepsilon + 280\varepsilon^2 + 5383\varepsilon^3 + 33516\varepsilon^4 + 148176\varepsilon^5 + 592704\varepsilon^6 \le 3\varepsilon + 108\varepsilon^2$, при $\varepsilon \le 1/200$. На четвертом шаге итерации построим схему $\varphi^3(\tilde{S}, \tilde{S}')$, ненадежность которой $P(\varphi^3(\tilde{S}, \tilde{S}')) \le 2\varepsilon + 88\varepsilon^2 + 3915\varepsilon^3 + 37908\varepsilon^4 + 104976\varepsilon^5 + 1259712\varepsilon^6 \le 2\varepsilon + 109\varepsilon^2$, при $\varepsilon \le 1/200$. По схеме $\varphi^3(\tilde{S}, \tilde{S}')$ построим схему $\varphi^4(\tilde{S}, \tilde{S}')$, реализующую f с ненадежностью $P(\varphi^4(\tilde{S}, \tilde{S}')) \le 2\varepsilon + 55\varepsilon^2 + 3278\varepsilon^3 +$

$36951\varepsilon^4 + 71286\varepsilon^5 + 1295029\varepsilon^6 \le 2\varepsilon + 73\varepsilon^2$, при $\varepsilon \le 1/200$. Аналогично, по схеме $\varphi^4(\tilde{S}, \tilde{S}')$ строим схему $\varphi^5(\tilde{S}, \tilde{S}')$, ненадежность которой $P(\varphi^5(\tilde{S}, \tilde{S}')) \le 2\varepsilon + 55\varepsilon^2 + 2198\varepsilon^3 + 16863\varepsilon^4 + 31974\varepsilon^5 + 389017\varepsilon^6 \le 2\varepsilon + 67\varepsilon^2$, при $\varepsilon \le 1/200$. По схеме $\varphi^5(\tilde{S}, \tilde{S}')$ построим схему $\varphi^6(\tilde{S}, \tilde{S}')$, реализующую f с ненадежностью $P(\varphi^6(\tilde{S}, \tilde{S}')) \le 2\varepsilon + 55\varepsilon^2 + 2018\varepsilon^3 + 14271\varepsilon^4 + 26934\varepsilon^5 + 300763\varepsilon^6 \le 2\varepsilon + 66\varepsilon^2$, при $\varepsilon \le 1/200$. Схема $\varphi^6(\tilde{S})$ искомая, т.е. $S = \varphi^6(\tilde{S})$. Теорема 2 доказана.

Нижняя оценка ненадежности схем получена в теореме 5.

Пусть $K(n)$ — множество булевых функций вида x_i (где $i = 1, 2, ..., n$) и константы 1 и 0.

Очевидно, что функции x_i можно реализовать абсолютно надежно. Константу 1 можно реализовать с ненадежностью асимптотически не более $3\varepsilon^2$ при $\varepsilon \to 0$ (см. пример 1).

Теорема 5. *Пусть $\varepsilon \le 1/4$, $f(\tilde{x})$ — булева функция, $f \notin K(n)$, и S — любая схема, реализующая f в базисе $\{\to, \oplus\}$. Тогда $P(S) \ge 2\varepsilon - 2\varepsilon^2$.*

Доказательство теоремы проведем, используя лемму 1.

Лемма 1 [4]. *Пусть f — произвольная булева функция, отличная от константы, и S — любая схема ее реализующая. Пусть подсхема B схемы S содержит выход схемы S и реализует булеву функцию f' с ненадежностью $P(B) \le 1/2$. Обозначим p^1 — минимум вероятностей ошибок на выходе схемы B по таким входным наборам $\tilde{b}$, что $f'(\tilde{b}) = 0$. Аналогично p^0 — минимум вероятностей ошибок на выходе схемы B по таким входным наборам $\tilde{b}$, что $f'(\tilde{b}) = 1$. Тогда вероятности ошибок на выходе схемы S удовлетворяют условиям:*

$P_1(S, \tilde{a}) \ge p^1$, если $f(\tilde{a}) = 0$;

$P_0(S, \tilde{a}) \ge p^0$, если $f(\tilde{a}) = 1$.

Замечание 1 [1]. Из леммы 1 следует, что $P(S) \ge \max\{p^0, p^1\}$.

Пример 1. Константу 1 можно реализовать схемой, функционирующей с ненадежностью асимптотически не больше $3\varepsilon^2$ при $\varepsilon \to 0$. Действительно, моделируя формулу $x \to ((x \oplus x) \to (x \to x))$, строим схему S_2 из четырех элементов, реализующую константу 1. Нетрудно проверить, что $P(S_2) \le 3\varepsilon^2 + 12\varepsilon^3$.

Доказательство теоремы 5. Пусть f — булева функция, удовлетворяющая условиям теоремы, а S — произвольная схема, ее реализующая. Схема S содержит, по крайней мере, один элемент. Возможны два случая.

1. Выходному элементу E_1 приписана $\oplus$. Для него вероятности

ошибок на выходе равны: $P_0(01) = P_0(10) = 2\varepsilon - 2\varepsilon^2 = p^0$. При $\varepsilon \le 1/4$ применима лемма 1, поэтому (см. замечание 1), $P(S) \ge 2\varepsilon - 2\varepsilon^2$.

2. Выходному элементу E_1 приписана $\to$. Для него вероятность ошибки на выходе равна: $P_1(10) = 2\varepsilon - \varepsilon^2 = p^1$. При $\varepsilon \le 1/4$ применима лемма 1, поэтому (см. замечание 1), $P(S) \ge 2\varepsilon - 2\varepsilon^2$.

Теорема 5 доказана.

Из теоремы 5 следует, что любая схема, удовлетворяющая условиям теоремы 2 и реализующая булеву функцию $f(\tilde{x})$, $f \notin K(n)$, является асимптотически наилучшей по надежности и функционирует с ненадежностью, асимптотически равной 2ε при $\varepsilon \to 0$.

2. Базис $\{\not\to, \sim\}$.

Ненадежности двойственных схем при инверсных неисправностях на входах элементов равны [5], поэтому в базисе $\{\not\to, \sim\}$, двойственном базису $\{\to, \oplus\}$ справедливы теоремы 6 и 7.

Теорема 6. *При $\varepsilon \le 1/200$ любую булеву функцию f в базисе $\{\not\to, \sim\}$ можно реализовать схемой S с ненадежностью $P(S) \le 2\varepsilon + 66\varepsilon^2$.*

Теорема 7. *Пусть $\varepsilon \le 1/4$, $f(\tilde{x})$ — булева функция, $f \notin K(n)$, и S — любая схема, реализующая f в базисе $\{\not\to, \sim\}$. Тогда $P(S) \ge 2\varepsilon - 2\varepsilon^2$.*

Из теоремы 7 следует, что любая схема, удовлетворяющая условиям теоремы 6 и реализующая булеву функцию $f(\tilde{x})$, $f \notin K(n)$, является асимптотически наилучшей по надежности и функционирует с ненадежностью, асимптотически равной 2ε при $\varepsilon \to 0$.

Число функций в классе $K(n)$ равно $n + 2$ и мало по сравнению с общим числом 2^{2^n} булевых функций от n переменных. Поэтому при инверсных неисправностях на входах элементов в базисах $\{\to, \oplus\}$ и $\{\not\to, \sim\}$ почти все булевы функции можно реализовать асимптотически наилучшими по надежности схемами, функционирующими с ненадежностью, асимптотически равной 2ε при $\varepsilon \to 0$.

Список литературы

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

2. Алехина М. А., Чугунова В. В. Об асимптотически наилучших по надежности схемах в базисах $\{\not\to, ^-\}$ и $\{\to, ^-\}$ при инверсных неисправностях на входах элементов // Известия вузов. Поволжский регион. Естественные науки. — 2005. — № 6 (21). — С. 16–25.

3. Алехина М. А. О надежности схем из ненадежных элементов $x|y$ // Материалы XI Межгосударственной школы-семинара "Синтез и сложность управляющих систем". — М.: Изд-во центра прикл.

исслед. при мех-мат ф-те МГУ, 2001. — С. 9–14.

4. Алехина М. А. Нижние оценки ненадежности схем в некоторых базисах при однотипных константных неисправностях на входах элементов // Дискретный анализ и исследование операций. Серия 1. — 2002. — Т. 9, № 3. — С. 3–28.

5. Алехина М. А. О надежности двойственных схем // Материалы XI Межгосударственной школы-семинара "Синтез и сложность управляющих систем". – М.: Изд-во центра прикл. исслед. при мех-мат ф-те МГУ, 2001. — С. 6–8.

ВЕРШИНЫ ЦЕЛОЧИСЛЕННЫХ МНОГОГРАННИКОВ И РЕШЕНИЕ КРАМЕРОВСКИХ СИСТЕМ

В. В. Чумаков, В. Н. Шевченко (Нижний Новгород)

Известно, что крайняя точка полиэдра, заданного системой неравенств, определяется решением системы

$$Ax = b, \tag{1}$$

где $\det A = \Delta \neq 0$ и $b \in Z^n$.

Компоненты решения x^0 системы (1) определяются по правилу Крамера:

$$x_j^0 = \Delta_j(b)/\Delta, \tag{2}$$

где $\Delta_j(b)$ — определитель матрицы, получающейся из матрицы A заменой j-го столбца на вектор b. Обозначим через $q_i(A,b)$ значение знаменателя i-й компоненты x^0. Пусть $\max\limits_{i=1,\dots,n} q_i(A,b) = q(A,b)$, $\max\limits_{b\in Z^n} q(A,b) = q(A)$, $\max\limits_{A\in\mathbf{A}} q(A) = q(\mathbf{A})$. В ЦЛП (и не только) важно знать возможные пределы изменения величины $q(\mathbf{A})$ для различных классов матриц $\mathbf{A}$.

Из (2) следует известная верхняя оценка:

$$q(A,b) \le |\Delta_n(A)|. \tag{3}$$

Здесь $\Delta_i(A)$ — НОД миноров i-го порядка матрицы A, $i = 1,\dots,n$, т. е. $\Delta_n(A) = \det A$. Примем $\Delta_i(A) = 1$. Заметим, что величины $d_i(A) = \Delta_i(A)/\Delta_{i-1}(A)$, $i = 1,\dots,n$ определяют вид НДФ матрицы A

$$D(A) = diag(d_1(A),\dots,d_n(A)).$$

Введем величины

$$\delta_n(\mathbf{A}) = \max_{A\in\mathbf{A}}\{\Delta_n(A)\}, \quad d_n(\mathbf{A}) = \max_{A\in\mathbf{A}}\{d_n(A)\}$$

и перепишем неравенство (3): $q(\mathbf{A}) \le \delta_n(\mathbf{A})$.

Известно (см., например, [1]), что существуют целочисленные унимодулярные матрицы P и Q такие, что $PAQ = D(A)$. Тогда замена переменных $x' = Q^{-1}x$, $b' = Pb$ приводит систему (1) к виду $D(A)x' = b'$, из чего следуют равенства $q(A) = d_n(A)$, $q(\mathbf{A}) = d_n(\mathbf{A})$.

Данная работа посвящена исследованию характеристик $\delta_{n,k} = \delta_n(C(n,k))$, $d_{n,k} = d_n(C(n,k))$, $\delta^*_{n,k} = \delta_n(C^*(n,k))$, $d^*_{n,k} = d_n(C^*(n,k))$ при заданных натуральных n и k. Здесь

$$C(n,k) = \left\{ (a_{ij}) \in \{0,1\}^{n\times n} : \ \sum_{j=1}^{n} a_{rj} = k, \ \sum_{i=1}^{n} a_{ir} \le k, \ r = 1,\dots,n \right\},$$

$C^*(n,k)$ — подкласс класса $C(n,k)$, состоящий из матриц вида

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_n & a_1 & \dots & a_{n-1} \\ & & \dots & \\ a_2 & a_3 & \dots & a_1 \end{pmatrix}.$$

Определитель матрицы из класса $C^*(n,k)$ называется циркулянтом.

При $\mathbf{A} = \{0,1\}^{n\times n}$ известно [2], что $\delta_n(\mathbf{A}) > H(n)/\Delta(n)$, где $H(n) = 2^{-n}(n+1)^{(n+1)/2}$ — оценка Адамара для определителя $\{0,1\}$-матрицы, а $\Delta(n) = (0,8n+0,8)^{-1/4}\, e^{n/2}$.

Результаты настоящей работы являются продолжением исследований, начатых в [3, 4]. В [3] рассматривается аналогичная задача для класса матриц аксиальной трехиндексной транспортной задачи. В [4] детально исследована задача нахождения $\delta_{n,2}$ и $d_{n,2}$. Показано, что $\delta_{n,2} = 2^{\lfloor n/3\rfloor}$, $d_{n,2} = 2$. В настоящей работе приводятся оценки значения $\delta^*_{n,k}$ и $d^*_{n,k}$ при $k > 2$.

Теорема 1. Справедливы соотношения

$$(k-1)^{n/(k-1)} - (-1)^{n/(k-1)} \le d_{n,k} \le \delta_{n,k} \le k^{n/2},$$

причем нижняя оценка достигается на матрицах из $C^*_{n,k}$.

В частности, при $k = 3$: $2^{n/2} - (-1)^{n/2} \le d_{n,3} \le \delta_{n,3} \le 3^{n/2}$.

Верхняя оценка следует из неравенства Адамара. Докажем нижнюю оценку.

Рассмотрим произвольные матрицы $A_s = (a_{ij}^s)$, где $i, j = 1, ..., k$, $s = 1, ..., t$, $a_{ij}^s \in \{0, 1\}$. Назовем определитель

$$C_{A_1 \dots A_t} = \begin{vmatrix} A_1 & A_2 & \dots & A_t \\ A_t & A_1 & \dots & A_{t-1} \\ & & \dots & \\ A_2 & A_3 & & A_1 \end{vmatrix} \qquad (4)$$

матричным циркулянтом. Заметим, что циркулянт является частным случаем матричного циркулянта при $k = 1$, однако не каждый матричный циркулянт является циркулянтом.

Лемма 1. *Рассмотрим произвольные матрицы* $A_s = (a_{ij}^s)$, где $i, j = 1, ..., k, s = 1, ..., t$. *Рассмотрим матричный циркулянт* $C_{A_1, ..., A_t}$ *и матричный многочлен* $f(x) = A_1 + A_2 x + A_3 x^2 + ... + A_t x^{t-1}$. *Тогда*

$$\det C_{A_1 \dots A_t} = \prod_{j=0}^{t-1} \det f(\varepsilon^j),$$

где ε — *первообразный корень* t*-й степени из единицы.*

Для доказательства достаточно проверить матричное равенство

$$\begin{pmatrix} A_1 & A_2 & \dots & A_t \\ A_t & A_1 & \dots & A_{t-1} \\ & & \dots & \\ A_2 & A_3 & & A_1 \end{pmatrix} \begin{pmatrix} E_k & E_k & \dots & E_k \\ E_k & \varepsilon E_k & \dots & \varepsilon^{t-1} E_k \\ & & \dots & \\ E_k & \varepsilon^{t-1} E_k & \dots & \varepsilon^{(t-1)^2} E_k \end{pmatrix} =$$

$$= \begin{pmatrix} E_k & E_k & \dots & E_k \\ E_k & \varepsilon E_k & \dots & \varepsilon^{t-1} E_k \\ & & \dots & \\ E_k & \varepsilon^{t-1} E_k & \dots & \varepsilon^{(t-1)^2} E_k \end{pmatrix} \times$$

$$\times \begin{pmatrix} \sum\limits_{i=1}^{t} A_i & & & \dots & \\ & \sum\limits_{i=1}^{t} \varepsilon^{i-1} A_i & & \dots & \\ & & & \dots & \\ & & & \dots & \sum\limits_{i=1}^{t} \varepsilon^{(i-1)^2} A_i \end{pmatrix}$$

и воспользоваться теоремой об определителе произведения матриц.

Заметим, что лемма 1 является обобщением хорошо известного результата (см. [5, задача 479]): значение циркулянта определяется равенством

$$\begin{vmatrix} a_1 & a_2 & \dots & a_n \\ a_n & a_1 & \dots & a_{n-1} \\ & & \dots & \\ a_2 & a_3 & & a_1 \end{vmatrix} = h(\varepsilon_1) h(\varepsilon_2) \cdot \dots \cdot h(\varepsilon_n),$$

где $h(x) = a_1 + a_2 x + a_3 x^2 + ... + a_n x^{n-1}$, *и* $\varepsilon_1, \varepsilon_2, ..., \varepsilon_n$ — *все значения корня* n*-й степени из единицы.*

Подставив в (4) $(A_1 - \lambda E)$ вместо A_1, получим

Следствие 1. *Характеристический многочлен матрицы вида* (4) *имеет вид*

$$(-1)^t \lambda^t + (-1)^{t-2} \lambda^{t-2} \sum_{0 \le i < j \le t-1} f(\varepsilon^i) f(\varepsilon^j) +$$

$$+ (-1)^{t-3} \lambda^{t-3} \sum_{0 \le i < j < k \le t-1} f(\varepsilon^i) f(\varepsilon^j) f(\varepsilon^k) + + ... + (-1)^1 \prod_{j=0}^{t-1} f(\varepsilon^j) + A_1.$$

Подставив в (4) матрицы

$$B_1 = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 1 & \dots & 0 \\ & & & & \\ 0 & 0 & 1 & \ddots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ & & & & \\ 0 & 0 & 1 & \ddots & 0 \\ & & & \ddots & \\ 1 & 0 & 0 & \dots & 1 \end{pmatrix},$$

$B_3 = ... = B_t = E_k$ вместо $A_1, \dots, A_t$, получим

Следствие 2. *Пусть* $n = kt$, *где* $k \in N, t \in N$ *и* $k > 1$. *Тогда определитель матрицы*

$$C_{tk, t+1}^* = \begin{pmatrix} B_1 & B_2 & \dots & B_t \\ B_t & B_1 & \dots & B_{t-1} \\ & & \dots & \\ B_2 & B_3 & & B_1 \end{pmatrix}$$

по модулю равен $t^k - (-1)^k$.

Это утверждение дает нижнюю оценку $\delta_{n,k}^*$.

Лемма 2. *НОД миноров* $(n-1)$*-го порядка для циркулянтов вида* (4), *составленных из матриц* $B_1, \dots B_t$, *равен* 1.

Для доказательства достаточно проверить, что подматрица матрицы $C^*_{n,t+1}$, образованная первыми $(n-1)$ строками и первыми $(n-1)$ столбцами, имеет определитель, по модулю равный t^{k-2}. Очевидно, что для любых натуральных t и k НОД$\left(t^k-(-1)^k, t^{k-2}\right)=1$, т. е. существует минор $(n-1)$-го порядка матрицы $C^*_{n,t+1}$, взаимно простой с ее определителем, что доказывает утверждение леммы.

Лемма 2 дает нижнюю оценку величины $d^*_{n,k}$ и тем самым доказывает теорему 1.

Работа выполнена при частичной поддержке РФФИ (грант 05-01-00552).

Список литературы

1. Схрейвер А. Теория линейного и целочисленного программирования. — М.: "Мир", 1991.

2.Шевченко В. Н., Чумаков В. В. О некоторых количественных характеристиках целочисленных матриц // Вестник Нижегородского университета. — 2004. — С. 209–215.

3. Ильичев А. П., Шевченко В. Н. О крайних точках многогранников многоиндексных транспортных задач // Комбинаторно-алгебраические методы в прикладной математике. Межвузовский сборник. — Горький.: Издание ГГУ, 1981. — С. 66–72.

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

5. Проскуряков И. В. Сборник задач по линейной алгебре. — М.: Наука, 1970.

О СЛОЖНОСТИ ТЕСТИРОВАНИЯ ПЕРЕПУТЫВАНИЙ В СХЕМАХ

В. И. Шевченко (Нижний Новгород)

Рассматриваются схемы из функциональных элементов [1], любая из которых может содержать ошибки в соединениях некоторых входов схемы и выходов элементов с входами элементов и выходом схемы. Для диагностики (поиска) и контроля (обнаружения) рассматриваемых неисправностей используются деревья решений (условные тесты) [2–5]. В работе для различных конечных схемных базисов исследуются верхние и нижние оценки минимальной глубины деревьев решений в худшем случае.

Пусть B — некоторое конечное множество функциональных элементов (*схемный базис*), а S — схема в базисе B. Выходы функциональных элементов S и входы S иногда будем называть вершинами. Будем говорить, что в схеме S некоторый элемент b_{s_0} соединен с элементом $b_{s_{t+1}}$, если в S существует последовательность элементов $b_{s_0}, b_{s_1}, \ldots, b_{s_{t+1}}$ такая, что при $i=1,\ldots,t+1$ некоторый вход элемента b_{s_i} соединен с выходом элемента $b_{s_{i-1}}$.

Рассматриваемые в работе *неисправности* в схеме S (*ошибки в соединениях*) определяются путем введения в нее последовательности элементов, каждый из которых имеет два входа, один выход и реализует функцию $\psi(x,y)=y$. Пусть e — элемент, реализующий функцию $\psi(x,y)=y$, а U — это или исходная схема S, или схема, полученная из S путем введения в нее последовательности элементов e. Тогда введение элемента e в схему U осуществляется следующим образом. Присоединим входы элемента e к произвольной паре вершин (v_1,v_2) схемы U (при этом v_1 и v_2 могут совпадать). Если пара (v_1,v_2) содержит вершину, к которой присоединен выход схемы U, то отсоединим его от этой вершины и присоединим к выходу элемента e. Полученную схему обозначим через U'. Если пара (v_1,v_2) не содержит вершину, к которой присоединен выход схемы U, то возьмем в U элемент b такой, что: а) один вход b присоединен к вершине $v_i, i\in\{1,2\}$, б) ни вершина v_1, ни вершина v_2 не являются выходом b и в) элемент b не соединен ни с одним элементом, выходом которого может быть v_1 или v_2. Отсоединим от вершины v_i вход b и присоединим его к выходу e. Полученную схему обозначим через U''. О схемах U' и U'' будем говорить, что они получены из схемы U путем введения элемента e.

Обозначим через $H(S)$ множество схем, состоящее из схемы S и всех схем, которые могут быть получены из S путем введения в нее некоторой последовательности элементов e. Множество различных булевых функций, реализуемых схемами из $H(S)$, обозначим через $F(S)=\{f_1,f_2,\ldots,f_m\}$. Разобъем $H(S)$ на подмножества

$$H_1(S), H_2(S), \ldots, H_m(S)$$

такие, что для $i=1,\ldots,m$ все схемы из $H_i(S)$ реализуют одну и ту же булеву функцию f_i. Для удобства будем предполагать, что $S\in H_1(S)$.

Задача диагностики схемы S состоит в следующем: известно, что заданная схема U принадлежит одному из подмножеств

$$H_{i_1}(S), \ldots, H_{i_k}(S),$$

определить, к какому из этих k подмножеств принадлежит U. Пусть S содержит n входов, тогда *дерево решений* Y для решения этой задачи представляет собой конечное ориентированное корневое дерево, в котором каждой вершине, не являющейся концевой, приписан двоичный набор из $\{0,1\}^n$, каждой концевой вершине — некоторое число из множества $\{i_1,\dots,i_k\}$. Из каждой вершины, не являющейся концевой, исходят ровно две дуги, которым приписаны числа 0 и 1. Далее, для любой функции $f_{i_j} \in F(S)$, реализуемой схемами из $H_{i_j}(S)$, найдется полный путь (от корня до концевой вершины) $\gamma = v_1, u_1, \dots, u_r, v_{r+1}$ такой, что вершине v_{r+1} приписано число i_j и, если при $q = 1,\dots,r$ вершине v_q приписан набор $\alpha_q \in \{0,1\}^n$, а дуге u_q — число $\delta_q \in \{0,1\}$, то функция f_{i_j} — единственная функция в $F(S)$, которая на наборах $\alpha_1,\dots,\alpha_r$ принимает значения $\delta_1,\dots,\delta_r$ соответственно. Максимальная длина полного пути называется глубиной дерева решений Y и обозначается через $h(Y)$. Величина $d^{i_1,\dots,i_k}(S) = \min h(Y)$, где минимум берется по всем деревьям решений для диагностики S, называется *минимальной глубиной деревьев решений для диагностики схемы* S. Обозначим через $d^k(S) = \max d^{i_1,\dots,i_k}(S)$, где максимум берется по всем наборам $\{(i_1,\dots,i_k) : 1 \le i_1 < \dots < i_k \le m\}$, и $d_B(N,k) = \max d^k(S)$, где максимум берется по всем схемам в базисе B, число вершин в которых не роевосходит N.

Введем следущие обозначения:

$$\mu^d_{N,k} = \min\{N, k-1\}, \quad \alpha^d_{N,k} = \min\{2^{\lfloor N/6\rfloor - 1}, k-1\},$$

$$\gamma^d_{N,k} = \min\{2^{N-1}, k-1\}.$$

Теорема 1. *а) Если элементы базиса B реализуют только конъюнкции или константы, или только дизъюнкции или константы, или только линейные булевы функции, то для $N \ge 2$ и $k \ge 2$ справедливы неравенства*:

$$0 \le d_B(N,k) \le \mu^d_{N,k};$$

б) Если элементы базиса B не удовлетворяют ни одному из свойств, перечисленных в а), то имеют место неравества:

$$\alpha^d_{N,k} \le d_B(N,k) \le \gamma^d_{N,k}.$$

Задача контроля схемы S состоит в следущем: известно, что схема $U \in \bigcup_{j=1}^{k} H_{i_j}(S)$, где $i_1 = 1$. Требуется определить, принадлежит

схема U подмножеству $H_1(S)$ или нет. *Дерево решений* Y для решения этой задачи представляет собой конечное ориентированное корневое дерево, состоящее из: 1) вершин $v_0, v_1, \dots, v_r$, которым приписаны двоичные наборы $\alpha_1,\dots,\alpha_r \in \{0,1\}^n$ соответственно, вершины v_{r+1}, которой приписана функция f_1, и вершин $v'_1,\dots,v'_{r+1}$, которым приписана функция $\bar{f}_1$; 2) дуг

$$(v_0,v_1),(v_1,v_2),\dots,(v_r,v_{r+1}),$$

которым приписаны числа $\delta_1,\dots,\delta_r \in \{0,1\}$ соответственно, и дуг $(v_0,v'_1),(v_1,v'_1),\dots,(v_r,v'_{r+1})$, которым приписаны числа $\bar{\delta}_1,\dots,\bar{\delta}_r$ соответственно. При этом функция f_1 — единственная функция в $F(S)$, которая на наборах $\alpha_1,\dots,\alpha_r$ принимает значения $\delta_1,\dots,\delta_r$ соответственно. Число r называется глубиной дерева решений Y и обозначается через $h(Y)$. Величина $c^{i_1,\dots,i_k}(S) = \min h(Y)$, где минимум берется по всем деревьям решений для контроля S, называется *минимальной глубиной деревьев решений для контроля схемы* S.

Обозначим через $c^k(S) = \max c_p^{i_1,\dots,i_k}(S_n)$, где максимум берется по всем наборам $\{(i_1,\dots,i_k) : 1 \le i_1 < \dots < i_k \le m\}$ и $c_B(N,k) = \max c^k(S)$, где максимум берется по всем схемам в базисе B, число вершин в которых не превосходит N.

Введем следущие обозначения:

$$\mu^c_{N,k} = \min\{N, k-1\}, \quad \alpha^c_{N,k} = \min\{2^{\lfloor N/8\rfloor - 1} - 2, k-1\},$$

$$\gamma^c_{N,k} = \min\{2^{N-1} - 1, k-1\}.$$

Теорема 2. *а) Если элементы базиса B реализуют только конъюнкции или константы, или только дизъюнкции или константы, или только линейные булевы функции, то для $N \ge 2$ и $k \ge 2$ справедливы неравенства*:

$$0 \le c_B(N,k) \le \mu^c_{N,k};$$

б) Если элементы базиса B не удовлетворяют ни одному из свойств, перечисленных в а), то имеют место неравества:

$$\alpha^c_{N,k} \le c_B(N,k) \le \gamma^c_{N,k}.$$

Доказательства теорем 1 и 2 основываются на следующих вспомогательных утверждениях.

Лемма 1. *Если ϕ — монотонная булева функция, не являющаяся ни конъюнкцией, ни дизъюнкцией, ни константой, то из нее путем отождествления переменных может быть получена или одна из следующих функций: $x(y \vee z)$, $x \vee yz$, $xy \vee yz \vee xz$, или функции xy и $x \vee y$.*

Лемма 2. *Если ϕ — произвольная немонотонная булева функция, то из нее путем подстановки функций вида x и константы 1 можно получить одну из следующих функций: $\bar{x}$, $\bar{x}\bar{y}$, $x+y+1$ и $x \vee \bar{y}$.*

Лемма 3. *Если ϕ — произвольная нелинейная булева функция, то из нее путем подстановки функций вида x можно получить или одну из функций множества*

$$\{x_1 \cdot x_2, x_1 \cdot \bar{x}_2, \bar{x}_1 \cdot \bar{x}_2, x_1 \vee x_2, x_1 \vee \bar{x}_2, \bar{x}_1 \vee \bar{x}_2\}$$

или одну из функций множества

$$\{x_1 \cdot x_2 + x_2 \cdot x_3 + \bar{x}_1 \cdot x_2 + a \cdot x_1 + b \cdot x_2 + c \cdot x_3 + d : a, b, c, d \in \{0, 1\}\}.$$

Список литературы

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

2. Мошков М. Ю. Деревья решений. Теория и приложения. — Нижний Новгород: Изд-во ННГУ, 1994.

3. Чегис И. А., Яблонский С. В. Логические способы контроля работы электрических схем // Тр. Матем. ин-та АН СССР. — 1958. — Т. 51. — С. 270–360.

4. Шевченко В. И., Мошков М. Ю., Мошкова А. М. Эффективные методы диагностики схем из функциональных элементов // Материалы XI Межгосударственной школы-семинара "Синтез и сложность управляющих систем" (Нижний Новгород, 20–25 ноября 2000 г.). Часть II. — М.: Изд-во центра прикладных исследований механико-математического факультета МГУ, 2001. — С. 228–238.

5. Яблонский С. В., Чегис И. А. О тестах для электрических схем // УМН. — 1955. — Т. 10, вып. 4. — С. 182–184.

ТРИАНГУЛЯЦИИ ВЫПУКЛЫХ МНОГРАННИКОВ И ИХ БУЛЕВЫ ФУНКЦИИ

В. Н. Шевченко (Нижний Новгород)

Каждому выпуклому многограннику P поставим в соответствие булеву функцию φ_p, считая её равной 0 тогда и только тогда, когда на вход подаётся характеристический вектор грани многогранника P. Аналогичный подход удобно использовать и для триангуляций многогранников, в этом случае булевы функции будут многотонными. Цель доклада — изложить имеющиеся и некоторые вновь полученные результаты о граневых комплексах выпуклых многогранников и их триангуляций с точки зрения их связи с соответствующими булевыми функциями. Поскольку возникающие при этом вопросы имеют ответы, как правило, лишь для симплициальных многогранников, которые с комбинаторной (и топологической) точки зрения эквивалентны граничным комплексам триангуляций, последние и вынесены в название.

1. Пусть P — множество решений (называемое далее *полиэдром*) системы линейных неравенств (в вещественном евклидовом пространстве R^d)

$$\sum_{k=1}^{d} a_{ik} x_k \le a_{i0}, i = 1, ..., m. \quad (1)$$

Под *размерностью* P ($\dim P$) понимают максимальное число аффинно независимых решений системы (1), если она совместна, и считают $\dim P = -1$ в противном случае. Ограниченный полиэдр называют *выпуклым многогранником*. Будем называть его также *политопом* или *r-политопом*, если $\dim P = r$. Рассмотрим такую линейную функцию ax, для которой достигается $\max_{x \in P} ax = \alpha$. Множество $P_a = \{x \in P / ax = \alpha\}$ называют *гранью* полиэдра P, в частности при $a = 0$ получим, что P является (единственной) r-мерной гранью r-политопа P. Удобно также считать пустое множество (-1)-мерной гранью любого полиэдра P. Хорошо известно (см., например, [1–5], что любой политоп P можно задать как выпуклую оболочку своих вершин (т. е. 0-мерных граней) $P = conv(v_1, v_2, ..., v_n)$, где

$$conv(v_1, ..., v_n) = \left\{ x = \sum_{j=1}^{n} \lambda_j v_j / \sum_{j=1}^{n} \lambda_j = 1, \lambda_j \ge 0, j = 1, ..., n \right\}, \quad (2)$$

а каждая его грань $P_a = conv(v_j, j \in J_a)$, где $J_a = \{j / av_j = \alpha\}$ Обозначим через $\Gamma_k(P)$ множество k-мерных граней политопа P и положим $\Gamma(P) = \bigcup_{k=-1}^{r} \Gamma_k(P)$, $\delta P = \Gamma(P) / \{P\}$, $f(P) = (f_{-1}(P), f_0(P), ..., f_r(P))$, где $f_k(P) = |\Gamma_k(P)|$ — число k-мерных граней политопа P,

$$f(\lambda, P) = \sum_{k=-1}^{r} f_k(P) \lambda^{k+1}$$

и $f(\lambda, \delta P) = f(\lambda, P) - \lambda^{r+1}$.

Известно также [3–5], что множество

$$\Gamma(P) = \bigcup_{k=-1}^{r} \Gamma_k(P))$$

с естественным частичным упорядочиванием $F \subseteq G$ является градуированной решёткой (определение и свойства решётки см. в [6]), в частности $\inf(P_a, P_b) = P_{a+b}$.

Множество δP называется *граничным комплексом политопа* P.

Политоп P называется r-*симплексом*, если $f(P) = r+1$. Нетрудно видеть, что для него $\Gamma_k(P)$ составляет $(k+1)$-мерный слой $(r+1)$-мерного булева куба, $f_k(P) = \binom{r+1}{k+1}$, $f(\lambda, P) = (1+\lambda)^{r+1}$.

Рассмотрим булеву функцию $\varphi_p = \varphi_p(v_1, ..., v_n)$, множество нулей которой совпадает с множеством характеристических векторов граней политопа P. Тогда, следуя [7], можно получить для φ_p совершенную конъюнктивную и дизъюнктивную нормальные формы (как обычно, $\overline{v}$ — отрицание v):

$$\varphi_p(v_1, ..., v_n) = \prod_{F \in \Gamma(P)} ((\bigvee_{v_j \notin F} v_j) \vee (\bigvee_{v_j \in F} \overline{v_j})), \tag{3}$$

$$\varphi_p(v_1, ..., v_n) = \bigvee_{F \notin \Gamma(P)} \prod_{v_j \in F} v_j \prod_{v_j \notin F} \overline{v_j}. \tag{4}$$

Заменяя в (3) и (4) множество $\Gamma(P)$ на δP получим аналогичные формулы для $\varphi_{\delta P}$, из которых следует, что

$$\varphi_{\delta P}(v_1, ..., v_n) = \varphi_p(v_1, ..., v_n) \bigvee \prod_{j=1}^{n} v_j.$$

В теории линейных неравенств [1, 4] известен алгоритм (назовём его алгоритмом Фурье — Моцкина), позволяющий переходить от описания политопа в виде (1) к виду (2) и обратно. В связи с оценкой трудоёмкости этого алгоритма возникает Задача 1: при заданном $f_0(P) = n$ найти $\max f_k(P)$, — решенная в 1970 г. МакМюлленом [8].

Введённые нами булевы функции φ_p и $\varphi_{\delta P}$ позволяют по-новому взглянуть на Задачу 1 и ставить новые разнообразные вопросы, связанные прежде всего со сложностью. При решении таких вопросов нельзя не воспользоваться необозримым множеством результатов, накопленных маткибернетикой о сложности булевых функций, (см., например, [9]).

Следующее понятие является одним из основных в комбинаторной геометрии [2–5]. Политоп P' называется *комбинаторно эквивалентным* политопу P ($P \sim P'$), если существует взаимно однозначное отображение множества $\Gamma(P)$ на множество $\Gamma(P')$, сохраняющее

отношение включения (при этом решётки называют изоморфными и пишут $\Gamma(P) \approx \Gamma(P')$).

Естественно возникает Задача 2 о реализации f-вектора: перечислить необходимые и достаточные условия, которыми должен обладать целочисленный вектор f, для того, чтобы он совпадал с $f(P)$ для некоторого d-политопа P.

Со времён Штейница, решившего Задачу 2 при $d = 3$ в 1922 г. (см. например, [2]), прогресс невелик. В общем случае известно лишь необходимое условие Эйлера — Пуанкаре

$$f(-1, P) = \sum_{k=-1}^{d} f_k(P)(-1)^{k+1} = 0.$$

Ещё меньше известно про Задачу 3 о числе комбинаторно неэквивалентных d-политопов с заданными f-векторами.

На множестве булевых функций от n переменных введём отношение эквивалентности, положив $\varphi(y_1, ..., y_n) \sim \varphi(y'_1, ..., y'_n)$, если $\varphi(y'_1, ..., y'_n) = \varphi(y_{\pi_1}, ..., y_{\pi_n})$, при некоторой перестановке π переменных $y_1, ..., y_n$.

Следующее легко проверяемое утверждение позволяет дать точный перевод задач комбинаторной геометрии (подобных задачам 2 и 3) на язык булевых функций.

Утверждение 1. $P \sim P' \iff \varphi_p \sim \varphi_{p'}$.

2. В этом пункте рассмотрим класс $P^s(d, n)$ симплициальных (политоп P называется *симплициальным*, если любая его грань, отличная от P, является симплексом) d-политопов с n вершинами.

Граничный комплекс δP симплициального политопа P удовлетворяет условию: если $F \in \delta P$ и $G \subseteq F$, то $G \in \delta P$, — и, следовательно, даёт пример того, что в топологии называется *симплициальным комплексом* [4, 5, 10]. Отсюда следует, что для его задания достаточно знать множество $\Gamma_{d-1}(P) = \{F_1, ..., F_m\}$ или множество $N(P)$ минимальных по включению подмножеств $\{N_1, ..., N_l\}$ вершин булева n-куба, не принадлежащих δP . Множество $N(P)$ необходимо для построения *кольца Стенли-Райснера* [4, 5, 10], применяемого при изучении симплициального комплекса δP алгебраическими методами.

Следующее утверждение, в частности, позволяет решить возникающий при этом вопрос о связи множеств $\Gamma_{d-1}(P)$ и $N(P)$ стандартными методами булевой алгебры.

Утверждение 2. *Если* $P \in P^s(d, n)$, *то булева функция* $\varphi_{\delta p}$ *монотонна,* $\Gamma_{d-1}(P)$ *есть множество её верхних нулей, а* $N(P)$ — *множество её нижних единиц,*

$$\varphi_{\delta P}(v_1,...,v_n)=\prod_{i=1}^{m}\bigvee_{j\notin F_m} v_j,$$

$$\varphi_{\delta p}(v_1,...,v_n)=\bigvee_{k=1}^{l}\prod_{j\in N_k} v_j.$$

Для решения вопросов, связанных с эффективным представлением монотонной булевой функции (в различных базисах) отошлём к обзору [11]).

Отметим следующий результат, полученный в [12]: для любого $P\in P^s(d,n)$ симплициальный комплекс δP линейно разворачиваем, то есть грани из $\Gamma_{d-1}(P)$ можно упорядочить так, что

$$\delta P=\bigcup_{i=1}^{m}[G_i,F_i],$$

где $[G,F]=\{H\in\Gamma(P)/G\subseteq H\subseteq F\}$ и G_i — наименьшая по включению грань грани F_i, не принадлежащая подкомплексу $(\delta P)_k=\bigcup_{i=1}^{k}[G_i,F_i]$

$$\varphi_{(\delta P)_{(k+1)}}(v_1,...,v_n)=\varphi_{(\delta P)_k}(v_1,...,v_n)(\bigvee_{v_j\notin F_k} v_j).$$

Соответствующее утверждение можно сделать и для дизъюнктивной нормальной формы.

Из [12] следует также, что для любого $P\in P^s(d,n)$ многочлен $f(\lambda,\delta P)$ можно представить в виде

$$f(\lambda,\delta P)=\sum_{k=0}^{\lfloor d/2\rfloor} g_k(P)(\lambda^k(1+\lambda)^{d+1-k}-\lambda^{d+1-k}(1+\lambda)^k),$$

где $g_0(P)\equiv 1$ и $g_k(P)$ — целые неотрицательные числа.

Для того, чтобы полностью охарактеризовать f-векторы симплициальных политопов (а, значит, и представляемых ими булевых функций) нам понадобится следующее определение. Для любых натуральных чисел a и i существует единственное *биномиальное i-разложение числа* $a=\binom{a_i}{i}+\binom{a_{i-1}}{i-1}+...+\binom{a_j}{j}$, где $a_i>a_{i-1}>...>a_j\geq j\geq 1$. Тогда число $a^{<i>}=\binom{a_{i+1}}{i+1}+...+\binom{a_{j+1}}{j+1}$ называется *i-й псевдостепенью числа a*.

МакМюллен в 1971 г. (см., например, [4]) предположил, что добавление условий $g_{k+1}(P)\leq(g_k(P))^{<k>}$, $k=1,...,\lfloor d/2\rfloor-1$, решает задачу 2 для класса симплициальных политопов. В 1980 г. это было доказано [12, 13].

3. Множество $B=\{b_1,...,b_n\}$, где $b_j\in\mathbf{R}^d$, назовём *(d,n)-точечной конфигурацией*, если $P=convB$ есть d-политоп. *Триангуляцией политопа P с узлами из множества B* назовём множество $T(B)=\{S_1,...,S_t\}$ таких d-симплексов S_τ, для которых выполнены следующие условия: $\Gamma_0(S_\tau)\subseteq B$, $\bigcup_{\tau=1}^{t}S_\tau=P$, пересечение любых двух d-симплексов является гранью каждого из них.

Тогда множество $\Delta=\bigcup_{\tau=1}^{t}\Gamma(S_\tau)$ даёт ещё один пример симплициального комплекса. При $k=-1,0,...,d$ обозначим через $\Delta_k=\bigcup_{\tau=1}^{t}\Gamma_k(S_\tau)$ множество k-мерных граней симплициального комплекса Δ , через $\delta\Delta=\Delta\bigcap\delta P$ — его граничный подкомплекс, положим $f_k(\Delta)=|\Delta_k|$ и определим многочлены $f(\lambda,\Delta),f(\lambda,\delta\Delta)$ и булевы функции φ_Δ и $\varphi_{\delta\Delta}$ аналогично прежнему.

Утверждение 3. *Для любой триангуляции любой точечной конфигурации булевы функции φ_Δ и $\varphi_{\delta\Delta}$ монотонны. Если $B=\Gamma_0(P)$, то $\varphi_{\delta\Delta}=\varphi_{\delta P}$.*

Для построения триангуляции $T(B)$ необходимо найти систему (1) по заданному множеству B, для чего естественно модифицировать алгоритм Фурье-Моцкина, являющийся итеративной (по n) процедурой. Назовём такие триангуляции ФМ-триангуляциями.

Вопросам построения ФМ-триангуляций, обладающих различными дополнительными свойствами, посвящена недавно защищённая Д. В. Груздевым кандидатская диссертация (см. также [15]). Отсюда можно получить алгоритмы для нахождения множеств верхних нулей и нижних единиц функций $\varphi_{\delta\Delta}=\varphi_{\delta P}$. Отметим, что при оценке трудоёмкости этих алгоритмов использовалась следующая из [16] оценка $t\leq O(n^{\lfloor(d+1)/2\rfloor})$.

Заметим, что симплициальный комплекс Δ, соответствующий ФМ-триангуляции, имеет линейную развёртку, что неверно [17] для произвольных $T(B)$. Однако, из [18] следует, что

$$f(\lambda,\Delta)=\sum_{k=0}^{d+1}\gamma_k(\Delta)\lambda^k(1+\lambda)^{(d+1-k)},$$

где $\gamma_k(\Delta)$ — целые неотрицательные числа, $\gamma_0(\Delta)=1,\gamma_{d+1}(\Delta)=0$, числа $g_k(\Delta)=(\gamma_k(\Delta)-\gamma_{d-k+1}(\Delta))\geq 0$ и удовлетворяют неравенствам $g_{k+1}(\Delta)\leq g_k^{<k>}(\Delta)$ для $k=1,...,\lfloor d/2\rfloor$.

Ещё одно условие, являющееся необходимым по крайней мере для ФМ-триангуляций, сформулировано в [19]: $0\leq\gamma_d(\Delta)\leq\gamma_{d-1}(\Delta)\leq...\leq\gamma_{\lfloor(d+1)/2\rfloor}(\Delta)$.

Вопрос о характеризации многочленов $f(\lambda,\Delta)$ остаётся открытым.

Работа выполнена при поддержке РФФИ (грант 05-01-00552).

Список литературы

1. Черников С. Н. Линейные неравенства. — М.: Наука, 1968.

2. Емеличев В. А., Ковалёв М. М., Кравцов М. К. Многогранники, графы, оптимизация. — М.: Наука, 1981.

3. Grunbaum B. Convex polytopes. — N-Y: Wiley and Sons, 1967.

4. Ziegler G. Lectures on polytopes. — Berlin: Springer-Verlag, 1995.

5. Stanley R. P. Combinatorics and commutative algebra (2-nd ed.) // Progress in mathematics. — Boston: Birkhanser, 1996. — V. 41.

6. Биркгоф Г. Теория решёток. — М.: Наука, 1984.

7. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1979.

8. McMullen P. The maximum numbers of faces of a convex polytop // Mathematika. — 1970. — V. 17. — P. 179–189.

9. Сэвидж Дж. Е. Сложность вычислений. — М.: Факториал, 1998.

10. Бухштабер В. М., Панов Т. Е. Торические действия в топологии и комбинаторике. — М.: МЦНМО, 2004.

11. Коршунов А. Д. Монотонные булевы функции // Успехи математических наук. — 2003. — Т. 58, вып. 5 (353). — С. 89–162.

12. Bruggesser H., Mani P. Shellable decompositions of cells and spheres // Math Scand. — 1971. — V. 29. — P. 197–205.

13. Billera L., Lee C. Sufficiency of Me Mullens conditions for f-vectors of simplicial polytopes // Bull. AMS. — 1980. — V. 2, № 1. — P. 181–185.

14. Stanley R. The number of faces of simplicial convex polytope // Advances in Math. — 1980. — V. 35, № 3. — P. 236–238.

15. Шевченко В. Н. Груздев Д. В. Модификация алгоритма Фурье — Моцкина для построения триангуляции и её звёздной развёртки // Дискретный анализ и исследование операций. Сер. 2. — Новосибирск: Изд-во Ин-та математики, 2006. — Т. 13, № 1. — С. 1–101.

16. Шевченко В. Н. О максимальных триангуляциях выпуклых политопов // Материалы Международной конференции "Дискретный анализ и исследование операций" (Новосибирск, 26 июня – 1 июля 2000 г.). — Новосибирск: Изд-во Ин-та математики, 2000. — С. 163.

17. Rudin M. E. An unshellable triangulation of a tetrahedron // Bulletin AMS. — 1958. — V. 64. — P. 90–91.

18. Kleinschmidt P., Smilasky Z. New results for simplicial spherical polytopes // Discrete and Computation Geometry. DIMACS Scries in Discrete Mathematics and Theoretical Computer Science. — AMS, 1991. — V. 6. — P. 187–197.

19. Шевченко В. Н. Триангуляции точечных конфигураций и их f-вектора // Тезисы докладов XII Международной конференции "Проблемы теоретической кибернетики" ч. II. — М.: Изд-во ЦПИ при механико-математическом ф-те МГУ, 1999. — С. 255.

О ПОСЛЕДОВАТЕЛЬНОЙ РЕАЛИЗАЦИИ ЧАСТИЧНЫХ БУЛЕВЫХ ФУНКЦИЙ

Л. А. Шоломов (Москва)

Рассматриваются схемы из функциональных элементов в произвольном полном конечном базисе, элементам приписаны положительные веса и под сложностью $L(S)$ схемы S понимается сумма весов входящих в нее элементов [1]. Схема S реализует частичную функцию f (обозначение Srf), если она реализует некоторое ее доопределение, т. е. функцию, полученную из f произвольной заменой всех неопределенных символов $*$ значениями 0 и 1. Сложность $L(f)$ функции f — минимальная из сложностей схем, реализующих f. Аналогичные понятия реализуемости $Sr(f,g)$ и сложности $L(f,g)$ могут быть введены для пары (f,g) частичных булевых функций.

Рассматривается последовательная реализация пары (f,g), когда вначале строится схема S_1, реализующая функцию f, затем ее выход используется в схеме S_2, реализующей g. Возможны различные требования к последовательным реализациям. Наиболее сильное состоит в том, чтобы схема S_2 не зависела от S_1 и при присоединении к ней выхода любой схемы, реализующей f, реализовала g. Более слабое требование допускает зависимость S_2 от S_1, но построение S_1 не должно использовать информацию о g. И, наконец, ограничения на S_1 и S_2 могут отсутствовать. Различные типы требований приводят к разным характеристикам сложности последовательной реализации. Введем соответствующие понятия.

Будем считать, что f и g зависят от переменных $x_1,\dots,x_n$. Пусть S_1 — схема с входами $x_1,\dots,x_n$ и выходом y_1, S_2 — схема с входами $x_1,\dots,x_n$, z и выходом y_2. Обозначим через $S_1\circ S_2$ схему с входами $x_1,\dots,x_n$ и выходами y_1,y_2, образованную из S_1 и S_2 присоединением y_1 к входу z. Скажем, что схема $S_1\circ S_2$ *последовательно реализует* пару (f,g), если S_1rf и $(S_1\circ S_2)r(f,g)$. Задавшись

параметром t, $t \geq L(f)$, введем следующие характеристики *сложности последовательной реализации* пары (f,g) при ограничении t на сложность схемы S_1:

$$L_t^{\exists\forall}(f,g) = \min\{s \mid \exists S_2 \forall S_1((S_1 r f \wedge L(S_1) \leq t) \to \\ \to ((S_1 \circ S_2) r(f,g) \wedge L(S_1 \circ S_2) \leq s))\},$$

$$L_t^{\forall\exists}(f,g) = \min\{s \mid \forall S_1 \exists S_2((S_1 r f \wedge L(S_1) \leq t) \to \\ \to ((S_1 \circ S_2) r(f,g) \wedge L(S_1 \circ S_2) \leq s))\},$$

$$L_t^{\exists\exists}(f,g) = \min\{s \mid \exists S_1 \exists S_2(S_1 r f \wedge L(S_1) \leq t \wedge \\ \wedge (S_1 \circ S_2) r(f,g) \wedge L(S_1 \circ S_2) \leq s)\}.$$

Очевидно, $L_t^{\exists\forall}(f,g) \geq L_t^{\forall\exists}(f,g) \geq L_t^{\exists\exists}(f,g) \geq L(f,g)$.

Пару функций (f,g) будем характеризовать набором параметров $l_{\alpha\beta}$, $\alpha,\beta \in \{0,1,*\}$, где $l_{\alpha\beta}$ — число наборов $\tilde{x} = (x_1,\ldots,x_n)$, на которых $f(\tilde{x}) = \alpha$, $g(\tilde{x}) = \beta$. Положим $l(f,g) = (l_{\alpha\beta},\ \alpha,\beta \in \{0,1,*\})$. Обозначим через $p_{\alpha\beta}$ частоту $l_{\alpha\beta}2^{-n}$ пары (α,β) и введем набор частот $p(f,g) = (p_{\alpha\beta},\ \alpha,\beta \in \{0,1,*\})$. Класс всех пар функций (f',g') с $l(f',g') = l(f,g)$ (эквивалентно, с $p(f',g') = p(f,g)$) будем обозначать $\mathcal{K}_n(f,g)$ и называть *частотным классом*, порожденным (f,g). Определим *функцию Шеннона* $L(n,f,g)$ для класса $\mathcal{K}_n(f,g)$ как максимальную из сложностей пар $(f',g') \in \mathcal{K}_n(f,g)$. Аналогичным образом для функции f могут быть определены параметры l_α, p_α, введены наборы $l(f)$ и $p(f)$, частотный класс $\mathcal{K}_n(f)$ и функция $L(n,f)$.

Задавшись функцией $t(n)$, $t(n) \geq L(n,f)$, можно ввести функции Шеннона $L_{t(n)}^{\exists\forall}(n,f,g)$, $L_{t(n)}^{\forall\exists}(n,f,g)$ и $L_{t(n)}^{\exists\exists}(n,f,g)$ для последовательной реализации. Так например, $L_{t(n)}^{\exists\forall}(n,f,g)$ представляет собой максимум величин $L_{t(n)}^{\exists\forall}(f',g')$ по всем $(f',g') \in \mathcal{K}_n(f,g)$. Ясно, что $L_{t(n)}^{\exists\forall}(n,f,g) \geq L_{t(n)}^{\forall\exists}(n,f,g) \geq L_{t(n)}^{\exists\exists}(n,f,g) \geq L(n,f,g)$. В работе изучается возможность одновременного достижения асимптотик для $L(n,f)$ и $L(n,f,g)$ при последовательной реализации, т. е. выполнимости соотношения $L_{t(n)}^{(\cdot)(\cdot)}(n,f,g) \sim L(n,f,g)$ при $t(n) \sim L(n,f)$.

Для $\alpha \in \{0,1,*\}$, $\mu \in \{0,1\}$ запись $\alpha \succeq \mu$ будет означать, что μ является доопределением α. С набором частот $p(f,g)$ и набором

$$Q = (q_{00},q_{01},q_{10},q_{11}),\ q_{\mu\nu} \geq 0,\ q_{00} + \ldots + q_{11} = 1, \tag{1}$$

свяжем функцию

$$\mathcal{H}(p(f,g),Q) = -\sum_{\alpha,\beta\in\{0,1,*\}} p_{\alpha\beta} \log \sum_{\mu\preceq\alpha,\nu\preceq\beta} q_{\mu\nu} \tag{2}$$

(логарифмы двоичные). Положим $\mathcal{H}(p(f,g)) = \min_Q \mathcal{H}(p(f,g),Q)$ и $h_n(f,g) = 2^n\mathcal{H}(p(f,g))$.

Обозначим через $N_n(f,g)$ наименьшую мощность множества пар всюду определенных функций, в котором имеется доопределение для каждой пары $(f',g') \in \mathcal{K}_n(f,g)$. Из [2] следует, что

$$h_n(f,g) - c_1 n \leq \log N_n(f,g) \leq h_n(f,g) + c_2 n, \quad c_1,c_2 = \text{const}.$$

Отсюда при $h_n(f,g)/(n\log n) \to \infty$ вытекает нижняя оценка

$$L(n,f,g) \gtrsim \rho \frac{h_n(f,g)}{\log h_n(f,g)}, \tag{3}$$

где ρ — приведенный вес базиса [1].

Пусть $D(f) = \{\tilde{\alpha} | f(\tilde{\alpha}) \in \{0,1\}\}$ — область определения частичной функции f. Скажем, что функция f *конкретнее* g , если $D(f) \supseteq D(g)$. В случае, когда f конкретнее g, функционал $h_n(f,g)$ может быть выражен через элементы наборов $l(f)$ и $l(f,g)$ явно

$$h_n(f,g) = (\varphi(l_0 + l_1) - \varphi(l_0) - \varphi(l_1)) + \\ + (\varphi(l_{00} + l_{01}) - \varphi(l_{00}) - \varphi(l_{01})) + (\varphi(l_{10} + l_{11}) - \varphi(l_{10}) - \varphi(l_{11})),$$

где $\varphi(x) = x\log x$, параметры l_σ и $l_{\sigma\tau}$ заимствованы из $l(f)$ и $l(f,g)$.

Из результатов работы [3] вытекает

Теорема 1. *Если f конкретнее g и $h_n(f,g)/(n\log n) \to \infty$, то при $t(n) \sim L(n,f)$ имеет место асимптотическое равенство*

$$L_{t(n)}^{\exists\forall}(n,f,g) \sim \rho \frac{h_n(f,g)}{\log h_n(f,g)} \sim L(n,f,g).$$

Очевидно, что этот результат распространяется на функции Шеннона $L_{t(n)}^{(\cdot)(\cdot)}(n,f,g)$ для других типов последовательной реализации. В случае всюду определенных функций f и g все три типа последовательной реализации совпадают и можно просто говорить о функции Шеннона $L_{t(n)}(n,f,g)$ для последовательной реализации.

Следствие 1. *Если функции f и g полностью определены, то при $h_n(f,g)/(n\log n) \to \infty$ и $t(n) \sim L(n,f)$*

$$L_{t(n)}(n,g,f) \sim L_{t(n)}(n,f,g) \sim L(n,f,g).$$

Таким образом асимптотика функции Шеннона для последовательной реализации всюду определенных функций не зависит от порядка их реализации. Для частичных функций это не так.

Дальше будем рассматривать последовательность пар $(f,g) = (f_n, g_n)$ частичных функций с фиксированным набором частот $p(f,g)$ (правильнее было бы говорить об асимптотическом постоянстве набора частот, ибо каждая из величин $l_{\sigma\tau} = 2^n p_{\sigma\tau}$ должна быть целой). Это предположение обеспечивает асимптотическую оценку [2]

$$L(n,f,g) \sim \rho \frac{h_n(f,g)}{\log h_n(f,g)}.$$

При фиксированном $p(f,g)$ набор частот $p(f) = (p_0, p_1, p_*)$ также будет фиксирован. Положим $p_0^0 = p_0/(p_0+p_1)$, $p_1^0 = p_1/(p_0+p_1)$ и $p^0(f) = (p_0^0, p_1^0)$. Скажем, что набор Q, удовлетворяющий условию (1), *согласован* с $p^0(f)$, если $q_{00} + q_{01} = p_0^0$, $q_{10} + q_{11} = p_1^0$. Следующая теорема позволяет получать более высокие оценки сложности последовательной реализации, чем (3).

Теорема 2. *При $t(n) \sim L(n,f)$ имеет место оценка*

$$L^{\exists\exists}_{t(n)}(n,f,g) \gtrsim \rho \frac{h'_n(f,g)}{\log h'_n(f,g)}, \qquad (4)$$

где $h'_n(f,g) = 2^n \min_{Q\in\mathbf{Q}(f)} \mathcal{H}(p(f,g),Q)$, $\mathbf{Q}(f)$ — множество наборов Q, согласованных с $p^0(f)$.

Следствие 2. *Если $t(n) \sim L(n,f)$ и среди точек Q минимума функции (2) нет согласованных с $p^0(f)$, то*

$$L^{\exists\exists}_{t(n)}(n,f,g) \gtrsim L(n,f,g),$$

где $\gtrsim$ обозначает асимптотически строгое неравенство.

Пусть $R = \|r_{\alpha\beta\mu\nu}\|$ — матрица, строки которой соответствуют парам $\alpha\beta$, $\alpha,\beta \in \{0,1,*\}$, столбцы — парам $\mu\nu$, $\mu,\nu \in \{0,1\}$ и элементы удовлетворяют условиям $r_{\alpha\beta\mu\nu} \geq 0$, $\sum_{\alpha,\beta,\mu,\nu} r_{\alpha\beta\mu\nu} = 1$. С матрицей R свяжем функцию

$$\mathcal{I}(R) = \sum_{\alpha,\beta,\mu,\nu} r_{\alpha\beta\mu\nu} \log \frac{r_{\alpha\beta\mu\nu}}{\sum_{\alpha,\beta} r_{\alpha\beta\mu\nu} \sum_{\mu,\nu} r_{\alpha\beta\mu\nu}}.$$

Будем говорить, что *матрица R согласована с $p(f,g)$ и $p^0(f)$*, если $\sum_{\mu,\nu} r_{\alpha\beta\mu\nu} = p_{\alpha\beta}$, $\sum_{\alpha,\beta,\nu} r_{\alpha\beta\mu\nu} = p^0_\mu$.

Следующая теорема улучшает оценку теоремы 2.

Теорема 3. *При $t(n) \sim L(n,f)$ имеет место оценка* (4)*, в которой $h'_n(f,g) = 2^n \min_{R\in\mathbf{R}(f,g)} \mathcal{I}(R)$, где $\mathbf{R}(f,g)$ — множество матриц R, согласованных с $p(f,g)$ и $p^0(f)$.*

В качестве примера рассмотрим пару (f,g) с параметрами $p_{00} > 0$, $p_{11} > 0$, $p_{1*} > 0$ и $p_{\alpha\beta} = 0$ для остальных пар $\alpha\beta$. Пусть $t(n) \sim L(n,f)$, $t'(n) \sim L(n,g)$. Поскольку f конкретнее g и доопределяет g, учитывая результат из [1] о реализации функций с данным числом единиц, получаем $L^{\exists\forall}_{t(n)}(n,f,g) \sim L(n,f,g) \sim L(n,f) \sim c_1 L_n$, где $L_n = \rho 2^n/n$, $c_1 = -p_{00}\log p_{00} - (1-p_{00})\log(1-p_{00})$. Оценка теоремы 2 применительно к паре (g,f) имеет вид $L^{\exists\exists}_{t'(n)}(n,g,f) \gtrsim c_2 L_n$, где $c_2 = -p_{00}\log p_{00} - p_{11}\log\dfrac{p_{11}}{1-p_{1*}} - p_{1*}\log(1-p_{00})$. Разность $c_2 - c_1$ может быть преобразована к виду $p_{11}\log\dfrac{p_{11}+p_{00}p_{1*}}{p_{11}}$. Эта величина положительна, поэтому $c_2 > c_1$. Теорема 3, примененная к паре (g,f), дает оценку $L^{\exists\exists}_{t'(n)}(n,g,f) \gtrsim c_3 L_n$, где $c_3 = -p_{00}\log p_{00} - p_{11}\log\dfrac{p_{11}}{1-p_{1*}} - \dfrac{p_{00}p_{1*}}{1-p_{1*}}\log p_{1*}$. Разность $c_3 - c_2$ может быть эквивалентно преобразована к виду $p_{1*}p_{00}\left(\dfrac{\log p_{1*}}{1-p_{1*}} + \dfrac{\log(1-p_{00})}{p_{00}}\right)$. Учитывая, что $p_{1*} < 1 - p_{00}$ и функция $(\log x)/x$ возрастает при $0 \leq x \leq 1$, получаем $c_3 > c_2$. Можно указать метод, который для почти всех пар (f,g) с рассматриваемыми в примере параметрами дает оценку $L^{\forall\exists}_{t'(n)}(g,f) \lesssim c_3 L_n$ и для них оценка теоремы 3 является точной.

Работа выполнена при финансовой поддержке ОИТВС РАН (проект 1-1) и РФФИ (проект 06-01-00577).

Список литературы

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

2. Шоломов Л. А. О функционалах, характеризующих сложность систем недоопределенных булевых функций // Проблемы кибернетики. Вып. 34. — М.: Наука, 1978. — С. 133–150.

3. Шоломов Л. А. Об относительной сложности булевых функций // Синтез и сложность управляющих систем. Материалы XIV Международной школы-семинара. — Нижний Новгород: Изд-во НГПУ, 2003. — С. 118–122.

О СЛОЖНОСТИ РАСПОЗНАВАНИЯ ЭКВИВАЛЕНТНОСТИ МАШИН ТЬЮРИНГА БЕЗ ЗАПИСИ НА ЛЕНТУ

В. Л. Щербина, В. А. Захаров (Москва)

Рассматривается проблема эквивалентности особых автоматов, являющихся по сути детерминированными одноленточными машинами Тьюринга с ограничением, запрещающим изменять содержимое ленты в процессе работы. Результат вычисления для такой модели определяется как номер ячейки, в которой останавливается головка машины (отсчет производится от стартовой ячейки).

Опишем модель формально. Фиксируем $\mathcal{A}$ — алфавит символов на ленте. *Автоматом* назовем четверку $\langle S, s_0, T, M\rangle$, где S — конечное множество состояний автомата, $s_0 \in S$ — начальное состояние, $T : S \times \mathcal{A} \to S$, $M : S \times \mathcal{A} \to \{-1, 1\}$, причем $\operatorname{dom} T = \operatorname{dom} M$. *Размером* автомата будем считать количество его состояний.

Содержимое ленты задано полным отображением $F : \mathbb{Z} \to \mathcal{A}$. *Вычислением* автомата на этой ленте назовем последовательность пар

$$\langle s_0, n_0\rangle, \langle s_1, n_1\rangle, \ldots \langle s_k, n_k\rangle, \ldots, \qquad (*)$$

где $n_0 = 0$, $s_{i+1} = T(s_i, F(n_i))$, $n_{i+1} = n_i + M(s_i, F(n_i))$, и последовательность заканчивается парой $\langle s_k, n_k\rangle$ тогда и только тогда, когда значение $T(s_k, F(n_k))$ не определено. *Результатом* этого вычисления является число n_k в случае, когда вычисление конечно, и особое значение $\perp$ иначе.

Два автомата называются *эквивалентными*, если для любой функции $F : \mathbb{Z} \to \mathcal{A}$ результаты вычислений этих автоматов на ленте, заданной этой функцией, совпадают.

PSPACE-трудность задачи устанавливается сведением к ней проблемы пустоты пересечения языков, заданных детерменированными конечными автоматами (а PSPACE-полнота этой проблемы установлена Козеном[4]).

Алгоритм, использующий полиномиальную память, строится на основе результата Летичевского, позволяющего свести задачу к исследованию поведения автоматов на лентах ограниченной длины. В несколько ослабленном виде его можно сформулировать таким образом.

Лемма. *Два автомата $\langle S_i, s_{i0}, T_i, M_i\rangle, i = 1, 2$, не являются эквивалентными тогда и только тогда, когда существует лента, на которой выполняется одно из следующих условий*

- *оба автомата работают только в пределах интервала $[-\beta, \beta]$ и останавливаются в различных точках,*

- *оба автомата работают только в пределах интервала $[-\beta, \beta]$, один из них останавливается, другой — нет,*
- *один автомат работает в пределах интервала $[-\beta, \beta]$ и останавливается, а другой выходит за пределы этого интервала,*

где $\beta = 2|\mathcal{A}|(m+1)^{2m}$, $m = \max(|S_1|, |S_2|)$.

Основная идея состоит в том, чтобы выразить условие существования такой ленты для пары конкретных автоматов в виде квантифицированной булевой формулы (QBF), длина которой ограничена полиномом от размеров автоматов.

Для этого достаточно разбить вычисления обоих автоматов и содержимое ленты на ограниченные блоки информации, относящиеся к каждой ячейке ленты, и записать требуемые свойства ленты локальными соотношениями между такими блоками. На основе такого представления нетрудно построить QBF, истинную тогда и только тогда, когда фрагмент ленты с требуемыми свойствами существует, и длина которой логарифмически зависит от допустимой длины этого фрагмента. Делается это с помощью стандартного приема, позволяющего компактно представить формулу вида $\exists b(P(a, b) \wedge P(b, c))$ в виде

$$\exists b \forall x \forall y (x = a \wedge y = b \vee x = b \wedge y = c \to P(x, y))$$

Этот прием позволяет на основе формулы, описывающей соотношение между соседними блоками, строить формулу, связывающую блоки, разделенные между собой $2^k - 1$ неизвестными блоками, причем длина такой формулы линейно зависит от k. Такая формула, дополненная кванторами существования по крайним блокам и соответствующими "граничными условиями", и будет искомой.

Естественными составляющими такого блока могут быть символ, записанный на ленте, и следы обоих вычислений в данной ячейке. *Следом* вычисления $(*)$ в ячейке n называется последовательность всех элементов s_{i_j} таких, что соответствующие $n_{i_j} = n$, взятых в том же порядке, в котором они следуют в вычислении. Очевидно, что если состояния в следе повторились, то соответствующее вычисление зацикливается, и эти состояния обозначают начала первого и второго периода следа. Значит, количество следов ограничено, и для их описания достаточно полиномиального от размеров автоматов числа булевых переменных. Условие, связывающее соседние блоки, является в каком-то смысле "законом сохранения": оно гласит, что каждому перемещению головки из ячейки, например, вправо, отвечает прибытие головки в ячейку, непосредственно соседствующую справа с данной (а также устанавливает порядок таких прибытий).

На ленте можно выделить несколько существенных для выражения леммы ячеек: границы рассматриваемого фрагмента, начальная ячейка, конечные ячейки для обоих автоматов (если они завершают работу). Каждый блок можно расширить парой переменных на каждую такую особую точку, сигнализирующих, расположена ли эта точка в данной ячейке, левее или правее нее, и соответствующим образом дополнить соотношения между соседними блоками, а также добавить условия из леммы (к примеру, что оба вычисления не должны завершаться в одной точке).

При таком подходе используется тот факт, что выполнение условий на соседние "следы" (в действительности просто последовательности состояний автомата) при некоторых дополнительных требованиях влечет принадлежность этих "следов" одному вычислению, осуществляемому на соответствующей ленте. В качестве дополнительных требований можно взять условие наличия начальной ячейки, в которой автомат впервые оказывается в начальном состоянии, и условия пустоты "следов" в крайних ячейках (т.е. ограниченность вычисления рассматриваемым фрагментом). Нетрудно показать, что когда все эти условия выполняются, вычисление автомата можно восстановить по шагам (возможность осуществить каждый шаг обеспечивается "законом сохранения"). Если не требовать пустоты "следов" в крайних ячейках, можно утверждать лишь, что некоторые префиксы "следов" (непустые в случае непустоты этих "следов"), будут являться префиксами следов вычисления на данной ленте в соответствующих ячейках. Этот ослабленный вариант используется при переводе в QBF третьего случая леммы (когда существенным является лишь то, что автомат покинул рассматриваемый фрагмент).

Результатом является возможность построения QBF, длина которой ограничена полиномом от размеров автоматов, и соответственно принадлежность рассматриваемой задачи классу PSPACE.

Теорема. *Проблема распознавания эквивалентности автоматов является PSPACE-полной.*

Заметим, что метод очень похож на применяемый в доказательстве PSPACE-полноты проблемы выполнимости QBF. Отличие состоит в том, что там разбиение на блоки происходило по времени (по шагам машины Тьюринга), и весь блок включал содержимое всей ленты в выбранный момент, а здесь разбиение осуществляется в пространстве (по ячейкам ленты), и каждый блок содержит информацию обо всем, что происходило в выбранной ячейке на протяжении всего вычисления.

Список литературы

1. Летичевский А. А. Эквивалентность автоматов относительно полугрупп // Теоретическая кибернетика. Выпуск 6. — Киев, 1970.

2. Алексеев В. Б. Введение в теорию сложности алгоритмов. — М.: Издательский отдел факультета ВМиК МГУ, 2002.

3. Стокмейер Л. Классификация вычислительной сложности проблем // Кибернетический сборник — М.: Мир, 1989.

4. Kozen D., Lower bounds for natural proof systems // Proc. 18th Symposium on Foundations of Computer Science. — Los Alamitos: IEEE Computer Society Press, 1977. — P. 254–266.

О ПРЕОБРАЗОВАНИЯХ ВЕРОЯТНОСТИ БЕСПОВТОРНЫМИ БУЛЕВЫМИ ФОРМУЛАМИ

А. Д. Яшунский (Москва)

Булевы функции как преобразователи вероятности рассматривались ранее многими авторами (см., например, [1–4]). В частности, Р. М. Колпаков [2] исследовал различные постановки задачи о точном получении некоторого значения вероятности с помощью булевых комбинаций независимых бернуллиевских случайных величин, вероятности которых принадлежат некоторому заданному множеству.

В данной работе рассматриваются значения вероятности, которые могут быть получены приближённо путём комбинирования независимых бернуллиевских случайных величин, у которых вероятность обращения в единицу одна и та же, и равна p. В качестве преобразователей вероятности выступают всевозможные бесповторные формулы над заданным базисом B.

Пусть $\hat{\Phi}[x_1, \ldots, x_m]$ обозначает бесповторную булеву формулу [5], содержащую символы переменных $x_1, \ldots, x_m$. Формула $\hat{\Phi}$ задаёт некоторую булеву функцию $f_{\hat{\Phi}}(x_1, \ldots, x_m)$. Функции $f_{\hat{\Phi}}$, в свою очередь, однозначно сопоставляется числовая функция $h_{\hat{\Phi}}(p_1, \ldots, p_m)$, равная вероятности обращения функции $f_{\hat{\Phi}}$ в единицу при подстановке вместо её переменных $x_1, \ldots, x_n$ независимых бернуллиевских случайных величин, у которых вероятность обращения в 1 равна, соответственно, $p_1, \ldots, p_n$.

Определим *функцию вероятности формулы* $\hat{\Phi}$ как $P_1(p|\hat{\Phi}) = h_{\hat{\Phi}}(p, \ldots, p)$. Фактически, функция вероятности формулы $\hat{\Phi}$ есть вероятность обращения формулы в единицу при подстановке вместо

всех её переменных независимых бернуллиевских случайных величин, равных 1 с вероятностью p, и 0 с вероятностью $1-p$.

Запись $\hat{\Phi}[\hat{\Phi}_1, \ldots, \hat{\Phi}_m]$ будем понимать как подстановку формул $\hat{\Phi}_1, \ldots, \hat{\Phi}_m$ в формулу $\hat{\Phi}$ с последующим переименованием переменных таким образом, что получается вновь бесповторная формула (в рассматриваемой задаче наименование переменных в формуле не существенно).

Такая подстановка бесповторных формул, очевидно, согласована с композицией функций $h_{\hat{\Phi}}$ (см., например, [2]): функция h формулы $\hat{\Phi}[\hat{\Phi}_1, \ldots, \hat{\Phi}_m]$ равна $h_{\hat{\Phi}}(h_{\hat{\Phi}_1}, \ldots, h_{\hat{\Phi}_m})$.

Обозначим через $W_B(p)$ замыкание множества значений функций вероятности бесповторных формул над базисом B в точке p, т. е. множество значений всех функций вероятности в точке p с добавлением всех его предельных точек. Целью данной работы является исследование условий на базис B и значение p, при которых множество $W_B(p)$ совпадает с отрезком $[0,1]$. Иными словами, выясняется, для каких базисов B значения функций вероятности бесповторных формул над базисом B сколь угодно точно приближают любое число из отрезка $[0,1]$.

Отметим, что для любого базиса B выполняется $W_B(0), W_B(1) \subseteq \{0,1\}$, поэтому далее будем рассматривать значения $p \in (0,1)$.

Рассмотрим сначала базисы из некоторых специальных классов. Пусть L обозначает класс линейных функций, K — класс функций, являющихся конъюнкциями переменных или константами, и D — класс функций, являющихся дизъюнкциями переменных или константами.

Если $B \subseteq L$, то $W_B(p) \subseteq \bigcup\limits_m \{\frac{1}{2}\,(1 \pm (1-2p)^m)\} \cup \{\frac{1}{2}\}$. Если $B \subseteq K$, то $W_B(p) \subseteq \bigcup\limits_m \{p^m\} \cup \{0,1\}$. Если $B \subseteq D$, то $W_B(p) \subseteq \bigcup\limits_m \{1-(1-p)^m\} \cup \{0,1\}$. Легко видеть, что ни в одном из этих случаев множество $W_B(p)$ не совпадает с отрезком $[0,1]$ ни при каком фиксированном значении p.

Покажем, что для базиса $\{\&, \neg\}$ множество $W_{\{\&,\neg\}}(p)$ при любом фиксированном $p \in (0,1)$ совпадает с отрезком $[0,1]$.

Функция вероятности формулы $\hat{\Psi}_m = x_1 \,\&\, \ldots \,\&\, x_{m+1}$ равна p^{m+1}. Легко видеть, что $P_1(p|\hat{\Psi}_{n-1}[\neg\hat{\Psi}_m, \ldots, \neg\hat{\Psi}_m]) = (1-p^{m+1})^n$.

Покажем, что для любого $p \in (0,1)$, любого $x \in (0,1)$, любого $\varepsilon > 0$ найдутся натуральные m, n такие, что $(1-p^{m+1})^n \in (x-\varepsilon, x+\varepsilon)$. Пусть m таково, что выполняется неравенство $1-p^{m+1} > x$. При любом m имеет место неравенство $1-p^{m+1} < 1$, поэтому последовательность $(1-p^{m+1})^n, n = 1,2,\ldots$ является убывающей. Предел $\lim\limits_{n\to\infty} (1-p^{m+1})^n$ равен нулю, следовательно найдётся такое N, что $(1-p^{m+1})^{N+1} < x \le (1-p^{m+1})^N$.

Рассмотрим разность: $(1-p^{m+1})^N - (1-p^{m+1})^{N+1} = (1-p^{m+1})^N(1-1+p^{m+1}) \le p^{m+1}$. Для достаточно больших значений m выполнено неравенство $p^{m+1} < \varepsilon$. Пусть M таково, что $1-p^{M+1} > x$ и $p^{M+1} < \varepsilon$. Тогда $(1-p^{M+1})^N \in (x-\varepsilon, x+\varepsilon)$.

Доказанное утверждение очевидно распространяется и на значения $x = 0$ и $x = 1$. Таким образом, доказана

Лемма 1. *Для любого $p \in (0,1)$ множество $W_{\{\&,\neg\}}(p)$ есть отрезок $[0,1]$.*

Для базиса $\{\&, \vee\}$ рассуждения весьма схожи со случаем базиса $\{\&, \neg\}$. Функция вероятности формулы $\hat{\Theta}_n[\hat{\Psi}_m, \ldots, \hat{\Psi}_m]$, где $\hat{\Theta}_n = x_1 \vee \ldots \vee x_n$, равна $P_1(p|\hat{\Theta}_n[\hat{\Psi}_m, \ldots, \hat{\Psi}_m]) = 1-(1-p^{m+1})^n$.

Пусть $x \in [0,1]$ и $y = 1-x$. По ранее доказанному, для любого $p \in (0,1)$, любого $\varepsilon > 0$ найдутся натуральные m, n такие, что $(1-p^{m+1})^n \in (y-\varepsilon, y+\varepsilon)$. Следовательно, $1-(1-p^{m+1})^n \in (x-\varepsilon, x+\varepsilon)$. Таким образом, доказана

Лемма 2. *Для любого $p \in (0,1)$ множество $W_{\{\&,\vee\}}(p)$ есть отрезок $[0,1]$.*

Утверждения лемм 1, 2 можно распространить на достаточно широкий класс базисов. Приведём одно вспомогательное утверждение (см., например, [1]):

Лемма 3. *Пусть f — монотонная функция. Если $f \notin K$, то подстановкой констант 0 и 1 из функции f можно получить дизъюнкцию двух переменных. Если $f \notin D$, то подстановкой констант 0 и 1 из функции f можно получить конъюнкцию двух переменных.*

Кроме того, далее будем пользоваться известными леммами о нелинейной и о немонотонной функции [4]. Отметим, что в этих леммах, а также в лемме 3, осуществляется подстановка констант и функций отрицания, и такие подстановки (а также подстановки бесповторных реализаций констант и отрицаний) не нарушают бесповторность формул.

Теорема 1. *Пусть B — некоторый базис. Если $B \not\subseteq L, K, D$, и B содержит константные функции 0 и 1, то для любого $p \in (0,1)$ множество $W_B(p)$ есть отрезок $[0,1]$.*

Доказательство. Если в базисе B найдётся немонотонная функция, то по лемме о немонотонной функции над базисом B можно со-

ставить бесповторную формулу, реализующую отрицание. По условию теоремы в базисе B найдётся нелинейная функция, с помощью которой, по лемме о нелинейной функции, можно составить бесповторную формулу, реализующую конъюнкцию. Согласно лемме 1 множество значений функций вероятности формул, составленных из конъюнкции и отрицания, является всюду плотным на отрезке $[0,1]$ при любом $p \in (0,1)$.

Пусть все функции базиса B монотонные. Согласно условию теоремы, в B найдётся функция, отличная от конъюнкции переменных, и функция, отличная от дизъюнкции переменных. Тогда по лемме 3, над базисом B существуют бесповторные формулы, реализующие конъюнкцию и дизъюнкцию двух переменных. В силу леммы 2, множество значений функций вероятности формул, составленных из конъюнкции и дизъюнкции, является всюду плотным на отрезке $[0,1]$ при любом $p \in (0,1)$. Теорема доказана.

Наличие в базисе B констант 0 и 1 не является необходимым для того, чтобы множество $W_B(p)$ при некотором p совпадало с отрезком $[0,1]$. Вместо констант 0 и 1 можно использовать бесповторные формулы, функции вероятности которых близки к 0 и 1, соответственно.

Пусть значение $p \in (0,1)$ фиксировано. Бесповторную формулу $\hat{\Phi}$ будем называть 0_ε-*формулой* (соответственно, 1_ε-*формулой*) при данном значении p, если имеет место неравенство $P_1(p|\hat{\Phi}) < \varepsilon$ (соответственно, $P_1(p|\hat{\Phi}) > 1-\varepsilon$).

Результат подстановки 0_ε-формул и 1_ε-формул в другие формулы является, в определённом смысле, близким к результату подстановок констант в те же формулы. Легко проверяется

Лемма 4. *Для любой бесповторной формулы $\hat{\Phi}[x_1,\dots,x_r]$, любого набора значений $\alpha_1,\dots,\alpha_m \in \{0,1\}$, любого $p \in (0,1)$, любого $\varepsilon > 0$ и любых бесповторных формул $\hat{\Psi}_1,\dots,\hat{\Psi}_m$ таких, что каждая $\hat{\Psi}_i$ является $(\alpha_i)_\varepsilon$-формулой, справедливо неравенство*:

$$\left|P_1(p|\hat{\Phi}[\alpha_1,\dots,\alpha_m,x_{m+1},\dots]) - P_1(p|\hat{\Phi}[\hat{\Psi}_1,\dots,\hat{\Psi}_m,x_{m+1},\dots])\right| < m\varepsilon.$$

Обобщим теорему 1.

Теорема 2. *Пусть задан базис B и число $p \in (0,1)$. Множество $W_B(p)$ совпадает с отрезком $[0,1]$ тогда и только тогда, когда $B \not\subseteq L, K, D$ и $0,1 \in W_B(p)$.*

Доказательство. Достаточность. Базис $B \cup \{0,1\}$ удовлетворяет условиям теоремы 1. Следовательно, для любого $x \in [0,1]$ и любого $\varepsilon > 0$ найдётся бесповторная формула $\hat{\Phi}$ над базисом $B \cup \{0,1\}$ такая, что $P_1(p|\hat{\Phi}) \in (x-\varepsilon/2, x+\varepsilon/2)$.

Пусть число вхождений константных функций в формулу $\hat{\Phi}$ равно k. Из условия $0,1 \in W_B(p)$ следует, что для любого $\varepsilon > 0$ над базисом B существует бесповторная $0_{\varepsilon/2k}$-формула и бесповторная $1_{\varepsilon/2k}$-формула. Пусть $\hat{\Phi}_{\varepsilon/2k}$ обозначает формулу, получающуюся из формулы $\hat{\Phi}$ заменой всех константных функций 0 и 1 на $0_{\varepsilon/2k}$- и $1_{\varepsilon/2k}$-формулы, соответственно. По лемме 4, имеет место неравенство $|P_1(p|\hat{\Phi}) - P_1(p|\hat{\Phi}_{\varepsilon/2k})| < \frac{\varepsilon}{2k}k = \frac{\varepsilon}{2}$. Отсюда вытекает, что $P_1(p|\hat{\Phi}) \in (x-\varepsilon, x+\varepsilon)$, и, следовательно, замыкание множества значений функций вероятности совпадает с отрезком $[0,1]$.

Необходимость. Необходимость условия $0,1 \in W_B(p)$ очевидна.

Если B является подмножеством L, K или D, то, как отмечено ранее, $W_B(p)$ не может совпадать с отрезком $[0,1]$. Теорема доказана.

Приведём одно достаточное условие того, что $0,1 \in W_B(p)$ при всех $p \in (0,1)$.

Теорема 3. *Пусть базис B таков, что для каждой точки $p_0 \in (0,1)$ найдётся функция $f \in B$ такая, что $h_f(p_0,\dots,p_0) < p_0$ и функция $g \in B$ такая, что $h_g(p_0,\dots,p_0) > p_0$. Тогда при любом $p \in (0,1)$ множество $W_B(p)$ содержит точки 0 и 1.*

Автор выражает благодарность своему научному руководителю О. М. Касим-Заде за всестороннее внимание к данной работе. Работа выполнена при поддержке РФФИ (проект 05-01-00994), Программы поддержки ведущих научных школ РФ (проект НШ-5400.2006.1) и Программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики» (проект «Синтез и сложность управляющих систем»).

Список литературы

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

2. Колпаков Р. М. О преобразованиях булевых случайных величин // Математические вопросы кибернетики, вып. 9. — М.: Физматлит, 2000. — С. 227–252.

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

4. Moore E. F., Shannon C. Reliable circuits using less reliable relays // J. Franklin Institute. — 1956. — Vol. 262. — P. 191–208. [Имеется перевод: Кибернетич. сб., вып. 1. — М.: ИЛ, 1960. — С. 109–148.]

5. Яблонский С. В. Введение в дискретную математику. — М.: Высш. шк., 2001.

ИНФОРМАЦИЯ

Школы-семинары под общим названием «Синтез и сложность управляющих систем» проводятся, начиная с 1988 года, под руководством академика О. Б. Лупанова. Первая Всесоюзная школа семинар этого цикла была организована во Львове (1988) [1], затем последовали школы-семинары в Новосибирске (1989) [2], Ташкенте (1990), Нижнем Новгороде (1992), Минске (1993) [3], Нижнем Новгороде (1994) [4], Минске (1995) [5], Нижнем Новгороде (1996), снова в Нижнем Новгороде (1998) [6], в Минске (1999) [7], Нижнем Новгороде (2000) [8], Пензе (2001) [9], снова в Пензе (2002) [10], в Нижнем Новгороде (2003) [11] и Новосибирске (2004) [12].

XVI Международная школа-семинар «Синтез и сложность управляющих систем», материалы которой публикуются в данном сборнике, прошла в Санкт-Петербурге с 26 по 30 июня 2006 г. Эта школа-семинар была организована механико-математическим факультетом Московского государственного университета им. М. В. Ломоносова и Научно-исследовательским институтом математики и механики им. акад. В. И. Смирнова Санкт-Петербургского государственного университета.

В работе школы-семинара приняли участие более 50 математиков из Москвы, Санкт-Петербурга, Новосибирска, Нижнего Новгорода, Пензы, Иркутска, Саратова, Ярославля и Смоленска. Был заслушен 41 доклад, большинство из которых представлены в настоящем сборнике. Полный список докладов приводится ниже:

С. И. Аксенов (Пенза). Об асимптотически надежных схемах в базисе отрицание, конъюнкция при инверсных неисправностях на выходах элементов.

М. А. Алехина (Пенза). О функциях и схемах, корректирующих ошибки.

А. С. Балюк, С. В. Балюк (Иркутск). Минимизация термальных представлений булевых функций небольшой размерности в бинарных и тернарных базисах.

Л. Н. Бондаренко (Пенза). Применение "метода вронскианов" для решения комбинаторных задач.

Я. В. Вегнер (Москва). Сложность вычисления экспоненты методом Карацубы.

С. Ф. Винокуров (Иркутск). LP-классификация булевых функций с использованием специальной операторной формы

М. А. Герасимов (Санкт-Петербург). Некоторые признаки линейной зоны емкостной сложности на алгоритмических языках программирования.

А. С. Герасимов (Санкт-Петербург). Программная реализация поиска доказательств в бесконечнозначной предикатной логике, основанной на линейных неравенствах.

О. С. Дудакова (Москва). О конечной порожденности некоторых семейств предполных классов монотонных функций k-значной логики.

Р. Н. Забалуев (Москва). О средней глубине монотонных функций.

В. А. Захаров, В. С. Щербина (Москва). О сложности распознавания эквивалентности машин Тьюринга без записи на ленту.

А. А. Иванов (Санкт-Петербург). Математическое моделирование k-ядерной архитектуры многопроцессорной системы при помощи k-головочной машины Тьюринга с плоской лентой на примере реализации метода Гаусса.

М. А. Иорданский (Нижний Новгород). Индуктивное описание класса планарных графов.

А. Е. Казачёк, Д. С. Романов (Москва). О функциях Шеннона длин локальных тестовпри неисправностях на входах схем.

А. С. Казимиров (Иркутск). Оценка числа инвариантных функций для OP- и LP-преобразований.

Р. М. Колпаков (Москва). Экспоненциальный рост числа трехбуквенных слов с предельным минимальным порядком запретных подслов.

Н. К. Косовский (Санкт-Петербург). Доопределение до всегда завершающих работу любых процедур-операторов, написанных на языке Паскаль.

В. В. Кочергин (Москва). О сложности вычисления элементов в коммутативных полугруппах и группах.

С. Г. Курносова (Саратов). T-неприводимые расширения для симметричных ориентаций цепей.

Ю. М. Лифшиц (Санкт-Петербург). Алгоритмы обработки автоматически-порожденных текстов.

С. А. Ложкин, М. С. Шуплецов (Москва). Оценки высокой степени точности для функции Шеннона в одном классе предикатных схем.

Ю. В. Мерекин (Новосибирск). Об одной форме представления рекуррентных схем порождения слов и их аддитивная сложность.

Е. В. Михайлец (Москва). О ранге неявных представлений функций k-значной логики над классом монотонных функций.

Е. А. Окольнишникова (Новосибирск). О сложности одного класса схем.

Т. Г. Петросян (Москва). Размер максимального множества, свободного от произведений.

В. Н. Потапов (Новосибирск). Описание n-квазигрупп порядка 4.

В. С. Рублев, Д. В. Чехранов (Ярославль). Алгебра объектных операций систем управления данными DIM.

О. Б. Седелев (Москва). О реализации функций алгебры логики BDD, вложенными в единичный куб.

И. С. Сергеев (Москва). О реализации некоторых операций в конечных полях характеристики 2 схемами логарифмической глубины.

С. В. Сидоров (Нижний Новгород). О подобии матриц третьего порядка над кольцом целых чисел.

Д. В. Сперанский (Саратов). Эволюционный подход к проблеме сокращения диагностической информации.

Фам Тхань Лам (Санкт-Петербург). Оценка памяти, необходимой для доопределения до всегда завершающих работу любых процедур-операторов, написанных на языке Паскаль.

Р. В. Хелемендик (Москва). О полной записи шахматных правил на языке конечнозначной логики предикатов.

А. В. Чашкин (Москва). О вложенияи графов в решетки ограниченной высоты.

А. Н. Черепов (Смоленск). Оценки сложности приближения непрерывных функций детерминированными функциями с задержкой.

В. В. Чугунова (Пенза). Об асимптотически наилучших по надежности схемах в некоторых базисах при инверсных неисправностях на входах элементов.

В. В. Чумаков (Нижний Новгород). Вершины целочисленных многогранников и знаменатели решений целочисленных крамеровских систем.

В. И. Шевченко (Нижний Новгород). О сложности тестирования перепутываний в схемах.

В. Н. Шевченко (Нижний Новгород). Триангуляции и монотонные булевы функции.

Л. А. Шоломов (Москва). О последовательной реализации булевых функций.

А. Д. Яшунский (Москва). О вероятностных свойствах бесповторных булевых формул.

На заключительном заседании единогласно было принято решение присвоить серии школ-семинаров «Синтез и сложность управляющих систем» имя академика Олега Борисовича Лупанова — основателя и бессменного руководителя этой серии школ-семинаров.

Список литературы

1. Вісн. АН УРСР [Вестник АН УССР, на укр. языке]. — 1989. — № 3. — С. 104–105.

2. Методы дискретного анализа в изучении булевых функций и графов. Вып. 48. — Новосибирск, 1989. — С. 95–103.

3. Сибирский журнал исследования операций. — 1994. — Т. 1, № 1. — С. 75–84.

4. Дискретный анализ и исследование операций. — 1995. — Т. 2, № 1. — С. 68–81.

5. Материалы VII Межгосударственной школы-семинара «Синтез и сложность управляющих систем» (Минск, 13–16/XI 1995.). — М.: Изд-во механико-математического факультета МГУ, 1996. — 30 с.

6. Материалы IX Межгосударственной школы-семинара «Синтез и сложность управляющих систем» (Нижний Новгород, 16–19 декабря 1998 г.). — М.: Изд-во механико-математического факультета МГУ, 1999. — 100 с.

7. Материалы X Межгосударственной школы-семинара «Синтез и сложность управляющих систем» (Минск, 29 ноября – 3 декабря 1999 г.). — М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2000. — 31 с.

8. Материалы XI Международной школы-семинара «Синтез и сложность управляющих систем» (Нижний Новгород, 20–25 ноября 2000 г.). Части I, II. — М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2001. — 264 с.

9. Материалы XII Межгосударственной школы-семинара «Синтез и сложность управляющих систем» (Пенза, 15–21 октября 2001 г.). Части I, II. — М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2001. — 263 с.

10. Материалы XIII Международной школы-семинара «Синтез и сложность управляющих систем» (Пенза, 14–20 октября 2002 г.). Части I, II. — М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2002. — 216 с.

11. Материалы XIV Международной школы-семинара «Синтез и сложность управляющих систем» (Нижний Новгород, 27 октября – 1 ноября 2003 г.). — Нижний Новгород: Изд-во Нижегородского государственного педагогического университета, 2003. — 132 с.

12. Материалы XV Международной школы-семинара «Синтез и сложность управляющих систем» (Новосибирск, 18–23 октября 2004 г.). — Новосибирск: Изд-во Института математики, 2004. — 118 с.