ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ им. М. В. КЕЛДЫША
РОССИЙСКОЙ АКАДЕМИИ НАУК

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

МАТЕРИАЛЫ VI МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

(Москва, 16–21 апреля 2007 г.)

ЧАСТЬ I

Москва 2007

МАТЕРИАЛЫ
VI МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

(Москва, 16–21 апреля 2007 г.)

ЧАСТЬ I

Москва 2007

М34
УДК 519.7

Издание осуществлено при поддержке Российского фонда фундаментальных исследований по проекту 07–01–06018

М34 Материалы VI молодежной научной школы по дискретной математике и ее приложениям (Москва, 16–21 апреля 2007 г.). Часть I. Под редакцией А. В. Чашкина. 2007. — 56 с.

Сборник содержит материалы VI молодежной научной школы по дискретной математике и ее приложениям, проходившей в Москве с 16 по 21 апреля 2007 г. при поддержке Российского фонда фундаментальных исследований (проект 07–01–06018). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание
МАТЕРИАЛЫ
VI МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ
(Москва, 16–21 апреля 2007 г.)

Под общей редакцией А. В. ЧАШКИНА

Ответственный за выпуск *Ф. М. Ковалев*

СОДЕРЖАНИЕ

О НЕКОТОРЫХ КРИПТОГРАФИЧЕСКИХ СВОЙСТВАХ МНОЖЕСТВА ЧЕТНЫХ ФУНКЦИЙ

Е. К. Алексеев (Москва)

1. Введение

В последние годы обозначился существенный интерес к вопросам синтеза и анализа потоковых шифров. Корреляционно-иммунные функции являются важным строительным блоком при синтезе этого класса шифров. Эти функции являются хорошо известным объектом в таких разделах математики как комбинаторный анализ и терия кодирования.

В данной работе рассматривается множество четных функций. Доказываются некоторые утверждения, которые показывают важность этого класса функций при изучении множества корреляционно-иммунных булевых функций в целом. Приводятся некоторые комбинаторные следствия.

2. Основные понятия и определения

Пусть $F_2 = GF(2)$, $V_n = F_2^n$ — векторное пространство наборов длины n с компонентами из поля F_2. Пусть $\mathcal{F}_n = \{f | f : V_n \to F_2\}$ — множество булевых функций от n переменных.

Определение. *Преобразованием Фурье булевой функции $f \in \mathcal{F}_n$ называется целочисленная функция на V_n, определяемая следующим равенством*

$$F_f(u) = \sum_{x \in V_n} f(x)(-1)^{<x,u>}$$

(суммирование производится в действительной области). Для каждого $u \in V_n$ значение $F_f(u)$ называется коэффициентом Фурье.

Определение. *Преобразованием Уолша–Адамара булевой функции $f \in \mathcal{F}_n$ называется целочисленная функция на V_n, определяемая следующим равенством*

$$W_f(u) = \sum_{x \in V_n} (-1)^{f(x) \oplus <x,u>}$$

(суммирование производится в действительной области). Для каждого $u \in V_n$ значение $W_f(u)$ называется коэффициентом Уолша–Адамара.

Определение. *Булева функция $f(x^{(1)}, x^{(2)}, \ldots, x^{(n)}) \in \mathcal{F}_n$ называется корреляционно-иммунной порядка $m, 0 < m \leq n$, если для любых наборов $1 \leq i_1 < i_2 < \cdots < i_m \leq n, a^{(i)} \in F_2, j = 1, \ldots, m$, выполняются соотношения $wt(f_{i_1,\ldots,i_m}^{a^{(1)},\ldots,a^{(m)}}) = \frac{wt(f)}{2^m}$.*

Определение. *Порядком корреляционной иммунности называется число* $corf = max\{m \in \mathbb{N} | f - корреляционно\text{-}иммунна\ порядка\ n\}$.

Существует критерий того, что функция корреляционно-иммунна порядка m (см. [1]).

Теорема 1. *Булева функция* $f \in \mathcal{F}_n$ *корреляционно-иммунна порядка* m *тогда и только тогда, когда* $W_f(u) = 0$ *для всех векторов* $u \in V_n$ *таких, что* $1 \leq wt(u) \leq m$.

Определение. $CI(n) = \{f \in \mathcal{F}_n | corf \geq 1\}$

Определение. *Булева функция* $f \in \mathcal{F}_n$ *называется четной, если для любого вектора* $x \in V_n$ *выполняется* $f(x) = f(x \oplus \overline{1})$. *Обозначим множество всех четных функций через* $Mir(n)$.

3. Криптографические свойства множества четных функций

Утверждение 1. $Mir(n)$ *является линейным подпространством пространства* V_{2^n} *размерности* 2^{n-1}.

Доказательство непосредственно следует из определения.

Утверждение 2. *Для любой* $f \in Mir(n)$ *справедливы равенства* $W_f(u) = 0$, *если* $wt(u) = 2k + 1, k \geq 0$.

Доказательство. Так как $W_f(u) = 0 \iff F_f(u) = 0$ при $u \neq 0$, то рассмотрим коэффициенты Фурье $F_f(u)$ функции f:

$$
\begin{aligned}
F_f(u) &= \sum_{x \in V_n} f(x)(-1)^{<x,u>} = \sum_{x \in V_n : f(x)=1} (-1)^{<x,u>} = \\
&= \sum_{x \in V_n : x_1 = 1 \& f(x)=1} (-1)^{<x,u>} + \sum_{x \in V_n : x_1 = 0 \& f(x)=1} (-1)^{<x,u>} = \\
&= \sum_{x \in V_n : x_1 = 1 \& f(x)=1} ((-1)^{<x,u>} + (-1)^{<x \oplus \overline{1},u>}) = \\
&= \sum_{x \in V_n : x_1 = 1 \& f(x)=1} (-1)^{<x,u>}(1 + (-1)^{<\overline{1},u>}) = 0.
\end{aligned}
$$

Последнее равенство справедливо, т. к. $< \overline{1}, u >= 1$ при нечетном $wt(u)$.

Следствие 1. *Любая четная функция является корреляционно-иммунной как минимум первого порядка.*

Доказательство. Для того, чтобы функция f была корреляционно-иммунной как минимум первого порядка необходимо и достаточно, чтобы $W_f(u) = 0$ при всех $u : wt(u) = 1$. Из утверждения 1 следует, что такое соотношение выполнено для любой четной функции.

В работе [2] представлена асимптотическая формула для числа корреляционно-иммунных порядка k булевых функций. Из утверждения 2 следует конструктивная нижняя оценка для мощности множества корреляционно-иммунных функций как минимум первого порядка.

Следствие 2. *Для мощности множества $CI(n)$ выполнено неравенство $\#CI(n) \geq 2^{2^{n-1}}$.*

Доказательство. $\#CI(n) \geq \#Mir(n) = 2^{2^{n-1}}$.

Следствие 3. *Для любой функции $f \in Mir(n)$ и $f \neq const$ справедливо соотношение $cor(f) = 2k + 1$, для $k \geq 0$.*

Доказательство. Если $cor(f) = n$, то $f \equiv const$. Поэтому, из условий следствия следует, что $cor(f) < n$. Докажем, что $cor(f)$ не может быть четным числом. Предположим, что существует $f \in Mir(n)$ такая, что $cor(f) = 2m$ для некоторого $m \geq 1$. Из теоремы 1 следует, что $W_f(u) = 0$ для всех $u : 1 \leq wt(u) \leq 2m$. Из утверждения 2 следует, что $W_f(u) = 0$ при $wt(u) = 2m+1$. Из теоремы 1 и определения получаем, что $cor(f) = 2m+1$. Полученное противоречие доказывает утверждение.

Для функции $f \in \mathcal{F}_n$ обозначим через 1_f следующее множество

$$1_f = \{x \in V_n | f(x) = 1\}.$$

Утверждение 3. *Пусть f — произвольная четная функция. Если для подфункции f_1^0 справедливо неравенство $cor(f_1^0) \geq 2k$, то справедливо неравенство $cor(f) \geq 2k + 1$.*

Доказательство. Из утверждения 2 следует, что справедливо следующее условие. Функция $f \in Mir(n)$ является корреляционно-иммунной порядка $2k + 1$, если $F_f(u) = 0$ для любого $u : 1 \leq wt(u) \leq 2k$. Для любой четной функции f и для любого набора $u : wt(u) = 2m$, где $1 \leq m \leq k$, справедливо следующее соотношение:

$$F_f(u) = \sum_{x \in 1_f} (-1)^{<u,x>} = \sum_{x \in 1_f \& x_0 = 0} (-1)^{<u,x>} + \sum_{x \in 1_f \& x_0 = 1} (-1)^{<u,x>} =$$

$$\sum_{x \in 1_f \& x_0 = 0} (-1)^{<u,x>} \cdot (1 + (-1)^{<u,\overline{1}>}) = 2 \cdot F_{f_1^0}(\widetilde{u}), \text{ где } \widetilde{u} = (0, u_1, \ldots, u_{n-1}).$$

Условие $F_f(u) = 0$ для любого $u : wt(u) = 2k$ эквивалентно условию $F_{f_1^0}(\widetilde{u}) = 0$ для любых $\widetilde{u}$ таких, что $2k \leq wt(\widetilde{u}) \leq 2k+1$. Следовательно, $F_f(u) = 0$ для любых наборов четного веса w, где $w \leq 2k$. Для наборов нечетного веса меньшего $2k+1$ равенство нулю коэффициентов $F_f(u)$ следует из утверждения 2.

Список литературы

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

2. Денисов О. В. Асимптотическая формула для числа корреляционно-иммунных порядка k булевых функций //Дискретная математика. — 1991. — Т. 3, вып. 2. — С. 25—47.

ЭФФЕКТИВНАЯ ПРОВЕРКА НИЖНЕЙ ГРАНИЦЫ АЛГЕБРАИЧЕСКОЙ ИММУННОСТИ МНОГОЧЛЕНА ЖЕГАЛКИНА И ДНФ

В. В. Баев (Москва)

Для булевой функции f значение алгебраической иммунности $AI(f)$ равно минимальному значению числа d, для которого существует ненулевая булева функция g степени $\leqslant d$ такая, что $fg = 0$ или $(f+1)g = 0$. Если $fg = 0$, то g называется аннигилятором функции f. Иногда достаточно найти только значение $AI(f)$. А бывает так, что нужно найти все аннигиляторы наименьшей степени функции f. В последнее время были разработаны различные алгоритмы поиска аннигиляторов. Сложность этих алгоритмов зависит от способа представления функции f.

В работах [6] и [5] функция f задаётся таблицей значений на всех булевых векторах. В [3] функция f задаётся многочленом Жегалкина, в [2] — трэйс представлением, а в [1] — дизъюнктивной нормальной формой и формулой в операциях $\&, \vee, \neg$.

В данной работе представлено 3 алгоритма. Они являются адаптациями алгоритмов из [5] для других представлений функции f. Первым двум алгоритмам на вход подаётся число d и многочлен Жегалкина от n переменных. 3-му алгоритму вместо многочлена Жегалкина подаётся ДНФ.

Введём необходимые обозначения. $\mathbb{F}_2$ — поле из двух элементов. $\mathcal{F}_n$ — множество всех булевых функций $\mathbb{F}_2^n \to \mathbb{F}_2$. $\deg f$ — степень многочлена Жегалкина булевой функции f. $A_d^n(f) := \{g \in \mathcal{F}_n \mid fg = 0,\ \deg g \leqslant d\}$. M_f

— количество мономов в многочлене Жегалкина функции f. Для $x, u \in \mathbb{F}_2^n$ обозначим $x^u := \prod_{i:u_i=1} x_i$ — моном Жегалкина.

1-й алгоритм пытается проверить, есть ли в линейном пространстве $A_d^n(f)$ ненулевые функции. Алгоритм основан на разложении многочлена Жегалкина функции f по последней переменной:

$$f(x_1, ..., x_n) = u(x_1, ..., x_{n-1}) + x_n v(x_1, ..., x_{n-1}). \tag{1}$$

Если существует $g \in A_d^n(f) \backslash 0$, то рассмотрим разложение

$$g(x_1, ..., x_n) = u'(x_1, ..., x_{n-1}) + x_n v'(x_1, ..., x_{n-1}),$$

где $\deg u' \leqslant d$, $\deg v' \leqslant d-1$ и u', v' не равны нулю одновременно. Из уравнения

$$(u + x_n v)(u' + x_n v') = 0$$

получим, что если $u' \neq 0$, то $u' \in A_d^{n-1}(u) \backslash 0$, а если $u' = 0$, то $v' \in A_{d-1}^{n-1}(u + v) \backslash 0$. Итого мы получили такое необходимое условие:

$$\exists g \in A_d^n(f) \backslash 0 \quad \Rightarrow \quad (\exists u' \in A_d^{n-1}(u) \backslash 0 \text{ или } \exists v' \in A_{d-1}^{n-1}(u+v) \backslash 0),$$

что равносильно

$$(A_d^{n-1}(u) = 0 \ \text{ и } \ A_{d-1}^{n-1}(u+v) = 0) \quad \Rightarrow \quad A_d^n(f) = 0. \tag{2}$$

Проверку $A_d^{n-1}(u) = 0$ и $A_{d-1}^{n-1}(u+v) = 0$ мы выполним рекурсивно, разложив многочлены Жегалкина функций u и $u+v$ по переменной x_{n-1}. В общем случае в вершине (n', d', f') дерева рекурсии мы имеем многочлен Жегалкина f' от n' переменных, для которого проверяем тривиальность пространства $A_{d'}^{n'}(f')$. На этом шаге рекурсии мы производим разложение многочлена $f' = u' + x_{n'} \cdot v'$. Это потребует $O(M_{f'}) = O(M_f)$ операций. Рекурсию продолжаем, пока n' больше некоторого числа m, и $d' \neq 0$. Далее считаем d константой в асимптотических оценках $O(...)$.

В листьях (m, d', f') дерева рекурсии воспользуемся алгоритмом вычисления базиса линейного пространства $A_{d'}^m(f')$ из [3]. Его сложность — $O(M_{f'} \cdot m^{3d'})$. В листьях $(n', 0, f')$ нам нужно проверить $A_0^{n'}(f') \stackrel{?}{=} 0$. $A_0^{n'}(f') = 0$ тогда и только тогда, когда $f' \neq 0$. Проверить, что многочлен Жегалкина f' является ненулевым можно за $O(1)$ операций.

Если во всех листьях получилось $A_{d'}^{n'}(f') = 0$, значит мы доказали, используя импликацию (2), что $A_d^n(f) = 0$. В этом случае алгоритм выдаёт "f не имеет ненулевых аннигиляторов степени $\leqslant d$". В противном случае алгоритм выдаёт "не удалось доказать, что $A_d^n(f) = 0$".

Утверждение 1. *В полученном дереве рекурсии ровно* $\sum_{k=1}^{d}\binom{n-m}{k}$ *внутренних вершин,* $\binom{n-m}{d-d'}$ *листьев с* m *переменными и ненулевым числом* d'*, а также* $\binom{n-m}{d}$ *листьев с* $d'=0$*.*

Общая сложность C алгоритма складывается из разложений $f' = u' + x_{n'}\cdot v'$ в каждой внутренней вершине дерева рекурсии и из вычисления $A^{n'}_{d'}(f')$ в каждом листе. Если положить $m = O(\log n)$, то, используя утверждение 1, получим

$$C = O(M_f)\cdot\sum_{k=1}^{d}\binom{n-m}{k} + O(1)\cdot\binom{n-m}{d} + \\ + \sum_{d'=1}^{d}\binom{n-m}{d-d'}\cdot O(M_f\cdot m^{3d'}) = \qquad (3)$$

$$= O(M_f\cdot n^d) + \sum_{d'=1}^{d} n^{d-d'}\cdot O(M_f\cdot(\log n)^{3d'}) = O(M_f\cdot n^d).$$

Для сравнения: в [5] показано, что средняя сложность аналогичного алгоритма для табличного представления функции f есть $O(n^d)$. Сложность там усредняется по всем уравновешенным функциям от n переменных, в то время как в изложенном выше алгоритме сложность оценивается для каждой функции в отдельности. В [5] также доказано, что при $m = \lceil\log_2 n\rceil + 2d + 1$ доля уравновешенных функций f, для которых наш алгоритм выдаёт ответ "не удалось доказать, что $A^n_d(f) = 0$", мала.

2-й алгоритм решает более общую задачу. Он находит базис пространства $A^n_d(f)$. Верхняя оценка его сложности есть $O(M_f\cdot n^{3d})$. Она совпадает с оценкой для известного ранее алгоритма, [3]. Оба этих алгоритма решают одну и ту же систему линейных однородных уравнений методом Гаусса. Новый алгоритм отличается от старого тем, что явно указывает удобный порядок уравнений и переменных, и тем, что в процессе решения отбрасывает некоторые линейно зависимые уравнения.

Многочлены Жегалкина функций f и $g \in A^n_d(f)$:

$$f(x) = \sum_{u\in\mathcal{M}_f} x^u, \quad g(x) = \sum_{v\in\mathbb{F}_2^n\,:\,wt(v)\leqslant d} b_v x^v,$$

где $\mathcal{M}_f \subset \mathbb{F}_2^n$, а $b_v \in \mathbb{F}_2$ — неопределённые коэффициенты, относительно

которых составим систему уравнений. Имеем

$$f(x)g(x) = \sum_{u\in\mathcal{M}_f} x^u \sum_{\substack{v\in\mathbb{F}_2^n:\\ wt(v)\leqslant d}} b_v x^v =$$

$$= \sum_{u\in\mathcal{M}_f} \sum_{\substack{v\in\mathbb{F}_2^n:\\ wt(v)\leqslant d}} b_v x^{u\vee v} = \sum_{w\in\mathcal{M}} \left(\sum_{v\in\mathcal{N}_w} b_v\right) x^w = 0 \qquad (4)$$

$$\Leftrightarrow \quad \left\{ \sum_{v\in\mathcal{N}_w} b_v = 0, \text{ для каждого } w\in\mathcal{M}. \right.$$

В [3] явно выписаны множества $\mathcal{M}$ и $\mathcal{N}_w$.

Утверждение 2. *Для любого $w\in\mathcal{M}$ и для любого $v\in\mathcal{N}_w$ выполнено $v\preccurlyeq w$, где "$\preccurlyeq$" — стандартное отношение частичного порядка в $\mathbb{F}_2^n$ (каждая компонента вектора v не превосходит соответствующей компоненты вектора w).*

Утверждение 2 выявляет ключевое свойство системы (4), позволяющее адаптировать алгоритм 2 из [5] для решения этой системы. Новый алгоритм пошагово находит базис решения, добавляя по очереди новые уравнения. Если на очередном шаге получается "вырожденное" решение, то оказывается, что за счёт структуры системы можно отбросить уравнения для некоторых $w\in\mathcal{M}$, никак не анализируя соответствующие им множества $\mathcal{N}_w$.

3-й алгоритм является модификацией 1-го алгоритма для представления функции f в виде ДНФ. Пусть множество пар векторов $\mathcal{D}_f\subset\mathbb{F}_2^n\times\mathbb{F}_2^n$ задаёт ДНФ:

$$f(x) = \bigvee_{(\sigma,\alpha)\in\mathcal{D}_f} (x+\sigma)^\alpha.$$

Разложим её по переменной x_n.

$$f(x) = \overbrace{\bigvee_{\substack{(\sigma,\alpha)\in\mathcal{D}_f:\\ \alpha_n=0}} (x+\sigma)^\alpha}^{w(x_1,\ldots,x_{n-1})} \vee \overbrace{\bigvee_{\substack{(\sigma,\alpha)\in\mathcal{D}_f:\\ \alpha_n=1,\\ \sigma_n=1}} (x+\sigma)^\alpha}^{u(x_1,\ldots,x_{n-1})(x_n+1)} \vee \overbrace{\bigvee_{\substack{(\sigma,\alpha)\in\mathcal{D}_f:\\ \alpha_n=1,\\ \sigma_n=0}} (x+\sigma)^\alpha}^{v(x_1,\ldots,x_{n-1})x_n} =$$

$$= (w\vee u)(x_n+1)\vee(w\vee v)x_n = (w\vee u)(x_n+1) + (w\vee v)x_n. \qquad (5)$$

Теперь мы можем действовать так же, как для многочлена Жегалкина. Будем использовать разложение (5) вместо (1). Аналогично импликации (2) получим

$$(A_d^{n-1}(w\vee u) = 0 \ \text{ и } \ A_{d-1}^{n-1}(w\vee v) = 0) \quad \Rightarrow \quad A_d^n(f) = 0.$$

Для разложения (5) нужно $O(|\mathcal{D}_f|)$ операций. Используем то же самое дерево рекурсии. В его листьях (m, d', f') воспользуемся алгоритмом вычисления базиса линейного пространства $A^m_{d'}(f')$ из [1]. Его сложность — $O(|\mathcal{D}_f| \cdot m^{3d'})$. По аналогии с (3) получаем оценку общей сложности 3-го алгоритма:

$$C_{\text{ДНФ}} = O(|\mathcal{D}_f| \cdot n^d).$$

Работа выполнена при частичной финансовой поддержке РФФИ, проект номер 07-01-00154.

Список литературы

1. Баев В. В. О сложности поиска аннигиляторов низкой степени для булевых функций, Материалы международной научной конференции по проблемам безопасности и противодействия терроризму. Интеллектуальный Центр МГУ. 2–3 ноября 2005 г. — М: МЦНМО, 2006. стр. 198–204.

2. Баев В. В. Некоторые нижние оценки на алгебраическую иммунность функций, заданных своими трэйс формами, Дискретные модели в теории управляющих систем: VII Международная конференция, Покровское, 4–6 марта 2006 г.: Труды. — М.: МАКС Пресс, 2006. стр. 25–29.

3. Баев В. В. О некоторых алгоритмах построения аннигиляторов низкой степени для булевых функций, Дискретная математика, том 18, выпуск 3, 2006. стр. 138–151.

4. Courtois N., Meier W. Algebraic Attacks on Stream Ciphers with Linear Feedback, Eurocrypt 2003, LNCS 2656, pp. 345–359, Springer, 2003.

5. Didier F., Tillich J.-P. Computing the Algebraic Immunity Efficiently, FSE 2006, LNCS 4047, pp. 359–374, Springer, 2006.

6. Meier W., Pasalic, E., Carlet C. Algebraic Attacks and Decomposition of Boolean Functions, Eurocrypt 2004, LNCS 3027, pp. 474–491, Springer, 2004.

О БУЛЕВЫХ СХЕМАХ УМНОЖЕНИЯ В КОНЕЧНЫХ ПОЛЯХ НЕЧЕТНОЙ ХАРАКТЕРИСТИКИ

А. А. Бурцев (Москва)

Для некоторых криптографических приложений (например, [1-9]) необходимо реализовать арифметику в полях $k = GF(p^n)$ и $K = GF(p^{2pn})$. В случае $p = 3$ это сделано в [2-5]. В [6] описан метод построения арифметики в этих полях при любом простом $p \equiv 3 \pmod 4$. Из этого описания следует, что с ростом p сложность схемной реализации умножения в поле $GF(p^{2pn})$ уменьшается (при условии, что n изменятся так, что порядок поля существенно не меняется). В [6] также показано, что с ростом p битовая сложность криптоалгоритма [1, 8, 9] уменьшается (при сохранении того же уровня надежности). Поэтому представляется более эффективным использовать этот алгоритм при $p = 7$. Предлагаемая в настоящей работе реализация арифметики в этом случае может также найти применение и в алгоритмах из [7].

Под схемной реализацией понимается реализация операций булевыми (не автоматными) схемами, а под сложностью — число базисных элементов, составляющих схему (базис состоит из двуместных булевых функций $\&, \vee, \oplus$ и их отрицаний). Понятие схемной сложности по существу совпадает с понятием битовой сложности. Глубина схемы есть длина самой длинной цепи элементов, соединяющей входы и выходы схемы [14].

Пусть $M(G)$ — схемная сложность умножения в конечном поле G, $A(G)$ — сложность сложения в поле G, $A(p)$ — сложность сложения в поле $GF(p)$, $M(p)$ — сложность умножения в поле $GF(p)$, $D(M(G))$ — глубина схемы умножения в поле G, $D(A(G))$ — глубина схемы сложения в поле G, $GF(q)$ — конечное поле порядка q, n — произвольное натуральное число, p — простое.

Теорема 1. *Умножение в поле $GF(p^{2pn})$ имеет оценку сложности*

$$M(GF(p^{2pn})) \le (6p-3)M(GF(p^n)) + (18p^2 - 23p + 7)nM(p) +$$

$$+(24p^2 - 32p + 8)nA(p).$$

Замечание. Указанную оценку можно переписать в виде

$$M(GF(p^{2pn})) \le (6p-3)M(GF(p^n)) + O(p^2 n \log p \log\log p \log\log\log p),$$

так как для оценки $M(p)$ можно использовать метод Шенхаге-Штрассена.

Теорема 2. *Умножение элементов поля* $GF(7^{14n})$ *может быть выполнено схемой сложности*

$$M(GF(7^{14n})) \le 13M(GF(7^{2n})) + 258nA(7)$$

и глубины

$$D(M(GF(7^{14n}))) \le 11D(A(7)) + D(M(GF(7^{2n}))).$$

В частности,

$$M(GF(7^{14\cdot 31})) \le 698\ 554.$$

Для доказательства и применения этой и остальных теорем полезны следующие леммы.

Лемма 1. *Умножение в* $GF(7)$ *выполняется схемой сложности* 25 *и глубины* 5.

Лемма 2. *Сложение в* $GF(7)$ *выполняется схемой сложности* 17 *и глубины* 7. *Существует также схема для сложения сложности* 18 *и глубины* 6.

Лемма 3. *Сложение в* $GF(7)$ *может быть выполнено схемой сложности* 21 *и глубины* 4.

Для реализации криптоалгоритма [1, 8, 9] полезна

Теорема 3. *Умножение в поле* $GF(7^{14n})$ *элемента* f, *представимого многочленом степени* 6, *на элемент* g, *представимый многочленом степени* 4 *с единичным старшим коэффициентом имеет сложность не выше*

$$10M(GF(7^{2n})) + 176nA(7).$$

Глубина схемы равна $13D(A(7)) + D(M(GF(7^{2n})))$.

В частности, при $n = 31$ *указанная сложность не выше* 557 392, *а глубина схемы равна* $31D(A(7)) + D(M(7))$.

Пусть $M(n)$ — сложность умножения многочленов степени $n-1$ над $GF(7^2)$. Справедливы следующие асимптотические оценки.

Теорема 4.

$$M(n) \lesssim \left(\frac{12443}{8}\right) n^{\log_5 7}$$

при $n = 25^s$, *и*

$$M(n) \lesssim \left(\frac{609707}{8}\right) n^{\log_5 7}$$

в случае произвольного n.

Пусть $M_o(n)$ обозначает сложность умножения многочленов n-й степени над $GF(7^2)$, $M_o(n \times m)$ — сложность умножения многочленов степени n и m над $GF(7^2)$, $M(7^2)$ — сложность умножения в поле $GF(7^2)$, $A(7^2)$ - сложность сложения в этом поле; $A(7^2) = 2A(7)$. В правой колонке следующей таблицы указано условное название наилучшего алгоритма умножения (при поиске такого алгоритма рассматривались, кроме стандартного, методы Тоома, Карацубы [10–12], метод, основанный на применении ДПФ [10, 13], а также их композиции и модификации).

$M_o(0) \le$	$M(7^2)$			$=$	138	
$M_o(1) \le$	$3M(7^2)$	$+$	$4A(7^2)$	$=$	550	Карацуба
$M_o(2) \le$	$6M(7^2)$	$+$	$12A(7^2)$	$=$	1 236	ДПФ
$M_o(3) \le$	$8M(7^2)$	$+$	$28A(7^2)$	$=$	2 056	ДПФ
$M_o(4) \le$	$12M(7^2)$	$+$	$38A(7^2)$	$=$	2 948	ДПФ
$M_o(5) \le$	$12M(7^2)$	$+$	$74A(7^2)$	$=$	4 172	ДПФ
$M_o(6) \le$	$16M(7^2)$	$+$	$86A(7^2)$	$=$	5 132	ДПФ
$M_o(7) \le$	$22M(7^2)$	$+$	$100A(7^2)$	$=$	6 436	ДПФ
$M_o(8) \le$	$20M(7^2)$	$+$	$154A(7^2)$	$=$	7 996	ДПФ
$M_o(11) \le$	$30M(7^2)$	$+$	$228A(7^2)$	$=$	11 892	ДПФ
$M_o(12) \le$	$37M(7^2)$	$+$	$246A(7^2)$	$=$	13 470	ДПФ
$M_o(6 \times 3) \le$	$10M(7^2)$	$+$	$67A(7^2)$	$=$	3 658	ДПФ
$M_o(6 \times 4) \le$	$10M(7^2)$	$+$	$73A(7^2)$	$=$	3 862	ДПФ
$M_o(15) \le$	$38M(7^2)$	$+$	$369A(7^2)$	$=$	17 790	ДПФ
$M_o(22) \le$	$66M(7^2)$	$+$	$605A(7^2)$	$=$	29 678	ДПФ
$M_o(23) \le$	$76M(7^2)$	$+$	$637A(7^2)$	$=$	32 146	ДПФ
$M_o(24) \le$	$49M(7^2)$	$+$	$817A(7^2)$	$=$	34 540	ДПФ
$M_o(25) \le$	$52M(7^2)$	$+$	$826A(7^2)$	$=$	35 260	ДПФ
$M_o(30) \le$	$82M(7^2)$	$+$	$940A(7^2)$	$=$	43 276	ДПФ
$M_o(31) \le$	$92M(7^2)$	$+$	$972A(7^2)$	$=$	45 744	ДПФ

Можно получить оценку сложности умножения многочленов 49-й степени

$$M_o(49) \le 94\,984, \quad \text{ДПФ},$$

и оценку сложности умножения многочленов 47-й степени

$$M_o(47) \le 95\,826, \quad \text{ДПФ}.$$

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

Работа выполнена при частичной поддержке грантов РФФИ 05-01-0099, НШ 5400.2006.1, ОМН РАН (проект «Оптимальный синтез управляющих систем»).

Список литературы

1. Kwon S. Efficient Tate pairing computation for supersingular elliptic curves over binary fields. Cryptology ePrint Archive, Report 2004/303. http://eprint.iacr.org/2004/303.

2. Scott M. and Barreto P.S.M.L. Compressed pairing. CRYPTO-2004, LNCS 3152(2004), 140-156.

3. Kerins T., Marname W. P., Popovici E. M., and Barreto P.S.L.M. Efficient hardware for Tate pairing calculation in characteristic three. CHES-2005.

4. Page D., Smart N. P. Hardware implementation of finite fields of characteristic three, CHES-2002, LNCS, 2002.

5. Granger R., Page D., Stam M. Hardware and software normal basis arithmetic for pairing based cryptography in characteristic three. IEEE Trans. on Comp. v.54, No 7 (2005), 852–860.

6. Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А. Элементарное введение в эллиптическую криптографию: протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006.

7. Eunjeong Lee, Huang-Sook Lee and Yoonjin Lee. Fast computation of Tate pairing on general divisors for hyperelliptic curves of genus 3. Cryptology ePrint Archive, Report 2006/125. http://eprint.iacr.org/2006/125

8. Duursma I. and Lee H.-S. Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$. Asiacrypt-2003, LNCS 2894(2003), 111-123.

9. Duursma I. and Lee H.-S. Tate pairing implementation for tripartite key agreement. Cryptology ePrint Archive, Report 2003/053. http://eprint.iacr.org/2003/053

10. Кнут Д. Искусство программирования, т.2 2-е изд., 2000.

11. Карацуба А. А., Офман Ю. П. Умножение многозначных чисел на автоматах. // ДАН СССР. — 1962. — Т. 145(2). — С. 293–294.

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

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

14. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. Изд. МГУ, Москва, 1984.

ГЛУБИНА ПРИБЛИЖЕННОГО ВЫЧИСЛЕНИЯ ГЛАДКИХ ФУНКЦИЙ

Я. В. Вегнер (Москва)

Рассматривается способ построения схем из функциональных элементов, приближённо вычисляющих гладкие функции в двоичном виде. Фиксируем фунцкию $f(x)$ и отрезок $[a, b]$. Основной результат формулируется так.

Теорема 1. *Для произвольной 4 раза дифференцируемой на отрезке $[a, b]$ функции $f(X)$ и произвольного $n \in \mathbf{N}$ в базисе из всех двухвходовых функций можно построить схему из функциональных элементов S_n, приближённо вычисляющую функцию f. Определяются параметры s, S, s_0, s_1, s_2, s_3, A, B, зависящие только от функции f и отрезка $[a, b]$, и параметры $E = 4n + A - 4$, $N = 4n + B$. Схема требует $s + N$ битов входного числа*

$$X = x_{-s+1} \dots x_0, x_1 \dots x_N,$$

и выдаёт $S + E$ битов результата

$$f(X) = f_{-S+1} \dots f_0, f_1 \dots f_E.$$

Функция f вычислена с погрешностью не более 2^{-E}. Если выполнены условия $A + s_2 \geq 0$, $\sqrt{2}A \geq s_1$, то глубина схемы не превосходит

$$D \leq (n + s) + 4\lceil \log(E + 5 - 2n + s_2) \rceil + 4\lceil \log(E + 4 - 2n + s_2) \rceil +$$

$$+ 25 + 2\lceil \log(N + S) \rceil.$$

1. Приближение функции многочленом

Разобьём отрезок $[a, b]$ на отрезки вида $[m2^{-n},\ (m + 1)2^{-n}]$. На каждом таком отрезке будем приближать фунцкию $f(X)$ многочленом третьей степени:

$$f(X) \approx p_3(x, y) = a_0(x) + a_1(x)y + a_2(x)y^2 + a_3(x)y^3,$$

где

$$X = x_{-s+1} \dots x_0, x_1 \dots x_N, \quad x = x_{-s+1} \dots x_0, x_1 \dots x_n,$$

$$y = 0, 0 \dots 0 x_{n+1} \dots x_N, \quad Y = 0, x_{n+1} \dots x_N \in [0, 1),$$

$\delta = 2^{-n}$, $y = \delta Y$. Потребуем, чтобы на каждом отрезке $[x, x+\delta]$ многочлен $p_3(x, y)$ интерполировал функцию f в заданных точках $x + U_i\delta$,

$$U_i = \frac{1}{2} + \frac{1}{2}\cos\frac{2i+1}{2\cdot 3+2}\pi,\ i = 0, \ldots, 3,$$

$i = 0, \ldots, 3$. Тогда $p_3(x, y)$ совпадает со смещённым многочленом Чебышёва, и погрешность приближения можно оценить как

$$\|f - p_3\|_{C[x,x+\delta]} \le \frac{\delta^4}{128}\frac{\|f^{(4)}\|_{C[x,x+\delta]}}{4!}.$$

2. Глубина арифметических операций

Сложение двух n-значных чисел можно реализовать схемой глубины $2\lceil\log_2 n\rceil + 2$ [1].

Теорема 2. *Для любого натурального n в базисе из всех двухвходовых функций можно построить схему $S(n, 2)$, преобразующую n двоичных чисел любой длины в два числа с такой же суммой, с глубиной $4\lceil\log_2 n\rceil + 1$.*

Доказательство проводится индукцией по n с использованием явного вида схемы $S(3, 2)$.

Следствие 1. *Пусть заданы два числа, имеющих в двоичной записи n знаков. Можно построить схему глубины $4\lceil\log n\rceil + 2$, вычисляющую по ним два числа, сумма которых равна произведению исходных чисел.*

Доказательство. С глубиной 1 можно вычислить все попарные произведения битов исходных чисел. Получится n чисел, имеющих в двоичной записи n знаков. Чтобы получить произведение исходных чисел, нужно сложить полученные числа с правильными сдвигами. Используем компрессор $S(n, 2)$, чтобы получить два числа, удовлетворяющих утверждению теоремы.

Лемма 1. (*Вычитание*) *Пусть требуется сложить m чисел $p_1, \ldots p_m$, причём*

$$p_1 < 0, \ldots, p_l < 0, \quad p_{l+1} \ge 0, \ldots, p_m \ge 0,$$

и все числа имеют s знаков до запятой и t знаков после запятой. Если заменить числа $p_1, \ldots, p_l$ побитовыми отрицаниями чисел $|p_i|$ и добавить к сумме число $l2^{-t}$, то сумма увеличится на $l2^s$, так что s битов суммы до запятой и все биты после запятой при этом не изменятся.

Теорема 3. (*Умножение с заданной точностью*) *Пусть заданы числа $\alpha, \beta > 0$, имеющие в двоичной записи соответственно a и b знаков после*

запятой и p и q знаков до запятой; и пусть задано такое число k, что $a \geq q + k + 1$, $b \geq p + k + 1$. Тогда можно построить схему $M(a, b, p, q, k)$, вычисляющую два числа c и d, сумма которых приближает произведение $\alpha\beta$ с погрешностью, меньшей 2^{-k}, причём глубина схемы $M(a, b, p, q, k)$ оценивается как

$$D(M(a, b, p, q, k)) \leq 4\lceil \log(p + q + k + 1) \rceil + 2.$$

3. Построение схемы

По набору $x = (x_{-s+1}, \ldots, x_0, x_1, \ldots, x_n)$ схема находит все коэффициенты $a_i(x)$, $i = 0, 1, 2, 3$ вместе с битом знака b_i, равным 1, если $a_i < 0$.

Схема строится по формуле

$$p_3(x, y) = a_0 + a_1 Y 2^{-n} + a_2 Y^2 2^{-2n} + (a_3 Y) Y^2 2^{-3n}.$$

Везде используется умножение положительных чисел с заданной точностью по методу из теоремы 3. Результатом каждого умножения являются два числа, которые дальше используются в умножении по отдельности. В конце все полученные числа складываются, при этом отрицательные слагаемые заменяются по лемме 1. Для сложения 16 результирующих чисел используем компрессор $S(16, 2)$ и сумматор.

Схема строится в виде нескольких уровней, на каждом из которых все вычисления проводятся параллельно. На первом уровне вычисляются все коэффициенты $a_i(x)$. На втором уровне вычисляются произведения $a_1 Y$, $a_3 Y$ и Y^2. На третьем уровне одновременно вычисляются произведения $a_2 Y^2$ и $(a_3 Y) Y^2$. Сдвиги, соответствующие умножению на $2^{-n}, 2^{-2n}, 2^{-3n}$, выполняются бесплатно.

На четвёртом уровне выполняется побитовое отрицание слагаемых, соответствующих отрицательным коэффициентам a_i. Это делается с глубиной 3. Помимо этого, к сумме добавляется константна, равная числу отрицательных слагаемых, в соответствии с леммой 1. Это число равно $b_0 + 2b_1 + 4b_2 + 8b_3$, и потому может быть вычислено без затрат глубины.

На пятом уровне к 16 числам применяется компрессор $S(16, 2)$. Полученные два числа подаются на вход сумматора.

4. Оценка погрешности

Обозначим через s_i такие целые неотрицательные константы, что $\|a_i\| < 2^{s_i}$, так что в двоичной записи каждого коэффициента a_i не более s_i знаков перед запятой. Как было доказано выше, погрешность приближения функции f многочленом p_3 не превосходит

$$\|f - p_3\|_{C[a,b]} \leq \frac{\delta^4}{128} \frac{\|f^{(4)}\|_{C[a,b]}}{24} = \varepsilon.$$

Определим параметр

$$E = \lfloor -\log \varepsilon \rfloor - 1 = 4n + 6 - \left\lceil \log \frac{\|f^{(4)}\|_{C[a,b]}}{24} \right\rceil.$$

Теорема 4. *Если коэффициенты $a_i(x)$ заданы с точностью*

$$a_0(x) \ -E+3 \text{ битов}, \quad a_1(x) \ -E+4-n \text{ битов},$$

$$a_2(x) \ -E+4-2n \text{ битов}, \quad a_3(x) \ -E+5-3n \text{ битов},$$

и, помимо этого,

$$N \geq E + 4 + \max(s_1, s_2, s_3),$$

то схема вычисляет приближённое значение функции f с погрешностью, не превосходящей 2^{-E}.

Доказательство. Все сложения в схеме выполняются точно, так что погрешность возникает только при умножении. Можно доказать, что каждое слагаемое $a_i(x)y^i$ даёт вклад в погрешность, не превосходящий 2^{-E-3}. Тогда погрешность приближения составит

$$\|f - p_3(x,y)\|_{C[a,b]} + 4 \cdot 2^{-E-3} \leq \varepsilon + 2^{-E-1} \leq 2^{-E}.$$

Последнее неравенство верно в силу выбора параметра E. Утверждение о том, что каждое слагаемое даёт вклад в погрешность, меньший 2^{-E-3}, доказывается с использованием теоремы 3 в силу ограничений, наложенных на $a_i(x)$.

Теорема 5. (*Оценка глубины схемы*) *Пусть S — такая константа, что*

$$\sum_{i=0}^{3} \|a_i\| 2^{-ni} \leq 2^S.$$

Пусть $A = 10 - \left\lceil \log \frac{\|f^{(4)}\|}{24} \right\rceil$, и выполнены условия $A + s_2 \geq 0$, $\sqrt{2}A \geq s_1$. Тогда глубина схемы не превосходит

$$D \leq (n+s) + 4\lceil \log(E + 5 - 2n + s_2) \rceil + 4\lceil \log(E + 4 - 2n + s_2) \rceil +$$

$$+ 25 + 2\lceil \log(E + S) \rceil.$$

Доказательство. На уровне схемы, вычисляющем $a_1 Y$, Y^2, $a_3 Y$, наибольший вклад в глубину даёт слагаемое $a_1 Y$. Однако если учесть, что оно может продолжать вычисляться параллельно работе следующего уровня схемы, то наибольший вклад в глубину даёт слагаемое Y^2:

$$D(Y^2) \leq \lceil \log(E + 5 - 2n + s_2) \rceil + 2.$$

Глубина следующего уровня схемы, вычисляющего a_2Y^2 и $(a_3Y)Y^2$, оценивается глубиной самого сложного произведения a_2Y^2

$$D(a_2Y^2) \le \lceil \log(E+4-2n+s_2) \rceil + 2.$$

Условия на A нужны, чтобы сумма $D(Y^2)+D(a_2Y^2)$ превосходила глубину любых других слагаемых на этих двух уровнях.

Глубина уровня схемы, вычисляющего $a_i(x)$, не превосходит $n+s+1$. Инверсия битов отрицательных слагаемых выполняется с глубиной 3. Согласно теореме 2, глубина схемы $S(16,2)$ не превосходит 17. Суммируемые числа имеют E знаков после запятой и S знаков до запятой. Сумматор строится с глубиной $2\lceil \log(E+S) \rceil + 2$. Получаем оценку теоремы.

Список литературы

1. Wegener I. The complexity of Boolean functions. — Stuttgart: Teubner–Wiley, 1987.

УЛУЧШЕНИЕ НИЖНИХ ОЦЕНОК ПОРОГА k-ВЫПОЛНИМОСТИ ДЛЯ НЕБОЛЬШИХ k

Ф. Ю. Воробьев (Москва)

1. Введение. Пусть $x_1, \ldots, x_n$ — множество из n булевых переменных. Назовем k-буквенной скобкой дизъюнкцию вида $(x_{i_1}^{\sigma_1} \vee x_{i_2}^{\sigma_2} \vee \ldots \vee x_{i_k}^{\sigma_k})$. При этом одна переменная может встречаться в скобке несколько раз (такую скобку будем называть неправильной). Построим случайную k-КНФ путем случайного, равновероятностного и независимого выбора m скобок из числа $(2n)^k$ всех скобок. При этом вероятность того, что некоторая скобка – неправильная, меньше k^2/n. С высокой вероятностью $(P \to 1)$ число неправильных скобок в формуле не превосходит $o(n)$. Следовательно, если для некоторого r формула над n переменными с $m = rn$ скобками выполнима с высокой вероятностью, то это же верно при $m = rn - o(n)$ для модели, где выбираются только правильные скобки. Пусть $S_k(n,r)$ — вероятность того, что $F_k(n, nr)$ выполнима. Определим

$$r_k \equiv \sup\{r : \lim_{n\to\infty} S_k(n,r) = 1\},$$

$$r_k^* \equiv \inf\{r : \lim_{n\to\infty} S_k(n,r) = 0\},$$

то есть r_k — точная верхняя грань таких r, что вероятность выполнимости формулы все еще стремится к единице, r_k^* — точная нижняя грань таких r, что вероятность выполнимости формулы стремится к нулю. Ясно, что $r_k \le r_k^*$. Существует предположение, что $r_k = r_k^*$, то есть при увеличении r в определенный момент происходит скачок предела вероятности выполнимости от единицы к нулю. Такое число r_k называется порогом выполнимости.

Существование порога не доказано, но известно следующее утверждение.

Теорема 1. [2] *Для любого $k \ge 2$ существует такая последовательность $r_k(n)$, что для любого $\varepsilon > 0$*

$$\lim_{n\to\infty} S_k\big(n, (1-\varepsilon)r_k(n)\big) = 1,$$

$$\lim_{n\to\infty} S_k\big(n, (1+\varepsilon)r_k(n)\big) = 0.$$

Следствие 1. *Зафиксируем $k \ge 2$. Если $F_k(n, rn)$ выполнима с вероятностью $P_n > C > 0$, то $r_k > r$.*

Как правило, улучшение нижних оценок порога выполнимости происходило благодаря анализу алгоритмов. Тем не менее, в работе [5] удалось успешно применить метод вторых моментов для улучшения нижней оценки r_k, а в работе [1] похожий метод позволил получить следующий хорошо известный результат.

Теорема 2. [1] *Существует последовательность $\delta_k \to 0$, такая что для всех $k \ge 3$*

$$r_k \ge 2^k \log 2 - (k+1)\frac{\log 2}{2} - 1 - \delta_k.$$

Кроме того, были получены явные нижние оценки r_k для всех $k \ge 3$. Для всех $k > 3$ были улучшены предыдущие нижние оценки. Для $k = 3$ алгоритмические методы дают более высокую нижнюю оценку. Предлагаемый метод позволяет улучшить результаты [1] для $k = 3$, 4 и 5:

k	3	4	5
Верхняя оценка	4.51	10.23	21.33
Результат данной работы	2.82	8.09	18.91
Нижняя оценка [1]	2.68	7.91	18.79
Алгоритмическая нижняя оценка	3.52	5.54	9.63

2. Метод вторых моментов. Мы будем применять метод вторых моментов в следующем виде:

Лемма 1. *Для любой неотрицательной случайной величины X,*

$$P(X > 0) \geq \frac{M(X)^2}{M(X^2)}.$$

В работе [1] исследовалась применимость метода вторых моментов к различным случайным величинам, зависящим от случайных k-КНФ. В частности, если X — это число выполняющих наборов случайной формулы $F_k(n, rn)$, то можно получить нижнюю оценку вероятности выполнимости, применив лемму 1 к X. Действительно, по следствию 1, если $P(X > 0) > 1/C$ для некоторой константы $C > 0$, то $r_k \geq r$.

Следовательно, если для некоторого r $M(X^2) = O\big(M(X)^2\big)$, то $r_k > r$. Но в работе [1] было продемонстрировано, что для любого положительного r существует константа $\beta = \beta(r) > 0$, такая что $M(X^2) > (1+\beta)^n M(X)^2$.

Итак, требуется выбрать такую случайную величину X, что из $X > 0$ следует выполнимость формулы, и к X применим метод вторых моментов. В [1] был найден целый класс случайных величин, удовлетворяющих этим свойствам.

3. Выбор случайной величины. Пусть c обозначает k-буквенную скобку, $\sigma \in \{0,1\}^n$, а $w(\sigma, c)$ — некоторая действительнозначная функция. Рассмотрим следующий класс случайных величин:

$$X = \sum_{\sigma} \prod_{c} w(\sigma, c).$$

Здесь сумма берется по всем $\sigma \in \{0,1\}^n$, а произведение — по всем скобкам случайной формулы. Так как переменные, входящие в формулу, выбираются равновероятно, естественно рассматривать функции вида $w(\sigma, c) = w(v) = w(|v|)$, где $v_i = +1$ если i-я переменная скобки c обращается в 1 на σ, и -1 в противном случае, а $|v|$ равняется числу $+1$ в v. Таким образом, выбор функции w сводится к выбору $k+1$ значений $w(0) = w_0, w(1) = w_1, \ldots, w(k) = w_k$. Пусть $A = \{-1, +1\}^k$. Из необходимых условий применимости метода вторых моментов следуют ограничения на $w_0, w_1, \ldots, w_k$:

$$w_0 = 0,$$

$$\sum_{v \in A} w(v) v = 0.$$

Добавим условие нормировки:

$$\sum_{v \in A} w(v) = 1.$$

Это позволяет свести выбор функции $w(v)$ к выбору $k-2$ параметров. Для небольших k это существенно упрощает вычисления.

4. Улучшенный метод. В работе [1] значения $w(1), ..., w(k)$ были выбраны эвристически. Вместо того, чтобы фиксировать эти значения на данном этапе, изменим метод из [1] так, чтобы он не зависел от конкретных значений $w(1), ..., w(k)$, а затем выберем $w(1), ..., w(k)$ используя численные методы, чтобы получить более высокие нижние оценки.

Пусть для $\sigma \in \{0,1\}^n$ $H(\sigma, F)$ обозначает число букв формулы F, обращающихся в единицу на σ, минус число букв, обращающихся в ноль. Пусть $S^+ = \{\sigma \in \{0,1\}^n : H(\sigma, F) \geq 0\}$ – множество наборов, на которых не менее половины букв формулы F обращаются в единицу.

В [1] было показано, что основной вклад в $M(X^2)$ дают наборы, на которых в единицу обращается меньше половины букв формулы. Поэтому имеет смысл рассмотреть случайную величину

$$X_+ = \sum_{\sigma \in S^+} \prod_c w(\sigma, c).$$

При этом математическое ожидание произведения нельзя заменить на произведение математических ожиданий. Аналогичные трудности возникают при вычислении $M(X_+^2)$. Тем не менее, оказывается, что к X_+ можно применить метод вторых моментов.

Нам понадобится следующее утверждение из [3].

Лемма 2. *Пусть ϕ — действительная, положительная, дважды дифференцируемая функция на $[0,1]$ и*

$$S_n = \sum_{z=0}^{n} C_n^z \phi(z/n)^n.$$

Полагая $0^0 \equiv 1$, определим g на $[0,1]$ как

$$g(\alpha) = \frac{\phi(\alpha)}{\alpha^\alpha (1-\alpha)^{(1-\alpha)}}.$$

Если существует $\alpha_{max} \in (0,1)$, такое, что $g(\alpha_{max}) \equiv g_{max} > g(\alpha)$ для всех $\alpha \neq \alpha_{max}$, и $g''(\alpha_{max}) < 0$, то существуют константы $B, C > 0$ такие что для всех достаточно больших n

$$B g_{max}^n \leq S_n \leq C g_{max}^n.$$

Лемма 3. $M(X_+)/M(X) \to 1/2$.

Это утверждение позволяет применить метод вторых моментов к X_+ без вычисления ее математического ожидания. Для этого требуется следующее утверждение, ограничивающее $M(X_+^2)$.

Утверждение 1.

$$M(X_+^2) \le 2^n \sum_{z=0}^{n} C_n^z \left(\inf_{\beta \ge 1} f_w(\alpha, \beta)^r \right)^n,$$

где

$$f_w(\alpha,\beta) = 2^{-k} \sum_{u,v=1}^{k} w(u)w(v)\beta^{2u+2v-2k} C_k^u \sum_s C_u^{s-p} C_{k-u}^p \alpha^s (1-\alpha)^{k-s},$$

$p = (k - |u| - |v| + s)/2$.

Определим

$$g_r(\alpha,\beta) = \frac{f_w(\alpha,\beta)^r}{\alpha^\alpha (1-\alpha)^{1-\alpha}}.$$

В работе [1] было доказано, что $M(X)^2 = 2^n g_r(1/2,1)^n$.

Из леммы 3 следует, что существует константа C_1, такая что

$$C_1 M(X_+)^2 > M(X)^2 = 2^n g_r(1/2,1)^n.$$

Если $b(\alpha) \ge 1$ – кусочно-постоянная функция, такая что для некоторого значения r верно $g_r(1/2,1) > g_r(\alpha, b(\alpha))$ для всех $\alpha \ne 1/2$, то применив лемму 2 мы получим, что $M(X_+^2) < C \times M(X_+)^2$, где C — некоторая константа. Тогда из леммы 1 будет следовать, что $r_k \ge r$.

5. Применение метода. Наконец, задача получения нижней оценки порога k-выполнимости для некоторого фиксированного k сведена к следующей задаче. Нужно найти такое r, что существуют $w(i)$, $i = \overline{1,k}$ и кусочно-постоянная функция $b(\alpha) \ge 1$, такие что для всех $\alpha \ne 1/2$ выполняется неравенство $g_r(1/2,1) > g_r(\alpha, b(\alpha))$. Если это условие выполнено, то r – нижняя оценка порога k-выполнимости. Другими словами, требуется найти такое r, что

$$\inf_{w(1),\ldots,w(k)} \sup_{\alpha > \frac{1}{2}} \inf_{\beta \ge 1} \left(g_r(\alpha,\beta) - g_r(1/2,1) \right) < 0.$$

Значения r, $w(1),\ldots,w(k)$ и $b(\alpha)$ могут быть получены различными способами. Результаты данной работы получены с помощью простейшего метода итеративного спуска.

Список литературы

1. Achlioptas D and Peres Y. The threshold for random k-SAT is $2^k \ln 2 - O(k)$. J. Amer. Math. Soc. (2004), 17: 947–973.

2. Friedgut E. Necessary and sufficient conditions for sharp thresholds of graph properties, and the k-SAT problem. J. Amer. Math. Soc. (1999), 12: 1017–1054.

3. de Bruijn N. G. Asymptotic methods in analysis. Dover Publications Inc., New York, 3rd edition (1981).

4. Kaporis A. C., Kirousis L. M. and Lalas E. G. The probabilistic analysis of a greedy satisfiability algorithm. Random Structures and Algorithms (2006) 28(4): 444–480.

5. Achlioptas D. and Moore C. The asymptotic order of the random k-SAT threshold. In Proc. 43th Annual Symposium on Foundations of Computer Science (2002) 126–127.

О НЕКОТОРЫХ ВОПРОСАХ, СВЯЗАННЫХ С ГИПОТЕЗОЙ АЛОНА О ЧИСЛЕ НЕЗАВИСИМЫХ МНОЖЕСТВ

А. Б. Дайняк (Москва)

Для всякого графа G будем через $V(G)$ и $E(G)$ обозначать множества вершин и ребер G соответственно. Граф, степени всех вершин в котором равны k, называется *k–регулярным*. Всякое множество попарно несмежных вершин в графе называется *независимым*. Для графа G через $I(G)$ и $\beta_0(G)$ будем обозначать соответственно число независимых множеств и размер максимального по мощности независимого множества.

Большой интерес в связи с приложениями представляет проблема оценки числа н. м. в регулярных и "квазирегулярных" графах. Н. Алон в работе [1] доказал существование такой функции $\phi(k) = O(k^{-0.1})$, что для всякого k–регулярного графа G на n вершинах

$$I(G) \leq 2^{\frac{n}{2}(1+\phi(k))}. \tag{1}$$

А. А. Сапоженко в [3] показал, что это неравенство справедливо для некоторой функции $\phi(k) = O(\sqrt{(\log k)/k})$, и получил аналогичную оценку для почти регулярных графов.

В статье [1] было высказано предположение (до сих пор не доказанное) о том, что в классе всех k-регулярных n-вершинных графов при $(2k)|n$ наибольшим числом н. м. обладает объединение $\frac{n}{2k}$ вершинно-непересекающихся полных двудольных графов (будем называть этот граф *графом Алона*). Если эта гипотеза верна, то в оценке (1) можно положить $\phi(k) = O(k^{-1})$. Граф

Алона обладает несколькими интересными свойствами: этот граф доставляет максимум величины β_0 среди всех k-регулярных n-вершинных графов, и при этом число максимальных н. м. в нем достаточно велико. Возникает вопрос, каким может быть число н. м. в регулярном n-вершинном графе при условии, что величина β_0 "существенно меньше" максимально возможного значения $n/2$. Справедливо следующее утверждение.

Утверждение 1. *Пусть последовательность графов $\{G_i\}_{i=1}^{\infty}$ такова, что минимальная степень вершины в графе G_i и число вершин в G_i стремятся к бесконечности. Пусть также для некоторого фиксированного $\epsilon > 0$ и для всех номеров i выполнено неравенство*

$$\beta_0(G_i) \leq \frac{|V(G_i)|}{2}(1-\epsilon).$$

Тогда найдется такая константа $c = c(\epsilon) > 0$ и такое натуральное число $i_0(\epsilon)$, что

$$\forall i \geq i_0 \quad I(G_i) \leq 2^{\frac{|V(G_i)|}{2}(1-c)}.$$

Утверждение 1 является прямым следствием следующей теоремы, доказанной А. А. Сапоженко в работе [2].

Теорема 1. *Пусть граф G на n вершинах является регулярным степени k, $\beta_0(G) = \mu$. Тогда*

$$I(G) \leq 2^{\mu \log_2\left(1+\frac{n}{2\mu}\right)+O\left(n\sqrt{k^{-1}\log k}\right)}.$$

Для вывода из приведенной теоремы утверждения 1 достаточно заметить, что функция $f(\mu) = \mu \log_2\left(1+\frac{1}{2\mu}\right)$ возрастает на интервале вида $(0, 1/2-\epsilon)$ и ограничена на этом интервале сверху некоторой константой $\delta = \delta(\epsilon) < \frac{1}{2}$.

Цель настоящей работы заключается в доказательстве того, что для выполнения неравенства $I(G) \leq 2^{|V(G)|(1/2+o(k^{-1}))}$ в общем случае недостаточно требования $\beta_0(G) \leq \frac{|V(G)|}{2}(1-\Omega(k^{-1}))$.

Лемма 1. *Для всякого натурального $k \geq 3$ существует связный k-регулярный граф G_k, для которого выполнены неравенства*

1) $\beta_0(G_k) < \frac{|V(G_k)|}{2}(1-\Omega(k^{-1}))$,

2) $\log_2(I(G_k)) > \frac{|V(G_k)|}{2}(1+\Omega(k^{-1}))$.

Доказательство. Будем рассматривать графы G_k следующего вида:

- Если k четно, то

$$\begin{aligned} V(G_k) &= \{u_i \mid i = \overline{1,k}\} \cup \{v_i^j \mid i = \overline{1,k},\ j = \overline{1,k-2}\} \cup \\ &\cup \{w_l^j \mid l = \overline{1,k-2},\ j = \overline{1,k-2}\}; \\ E(G_k) &= \{\{u_i, u_{i+1}\} \mid i = \overline{1,k-1}\} \cup \{\{u_k, u_1\}\} \cup \\ &\cup \{\{u_i, v_i^j\} \mid i = \overline{1,k},\ j = \overline{1,k-2}\} \cup \\ &\cup \{\{v_i^j, w_l^j\} \mid i = \overline{1,k},\ l = \overline{1,k-2},\ j = \overline{1,k-2}\} \cup \\ &\cup \{\{v_i^j, v_i^{j+1}\} \mid i = \overline{1,k},\ j = 1, 3, \ldots, k-3\}. \end{aligned}$$

- Если k нечетно, то

$$\begin{aligned} V(G_k) &= \{u_i \mid i = \overline{1,k}\} \cup \{v_i^j \mid i = \overline{1,k},\ j = \overline{1,k-2}\} \cup \\ &\cup \{w_l^j \mid l = \overline{1,k-2},\ j = \overline{1,k-3}\} \cup \\ &\cup \{w_l^{k-2} \mid l = \overline{1,k-1}\}; \\ E(G_k) &= \{\{u_i, u_{i+1}\} \mid i = \overline{1,k-1}\} \cup \{\{u_k, u_1\}\} \cup \\ &\cup \{\{u_i, v_i^j\} \mid i = \overline{1,k},\ j = \overline{1,k-2}\} \cup \\ &\cup \{\{v_i^j, w_l^j\} \mid i = \overline{1,k},\ l = \overline{1,k-2},\ j = \overline{1,k-3}\} \cup \\ &\cup \{\{v_i^{k-2}, w_l^{k-2}\} \mid i = \overline{1,k},\ l = \overline{1,k-1}\} \cup \\ &\cup \{\{v_i^j, v_i^{j+1}\} \mid i = \overline{1,k},\ j = 1, 3, \ldots, k-4\}. \end{aligned}$$

При любом $k \geq 3$ граф G_k является k-регулярным.

Далее мы будем рассматривать только случай четного k; рассуждения в случае нечетного k аналогичны.

В этом случае G_k — граф на $p = 2k^2 - 5k + 4$ вершинах. Покажем, что $\beta_0(G_k) \leq \frac{p}{2}(1 - \Omega(k^{-1}))$. Пусть A — произвольное независимое множество в графе G_k. Возможны два случая:

i) Какая-либо из вершин $u_1, \ldots, u_k$ входит во множество A. Пусть это вершина u_1. Тогда ни одна из вершин $v_1^1, \ldots, v_1^{k-2}$ не принадлежит множеству A. Кроме того, всего из множества $\{u_1, \ldots, u_k\}$ в A может входить не более $\lfloor \frac{k}{2} \rfloor$ вершин. Для каждого $j \in \{1, 3, \ldots, k-3\}$ из множества

$$\{v_i^j \mid i = \overline{1,k}\} \cup \{v_i^{j+1} \mid i = \overline{1,k}\} \cup \{w_l^j \mid l = \overline{1,k-2}\} \cup \{w_l^{j+1} \mid l = \overline{1,k-2}\}$$

в A может входить не более $(k-1) + (k-2)$ вершин. Поэтому $|A| \leq \frac{k}{2} + \frac{k-2}{2}(2k-4) = k^2 - 3k + 3 = \frac{p}{2}(1 - \Omega(k^{-1}))$.

ii) Ни одна из вершин $u_1, \ldots, u_k$ не входит в A. В данном случае $|A| \leq \frac{k-2}{2}(2k-2) = k^2 - 3k + 2$ (это значение достигается при $A = \{v_i^j \mid i = \overline{1,k},\ j \equiv 1 (\mathrm{mod}\, 2)\} \cup \{w_l^j \mid l = \overline{1,k-2},\ j \equiv 0 (\mathrm{mod}\, 2)\}$).

Как и в предыдущем случае, $|A| = \frac{p}{2}(1 - \Omega(k^{-1}))$, а значит первое неравенство из утверждения леммы выполнено.

Оценим теперь снизу число н. м. в графе G_k. Заметим, что $I(G) > (I(G'_k))^{(k-2)/2}$, где G'_k — подграф графа G, порожденный множеством вершин

$$\{u_i \mid i = \overline{1,k}\} \cup \{v_i^j \mid i = \overline{1,k},\ j = 1,2\} \cup \{w_l^j \mid l = \overline{1,k-2},\ j = 1,2\};$$

Число $I(G'_k)$ можно выписать в явном виде:

$$I(G'_k) = (2^{k-2} - 1)(2^k + 2^{k-2} - 1) + \sum_{j=0}^{k} \binom{k}{j} (2^{k-j} + 2^{k-2} - 1) =$$
$$= \frac{9}{16} \cdot 2^{2k} + 3^k - \frac{5}{2} \cdot 2^k + 1 > \frac{9}{16} \cdot 2^{2k}.$$

Отсюда

$$\log_2(I(G)) > (2k + \log_2(9/16))(k-2)/2 =$$
$$= k^2 + k \log_2 \frac{3}{16} - \log_2 \frac{9}{16} = \frac{p}{2}(1 + \Omega(k^{-1})).$$

Утверждение 2. *Найдутся такие положительные константы c', c'', что для всякого натурального числа $k \geq 3$ существует последовательность k–регулярных графов $\{G_{k,n}\}_{n=1}^{\infty}$ такая, что $p = |V(G_{k,n})| \to \infty$ при $n \to \infty$, и для всех n выполнены неравенства*

1) $\beta_0(G_{k,n}) < \frac{p}{2}(1 - c'k^{-1})$,

2) $I(G_{k,n}) > 2^{\frac{p}{2}(1+c''k^{-1})}$.

Доказательство. Зафиксируем произвольное натуральное число n. Рассмотрим n графов G_k^s, $s = \overline{1,n}$, каждый из которых изоморфен графу G_k, описанному в лемме. Будем предполагать, что $V(G_k^i) \cap V(G_k^j) = \emptyset$ при $i \neq j$. Рассмотрим граф $G_{k,n}$ такой, что

$$V(G_{k,n}) = \bigcup_{s=1}^{n} V(G_k^s), \quad E(G_{k,n}) = \bigcup_{s=1}^{n} E(G_k^s).$$

Для завершения доказательства достаточно заметить, что выполнены равенства

$$\beta_0(G_{k,n}) = \sum_{s=1}^{n} \beta_0(G_k^s), \quad I(G_{k,n}) = \prod_{s=1}^{n} I(G_k^s),$$

и учесть результат леммы.

Можно построить и последовательность *связных* k–регулярных графов $\{G'_{k,n}\}_{n=1}^{\infty}$, обладающую указанным в утверждении 2 свойством. Обозначим через u_i^s вершину графа G_k^s $(s = \overline{1,n})$, переходящую при изоморфизме соответственно в вершину u_i графа G_k. Граф $G'_{k,n}$ может быть получен из $G_{k,n}$ следующим образом: в $G_{k,n}$ удаляются все ребра $\{u_1^s, u_k^s\}$, и добавляются ребра $\{u_k^s, u_1^{s+1}\}$, $s = \overline{1,n-1}$, а также ребро $\{u_k^n, u_1^1\}$. Рассуждения из доказательства леммы и утверждения 2 переносятся на этот случай с незначительными изменениями.

Список литературы

1. Alon N. Independent Sets In Regular Graphs And Sum-free Subsets Of Finite Groups — Isr. J. Math., **73**, 2, 1991.

2. Сапоженко А. А. Верхняя оценка числа независимых множеств в квазирегулярных графах. Сдано в печать.

3. Сапоженко А. А. Доказательство гипотезы Камерона–Эрдеша о числе множеств, свободных от сумм — в сб. Матем. вопросы киберн. Вып. 12 — М., Физматлит, 2003.

О ВЕСОВОЙ ФУНКЦИИ БЕНТ-КОДОВ

М. П. Денисенко (Москва)

1. Введение

Конструкции, связанные с булевыми функциями, занимают заметное место в теории кодирования и криптологии. Так коды Рида-Маллера, построенные на основе булевых функций, тесно связаны как с вопросами построения криптографических примитивов с одной стороны, так и с разработкой методов криптографического анализа — с другой. В работе [3] была предложена новая кодовая конструкция, основывающаяся уже не на классе булевых функций, а на конкретной булевой функции. С помощью этой конструкции в настоящей работе мы рассматриваем весовую характеризацию линейных кодов, ассоциированных с бент-функциями. Получена весовая функция соответствующих кодов и дуальных к ним кодов.

2. Основные понятия и обозначения

Пусть $\mathbb{F}_2 = GF(2)$ и $\mathbb{N}$ — множество натуральных чисел. Для векторного пространства $\mathrm{V}_n = \mathbb{F}_2^n$, $n \in \mathbb{N}$ через $x = (x_1, \ldots, x_n)$ будем обозначать наборы длины n, являющиеся элементами этого пространства. Элементы x векторного пространства V_n будем называть векторами. Обозначим через " $\oplus$ " — операцию сложения по модулю 2 в поле $\mathbb{F}_2$.

Пусть $f : \mathrm{V}_n \to \mathbb{F}_2$ — булева функция от n переменных — отображение из V_n в $\mathbb{F}_2$, $\mathcal{F}_n$ — множество всех булевых функций от n переменных.

Определение. *Преобразованием Фурье булевой функции f называется целочисленная функция на V_n, определяемая следующим равенством*

$$\overline{W_f}(\boldsymbol{u}) = \sum_{\boldsymbol{x} \in \mathrm{V}_n} f(\boldsymbol{x})(-1)^{\langle \boldsymbol{x}, \boldsymbol{u} \rangle}$$

(суммирование производится в действительной области). Для каждого $\boldsymbol{u} \in \mathrm{V}_n$ значение $\overline{W_f}(\boldsymbol{u})$ называется коэффициентом Фурье.

Определение. *Преобразованием Уолша-Адамара булевой функции f называется целочисленная функция на V_n, определяемая следующим равенством*

$$W_f(\boldsymbol{u}) = \sum_{\boldsymbol{x} \in \mathrm{V}_n} \exp f(\boldsymbol{x})(-1)^{\langle \boldsymbol{x}, \boldsymbol{u} \rangle} = \sum_{\boldsymbol{x} \in \mathrm{V}_n} (-1)^{f(\boldsymbol{x}) \oplus \langle \boldsymbol{x}, \boldsymbol{u} \rangle}$$

(суммирование производится в действительной области).

Теорема 1. [1] *Коэффициенты Фурье и коэффициенты Уолша-Адамара связаны соотношением*

$$W_f(\boldsymbol{u}) = 2^n \delta(\boldsymbol{u}) - 2\overline{W_f}(\boldsymbol{u}),$$

где $\delta(\boldsymbol{u})$ — δ-функция Дирака:

$$\delta(\boldsymbol{u}) = \begin{cases} 1, & \text{если } \boldsymbol{u} = \boldsymbol{0}; \\ 0, & \text{если } \boldsymbol{u} \neq \boldsymbol{0}. \end{cases}$$

Определение. *Линейный блочный код $\boldsymbol{C}$ длины n — это линейное подпространство векторного пространства V_n.*

Определение. *Код длины n, размерности k и с минимальным расстоянием d называется $[n, k, d]$-кодом. В случае, когда минимальное расстояние d не является центральным в рассуждениях или неизвестно, используется обозначение $[n, k]$-код.*

Линейные блочные коды можно описывать с помощью матричного аппарата. Введем понятие кода, ассоциированного с булевой функцией.

Определение. *Пусть n — четное, $f \in \mathcal{F}_n$.*

$$\mathrm{supp}(f) = \{\boldsymbol{u}^1, \boldsymbol{u}^2, \ldots, \boldsymbol{u}^t\},$$

где $t = \mathrm{wt}(f)$. Рассмотрим матрицу G_f размера $n \times t$, столбцами которой являются векторы множества $\mathrm{supp}(f)$:

$$G_f = \left[\boldsymbol{u}^1 \ \boldsymbol{u}^2 \ \ldots \ \boldsymbol{u}^t\right].$$

Код $\boldsymbol{C}_f$, порождаемый этой матрицей

$$\boldsymbol{C}_f = \{\boldsymbol{c_v} \mid \boldsymbol{v} = (v_1, \ldots, v_n) \in \mathrm{V}_n\},$$

где

$$\boldsymbol{c_v} = \boldsymbol{v}G_f = \left(\langle \boldsymbol{v}, \boldsymbol{u}^1\rangle, \ldots, \langle \boldsymbol{v}, \boldsymbol{u}^t\rangle\right),$$

называется кодом, ассоциированным с булевой функцией f.

Поскольку код $\mathbf{C}$ является подпространством в V_n, для него определено подпространство — ортогональное дополнение

$$\mathbf{C}^{\perp} = \{\mathbf{x} \in \mathrm{V}_n \mid \langle \mathbf{x},\mathbf{c}\rangle = 0 \text{ для всех } \mathbf{c} \in \mathbf{C}\}.$$

Определение. *Код $\boldsymbol{C}^{\perp}$ называется дуальным кодом к коду* C.

Пусть $\mathbf{C}$ — произвольный $[n, k]$-код. Обозначим через $A_i,\ i = 0, 1, \ldots, n$, число его кодовых слов, вес которых равен i :

$$A_i = \sharp\{\mathbf{c} \in \mathbf{C} \mid \mathrm{wt}(\mathbf{c}) = i\}.$$

Определение. *Совокупность чисел $A_0, A_1, \ldots, A_n$ называется весовым спектром кода $\boldsymbol{C}$.*

Определение. *Полином*

$$\mathcal{W}_{\boldsymbol{C}}(\lambda, \nu) = \sum_{i=0}^{n} A_i \lambda^{n-i} \nu^i$$

от двух переменных λ и ν называется весовой функцией кода $\boldsymbol{C}$.

Теорема 2. Тождество Мак-Вильямс [2] *Пусть $\boldsymbol{C}$ — $[n, k]$-код, $\boldsymbol{C}^{\perp}$ — дуальный к нему $[n, n-k]$-код. Тогда*

$$\mathcal{W}_{\boldsymbol{C}^{\perp}}(\lambda, \nu) = \frac{1}{\sharp \boldsymbol{C}} \mathcal{W}_{\boldsymbol{C}}(\lambda + \nu, \lambda - \nu).$$

Через $A'_0, A'_1, \ldots, A'_n$ будем обозначать весовой спектр дуального кода $\mathbf{C}^{\perp}$.

При этом имеем следующие соотношения (следствие тождества Мак-Вильямс):

$$A'_k = \frac{1}{\sharp \mathbf{C}} \sum_{i=0}^{n} A_i P_k(i). \tag{1}$$

Выражения $P_k(i)$ называются полиномами Кравчука.

Определение. *Пусть n — фиксированное натуральное число. Полиномами Кравчука называются следующие выражения*

$$P_k(z) = \sum_{j=0}^{k} (-1)^j \binom{z}{j} \binom{n-z}{k-j},$$

где z — свободная переменная, $k = 0, 1, \ldots,$ и

$$\binom{z}{m} = \begin{cases} \frac{z(z-1)\ldots(z-m+1)}{m!}, & \text{если } m > 0; \\ 1, & \text{если } m = 0. \end{cases}$$

Определение. *Функция $f \in \mathcal{F}_n$ называется бент-функцией, если все ее коэффициенты Уолша-Адамара равны $\pm 2^{n/2}$.*

Множество всех бент-функций от n переменных будем обозначать $\mathcal{B}_n$. Поскольку коэффициенты Уолша-Адамара являются целыми рациональными числами, то при нечетном n бент-функций не существует.

Если $f \in \mathcal{B}_{2n}$, то, очевидно, существует такая булева функция $\tilde{f} \in \mathcal{F}_{2n}$, что

$$W_f(\alpha) = 2^n (-1)^{\tilde{f}(\alpha)}.$$

Указанную выше булеву функцию $\tilde{f} \in \mathcal{F}_{2n}$, называют дуальной функцией к бент-функции f.

При вычислении весовой функции бент-кода мы использовали следующие утверждения, доказанные в работе [3].

Теорема 3. *Пусть $f \in \mathcal{F}_n$ и $\boldsymbol{C}_f$ — ассоциированный с f код. Тогда для любого $\boldsymbol{v} \in \mathrm{V}_n$, $\boldsymbol{v} \neq \mathbf{0}$ имеем*

$$\mathrm{wt}(\boldsymbol{c}_{\boldsymbol{v}}) = 2^{n-2} + \frac{1}{4} \left(W_f(\boldsymbol{v}) - W_f(\mathbf{0}) \right). \tag{2}$$

Доказательство. Для произвольной функции $f \in \mathcal{F}_n$ выразим вес кодового слова

$$\mathbf{c}_{\mathbf{v}}, \ \mathbf{v} \neq (0, \ldots, 0) \in \mathrm{V}_n$$

кода $\mathbf{C}_f$ следующим образом:

$$\mathrm{wt}(\mathbf{c}_{\mathbf{v}}) = \sum_{\mathbf{x} \in \mathrm{V}_n} f(\mathbf{x}) \frac{1 - (-1)^{\langle \mathbf{v}, \mathbf{x} \rangle}}{2} = \frac{1}{2} \sum_{\mathbf{x} \in \mathrm{V}_n} f(\mathbf{x}) - \frac{1}{2} \sum_{\mathbf{x} \in \mathrm{V}_n} f(\mathbf{x}) (-1)^{\langle \mathbf{v}, \mathbf{x} \rangle} =$$

$$= \frac{1}{2} \overline{W_f}(\mathbf{0}) - \frac{1}{2} \overline{W_f}(\mathbf{v}) = \frac{1}{4} (2^n - W_f(\mathbf{0})) + \frac{1}{4} W_f(\mathbf{v}) = 2^{n-2} + \frac{1}{4} (W_f(\mathbf{v}) - W_f(\mathbf{0})). \tag{3}$$

Следующую теорему приведем без доказательства (см. [3]).

Теорема 4. *Пусть n — четное число. Функция $f \in \mathcal{F}_n$ является бент-функцией (т. е. $f \in \mathcal{B}_n$) тогда и только тогда, когда* $\dim \boldsymbol{C}_f = n$ *и веса ненулевых кодовых слов равны*

$$\mathrm{wt}(f) - 2^{n-2},\ 2^{n-2}.$$

3. Основной результат

Основная задача данной работы связана с вычислением весовой функции бент-кода, т. е. кода, ассоциированного с бент-функцией. Далее, используя выражения (1), следующие из тождества Мак-Вильямс (2), можно получить весовой спектр дуального к $\mathbf{C}_f$ кода.

Сформулируем и докажем следующую основную теорему.

Теорема 5. *Пусть n — четное число, $f \in \mathcal{B}_n$. Пусть*

$$\boldsymbol{C}_f = \{\boldsymbol{c}_{\boldsymbol{v}} \mid \boldsymbol{v} = (v_1, \ldots, v_n) \in \mathrm{V}_n\}$$

является ассоциированным с f кодом. $\tilde{f}$ — функция, дуальная к бент-функции f. Тогда весовой спектр кода $\boldsymbol{C}_f$ имеет следующий вид:
1) *если* $W_f(\mathbf{0}) > 0,\ W_{\tilde{f}}(\mathbf{0}) > 0$, *то*

$i = \mathrm{wt}(\boldsymbol{c}_{\boldsymbol{v}})$	$A_i = \sharp\{\boldsymbol{c}_{\boldsymbol{v}} \in \boldsymbol{C}_f \mid i = \mathrm{wt}(\boldsymbol{c}_{\boldsymbol{v}})\}$
0	1
2^{n-2}	$2^{n-1} + 2^{n/2-1} - 1$
$2^{n-2} - 2^{n/2-1}$	$2^{n-1} - 2^{n/2-1}$

;

2) *если* $W_f(\mathbf{0}) < 0,\ W_{\tilde{f}}(\mathbf{0}) > 0$, *то*

$i = \mathrm{wt}(\boldsymbol{c}_{\boldsymbol{v}})$	$A_i = \sharp\{\boldsymbol{c}_{\boldsymbol{v}} \in \boldsymbol{C}_f \mid i = \mathrm{wt}(\boldsymbol{c}_{\boldsymbol{v}})\}$
0	1
2^{n-2}	$2^{n-1} - 2^{n/2-1} - 1$
$2^{n-2} + 2^{n/2-1}$	$2^{n-1} + 2^{n/2-1}$

;

3) *если* $W_f(\mathbf{0}) > 0,\ W_{\tilde{f}}(\mathbf{0}) < 0$, *то*

$i = \mathrm{wt}(\boldsymbol{c}_{\boldsymbol{v}})$	$A_i = \sharp\{\boldsymbol{c}_{\boldsymbol{v}} \in \boldsymbol{C}_f \mid i = \mathrm{wt}(\boldsymbol{c}_{\boldsymbol{v}})\}$
0	1
2^{n-2}	$2^{n-1} - 2^{n/2-1} - 1$
$2^{n-2} - 2^{n/2-1}$	$2^{n-1} + 2^{n/2-1}$

;

4) *если* $W_f(\mathbf{0}) < 0,\ W_{\tilde{f}}(\mathbf{0}) < 0$, *то*

$i = \mathrm{wt}(\boldsymbol{c_v})$	$A_i = \sharp\{\boldsymbol{c_v} \in \boldsymbol{C_f} \mid i = \mathrm{wt}(\boldsymbol{c_v})\}$
0	1
2^{n-2}	$2^{n-1} + 2^{n/2-1} - 1$
$2^{n-2} + 2^{n/2-1}$	$2^{n-1} - 2^{n/2-1}$

.

Доказательство. При доказательстве будем использовать соотношение $\mathrm{wt}(f) = 2^{n-1} - \frac{1}{2}W_f(\mathbf{0})$. Кроме того, $W_f(\mathbf{0}) = \pm 2^{n/2}$, т. к. $f \in \mathcal{B}_n$. Из определения дуальной функции имеем: $W_f(\mathbf{v}) = 2^{n/2} \cdot (-1)^{\tilde{f}(\mathbf{v})}$. Следовательно,

$$W_f(\mathbf{v}) > 0 \;\Leftrightarrow\; \tilde{f}(\mathbf{v}) = 1;$$

$$W_f(\mathbf{v}) < 0 \;\Leftrightarrow\; \tilde{f}(\mathbf{v}) = 0.$$

В силу теоремы (4) имеем следующее соотношение:

$$\mathrm{wt}(\mathbf{c_v}) = \begin{cases} 0, & \text{если } \mathbf{v} = (0, \ldots, 0); \\ 2^{n-2}, & \text{если } W_f(\mathbf{0}) = W_f(\mathbf{v}),\ \mathbf{v} \neq (0, \ldots, 0); \\ \mathrm{wt}(f) - 2^{n-2}, & \text{если } W_f(\mathbf{0}) = -W_f(\mathbf{v}),\ \mathbf{v} \neq (0, \ldots, 0). \end{cases}$$

На основе данных утверждений и соотношений легко получается результат теоремы.

Список литературы

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

2. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.

3.Carlet C. Boolean functions for cryptography and error correcting codes. http://www-rocq.inria.fr/codes/Claude.Carlet/chap-fcts-Bool.pdf

О СПЕЦИАЛЬНОМ ПРЕДСТАВЛЕНИИ ГРАФОВ В ТРЕХМЕРНОМ ЕВКЛИДОВОМ ПРОСТРАНСТВЕ

М. Н. Еникеев (Москва)

1. Среди множества проблем дискретной геометрии и задач об упаковках есть ряд малоисследованных задач. Одной из них является изучение систем выпуклых тел (которыми в природе могут быть, например, клетки

органических тканей, кристаллы и т.д.) на предмет возможности их взаимосвязи через некоторый общий участок поверхности. Множество взаимосвязей между объектами системы выражается графом, вершины которого взаимно-однозначно соответствуют рассматриваемым выпуклым телам, а наличие или отсутствие ребер между ними — соответственно, наличию или отсутствию общего участка поверхности тел. Для начала требуется выяснить, возможно ли в принципе представить произвольный граф в виде системы выпуклых тел с описанными свойствами.

Теперь опишем проблему более строго. В работе рассматриваются специальные представления графов без кратных ребер и петель на n вершинах в трехмерном евклидовом пространстве в виде систем n ограниченных выпуклых тел с определенными свойствами.

Напомним, что выпуклым телом в $\mathbb{R}^3$ называется всякое множество точек, содержащее, вместе с любыми двумя своими точками, весь отрезок между ними. В этой работе мы полагаем, что выпуклое тело содержит свою границу (поверхность) [1].

Назовем два выпуклых тела *соприкасающимися*, если они не имеют общих внутренних точек, и существует множество их общих точек, имеющее ненулевую площадь. Очевидно, что все общие точки двух соприкасающихся выпуклых тел лежат в одной плоскости.

Пусть имеется система n выпуклых тел в $\mathbb{R}^3$, никакие два из которых не имеют общих внутренних точек. Сопоставим этой системе граф G на n вершинах, такой, что между множеством вершин графа и множеством выпуклых тел существует взаимно-однозначное соответствие, причем две вершины графа соединены ребром тогда и только тогда, когда соответствующие этим вершинам выпуклые тела соприкасаются. Будем говорить, что такая система соприкасающихся выпуклых тел представляет граф G (вообще говоря, когда мы употребляем выражение "система соприкасающихся тел", это не означает, что каждые два тела из этой системы соприкасаются).

Назовем два выпуклых тела *слабо соприкасающимися*, если они не имеют общих внутренних точек, и существует их общая точка, лежащая в области гладкости поверхности каждого из этих тел. Очевидно, что если два выпуклых тела соприкасаются, то они слабо соприкасаются. Представление графа G на n вершинах в виде системы слабо соприкасающихся выпуклых тел определяется аналогично случаю системы соприкасающихся тел.

Пусть задан произвольный граф без кратных ребер и петель G на n вершинах. Задачами работы является исследовать возможность представления графа G: а) в виде системы n выпуклых тел, слабо соприкасающихся по графу G; б) в виде системы n выпуклых тел, соприкасающихся по графу G; в) в виде системы n соприкасающихся по графу G выпуклых многогранников. В данной работе показано, что любой граф G без петель и кратных ребер

может быть представлен всеми этими способами. Сначала доказывается, что существование представления графа в виде системы соприкасающихся многогранников равносильно существованию его представления в виде системы слабо соприкасающихся выпуклых тел. Также, из этого очевидно следует равносильность представления графа в виде а) и б).

2. Естественно в первую очередь пытаться построить примеры представлений для случая полного графа на n вершинах.

Теорема 1. *Для любого $n > 0$ существует представление полного графа G без петель и кратных ребер на n вершинах системой n слабо соприкасающихся выпуклых тел.*

По причине недостатка места доказательство теоремы опустим. Покажем теперь, каким образом, имея такое представление, можно получить представление графа G в виде n соприкасающихся выпуклых многогранников.

Возьмем существующее согласно теореме 1 представление полного графа G на n вершинах в виде системы n слабо соприкасающихся выпуклых тел
$\Phi = \{\Phi_1, \ldots, \Phi_n\}$. Любые два тела из множества Φ слабо соприкасаются. Для тела Φ_i можно определить множество общих с остальными телами системы Φ касательных плоскостей Γ_{ij}, где $j = 1, \ldots, i-1, i+1, \ldots, n$, содержащих все общие точки тел Φ_i и Φ_j. Пусть многогранник F_i ограничен плоскостями Γ_{ij} таким образом, что тело Φ_i лежит внутри многогранника F_i. Такой многогранник существует: пусть есть тело Φ_i с касательными плоскостями Γ_{ij} для $j = 1, \ldots, i-1, i+1, \ldots, n$. По определению, выпуклый многогранник задается системой линейных неравенств. Возьмем одну из плоскостей с уравнением $\gamma_{ij} = 0$. Два полупространства, на которые делит все пространство эта плоскость, задаются неравенствами $\gamma_{ij} \geqslant 0$ и $\gamma_{ij} \leqslant 0$. Мы берем то полупространство, в котором лежит тело Φ_i и записываем неравенство, соответствующее этому полупространству в систему. Для всех пар (i, j), $1 \geqslant i \neq j \geqslant n$, получаем систему неравенств, задающих выпуклый многогранник. Эта система разрешима в силу существования тела Φ_i, для всех точек которого выполняются все неравенства системы.

Заметим, что F_i не обязательно является ограниченным многогранником. Пусть среди многогранников есть неограниченный многогранник F_i. Поскольку объединение выпуклых тел $\bigcap \Phi_i$ является ограниченным множеством, существует куб Λ, внутри которого находится все это объединение. Тогда отбросим от многогранника F_i все точки, лежащие вне куба Λ и получим ограниченный выпуклый многогранник с вписанным в него телом Φ_i.

Итак, есть система многогранников $F = \{F_1, \ldots, F_n\}$. Приведем несколько утверждений, которые, в целях экономии места, либо ввиду их очевидности, оставим без доказательства.

Лемма 1. *У любых двух многогранников из $F = \{F_1, \ldots, F_n\}$ нет общих внутренних точек.*

Все общие точки двух многогранников из $F = \{F_1, \ldots, F_n\}$ лежат в одной плоскости. Любая общая точка тела Φ_i с каким-либо телом Φ_j, расположенная в области гладкости границы обоих тел, лежит на поверхности многогранника F_i, причем является внутренней точкой некоторой его грани, из чего следует, что множество всех общих точек двух многогранников имеет ненулевую площадь.

Лемма 2. *Многогранники F_i и F_j, построенные вокруг слабо соприкасающихся тел Φ_i и Φ_j из множества Φ, соприкасаются.*

Из Теоремы 1 и Лемм 1, 2 следует

Теорема 2. *Пусть $\Phi = \{\Phi_1, \ldots, \Phi_n\}$ — множество попарно слабо соприкасающихся выпуклых тел. Тогда можно построить множество многогранников $F = \{F_1, \ldots, F_n\}$, любые два из которых соприкасаются.*

Таким образом, если система Φ представляет полный граф G на n вершинах в виде системы слабо соприкасающихся выпуклых тел, то система F является представлением графа G в виде системы соприкасающихся выпуклых многогранников.

3. Пусть G' - произвольный граф без петель и кратных ребер на n вершинах. Имея пример представления полного графа G на n вершинах системой n слабо соприкасающихся выпуклых тел, и совершив некоторые преобразования над телами из этой системы, можно построить представление графа G' слабо соприкасающимися выпуклыми телами (напомним снова, что не любые два из тел новой системы являются слабо соприкасающимися). Выражаясь буквально, мы отсекаем некоторые множества точек от тел из системы, представляющей полный граф, и, таким образом, изолируем друг от друга тела, соответствующие несмежным вершинам графа G'.

Теорема 3. *Для любого графа G' без петель и кратных ребер на n вершинах существует представление в виде системы слабо соприкасающихся выпуклых тел в $\mathbb{R}^3$.*

Кроме этого, верно следующее утверждение.

Теорема 4. *Для любого графа G' без петель и кратных ребер на n вершинах существует представление в виде системы n соприкасающихся выпуклых многогранников в $\mathbb{R}^3$.*

Дальнейшие исследования проблемы могут быть направлены на обобщение результатов, например на случай представлений бесконечных графов, упрощение представлений описанных видов для определенных типов графов, а также представления графов при заданных ограничениях на вид представляющих их тел.

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

Список литературы

1. Болтянский В. Г., Яглом И. М. Выпуклые фигуры и тела // Энциклопедия элементарной математики. Том V. Геометрия. С. 182-269. М.: Наука, 1966.

О ЕДИНИЧНЫХ ДИАГНОСТИЧЕСКИХ ТЕСТАХ ДЛЯ БЛОЧНЫХ КОНТАКТНЫХ СХЕМ НЕКОТОРОГО КЛАССА

И. А. Ильин (Москва)

В работе развивается метод мультиразбиений, предложенный ранее в [4–6] для построения единичных диагностических тестов размыкания для некоторых классов блочных контактных схем.

Определения понятий, которые не даны в этом тексте, можно найти, например, в [1–3]. Всякую последовательность упорядоченных покрытий некоторого множества A будем называть *мультипокрытием* множества A. Мультипокрытие назовем *различимым*, если все компоненты всех входящих в него покрытий попарно различны. Пусть S – КС с множеством входных полюсов $\{a_1, \ldots, a_{p_0}\}$ и с множеством выходных полюсов $\{b_1, \ldots, b_{p_1}\}$. Построим по S двухполюсную КС $\hat{S}^{\mu,\nu}$ как подсхему схемы S, содержащую лишь проводящие цепи, идущие из полюса a_μ в полюс b_ν. Процесс получения схемы $\hat{S}^{\mu,\nu}$ из S будем называть *операцией усечения*. Если число выходов КС S_1 равно числу входов КС S_2 и равно p, то определена *операция присоединения* S_2 *к* S_1, заключающаяся в отождествлении i-го выхода S_1 с i-м входом S_2, $i = \overline{1,p}$. В результате получается схема $S = S_1 S_2$, входами

которой являются входы S_1, а выходами – выходы S_2. Если число выходов S_1 не равно числу входов S_2, то операция присоединения S_2 к S_1 не определена.

Определим по индукции понятие *последовательной блочной схемы (ПБС) над базисом* $\mathcal{B}$.

Базис индукции. Пусть дано некоторое (как правило – конечное) множество $\mathcal{B}$ схем (называемых *блоками*) с выделенными входами и выходами. Каждый блок из указанного множества является ПБС над базисом $\mathcal{B}$.

Шаг индукции. Если схема S_1 – ПБС над $\mathcal{B}$, а схема S_2 – схема, однотипная блоку из $\mathcal{B}$, такая, что ни одно из управляющих ей реле не управляет схемой S_1, и операция присоединения S_2 к S_1 определена, то получающаяся в результате применения этой операции схема S является ПБС над $\mathcal{B}$.

ПБС S называется *периодической*, если последовательность типов составляющих ее блоков является периодической с нулевым предпериодом. Если S – периодическая ПБС, то и $\hat{S}^{\mu,\nu}$ будем считать *двухполюсной периодической* ПБС. ПБС S с n блоками называется *r-достижимой*, если из любого входа i-го блока можно попасть по проводящей цепи в любой выход $(i+r-1)$-го блока, $i = 1, \ldots, n-r+1$. Назовем некоторое множество простых проводящих цепей некоторой контактной схемы S *покрывающим*, если любой контакт схемы принадлежит какой-либо цепи этого множества. Покрывающее множество цепей будем называть *диагностическим* множеством цепей, если для любой пары контактов схемы в этом множестве найдется цепь, которой принадлежит ровно один контакт этой пары. Простую проводящую цепь, соединяющую вход и выход с одинаковыми номерами (например, вход a_μ с выходом b_μ) в схеме S, назовем *циклической*. Множество цепей, в котором все цепи – циклические, будем называть *циклическим*.

Будем рассматривать ПБС, блоки которых являются однозначно проводящими разделительными по входам и выходам схемами. Класс таких периодических ПБС с максимальным количеством контактов в блоках, равным λ, обозначим через Φ_λ, а класс схем, полученных усечением схем из класса Φ_λ, обозначим через $\hat{\Phi}_\lambda$.

Допустим, что основной период длины τ некоторой схемы $S \in \Phi_\lambda$ имеет вид $\Pi_d = H_1 H_2 \ldots H_\tau$. Пусть D_0 – покрывающее множество цепей для S, обладающее следующим свойством: найдется такое натуральное q, что каждая цепь множества D_0 представляет собой периодическое повторение своего начала, проходящего через первые τq блоков схемы (при этом номера принадлежащих этой цепи входа первого блока схемы и выхода (τq)-го блока схемы должны совпадать). Пусть q_0 – минимальное из таких q. Тогда величину (τq_0) назовем *длиной сверхпериода*, а схему $[\Pi_d]^{q_0}$ – *сверхпериодом*), порожденным периодом Π_d и множеством цепей D_0. Длину сверхпериода будем обозначать через $T = T(\Pi_d, D_0)$, а сам сверхпериод – через $\tilde{\Pi}_d$. Множество цепей D_0 будем называть *базовым*. Пусть D $(|D| = k)$ – некото-

рое множество простых проводящих цепей в схеме $S_n(\Pi_d)$ со сверхпериодом $\tilde{\Pi}_d$ относительно базового множества D_0. Тогда по признаку прохождения через контакты i-го блока схемы данные цепи образуют покрытие с упорядоченными компонентами (к j-ой компоненте покрытия относятся те и только те цепи, которые проходят через j-ый контакт блока), а при рассмотрении всех покрытий, порожденных множеством D и блоками схемы, возникает последовательность покрытий, элементами покрытий которой являются цепи множества D. Эту последовательность покрытий мы в дальнейшем будем называть $(\tilde{\Pi}_d, D, k, n)$-*мультипокрытием, порожденным множеством цепей* D. Всякую комбинаторную конфигурацию, являющуюся $(\tilde{\Pi}_d, D, k, n)$-мультипокрытием при некотором D, будем называть $(\tilde{\Pi}_d, k, n)$-мультипокрытием. $(\tilde{\Pi}_d, k, n)$-мультипокрытие назовем *циклическим*, если n кратно $T(\tilde{\Pi}_d)$ и D – циклическое множество цепей. Назовем $(\tilde{\Pi}_d, k, n)$-мультипокрытие *различимым*, если все компоненты его покрытий попарно различны. Назовем $(\tilde{\Pi}_d, k, n)$-мультипокрытие *слаборазличимым относительно* D_0, если $(\tilde{\Pi}_d, k, n)$-мультипокрытие, порожденное множеством цепей $D \cup D_0$, различимое. При этом будут допускаться и пустые компоненты.

Утверждение 1. *Если в схеме* $S_n(\Pi_d) \in \Phi_\lambda$ *множество цепей* D *порождает различимое мультипокрытие, то* D *– диагностическое множество цепей.*

Утверждение 2. *В двухполюсной однозначно-проводящей КС существование диагностического множества цепей мощности* l *равносильно существованию единичного диагностического теста размыкания длины* l.

Рассмотрим ПБС S_1 и S_2. Пусть V_1 — множество вершин схемы S_1, V_2 — множество вершин S_2; соответственно X_1, X_2 — совокупности их управляющих переменных. Будем говорить, что S_1 изоморфна S_2, если существуют взаимно однозначные отображения $\varphi : V_1 \to V_2$ и $\xi : X_1 \to X_2$ такие, что если вершина v_1 в схеме S_1 инцидентна вершине v_2 и они соединены контактом с пометкой $x_i^{\sigma_i}$, то $\varphi(v_1)$ в S_2 инцидентна $\varphi(v_2)$, а соединены они контактом, помеченным $\xi(x_i)^{\sigma_i}$. Пусть ПБС S_1 и S_2 изоморфны. Упорядоченные множества цепей $D_1 = (z'_1, \ldots, z'_k)$ в S_1 и $D_2 = (z''_1, \ldots, z''_k)$ в S_2 назовем *изоморфными*, если z'_1 изоморфна z''_1 (то есть z'_1 проходит в S_1 через те же контакты, что и z''_1 в S_2), ... , z'_k изоморфна z''_k. Под записью $z \subset S$ будем понимать «цепь z принадлежит схеме S», под записью $k \div l$ $(k, l \in \mathbb{N})$ — результат деления нацело числа k на число l, под записью $k \bmod l$ – остаток от деления k на l. Пусть, далее, имеются две ПБС S_1 и S_2, для которых определено их последовательное соединение $S = S_1 S_2$, $z_1 \subset S_1, z_2 \subset S_2$, z_1 инцидентна выходу схемы S_1 с номером j, z_2 инцидентна входу схемы S_2 с номером j. Тогда *последовательным соединением цепей* z_1 *и* z_2 будем называть цепь $z \subset S$, проходящую в S_1 по контактам z_1, а в S_2 — по контактам

z_2. Будем обозначать это как $z = z_1 z_2$ или $z = z_1 \bullet z_2$. Предположим, что в периодической ПБС S имеется некоторое циклическое множество цепей $D = (z_1, z_2, \ldots, z_k)$. Пусть ПБС $S' = S_1 S_2 \ldots S_m$, где $S_i, i = \overline{1,m}$ — схемы, изоморфные S. Тогда за D^m будем обозначать множество цепей $(z_1^m, \ldots, z_k^m)$ в схеме S', где $z_j^m = \underbrace{z_j z_j \ldots z_j}_{m \text{ раз}}, j = \overline{1,k}$ (эти цепи могут быть построены в силу цикличности D).

Рассмотрим некоторую r-достижимую периодическую ПБС S с периодом длины τ, состоящую из l (l кратно τ) блоков и некоторую цепь z в этой схеме. Пусть z инцидентна входу схемы S с номером j_1 и выходу с номером j_2. Пусть, также, z проходит через k_1-й выход r-го блока и через вход $(l-r+1)$-го блока, имеющий номер k_2. *Правым циклическим r-дополнением цепи z в схеме S* будем называть любую из цепей $z' \subset S$, построенных следующим образом: в первых (левых) $l-r$ блоках S цепь z' проходит через те же контакты, что и z; в последних r блоках схемы S z' проходит через контакты любой из цепей, соединяющих вход $(l-r+1)$-го блока под номером k_2, с j_1-ым выходом S (в силу r-достижимости S, хотя бы одна такая цепь найдется). Аналогично, *левым циклическим r-дополнением цепи z в схеме S* назовем любую из цепей $z'' \subset S$, построенных следующим образом: в первых l блоках S цепь z'' проходит через контакты любой из цепей, соединяющих j_2-й вход схемы S с k_1-м выходом r-го блока; в остальных $l-r$ блоках z'' проходит по тем же контактам, что и z. Правое и левое циклические r-дополнения цепи z в схеме S обозначим за $\mathcal{E}_r^+(z,S)$ и $\mathcal{E}_r^-(z,S)$ соответственно. Отметим важное свойство $(*)$ циклических r-дополнений: если для схемы S имеется $(\tilde{\Pi}_d, k, l)$-мультипокрытие $\mathcal{M}$, порожденное некоторым множеством цепей D, $z \in D$, а z' (z'') – правое (левое) циклическое r-дополнение цепи z, то при добавлении z' (z'') в D в первых (последних) $l-r$ покрытиях мультипокрытия $\mathcal{M}$ цепь z' (z'') попадет в те же компоненты, что и z.

Лемма 1. *Если для r-достижимой периодической ПБС $S_m(\Pi_d) \in \Phi_\lambda$ существует циклическое слаборазличимое относительно базового множества цепей D_0 $(\tilde{\Pi}_d, k, m)$-мультипокрытие и $T \geqslant 2r$, то для любого $s \in \mathbb{N}$ существует циклическое слаборазличимое относительно множества $D_0^{\frac{n_s}{m}}$ $(\tilde{\Pi}_d, k_s, n_s)$-мультипокрытие, где $k_s = k(2s-1)$, $n_s = m(\frac{m}{T})^{s-1}$.*

Доказательство проводится индукцией по s.

Базис индукции. При $s = 1$ утверждение равносильно условию леммы, и справедливость его очевидна.

Шаг индукции. Пусть утверждение верно для $s = s'$, то есть построено циклическое слаборазличимое относительно D_0 $(\tilde{\Pi}_d, k_{s'}, n_{s'})$-мультипокрытие. Покажем, что оно верно и для $s = s' + 1$. Рассмотрим схему $S_{s'+1} =$

$S_{n_{s'+1}}(\Pi_d)$, соответствующую $s = s' + 1$. Обозначим за $S^{[1]}_{s'+1}, \ldots, S^{[m/T]}_{s'+1}$ подсхемы схемы $S_{s'+1}$ длины s'. По предположению индукции, для каждой из схем $S^{[1]}_{s'+1}, \ldots, S^{[m/T]}_{s'+1}$ существует циклическое слаборазличимое $(\tilde{\Pi}_d, k_{s'}, n_{s'})$-мультипокрытие. Пусть такие мультипокрытия порождены множествами цепей
$D^{[1]}_{s'+1}, \ldots, D^{[m/T]}_{s'+1}$, и $D^{[1]}_{s'+1} = (\hat{z}^{[1]}_1, \ldots, \hat{z}^{[1]}_{k_{s'}}), \ldots, D^{[m/T]}_{s'+1} = (\hat{z}^{[m/T]}_1, \ldots, \hat{z}^{[m/T]}_{k_{s'}})$. Так как (в силу периодичности) схемы $S^{[1]}_{s'+1}, \ldots, S^{[m/T]}_{s'+1}$ изоморфны друг другу, то будем считать, что и множества цепей $D^{[1]}_{s'+1}, \ldots, D^{[m/T]}_{s'+1}$ также изоморфны друг другу (всегда можно таким образом построить соответствующие мультипокрытия). И поскольку эти множества цепей циклические, то в схеме $S_{s'+1}$ может быть построено множество цепей $\hat{D}_{s'+1} = (\hat{z}_1, \ldots, \hat{z}_{k_{s'}})$, где $\hat{z}_j = \hat{z}^{[1]}_j \hat{z}^{[2]}_j \ldots \hat{z}^{[m/T]}_j$, $j = \overline{1, k_{s'}}$.

Рассмотрим схему $S_1 = S_m(\Pi_d)$, соответствующую базису индукции. Пусть исходное $(\tilde{\Pi}_d, k, m)$-мультипокрытие порождено множеством цепей $D_1 = (\check{z}_1, \ldots, \check{z}_k)$. За $S^{(1)}_1, \ldots, S^{(m/T)}_1$ обозначим подсхемы схемы S_1 длины T, а за $\check{z}^{(1)}_1, \ldots, \check{z}^{(m/T)}_1, \ldots, \check{z}^{(1)}_k, \ldots, \check{z}^{(m/T)}_k$ обозначим участки цепей из D_1, проходящие через $S^{(1)}_1, \ldots, S^{(m/T)}_1$ (то есть $\check{z}^{(j)}_1, \check{z}^{(j)}_2, \ldots, \check{z}^{(j)}_k \subset S^{(j)}_1$, $j = \overline{1, m/T}$).

Обозначим за $S^{(1)}_{s'+1}, \ldots, S^{(n_{s'+1}/T)}_{s'+1}$ подсхемы схемы $S_{s'+1}$ длины T. Эти подсхемы изоморфны схемам $S^{(1)}_1, \ldots, S^{(m/T)}_1$, и, следовательно, мы можем рассматривать в них упомянутые цепи $\check{z}^{(i)}_j, i = \overline{1, m/T}, j = \overline{1, k}$. С учетом вышесказанного, построим в $S_{s'+1}$ множество цепей $D^+_{s'+1} = \{z^+_j\}$, где

$$z^+_j = \left(\mathcal{E}^+_r(\check{z}^{(1)}_j, S^{(1)}_{s'+1}) \ \ldots \ \mathcal{E}^+_r(\check{z}^{(1)}_j, S^{(\frac{s'}{T}-1)}_{s'+1}) \ \check{z}^{(1)}_j\right) \bullet$$
$$\bullet \ldots \bullet \left(\mathcal{E}^+_r(\check{z}^{(m/T)}_j, S^{(\frac{(m/T-1)s'}{T}+1)}_{s'+1}) \ \ldots \ \mathcal{E}^+_r(\check{z}^{(m/T)}_j, S^{(\frac{(m/T)s'}{T}-1)}_{s'+1}) \ \check{z}^{(m/T)}_j\right),$$

$j = \overline{1, k}$, и множество цепей $D^-_{s'+1} = \{z^-_j\}$, где

$$z^-_j = \left(\check{z}^{(1)}_j \ \mathcal{E}^-_r(\check{z}^{(1)}_j, S^{(2)}_{s'+1}) \ldots \mathcal{E}^-_r(\check{z}^{(1)}_j, S^{(s'/T)}_{s'+1})\right) \bullet \ldots \bullet$$
$$\bullet \left(\check{z}^{(m/T)}_j \ \mathcal{E}^-_r(\check{z}^{(m/T)}_j, S^{(\frac{(m/T-1)s'}{T}+2)}_{s'+1}) \ \ldots \ \mathcal{E}^-_r(\check{z}^{(m/T)}_j, S^{(\frac{(m/T)s'}{T})}_{s'+1})\right),$$

и также $j = \overline{1, k}$. Отметим, что множества цепей $D^+_{s'+1}$ и $D^-_{s'+1}$ являются циклическими.

Покажем, что $(\tilde{\Pi}_d, k_{s'+1}, n_{s'+1})$-мультипокрытие, порожденное множеством цепей $D_{s'+1} = \hat{D}_{s'+1} \cup D^+_{s'+1} \cup D^-_{s'+1}$ в схеме $S_{s'+1}$, является циклическим слаборазличимым относительно $D_0^{\frac{n_{s'+1}}{m}}$ мультипокрытием. Заметим, что $|D_{s'+1}| = |D_{s'}| + 2k$.

Пусть множество цепей $\bar{D}_{s'+1} = D_0^{\frac{n_{s'+1}}{m}} \cup D_{s'+1}$ в $S_{s'+1}$. Рассмотрим соответствующее $(\tilde{\Pi}_d, \bar{D}_{s'+1}, k_{s'+1}, n_{s'+1})$-мультипокрытие. Покажем, что оно является различимым, то есть любые две компоненты любых двух покрытий этого мультипокрытия различны.

Обозначим за $r_1, \ldots, r_{n_{s'+1}}$ покрытия упомянутого $(\tilde{\Pi}_d, \bar{D}_{s'+1}, k_{s'+1}, n_{s'+1})$-мультипокрытия, а за r_j^i – i-ю компоненту покрытия r_j. Выделим из совокупности всех компонент всех покрытий пару $r_{j_1}^{i_1}$ и $r_{j_2}^{i_2}$. Возможны следующие случаи:

1. $j_1 \div n_{s'} = j_2 \div n_{s'}$;
2. $j_1 \div n_{s'} \neq j_2 \div n_{s'}$:
   - 2.1. $j_1 \bmod n_{s'} \neq j_2 \bmod n_{s'}$;
   - 2.2. $j_1 \bmod n_{s'} = j_2 \bmod n_{s'}$:
     - 2.2.1. $i_1 \neq i_2$;
     - 2.2.2. $i_1 = i_2$.

При рассмотрении каждого из этих случаев получаем, что $r_{j_1}^{i_1} \neq r_{j_2}^{i_2}$ при $i_1 \neq i_2$ или $j_1 \neq j_2$. Таким образом, рассмотренное $(\tilde{\Pi}_d, \bar{D}_{s'+1}, k_{s'+1}, n_{s'+1})$-мультипокрытие действительно является различимым циклическим мультипокрытием, а, следовательно, $D_{s'+1}$ порождает в схеме $S_{s'+1}$ слаборазличимое относительно базового множества $D_0^{\frac{n_{s'+1}}{m}}$ $(\tilde{\Pi}_d, k_{s'+1}, n_{s'+1})$-мультипокрытие, что и доказывает утверждение леммы.

Из Леммы 1 следует

Лемма 2. *Если для r-достижимой периодической ПБС $S_m(\Pi_d) \in \Phi_\lambda$ существует циклическое слаборазличимое относительно базового множества цепей D_0 $(\tilde{\Pi}_d, k, m)$-мультипокрытие, T — длина сверхпериода схемы и $T \geqslant 2r$, то при любом $n \geqslant m$ существует диагностическое множество цепей схемы $S_n(\Pi_d)$ мощности, не превосходящей величины* $l_0(d, n, m, k) = \dfrac{2k}{\log_2(m/T)} \log_2 \dfrac{n}{m} + 3k + |D_0|$.

Лемма 3. *Пусть ПБС $S_n \in \Phi_\lambda$ r-достижима и $n \geqslant 5r$. Если D — диагностическое множество цепей для S_n, а $\hat{S}_n \in \hat{\Phi}_\lambda$ — двухполюсная ПБС, полученная из S_n усечением. Тогда для $\hat{S}_n$ существует диагностическое множество цепей $\hat{D}$ такое, что $|\hat{D}| \leqslant |D| + O(\lambda r)$.*

Сформулируем основной результат работы, вытекающий из утверждений 1,2, леммы 2 и леммы 3.

Теорема 1. *Если существует циклическое слаборазличимое относительно базового множества цепей D_0 $(\tilde{\Pi}_d, k, m)$-мультипокрытие, то для двухполюсной периодической n-блочной r-достижимой ПБС $\hat{S}_n(\Pi_d) \in \hat{\Phi}_\lambda$*

со сверхпериодом $\tilde{\Pi}_d$ *длины* T *при* $n \geqslant \max\{m, 5r\}$ *и* $T \geqslant 2r$ *существует единичный диагностический тест размыкания длины* $l^p(\hat{S}_n(\Pi_d)) \leqslant \dfrac{2k}{\log_2(m/T)} \cdot \log_2 \dfrac{n}{m} + 3k + |D_0| + O(\lambda r)$.

Список литературы

1. Чегис И. А., Яблонский С. В. Логические способы контроля работы электрических схем // Труды МИАН СССР. — Т. 51. — С. 270-360.

2. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1979 г.

3. Ложкин С. А. Лекции по основам кибернетики. — М.: Издательский отдел факультета ВМиК МГУ, 2004 г.

4. Романов Д. С. Построение тестов и оценка их параметров для некоторых классов контактных схем. — Дисс. на соиск. уч. ст. к. ф.-м. н. — М.: МГУ, 2000 г. — 114 с.

5. Ложкин С. А., Романов Д. С. Об одном методе построения единичных диагностических тестов для некоторого класса блочных контактных схем. // Труды IV Межд. конф. «Дискретные модели в теории управляющих систем» (19-25 июня 2000 г.). — М.: МАКС Пресс, 2000 г. — С. 114-116.

6. Ложкин С. А., Романов Д. С. О единичных тестах для блочных контакных схем некоторого класса. // Труды VI Межд. конф. «Дискретные модели в теории управляющих систем» (7-11 декабря 2004 г.). — М.: МАКС Пресс, 2004 г. — С. 47-50.

О ПОДМНОЖЕСТВАХ ВЕРШИН БУЛЕВА КУБА, УНИВЕРСАЛЬНЫХ ОТНОСИТЕЛЬНО ПРОЕКЦИЙ

Ф. М. Ковалев (Москва)

Рассмотрим n-мерный булев куб B^n. Он состоит из 2^n вершин, каждая вершина представляется последовательностью $(x_1, ..., x_n)$ из нулей и единиц длины n. Члены этой последовательности называются координатами вершины.

Будем рассматривать проекции вершин на k-мерные грани этого куба. Назовем грань заданную направлениями $i_1, i_2, ..., i_k$ и проходящую через точку с координатами $(0, \ldots, 0)$ канонической k-мерной гранью $\Gamma_{i_1,\ldots,i_k}$. Например, грань $\Gamma_{1,\ldots,k}$ состоит из всевозможных наборов $(\alpha_1, \ldots, \alpha_k, 0, \ldots, 0)$,

где $\alpha_1, \ldots, \alpha_k \in \{0, 1\}$. Число различных наборов в любой грани $\Gamma_{i_1,\ldots,i_k}$ равно 2^k. Любую k-мерную грань $\Gamma_{i_1,\ldots,i_k}$ можно рассматривать как k-мерный булев куб B^k. Проекцией вершины $(x_1, \ldots, x_n)$ n-мерного куба B^n на грань $\Gamma_{i_1,\ldots,i_k}$ называется вершина куба B^k с координатами $(x_{i_1}, \ldots, x_{i_k})$. Проекцией подмножества вершин $\{(x_1^1, \ldots, x_n^1), \ldots, (x_1^m, \ldots, x_n^m)\}$ n-мерного куба B^n на грань $\Gamma_{i_1,\ldots,i_k}$ называется подмножество вершин с координатами $\{(x_(^1 i_1), \ldots, x_(^1 i_n)), \ldots, (x_(^m i_1), \ldots, x_(^m i_n))\}$.

Пусть задано подмножество Σ вершин n-мерного булева куба B^n. Тогда при проецировании его на грань $\Gamma_{i_1,\ldots,i_k}$ получится некоторое подмножество σ вершин k-мерного булева куба B^k. Любое подмножество вершин булевого куба $\Sigma = \{(x_1^1, \ldots, x_n^1), \ldots, (x_1^{|\Sigma|}, \ldots, x_n^{|\Sigma|})\}$ можно задать матрицей M_Σ размера $n \times |\Sigma|$ состоящей из столбцов координат вершин входящих в это подмножество. Эта матрица имеет следующий вид:

$$\begin{pmatrix} x_1^1 & \ldots & x_1^{|\Sigma|} \\ \vdots & \ddots & \vdots \\ x_n^1 & \ldots & x_n^{|\Sigma|} \end{pmatrix}$$

Тогда матрица M_σ подмножества σ, полученного в результате проекции подмножества Σ на грань $\Gamma_{i_1,\ldots,i_k}$, будет выглядеть так:

$$\begin{pmatrix} x_{i_1}^1 & \ldots & x_{i_1}^{|\Sigma|} \\ \vdots & \ddots & \vdots \\ x_{i_k}^1 & \ldots & x_{i_k}^{|\Sigma|} \end{pmatrix}$$

Эта матрица будет иметь размер $k \times |\Sigma|$.

Если различные вершины n-мерного куба B^n проецируются в одну и ту же вершину k-мерного куба B^k, то в матрице M_σ возникают одинаковые столбцы. Если удалить все повторения этих столбцов, то получившаяся матрица M'_σ задает то же множество σ.

Проецирование на грань $\Gamma_{i_1,\ldots,i_k}$ равнозначно выбору k строк с номерами $i_1, \ldots, i_k$ и вычеркиванию остальных с последующим удалением повторений столбцов. Всего имеется $2^{2^k} - 1$ различных непустых подмножеств σ.

Назовем подмножество Σ куба B^n (n, k)-универсальным если среди всех его проекций на канонические k-мерные грани содержатся все возможные $2^{2^k} - 1$ непустые подмножества k-мерного куба B^k. Для всякого k обозначим через $n(k)$ наименьшее число n, для которого в кубе B^n существует хотя бы одно (n, k)-универсальное подмножество вершин.

Основная цель работы состоит в нахождении оценок величины $n(k)$ и в построении соответствующего (n, k)-универсального подмножества вершин в кубе B^n.

Приведем пример. Пусть $k = 1$, тогда $n = 3$ и (n, k)-универсальное подмножество вершин Σ имеет следующий вид:

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

Одномерный булев куб B^1 состоит из двух вершин. Их координаты: (0) и (1). Всего есть три непустых подмножества вершин: $\{(0)\}$, $\{(1)\}$ и $\{(0), (1)\}$. Беря проекции на первое, второе и третье направления, получаем все подмножества одномерного куба.

Простейшие оценки величины $n(k)$ даются в следующем утверждении.

Утверждение 1. *При любом k выполняются неравенства*:

$$\frac{k}{e} 2^{\frac{2^k}{k}} (1 - 2^{-2^k})^{\frac{1}{k}} \leq n(k) \leq k 2^{2^k}.$$

Доказательства этих оценок приведены в леммах 1 и 2.

Обозначим через N число вершин в кубе B^k, $N = 2^k$.

Лемма 1. *Для любого k выполняется неравенство* $\frac{k}{e} 2^{\frac{2^k}{k}} (1 - 2^{-2^k})^{\frac{1}{k}} \leq n(k)$.

Доказательство. Число возможных непустых подмножеств σ не превышает числа канонических граней $\Gamma_{i_1,\ldots,i_k}$. Всего различных непустых подмножеств σ будет $2^N - 1$, а число граней $\Gamma_{i_1,\ldots,i_k}$ равно C_n^k, то есть равно количеству способов выбрать k индексов из n. Следовательно $2^N - 1 \leq C_n^k$. Отсюда:

$$2^N - 1 \leq C_n^k \leq \left(\frac{en}{k}\right)^k.$$

Возводим все в степень $\frac{1}{k}$

$$2^{\frac{N}{k}} (1 - 2^{-N})^{\frac{1}{k}} = (2^N - 1)^{\frac{1}{k}} \leq \frac{en}{k}.$$

Лемма 1 доказана.

Лемма 2. *Для любого k при $n = k(2^N - 1)$ существует (n, k)-универсальное подмножество Σ в кубе B^n.*

Доказательство. Построим такое подмножество Σ. Будем строить матрицу M_Σ задающую Σ. Рассмотрим матрицы M_{σ_i} задающие различные подмножества σ_i, у них разное число столбцов. Число столбцов матрицы M_{σ_i} равно количеству вершин, входящих в подмножество σ_i. Максимальное число столбцов у матрицы задающей подмножество содержащее все вершины,

равно $N = 2^k$. Если в матрицу M_{σ_i}, задающей подмножество σ_i, добавить ее же первый столбец, то получившаяся матрица M'_{σ_i} будет задавать то же подмножество. Чтобы во всех матрицах число столбцов было одинаково дополним все матрицы M_{σ_i} их первыми столбцами до максимального количества столбцов, встречающегося в матрицах, то есть до N, в результате получим матрицы, которые обозначим M'_{σ_i}. Эти матрицы будут одинакового размера $k \times N$ Они будут иметь следующий вид для всех подмножеств σ_i, $i = 1, 2, ..., 2^N - 1$:

$$\underbrace{\begin{pmatrix} x^1_{i,1} & \dots & x^{|\sigma_i|}_{i,1} & x^1_{i,1} & \dots & x^1_{i,1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ x^1_{i,k} & \dots & x^{|\sigma_i|}_{i,k} & x^1_{i,k} & \dots & x^1_{i,k} \end{pmatrix}}_{N}$$

Теперь у нас есть $2^N - 1$ различных матриц M'_{σ_i} размера $k \times N$, задающих все возможные непустые подмножества σ_i. Запишем эти матрицы друг над другом, в результате чего получим матрицу M_Σ размера $k(2^N - 1) \times N$, задающую некоторое подмножество Σ.

$$M_\Sigma = \begin{pmatrix} \begin{pmatrix} x^1_{1,1} & \dots & x^N_{1,1} \\ \vdots & \ddots & \vdots \\ x^1_{1,k} & \dots & x^N_{1,k} \end{pmatrix} \\ \begin{pmatrix} x^1_{2,1} & \dots & x^N_{2,1} \\ \vdots & \ddots & \vdots \\ x^1_{2,k} & \dots & x^N_{2,k} \end{pmatrix} \\ \dots\dots \\ \begin{pmatrix} x^1_{2^N-1,1} & \dots & x^N_{2^N-1,1} \\ \vdots & \ddots & \vdots \\ x^1_{2^N-1,k} & \dots & x^N_{2^N-1,k} \end{pmatrix} \end{pmatrix}$$

Легко видеть, что, вычеркивая строки в матрице M_Σ, можно получить любую из $2^{2^k} - 1$ матриц M'_σ. То есть, получить в проекции подмножества Σ любое подмножество σ. Итак, найдено (n, k)-универсальное подмножество Σ, оно задано на кубе B^n размерности $n = k(2^{2^k} - 1)$. Лемма 2 доказана.

Оценка сверху из леммы 2 получена из очень простого рассуждения и ее можно улучшить, поменяв порядок строк, и выкинув одинаковые строки.

Теорема 1. *Для любого k при $n(k) \le k2^k 2^{\frac{2^k}{k}(c_1 \log(k) + c_2)}$ существует (n, k)-универсальное подмножество Σ в кубе B^n, где c_1 и c_2 некоторые константы.*

Доказательство. Построим (n,k)-универсальное подмножество как в лемме 2. Затем перегруппируем строки в матрице M_Σ из леммы 2 следующим образом: сначала выпишем все первые строки

$$(x^1_{1,1}\dots x^l_{1,1}),\quad (x^1_{2,1}\dots x^l_{2,1}),\quad \dots,\quad (x^1_{C^l_N,1}\dots x^l_{C^l_N,1}),$$

затем все вторые строки

$$(x^1_{1,2}\dots x^l_{1,2}),\quad (x^1_{2,2}\dots x^l_{2,2}),\quad \dots,\quad (x^1_{C^l_N,2}\dots x^l_{C^l_N,2}),$$

и так далее, в конце выпишем все последнии строки

$$(x^1_{1,k}\dots x^l_{1,k}),\quad (x^1_{2,k}\dots x^l_{2,k}),\quad \dots,\quad (x^1_{C^l_N,k}\dots x^l_{C^l_N,k}).$$

Получится новая матрица $M_{\Sigma'}$:

$$\begin{pmatrix} \begin{pmatrix} x^1_{1,1} & \dots & x^l_{1,1} \\ \vdots & \ddots & \vdots \\ x^1_{1,k} & \dots & x^l_{1,k} \end{pmatrix} \\ \begin{pmatrix} x^1_{2,1} & \dots & x^l_{2,1} \\ \vdots & \ddots & \vdots \\ x^1_{2,k} & \dots & x^l_{2,k} \end{pmatrix} \\ \dots\dots \\ \begin{pmatrix} x^1_{C^l_N,1} & \dots & x^l_{C^l_N,1} \\ \vdots & \ddots & \vdots \\ x^1_{C^l_N,k} & \dots & x^l_{C^l_N,k} \end{pmatrix} \end{pmatrix} \to \begin{pmatrix} \begin{pmatrix} x^1_{1,1} & \dots & x^l_{1,1} \\ \vdots & \ddots & \vdots \\ x^1_{C^l_N,1} & \dots & x^l_{C^l_N,1} \end{pmatrix} M_1 \\ \begin{pmatrix} x^1_{1,2} & \dots & x^l_{1,2} \\ \vdots & \ddots & \vdots \\ x^1_{C^l_N,2} & \dots & x^l_{C^l_N,2} \end{pmatrix} M_2 \\ \dots\dots \\ \begin{pmatrix} x^1_{1,k} & \dots & x^l_{1,k} \\ \vdots & \ddots & \vdots \\ x^1_{C^l_N,k} & \dots & x^l_{C^l_N,k} \end{pmatrix} M_k \end{pmatrix}$$

Теперь для получения матриц M'_{σ_j} задающей j-е по порядку множество σ мы вычеркиваем в каждой матрице M_i все строки кроме j-й. То есть из каждой матрицы M_i для построения любой матрицы M'_σ задающей некоторое множество σ мы выбираем только по одной строке. Следовательно если мы выкинем все повторяющиеся строки из каждой матрицы M_i, то полученная матрица тоже будет задавать (n,k)-универсальное множество.

Любую матрицу M_σ можно получить, выбрав нужные столбцы из матрицы M^k_σ, состоящей из всех двоичных столбцов высоты k. Например матрица M^3_σ с лексикографическим порядком столбцов имеет вид:

$$M^3_\sigma = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Мы можем получить любую наперед заданную матрицу M_σ задающую множество из 6 точек выбрав из нее шесть столбцов, задающих координаты

этих точек, например так:

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

Каждая матрица M_i будет состоять из всех комбинаций i-й строки матрицы M_σ^k с выкидыванием различных элементов и добавлением первого из оставшихся элементов количестве равном количеству выкинутых. При этом количество неповторяющихся строк в каждой матрице M_i будет зависеть от вида i-ой строки матрицы M_σ^k.

Легко видеть, что из первой строки матрицы M_σ^3 в результате выкидывания различных элементов и добавления первого из оставшихся элементов количестве равном количеству выкинутых могут получаться только строки вида $\underbrace{00...0}_{a}\underbrace{11...1}_{b}$, где $a \geq 0, b \geq 0$ и $a + b = 2^3$, существует только 9 различающихся строк такого вида. Уже из второй строки матрицы M_σ^3 получаются строки вида $\underbrace{00...0}_{a}\underbrace{11...1}_{b}\underbrace{00...0}_{c}\underbrace{11...1}_{d}$, где $a \geq 0, b \geq 0, c \geq 0, d \geq 0$ и $a+b+c+d = 2^3$, Различных строк такого вида существует C_{8+4-1}^{4-1}, это количество решений уравнения $x_1 + x_2 + ... + x_4 = 8$ в целых числах [1]. В общем случае матрица M_i будет содержать не более $C_{l_i+b_i-1}^{b_i-1}$ неповторяющихся строк, где b_i количество блоков из нулей или единиц в i-й строке матрицы M_σ^k, а l_i длина i-й строки матрицы M_σ^k. В рассмотренном случае $l_i = 2^k$, но можно строить матрицы $M_{m,i}$ для подмножеств состоящих ровно из m точек по отдельности, где $m = 1, ..., 2^k$. Можно показать, что наибольшего значения величина $d_{m,i}$ $m = 1, ..., 2^k$, равная количеству различных строк в матрице M_i для подмножеств состоящих ровно из m точек, достигает при $m = 2^{k-1}$.

Отсюда видно, что чем меньше блоков из нулей и единиц в i-й строке матрицы M_σ^k, тем меньше различных строк будет содержать матрица M_i.

Лемма 3. *Можно так упорядочить столбцы матрицы M_σ^k, которые задают координаты вершин булева куба B^k, что в любой строке $m_\sigma^{k,i}$ матрицы M_σ^k будет не более чем $\frac{2^{k+1}}{k} + 1$ блоков из нулей или единиц. То есть для любого i будет справедливо неравенство $b_i \leq \frac{2^{k+1}}{k} + 1$, где b_i — количество блоков в i-й строке.*

Доказательство этой леммы, использующее некоторые свойста кодов Грэя [2], опущено ввиду недостатка места.

Имея оценку $b_i \leq \frac{2^{k+1}}{k} + 1$, числа блоков в матрице M_i, можно подставить верхнее значение для b_i в формулу оценки числа неповторяющихся строк $C_{l_i+b_i-1}^{b_i-1}$, учтя так же, что наибольшее количество строк в

матрице M_i для подмножеств состоящих ровно из m точек, будет при $m = 2^{k-1}$, а $l_i = m$, и сделав ряд преобразований получаем верхнюю оценку $n(k) \leq k2^k 2^{\frac{2^k}{k}(c_1 \log(k)+c_2)}$.

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

Список литературы

1. Комбинаторный анализ: задачи и упражнения. Под редакцией К. А. Рыбникова. — М.: Наука, 1982.

2. Берлекэмп Э. Алгебраическая теория кодирования — М.: Мир, 1971.

3. Родионов С. Г. дипломная работа (мех-мат ф-т МГУ, 1996г.)

ФРАКТАЛЬНЫЕ ГРАФЫ И ИХ СВОЙСТВА

А. А. Кочкаров (Москва)

Современные исследования сложных систем таких, как информационные, электроэнергетические, WWW (Internet), сети научного сотрудничества показывают, что структуры этих систем по истечении времени претерпевает определенные изменения, вызываемые различными внешними обстоятельствами. Структуру системы, произвольной природы (социальной, социально-экономической, технической, химико-биологической и т.п.) можно представить в виде графа. Граф [1] – это абстрактный объект, как правило, вершины графа соответствуют элементам системы, а ребра - связям между элементами этой системы. Изменения, происходящие в структуре сложной системы, могут быть описаны простейшими теоретико-графовыми операциями [1]: стягивание ребра, удаление (добавление) ребра, удаление (добавление) вершины. Изменения структуры системы могут быть разовыми, а могут быть постоянными. Для второго случая, разумно, ввести понятие *структурной динамики* – изменение структуры системы с течением времени. Несомненно, для описании структурной динамики лучше всего подходит аппарат теории графов.

Одним из наиболее распространенных сценариев структурной динамики является *рост структуры*. Рост структуры – это регулярное появление

новых элементов и связей в структуре системы. Рост структуры может происходит по строго сформулированным правилам, не исключая наличие в них фактора случайности.

Исследование структурной динамики, как модели изменчивости связей информационных сетей и систем, представляется важной актуальной задачей. Изменение структуры информационных систем (сетей), вызванное выходом из строя элементов этой системы (сети), некоторым негативным образом отразится на ее качественных и количественных характеристиках. Положение некоторых элементов в структуре информационной (коммуникационной) сети могут оказаться более значимыми чем у остальных, поскольку выход из строя таких элементов в состоянии существенно ухудшить функционирование всей сети. При росте информационной сети важно не допускать появление таких связей и элементов, и целых подструктур (набор взаимодействующих элементов системы (сети)). Это задача усложняется тем, что с одной стороны рост – динамическое развитие можно наблюдать во многих "местах" сети одновременно. С другой стороны, нелегко распознать правила такого роста –"время и место" появления новых элементов и связей в сети. Вообще говоря, возможны различные правила структурной динамики.

В настоящей работе рассматривается одно из возможных правил задающих структурную динамику сложных информационных сетей. Формальным представлением изменения структур информационных сетей по этому правилу являются масштабно-инвариантные или самоподобные [2] графы большой размерности, называемые *фрактальными (предфрактльные)*. Правила порождения предфрактального графа позволяют прогнозировать и оценивать его качественные и количественные характеристики. Это позволило заложить основы нового метода проектирования и анализа сложных многоэлементных структур. Метод базируется на свойстве самоподобия фрактальных графов. Использование свойства самоподобия дает возможность "программирования" предфрактального графа, наделения его требуемыми характеристиками и свойствами. При этом особенно важным представляется рассмотрение и числа "окон уязвимости" – точек сочленения и мостов [1] предфрактального графа. Доказанные в работе теоремы устанавливают зависимость характеристик всего предфрактального графа от характеристик его самой меньшей несамоподобной части – затравки, что позволяет оценить число и диапазон "окон уязвимости".

Фрактальные графы [3,4] используются для моделирования структур растущих по одним и тем же правилам, независимо от точки роста. Не исключается множественный одновременный рост во всей структуре системы (информационной сети). Формальным отражением этих правил является операция *замены вершины затравкой* (ЗВЗ) [3,4], она же и лежит в основе определения фрактальных графов.

Термином *затравка* условимся называть какой-либо связный граф $H = (W, Q)$. Суть операции ЗВЗ заключается в следующем. В данном графе $G = (V, E)$ у намеченной для замещения вершины $\tilde{v} \in V$ выделяется множество $\widetilde{V} = \{\tilde{v}_j\}$, $j = 1, 2, ..., \left|\widetilde{V}\right|$, смежных ей вершин. Далее из графа G удаляется вершина $\tilde{v}$ и все инцидентные ей ребра. Затем каждая вершина $\tilde{v}_j \in \widetilde{V}$, $j = 1, 2, ..., \left|\widetilde{V}\right|$, соединяется ребром с одной из вершин затравки $H = (W, Q)$. Вершины соединяются произвольно (случайным образом) или по определенному правилу, при необходимости.

Предфрактальный граф будем обозначать через $G_L = (V_L, E_L)$, где V_L - множество вершин графа, а E_L – множество его ребер. Определим его рекуррентно, поэтапно, заменяя каждый раз в построенном на предыдущем этапе $l = 1, 2, ..., L-1$ графе $G_l = (V_l, E_l)$ каждую его вершину затравкой $H = (W, Q)$. На этапе $l = 1$ предфрактальному графу соответствует затравка $G_1 = H$. Об описанном процессе говорят, что *предфрактальный граф* $G_L = (V_L, E_L)$ *порожден затравкой* $H = (W, Q)$. Процесс порождения предфрактального графа G_L, по существу, есть процесс построения последовательности предфрактальных графов $G_1, G_2, ..., G_l, ..., G_L$, называемой *траекторией*. Фрактальный граф $G = (V, E)$, порожденный затравкой $H = (W, Q)$, определяется бесконечной траекторией. Ранг L, фактически, определяет "возраст" (число этапов порождения) и размер (число вершин) предфрактального графа.

Использование операции ЗВЗ в процессе порождения предфрактального графа G_L, для элементов $G_l = (V_l, E_l)$, $l \in \{1, 2, ..., L-1\}$, его траектории позволяет ввести отображение $\varphi : V_l \to V_{l+1}$ или $\varphi(V_l) = V_{l+1}$, а в общем виде

$$\varphi^t(V_l) = V_{l+t}, \quad t = 1, 2, ..., L-l. \tag{1}$$

В этом выражении множество V_{l+t} – образ множества V_l, а множество V_l – прообраз множества V_{l+t}.

Для предфрактального графа G_L, ребра, появившиеся на l-ом, $l \in \{1, 2, ..., L\}$, этапе порождения, будем называть *ребрами ранга* l. *Новыми ребрами* предфрактального графа G_L назовем ребра ранга L, а все остальные ребра назовем - *старыми*.

Если из предфрактального графа G_L, порожденного n-вершинной затравкой H, последовательно удалить все старые ребра (ребра ранга l, $l = 1, 2, ..., L-1$), то исходный граф распадется на множество связных компонент $\left\{B_L^{(1)}\right\}$, каждая из которых изоморфна [1] затравке H. Множество компонент $\left\{B_L^{(1)}\right\}$ будем называть *блоками первого ранга*. Аналогично, при удалении из предфрактального графа G_L всех старых ре-

бер рангов $l = 1, 2, ..., L-2$, получим множество блоков $\left\{B_L^{(2)}\right\}$ *второго ранга*. Обобщая, скажем, что при удалении из предфрактального графа G_L всех ребер рангов $l = 1, 2, ..., L-r$, получим множество $\left\{B_{L,i}^{(r)}\right\}$, $r \in \{1, 2, ..., L-1\}$, блоком *r-го ранга*, где $i = 1, 2, ..., n^{L-r}$ – порядковый номер блока. Блоки $B_L^{(1)} \subseteq G_L$ первого ранга также будем называть *подграф-затравками* H предфрактального графа G_L.Очевидно, что всякий блок $B_L^{(r)} = \left(U_L^{(r)}, M_L^{(r)}\right)$, $r \in \{1, 2, ..., L-1\}$, является предфрактальным графом $B_r = (U_r, M_r)$, порожденным затравкой H.

$$\varphi^t(v_j) = U_{l+t,j}^{(t)}, \tag{2}$$

Для любой вершины $v_j \in V_l$, $j \in \{1, 2, ..., n^l\}$, предфрактального графа $G_l = (V_l, E_l)$, $l \in \{1, 2, ..., L-1\}$, из траектории графа G_L, справедливо

$$\varphi^t(v_j) = B_{l+t,j}^{(t)}, \quad \text{где} \quad B_{l+t,j}^{(t)} = \left(U_{l+t,j}^{(t)}, M_{l+t,j}^{(t)}\right) \subseteq G_{l+t}, \quad t = 1, 2, ..., L-l.$$

Аналогично,

$$\varphi^t\left(U_{l,i}^{(r)}\right) = U_{l+t,i}^{(r+t)}, \tag{3}$$

$$\varphi^t\left(B_{l,i}^{(r)}\right) = B_{l+t,i}^{(r+t)}, \quad r \in \{1, 2, ..., L-t\}, \quad i \in \{1, 2, ..., n^{l-r}\}.$$

Два блока предфрактального графа назовем *смежными*, если существует ребро, вершины которого принадлежат различным блокам. Не требует доказательства тот факт, что блоки предфрактального графа смежны тогда и только тогда, когда смежны их прообразы.

Обобщением описанного процесса порождения предфрактального графа G_L является такой случай, когда вместо единственной затравки H используется множество затравок $\mathcal{H} = \{H_t\} = \{H_1, H_2, ..., H_t, ..., H_T\}$, $T \geq 2$. Суть этого обобщения состоит в том, что при переходе от графа G_{l-1} к графу G_l каждая вершина замещается некоторой затравкой $H_t \in \mathcal{H}$, которая выбирается случайно или согласно определенному правилу, отражающему специфику моделируемого процесса или структуры.

Термином *подграф-затравка* $z_s^{(l)}$ будем называть блок $B_{l,s}^{(1)}$, $s = \overline{1, n^{l-1}}$, первого ранга предфрактального графа G_l, $l = \overline{1, L}$ из траектории. Последовательное выделение подграф-затравок $z_s^{(l)}$ на графах $G_1, G_2, ..., G_L$ из траектории предфрактального графа G_L разбивает множество ребер E_L на непересекающиеся подмножества подграф-затравок $Z(G_L) = \left\{z_s^{(l)}\right\}$,

$l = \overline{1,L}$, $s = \overline{1,n^{l-1}}$. Такое разбиение на подмножества позволит нам сохранить информацию смежности старых ребер на момент их появления в предфрактальном графе. В траектории переход от графа G_{l-1} к G_l осуществляется $|V_{l-1}| = n^{l-1}$ операциями ЗВЗ, поэтому общее число использованных затравок в порождении предфрактального графа G_L равно $1 + n + n^2 + ... + n^{L-1} = \frac{n^L-1}{n-1}$. Тогда мощность множества $Z(G_L)$ всех подграф-затравок из траектории графа G_L также равно $Z(G_L) = \frac{n^L-1}{n-1}$.

Предфрактальный граф $G_L = (V_L, E_L)$ условимся называть (n, q, L)-графом, если он порожден n-вершинной q-реберной затравкой $H = (W, Q)$.

Число точек сочленения графа $H = (W, Q)$обозначим через $m(H)$.

ТЕОРЕМА 1. *Для всякого предфрактального (n, q, L)-графа G_L, порожденного затравкой $H = (W, Q)$, справедливы верхняя и нижняя оценки числа точек сочленения $m(H)n^{L-1} \le m(G_L) \le m(H)n^{L-1} + \frac{n^L-n}{n-1}$, если смежность старых ребер одного ранга не нарушается.*

Число мостов графа $H = (W, Q)$ обозначим через $k(H)$.

ТЕОРЕМА 2. *Для всякого предфрактального (n, q, L)-графа $G_L = (V_L, E_L)$ порожденного затравкой $H = (W, Q)$, справедливы верхняя и нижняя оценки числа мостов: $k(H) \le k(G_L) \le k(H)\frac{n^L-n}{n-1}$.*

ТЕОРЕМА 3. *Число всех предфрактальных графов L-го ранга, порожденных затравкой $H = (W, Q)$, $|W| = n$, $|Q| = q$, равно $n^{2q\frac{n^L+L(1-n)-1}{(n-1)^2}}$.*

Динамические системы, имеющие *конечный горизонт прогноза,* принято называть *системами с хаотическим поведением* [2]. Траектории системы с хаотическим поведением с близкими начальными данными "разбегаются" экспоненциально, а поэтому для таких систем долгосрочный прогноз невозможен.

Для анализа работоспособности системы с динамически меняющейся структурой необходимо прогнозирование поведение структуры этой системы. Для этого иногда достаточно просмотреть все возможные варианты изменений в структуре, и сравнить их количественные оценки. В нашем случае – фрактальные графы, динамически растущие структуры, причем рост структуры, т.е. увеличение числа вершин предфрактального графа, происходит очень быстро. Число всевозможных предфрактальных графов одного ранга, порожденного одной и той же затравкой, как свидетельствует теорема 3, зависит экспоненциально от числа вершин самого предфрактального графа. Структурную динамику такого рода, по аналогии с системами с хаотическим поведением, назовем *структурным хаосом.* На первый взгляд, такое свойство может привести к мысли о невозможности получения хоть сколько-нибудь полезных, т.е. полиномиальных, количественных оценок для характеристик предфрактального графа. О том, что это не так, говорят результаты, представленные в настоящей главе (см. теоремы 1-2). И действительно, количественные оценки, полученные в работе, ограничены

сверху полиномами $O(N)$ от числа N – вершин предфрактального графа, в то время как число всех предфрактальных графов с N – вершинами ограничено сверху экспонентой $O(n^{N+1})$, где n – число вершин затравки (см. теорему 3).

Основная цель настоящей работы - продемонстрировать возможность получения "хороших" диапазонов количественных оценок, связанных со стойкостью, для несравнимо большего числа предфрактальных графов.

Подводя итог, можно сказать, что использование архитектур компьютерных сетей, систем сетевой связи, информационных и коммуникационных сетей реализующих предфрактальные графы, дает ряд важных преимуществ с точки зрения обеспечения *структурной стойкости* таких объектов к внешним воздействиям и внутренним поломкам.

Работа выполнена при финансовой поддержке РФФИ (проект № 07-01-00618)и РГНФ (проект № 05-03-03188).

Список литературы

1. Емеличев В.А., Мельников О.И., Сарванов В.И., Тышкевич Р.И. Лекции по теории графов. — М.: Наука, 1990.

2. Ахромеева Т.С., Курдюмов С.П., Малинецкий Г.Г., Самарский А.А. Нестационарные структуры и диффузионный хаос. — М.: Наука, 1992.

3. Кочкаров А.М. Распознавание фрактальных графов. Алгоритмический подход. – Нижний Архыз: РАН САО, 1998.

4. Кочкаров А.А., Кочкаров Р.А. Параллельный алгоритм поиска кратчайшего пути на предфрактальном графе // Журнал вычисл. матем. и матем. физики. – 2004. – Т. 44, № 6. – С. 1157-1162.

ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ им. М. В. КЕЛДЫША
РОССИЙСКОЙ АКАДЕМИИ НАУК

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

МАТЕРИАЛЫ
VI МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

(Москва, 16–21 апреля 2007 г.)

ЧАСТЬ II

Москва 2007

МАТЕРИАЛЫ
VI МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

(Москва, 16–21 апреля 2007 г.)

ЧАСТЬ II

Москва 2007

М34
УДК 519.7

Издание осуществлено при поддержке Российского фонда фундаментальных исследований по проекту 07–01–06018

М34 Материалы VI молодежной научной школы по дискретной математике и ее приложениям (Москва, 16–21 апреля 2007 г.). Часть II. Под редакцией А. В. Чашкина. 2007. — 52 с.

Сборник содержит материалы VI молодежной научной школы по дискретной математике и ее приложениям, проходившей в Москве с 16 по 21 апреля 2007 г. при поддержке Российского фонда фундаментальных исследований (проект 07–01–06018). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание
МАТЕРИАЛЫ
VI МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ
(Москва, 16–21 апреля 2007 г.)

Под общей редакцией А. В. ЧАШКИНА

Ответственный за выпуск *Ф. М. Ковалев*

СОДЕРЖАНИЕ

НЕКОТОРЫЕ СВОЙСТВА АЛГЕБР, СОДЕРЖАЩИХ ПОДАЛГЕБРУ, ИЗОМОРФНУЮ АЛГЕБРЕ МАТРИЦ

В. Б. Ларионов (Москва)

Одной из интересных и тяжёлых задач является задача умножения матриц. Её история начинается с замечательного результата Штрассена. Он показал в [5], что две квадратные матрицы размера 2 можно умножить, используя только 7 умножений линейных комбинаций элементов матриц, что повлекло за собой асимптотическую оценку $n^{\log_2 7}$ на количество умножений. Этот результат неоднократно улучшался (историю этого можно посмотреть в [7] и остановился на $O(n^{2.38})$ в работе [4] более пятнадцати лет назад.

В [2] показано, что для задачи умножения матриц может быть использована идея "расширения модели". Для этого нам понадобится несколько определений.

Определение. *Алгеброй называется линейное пространство с заданной на нём операцией умножения, линейной по обоим сомножителям.*

Определение. *Алгебра P называется алгеброй с простым умножением, если существует базис $e_1, e_2, \ldots, e_k$ в P и подстановка σ порядка k такие, что $e_i e_j = 0$ при $j \neq \sigma(i)$.*

В данном случае метод "расширения модели"приводит нас к задаче поиска алгебры с простым умножением, содержащей подалгебру матриц ([2]) и удовлетворяющей тому, что линейная оболочка строк её таблицы умножения ([1]) есть в точности подалгебра матриц (это следует из утверждения, доказанного в [6]). В данной работе будут построены все 7-мерные алгебры с простым умножением, содержащие подалгебру матриц размера 2 на 2 при условии наличия на всей алгебре антиавтоморфизма.

Пусть P — 7-мерная алгебра, $M \subset P$ – подалгебра, изоморфная алгебре квадратных матриц размера 2 на 2.

Определение. *Пусть вектору $f \in M$ при отображении из алгебры в матрицы соответствует матрица M_f размера 2 на 2. Тогда весом матрицы M_f будем называть количество ненулевых координат вектора f.*

Итак, предположим, что на P есть антиавтоморфизм Ψ, удовлетворяющий свойству линейности и соотношению

$$\Psi^2 = e, \tag{1}$$

где e — тождественное отображение.

Следующие технические леммы приведём без доказательства, поскольку они очень громоздкие (все они опираются на свойства алгебры матриц и антиавтоморфизмов, которые можно найти в [3]).

Лемма 1. *Все собственные значения описанного выше антиавтоморфизма Ψ равны ± 1, и Ψ имеет полный набор собственных векторов. Кроме того, n линейно независимых собственных векторов лежат в M.*

Лемма 2. *Не существует линейного антиавтоморфизма Ψ, на алгебре квадратных матриц размера 2 на 2 M такого, что выполнено (1) и собственное значение данного антиавтоморфизма λ_0 ($\lambda_0 = \pm 1$) имеет кратность 3, а $(-\lambda_0)$ — кратность 1, и собственное подпространство, отвечающее $(-\lambda_0)$ имеет базисом матрицу M_0 ранга 1.*

Линейную оболочку векторов $v_1, \ldots, v_n$ будем обозначать $\ell(v_1, \ldots, v_n)$, а подпространство матриц размера 2 на 2, у которых оба собственных значения нулевые, обозначим L_0. Несложно проверить, что размерность L_0 равна 3.

Лемма 3. 1) *Не существует антиавтоморфизма Ψ на алгебре квадратных матриц размера 2 на 2 такого, что выполнено (1), у Ψ есть двухмерное собственное подпространство L с собственным значением α, натянутое на две матрицы H_1, H_2 ранга 1.*

2) *Если расширять L, добавляя матрицу H_3 ранга 1 (линейно независимую с H_1, H_2), чтобы существовал антиавтоморфизм Ψ с собственным подпространством $L \oplus \ell(H_3)$ (где "$\oplus$" означает прямую сумму подпространств) с собственным значением α, то в случае $\alpha = -1$ $L \oplus \ell(H_3) = L_0$, а в случае $\alpha = 1$ $L \oplus \ell(H_3) = L_1 = \ell\left(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}\right)$ (с точностью до изоморфизма).*

3) *В предыдущем пункте в случае подпространства L_0 в некотором базисе*

$$\Psi = \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}, \tag{2}$$

а в случае L_1 :

$$\Psi = \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} a & -c \\ -b & d \end{bmatrix}. \tag{3}$$

Будем обозначать эти антиавтоморфизмы соответственно Ψ_0 и Ψ_1.

Пусть $\{e_i\}_{i=0}^{6}$ — базис P из определения алгебры с простым умножением. Будем предполагать, что такой базис единственный. Тогда

$$\Psi(e_i) = e_{\beta(i)} c_i,$$

где β — перестановка на множестве $\{0,\dots,6\}$, c_i — некоторые константы.

Из (1) следует, что перестановка β состоит только из неподвижных элементов и циклов длины 2.

Определим теперь класс антиавтоморфизмов, который мы будем исследовать. Вначале рассмотрим случай, когда 3 собственные значения автоморфизма, не относящиеся к подалгебре M (лемма 1) равны между собой и равны α. Соответствующее 3-мерное собственное подпространство обозначим M'.

Лемма 4. 1) *В β есть хотя бы один цикл длины* 2.

2) *При сделанном выше предположении у β есть как минимум* 2 *цикла длины* 2.

Итак, по лемме 4 у перестановки β будет как минимум 2 цикла длины 2. Пусть это (12)(34), тогда:

$$e_1 = g_1 + m_1, \quad e_2 = g_1 + \alpha\Psi(m_1), \quad e_3 = g_2 + m_2, \quad e_4 = g_2 + \alpha\Psi(m_2),$$

где $g_i \in M'$, $m_i \in M$. Обозначим

$$h_i = m_i - \alpha\Psi(m_i).$$

Будем обозначать H_i матрицу, соответствующую вектору h_i при вложении в алгебру. Предположим, что у перестановки β 3 неподвижных элемента. Тогда антиавтоморфизм Ψ обладает двухмерным собственным подпространством, с собственным значением $(-\alpha)$ натянутым на матрицы H_1 и H_2 (очевидно, они линейно независимы). Это следует из того факта, что у Ψ собственное подпространство с собственным значением α $\ell(e_0, e_5, e_6, e_1 + e_2, e_3 + e_4)$ размерности 5. Но матрицы H_i веса 2, ранга 1. Получаем противоречие с леммой 3.

Следовательно, $\beta = (0)(12)(34)(56)$ и

$$e_5 = g_3 + m_3, \quad e_6 = g_3 + \alpha\Psi(m_3), \quad h_3 = m_3 - \alpha\Psi(m_3).$$

Перенумеруем базисные вектора так, чтобы

$$h_1 = [0,1,0,0,0,0,-1],\ h_2 = [0,0,1,0,0,-1,0],\ h_3 = [0,0,0,1,-1,0,0]. \quad (4)$$

Рассмотрим вначале случай $\alpha = 1$.

В этом случае по лемме 3 $H_1 \sim H_2 \sim H_3 \sim \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

Лемма 5. *В этом случае с точностью до изоморфизма возможна только одна алгебра, задаваемая таблицей умножения:*

$$\begin{array}{ll} e_0e_0 & f_e \\ e_1e_2 & h_1h_2 \\ e_2e_3 & h_2h_3 \\ e_3e_1 & h_3h_1 \\ e_4e_5 & h_3h_2 \\ e_5e_6 & h_2h_1 \\ e_6e_4 & h_1h_3. \end{array} .$$

Доказательство. Заметим, что $H_i^2 = 0$ $(i = 1, 2, 3)$.

Поскольку P — алгебра с простым умножением, а H_i — матрицы веса 2, то для каждого i найдутся j, k такие, что $H_iH_j = 0$ и $H_kH_i = 0$ $(i, j, k = 1, 2, 3)$. Причём, так как мы предположили, что базис $\{e_i\}_{i=1}^7$ — единственный, то такие номера j, k для каждого i будут тоже единственными. В данном случае $i = j = k$. Следовательно,

$$H_iH_j \neq 0 \text{ при } i \neq j, \tag{5}$$

поэтому произведения базисных векторов вида e_0e_i, e_ie_0, e_ie_i $(i > 0)$ обязаны равняться нулю, иначе легко понять, что условие выше нарушиться. Заметим, что (5) верно для любых матриц из L_0 ранга 1.

Простыми рассуждениями легко понять, что для обеспечения условия (5), перестановка σ обязана иметь два цикла длины 3, то есть можно занумеровать вектора базиса так, что $\sigma = (0)(123)(456)$ (при этом можно сохранить условие (4)). Также очевидно, чему будут равняться произведения $e_ie_{\sigma(i)}$ $(i > 0)$.

Докажем, что при некотором масштабировании вектора e_0 произведение e_0e_0 будет равно единичной матрице. Пусть вектор из алгебры, соответствующий единичной матрице

$$f_e = [a, b, c, d, d, c, b] .$$

Это общий случай для вектора, для которого выполнено $\Psi_0(f_e) = f_e$.

$$f_e^2 = a^2e_0e_0 + bch_1h_2 + cdh_2h_3 + dbh_3h_1 + dch_3h_2 + cbh_2h_1 + bdh_1h_3 =$$

$$= a^2e_0e_0 + bc(h_1h_2 + h_2h_1) + cd(h_2h_3 + h_3h_2) + bd(h_1h_3 + h_3h_1).$$

Из первого пункта леммы 3 следует, что $h_ih_j + h_jh_i = const\ E$ для $i \neq j$. Пусть

$$H_1H_2 + H_2H_1 = \alpha E,$$

$$H_1H_3 + H_3H_1 = \beta E,$$

$$H_2H_3 + H_3H_2 = \gamma E.$$

Домножим h_i (то есть, соответствующие базисные вектора e_i и e_{7-i}) $i = 1, 2, 3$ на соответственно

$$-\sqrt{\frac{\alpha\beta}{\gamma}},\ -\sqrt{\frac{\alpha\gamma}{\beta}},\ -\sqrt{\frac{\beta\gamma}{\alpha}}.$$

Очевидно, после этой операции будет справедливо

$$H_iH_j + H_jH_i = -E \quad i \neq j.$$

С учётом этого

$$f_e^2 = a^2 e_0 e_0 - f_e(bc + cd + bd) = f_e,$$

$$e_0 e_0 = f_e \frac{1 + bc + cd + bd}{a^2}.$$

Понятно, что $a \neq 0$ (иначе M построено на $e_1, \ldots, e_6$). Осталось масштабировать e_0 так, чтобы

$$a^2 = 1 + bc + cd + bd.$$

Пользуясь доказанными леммами 3 и 6, легко получить следующую таблицу для алгебры:

$$\begin{array}{lccccccc}
e_0e_0 & 2 & -1 & -1 & -1 & -1 & -1 & -1 \\
e_1e_2 & -1 & 0 & 0 & 1 & 0 & 1 & 1 \\
e_2e_3 & -1 & 1 & 0 & 0 & 1 & 1 & 0 \\
e_3e_1 & -1 & 0 & 1 & 0 & 1 & 0 & 1 \\
e_4e_5 & -1 & 0 & 1 & 1 & 0 & 0 & 1 \\
e_5e_6 & -1 & 1 & 1 & 0 & 1 & 0 & 0 \\
e_6e_4 & -1 & 1 & 0 & 1 & 0 & 1 & 0.
\end{array} \tag{6}$$

Случай $\alpha = -1$ аналогичным образом даёт алгебру:

$$\begin{array}{lccccccc}
e_0e_0 & 0 & 1 & 0 & -1 & 1 & 0 & -1 \\
e_1e_5 & -1 & 0 & 0 & 1 & 0 & 1 & 1 \\
e_2e_6 & 1 & -1 & -1 & 0 & -1 & 0 & 0 \\
e_3e_4 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\
e_4e_2 & -1 & 0 & 1 & 1 & 0 & 0 & 1 \\
e_5e_3 & 1 & -1 & 0 & 0 & -1 & -1 & 0 \\
e_6e_1 & 0 & -1 & 0 & 0 & 0 & 0 & 1.
\end{array} \tag{7}$$

А случай, когда антиавтоморфизм имеет собственные значения разных знаков на M':

$$\begin{array}{lccccccc}
e_0e_0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
e_1e_1 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\
e_2e_2 & 0 & 0 & 1 & 0 & 0 & -1 & 0 \\
e_3e_3 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\
e_4e_5 & -1 & -1 & 0 & 0 & -1 & -1 & 0 \\
e_5e_6 & -1 & 0 & -1 & 0 & -1 & 0 & -1 \\
e_6e_4 & -1 & 0 & 0 & -1 & 0 & -1 & -1.
\end{array} \qquad (8)$$

Итак, доказана следующая

Теорема 1. *При условии наличия антиавтоморфизма существует ровно три неизоморфные 7-мерные алгебры, содержащие подалгебры матриц размера 2 на 2, задаваемые таблицами* (6), (7), (8).

Список литературы

1. Алексеев В. Б., Ларионов В. Б. О расширениях с простым умножением для алгебры матриц. // Труды VII международной конференции "Дискретные модели в теории управляющих систем", М. 2006 С. 17–22.

2. Алексеев В. Б. Минимальные расширения с простым умножением для алгебры матриц второго порядка. // Дискретная математика, 1997, т.9, № 1. С. 71–82.

3. Маркус М., Минк Х. Обзор по теории матриц и матричных неравенст. //М. Едиториал УРСС. 1994. 232 с.

4. Coppersmith D., Winograd S. Matrix multiplication via arithmetic progression. //J. Symb. Comp., 1990, 9, 251–280.

5. Strassen V. Gaussian elimination is not optimal. //Numer. Math., 1969, v.13, 454–456.

6. Плукас М. О некоторых свойствах алгебр с простым умножением, содержащих ассоциативные подалгебры. //Дискретная математика, 1997, № 2, С. 79–90.

7. Алексеев В.Б. Сложность умножения матриц. Обзор. //кибернетический сборник М.: Мир, 1988, № 25, С. 189–236.

ОЦЕНКА НЕЛИНЕЙНОСТИ ВЫСОКИХ ПОРЯДКОВ БУЛЕВОЙ ФУНКЦИИ ЧЕРЕЗ ЗНАЧЕНИЕ ЕЕ АЛГЕБРАИЧЕСКОЙ ИММУННОСТИ

М. С. Лобанов (Москва)

С появлением "алгебраических" атак (см. например [2,5]) на потоковые шифры от булевых функций, используемых в этих криптографических схемах в качестве нелинейных фильтров, наряду с другими стало требоваться и условие обладания высокой алгебраической иммунностью. В связи с этим возник вопрос, как связана алгебраическая иммунность с другими важными криптографическими свойствами булевых функций.

В работе [3] был доказан результат, эквивалентный следующей оценке на нелинейность r-ого порядка:

$$nl_r(f) \geq \sum_{i=0}^{k-r-1} \binom{n}{i}.$$

Позже в [4] нами была доказана нижняя оценка нелинейности (r=1) функции через значенниее ее алгебраической иммунности:

$$nl(f) \geq 2\sum_{i=0}^{k-2} \binom{n-1}{i}.$$

И там же для всех допустимых значений алгебраической иммунности были построены функции, на которых достигается равенство в приведенной оценке.

Еще позднее C.Carlet в [1] обобщил доказанную нами оценку на случай других r:

$$nl_r(f) \geq 2\sum_{i=0}^{k-r-1} \binom{n-r}{i}.$$

Отметим, что ни одна из двух приведенных выше оценок для нелинейности r-ого порядка не влечет другую.

В данной работе мы покажем, что задача получения оценки нелинейность r-ого порядка через значение алгеброической иммунности полностью сводиться к оценки размерности определенного линейного пространства. И как следствие из этого получим новую оценку, перекрывающую обе существовавшие ранее.

Известно, что булева функция единственным образом представляется полиномом.

Определение. *Степенью булевой функции называется длина самого длинного слагаемого в ее полиноме (количество переменных в этом слагаемом).*

Определение. *Булева функция g над F_2^n называется аннигилятором булевой функции f над F_2^n, если $fg = 0$.*

Очевидно, что аннигиляторы f образуют линейное подпространство в пространстве всех булевых функций от n переменных.

Определение. *Алгебраической иммунностью $AI(F)$ булевой функции f над F_2^n называется степень булевой функции g над F_2^n, где g не равная тождественно нулю функция с минимальной степенью, такая что $fg = 0$ или $(f+1)g = 0$.*

Известно [2, 5], что для любой f над F_2^n выполнено $AI(f) \leq \lceil \frac{n}{2} \rceil$.

Определение. *Весом $wt(x)$ набора x из F_2^n называется число единиц в x.*

Определение. *Расстояние между булевыми функциями f_1 и f_2 определяется как $d(f_1, f_2) = \mid \{x \in F_2^n \mid f_1(x) \neq f_2(x)\} \mid$.*

Определение. *Нелинейностью r-того порядка $nl_r(f)$ булевой функции f над F_2^n называется $\min\limits_{l,\ deg(l) \leq r} d(f, l)$.*

Определение. *Пусть h булева функция от n переменны. Обозначим через $An_k(h)$ линейное пространство аннигиляторов степени не выше k и через $d_{k,h}$ его размерность.*

Определение. *Пусть $C = \{\overline{x}_1, \ldots, \overline{x}_n\}$ множество двоичных наборов длины n. При любого $k \leq n$, произвольному набору $x = (x_1, \ldots, x_n)$ можно сопоставить однородное линейное уравнение, получаемое подстановкой компонент набора в*

$$a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j + \cdots + \sum_{1 \leq i_1 \leq \ldots \leq i_k \leq n} a_{i_1 \ldots i_k} x_{i_1} \ldots x_{i_k}$$

и приравниванием полученного выражения к 0. Тогда назовем k-рангом множества C ранг системы линейных уравнений, полученных таким образом из наборов множества C. Обозначим его через $r_k(C)$.

Ищем для функции f аннигиляторы степени не выше k методом неопределенных коэффициентов:

$$g = a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j + \cdots + \sum_{1 \leq i_1 \leq \ldots \leq i_k \leq n} a_{i_1 \ldots i_k} x_{i_1} \ldots x_{i_k}.$$

Функция g является аннигилятором f тогда и только тогда, когда $f(x) = 1$ влечет $g(x) = 0$. Получаем систему линейных уравнений.

Несложно заметить, что $d_{k,f} = dim(An_k(f)) = \sum_{i=0}^{k} \binom{n}{i} - r_k(supp(f))$.

Утверждение 1. *Пусть f и f_0 функции от n переменных, $AI(f_0) \geq k$. Тогда $d(f, f_0) \geq dim(An_{k-1}(f)) + dim(An_{k-1}(f+1))$.*

Доказательство. Так как $AI(f_0) \geq k$, то $r_{k-1}(supp(f_0)) = \sum_{i=0}^{k-1} \binom{n}{i}$.

В тоже время $r_{k-1}(supp(f)) = \sum_{i=0}^{k-1} \binom{n}{i} - d_{k-1,f}$. Следовательно, существует не меньше чем $d_{k-1,f}$ наборов, где f_0 равна единице, а f нулю.

Аналогично рассматриваем $f + 1$ и $f_0 + 1$, получаем оценку на число наборов, где f единица, а f_0 ноль.

Определение. *Пусть h булева функция от n переменных. Обозначим через $B_k(h)$ линейное пространство функций от n переменных степени не выше k, которые при умножении на h снова дают функции степени не выше k.*

Утверждение 2. *Сумма $dim(An_k(f))$ и $dim(An_k(f+1))$ равна $dim(B_k(f))$.*

Доказательство. Рассмотрим пару (g_1, g_2), где $g_1 \in An_k(f)$, $g_2 \in An_k(f+1)$, тогда имеем $fg_1 + (f+1)g_2 = 0$, отсюда $f(g_1 + g_2) = g_2$. Получаем соответствие между парами функций, первая из которых из $An_k(f)$, вторая из $An_k(f+1)$, и функциями из $B_k(f)$. Несложно проверить, что соответствие взаимооднозначное.

Лемма 1. *Пусть $r_k(supp(f)) = wt(f)$, где $k < \lceil \frac{n}{2} \rceil$, тогда $dim(An_k(f+1)) = 0$.*

Доказательство. Из условия следует, что для любого набора x, такого что $f(x) = 1$, существует функция g степени не выше k, что произведение fg равно 1 только на одном наборе x. В противном случае существовала бы функция отличная от f лишь на наборе x с k-рангом $r_k(supp(f)) = wt(f)$ и весом равным $wt(f) - 1$, что невозможно.

Пусть существует функция f', $deg(f') \leq k$ и $f \neq 0$, что $(f+1)f' = 0$. Возьмем набор x, такой что $f'(x) = 1$. Из того что $supp(f') \subseteq supp(f)$, следует, что существует g' степени не выше k, что произведение $f'g'$ равно 1 только на одном наборе x. Но степень произведения двух булевых функций не превосходит суммы степеней этих функций, тогда $deg(f'g') < n$, что противоречит, тому что $f'g'$ равно 1 ровно на одном наборе.

Следствие 1. *Пусть $dim(An_k(f)) = \sum_{i=0}^{k} \binom{n}{i} - wt(f)$, где $k \leq \lceil \frac{n}{2} \rceil$, тогда $dim(An_{\lceil \frac{n}{2} \rceil - 1}(f+1)) = 0$.*

Следствие 2. *Пусть* $n = 2k + 1$ *и* $An_k(f) = 0$, *тогда* $AI(f) = k + 1$.

Утверждение 3. *Пусть* $deg(f) \leq \lceil \frac{n}{2} \rceil$, $k \leq \lceil \frac{n}{2} \rceil$, *тогда существует функция* g, *такая что* $AI(g) = k$ *и* $d(f, g) = dim(B_{k-1}(f))$.

Доказательство. Среди наборов, на которых f равна 1 найдется $r_{k-1}(supp(f))$ таких, что их $(k-1)$-ранг тоже будет равен $r_{k-1}(supp(f))$, обозначим это множество наборов через C_1. Аналогично, рассмотрев $f+1$ получим множество C_0 из $r_{k-1}(supp(f+1))$ наборов. Из леммы 1 следует, что мы можем дополнить C_1 за счет $\sum_{i=0}^{k-1} \binom{n}{i} - r_{k-1}(supp(f))$ наборов, которые не входят в C_0 и на которых f равна 0, так чтобы k-ранг нового множества был в точности $\sum_{i=0}^{k-1} \binom{n}{i}$. Аналогично мы можем дополнить и множество C_0 за счет $\sum_{i=0}^{k-1} \binom{n}{i} - r_{k-1}(supp(f+1))$ наборов, которые не входят в C_1 и на которых f равна 1, так чтобы k-ранг нового множества был в точности $\sum_{i=0}^{k-1} \binom{n}{i}$.

Из выше сказанного следует, что можно изменить значение f на $\sum_{i=0}^{k-1} \binom{n}{i} - r_{k-1}(supp(f)) + \sum_{i=0}^{k-1} \binom{n}{i} - r_{k-1}(supp(f+1)) = dim(An_{k-1}(f)) + dim(An_{k-1}(f+1)) = dim(B_{k-1}(f))$ наборах и получить функцию g, такую что $dim(An_{k-1}(g)) = dim(An_{k-1}(g+1)) = 0$, следовательно $AI(g) = k$.

Таким образом, с учетом утверждений 1-3 мы доказали, что задача нахождения наиболее сильной оценки нелинейности r-ого порядка функции через значение ее алгебраической иммунности k полностью сводиться к нахождению $min_{deg(g) \leq r} dim(B_{k-1}(g))$. Сформулируем это в качестве теоремы:

Теорема 1. *Пусть* $f(x_1, \ldots, x_n)$ *имеет* $AI(f) = k$, *тогда*

$$nl_r(f) \geq min_{deg(g) \leq r} dim(B_{k-1}(g)).$$

И существует функция f_0, $AI(f_0) = k$, *для которой*

$$nl_r(f_0) = min_{deg(g) \leq r} dim(B_{k-1}(g)).$$

Теперь посмотрим какие конкретные оценки можно получить из этой теоремы.

Утверждение 4. *Пусть* $deg(f) = r$, *тогда* $dim(B_{k-1}(f))$ *не меньше чем* $\sum_{i=0}^{k-r-1} \binom{n}{i}$.

Доказательство. Просто берем все функции степени не больше $(k-r-1)$.

Следствие 3. *Пусть* $AI(g) = k$, *тогда*

$$nl_r(g) \geq \sum_{i=0}^{k-r-1} \binom{n}{i}.$$

Мы получили оценку из работы [3].

Утверждение 5. *Пусть* $deg(f) = r$, *тогда* $dim(B_{k-1}(f))$ *не меньше чем* $2\sum_{i=0}^{k-r-1}\binom{n-r}{i}$.

Доказательство. Можно считать, что полином f содержит слагаемое $x_1x_2\dots x_r$. Рассмотрим функции вида $fg_1 + (f+1)g_2$, где g_1 и g_2 любые функции от $x_{m+1},\dots,x_n$ степени не более $(k-r-1)$. Несложно проверить, что все такие функции различны и принадлежат $B_{k-1}(f)$.

Следствие 4. *Пусть* $AI(g) = k$, *тогда*

$$nl_r(g) \geq 2\sum_{i=0}^{k-r-1}\binom{n-r}{i}.$$

Мы получили оценку из работы [1].

Утверждение 6. *Пусть* $deg(f) = r$, *тогда* $dim(B_{k-1}(f))$ *не меньше чем*

$$\sum_{i=0}^{k-r-1}\binom{n}{i} + \sum_{i=k-2r}^{k-r-1}\binom{n-r}{i}.$$

Доказательство. Можно считать, что полином f содержит слагаемое $x_1x_2\dots x_r$. Рассмотрим функции вида $g_1 + fg_2$, где g_1 любая функции степени не более $(k-r-1)$, а g_2 любая функция от $x_{r+1},\dots,x_n$ степени не более $(k-r-1)$, содержащая лишь мономы длины не менее $k-2r$.

Несложно проверить, что все такие функции принадлежат $B_{k-1}(f)$. Проверка того, что все функции различны, сводиться к проверке того, что из $g_1 + fg_2 = 0$ следует $g_1 = 0$ и $g_2 = 0$. Равенство $g_2 = 0$ следует из того, что в противном случае функция fg_2 содержала бы моном длины не менее $(k-r)$, который был бы и в полиноме f (т.к. $\deg(f_1) \leq (k-r-1)$). Равенство $g_1 = 0$ следует непосредственно из $g_1 + fg_2 = 0$ и $g_2 = 0$.

Следствие 5. *Пусть* $AI(g) = k$, *тогда*

$$nl_r(g) \geq \sum_{i=0}^{k-r-1}\binom{n}{i} + \sum_{i=k-2r}^{k-r-1}\binom{n-r}{i}.$$

Мы получили оценку, которая улучшает обе существовавших ранее оценки.

Список литературы

1. Carlet C. On the higher order nonlinearities of algebraic immune functions. CRYPTO 2006, LNCS 4117, pp. 584–601.

2. Courtois N and Meier W. Algebraic attacks on stream ciphers with linear feedback. In Anvances in Cryptology — EUROCRYPT 2003, LNCS 2656, pp. 345–359. Springer Verlag, 2003.

3. Dalai D. K., Gupta K. C. and Maitra S. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions. Indocrypt 2004, Chennai, India, December 20-22, pages 92–106, LNCS 3348, Springer Verlag, 2004.

4 Lobanov M. Tight bound between nonlinearity and algebraic immunity. Cryptology ePrint archive(http://eprint.iacr.org/), Report 2005/437.

5. Meier W., Pasalic E. and Carlet C. Algebraic attacks and decomposition of Boolean functions. In Advances in Cryptology — EUROCRYPT 2004, LNCS 3027, pp. 474–491. Springer Verlag, 2004.

ГРАНИЧНЫЕ КЛАССЫ ОТНОСИТЕЛЬНО КЛАССА ПЛАНАРНЫХ ГРАФОВ ДЛЯ ЗАДАЧИ О НЕЗАВИСИМОМ МНОЖНСТВЕ

Д. С. Малышев (Нижний Новгород)

Введение

Независимым множеством в обыкновенном графе называется множество попарно несмежных вершин. Задача о независимом множестве для данного графа состоит в нахождении независимого множества наибольшей мощности. Для краткости задачу о независимом множестве будем называть *задачей НМ*.

Класс графов $\mathbf{K}$ называется *НМ-простым*, если существует алгоритм, решающий эту задачу для любого графа $G \in \mathbf{K}$ за полиномиальное время и *НМ-сложным*, если для графов этого класса задача НМ остается NP-полной [1].

Класс графов $\mathbf{X}$ называется *наследственным*, если он замкнут относительно изоморфизма, переименования ребер, удаления вершин и *сильно наследственным*, если он замкнут еще и относительно удаления ребер. Любой наследственный класс (и только наследственный класс) графов $\mathbf{X}$ может быть задан множеством запрещенных порожденных подграфов $\mathbf{S}$, это означает, что $\mathbf{X}$ состоит из тех и только тех графов, которые не имеют порожденных подграфов из $\mathbf{S}$. В этом случае принята запись $\mathbf{X}=Free(S)$. Если $\mathbf{S}$ является конечным, то такой наследственный класс называется *конечно определенным*.

В [1] дано определение граничного класса и доказано, что конечно определенный класс графов является НМ-сложным тогда и только тогда, когда в нем содержится какой-нибудь граничный класс. В этой работе вводится

более широкое понятие относительного граничного класса. Наследственный класс графов $\mathbf{X}$ назовем *предельным классом относительно наследственного класса* $\mathbf{Y}$ (*или предельным относительно* $\mathbf{Y}$), если существует такая последовательность $\mathbf{X}_1 \supseteq \mathbf{X}_2 \supseteq \ldots$ НМ-сложных классов, содержащихся в классе $\mathbf{Y}$, что $\cap_n \mathbf{X}_n = \mathbf{X}$. Минимальный по включению предельный относительно $\mathbf{Y}$ класс назовем *граничным относительно* $\mathbf{Y}$ *классом.* Из последнего определения следует, что $\mathbf{X} \subseteq \mathbf{Y}$. Класс $\mathbf{X}$ назовем *конечно определенным относительно наследственного класса* $\mathbf{Y}$, если существует такое конечное множество графов $\mathbf{M}$, что $\mathbf{X} = \mathbf{Y} \cap Free(\mathbf{M})$. Для относительных граничных классов легко доказывается обобщение теоремы 3 из работы [1], а именно, относительный конечно определенный класс графов является НМ-сложным тогда и только тогда, когда в нем содержится какой-нибудь относительный граничный класс.

Триодом $T_{i,j,k}$ называется дерево, имеющее ровно одну вершину степени три и ровно три листа, отстоящих от вершины степени три на расстояниях i, j, k соответственно. Пусть $\mathbf{T}$ — класс всех графов, у которых каждая из компонент связности является деревом не более чем с тремя листьями. Иными словами, класс $\mathbf{T}$ состоит только из тех графов, у которых каждая из компонент является либо триодом, либо простым путем. В работе [1] доказано, что $\mathbf{T}$ является граничным классом, а если $P \neq NP$, то $\mathbf{T}$— единственный сильно наследственный граничный класс. Возможно, $\mathbf{T}$— единственный граничный класс не только среди сильно наследственных. Доказательство этого предположения равносильно доказательству того, что для любого графа $G \in \mathbf{T}$ класс $Free(G)$ является НМ-простым. К настоящему времени это доказано для графов с не более 5 вершинами из $\mathbf{T}$ (за исключением P_5 и графов вида $pK_2 + qK_1$). Таким образом, вопрос о единственности $\mathbf{T}$ как граничного класса оказался сложным.

В настоящей работе рассматривается класс планарных графов. Класс $\mathbf{T}$ является граничным относительно **Planar**. Доказательство этого легко получить по аналогии с доказательством теоремы 4 из [1]. Возможно, что $\mathbf{T}$ — единственный граничный класс относительно **Planar**. Это утверждение пока не доказано, но в его исследовании удалось продвинуться значительно дальше, чем в исследовании аналогичного предположения для класса всех графов. В настоящей публикации доказывается НМ-простота класса $\mathbf{Planar} \cap Free(T_{1,1,i})$ для любого натурального i.

Определения и результаты

Предположим, что имеется планарный граф G и что он задан в виде своей плоской укладки. Определим понятие *глубины* графа G. Из плоской укладки графа G удалим вершины с инцидентными им ребрами, принадлежащие внешней грани. Множество этих вершин обозначим через V_1. С оставшейся укладкой будем проделывать аналогичную операцию до тех

пор, пока множество вершин не станет пустым. В результате мы получим разбиение множества вершин графа на подмножества $V_1, V_2, \ldots, V_k$, которые будем называть *уровнями* графа. Величину k назовем глубиной графа G и будем обозначать $\gamma(G)$.

Разделяющая клика графа — это множество вершин, порождающее полный подграф, удаление которого приводит к увеличению числа компонент связности. Назовем *C-блоком* максимальный по включению порожденный подграф данного графа, не имеющий разделяющей клики. Пусть $\mathbf{K}$— некоторый класс графов, тогда обозначим через $[\mathbf{K}]_c$ множество всех графов, у которых каждый C-блок принадлежит $\mathbf{K}$. В дальнейшем, нам понадобятся две операции над классами графов, которые сохраняют свойство HM-простоты.

Лемма 1 [1]. *Если* $\mathbf{X}$ *— HM-простой наследственный класс графов, то* $[\mathbf{X}]_c$ *также является HM-простым.*

Следствие. *Класс планарных графов единичной глубины является HM-простым.*

Лемма 2 [2]. *Если* $\mathbf{K}$ *— HM-простой наследственный класс, то для любого фиксированного* r *класс* $[\mathbf{K}]_r$ *является HM-простым.*

Лемма 3. *Если* G *- связный граф и* G *не принадлежит классу* $Free(T_{1,1,i})$ $(i \geq 3)$, *то либо* $G \in Free(T_{1,1,1})$, *либо* $diam(G) < 2i + 3$.

Следствие. *Если* G *— связный граф* и $G \in \mathbf{Planar} \cap Free(T_{1,1,i})$ $(i \geq 3)$, *то* $\gamma(G) < 2i + 3$.

Если G не содержит разделяющих клик, а V_1 — первый уровень графа G, то граф, порожденный множеством V_1, является простым циклом. Для каждой вершины $x \in V(G) \setminus V_1$ определим множество $N(x, V_1)$ всех вершин из V_1, смежных с x. Пусть $deg(x, V_1)$ - мощность множества $N(x, V_1)$. Для каждой вершины $x \in V(G) \setminus V_1$ определим величину $m(x)$ как максимальное количество последовательных вершин из V_1, не смежных с x.

Лемма 4. *Пусть* $\gamma(G) > 1$ *и* G *— C-блок, не содержащий порожденного* $T_{1,1,i}$, V_1 *— первый уровень графа* G. *Тогда, если для некоторой вершины* $x \in V(G) \setminus V_1$ *выполнено неравенство* $deg(x, V_1) > 5$, *то* $m(x) < i + 1$.

Теорема. *Для любого натурального* i *класс* $\mathbf{Planar} \cap Free(T_{1,1,i})$ *является HM-простым*

Доказательство. Обозначим через $\mathbf{Q}_{i,r}$ подмножество класса $\mathbf{Planar} \cap Free(T_{1,1,i})$, состоящее из графов глубины не более чем r. Покажем, что для любых натуральных i и r класс $\mathbf{Q}_{i,r}$ является НМ-простым.

Известно [3,4], что классы $Free(T_{1,1,i})$ при $i = 1, 2$ являются НМ-простыми. Отсюда следует НМ-простота рассматриваемых классов $\mathbf{Q}_{i,r}$ при $i = 1, 2$ и любых r. Пусть теперь $i \geq 3$. Дальнейшее доказательство проведем индукцией по r. Класс $\mathbf{Q}_{i,1}$ является НМ-простым ввиду следствия леммы 1.

Пусть G — связный граф из $\mathbf{Q}_{i,r+1}$. Если $G \in Free(T_{1,1,1})$, то задача НМ для графа G полиномиально разрешима. Поэтому будем считать, что $G \in \mathbf{Q}_{i,r+1} \setminus Free(T_{1,1,1})$. Ввиду леммы 1 можно считать, что G не содержит разделяющих клик. Из леммы 3 следует, что $diam(G) < 2i + 3$. Пусть V_1 — первый уровень графа G. Если $|V_1| \leq 2i + 3$, то $G \in [\mathbf{Q}_{i,r}]_{2i+3}$. Из леммы 2 следует, что класс $[\mathbf{Q}_{i,r}]_{2i+3}$ НМ-простой. Далее будем считать, что $|V_1| > 2i + 3$.

Пусть $v_1, v_2, \ldots, v_t$ — все вершины из V_1 и пусть они покрашены в черный цвет. Рассмотрим вершины v_1 и $v_{[t/2]}$. Пусть P — путь из v_1 в $v_{[t/2]}$ длины, меньшей чем $2i+3$. Рассмотрим всевозможные независимые множества подграфа, порожденного множеством вершин этого пути. Для каждого такого множества S рассмотрим граф $G^*(S)$, порожденный множеством вершин $V(G) \setminus (N(S) \cup V(P))$, где $V(P)$ — множество вершин подграфа, порожденного вершинами из P, $N(S)$ — множество тех вершин графа G, которые смежны хотя бы с одной вершиной из множества S. Ясно, что зная решение задачи НМ для графов $G^*(S)$ для всех S, можно за время $O(1)$ найти решение задачи НМ для графа G. Пусть $G_1(S), \ldots, G_p(S)$ — те компоненты связности графа $G^*(S)$, которые содержат черные вершины и имеют глубину, равную $r + 1$. (Остальные компоненты принадлежат классу $\mathbf{Q}_{i,r}$) Если множество S содержит такую вершину x, что $deg(x, V_1) > 5$, то ввиду леммы 4 каждый из этих графов содержит не более чем $i + 1$ черную вершину, а следовательно, каждый из них принадлежит НМ-простому классу $[\mathbf{Q}_{i,k}]_{i+1}$. Если такой вершины не найдется, то ясно, что $p \leq 5|S| < 10i + 15$. Каждый из графов $G_1(S), \ldots, G_p(S)$ содержит не более $[t/2]+1$ черных вершин, причем в каждом из них на первом уровне все черные вершины стоят последовательно. К каждому из этих графов применимы те же действия, что и к графу G. (т.е. если рассматриваемый граф $G_i(S)$ $(i = 1, \ldots, p)$ не принадлежит ни классу $Free(T_{1,1,1})$, ни классу $[\mathbf{Q}_{i,k}]_{2i+3}$, то концы пути P_i следует выбирать по следующему правилу — на первом уровне графа $G_i(S)$ такие две вершины, что одна из них является черной, делящей последовательно стоящие черные вершины на две "дуги", отличающиеся не более чем на одну вершину.)

Таким образом, всю процедуру решения задачи НМ для графа G можно изобразить в виде дерева решений. Листья этого дерева соотвествуют

графам из классов $[\mathbf{Q}_{i,k}]_{2i+3} \setminus Free(T_{1,1,1})$, $Free(T_{1,1,1})$, а внутренние узлы соответствуют графам, содержащим не менее $2i+3$ черных вершин и имеющих глубину, равную $k+1$ и не принадлежащих классу $Free(T_{1,1,1})$. Т.к. множество черных вершин каждый раз делится на две почти равные части, то высота данного дерева ограничена сверху величиной $\lceil \log_2(n) \rceil$.

Оценим в дереве решений общее количество внутренних узлов. Каждый внутренний узел имеет не более чем $c = (10i+15)2^{2i+3}$ непосредственных потомков, являющихся внутренними узлами, следовательно, общее количество внутренних узлов в дереве решений не превосходит $c^{\lceil \log_2(n) \rceil + 1}$, т.е. ограничено полиномом от n. Общее число потомков каждого внутреннего узла, являющихся листьями, не превосходит n, следовательно, число узлов в дереве решений ограничено сверху полиномом от n.

Утверждение теоремы следует из следствия леммы 3 и НМ-простоты класса $Q_{i,r}$ для любых натуральных i и r.

Список литературы

1 Alekseev V.E. On easy and hard hereditary classes of graphs with respect to the independent set problem. Discrete Applied Mathematics 132(2004

2 Алексеев В.Е., Коробицын Д.В. О сложности некоторых задач на наследственных классах графов. Дискретная математика, 1992г. Т. 4, вып. 4.

3 Minty.G.J. On maximal independent sets in claw-free graphs. J.Combin Theory Ser.B 28(3) (1980).

4 Алексеев. В.Е. Полиномиальный алгоритм для нахождения наибольшего независимого множества в графах без вилок. Дискретный анализ и исследование операций. Серия 1. Том 6, номер 4. Новосибирск: Из-во института математики, 1999г.

СЛОЖНОСТЬ ПРИМЕНЕНИЯ СИМВОЛЬНЫХ МЕТОДОВ В КРИПТОАНАЛИЗЕ АЛГОРИТМА ГОСТ 28147-89

А. С. Мелузов (Москва)

Введение. В статье описан способ применения символьных методов криптографического анализа к алгоритму ГОСТ 28147-89. Для этого приведены способы построения системы полиномиальных уравнений, описывающих работу алгоритма ГОСТ 28147-89, проведена оценка сложности и

структуры получаемой системы полиномиальных уравнений, а также проведена оценка эффективности алгоритмов решения систем полиномиальных уравнений над конечными полями с использованием стандартных базисов (базисов Гребнера).

1. Постановка задачи. В настоящее время в целях криптоанализа широко используется следующий подход, целиком и полностью основанный на методах символьных вычислений в кольцах многочленов над различными алгебраическими структурами. А именно: с использованием различных методик функционирование криптосхемы описывается с помощью системы полиномиальных уравнений над какой-либо алгебраической структурой (как правило, над конечным полем) с тем, чтобы иметь возможность свести задачу криптоанализа к решению построенной системы полиномиальных уравнений в символьном виде. Как правило, этот шаг выполняется путем построения базиса Грёбнера соответствующего полиномиального идеала с использованием одного из широко известных алгоритмов, таких, как алгоритм Бухбергера, XL-метод, алгоритмы F_4 и F_5, принадлежащие Ж.-К. Фажере.

Необходимо применить данный подход к алгоритму блочного шифрования ГОСТ 28147-89 в режиме простой замены.

2. Алгоритм ГОСТ 28147-89. В режиме простой замены алгоритм ГОСТ 28147-89 работает следующим образом: открытые данные, подлежащие зашифрованию, разбивают на блоки по 64 бит в каждом. Блок открытого текста представляется в виде конкатенации двух блоков по 32 бита каждый:

$$T_0 = (a_1(0), \ldots, a_{32}(0), b_1(0), \ldots, b_{32}(0)) = a(0)||b(0), \tag{1}$$

где в последующем a_1 считается младшим, а a_{32} — старшим битом двоичной записи некоторого целого числа.

Объем ключа составляет 256 бит $(W_{256}, \ldots, W_1)$, которые разбиваются на восемь 32-х разрядных вектора

$$\begin{gathered} X_0 = (W_{32}, \ldots, W_1), \\ X_1 = (W_{64}, \ldots, W_{33}) \\ \ldots\ldots \\ X_7 = (W_{256}, \ldots, W_{225}). \end{gathered} \tag{2}$$

Уравнения зашифрования в режиме простой замены имеют вид:

$$\begin{cases} a(j) = \big(a(j-1) + X_{(j-1) \bmod 8}\big)\, KR \oplus b(j-1), \\ b(j) = a(j-1), j = \overline{1,24}, \\ a(j) = \big(a(j-1) + X_{(32-j)}\big)\, KR \oplus b(j-1), \\ b(j) = a(j-1), j = \overline{25,31}, \\ a(32) = a(31), \\ b(32) = (a(31) + X_0)\, KR \oplus b(31). \end{cases} \tag{3}$$

Здесь $+$ — операция сложения по модулю 2^{32} двух чисел, двоичным представлением которых являются операнды, причем результатом операции является двоичный вектор длины 32, являющийся двоичным представлением получившегося 32-х разрядного числа.

Преобразование K выглядит следующим образом: поступающтй на его вход 32-х разрядный вектор разбивается на 8 подвекторов длины 4, каждый из которых, в свою очередь, поступает на вход соответствующего *узла замены* $K_1, \ldots, K_8$, осуществляющего перестановку на множестве двоичных векторов длины 4. Восемь результатов перестановок путем конкатенации составляют результирующий вектор:

$$XK = (X_8 || \ldots || X_1)\, K = (K_8(X_8) || \ldots || K_1(X_1))\,. \tag{4}$$

R — операция циклического сдвига на одиннадцать шагов в сторону старших разрядов:

$$(y_{32}, \ldots, y_1)R = (y_{21}, y_{20}, \ldots, y_2, y_1, y_{32}, y_{31}, \ldots, y_{23}, y_{22}). \tag{5}$$

Операция $\oplus$ есть покоординатное суммирование 32-разрядных векторов по модулю 2.

3. Построение системы полиномиальных уравнений. Обратимся теперь к вопросу о построении системы полиномиальных уравнений, аппроксимирующей зашифрование в режиме простой замены согласно алгоритму ГОСТ 28147-89.

Очевидно, что для того, чтобы построить полиномиальную аппроксимацию полного алгоритма зашифрования, достаточно построить полиномиальную аппроксимацию для одного раунда. Полиномиальная аппроксимация для 32 раундов получается путем введения дополнительных переменных и дупликации системы.

3.1. Модульное сложение. Первый этап при построении системы полиномиальных уравнений, аппроксимирующей один раунд алгоритма ГОСТ 28147-89, состоит в том, чтобы выразить координаты двоичного представления суммы двух чисел по модулю 2^{32} как булевы функции от координат двоичных представлений складываемых чисел.

Это можно сделать, итеративно вычисляя функции переноса в старший разряд и, на их основе, координатные функции, согласно формулам [4,(1)]: для $\bar{r} = (r_0, \ldots, r_{n-1}), \bar{x} = (x_0, \ldots, x_{n-1}), \bar{a} = (a_0, \ldots, a_{n-1})$ при

$$\begin{aligned} &r_0 + r_1 \cdot 2 + \cdots + r_{n-1} \cdot 2^{n-1} = \\ &\quad = (x_0 + \cdots + x_{n-1} \cdot 2^{n-1}) + (a_0 + \cdots + a_{n-1} \cdot 2^{n-1}) \pmod{2^n} \end{aligned} \tag{6}$$

имеют место равенства:

$$\begin{aligned} &r_0 = x_0 \oplus a_0 \oplus c_0, \quad c_0 = 0, \\ &r_i = x_i \oplus a_i \oplus c_i, \quad c_i = x_{i-1}a_{i-1} \oplus x_{i-1}c_{i-1} \oplus a_{i-1}, \\ &i = \overline{1, n-1}. \end{aligned} \tag{7}$$

Как видно из соотношений (6) и (7), i-я координатная функция суммы $\bar{x} + \bar{a}$ имеет степень $i + 1$, и содержит $2^i + 1$ термов. Поэтому нахождение координатных функций суммы $\bar{x} + \bar{a}$ при значениях i, близких к 32, является трудоемкой вычислительной задачей, невыполнимой на обычном персональном компьютере.

3.2. Блоки замены. Второй этап построения системы полиномиальных уравнений, аппроксимирующей один раунд криптоалгоритма ГОСТ 28147-89, состоит в том, чтобы построить покоординатную аппроксимацию булевыми функциями узлов замены с последующим вычислением композиции полученной аппроксимации и найденных на первом этапе координатных функций модульного сложения. Можно сделать двумя способами.

Во-первых, естественный способ состоит в представлении каждого узла замены $K_i, i = \overline{1,8}$ как вектора $(f_{i,1}, \ldots, f_{i,4})$ из четырех булевых функций от четырех переменных.

Во-вторых, можно обратиться к методике, предложенной в статье [2, Раздел 3.2].

Каждая методика имеет свои плюсы и свои минусы. Первый способ предпочтителен по той причине, что в этом случае не приходится вводить новые служебные переменные, и, таким образом, число переменных, входящих в уравнения системы, значительно ниже. Однако сами уравнения, как правило, имеют более высокую степень и состоят из большего числа термов. Второй способ имеет своим преимуществом то, что этот путь позволяет получить значительно большее число уравнений, причем фиксированной степени (а именно по 21 уравнению степени не выше 2 от входных переменных для каждого узла замены).

При использовании второго способа, структура итоговой системы полиномиальных уравнений представляется более ясной, поэтому будем использовать именно его.

3.3. Сдвиг и побитовое сложение. Последний этап построения системы полиномиальных уравнений, аппроксимирующей один раунд криптоалгоритма ГОСТ 28147-89, состоит в подстановке в полученные уравнения переменных, соответствующих результату работы данного раунда, просуммированных с переменными, описывающими результат работы раунда за два до текущего в соответствии с (3) (или с битами левой части открытого текста, если описываемый раунд — первый и правой части открытого текста, если второй) с учетом операции побитового сдвига, в соответствии с (3). Для этого выходы узлов замены были выражены через левую (правую) часть открытого текста (или результат работы раунда за два до текущего), а выходы — через результат работы описываемого раунда работы алгоритма (или зашифрованный текст, если описываемый раунд — последний или предпоследний). Если y_i — i-й бит выхода узлов замены, z_i — i-й бит результата работы текущего раунда текста, а l_i — i-й бит результата работы

предыдущего раунда, то верно следующее соотношение:

$$y_i = z_{(i+11) \bmod 32} + l_{(i+11) \bmod 32}.$$

3.3. Построение итоговой системы. Таким образом, мы получим системы полиномиальных уравнений, описывающие каждый раунд алгоритма шифрования ГОСТ 28147-89. С помощью отождествления переменных, соответствующим одним и тем же значениям (например, результаты работы первого раунда будут складываться со значениями, полученными после побитового сдвига в третьем раунде, а также подаваться на вход регистра модульного сложения с ключом во втором раунде), получим систему полиномиальных уравнений, описывающую алгоритм шифрования ГОСТ 28147-89 целиком.

Итак, при анализе криптографического алгоритма ГОСТ 28147-89 было показано, что система полиномиальных уравнений, аппроксимирующая его работу в режиме простой замены зависит от 1248 переменных (из которых 256 — биты ключа, а 992 — вспомогательные переменные (промежуточные результаты работы на каждом раунде)), и состоит из 5376 уравнений, по 672 уравнения 7,15,23,31,39,47,55 и 63 степени.

4. Оценка сложности решения построенной системы. После построения системы полиномиальных уравнений, аппроксимирующей работу алгоритма ГОСТ 28147-89, необходимо её решить. Решение СПУ будем осуществлять методом построения базиса Грёбнера.

Существует довольно много алгоритмов, строящих базис Грёбнера заданной системы уравнений, однако, самым быстрым на данный момент является алгоритм F_5, принадлежащий Ж.-К. Фажере.

В статье [1] подробно рассматриваются особенности применения этого алгоритма к полиномам над полем $GF(2)$.

Суть алгоритма состоит в построении последовательности матриц $\mathcal{M}_{d,m}$, столбцы которых соответствуют всевозможным мономам степени d, выстроенным в лексикографичеком порядке, а строки соответствуют всевозможным произведениям $t \times f_j$, где t — моном, такой что $deg(t \times f_j) = d$, а $1 \leq j \leq m$, $f_1, \ldots, f_m$ – полиномы, входящие в исходную систему.

Далее, над каждой такой матрицей производятся преобразования, приводящие её к треугольному виду. Поскольку матрица сильно разряжена, можно считать, что сложность таких преобразований будет равна $\mathcal{O}(k^2)$, где k — ранг матрицы $\mathcal{M}_{d,m}$.

Общая сложность алгоритма определяется сложностью вычислений линейной алгебры для наибольшей матрицы. В соответствии с [1] такой матрицей будет та, которая соответствует полиномам степени D_{reg}. А D_{reg} — степень полурегулярности исходной системы. Степень полурегулярности вычисляется как номер первого неположительного члена порождающего ряда

последовательности полиномов (исходной системы). Сумма порождающего ряда равна $S_{m,n}(z) = (1+z)^n / \prod_{k=1}^{m}(1+z^{d_k})$, где n — число неизвестных в исходной системе, d_k — степень k-того полинома, $f_1, \ldots, f_m$ — полиномы, входящие в исходную систему.

В соответствии с описанной в [1] методикой, был построен порождающий ряд последовательности полиномов, описывающей работу алгоритма ГОСТ 28147-89 в режиме простой замены:

$$\frac{(1+z)^{1248}}{((1+z^7)(1+z^{15})(1+z^{23})(1+z^{31})(1+z^{39})(1+z^{47})(1+z^{55})(1+z^{63}))^{672}}$$

и найден его первый неположительный член, номер которого соответствует степени регулярности системы полиномиальных уравнений (последовательности полиномов). Степень полурегулярности для системы полиномиальных уравнений, описывающей работу криптоалгоритма ГОСТ 28147-89 в режиме простой замены $D_{reg} = 402$.

Следовательно, максимальный размер матрицы в алгоритме F_5 будет равен рангу матрицы $\mathcal{M}_{d,m}$ на шаге D_{reg} и равен числу столбцов этой матрицы, то есть

$$\binom{n}{D_{reg}} = \binom{1248}{402} \approx 2^{1126},$$

а сложность вычисления базиса Гребнера построенной системы будет равна $\mathcal{M} \cdot 2^{2252}$, при допущении, что коэффициент сложности вычислений линейной алгебры $\omega = 2$, по причине сильной разреженности матриц. Здесь $\mathcal{M}$ – константа, зависящая от вычислительной техники, на которой будет выполняться алгоритм.

Однако, можно добиться ускорения алгоритма с помощью применения параллельных вычислений. Векторные команды и одновременное вычисление независимых по данным частей алгоритма могут значительно ускорить вычисления.

Необходимо заметить, что основную роль в сложности играет длина блока и количество раундов. Например, если применить аналогичные рассуждения к алгоритму, в котором по сравнению с ГОСТ 28147-89 длина блока 16 бит, длина ключа 16 бит, а число раундов равно 2, то получим систему уравнений, его аппроксимирующую, которая состоит из 84 уравнений, по 42 уравнения 7 и 15 степеней. Дополнительных переменных не будет (результат работы первого раунда является левой частью шифрованного текста), то есть всего будет 16 неизвестных – биты ключа. В разложении в ряд следующего выражения:

$$\frac{(1+z)^{16}}{((1+z^7)(1+z^{15}))^{42}}$$

первым неположительным членом будет член с номером 10. То есть степень полурегулярности такой системы равна 10, размер матрицы в алгоритме F_5 будет равен 8008, а сложность вычислений $\approx 2^{26}$. Отметим, что это верхняя оценка. На практике, уравнения могут иметь меньшие степени, и сложность вычислений будет меньше.

Список литературы

1. Magali Bardet, Jean-Charles Faugère, Bruno Salvy. Complexity of Gröebner basis computation for Semi-regular Overdetemined sequences over F_2 with solutions in F_2.

2. Courtois N. T., PieprzykJ . Crytoanalysis of block ciphers with overdefined systems of equations. // ASIACRYPT 2002, LNCS 2501, pp.267–287, 2002.

3. Jean-Charles Faugère. A new efficient algorithm for computation Gröebner bases without reduction to zero (F_5).

4. Braeken A., Semaev I. The ANF of the Composition of Addition and Multiplication mod2^n with a Boolean Function // Fast Software Encryption 2005, Proceedings, pp. 115–127.

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

Е. В. Михайлец (Москва)

Понятие неявной выразимости функций k-значной логики введено А. В. Кузнецовым как одно из обобщений понятия выразимости функций суперпозициями [3].

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

$$\begin{cases} \Phi_1(x_1, \ldots, x_n, y) = \Psi_1(x_1, \ldots, x_n, y), \\ \ldots \\ \Phi_q(x_1, \ldots, x_n, y) = \Psi_q(x_1, \ldots, x_n, y), \end{cases} \tag{1}$$

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

Говорят, что функция $f(x_1, \ldots, x_n)$ k-значной логики *неявно выразима* над системой функций A, если существует система неявных уравнений над

A вида (1), имеющая при любых фиксированных значениях $x_1, \ldots, x_n$ единственное решение $y = f(x_1, \ldots, x_n)$. При этом соответствующую систему уравнений называют *неявным представлением* функции $f(x_1, \ldots, x_n)$ над A.

Множество всех функций f, $f \in P_k$, неявно выразимых над системой функций A, называется *неявным расширением* системы A и обозначается через $I(A)$ [2]. Благодаря очевидному соотношению $I(A) = I([A])$, при исследовании неявных расширений можно ограничиться рассмотрением только замкнутых относительно суперпозиции классов функций k-значной логики.

Если любая функция k-значной логики неявно выразима над A, т. е. $I(A) = P_k$, то систему функций A называют *неявно полной* в P_k.

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

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

О. М. Касим-Заде в работе [1] исследовал поведение ранговой функции $m_A^2(n)$ для всех замкнутых классов булевых функций. Для классов D_2 и F_i^μ, где $i = 2, 3, 6, 7$ и $\mu = 2, 3, \ldots, \infty$, в работе [1] 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 [1] доказал следующую теорему.

Теорема 1. *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 k-значной логике можно рассмотреть обобщения понятия монотонности, отвечающие различным частичным порядкам на множестве E_k, где $E_k = \{0, 1, \ldots, k-1\}$. В частности, можно ввести определение монотонной функции следующим образом.

Пусть $\mathfrak{M}$ — произвольный частичный порядок, заданный на множестве E_k. Отношение порядка $\mathfrak{M}$ будем обозначать символом "$\leq_{\mathfrak{M}}$".

Цепью в частично упорядоченном множестве $< E_k; \mathfrak{M} >$ будем называть всякую последовательность различных попарно сравнимых элементов $\alpha^0 \leq_{\mathfrak{M}} \alpha^1 \leq_{\mathfrak{M}} \cdots \leq_{\mathfrak{M}} \alpha^r$ из этого множества. *Длиной цепи* называется

величина, на единицу меньшая, чем число элементов цепи. То есть длина цепи из $r+1$ элементов равна r. Каждому частичному порядку $\mathfrak{M}$ можно поставить в соответствие максимальную длину цепи в частично упорядоченном множестве $< E_k; \mathfrak{M} >$, обозначаемую через $s(\mathfrak{M})$. Легко видеть, что $0 \le s(\mathfrak{M}) \le k-1$.

Пусть помимо частичного порядка $\mathfrak{M}$ на множестве E_k задан еще один частичный порядок $\mathfrak{M}'$. Если для любых $\alpha, \beta \in E_k$ таких, что $\alpha \le_{\mathfrak{M}'} \beta$, выполняется отношение $\alpha \le_{\mathfrak{M}} \beta$, то будем говорить, что порядок $\mathfrak{M}'$ *подчинен* порядку $\mathfrak{M}$ и факт подчиненности обозначать через $\mathfrak{M}' \subseteq \mathfrak{M}$. Легко видеть, что для порядков, удовлетворяющих условию $\mathfrak{M}' \subseteq \mathfrak{M}$, справедливо $s(\mathfrak{M}') \le s(\mathfrak{M})$.

Совокупность всех наборов $(\alpha_1, \ldots, \alpha_n)$ с компонентами из E_k: $\alpha_i \in E_k, 1 \le i \le n$, будем обозначать через E_k^n ($E_k^n = \underbrace{E_k \times \cdots \times E_k}_{n \text{ раз}}$) [4].

Отношение частичного порядка $\mathfrak{M}$, заданное на множестве E_k, можно естественным образом распространить на множество E_k^n. Пусть $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_n)$ — наборы с компонентами из $< E_k; \mathfrak{M} >$. Положим $\tilde{\alpha} \le_{\mathfrak{M}} \tilde{\beta}$, если $\alpha_i \le_{\mathfrak{M}} \beta_i$ для любого $i, 1 \le i \le n$.

Рассмотрим произвольную функцию k-значной логики $f(x_1, \ldots, x_n)$, $f : E_k^n \to E_k$. Зададим на области определения функции f частичный порядок $\mathfrak{M}$, на области значений — порядок $\mathfrak{M}'$, причем $\mathfrak{M}' \subseteq \mathfrak{M}$. Назовем функцию f *монотонной относительно пары порядков* $(\mathfrak{M}, \mathfrak{M}')$, если для любых наборов значений аргумента $\tilde{\alpha}$ и $\tilde{\beta}$ таких, что $\tilde{\alpha} \le_{\mathfrak{M}} \tilde{\beta}$, имеет место соотношение $f(\tilde{\alpha}) \le_{\mathfrak{M}'} f(\tilde{\beta})$.

В настоящей работе утверждается, что все классы функций k-значной логики, монотонных относительно любой пары порядков $(\mathfrak{M}, \mathfrak{M}')$, удовлетворяющей условиям $\mathfrak{M}' \subseteq \mathfrak{M}$ и $s(\mathfrak{M}') \ge 1$, являются неявно полными. Ограничение $s(\mathfrak{M}') \ge 1$ означает наличие в частично упорядоченном множестве $< E_k; \mathfrak{M}' >$ хотя бы одной пары сравнимых элементов, отличных друг от друга. Также получено точное выражение для ранговой функции указанных классов функций, зависящее явно только от n и от максимальных длин цепей $s(\mathfrak{M})$ и $s(\mathfrak{M}')$. В случае совпадения максимальных длин цепей, отвечающих порядкам $\mathfrak{M}$ и $\mathfrak{M}'$, выражение для ранговой функции совпадает с выражением из теоремы 1. Сформулируем основную теорему.

Теорема 2. *Пусть $k \ge 2$ и на множестве E_k заданы частичные порядки $\mathfrak{M}$ и $\mathfrak{M}'$ такие, что $\mathfrak{M}' \subseteq \mathfrak{M}$ и $s(\mathfrak{M}') \ge 1$. Пусть A — класс всех функций в P_k, монотонных относительно пары порядков $(\mathfrak{M}, \mathfrak{M}')$. Тогда система функций A неявно полна в P_k и ранговая функция системы A имеет вид*

$$m_A^k(n) = \left\lceil \frac{(n+1)s(\mathfrak{M}) + 1}{2s(\mathfrak{M}')} \right\rceil .$$

Следствие 1. *В условиях теоремы 2 при выполнении равенства* $s(\mathfrak{M}) = s(\mathfrak{M}')$ *выражение для ранговой функции системы* A *приобретает вид*

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

В частности, следствие имеет место, если частичный порядок $\mathfrak{M}'$ совпадает с порядком $\mathfrak{M}$.

Автор выражает благодарность своему научному руководителю О. М. Касим-Заде за всестороннее внимание к данной работе. Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 05-01-00994), Программы поддержки ведущих научных школ РФ и Программы фундаментальных исследований Отделения математических наук РАН "Алгебраические и комбинаторные методы математической кибернетики" (проект "Синтез и сложность управляющих систем").

Список литературы

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

2. Касим–Заде О. М. О неявной выразимости булевых функций // Вестник МГУ. Математика. Механика. — 1995. — № 2. — С. 44–49.

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

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

ПЕРИОДИЧНОСТЬ СОВЕРШЕННЫХ РАСКРАСОК РАДИУСА r > 1 БЕСКОНЕЧНОЙ ПРЯМОУГОЛЬНОЙ РЕШЕТКИ

С. А. Пузынина (Новосибирск)

Раскраска вершин графа G в n цветов называется совершенной радиуса r, если количество вершин цвета j в шаре радиуса r с центром в вершине цвета i не зависит от выбора вершины. Параметры совершенной раскраски задаются квадратной матрицей порядка n. Совершенные раскраски радиуса 1 ранее изучались и имели различные названия, в частности,

equitable partitions, partition designes, делитель графа. Понятие совершенной раскраски является обобщением понятия совершенного кода, фактически совершенный код является частным случаем совершенной раскраски в два цвета.

Изучаются совершенные раскраски графа бесконечной прямоугольной решетки. Раскраски этого графа можно рассматривать как двумерные слова над конечным алфавитом цветов.

Доказано, что каждая совершенная раскраска радиуса $r > 1$ графа бесконечной прямоугольной решетки является периодической.

1. Введение

Пусть G — граф, $A = (a_{ij})$ — квадратная матрица порядка n, $r \geq 1$. Рассмотрим раскраску графа G в n цветов и произвольную вершину x цвета i. Если количество вершин цвета j (отличных от x) на расстоянии не более r от вершины x не зависит от выбора вершины x и равно a_{ij}, то раскраска называется *совершенной радиуса* r с матрицей A. Ранее совершенные раскраски радиуса 1 изучались в различных контекстах и имели различные названия, в частности, их называли equitable partitions (равномерными разбиениями) [3].

В настоящей работе рассматриваются совершенные раскраски графа $G(\mathbb{Z}^2)$ бесконечной прямоугольной решетки. Назовем матрицу A *допустимой*, если существует совершенная раскраска графа $G(\mathbb{Z}^2)$ с матрицей A для соответствующего r. Основной результат заключается в том, что любая совершенная раскраска радиуса $r > 1$ бесконечной прямоугольной решетки является периодической. Совершенные раскраски бесконечной прямоугольной решетки могут рассматриваться как двумерные слова над конечным алфавитом цветов. Для доказательства этого факта используется метод R-продолжаемых слов, который был предложен в [4] и использован для изучения двумерных слов другого типа, называемых центрированными функциями.

Заметим, что случай $r \geq 2$ принципиально отличается от случая $r = 1$. Существуют непериодические совершенные раскраски радиуса 1. В [5] доказано, что для любой допустимой матрицы радиуса 1 существует периодическая совершенная раскраска, причем она может быть получена из непериодической методом свитчинга бинарных диагоналей. Бинарная диагональ — это диагональ, состоящая из двух чередующихся цветов, под свитчингом бинарной диагонали подразумевается перестановка цветов внутри диагонали.

В [1] М. Аксенович классифицировала все допустимые матрицы совершенных раскрасок радиуса 1 в 2 цвета бесконечной прямоугольной решетки и нашла некоторые необходимые условия для того, чтобы матрица была допустимой радиуса $r \geq 2$.

Понятие совершенной раскраски — это обобщение понятия совершенного кода. Действительно, совершенная раскраска n-регулярного графа с матрицей $\begin{pmatrix} 0 & n \\ 1 & n-1 \end{pmatrix}$ является совершенным кодом с расстоянием 3 (кодовые вершины — это вершины цвета 1).

2. Определения и обозначения

Пусть $G = (V, E)$ — граф. Расстояние между двумя вершинами $\mathbf{x}$ и $\mathbf{y}$, обозначаемое $d(\mathbf{x}, \mathbf{y})$, — это обычная графская метрика. *Шар* $B_r(\mathbf{x})$ радиуса r с центром в вершине $\mathbf{x}$ определяется следующим образом:

$$B_r(\mathbf{x}) = \{\mathbf{y} \in V |\ d(\mathbf{x}, \mathbf{y}) \leq r\}.$$

Аналогично *сфера* $S_r(\mathbf{x})$ задается следующим условием:

$$S_r(\mathbf{x}) = \{\mathbf{y} \in V |\ d(\mathbf{x}, \mathbf{y}) = r\}.$$

Пусть $A = (a_{ij})_{i,j=1}^{n}$ — целочисленная неотрицательная матрица, r — целое число, $r \geq 1$. Рассмотрим раскраску вершин графа G в n цветов:

$$\varphi : V \to \{1, ..., n\}.$$

Пусть x — произвольная вершина цвета i: $\varphi(x) = i$. Если число вершин цвета j (отличных от вершины x) в шаре $B_r(x)$ не зависит от выбора вершины x и равно a_{ij}, то раскраски называется *совершенной радиуса* r с матрицей A. Другими словами, раскраска совершенная, если число вершин каждого цвета в шаре радиуса r зависит только от цвета центра этого шара.

Нас интересуют совершенные раскраски графа $G(\mathbb{Z}^2)$ бесконечной прямоугольной решетки. Этот граф 4-регулярный, его вершинами являются всевозможные упорядоченные пары целых чисел-координат. Две вершины $\mathbf{x} = (x_1, x_2)$ и $\mathbf{y} = (y_1, y_2)$ смежны, если $|x_1 - y_1| + |x_2 - y_2| = 1$. Обозначим $\|\mathbf{x}\| = d(\mathbf{x}, \mathbf{0})$, где $\mathbf{0} = (0, 0)$.

Примеры совершенных раскрасок в 2 цвета см. на Рис. 1. На рисунках для наглядности мы окрашиваем клетки вместо вершин, то есть фактически рассматриваем граф, двойственный к $G(\mathbb{Z}^2)$ и изоморфный ему.

3. Конструкции и примеры

Конструкция А. Одним из методов получения совершенных раскрасок является так называемый орбитный метод. Рассмотрим граф G с группой автоморфизмов H, пусть H' — подгруппы группы H. Если мы раскрасим каждую орбиту множества вершин V под действием H' в свой цвет, мы получим совершенную раскраску радиуса $r \in \mathbb{N}$ графа G (см. [2]).

Конструкция В. Другой метод получения совершенных раскрасок основывается на объединении цветов.

Лемма 1. *Пусть φ — совершенная раскраска радиуса r в n цветов с матрицей A, раскраска ψ получается из φ объединением цветов в m групп $L_1, ..., L_m$. Раскраска ψ является совершенной радиуса r в m цветов тогда и только тогда, когда матрица A удовлетворяет следующему условию: для любых $i, j \in \{1, ..., m\}$, $i \neq j$, для любых $p, s \in L_i$,*

$$\sum_{q \in L_j} a_{pq} = \sum_{q \in L_j} a_{sq}.$$

Матрицей совершенной раскраски ψ является $B = (b_{ij})_{i,j=1}^{m}$, где $b_{ij} = \sum_{q \in L_j} a_{pq}$, для $p \in L_i$.

1.

	1	0	1	0	1	0	1	0	1
	1	0	1	0	1	0	1	0	1
	1	0	1	0	1	0	1	0	1
	1	0	1	0	1	0	1	0	1
	1	0	1	0	1	0	1	0	1
	1	0	1	0	1	0	1	0	1

2.

	1	0	1	0	1	0	1	0	1
	0	1	0	1	0	1	0	1	0
	1	0	1	0	1	0	1	0	1
	0	1	0	1	0	1	0	1	0
	1	0	1	0	1	0	1	0	1
	0	1	0	1	0	1	0	1	0

3.

	1	1	0	0	1	1	0	0	1
	1	0	0	1	1	0	0	1	1
	0	0	1	1	0	0	1	1	0
	0	1	1	0	0	1	1	0	0
	1	1	0	0	1	1	0	0	1
	1	0	0	1	1	0	0	1	1

4.

	1	0	0	1	0	0	1	0	0
	0	0	1	0	0	1	0	0	1
	0	1	0	0	1	0	0	1	0
	1	0	0	1	0	0	1	0	0
	0	0	1	0	0	1	0	0	1
	0	1	0	0	1	0	0	1	0

5.

	0	0	0	0	1	0	0	0	0
	0	1	0	0	0	0	1	0	0
	0	0	0	1	0	0	0	0	1
	1	0	0	0	0	1	0	0	0
	0	0	1	0	0	0	0	1	0
	0	0	0	0	1	0	0	0	0

6.

	1	1	0	0	1	1	0	0	1
	1	1	0	0	1	1	0	0	1
	0	0	1	1	0	0	1	1	0
	0	0	1	1	0	0	1	1	0
	1	1	0	0	1	1	0	0	1
	1	1	0	0	1	1	0	0	1

7.

	1	0	0	1	0	0	1	0	0
	1	0	0	1	0	0	1	0	0
	1	0	0	1	0	0	1	0	0
	1	0	0	1	0	0	1	0	0
	1	0	0	1	0	0	1	0	0
	1	0	0	1	0	0	1	0	0

8.

	1	1	0	0	1	1	0	0	1
	1	1	0	0	1	1	0	0	1
	1	1	0	0	1	1	0	0	1
	1	1	0	0	1	1	0	0	1
	1	1	0	0	1	1	0	0	1
	1	1	0	0	1	1	0	0	1

9.

	1	0	1	0	1	0	1	0	1
	1	0	1	0	1	0	1	0	1
	0	1	0	1	0	1	0	1	0
	0	1	0	1	0	1	0	1	0
	1	0	1	0	1	0	1	0	1
	1	0	1	0	1	0	1	0	1

Рис. 1.

Примеры.

1. Орбитные раскраски в два цвета. Существует 9 орбитных раскрасок в два цвета (см. Рис. 1). Эти раскраски содержатся в множестве совершенных раскрасок радиуса 1, которые были описаны Аксенович [1].

2. Трансляционные раскраски. Пусть H' — группа трансляций, порожденная двумя неколлинеарными векторами $\mathbf{u} = (u_1, u_2)$ и $\mathbf{v} = (v_1, v_2)$. Раскрасив каждую орбиту $\mathbb{Z}^2$ под действием группы H' в свой цвет, мы

получим трансляционную раскраску. Эта раскраска совершенная любого радиуса в $|u_1v_2 - u_2v_1|$ цветов. Число цветов равно числу вершин в параллелограмме, натянутом на векторы $\mathbf{u}$ и $\mathbf{v}$.

3. Совершенный код и раскраски, получаемые из него объединением цветов. Рассмотрим трансляционную раскраску, порожденную векторами $(r+1, r)$ и $(r, -r-1)$. Эта раскраска совершенная радиуса r в $n = 2r^2+2r+1$ цветов с соответствующей матрицей

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

По Лемме 1 мы можем объединить цвета и получить совершенную раскраску с матрицей

$$\begin{pmatrix} k & n-k \\ k+1 & n-k-1 \end{pmatrix}.$$

При $k = 0$ эта раскраска является совершенным кодом с минимальным расстоянием $2r + 1$.

4. Периодичность

В этом разделе мы рассматриваем периодичность совершенных раскрасок радиуса $r > 1$ на графе $G(\mathbb{Z}^2)$.

Раскраска φ называется $\mathbf{v}$-*периодической* (или $\mathbf{v}$ – это вектор периодичности раскраски φ) если $\varphi(\mathbf{x} + \mathbf{v}) = \varphi(\mathbf{x})$ для всех $\mathbf{x} \in \mathbb{Z}^2$. Совершенная раскраска, которая является $\mathbf{v}$- и $\mathbf{u}$-периодической для некоторых неколлинеарных $\mathbf{v}$ и $\mathbf{u}$, называется *периодической. Фундаментальным параллелограммом* называется множество вершин в параллелограмме, порожденном векторами $\mathbf{u}$ и $\mathbf{v}$. В случае $\mathbf{u} = (a, 0)$, $\mathbf{v} = (0, b)$ мы используем слово "прямоугольник" вместо слова "параллелограмм".

Раскраски бесконечной прямоугольной решетки могут интерпретироваться как двумерные слова над конечным алфавитом цветов $\{1, ..., n\}$. Будем говорить, что двумерное слово ω *R-продолжаемое*, если для любых $\mathbf{x}, \mathbf{z} \in \mathbb{Z}^2$ равенство $\omega|_{B_R(\mathbf{x})} = \omega|_{B_R(\mathbf{z})}$ влечет $\omega|_{B_{R+1}(\mathbf{x})} = \omega|_{B_{R+1}(\mathbf{z})}$. Обозначение $\omega|_{B_R(\mathbf{x})} = \omega|_{B_R(\mathbf{z})}$ означает, что $\omega(\mathbf{x} + \mathbf{y}) = \omega(\mathbf{z} + \mathbf{y})$ для любых $\mathbf{y}$, таких что $\|\mathbf{y}\| \le R$.

Лемма 2. *Пусть ω — двумерное слово над конечным алфавитом. Если ω является R-продолжаемым для некоторого $R \ge 0$, то ω периодическое.*

Доказательство леммы можно найти в [4].

Замечание. В качестве следствия из доказательства этой леммы мы можем получить, что векторы периодичности могут быть выбраны следующим образом: $\mathbf{u} = (a, 0)$ и $\mathbf{v} = (0, b)$, где $a, b \le n^{2R^2+2R+1}$ (n — это число

элементов алфавита, $2R^2 + 2R + 1$ — число вершин в шаре радиуса R). Поэтому число вершин в фундаментальном прямоугольнике $a \times b$ не более $n^{2(2R^2+2R+1)}$.

Доказана следующая теорема.

Теорема 1. *Пусть $\varphi : \mathbb{Z}^2 \to \{1, ..., n\}$ — совершенная раскраска радиуса $r \geq 2$ бесконечной прямоугольной решетки. Тогда φ периодическая.*

Из доказательства теоремы 1 и замечания к лемме 2 можно получить верхнюю границу на число вершин в фундаментальном прямоугольнике:

Следствие 1. *Пусть φ — совершенная раскраска радиуса $r \geq 2$ бесконечной прямоугольной решетки в n цветов. Тогда число вершин в фундаментальном прямоугольнике для φ не более чем*

$$n^{2(2(2r^2+5r+1)^2+2(2r^2+5r+1)+1)}.$$

Заметим, что если $\mathbf{v}$ и $\mathbf{u}$ — векторы периодичности совершенной раскраски φ, то φ может быть получена объединением цветов (Конструкция B) из трансляционной раскраски, порожденной векторами $\mathbf{v}$ и $\mathbf{u}$ (Конструкция A, пример 2). Следствие 1 дает верхнюю оценку на число цветов в соответствующей трансляционной раскраске: это число не более чем

$$n^{2(2(2r^2+5r+1)^2+2(2r^2+5r+1)+1)}.$$

Таким образом, мы нашли общий способ получения всех совершенных раскрасок радиуса $r \geq 2$ в n цветов, но он требует проверки большого числа случаев, поэтому у нас до сих пор нет даже описания всех совершенных раскрасок радиуса 2 в 2 цвета.

Автор выражает благодарность С. В. Августиновичу за внимание к работе и ценные замечания.

Работа выполнена при поддержке РФФИ (грант 07-01-00248) и Фонда содействия отечественной науке.

Список литературы

1. Axenovich M. On multiple coverings of the infinite rectangular grid with balls of constant radius. Discrete Mathematics, vol. 268, pp. 31–49, 2003.

2. Cvetkovic D. M., Doob M., Zahs H. Spectra of graphs. VEB Deutcher Verlag der Wissenschaften, Berlin, 1980.

3. Godsil C. D., Martin W. J. Quotients of association schemes. J. Combin. Theory, ser. A, vol. 69, no. 2, pp. 185–199, 1995.

4. Puzynina S. A., Avgustinovich S. V. On periodicity of two-dimensional words. сдано в печать в спец. выпуск Theoretical Computer Science.

5. Пузынина С. А. Периодичность совершенных раскрасок бесконечной прямоугольной решетки. Дискрет. анализ и исслед. операций, 1:11, №. 1, с. 79–92, 2004.

ОЦЕНКА ТРУДОЕМКОСТИ АЛГОРИТМА КОППЕРСМИТА-ТОМЕ ВЫЧИСЛЕНИЯ ЛИНЕЙНЫХ ГЕНЕРАТОРОВ ПОСЛЕДОВАТЕЛЬНОСТЕЙ МАТРИЦ НАД КОНЕЧНЫМИ ПОЛЯМИ ДЛЯ СЛУЧАЯ ПОЛЯ GF(2)

В. И. Рудской (Москва)

Одним из наиболее эффективных методов решения больших разреженных систем линейных уравнений над конечными полями является блочный алгоритм Видемана, предложенный Д. Копперсмитом в работе [1]. Он находит решение системы путем построения последовательности матриц специального вида и вычисления линейного генератора этой последовательности.

Введем несколько определений. Пусть $A(X)$ — матрица размера $m \times n$, элементами которой являются формальные степенные ряды над K. Степенью вектора-столбца из многочленов будем называть максимум степеней его элементов. Будем говорить, что $A(X)$ *линейно генерируется* вектором $u(X) \in K[X]^n$ до степени L, если существует такой вектор $v(X) \in K[X]^m$, что

$$A(X)u(X) = v(X) + \Omega(X^L),$$

где $\Omega(X^L) \in K[[X]]^m$ — некоторый вектор из степенных рядов над K, в которых отсутствуют члены степени меньше L. В случае когда $L = +\infty$, то будем говорить, что $A(X)$ линейно генерируется до любой степени. Копперсмит в работе [1] предложил использовать для вычисления линейного генератора наименьшей возможной степени следующий алгоритм.

Алгоритм Копперсмита. Алгоритм вычисляет линейный генератор до степени $L = \frac{N}{m} + \frac{N}{n}$ матрицы $A(X) \in K[X]^{m \times n}, m \geq n$, максимальная степень элементов которой равна $L - 1$. Здесь N намного больше, чем m и n (в блочном алгоритме Видемана N — размерность матрицы системы, m и n — размеры блоков). Алгоритм работает не с векторами $u(X)$ и $v(X)$, а с матрицами, составленными из нескольких таких векторов. Пусть потенциальные генераторы собраны в матрицу $f(X) \in K[X]^{n \times (n+m)}$, а соответствующие им $v(X)$ собраны в матрицу $g(X) \in K[X]^{m \times (n+m)}$. Для $1 \leq j \leq n+m$

введем число δ_j. Это число было названо Копперсмитом «номинальной степенью» и фактически является верхней границей степеней элементов j-го столбца матрицы $A(X)f(X)$. Алгоритм является итерационным и на шаге, соответствующем значению счетчика t, выполняется следующее равенство:

$$A(X)f(X) = g(X) + X^t e(X),$$

где матрица $e(X) \in K[X]^{m\times(m+n)}$ — текущая «невязка», которую мы стремимся обнулить, и каждый столбец этого матричного уравнения удовлетворяет условиям:

$$A(X)f_j(X) = g_j(X) + X^t e_j(X), \tag{1}$$

$$\deg f_j \le \delta_j, \quad \deg g_j < \delta_j, \quad \deg e_j \le L + \delta_j - t \tag{2}$$

(здесь и далее нижний индекс $_j$ обозначает столбец). Кроме того, потребуем выполнения еще одного условия:

$$rank([X^0]e_j) = m, \tag{3}$$

где $[X^k]P$ обозначает коэффициент при X^k в многочлене P.

Инициализация алгоритма. Положим $t_0 = \lceil \frac{m}{n} \rceil$. Все δ_j положим равными t_0. Первые m столбцов матрицы f заполняются таким образом, что столбцы $[X^{t_0}](Af_j)$ для всех $1 \le j \le m$ линейно независимы (это почти всегда можно сделать). Оставшаяся $n \times n$ подматрица инициализируется тождественной матрицей порядка n. Легко проверить, что условия (1)–(3) выполнены.

Итерация алгоритма. На каждом шаге итерации мы стремимся обнулить $[X^0]e$. Это достигается модификацией алгоритма Гаусса. Справедлива следующая

Теорема 1. [2, Theorem 2.2] *Если условия* (1)–(3) *выполняются на шаге* t*, тогда существует алгоритм* `ALG01`*, который по известным* $[X^0]e^{(t)}$ *и* $\delta_1^{(t)}, \ldots, \delta_{m+n}^{(t)}$ *вычисляет матрицу* $P^{(t)}$ *размерности* $(m+n)\times(m+n)$ *и числа* $\delta_1^{(t+1)}, \ldots, \delta_{m+n}^{(t+1)}$*, такие, что*

$$f^{(t+1)} = f^{(t)}P^{(t)},$$

$$g^{(t+1)} = g^{(t)}P^{(t)},$$

$$e^{(t+1)} = e^{(t)}P^{(t)}\frac{1}{X},$$

и числа $\delta_1^{(t+1)}, \ldots, \delta_{m+n}^{(t+1)}$ *удовлетворяют условиям* (1)–(3) *на шаге* $t+1$*. Кроме того, выполнено равенство*

$$\sum_j \delta_j^{(t+1)} - \sum_j \delta_j^{(t)} = m.$$

Доказательство теоремы проводится конструктивно с явным описанием алгоритма из работы [1]. Сложность алгоритма `ALGO1` в количестве **процессорных** операций в предположении, что вычисления происходят в поле $GF(2)$, а размеры матриц m, n меньше длины регистра, можно оценить как

$$C_{\texttt{ALGO1}} = \frac{1}{2}(m+n)^2 + 14m(m+n) + 3(m+n) + m.$$

Алгоритм Копперсмита выполняет на каждой итерации алгоритм `ALGO1` до наступления условия $t > \frac{N}{m} + \frac{N}{n} + t_0$. Алгоритм Копперсмита имеет квадратичную (от L) сложность из-за необходимости вычисления $[X^t](Af)$ на каждом шаге. Французский математик Э. Томе в [3] предложил модификацию алгоритма Копперсмита, имеющую субквадратичную сложность.

Алгоритм Копперсмита–Томе. Заметим, что если матрица $e^{(t)}(X)$ известна до степени k, то можно вычислить матрицы $P^{(t)} \dots P^{(t+k-1)}$ не вычисляя $f(X)$. Будем называть *k-контекстом* пару вида $E = (e(X), \Delta)$, где $\Delta = (\delta_j^{(t)})$ и $e(X)$ известна до степени $k-1$ включительно. Пусть E — контекст, соответствующий шагу алгоритма с номером t. Обозначим через $\pi_E^{(a,b)}$ матрицу $P^{(t+a)} \dots P^{(t+b-1)}$. Тогда исходная задача вычисления линейного генератора эквивалентна задаче нахождения $\pi_{E^{(t_0)}}^{(0,L-t_0)}$, где $E^{(t_0)} = (e^{(t_0)}, \Delta^{(t_0)})$ — начальный контекст. Для решения этой задачи Томе предложил рекурсивный алгоритм, действующий по принципу «разделяй и властвуй».

Алгоритм `MSLGDC` (matrix sequences linear generator by divide and conquer).
Вход: b-контекст $E = (e(X), \Delta)$
Выход: матрица $\pi_E^{(0,b)}$
{
$if(b == 0) \quad return\ I_{m+n}$
$if(b == 1) \quad return\ \texttt{ALGO1}(e, \Delta)$
$(e_L, \Delta_L) = ((e\ mod\ X^{\lfloor \frac{b}{2} \rfloor}), \Delta)$
$\pi_L = \texttt{MSLGDC}(e_L, \Delta_L)$
$(e_R, \Delta_R) = (((e\pi_L\ mod\ X^b)\ div\ X^{\lfloor \frac{b}{2} \rfloor}), \Delta\pi_L)$
$\pi_R = \texttt{MSLGDC}(e_R, \Delta_R)$
$\pi = \pi_L \times \pi_R$
$return\ \pi$
}

Теорема 2. [2, Theorem 3.4] *Если поле K поддерживает быстрое преобразование Фурье (FFT)[4], то сложность алгоритма `MSGDC` можно оценить как*

$$M_1 m(m+n)b\log^2 b + 3M_1 m(m+n)^2 b\log b + O((m+n)^2 b\log b),$$

где M_1 — сложность умножения в поле K.

К сожалению, в интересующем нас случае $K = GF(2)$ (возникающему, например, в алгоритмах факторизации больших целых чисел) утверждение теоремы непосредственно применить нельзя, потому что поле $GF(2)$ не поддерживает FFT. Однако можно модифицировать алгоритм Томе для этого случая.

Модификация алгоритма Томе для случая поля $GF(2)$. Рассмотрим алгоритм умножения многочленов из $GF(2)[x]$:

1. Рассматриваем многочлены из $GF(2)[x]$ как многочлены из $\mathbb{Z}[x]$
2. Используем эффективный алгоритм умножения в $\mathbb{Z}[x]$
3. В получившемся многочлене приводим коэффициенты по модулю 2
4. Рассматриваем приведенный многочлен как многочлен над $GF(2)$

Легко проверить корректность описанного алгоритма. Его сложность можно оценить как $M_{\mathbb{Z}}(n) + O(n)$, где $M_{\mathbb{Z}}(n)$ обозначает сложность умножения двух многочленов из $\mathbb{Z}[x]$ степени меньше n.

Будем рассматривать многочлен из $\mathbb{Z}[x]$ как многочлен над полем комплексных чисел $\mathbb{C}[x]$. Как известно, поле комплексных $\mathbb{C}$ чисел поддерживает FFT, то есть для умножения многочленов в $\mathbb{C}[x]$ можно использовать быстрое преобразование Фурье. С теоретической точки зрения это означает, что оценки, указанные в теореме 2, справедливы, при условии, что M_1 обозначает сложность умножения в поле $\mathbb{C}$. Расширение модели приведет к появлению членов порядка

$$O((m+n)^2 b) \lessapprox O((m+n)^2 b \log b),$$

которыми можно пренебречь при асимптотической оценке. Отметим, что указанные оценки линейны по числу умножений в поле и субквадратичны по степени рассматриваемых многочленов.

При реализации на ЭВМ операции над комплексными числами реализуются как операции над парами вещественных чисел, при этом операции над вещественными числами выполняются приближенно. При использовании высокой точности сложность операций будут зависеть от битовой длины чисел и, как будет показано далее, от степени перемножаемых многочленов. При реализации надо обеспечить точность вычисления, достаточную для однозначного определения коэффициентов при обратном переходе из $\mathbb{C}[x]$ в $GF(2)[x]$. Можно показать, что для умножения двух многочленов степени не выше b достаточно обеспечить точность

$$\varepsilon < \left(b^3 (3 \log_2 b + 4)\right)^{-1}.$$

При этом длина целой части чисел, над которыми производятся операции не превысит $3\log_2 b$ и следовательно общее число двоичных знаков должно быть не меньше

$$l(b) = 3\log_2 b + \log_2 \varepsilon = 6\log_2 b + \log_2(3\log_2 b + 4).$$

Вернемся к оценке величины M_1 для многочленов степени не выше b. Если использовать стандартный алгоритм умножения чисел, квадратичный по длине входа, то сложность операции умножения в $\mathbb{C}$ можно оценить как $M_1(b) = 4l(b)^2 + 2l(b)$, а сложность сложения как $M_2(b) = 2l(b)$ бинарных операций. Количество процессорных операций будет совпадать с указанными оценками с точностью до постоянного множителя, определенного разрядностью процессора.

Оценим сложность алгоритма Копперсмита–Томе вычисления $\pi_E^{(0,L)}$. Будем использовать арифметику с фиксированной длиной: для любой глубины рекурсии арифметические операции будут проводится над числами длины $l(L)$. Наибольшую сложность имеют операции $\pi = \pi_L \times \pi_R$ и

$$e_R = \left(\left(e\pi_L \ mod\ X^b \right) \ div\ X^{\lfloor \frac{b}{2} \rfloor} \right).$$

Для их реализации воспользуемся быстрым преобразование Фурье. Обозначим через $C(b)$ сложность алгоритма Копперсмита-Томе. Легко проверить, что она удовлетворяет рекурсивному равенству:

$$\begin{aligned} C(b) = {} & 2C\left(\frac{b}{2}\right) + 2m(m+n)\left(M_1\frac{b}{2}\log b + M_2 b\log b\right) \\ & + 3(m+n)^2\left(M_1\frac{b}{2}\log b + M_2 b\log b\right) + (m+n)^2(M_1+M_2)b \\ & + m(m+n)^2(M_1+M_2)b + (m+n)^3(M_1+M_2)b + 3m(m+n), \end{aligned}$$

$$C(1) = C_{\texttt{ALGO1}}(m,n).$$

Если предположить, что интересующее нас значение $L = 2^t$, то $C(L)$ оценивается величиной:

$$\frac{1}{2}F_1 L\log^2 L + \left(F_2 - \frac{1}{2}F_1\right) L\log L + \left(C_{\texttt{ALGO1}}(m,n) + 3(m+n)m\right) L,$$

где

$$F_1 = \left(\frac{1}{2}M_1(L) + M_2(L)\right)(m+n)(4m+3n),$$

$$F_2 = (M_1(L) + M_2(L))(m+n)^2(2m+n+1).$$

Или асимптотически более грубо, с учетом всех обозначений:

$$C(L) \approx O\left((m+n)^2 L \log^4 L + (m+n)^3 L \log^3 L\right).$$

Таким образом, нами показана возможность использования алгоритма Копперсмита–Томе вычисления линейного генератора последовательности матриц над конечным полем для случая поля $GF(2)$ с сохранением асимптотической субквадратичной оценки сложности.

Полученная оценка довольно точная, что позволяет сравнить алгоритмы `MSLGDC` с FFT и `MSLGDC` с обычным алгоритмом умножения многочленов, имеющим сложность $O(b^2)$, но с маленькой константой в $O(\cdot)$. Сравнение показывает, что для 128-разрядного (например, векторного) процессора и размеров блоков $m = n = 128$ асимптотическое преимущество проявляется при размерах системы порядка $6 \cdot 10^5$. На практике, например, в алгоритмах факторизации больших целых чисел, размеры систем могут достигать порядка $10^6 \sim 10^8$. В этом случае применение алгоритма `MSLGDC` с FFT оправдано и будет давать выигрыш по времени в несколько порядков.

Список литературы

1. Coppersmith D. Solving linear equations over $GF(2)$ via block Wiedemann algorithm. Math. Comp. 62, 205 (Jan. 1994), 333-350.

2. Thomé E. Fast computation of linear generators for matrix sequences and application to the block Wiedemann algorithm. In B. Mourrain, editor, ISSAC '2001, pages 323-331. ACM Press, 2001a. Proceedings

3. Thomé E. Fast Subquadratic computation of vector generating polynomials and improvement of the block Wiedemann algorithm // J. Symbolic Computation. — 2002.

4. von zur Gathen J. and Gerhard J. Modern Computer Algebra. Cambridge University Press, Cambridge, England, 1999.

О ГЛУБИНЕ СХЕМ ДЛЯ МНОГОКРАТНОГО СЛОЖЕНИЯ И УМНОЖЕНИЯ ЧИСЕЛ

И. С. Сергеев (Москва)

В настоящей работе рассматривается подход к построению схем из функциональных элементов, реализующих многократное сложение и умножение чисел с небольшой глубиной. Обзорная лекция, посвященная минимизации

глубины таких схем, была прочитана А. В. Чашкиным на одной из предыдущих школ этой серии [6]. Схемы строятся над базисом из всех двухвходовых элементов. Понятия сложности и глубины схем изложены в [3].

В начале 60-х гг. Ю. П. Офман [2] и ряд зарубежных авторов (см. [8]) предложили способ реализации умножения n-разрядных чисел схемой глубины $O(\log n)$. В этом способе умножение сводится к n-кратному сложению (как в школьном методе), которое, в свою очередь, сводится к обычному сложению при помощи схемы компрессоров.

Под (p,q)-компрессором, где $q<p$, понимается схема, по набору из p чисел вычисляющая q новых чисел с сохранением суммы, и имеющая глубину, не зависящую от разрядности слагаемых. Самым простым и наиболее популярным является (3,2)-компрессор. Он преобразует набор из трех чисел $X=[x_{k-1},\ldots,x_0]$, $Y=[y_{k-1},\ldots,y_0]$, $Z=[z_{k-1},\ldots,z_0]$ в пару чисел $U=[u_k,\ldots,u_1,0]$ и $V=[v_{k-1},\ldots,v_0]$, таких, что $U+V=X+Y+Z$. Пара разрядов (u_{i+1},v_i) вычисляется подсхемой, изображенной на рис. 1. Таким образом, k-разрядный (3,2)-компрессор имеет сложность $5k$ и глубину 3.

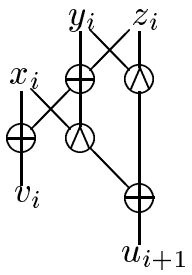

Рис. 1

При оптимизации глубины схем из (3,2)-компрессоров существенно используется несимметричность глубин выходов компрессора относительно глубин входов. В стандартном способе из двух (3,2)-компрессоров строится (4,2)-компрессор, используя который несложно построить схему сведения n-кратного сложения к обычному с глубиной $4\lceil\log_2 n\rceil-3$ (эта конструкция описана в [6] для другой интерпретации входов и с менее аккуратной оценкой глубины).

Обозначим через $D(n)$ глубину минимальной реализации сведения n-кратного сложения к обычному схемой из (3,2)-компрессоров. В дальнейшем для упрощения изложения, под входами и выходами компрессора будут пониматься числа-слагаемые, глубину числа определяет разряд с наибольшей глубиной. Асимптотически точная оценка величины $D(n)$ была получена в [8]. Пусть $\lambda=1,205\ldots$ — единственный вещественный корень уравнения $\lambda^3+\lambda^2-\lambda-2=0$. Справедлива

Теорема 1. [8] $\log_\lambda n-3,3<D(n)<\log_\lambda n+O(1)$.

Отметим, что $\log_\lambda n\approx 3,71\log_2 n$. Нижняя оценка следует из соотношения $\lambda^{D(n)}+\lambda^{D(n)-1}\geq n$, которое вытекает из следующей простой леммы.

Лемма 1. *Пусть a, b, c — глубины входов $(3,2)$-компрессора; d и $d-1$ — глубины выходов, тогда $\lambda^d+\lambda^{d-1}\geq\lambda^a+\lambda^b+\lambda^c$.*

Верхняя оценка доказывается в [8] общим, но практически не эффективным методом. Константа, которая скрывается за обозначением $O(1)$,

достаточно велика; кроме того, построенная методом [8] схема содержит примерно в шесть раз больше компрессоров, чем необходимо. На самом деле, верна

Теорема 2. *Для любого $n > 3$ выполнено: $D(n) > \log_\lambda n - 2,7$. Кроме того, существует схема Λ сведения n-кратного сложения к обычному, состоящая из $n-2$ компрессоров, глубина которой не превосходит $\log_\lambda n - 0,8$, а сложность — $5(nk + 4n - 2k)$, где k — разрядность суммируемых чисел.*

Перед тем, как дать пояснения к доказательству, введем некоторые понятия. Будем считать компрессор расположенным на глубине d, если его выходы имеют глубины $d + 2$ и $d + 3$. Пусть $T \subset \mathbf{N} \cup \{0\}$. Положим $\sigma(T) = \sum_{t \in T} \lambda^t$. Через S_r обозначим схему, образованную компрессорами схемы S, расположенными на глубинах, меньших r. Через $T(S_r)$ обозначим множество глубин выходов схемы S_r, в котором числа, меньшие r, заменены на r. Положим $\sigma(S_r) = \sigma(T(S_r))$. Из леммы 1 очевидно, что

$$n = \sigma(S_0) \le \sigma(S_1) \le \ldots \le \sigma(S_{d-2}) = \lambda^d + \lambda^{d-1}, \qquad (1)$$

где n — число входов, а d — глубина схемы S.

Нижняя оценка теоремы 2 следует из (1) и неравенств

$$\sigma(S_1) - \sigma(S_0) \ge n(\lambda - 1)/3, \quad \sigma(S_{d-2}) - \sigma(S_{d-6}) \ge \lambda^{d-5}(\lambda - 1),$$

справедливых для произвольной схемы S.

Для доказательства верхней оценки используется очевидный метод последовательного добавления компрессоров в схему, в котором каждый очередной компрессор располагается на возможно меньшей глубине. При оценке глубины построенной схемы Λ ключевой является следующая лемма, которая доказывается по индукции.

Лемма 2. *Пусть $r > 0$, а m_0, m_1 и m_2 — соответственно количество чисел r, $r + 1$ и $r + 2$ во множестве $T(\Lambda_r)$. Тогда выполнено:*

$$m_0 \le 2m_1 + 2, \quad m_1 \le 1,5m_0 + 2m_2, \quad m_2 \le m_1.$$

Обозначим $\Delta_r = \sigma(\Lambda_{r+1}) - \sigma(\Lambda_r)$. По построению, $\Delta_r = a_r(\lambda - 1)\lambda^r$, $a_r \in \mathbf{Z}$. Из первого неравенства леммы следует, что $a_r \le 2$. При этом, если $a_r = 2$, то, как легко убедиться, $a_{r+1} = 0$. Принимая во внимание $a_{d-4} \le 1$ и $a_{d-3} = 0$ (где d — глубина Λ), получаем

$$\sigma(\Lambda_{d-2}) - \sigma(\Lambda_1) \le (\lambda - 1) \sum_{i=1}^{d-4} \lambda^i,$$

что, с учетом $\Delta_0 \le (\lambda-1)(2+n/3)$, приводит к окончательной оценке $d < \log_\lambda n - 0,8$.

Оценка сложности схемы Λ складывается из величины $5k(n-2)$, отвечающей числу компрессоров, и добавочного члена, отвечающего удлинению чисел-слагаемых с увеличением глубины. Последний оценивается величиной $20n$, что выводится из следующих легко проверяемых фактов: (1) количество компрессоров, расположенных на глубине r не превосходит $(\lambda+1)\lambda^{d-r-1}/(\lambda+2)$ и (2) выход некоторого компрессора, имеющий глубину r, является не более чем $(k+\lfloor r/3\rfloor)$-разрядным числом.

Нижняя оценка теоремы 2 показывает, что глубина постренной схемы не более чем на единицу отличается от оптимальной. Схема, построенная стандартным способом, имеет худшую глубину для всех n, кроме 4, 8, 16, 32, для которых оба метода дают одинаковый результат.

Для окончательного вычисления суммы выходы схемы компрессоров подаются на входы сумматора. Сумматор n-разрядных чисел, построенный методом В. М. Храпченко [4], имеет асимптотически оптимальную глубину $(1+o(1))\log_2 n$. Для n в пределах нескольких тысяч выгоднее использовать другие методы, например, метод М. И. Гринчука с верхней оценкой глубины $2\log_3(16\lfloor n/2\rfloor)$ (см. [1]). Так, для умножения справедливо

Следствие 1. *Существует схема умножения двух n-разрядных чисел сложности $O(n^2)$ и глубины не более $5(\log_2 n+1)$.*

Для сравнения, вариантом метода А. А. Карацубы [2] можно построить схему с асимптотически меньшим порядком сложности $n^{\log_2 3}$, но с глубиной $(11+o(1))\log_2 n$ (см. [6], но там приводится менее аккуратная оценка глубины). Метод Карацубы обычно не применяется при $n < 300$. Вариант метода Шёнхаге—Штрассена [10] имеет сложность $O(n\log n\log\log n)$ и глубину $(9+o(1))\log_2 n$, однако почти не используется на практике.

Отметим, что компрессоры удобно использовать для вычислений по модулю 2^k-1 (перенося k-е разряды промежуточных слагаемых на место младших). В целях минимизации глубины для реализации заключительного модулярного сложения двух чисел можно использовать $2k$-разрядный сумматор.

В заключение — несколько замечаний о применении более сложных компрессоров. Примеры компрессоров, асимптотически более эффективных, чем (3,2)-компрессор, приводились в работах [5] (для базиса $\{\wedge,\vee,{}^-\}$) и [8]. Известны, например, (5,3)-компрессор и (6,3)-компрессор, из которых методом [8] строятся схемы сведения n-кратного сложения к обычному с глубиной асимптотически $3,65\log_2 n$ и $3,57\log_2 n$ соответственно. Можно также построить (11,5)-компрессор с показателем эффективности $3,55\log_2 n$. Для получения наилучшей известной асимптотической оценки $3,44\log_2 n$ [7] используются схемы из т. н. полукомпрессоров [9].

Методы [7–9] сугубо теоретические, однако предложенные компрессоры можно использовать для построения практических схем небольшой глубины. Используя (5,3) и (6,3)-компрессоры наряду с (3,2)-компрессорами, можно строить схемы меньшей глубины, чем описано выше, уже при малых n, в частности, при $n = 32$. Специальный (7,3)-компрессор позволяет реализовать умножение по методу Карацубы с глубиной $(10 + o(1)) \log_2 n$. Уменьшение глубины во всех случаях достигается ценой некоторого увеличения сложности: кажется, неизвестны (p, q)-компрессоры, у которых отношение сложности к $p - q$ меньше, чем $5k$, где k —разрядность слагаемых.

Автор признателен научному руководителю С. Б. Гашкову за постановку задачи и внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994), программы «Ведущие научные школы» (проект НШ–5400.2006.1) и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики» (проект «Синтез и сложность управляющих систем»).

Список литературы

1. Гашков С. Б., Гринчук М. И., Сергеев И. С. О построении схем сумматоров малой глубины. // Дискретный анализ и исследование операций. Серия 1. — 2007. — Т. 14, №1. — С. 27–44.

2. Карацуба А. А., Офман Ю. П. Умножение многозначных чисел на автоматах. // Докл. АН СССР. — 1962. — Т. 145(2). — С. 293–294.

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

4. Храпченко В. М. Об асимптотической оценке времени сложения параллельного сумматора. // Проблемы кибернетики. Вып. 19. — М.: Наука, 1967. — С. 107–120.

5. Храпченко В. М. Некоторые оценки для времени умножения. // Проблемы кибернетики. Вып. 33. — М.: Наука, 1978. — С. 221–227.

6. Чашкин А. В. Быстрое умножение и сложение целых чисел. // В сб. «Дискретная математика и ее приложения». II. — М.: изд-во ЦПИ при мех.-мат. ф-те МГУ, 2001. — С. 91–110.

7. Grove E. Proofs with potential. — Ph.D. thesis, U.C. Berkeley, 1993.

8. Paterson M., Pippenger N., Zwick U. Optimal carry save networks. // LMS Lecture Notes Series. — V. 169. Boolean function Complexity. — Cambridge University Press, 1992. — P. 174–201.

9. Paterson M., Zwick U. Shallow circuits and concise formulae for multiple addition and multiplication. // Comput. Complexity. — 1993. — V. 3. — P. 262–291.

10. Schönhage A., Strassen V., Schnelle multiplikation groser zahlen. // Computing. — 1971. — V. 7. — P. 271–282. [Русский перевод: Шёнхаге А., Штрассен В. Быстрое умножение больших чисел. // Кибернетический сборник. Вып. 10. — М.: Мир, 1973. — С. 87–98].

О СТРОЕНИИ КЛАССОВ ПОДОБИЯ МАТРИЦ ВТОРОГО И ТРЕТЬЕГО ПОРЯДКОВ НАД Z

С. В. Сидоров (Нижний Новгород)

1. Введение

Классическая задача о подобии матриц над полем рациональных чисел $\mathbf{Q}$ (см., например, [1]) естественным образом обобщается на кольцо целых чисел $\mathbf{Z}$. Квадратные матрицы A и B с коэффициентами из поля $\mathbf{Q}$ называются подобными над $\mathbf{Q}$, если существует такая невырожденная матрица S с рациональными коэффициентами, что $AS = SB$ (подобие над $\mathbf{Q}$ будем обозначать $A \approx B$).

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.*

Задача о подобии матриц над $\mathbf{Z}$ рассматривалась многими авторами (см., например, [3,4,5]). Хотя в [3] получен алгоритм определения подобия матриц над $\mathbf{Z}$ в общем случае, строение классов подобия изучено мало. Отношение подобия есть отношение эквивалентности. Следовательно, множество $\mathbf{Z}^{n\times n}$ разбивается на классы подобных матриц. При этом это разбиение различно для отношения подобия над полем $\mathbf{Q}$ и над кольцом $\mathbf{Z}$. Ясно, что подобие матриц над $\mathbf{Q}$ является необходимым условием для подобия над $\mathbf{Z}$, но не является достаточным даже для матриц второго порядка (см. контрпримеры в [2]). Отсюда следует, что класс $K_Q(A)$ матриц, подобных A над $\mathbf{Q}$, разбивается на подклассы матриц, подобных над $\mathbf{Z}$. Обозначим $K_Z(A) = \{B \in \mathbf{Z}^{n\times n} | B \sim A\}$. Тогда $K_Q(A) = \bigcup\limits_{i\in I} K_Z(A_i)$. Если матрицы подобны (над $\mathbf{Z}$ или над $\mathbf{Q}$), то они имеют один и тот же характеристический многочлен $d(\lambda)$. Цель работы — показать разбиение классов подобия для матриц второго и третьего порядков, характеристические многочлены которых раскладываются на линейные множители над $\mathbf{Q}$. В каждом из таких классов найдена каноническая матрица, характеризующая класс.

2. Случай матриц 2×2

Для характеристического многочлена $d(\lambda)$ матрицы $A \in \mathbf{Z}^{2\times 2}$ возможны следующие варианты:
1) $d(\lambda) = (\lambda-\alpha)^2$; 2) $d(\lambda) = (\lambda-\alpha)(\lambda-\beta)$; 3) $d(\lambda) = \lambda^2 + u\lambda + v$ неприводим над $\mathbf{Z}$.

В первом случае A подобна над $\mathbf{Q}$ одной из жордановых матриц:
$J_1(\alpha) = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$, $J_2(\alpha) = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$.

Во втором случае A подобна над $\mathbf{Q}$ матрице
$J_3(\alpha,\beta) = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$.

В третьем случае A подобна над $\mathbf{Q}$ матрице Фробениуса
$F_1 = \begin{pmatrix} -u & -v \\ 1 & 0 \end{pmatrix}$

Теорема 1. *Если $d(\lambda) = (\lambda-\alpha)^2$, где $\alpha \in \boldsymbol{Z}$, то*
1. $K_Q(J_1(\alpha)) = K_Z(J_1(\alpha)) = \{J_1(\alpha)\}$,
2. $K_Q(J_2(\alpha)) = \bigcup\limits_{s\geq 1} K_Z(R_s(\alpha))$, *где*

$R_s(\alpha) = \begin{pmatrix} \alpha & s \\ 0 & \alpha \end{pmatrix}$, $s \geq 1$ — *каноническая матрица.*

Теорема 2. *Если $d(\lambda) = (\lambda-\alpha)(\lambda-\beta)$, $\alpha,\beta \in \boldsymbol{Z}$, $\beta > \alpha$, то $K_Q(J_3(\alpha,\beta)) = \bigcup\limits_{s=0}^{\lfloor\frac{\beta-\alpha}{2}\rfloor} K_Z(R_s(\alpha,\beta))$, где*

$R_s(\alpha,\beta) = \begin{pmatrix} \alpha & s \\ 0 & \beta \end{pmatrix}$, $0 \leq s \leq \lfloor\frac{\beta-\alpha}{2}\rfloor$ — *каноническая матрица.*

Теорема 3. *Класс $K_Q(F_1)$ разбивается на конечное число классов целочисленно подобных матриц.*

3. Случай матриц 3×3

Пусть матрица $A \in \mathbf{Z}^{3\times 3}$ 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 $J_4(\alpha) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$, $J_5(\alpha) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & \alpha \end{pmatrix}$, $J_6(\alpha) = \begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & \alpha \end{pmatrix}$.
b) если $d(\lambda) = (\lambda-\alpha)(\lambda-\beta)^2$, то A подобна над $\mathbf{Q}$ либо $J_7(\alpha,\beta) =$

$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \beta \end{pmatrix}$, либо $J_8(\alpha,\beta) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 1 \\ 0 & 0 & \beta \end{pmatrix}$.

c) если $d(\lambda) = (\lambda-\alpha)(\lambda-\beta)(\lambda-\gamma)$, то A подобна над $\mathbf{Q}$ матрице $J(\alpha,\beta,\gamma) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$.

Во втором случае A подобна над $\mathbf{Q}$ матрице Фробениуса

$$F_2 = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & -u & -v \\ 0 & 1 & 0 \end{pmatrix}.$$

Теорема 4. *Пусть* $d(\lambda) = (\lambda-\alpha)^3, \alpha \in \mathbf{Z}$. *Тогда*

1. $K_Q(J_4(\alpha)) = K_Z(J_4(\alpha)) = \{J_4(\alpha)\}$,

2. $K_Q(J_5(\alpha)) = \bigcup K_Z(S_d(\alpha))$, $S_d(\alpha) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & d \\ 0 & 0 & \alpha \end{pmatrix}$, $d \geq 1$

3. $K_Q(J_6(\alpha)) = \bigcup K_Z(S_{a,b,r}(\alpha))$,

$S_{a,b,r}(\alpha) = \begin{pmatrix} \alpha & a & r \\ 0 & \alpha & b \\ 0 & 0 & \alpha \end{pmatrix}$, $a, b \geq 1$, $0 \leq r < \text{НОД}(a,b)$.

Теорема 5. *Пусть* $d(\lambda) = (\lambda-\alpha)(\lambda-\beta)^2, \alpha, \beta \in \mathbf{Z}$. *Тогда*

1. $K_Q(J_7(\alpha,\beta)) = \bigcup K_Z(S_d(\alpha,\beta))$,

$S_d(\alpha,\beta) = \begin{pmatrix} \alpha & d & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \beta \end{pmatrix}$, $d = 0$ *или* d *— положительный делитель* $|\beta-\alpha|$ (*не равный* $|\beta-\alpha|$)

2. $K_Q(J_8(\alpha,\beta)) = \bigcup K_Z(S_{a_1,a_2,a_3}(\alpha,\beta))$,

$$S_{a_1,a_2,a_3}(\alpha,\beta) = \begin{pmatrix} \alpha & a_1 & a_2 \\ 0 & \beta & a_3 \\ 0 & 0 & \beta \end{pmatrix},$$

где a_1, a_2, a_3 *удовлетворяют условиям*

I) $a_3 \geq 1$, $0 \leq a_2 \leq \lfloor \frac{|\beta-\alpha|}{2} \rfloor$, $a_1 = 0$

IIa) 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* $d = \text{НОД}(|\beta-\alpha|, a_1)$

IIb) 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) $a_1 = \frac{|\beta-\alpha|}{2}$, $a_3 \geq 1$,

если $\beta - \alpha > 0$, *то* $-\lfloor \frac{a_1 - r}{2} \rfloor \leq a_2 \leq \lfloor \frac{r}{2} \rfloor$,

если $\beta - \alpha < 0$, *то* $-\lfloor \frac{r}{2} \rfloor \le a_2 \le \lfloor \frac{a_1 - r}{2} \rfloor$,
где r — *остаток от деления* a_3 *на* a_1.

Теорема 6. *Пусть* $d(\lambda) = (\lambda - \alpha)(\lambda - \beta)(\lambda - \gamma), \alpha, \beta, \gamma \in \mathbf{Z}, \alpha < \beta < \gamma$. *Тогда* $K_Q(J(\alpha, \beta, \gamma)) = \bigcup K_Z(S_{a_1, a_2, a_3}(\alpha, \beta, \gamma))$,

$$S_{a_1, a_2, a_3}(\alpha, \beta, \gamma) = \begin{pmatrix} \alpha & a_1 & a_2 \\ 0 & \beta & a_3 \\ 0 & 0 & \gamma \end{pmatrix},$$

где a_1, a_2, a_3 *удовлетворяют условиям*
I) $a_1 = 0$, $0 \le a_2 \le \lfloor \frac{\gamma - \alpha}{2} \rfloor$, $0 \le a_3 \le \lfloor \frac{\gamma - \beta}{2} \rfloor$
IIa) если $\gamma - \beta$ – *нечетное, то*
$1 \le a_1 \le \lfloor \frac{\beta - \alpha}{2} \rfloor$, $0 \le a_2 < \gamma - \alpha$, $0 \le a_3 \le \lfloor \frac{\gamma - \beta}{2} \rfloor$
IIb) если $\gamma - \beta$ – *четное, то*
1) $1 \le a_1 \le \lfloor \frac{\beta - \alpha}{2} \rfloor$, $0 \le a_2 < \gamma - \alpha$, $0 \le a_3 \le \frac{\gamma - \beta}{2} - 1$
2) $1 \le a_1 \le \lfloor \frac{\beta - \alpha}{2} \rfloor$, $-\lfloor \frac{a_1}{2} \rfloor \le a_2 \le \lfloor \frac{\gamma - \alpha - a_1}{2} \rfloor$, $a_3 = \frac{\gamma - \beta}{2}$.

Теорема 7. *Класс* $K_Q(F_2)$ *разбивается на конечное число классов целочисленно подобных матриц.*

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. — 552с.

2. Шевченко В. Н., Сидоров С. В. О подобии матриц второго порядка над кольцом целых чисел// Известия ВУЗ. Математика — 2006. — N4. — С. 57–64.

3. Grunewald F. Solution of the conjugacy problem in certain arithmetic groups. in Word Problems II, (ed Adian, Boone, Higman). North-Holland, Amsterdam 1980, pp 101–139.

4. Newman M. Integral matrices. New York and London: Academic Press, 1972. 224p.

5. Latimer C.G. and MacDuffee C.C. A correspondence between classes of ideals and classes of matrices. Annals Math. 34, (1933), 313–316.

О СРЕДНЕЙ МОЩНОСТИ СХЕМ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ

П. С. Степанов (Москва)

Постановка задачи

Пусть дана схема A из функциональных элементов с n входами и одним выходом в базисе B, реализующая функцию F. Пусть булевы наборы $\tilde{\alpha}_i$ подаются на входы схемы с некоторыми вероятностями $p_{\tilde{\alpha}_i}$. Допускается любое распределение $\{p_{\tilde{\alpha}}\}_{\tilde{\alpha}\in B_n}$, где $p_{\tilde{\alpha}} \geqslant 0$ и $\sum\limits_{\tilde{\alpha}\in B_n} p_{\tilde{\alpha}} = 1$.

Определение 1. Пусть f_e — функция, реализуемая на элементе e схемы A. Величину $S(e) = \sum p_{\tilde{\alpha}} f_e(\tilde{\alpha})$, где сумма берется по всем наборам $\tilde{\alpha}$, будем называть *средней мощностью элемента* e.

Определение 2. Пусть $L(A)$ — сложность (число элементов) схемы A, $(e_1, \ldots, e_{L(A)})$ - элементы схемы A. Величина $S(A)$, определяемая соотношением $S(A) = \sum\limits_{i=1}^{L(A)} S(e_i)$, называется *средней мощностью* схемы A.

Определение 3. Схемы, реализующие одинаковые функции, называются *эквивалентными*.

Определение 4. Схема, имеющая наименьшую среднюю мощность среди всех эквивалентных ей схем, называется *оптимальной*.

Очевидно, что для любой схемы существует эквивалентная ей оптимальная схема.

С содержательной точки зрения, если предположить, что при появлении на выходе элемента схемы единицы, этот элемент имеет единичную тепловую мощность, т.е. выделяет единицу тепла в единицу времени, то средняя мощность схемы характеризует среднее тепловыделение схемы. Таким образом, возникает задача построения схемы с наименьшим тепловыделением по произвольному распределению вероятностей входных наборов, реализующей заданную функцию.

В данной статье рассматривается простейший случай этой задачи, когда $B = \{\&\}$, а реализуемая функция F есть конъюнкция n переменных, $F = x_1 \& \ldots \& x_n$.

Структура оптимальной схемы

Определение 5. Схема A называется *бесповторной*, если каждый вход схемы и выход каждого элемента схемы соединен не более, чем с одним входом не более, чем одного элемента схемы или выходом схемы.

Лемма 1. Для любого распределения $\{p_{\tilde{\alpha}}\}$ найдется бесповторная оптимальная схема.

Определение 6. Будем говорить, что схема имеет вид *цепи*, если ее входы и элементы можно занумеровать таким образом, что входы первого элемента будут соединены с двумя первыми входами схемы, а входы i-го элемента будут соединены с выходом $(i-1)$-го элемента и $(i+1)$-м входом схемы для всех $i = 2, \ldots, n-1$.

Теорема 1. Для любого распределения вероятностей $\{p_{\tilde{\alpha}}\}$ входных наборов длины n, среди схем, реализующих конъюнкцию n переменных в базисе $\{\&\}$, найдется оптимальная схема, имеющая вид цепи.

Таким образом, поиск оптимальной схемы достаточно производить только среди схем, имеющих вид цепи. Для исследования этой задачи воспользуемся геометрической интерпретацией.

Геометрическая интерпретация

Распределение вероятностей появления наборов длины n на входах схемы можно рассматривать, как точку в 2^n-мерном евклидовом пространстве. Обратное соответствие, очевидно, имеет место не для всех точек пространства, а только для тех, координаты которых неотрицательны и в сумме дают единицу. Таким образом, множество точек, которым можно поставить в соответствие некоторое распределение вероятностей входных наборов, представляет собой симплекс, натянутый на точки с координатами $(0, \ldots, 1, \ldots, 0)$, где единица занимеает i-ю позицию, $i = 1, \ldots, 2^n$. Обозначим его через T_0. Размерность симплекса T_0 равна $2^n - 1$.

Определение 7. Будем говорить, что схема A *оптимальна в точке* P симплекса T_0, если она оптимальна при распределении вероятностей входных наборов, соответствующем точке P.

Определение 8. Множество всех точек симплекса T_0, в которых схема A оптимальна назовем *областью оптимальности* схемы A.

Модифицируем задачу: вместо того, чтобы искать оптимальную схему по известному распределению вероятностей входных наборов, будем искать для каждой схемы ее область оптимальности.

Оси координат, соответствующие наборам, упорядочим по возрастанию количества единиц в наборах, причем порядок осей, соответствующих наборам с одинаковым числом единиц, выберем произвольный. Другими словами, первая координата соответствует набору из одних нулей, следующие n координат соответствуют наборам с одной единицей и так далее. Последняя координата соответствует набору из одних единиц.

Заметим, что вероятности некоторых наборов не влияют на оптимальность схемы. К таким наборам относятся:

1. Наборы, содержащие менее двух единиц. Мощность схемы на таких наборах будет равна нулю. Таких наборов $n+1$.

2. Набор из одних единиц. Мощность схемы на таком наборе равна сложности схемы, но так как все рассматриваемые схемы имеют одинаковую сложность, то вклад такого набора в среднюю мощность схемы будет одинаковым для всех схем.

Следовательно, при определении оптимальной схемы, вероятности появления указанных наборов можно не учитывать. Таким образом, без ограничения общности можно считать сумму вероятностей наборов, указанных в пунктах 1 и 2 равной нулю, т. е. вместо всего пространства рассматривать его сечение гиперплоскостью. Ограничение симплекса T_0 на полученное сечение обозначим через T_1. Легко показать, что T_1 тоже симплекс. Далее, можно отбросить оси координат, соответствующие несущественным наборам, уменьшив тем самым размерность пространства до $(2^n - n - 2)$. Обозначим полученное пространство через E_n. Такое сужение пространства избавляет нас от необходимости учитывать вероятности несущественных наборов, а также дает возможность наглядно представить пространство распределений при $n = 3$, т. к. его размерность уменьшится с 8 до 3. Проекцию симплекса T_1 на E_n обозначим через T_2.

Очевидно, что, если мы будем знать, как устроены области оптимальности схем в симплексе T_2, то мы будем знать, как устроены области оптимальности схем не только в симплексе T_1, но и в симплексе T_0, т. е. во всем пространстве распределений входных наборов.

Итак, пусть область Z есть пересечение областей оптимальности всех схем в симплексе T_2.

Рассмотрим следующие $n-2$ точки пространства E_n:

$P_k = (\underbrace{0,\ldots,0}_{N_k},\underbrace{p^{(k)},\ldots p^{(k)}}_{C_n^k},0,\ldots,0)$, где $p^{(k)} = \frac{1}{C_n^k}$, $N_k = \sum\limits_{i=2}^{k-1} C_n^i$, $k = 2,\ldots,n-1$. Другими словами, все координаты, соответствующие наборам, содержащим ровно k единиц, равны $p^{(k)}$, а остальные координаты равны нулю.

Теорема 2. Область Z имеет размерность $n-3$ и представляет собой выпуклую линейную оболочку точек P_k, где $k = 2,\ldots,n-1$. А именно, любую точку M области Z можно представить в виде $M = \sum\limits_{i=2}^{n-1} \lambda_i P_i$, где $\sum\limits_{i=2}^{n-1} \lambda_i = 1$, $\lambda_i \geq 0$ при $i = 2,\ldots,n-1$.

Пример

Для $n = 3$ пространство E_3 имеет размерность 3, а оси координат со-

ответствуют наборам $(0,1,1)$, $(1,0,1)$ и $(1,1,0)$. Симплекс T_2 представляет собой треугольник, вершины которого имеют координаты $(1,0,0)$, $(0,1,0)$ и $(0,0,1)$, а область Z состоит из одной точки с координатами $(\frac{1}{3},\frac{1}{3},\frac{1}{3})$.

Для $n = 4$ пространство E_4 имеет размерность 10, а оси координат соответствуют наборам с двумя и тремя единицами. Область Z в этом случае имеет размерность 2 и представляет собой отрезок с концами в точках $P_2 = (\frac{1}{6},\frac{1}{6},\frac{1}{6},\frac{1}{6},\frac{1}{6},\frac{1}{6},0,0,0,0)$ и $P_3 = (0,0,0,0,0,0,\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4})$. Средняя мощность любой оптимальной схемы A на этом отрезке в точке $M = tP_2 + (1-t)P_3, t \in [0,1]$, будет равна $S(A) = \frac{9-7t}{12}$.

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

Список литературы

1. Касим-Заде О.М. Об одной мере сложности схем из функциональных элементов //Проблемы кибернетики. Вып. 38. М.: Наука, 1981.

2. Касим-Заде О.М. О мощности индивидуальных функций //Сборник трудов семинара по дискретной математике и ее приложениям (Москва, МГУ, 2-4 февраля 1993г.). М.: Изд-во механико-математического факультета МГУ, 1998. С. 63–65.

3. Лейхтвейс К. Выпуклые множества. М.: Наука, 1985.

4. Люстерник Л.А. Выпуклые фигуры и многогранники. М.: Гостехиздат, 1956.

5. Яблонский С.В. Введение в дискретную математику. Издание 4-е, стереотипное. М.: Высшая школа, 2003.

ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ им. М. В. КЕЛДЫША
РОССИЙСКОЙ АКАДЕМИИ НАУК

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

МАТЕРИАЛЫ
VI МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

(Москва, 16–21 апреля 2007 г.)

ЧАСТЬ III

Москва 2007

МАТЕРИАЛЫ
VI МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

(Москва, 16–21 апреля 2007 г.)

ЧАСТЬ III

Москва 2007

М34
УДК 519.7

Издание осуществлено при поддержке Российского фонда фундаментальных исследований по проекту 07–01–06018

М34 Материалы VI молодежной научной школы по дискретной математике и ее приложениям (Москва, 16–21 апреля 2007 г.). Часть III. Под редакцией А. В. Чашкина. 2007. — 56 с.

Сборник содержит материалы VI молодежной научной школы по дискретной математике и ее приложениям, проходившей в Москве с 16 по 21 апреля 2007 г. при поддержке Российского фонда фундаментальных исследований (проект 07–01–06018). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание
МАТЕРИАЛЫ
VI МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ
(Москва, 16–21 апреля 2007 г.)

Под общей редакцией А. В. ЧАШКИНА

Ответственный за выпуск *Ф. М. Ковалев*

СОДЕРЖАНИЕ

ИЕРАРХИЯ КЛАССОВ БЕНТ-ФУНКЦИЙ КРАТНОЙ НЕЛИНЕЙНОСТИ

Н. Н. Токарева (Новосибирск)

В работе предлагается иерархия мер нелинейности булевых функций от четного числа m переменных. В ее основе лежит понятие *максимально k-нелинейной* (k-*бент*) функции — функции максимально нелинейной в k различных смыслах одновременно. Обычные бент-функции представляют класс 1-бент-функций. Для $k > j \geq 1$ класс k-бент-функций является собственным подклассом класса j-бент-функций. Для каждого допустимого k приводятся способы построения k-бент-функций и рассматриваются некоторые их свойства; при этом $k = 1, \ldots, m/2$.

1. Введение. Одной из важных характеристик булевой функции в криптографии является мера ее нелинейности. Линейность и близкие к ней свойства булевой функции, как правило, представляют собой богатый источник информации о многих других ее свойствах, что в криптографии, безусловно, является нежелательным. С целью максимизировать меру нелинейности булевой функции в криптографии выделяют класс *максимально нелинейных* (или *бент-*) функций — функций, определяемых как функции, удаленные от множества всех аффинных функций на наибольшее возможное расстояние (см. обзоры методов построения таких функций в [1] и [2]). В геометрической интерпретации векторы значений всех аффинных булевых функций $\langle \mathbf{u}, \mathbf{v} \rangle \oplus a$ от m переменных образуют двоичный линейный код Адамара длины 2^m, а векторы значений бент-функций удалены от этого кода на максимально возможное расстояние $2^{m-1} - 2^{(m/2)-1}$. Говоря неформально, каждая функция f из класса бент-функций "плохо" аппроксимируется аффинными функциями. Именно это свойство булевых функций, использующихся в блочных шифрах, способствует предельному повышению стойкости этих шифров к методам линейного и дифференциального криптоанализа, см. например [3].

Однако, принадлежность функции f классу бент-функций не исключает того, что f может оказаться "хорошо" аппроксимируемой функциями некоторого другого класса, являющимися нелинейными, но обладающими свойством "скрытой линейности— линейности в некотором другом смысле. Тогда использование таких бент-функций, например, в блочном шифре может обнаружить его слабость к соответствующим модификациям вышеупомянутых методов криптоанализа. С целью избежать подобные ситуации мы рассмотрим бент-функции с более сильными свойствами нелинейности, а именно бент-функции от m переменных максимально нелинейные при k различных смыслах линейности одновременно, где k меняется от 1 до $m/2$.

Поясним, что мы подразумеваем под "скрытой линейностью". С 90-х годов в теории кодирования активно стали исследоваться нелинейные коды, образы которых под действием подходящих (как правило, взаимно-однозначных и изометричных) отображений в другие метрические пространства линейны (см. [4], [5], [6]).Такие "скрыто линейные" коды среди всех кодов с некоторыми фиксированными параметрами, зачастую, немногочисленны и по своим свойствам близки к линейным.

Рассмотрим $\mathbb{Z}_2$- и $\mathbb{Z}_4$-линейные коды Адамара. Известно, что $\mathbb{Z}_2$-линейный (т. е. просто линейный) двоичный код Адамара длины 2^m единствен с точностью до эквивалентности. Д. С. Кротовым [7] было показано, что существуют в точности $\lfloor m/2 \rfloor$ попарно неэквивалентных $\mathbb{Z}_4$-линейных кодов Адамара длины 2^{m+1} при $m \geq 3$. Опираясь на данную Д. С. Кротовым [7] классификацию всех таких кодов, рассмотрим серию некоторых "скрыто линейных" двоичных кодов Адамара A_m^k, $1 \leq k \leq \lfloor m/2 \rfloor$ длины 2^m. Множество булевых функций, векторами значений которых являются кодовые векторы кода A_m^k, представляют собой аналог множества аффинных функций — это функции вида $\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus a$, где операция $\langle , \rangle_k$ играет роль скалярного произведения. В рассматриваемой серии кодов каждый код A_m^k получается из линейного четверичного кода $\mathcal{A}_m^k$ заменой элементов $0, 1$ на 0 и элементов $2, 3$ на 1 в каждой координате, где $\mathcal{A}_m^k$ — подкод соответствующего линейного четверичного кода Адамара типа $4^k 2^{m-2k}$, состоящий из всех кодовых векторов, имеющих в первой координате только 0 или 2. При этом код A_m^1 линеен, и все коды $A_m^1, \ldots, A_m^{\lfloor m/2 \rfloor}$ попарно неэквивалентны. Такие "скрыто линейные" коды Адамара выбраны для того, чтобы возникающие новые скалярные произведения $\langle , \rangle_k$ обладали многими свойствами обычного скалярного произведения (см. утверждение 1) и на их основе оказались возможными конструктивные построения. Булеву функцию f от четного числа переменных m назовем *максимально k-нелинейной* (k-*бент*) функцией, $1 \leq k \leq m/2$, если вектор значений функции f удален на наибольшее возможное расстояние $2^{m-1} - 2^{(m/2)-1}$ от каждого кода Адамара A_m^i, $i = 1, \ldots, k$. Обычные бент-функции представляют собой класс 1-бент-функций $\mathfrak{B}_m^1$. Для $k > j \geq 1$ класс k-бент-функций $\mathfrak{B}_m^k$ является собственным подклассом класса j-бент-функций $\mathfrak{B}_m^j$. Для каждого k, $k = 1, \ldots, m/2$, в работе приводятся способы построения k-бент-функций и рассматриваются некоторые их свойства.

2. Необходимые определения. Пусть $\langle \mathbf{u}, \mathbf{v} \rangle$ — обычное скалярное произведение двоичных векторов $\mathbf{u}$ и $\mathbf{v}$. Множество всех булевых функций от m переменных обозначим через $\mathfrak{F}_m$. Через $\mathfrak{A}_m$ обозначим класс всех аффинных булевых функций от m переменных. Каждой булевой функции $f \in \mathfrak{F}_m$ соответствует двоичный вектор $\mathbf{f}$ ее значений длины 2^m. Всюду далее векторы, в отличие от функций, будем выделять полужирным шрифтом. Вес Хэмминга и расстояние Хэмминга обозначим через $wt_H(\cdot)$ и $d_H(\cdot, \cdot)$ соот-

ветственно. Под расстоянием $dist(\cdot,\cdot)$ между булевыми функциями понимается расстояние Хэмминга между соответствующими векторами значений. Напомним, что для функции $f \in \mathfrak{F}_m$ целочисленная функция W_f, заданная на множестве $\mathbb{Z}_2^m$ равенством $W_f(\mathbf{v}) = \sum_{\mathbf{u}\in\mathbb{Z}_2^m}(-1)^{\langle \mathbf{u},\mathbf{v}\rangle \oplus f(\mathbf{u})}$, называется *преобразованием Уолша—Адамара* (или *дискретным преобразованием Фурье*) функции f. Имеет место равенство Парсеваля: $\sum_{\mathbf{v}\in\mathbb{Z}_2^m}\left(W_f(\mathbf{v})\right)^2 = 2^{2m}$, из которого следует, что $\max\limits_{\mathbf{v}\in\mathbb{Z}_2^m}|W_f(\mathbf{v})| \geq 2^{m/2}$. Под *нелинейностью* N_f булевой функции f понимается расстояние от данной функции до множества $\mathfrak{A}_m$, т. е. $N_f = dist(f,\mathfrak{A}_m) = 2^{m-1} - \frac{1}{2}\max\limits_{\mathbf{v}\in\mathbb{Z}_2^m}|W_f(\mathbf{v})|$. Функция $f \in \mathfrak{F}_m$ называется *максимально нелинейной* (m любое), если параметр N_f принимает наибольшее возможное значение, и *бент-функцией* (m четное), если для любого $\mathbf{v} \in \mathbb{Z}_2^m$ справедливо $W_f(\mathbf{v}) = \pm 2^{m/2}$. При четном m эти определения совпадают.

Пусть $\langle \mathbb{Z}_2^n, d_H\rangle$ — метрическое пространство на множестве двоичных векторов длины n с метрикой Хэмминга. Непустое множество $C \subseteq \mathbb{Z}_2^n$ мощности M с минимальным расстоянием d между его различными элементами называется *двоичным* $(n,M,d)_2$*-кодом*, а его элементы — *кодовыми словами*. Параметры n и d называются соответственно *длиной* и *кодовым расстоянием* кода. Код называется *линейным*, если он образует линейное подпространство в $\mathbb{Z}_2^n$. Пусть $\beta,\gamma : \mathbb{Z}_4 \to \mathbb{Z}_2$ — отображения такие, что: $\beta(0) = \beta(1) = 0$, $\beta(2) = \beta(3) = 1$ и $\gamma(0) = \gamma(3) = 0$, $\gamma(1) = \gamma(2) = 1$. Пусть $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$ — отображение Грея: $\phi(c) = (\beta(c),\gamma(c))$ для $c \in \mathbb{Z}_4$. Отображения β,γ и ϕ покоординатно продолжаются до отображений $\beta,\gamma : \mathbb{Z}_4^i \to \mathbb{Z}_2^i$ и $\phi : \mathbb{Z}_4^i \to \mathbb{Z}_2^{2i}$ для любого целого i. Напомним, что ϕ согласно [5] является изометрией, т. е. для любых $\mathbf{x},\mathbf{y} \in \mathbb{Z}_4^i$ выполняется $d_L(\mathbf{x},\mathbf{y}) = d_H(\phi(\mathbf{x}),\phi(\mathbf{y}))$. Четверичный код длины n *линеен*, если он является подгруппой группы $\mathbb{Z}_4^n$. Двоичный код C называется $\mathbb{Z}_4$*-линейным*, если код $\phi^{-1}(C)$ линеен. Пусть m,k положительные целые числа, причем $0 \leq k \leq m/2$. *Ядром* двоичного кода C, содержащего нулевой вектор, называется максимальный линейный подкод $Ker(C)$ кода C такой, что выполняется $\mathbf{x} \oplus C = C$ для любого вектора $\mathbf{x} \in Ker(C)$.

3. Коды Адамара A_m^k. Всюду далее пусть $n = 2^m$. Пусть $\mathbf{G}_m^k$ — четверичная $(m-k)\times n$ – матрица, состоящая из лексикографически упорядоченных столбцов $\mathbf{z}^T$, где $\mathbf{z} \in \{0,1,2,3\}^k \times \{0,2\}^{m-2k}$. Например,

$$\mathbf{G}_1^0 = \begin{pmatrix}02\end{pmatrix}, \mathbf{G}_2^1 = \begin{pmatrix}0123\end{pmatrix}, \mathbf{G}_2^0 = \begin{pmatrix}0022\\0202\end{pmatrix}, \mathbf{G}_3^1 = \begin{pmatrix}00112233\\02020202\end{pmatrix}.$$

Матрицы такого вида впервые рассматривались Д. С. Кротовым в работах [8] и [7] для построения $\mathbb{Z}_4$-линейных кодов Адамара длины $2n$ и получения их полной классификации. Определим взаимно-однозначное отображение

$\phi_k : \mathbb{Z}_4^k \times \mathbb{Z}_2^{m-2k} \to \mathbb{Z}_2^m$ по правилу:

$$\phi_k : (\mathbf{u}', \mathbf{u}'') \to (\phi(\mathbf{u}'), \mathbf{u}'') \text{ для любых векторов } \mathbf{u}' \in \mathbb{Z}_4^k, \mathbf{u}'' \in \mathbb{Z}_2^{m-2k}.$$

Аналогично тому как это было сделано в [6] определим бинарную операцию $\star : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ следующим образом:

$$\mathbf{u} \star \mathbf{v} = \phi_k(\phi_k^{-1}(\mathbf{u}) + \phi_k^{-1}(\mathbf{v})) \text{ для любых векторов } \mathbf{u} \in \mathbb{Z}_2^m, \mathbf{v} \in \mathbb{Z}_2^m.$$

Пусть $\mathbf{C}_m^k = (c_{\mathbf{u},\mathbf{v}}^k)$, $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$, — четверичная $n \times n$-матрица, строками которой являются всевозможные векторы $\mathbf{h}^{\mathbf{u}} = \phi_k^{-1}(\mathbf{u}) \cdot \mathbf{G}_m^k$, расположенные в порядке лексикографического возрастания векторов $\phi_k^{-1}(\mathbf{u})$. Считаем, что нумерация столбцов матрицы $\mathbf{C}_m^k$ также производится в порядке лексикографического возрастания векторов $\phi_k^{-1}(\mathbf{v})$. Например,

$$\mathbf{C}_1^0 = \begin{pmatrix} 00 \\ 02 \end{pmatrix}, \mathbf{C}_2^0 = \begin{pmatrix} 0000 \\ 0202 \\ 0022 \\ 0220 \end{pmatrix}, \mathbf{C}_2^1 = \begin{pmatrix} 0000 \\ 0123 \\ 0202 \\ 0321 \end{pmatrix}, \mathbf{C}_3^0 = \begin{pmatrix} 00000000 \\ 02020202 \\ 00220022 \\ 02200220 \\ 00002222 \\ 02022020 \\ 00222200 \\ 02202002 \end{pmatrix}, \mathbf{C}_3^1 = \begin{pmatrix} 00000000 \\ 02020202 \\ 00112233 \\ 02132031 \\ 00220022 \\ 02200220 \\ 00332211 \\ 02312013 \end{pmatrix}.$$

Пусть четверичный линейный код $\mathcal{A}_m^k$ состоит из векторов $\mathbf{h}^{\mathbf{u}}$ и $\mathbf{h}^{\mathbf{u}} + \mathbf{2}$, где $\mathbf{h}^{\mathbf{u}}$ — строка матрицы $\mathbf{C}_m^k$. Определим двоичный код $A_m^k = \beta(\mathcal{A}_m^k)$. Отметим, что на множестве A_m^k отображение β обратимо, что, вообще говоря, неверно на всём множестве $\mathbb{Z}_2^n$. Определим бинарную операцию $\bullet : A_m^k \times A_m^k \to A_m^k$, согласованную с операцией $+$ на $\mathcal{A}_m^k$:

$$\mathbf{x} \bullet \mathbf{y} = \beta(\beta^{-1}(\mathbf{x}) + \beta^{-1}(\mathbf{y})) \text{ для любых векторов } \mathbf{x}, \mathbf{y} \in A_m^k.$$

Нетрудно видеть, что $(A_m^k, \bullet)$ является абелевой группой.

Теорема 1. *При любом k, $0 \le k \le m/2$, двоичный код A_m^k с заданной на нем групповой операцией $\bullet$ является $(n, 2n, n/2)_2$-кодом Адамара. Коды A_m^0, A_m^1 линейны, при $k \ge 2$ код A_m^k нелинеен, причем размерность ядра кода A_m^k равна $m - k + 1$.*

4. Аналог скалярного произведения $\langle \cdot, \cdot \rangle_k$. Для любого k, $0 \le k \le m/2$, определим бинарную операцию $\langle , \rangle_k : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \to \mathbb{Z}_2$ (аналог скалярного произведения) следующим образом: $\langle \mathbf{u}, \mathbf{v} \rangle_k = \beta(c_{\mathbf{u},\mathbf{v}}^k)$ для любых $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$. Операция $\langle , \rangle_0$ совпадает с обычным скалярным произведением, т. е. $\langle \mathbf{u}, \mathbf{v} \rangle_0 = \langle \mathbf{u}, \mathbf{v} \rangle$. Пусть π_k обозначает подстановку $(1,2)(3,4)\dots(2k-1,2k)$ на m элементах, представленную в виде произведения транспозиций.

Утверждение 1. *Пусть $m \ge 0, k$ — целые, $0 \le k \le m/2$. Для любых векторов $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$ выполняется:*

(i) $\langle \mathbf{u}, \mathbf{v} \rangle_k = \langle \mathbf{v}, \mathbf{u} \rangle_k$;

(*ii*) $\langle a\mathbf{u}, \mathbf{v}\rangle_k = a\langle \mathbf{u}, \mathbf{v}\rangle_k$ *для любого* $a \in \mathbb{Z}_2$;

(*iii*) $\sum_{\mathbf{w}\in\mathbb{Z}_2^m}(-1)^{\langle \mathbf{u},\mathbf{w}\rangle_k \oplus \langle \mathbf{v},\mathbf{w}\rangle_k} = \begin{cases} 2^m, & \text{если } \mathbf{u} = \mathbf{v}, \\ 0, & \text{иначе.} \end{cases}$

(*iv*) $\langle (\mathbf{u}, a), (\mathbf{v}, b)\rangle_k = \langle \mathbf{u}, \mathbf{v}\rangle_k \oplus ab$ *для любых* $a, b \in \mathbb{Z}_2$;

(*v*) $\langle (a, a'), (b, b')\rangle_1 = \langle (a', a), (b, b')\rangle_0$ *для любых* $a, a', b, b' \in \mathbb{Z}_2$;

(*vi*) $\langle (a, a', \mathbf{u}), (b, b', \mathbf{v})\rangle_{k+1} = \langle (a, a'), (b, b')\rangle_\varepsilon \oplus \langle \mathbf{u}, \mathbf{v}\rangle_k$, *для любых* $a, a', b, b' \in \mathbb{Z}_2$, *где параметр* $\varepsilon \in \mathbb{Z}_2$ *определяется равенством* $\varepsilon = \langle \mathbf{u}, \mathbf{v}\rangle_k \oplus \langle \pi_k(\mathbf{u}), \mathbf{v}\rangle_k \oplus 1$;

(*vii*) $\langle \mathbf{u}, \mathbf{w}\rangle_k \oplus \langle \mathbf{v}, \mathbf{w}\rangle_k = \langle \mathbf{u} \star \mathbf{v}, \mathbf{w}\rangle_k \oplus \Big(\langle \mathbf{u}, \mathbf{w}\rangle_k \oplus \langle \pi_k(\mathbf{u}), \mathbf{w}\rangle_k\Big)\Big(\langle \mathbf{v}, \mathbf{w}\rangle_k \oplus \langle \pi_k(\mathbf{v}), \mathbf{w}\rangle_k\Big)$.

Для каждого k, $0 \le k \le m/2$, целочисленную функцию W_f^k, заданную на множестве $\mathbb{Z}_2^m$ равенством $W_f^k(\mathbf{v}) = \sum_{\mathbf{u}\in\mathbb{Z}_2^m}(-1)^{\langle \mathbf{u},\mathbf{v}\rangle_k \oplus f(\mathbf{u})}$ для любого $\mathbf{v} \in \mathbb{Z}_2^m$, назовем *$k$-преобразованием Уолша — Адамара* булевой функции $f \in \mathfrak{F}_m$. Заметим, что W_f^0 совпадает с W_f. Нетрудно видеть, что для W_f^k имеет место аналог равенства Парсеваля, из которого следует неравенство $\max\limits_{\mathbf{v}\in\mathbb{Z}_2^m} |W_f^k(\mathbf{v})| \ge 2^{m/2}$. Пусть каждому вектору $\mathbf{g}$ кода A_m^k отвечает функция $g \in \mathfrak{F}_m$, для которой вектор $\mathbf{g}$ является вектором значений, причем $g(\mathbf{v}) = \langle \mathbf{u}, \mathbf{v}\rangle_k \oplus a$ для некоторых $\mathbf{u} \in \mathbb{Z}_2^m$, $a \in \mathbb{Z}_2$ и произвольного $\mathbf{v} \in \mathbb{Z}_2^m$. Множество всех таких функций от m переменных назовем множеством *k-аффинных функций* и обозначим через $\mathfrak{A}_m^k$. Расстояние между булевой функцией $f \in \mathfrak{F}_m$ и множеством функций $\mathfrak{A}_m^k$ назовем *k-нелинейностью* функции f и обозначим через N_f^k. Можно показать, что имеет место равенство $N_f^k = 2^{m-1} - \frac{1}{2}\max\limits_{\mathbf{v}\in\mathbb{Z}_2^m} |W_f^k(\mathbf{v})|$. Для произвольного k, $1 \le k \le m/2$, булеву функцию $f \in \mathfrak{F}_m$ назовем *максимально k-нелинейной*, если каждый параметр N_f^j, $j = 1, \ldots, k$, принимает наибольшее возможное значение; и *k-бент-функцией*, если все коэффициенты $W_f^j(\mathbf{v})$, $j = 1, \ldots, k$, равны $\pm 2^{m/2}$ (m четно). В случае четного m эти определения эквивалентны. Наибольшее число k, для которого бент-функция является k-бент-функцией, назовем *кратностью нелинейности* этой функции. Класс всех k-бент-функций от m переменных обозначим через $\mathfrak{B}_m^k$. Из утверждения 1 несложно следует, что класс $\mathfrak{B}_m^1$ является классом обычных бент-функций $\mathfrak{B}_m$.

5. Построение k-бент-функций и их свойства. С помощью компьютера нами было проверено, что $|\mathfrak{B}_4^1| = 448$, $|\mathfrak{B}_4^2| = 192$. Функция $\xi(u_1, u_2, u_3, u_4) = u_1u_2 \oplus u_2u_3 \oplus u_3u_4$ представляет пример функции из $\mathfrak{B}_4^1 \setminus \mathfrak{B}_4^2$.

Пусть $\mathfrak{F}_2^1$ — множество всех симметрических функций от двух переменных. Приведем индуктивный способ построения k-бент-функций.

Теорема 2. *Пусть $m, r \in \mathbb{N}$ четны, $k, j \in \mathbb{N}$ — любые, причем $1 \le k \le m/2$. Пусть функция $f \in \mathfrak{F}_{2j+m+r}$ представима в виде*

$$f(a_1, a'_1, \ldots, a_j, a'_j, \mathbf{u}', \mathbf{u}'') = \left(\bigoplus_{i=1}^{j} s_i(a_i, a'_i) \right) \oplus p(\mathbf{u}') \oplus q(\mathbf{u}''),$$

где $s_1, \ldots, s_j \in \mathfrak{F}_2^1, p \in \mathfrak{F}_m$ и $q \in \mathfrak{F}_r$ — функции с непересекающимися множествами переменных. Тогда f принадлежит классу $\mathfrak{B}_{2j+m+r}^{j+k}$ тогда и только тогда, когда $s_1, \ldots, s_j \in \mathfrak{B}_2^1$, $p \in \mathfrak{B}_m^k$ и $q \in \mathfrak{B}_r^1$.

Следствие 1. *Справедливо $\mathfrak{B}_m^k \neq \emptyset$ для любого четного $m \ge 2$ и любого $k \le m/2$.*

Следствие 2. *Для четного $m \ge 2$ справедливо $\mathfrak{B}_m^1 \supset \mathfrak{B}_m^2 \supset \cdots \supset \mathfrak{B}_m^{m/2}$.*

Рассмотрим следующую взаимосвязь k-бент-функций с обычными бент-функциями. Обозначим через S_m^k подгруппу группы S_m подстановок на m координатах, порожденную k транспозициями: $(1,2), (3,4), \ldots, (2k-1, 2k)$. Пусть $\mathfrak{F}_m^k$ обозначает множество всех функций $f \in \mathfrak{F}_m$, постоянных на каждой орбите множества $\mathbb{Z}_2^m$ под действием группы S_m^k. Несложно проверить, что $|\mathfrak{F}_m^k| = 2^{2^{m - k \log \frac{4}{3}}}$, где log обозначает $\log_2$.

Теорема 3. *Справедливо равенство $\mathfrak{F}_m^k \cap \mathfrak{B}_m^k = \mathfrak{F}_m^k \cap \mathfrak{B}_m^1$ для четного $m \ge 2$ и любого k, $1 \le k \le m/2$.*

Однако, функциями из $\mathfrak{F}_m^k \cap \mathfrak{B}_m^1$ весь класс $\mathfrak{B}_m^k$ не исчерпывается. Интересным для дальнейшего исследования представляется вопрос: какие значения принимает кратность нелинейности для функций из известных классов бент-функций?

Работа выполнена при финансовой поддержке интеграционного проекта СО РАН № 35 «Древовидный каталог математических Интернет-ресурсов» и Российского фонда фундаментальных исследований (проект 07-01-00248).

Список литературы

1. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии // Москва, 2004.

2. Dobbertin H. and Leander G. A Survey of Some Recent Results on Bent Functions // Proc. Third Int. Conf. "Sequences and Their Applications" SETA, 2004. LNCS 3486. P. 1–29.

3. Молдовян А. А., Молдовян Н. А., Гуц Н. Д., Изотов Б. В. Криптография: скоростные шифры // СПб.: БХВ-Петербург, 2002. 496 с.

4. Нечаев А. А. Код Кердока в циклической форме // Дискретная математика. Т. 1. Вып. 4. 1989. С. 123–139.

5. Hammons A. R., Kumar P. V., Calderbank A. R., Sloane N. J. A., Solé P. The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes // IEEE Trans. Inform. Theory. 1994. V. 40. № 2. P. 301–319.

6. Borges J., Phelps K. T., Rifa J., Zinoviev V. A. On $\mathbb{Z}_4$-Linear Preparata-Like and Kerdock-Like Codes // IEEE Trans. Inform. Theory. 2003. V. 49. № 11. P. 2834–2843.

7. Krotov D. S. $\mathbb{Z}_4$-linear Hadamard and extended perfect codes // Proc. of the Int. Workshop on Coding and Cryptography WCC 2001, Jan. 8–12, 2001. Paris, France. P. 329–334.

8. Кротов Д. С. $\mathbb{Z}_4$-линейные совершенные коды // Дискретный анализ и исследование операций. Сер. 1. Новосибирск: Ин-т математики СО РАН. 2000. Т. 7. № 4. С. 78–90.

О ВЕРХНЕЙ ОЦЕНКЕ ЧИСЛА РАВНОМЕРНО УПАКОВАННЫХ ДВОИЧНЫХ КОДОВ

Н. Н. Токарева (Новосибирск)

В работе рассматриваются равномерно упакованные (в широком смысле) двоичные коды длины n с кодовым расстоянием d и радиусом покрытия ρ. Показано, что любой такой код однозначно определяется множеством своих кодовых слов весов $\lceil \frac{n}{2} \rceil - \rho, \ldots, \lfloor \frac{n}{2} \rfloor + \rho$, и в случае нечётного d число различных таких кодов не превышает числа $2^{2^{n - \frac{d}{2} \log_2 n + o(\log_2 n)}}$.

1. Введение. Пусть E^n — метрическое пространство на множестве двоичных векторов длины n с метрикой Хемминга $d(\cdot, \cdot)$ (расстояние между двумя векторами равно числу координат, в которых векторы различаются). *Вес Хемминга* $wt(\cdot)$ вектора из E^n определяется как число его ненулевых координат (т. е. как расстояние до нулевого вектора $\mathbf{0}$). Непустое подмножество C в пространстве E^n с минимальным расстоянием d между его различными элементами называется *двоичным* (n, d)*-кодом*, где n — *длина*, а d — *кодовое расстояние* кода. *Радиусом покрытия* ρ двоичного кода C длины n называется максимальное расстояние, на которое может быть удалён от кода C двоичный вектор длины n, т. е. $\rho = \max_{x \in E^n} d(x, C)$. Согласно работе Л. А. Бассалыго, Г. В. Зайцева и В. А. Зиновьева [2] двоичный (n, d)-код C с радиусом покрытия ρ называется *равномерно упакованным в широком смысле*, если существуют действительные числа $\alpha_0, \alpha_1, \ldots, \alpha_\rho$ такие, что для любого двоичного вектора x длины n выполняется равенство $\sum_{i=0}^{\rho} \alpha_i f_i(x) = 1$, где $f_i(x)$ — число кодовых слов кода C, находящихся на расстоянии i от вектора x, $i = 0, 1, \ldots, \rho$. Пусть $d = 2t + 1$. Далее под термином "равномерно упакованный" будем понимать "равномерно упакованный

в широком смысле". С. В. Августиновичем [1] было показано, что каждый двоичный совершенный код длины n с кодовым расстоянием 3 однозначно определяется множеством своих кодовых слов веса $(n-1)/2$. Используя это свойство, в [1] было показано, что число различных совершенных двоичных кодов не превосходит $2^{2^{n-\frac{3}{2}\log n+o(\log n)}}$ (здесь и далее log обозначает логарифм по основанию 2).

Рассмотрим произвольный класс $\mathbb{L}(n,d,\rho;\alpha_0,\ldots,\alpha_\rho)$ двоичных равномерно упакованных (в широком смысле) (n,d)-кодов с радиусом покрытия ρ и параметрами равномерной упаковки $\alpha_0,\ldots,\alpha_\rho$. Считаем, что d и ρ — константы. Число различных кодов в классе $\mathbb{L}(n,d,\rho;\alpha_0,\ldots,\alpha_\rho)$ обозначим через $L_{n,d}$. Используя границу сферической упаковки для мощности (n,d)-кода, несложно получить следующую тривиальную оценку: $L_{n,d}\le 2^{2^{n-\frac{d-1}{2}\log n+o(\log n)}}$. Обобщая метод работы [1], покажем, что любой код из класса $\mathbb{L}(n,d,\rho;\alpha_0,\ldots,\alpha_\rho)$ однозначно определяется множеством своих кодовых слов весов $\lceil n/2\rceil-\rho,\ldots,\lfloor n/2\rfloor+\rho$, и в случае нечётного d имеет место оценка:

$$L_{n,d}\le 2^{2^{n-\frac{d}{2}\log n+o(\log n)}}.$$

Заметим, что параметры ρ и $\alpha_0,\ldots,\alpha_\rho$ в полученную оценку не входят.

2. Необходимые утверждения. Пусть x,y — любые двоичные векторы длины n, и пусть $d(x,y)=k$. Известно (см., например, [4, гл. 21]), что число векторов $z\in E^n$ таких, что $d(x,z)=i$ и $d(y,z)=j$, не зависит от выбора векторов x и y, а зависит лишь от чисел i,j,k,n. Обозначим это число через p_{ijk} (подразумевая также зависимость этого параметра от n). Ясно, что $p_{ijk}=\binom{k}{(i-j+k)/2}\binom{n-k}{(i+j-k)/2}$, если число $i+j-k$ — чётное. В случае нечётного $i+j-k$ имеем $p_{ijk}=0$. Будем считать, что параметр p_{ijk} определён для любых значений i,j и k, $0\le i,j,k\le n$, и равен нулю, если соответствующее множество векторов z пусто.

Пусть C — произвольный код из класса равномерно упакованных кодов $\mathbb{L}(n,d,\rho;\alpha_0,\ldots,\alpha_\rho)$. Обозначим через C_i и E_i множества векторов веса i кода C и пространства E^n соответственно, где $i=0,1,\ldots,n$. Пусть μ_C^i — мощность множества C_i. Набор $\mu(C)=\{\mu_C^0,\mu_C^1,\ldots,\mu_C^n\}$ называется *весовым спектром* кода C, а числа μ_C^i, $i=0,1,\ldots,n$, — *спектральными значениями* кода. В работе [2] приведена формула для вычисления весового спектра (более точно: весовой функции) произвольного равномерно упакованного кода, содержащая ρ неизвестных констант. Для определения этих констант требуется знать любые ρ спектральных значений кода, при которых возможно решение соответствующей системы линейных уравнений (см. подробнее [2]).

Лемма 1. *Весовой спектр произвольного кода C из класса равномерно упакованных кодов $\mathbb{L}(n, d, \rho; \alpha_0, \ldots, \alpha_\rho)$ однозначно определяется значениями $\mu_C^0, \ldots \mu_C^{\rho-1}$.*

Доказательство. Покажем как с помощью известных значений $\mu_C^0, \ldots,$ $\mu_C^{j+\rho-1}$ при любом $j = 0, 1, \ldots, n-\rho$ восстановить значение $\mu_C^{j+\rho}$. При любом $i = 0, 1, \ldots, \rho$ имеет место следующее равенство

$$\sum_{x \in E_j} f_i(x) = \sum_{k=\max\{0, j-i\}}^{j+i} p_{ijk}\ \mu_C^k. \tag{1}$$

Действительно, каждый кодовый вектор веса k находится на расстоянии i в точности от p_{ijk} двоичных векторов веса j. Заметим, что в каждом соотношении (1) при $i = 0, 1, \ldots, \rho-1$ участвуют лишь известные спектральные значения $\mu_C^{\max\{0, j-\rho+1\}}, \ldots, \mu_C^{j+\rho-1}$, а при $i = \rho$ единственным неизвестным спектральным значением является $\mu_C^{j+\rho}$, причём оно входит в это равенство с ненулевым коэффициентом. В силу равномерной упакованности кода C справедливо равенство $\sum_{x \in E_j} \sum_{i=0}^{\rho} \alpha_i f_i(x) = \binom{n}{j}$. Меняя местами знаки суммирования в этом равенстве и пользуясь (1), получаем

$$\sum_{i=0}^{\rho} \alpha_i \sum_{k=\max\{0, j-i\}}^{j+i} p_{ijk}\ \mu_C^k = \binom{n}{j}.$$

Отсюда однозначно определяется значение $\mu_C^{j+\rho}$. Таким образом последовательно восстанавливаются значения $\mu_C^\rho, \ldots, \mu_C^n$.

Следующая лемма является обобщением одного свойства совершенных двоичных кодов, приведённого в работе [1].

Лемма 2. *Множество $X = C_{\lceil n/2 \rceil - \rho} \cup \cdots \cup C_{\lfloor n/2 \rfloor + \rho}$ однозначно определяет код C из класса равномерно упакованных кодов $\mathbb{L}(n, d, \rho; \alpha_0, \ldots, \alpha_\rho)$.*

Доказательство. Для кода C обозначим через A и B следующие множества: $A = C_0 \cup \cdots \cup C_{\lceil n/2 \rceil - \rho - 1}$ и $B = C_{\lfloor n/2 \rfloor + \rho + 1} \cup \cdots \cup C_n$. Тогда $C = A \cup X \cup B$. Несложно заметить, что расстояние между множествами A и B не меньше $2\rho + 1$ и, следовательно, не меньше d. Предположим, что существует другой код $C' = A' \cup X \cup B'$ из класса $\mathbb{L}(n, d, \rho; \alpha_0, \ldots, \alpha_\rho)$, и пусть $B \neq B'$. Тогда код C'', полученный из C заменой множества B на B', также имеет кодовое расстояние d. Покажем, что C'' принадлежит классу $\mathbb{L}(n, d, \rho; \alpha_0, \ldots, \alpha_\rho)$, т. е. является равномерно упакованным кодом с параметрами $\alpha_0, \ldots, \alpha_\rho$. Для произвольного вектора $x \in E^n$ рассмотрим сумму

$$\sum_{i=0}^{\rho} \alpha_i f_i(x), \tag{2}$$

где $f_i(x)$ — число кодовых слов кода C'', находящихся на расстоянии i от вектора x. Обозначим через $T_\rho^D(x)$ множество всех кодовых слов произвольного кода D длины n, содержащихся в шаре радиуса ρ с центром в вершине x, т. е. $T_\rho^D(x) = \{\, y \in D \mid d(x,y) \le \rho \,\}$. По построению кода C'' имеем

$$T_\rho^{C''}(x) = \begin{cases} T_\rho^C(x), & \text{если } wt(x) \le \lfloor n/2 \rfloor, \\ \\ T_\rho^{C'}(x), & \text{если } wt(x) \ge \lceil n/2 \rceil. \end{cases}$$

Так как коды C и C' являются равномерно упакованными с параметрами $\alpha_0, \ldots, \alpha_\rho$, то для любого вектора $x \in E^n$ сумма (2) равна 1. Таким образом, код C'' принадлежит классу равномерно упакованных кодов $\mathbb{L}(n, d, \rho; \alpha_0, \ldots, \alpha_\rho)$.

Поскольку $B \ne B'$, без ограничения общности можно считать, что найдётся вектор $y \in E^n$ такой, что $y \in B$ и $y \notin B'$. Пусть $z = y \oplus \mathbf{1}$, где $\mathbf{1}$ — вектор со всеми координатами, равными 1, и $\oplus$ обозначает покоординатное сложение векторов по модулю 2. Тогда, как нетрудно заметить, выполняется неравенство $wt(z) \le \lceil n/2 \rceil - \rho - 1$, поэтому

$$T_\rho^C(z) = T_\rho^{C''}(z).$$

Отсюда следует, что для равномерно упакованных кодов $z \oplus C$ и $z \oplus C''$ (сдвигов кодов C и C'' соответственно на вектор z) первые $\rho + 1$ спектральных значений одинаковы, т. е.

$$\mu^0_{z\oplus C} = \mu^0_{z\oplus C''}, \ldots, \mu^\rho_{z\oplus C} = \mu^\rho_{z\oplus C''}.$$

Тогда согласно лемме 1 коды $z \oplus C$ и $z \oplus C''$ имеют одинаковые весовые спектры. Но поскольку $\mathbf{1} \in z \oplus C$ и $\mathbf{1} \notin z \oplus C''$, имеем $\mu^n_{z\oplus C} \ne \mu^n_{z\oplus C''}$. Полученное противоречие доказывает лемму.

Лемма 3. *Для любого двоичного кода C длины n с кодовым расстоянием $d = 2t+1$ при любом $i = t, \ldots, n-t$ справедливо неравенство $|C_i| \le \frac{2^t t!}{n^t}\binom{n}{i}$.*

3. Верхняя оценка. Основным результатом работы является

Теорема 1. *Для числа $L_{n,d}$ различных кодов из класса равномерно упакованных кодов $\mathbb{L}(n, d, \rho; \alpha_0, \ldots, \alpha_\rho)$ при нечётном d справедлива оценка $L_{n,d} < 2^{2^{n - \frac{d}{2}\log n + o(\log n)}}$.*

Доказательство. Из леммы 2 следует, что

$$L_{n,d} \le \begin{pmatrix} |E_{\lceil n/2 \rceil - \rho}| + \cdots + |E_{\lfloor n/2 \rfloor + \rho}| \\ |C_{\lceil n/2 \rceil - \rho}| + \cdots + |C_{\lfloor n/2 \rfloor + \rho}| \end{pmatrix}. \qquad (3)$$

Имеем $|E_{\lceil n/2\rceil-\rho}|+\cdots+|E_{\lfloor n/2\rfloor+\rho}|\le(2\rho+1)\binom{n}{\lfloor n/2\rfloor}$. По лемме 3 для произвольного двоичного кода C длины n с кодовым расстоянием d выполняется неравенство $|C_{\lceil n/2\rceil-\rho}|+\cdots+|C_{\lfloor n/2\rfloor+\rho}|\le\frac{\lambda}{n^t}\binom{n}{\lfloor n/2\rfloor}$, где $\lambda=(2\rho+1)\cdot 2^t\cdot t!$ и $t=(d-1)/2$. Применяя формулу Стирлинга получаем $\binom{n}{\lfloor n/2\rfloor}\le 2^{n-\frac{1}{2}\log n+2}$. Тогда в силу (3) имеем

$$L_{n,d}<\left(\begin{array}{c}2^{n-\frac{1}{2}\log n+(2+\log(2\rho+1))}\\ 2^{n-\frac{d}{2}\log n+(2+\log\lambda)}\end{array}\right).$$

Поскольку d и ρ — константы, отсюда и из неравенств $\binom{a}{b}<\left(\frac{3a}{b}\right)^b$ и $c!\le\left(\frac{c+1}{2}\right)^c$ для любых $a>b>1$, $c\ge 1$, вытекает требуемое неравенство.

Приведём примеры классов двоичных кодов, к которым применима теорема 1.

1) Двоичные *совершенные коды* длины $n=2^m-1$ ($m\ge 2$), мощности $2^{n-\log(n+1)}$ с кодовым расстоянием $d=3$ и параметрами равномерной упаковки $\alpha_0=\alpha_1=1$ (см. [5]). Этот частный случай теоремы 1 был доказан в [1]. Другие примеры равномерно упакованных кодов с $d=3$ можно найти в [7] (см. также [2] и [8]).

2) Двоичные *коды Препараты* длины $n=2^m-1$ ($m\ge 4$ чётно), мощности $2^{n-2\log(n+1)+1}$ с кодовым расстоянием $d=5$ и параметрами упаковки

$$\alpha_0=\alpha_1=1,\alpha_2=\alpha_3=3/n$$

(см. [5] и [2]).

Следствие 1. *Число различных двоичных кодов Препараты длины n с кодовым расстоянием 5 не превосходит величины $2^{2^{n-\frac{5}{2}\log n+o(\log n)}}$.*

Отметим, что для числа кодов одного специального подкласса кодов Препараты имеет место более точная оценка. А именно, согласно [6, следствие 2], число неэквивалентных четверичных линейных кодов Препараты длины n с кодовым расстоянием 6 не превосходит величины $2^{n\log n}$.

3) Двоичные примитивные *коды типа БЧХ* длины $n=2^m-1$ ($m\ge 5$ нечётно), мощности $2^{n-2\log(n+1)}$ с кодовым расстоянием $d=5$, радиусом покрытия $\rho=3$ и параметрами

$$\alpha_0=\alpha_1=1,\alpha_2=\alpha_3=\frac{6}{n-1}$$

(см. [2]).

4) Двоичные *коды Геталса* (или *коды типа Геталса*) длины $n=2^m-1$ ($m\ge 4$ чётно), мощности $2^{n-3\log(n+1)+2}$ с кодовым расстоянием $d=7$,

радиусом покрытия $\rho = 5$ и параметрами упаковки

$$\alpha_0 = \alpha_1 = 1, \alpha_2 = \alpha_3 = \frac{15}{2n}, \alpha_4 = \alpha_5 = \frac{30}{n(n-3)}$$

(см. [7] и [3]).

Следствие 2. *Число различных двоичных кодов Гетапса длины n с кодовым расстоянием 7 не превосходит величины* $2^{2^{n-\frac{7}{2}\log n + o(\log n)}}$.

5) Двоичные примитивные *коды типа БЧХ* длины $n = 2^m - 1$ ($m \geq 5$ нечётно) мощности $2^{n-3\log(n+1)}$ с кодовым расстоянием $d = 7$, радиусом покрытия $\rho = 5$ и параметрами упаковки

$$\alpha_0 = \alpha_1 = 1, -\alpha_2 = -\alpha_3 = \alpha_4 = \alpha_5 = \frac{120}{(n-1)(n-7)}$$

(см. [7]).

Автор благодарен Д. С. Кротову за ценные замечания, позволившие существенно расширить множество кодов, для которых справедлива теорема. Работа выполнена при финансовой поддержке интеграционного проекта СО РАН № 35 «Древовидный каталог математических Интернет-ресурсов» и Российского фонда фундаментальных исследований (проект 07-01-00248).

Список литературы

1. Августинович С. В. Об одном свойстве совершенных двоичных кодов // Дискрет. анализ и исслед. операций. 1995. Т. 2, № 1. С. 4–6.

2. Бассалыго Л. А., Зиновьев В. А., Зайцев Г. В. О равномерно упакованных кодах // Проблемы передачи информации. 1974. Т. 10, вып. 1. С. 9–14.

3. Зиновьев В. А., Хеллесет Т. О весовых спектрах сдвигов кодов типа Гетапса // Проблемы передачи информации. 2004. Т. 40, вып. 2. С. 19–36.

4. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки, М: Связь, 1979.

5. Семаков Н. В., Зиновьев В. А., Зайцев Г. В. Равномерно упакованные коды // Проблемы передачи информации. 1971. Т. 7, вып. 1. С. 38–50.

6. Токарева Н. Н. Представление $\mathbb{Z}_4$-линейных кодов Препараты с помощью векторных полей // Проблемы передачи информации. 2005. Т. 41, вып. 2. С. 50–62.

7. Goethals J. M., Van Tilborg H. C. A. Uniformly packed codes // Philips Res. Repts. 1975. V. 30. P. 9–36.

8. Rifa J., Zinoviev V. A. On completely regular codes from perfect codes // Proc. Tenth Int. Workshop "Algebraic and Combinatorial Coding Theory", Zvenigorod, Russia, P. 225–229, September, 3–9, 2006.

СЛОЖНОСТЬ ПРОБЛЕМЫ ВЫПОЛНИМОСТИ ДЛЯ ОДНОГО ЯЗЫКА С ФУНКЦИОНАЛЬНЫМИ БУЛЕВЫМИ ПЕРЕМЕННЫМИ

В. С. Федорова (Москва)

Пусть $X = \{x_1, x_2, \ldots\}$ — множество индивидных переменных, $F = \{f_1^{(n_1)}, f_2^{(n_2)}, \ldots\}$, где n_i, $i = 1, 2, \ldots$, — натуральные числа, есть множество функциональных переменных, $C = \{\&, \vee, \neg\}$ — множество функциональных констант. Будем рассматривать язык L, содержащий индивидные переменные X, функциональные переменные F, функциональные константы C, скобки и запятую.

Определим синтаксис языка L. Назовем термом всякое слово в языке L, удовлетворяющее следующим условиям:

1. Если x принадлежит множеству индивидных переменных X, то x является термом.

2. Если $f_i^{(n)}$ принадлежит множеству функциональных переменных F, а $t_1, t_2, \ldots, t_n$ — термы, то $f_i^{(n)}(t_1, t_2, \ldots, t_n)$ является термом.

3. Если t_1, t_2 — термы, то $t_1 \& t_2$, $t_1 \vee t_2$, $\overline{t_1}$ — также термы.

Если t_1, t_2 — термы, то $t_1 = t_2$ есть равенство. Пусть T — конечная система равенств. Будем говорить, что данные значения всех функциональных переменных, входящих в систему T, выполняют эту систему, если все равенства системы верны при этих значениях функциональных переменных и всех значениях индивидных переменных, входящих в систему T. Конечная система равенств T выполнима, если на множестве всех булевых функций P_2 существуют значения всех функциональных переменных, которые выполняют систему T.

Для языка L можно сформулировать следующую проблему: по произвольной конечной системе равенств T выяснить, является ли T выполнимой. В данной работе получены верхняя и нижняя оценки временной сложности решения этой проблемы.

Получим верхнюю оценку.

Условимся, что все индивидные переменные, участвующие в системе равенств T, занумерованы по возрастанию без пропусков, то есть если в системе T используется индивидная переменная x_i, то в T найдется и переменная x_j, где $1 \leqslant j < i$.

Пусть система T состоит из t равенств, в которых участвуют m различных функциональных переменных

$$f_1^{(n_1)},\ f_2^{(n_2)}, \ldots, f_m^{(n_m)}.$$

Тогда справедлива следующая

Теорема 1. *Существует алгоритм, проверяющий выполнимость системы T за время, не превосходящее по порядку*

$$t \cdot l^3 \cdot 2^l \cdot \left(2^{2^l}\right)^m,$$

где l — длина входа данного алгоритма.

Доказательство. Построим такой алгоритм в классе одноленточных машин Тьюринга с алфавитом $\Psi = \{0, 1, *, \#, e, f, \Lambda\}$. Представим систему равенств T как слово длины l в алфавите Ψ. Для этого закодируем индивидные переменные x_i, $i = 1, 2, \ldots$, их номерами i в двоичной системе счисления; функциональные переменные — равномерным двоичным кодом длины $[\log_2 m] + 1$ с добавлением в начало каждого кода символа $f \in \Psi$; функциональные константы $\&, \vee, \neg$ — соответственно наборами символов $\#, \#\#, \#\#\#$; все запятые и закрывающиеся скобки — символом $*$; символ $=$ заменим e, а между различными равенствами системы T поставим ee. Легко заметить, что общее число индивидных переменных строго меньше l.

Искомая машина Тьюринга перебирает все возможные сочетания (возможно, с повторениями) из m булевых функций, зависящих соответственно от $n_1, n_2, \ldots, n_m$ переменных, и для каждого такого набора — все возможные 2^l значений индивидных переменных (в худшем случае). Теперь для того, чтобы проверить каждое из t равенств системы T, машина Тьюринга копирует код системы T правее на ленту (это займет порядка l^2 тактов) и начинает вычисление, заменяя коды индивидных переменных их запомненными значениями и сдвигая после каждой такой замены правый остаток кода влево за линейное по l число тактов, чтобы избежать разрывов кода. Всего замен может быть не больше l. При этом, если все аргументы функции являются константами, то ее код заменяется на ее значение. Для вычисления всех правых и левых частей равенств системы T потребуется не больше l проходов по скопированному коду. Таким образом, время работы машины Тьюринга не превосходит по порядку

$$\left(2^{2^l}\right)^m \cdot 2^l \cdot (l^2 + t \cdot l^3),$$

что и требовалось доказать.

Для получения нижней оценки временной сложности решения поставленной проблемы будут использоваться конечные однородные структуры. По произвольной конечной однородной структуре (далее — ОС) будет построена система равенств, принадлежащая описанному выше классу. Тогда временная сложность проверки этой системы равенств с использованием ОС и будет являться искомой нижней оценкой.

Введем необходимые понятия. Пусть $A = (Q, q)$ — конечный автомат с множеством состояний $Q = \{q_0, q_1, \ldots, q_{k-1}\}$ и функцией переходов $g : Q^3 \to Q$ (автомат A имеет два входа и два выхода). Для любого натурального числа m через M_m обозначим линейно упорядоченную последовательность из m копий $A_1, A_2, \ldots, A_m$ автомата A, в которой каждый автомат A_i, $1 < i < m$, связан с автоматами A_{i-1} и A_{i+1}. Автоматы A_1 и A_m связаны соответственно только с автоматами A_2 и A_{m-1}. ОС M_m работает в дискретном времени $t = 1, 2, \ldots$ В каждый момент времени $t + 1$ состояние автомата A_i, $1 < i < m$, определяется с помощью функции g состояниями автоматов A_{i-1}, A_i, A_{i+1} в момент времени t. Будем считать, что при вычислении состояний автоматов A_1 и A_m вместо соответственно первого и третьего аргументов в функцию g всегда подставляются значения q_1 и q_2 из Q соответственно.

Согласно приведенным определениям функционирование ОС M_m происходит следующим образом. В начальный момент времени автоматы $A_1, A_2, \ldots, A_m$ устанавливаются в некоторые состояния $q_{i_1}, q_{i_2}, \ldots, q_{i_m}$. Назовем этот набор состояний *инициальным*. В следующий момент времени вектор-состоянием (или конфигурацией) ОС M_m будет набор

$$(g(q_1, q_{i_1}, q_{i_2}), g(q_{i_1}, q_{i_2}, q_{i_3}), \ldots,$$
$$g(q_{i_{m-2}}, q_{i_{m-1}}, q_{i_m}), g(q_{i_{m-1}}, q_{i_m}, q_2)).$$

Затем к полученным состояниям вновь применяется функция g и так далее.

Выделим состояние $q_0 \in Q$ и назовем его заключительным. Также наложим ограничения на функцию переходов g: $g(q_0, q_i, q_j) = q_0$, $g(q_i, q_0, q_j) = q_0$, $g(q_i, q_j, q_0) = q_0$, где $q_i, q_j \in Q$. Тогда если все автоматы ОС M_m придут в заключительное состояние q_0, то в дальнейшем с течением времени конфигурация ОС M_m не поменяется. В этом случае будем считать, что ОС M_m закончила работу, а такую конфигурацию назовем *заключительной*.

Назовем функционирование ОС M_m при заданном инициальном наборе состояний $q_{i_1}, q_{i_2}, \ldots, q_{i_m}$ *правильным*, если ОС преобразовывает этот набор состояний в заключительную конфигурацию. Очевидно, что для того, чтобы выяснить, является ли функционирование данной ОС при заданном инициальном наборе состояний правильным, достаточно проверить лишь первые k^m тактов.

Пусть $Q_I = (q_{i_1}, q_{i_2}, \ldots, q_{i_m})$, $q_{i_j} \in Q$, $j = 1, 2, \ldots, m$, — произвольное инициальное вектор-состояние ОС M_m. Обозначим через $\Pi(A, m, Q_I)$ следующую проблему: функционирует ли ОС, составленная из m копий автомата A, правильно при инициальной конфигурации Q_I.

Теорема 2. *Существует алгоритм, сводящий проблему* $\Pi(A, m, Q_I)$ *к проблеме выполнимости некоторой системы равенств* T *за время порядка* m^2 *так, что система равенств* T *выполнима тогда и только тогда, когда*

ОС, составленная из m копий автомата A, функционирует правильно при инициальном вектор-состоянии Q_I.

Доказательство. Закодируем состояния $q_0, q_1, \ldots, q_{k-1}$ автомата A двоичными наборами длины $l = [\log_2 k] + 1$ так, чтобы код заключительного состояния q_0 являлся единичным булевым вектором, и построим по функции переходов g соответствующие булевы $(2l, l)-$ и $(3l, l)-$операторы G_1, G_2, G_3 следующим образом:

1. Если наборы $(a_1, a_2, \ldots, a_l)$, $(b_1, b_2, \ldots, b_l)$, $(c_1, c_2, \ldots, c_l)$ суть коды состояний q_a, q_b, q_c автомата A, $g(q_a, q_b, q_c) = q_d$ и набор $(d_1, d_2, \ldots, d_l)$ является кодом состояния q_d, то положим

$$G_2(a_1, a_2, \ldots, a_l, b_1, b_2, \ldots, b_l, c_1, c_2, \ldots, c_l) = \\ = (d_1, d_2, \ldots, d_l).$$

На остальных двоичных наборах длины $3l$ (если они есть) оператор G_2 определяется произвольным образом.

2. Если набор $(e_1, e_2, \ldots, e_l)$ кодирует состояние q_1, то в соответствии с соглашением о функционировании автомата A_1 в ОС M_m оператор G_1 задается следующим образом:

$$G_1(x_1, x_2, \ldots, x_{2l}) = G_2(e_1, e_2, \ldots, e_l, x_1, x_2, \ldots, x_{2l}).$$

3. Если набор $(e'_1, e'_2, \ldots, e'_l)$ кодирует состояние q_2, то аналогично получаем

$$G_3(x_1, x_2, \ldots, x_{2l}) = G_2(x_1, x_2, \ldots, x_{2l}, e'_1, e'_2, \ldots, e'_l).$$

Назовем объединение кодов m состояний автоматов $A_1, A_2, \ldots, A_m$ кодом соответствующей конфигурации ОС M_m. Пусть B_1 — булев вектор длины lm, кодирующий некоторый инициальный набор состояний. Тогда при функционировании ОС M_m под действием операторов G_1, G_2, G_3 вектор B_1 будет преобразовываться с течением времени в вектора $B_2, B_3, \ldots, B_{2^{lm}}$. Поскольку различных булевых векторов длины lm ровно 2^{lm}, дальнейшие преобразования будут повторением приведенных выше векторов или их части. Объединим вектора $B_1, B_2, \ldots, B_{2^{lm}}$ в один вектор B длины $lm \cdot 2^{lm}$.

Для упрощения изложения пусть числа l и m являются степенями двойки: $l = 2^{l_1}$, $m = 2^{m_1}$, где l_1, m_1 — целые. В этом случае длина вектора B есть $lm \cdot 2^{lm} = 2^{lm+l_1+m_1}$, и его можно рассматривать как вектор-столбец значений некоторой булевой функции f, зависящей от $n = lm + l_1 + m_1$ переменных.

Построим систему равенств, описывающую вычисление всех значений функции f:

1. Вектор, состоящий из первых lm значений функции f, расположенных в лексикографическом порядке, есть в точности вектор B_1.

2. Поделим вектор значений функции f на блоки длины lm. Тогда любые два соседних блока суть коды двух последовательных конфигураций ОС M_m.

3. Последний блок вектора значений функции f есть в точности код заключительной конфигурации ОС M_m.

Выпишем соответствующие равенства. Здесь $I_i^l(x_1, x_2, \ldots, x_l) = x_i$ — селекторная функция, $1 \leqslant i \leqslant l$, код заключительной конфигурации Q_0 есть единичный булев вектор. Также во всех равенствах необходимо заменить константы 0 и 1 соответственно на термы $x_1 \& \overline{x_1}$ и $x_1 \vee \overline{x_1}$, а функцию эквивалентности $x \sim y$ и импликацию $x \to y$ разложить по системе функциональных констант $\{\&, \vee, \neg\}$ следующим образом: $x \sim y = x\&y \vee \overline{x}\&\overline{y}$, $x \to y = x\&y \vee \overline{x}$.

1. $f(0, 0, \ldots, 0, 0) = I_1^{lm}(B_1)$
   $f(0, 0, \ldots, 0, 1) = I_2^{lm}(B_1)$
   $\ldots$
   $f(0, \ldots, 0, \underbrace{1, \ldots, 1}_{l_1+m_1}) = I_{lm}^{lm}(B_1)$

3. $f(1, \ldots, 1, \underbrace{0, \ldots, 0, 0}_{l_1+m_1}) = 1$
   $f(1, \ldots, 1, \underbrace{0, \ldots, 0, 1}_{l_1+m_1}) = 1$
   $\ldots$
   $f(1, 1, \ldots, 1) = 1$

2. Пусть наборы индивидных переменных $(x_1, x_2, \ldots, x_{lm})$ и $(y_1, y_2, \ldots, y_{lm})$ задают номера конфигураций ОС M_m, причем $(x_1, x_2, \ldots, x_{lm})_2$ есть номер не заключительной конфигурации. Это утверждение представляется термом

$$T_1 = (x_1 \& x_2 \& \cdots \& x_{lm}) \sim 0.$$

Также пусть $(y_1, y_2, \ldots, y_{lm})_2$ — номер конфигурации, непосредственно следующий за номером конфигурации $(x_1, x_2, \ldots, x_{lm})_2$, т. е. $(y_1, y_2, \ldots, y_{lm})_2 = (x_1, x_2, \ldots, x_{lm})_2 \oplus 1$ (сложение по модулю 2). Это описывает терм

$$T_2 = \Big(y_{lm} \sim \overline{x_{lm}}\Big) \& \cdots \& \Big(y_i \sim (\overline{x_i} \& x_{i+1} \& \cdots \& x_{lm} \vee x_i \& \overline{x_{i+1} \& \cdots \& x_{lm}})\Big) \&$$

$$\& \cdots \& \Big(y_1 \sim (\overline{x_1} \& x_2 \& \cdots \& x_{lm} \vee x_1 \& \overline{x_2 \& \cdots \& x_{lm}})\Big).$$

Тогда код состояния крайнего левого автомата A_1 ОС M_m есть значение булева $(2l, l)$-оператора G_1, взятое от кодов состояний автоматов A_1 и A_2 в предыдущий момент времени.

$$T_3 = \Big(f(y_1, \ldots, y_{lm}, \underbrace{0, \ldots, 0}_{l_1+m_1}) \sim$$

$$\sim I_1^l(G_1(f(x_1,\ldots,x_{lm},\underbrace{0,\ldots,0}_{l_1+m_1}),\ldots,f(x_1,\ldots,x_{lm},\underbrace{0,\ldots,0,1}_{m_1},\underbrace{1,\ldots,1}_{l_1})))\Big)\&$$

$$\&\cdots\&\Big(f(y_1,\ldots,y_{lm},\underbrace{0,\ldots,0}_{m_1},\underbrace{1,\ldots,1}_{l_1})\sim$$

$$\sim I_l^l(G_1(f(x_1,\ldots,x_{lm},\underbrace{0,\ldots,0}_{l_1+m_1}),\ldots,f(x_1,\ldots,x_{lm},\underbrace{0,\ldots,0,1}_{m_1},\underbrace{1,\ldots,1}_{l_1})))\Big).$$

Аналогично для крайнего правого автомата A_m ОС M_m:

$$T_4=\Big(f(y_1,\ldots,y_{lm},\underbrace{1,\ldots,1}_{m_1},\underbrace{0,\ldots,0}_{l_1})\sim$$

$$\sim I_1^l(G_3(f(x_1,\ldots,x_{lm},\underbrace{1,\ldots,1,0}_{m_1},\underbrace{0,\ldots,0}_{l_1}),\ldots,f(x_1,\ldots,x_{lm},\underbrace{1,\ldots,1}_{l_1+m_1})))\Big)\&$$

$$\&\cdots\&\Big(f(y_1,\ldots,y_{lm},\underbrace{1,\ldots,1}_{l_1+m_1})\sim$$

$$\sim I_l^l(G_3(f(x_1,\ldots,x_{lm},\underbrace{1,\ldots,1,0}_{m_1},\underbrace{0,\ldots,0}_{l_1}),\ldots,f(x_1,\ldots,x_{lm},\underbrace{1,\ldots,1}_{l_1+m_1})))\Big).$$

Вышесказанное суммирует равенство

$$(T_1\&T_2)\to(T_3\&T_4)=1.$$

Для наборов переменных $(z_1^1,\ldots,z_{m_1}^1)$, $(z_1^2,\ldots,z_{m_1}^2)$ и $(z_1^3,\ldots,z_{m_1}^3)$ аналогичным образом выписываются термы T_5 и T_6, показывающие, что

$$(z_1^2,\ldots,z_{m_1}^2)_2=(z_1^1,\ldots,z_{m_1}^1)_2\oplus 1,\quad (z_1^3,\ldots,z_{m_1}^3)_2=(z_1^2,\ldots,z_{m_1}^2)_2\oplus 1.$$

Тогда терм T_7, утверждающий, что в конфигурации с номером $(y_1,...,y_{lm})$ код любого не крайнего автомата получается из кодов соответствующих трех автоматов в предыдущий момент времени применением $(3l,l)$-оператора G_2, выглядит следующим образом:

$$T_7=\Big(f(y_1,\ldots,y_{lm},z_1^2,\ldots,z_{m_1}^2,\underbrace{0,\ldots,0}_{l_1})\sim$$

$$\sim I_1^l(G_2(f(x_1,\ldots,x_{lm},z_1^1,\ldots,z_{m_1}^1,\underbrace{0,\ldots,0}_{l_1}),\ldots,$$

$$\ldots,f(x_1,\ldots,x_{lm},z_1^3,\ldots,z_{m_1}^3,\underbrace{1,\ldots,1}_{l_1})))\Big)\&$$

$$\& \cdots \& \Big(f(y_1, \ldots, y_{lm}, z_1^2, \ldots, z_{m_1}^2, \underbrace{1, \ldots, 1}_{l_1}) \sim$$

$$\sim I_l^l(G_2(f(x_1, \ldots, x_{lm}, z_1^1, \ldots, z_{m_1}^1, \underbrace{0, \ldots, 0}_{l_1}), \ldots,$$

$$\ldots, f(x_1, \ldots, x_{lm}, z_1^3, \ldots, z_{m_1}^3, \underbrace{1, \ldots, 1}_{l_1}))) \Big).$$

Объединяя, получаем равенство

$$(T_1 \& T_2 \& T_5 \& T_6) \to T_7 = 1.$$

Назовем системой равенств T объединение $2lm + 2$ равенств из пунктов 1, 2, 3.

Длина полученной системы равенств T (число всех символов) есть m^2 по порядку. Таким образом, алгоритм сводит проблему $\Pi(A, m, Q_I)$ к проблеме выполнимости системы T за время порядка m^2, поскольку равномерное кодирование состояний автомата A может быть осуществлено эффективно с линейной сложностью.

Следствие 1. *Нижняя оценка временной сложности решения проблемы выполнимости системы равенств длины l по порядку не меньше $d^{\sqrt{l}}$, $d > 1$.*

Доказательство. Сложность решения проблемы $\Pi(A, m, Q_I)$ по порядку логарифма совпадает со сложностью вычисления функций на одноленточных машинах Тьюринга, работающих с линейной зоной [3]. Таким образом, проблему $\Pi(A, m, Q_I)$ нельзя решить за время, по порядку меньшее, чем d^m, $d > 1$, то есть существенно проще непосредственного перебора. Отсюда с учетом теоремы 2 получаем требуемое утверждение.

Список литературы

1. Марченков С. С. Итерация булевых $(n, n)-$операторов. Вестник Московского Университета. Серия 15. Вычислительная математика и кибернетика. 2006. № 4, стр. 36–41.

2. Кудрявцев В. Б., Подколзин А. С., Болотов А. А. Основы теории однородных структур. Москва. Наука. 1990.

3. Катериночкина Н. Н. Об эквивалентности некоторых вычислительных устройств. Кибернетика. 1970. №5, стр. 27–31.

ПРЕДСТАВИМОСТЬ ЯЗЫКОВ ДВУХСТОРОННИМИ АВТОМАТАМИ

К. Р. Хадиев (Казань)

1. Описание техники

Опишем технику нахождения количества классов эквивалентности для вероятностных автоматов, описанную в статье Anne Condon, Bounded Error Probabilistic Finite State Automata. Далее распространим ее на другие виды автоматов, рассматривая их как частные случаи или расширения вероятностных. **Граф, связанный с автоматом.** Рассмотрим двусторонний вероятностный автомат A, который работает на слове xy и имеет c состояний. Сейчас мы произвольно разбиваем слово на две части, однако в последствии это разбиение будет сознательным. Опишем поведение автомата на границе между словами x и y. Для этого сконструируем граф специального вида.

Рассмотрим граф, обозначим его $M[x]$, — двудольный, в первую долю поместим вершины типа $(q, 1)$, которые будут соответствовать конфигурациям автомата A, когда он находится в состоянии q и читающая головка считывает последний символ слова x. Во вторую долю поместим вершины типа $(q', 2)$, которые будут соответствовать конфигурациям автомата A, когда он находится в состоянии q' и читающая головка считывает первый символ слова y. Добавим дуги из вершин первой доли в вершины второй доли. На дуге, ведущей из вершины $(q, 1)$ в вершину $(q', 2)$ напишем вес p, если p — это вероятность того, что детерминировано начиная работу из состояния q и обозревая последний символ слова x, автомат будет как-то двигаться лишь по слову x и при первом пересечении границы он окажется именно в состоянии q', а значит в конфигурации, соответствующей вершине $(q', 2)$. Добавим в первую долю Вершину $Init$, соответствующую начальной конфигурации автомата A. Из нее будут исходить дуги во вторую долю по тому же принципу: на дуге в вершину $(q', 2)$ напишем вес p, если p — это вероятность того, что детерминировано начиная работу из начальной конфигурации, автомат будет как-то двигаться лишь по слову x и при первом пересечении границы он окажется именно в состоянии q'. Заметим, что все дуги этого графа зависят лишь от слова x, т. к. описывают поведения автомата именно на этой части входного слова.

Рассмотрим еще один граф построенный аналогичным образом, обозначим его через $M[y]$. В первую долю поместим вершины типа $(q, 1)$, которые будут соответствовать конфигурациям автомата A, когда он находится в состоянии q и читающая головка считывает последний символ слова x. Во

вторую долю поместим вершины типа $(q', 2)$, которые будут соответствовать конфигурациям автомата A, когда он находится в состоянии q' и читающая головка считывает первый символ слова y. Добавим дуги из вершин второй доли в вершины вида $(*, 1)$ первой доли. На дуге, ведущей из вершины $(q', 2)$ в вершину $(q, 1)$ напишем вес p, если p — это вероятность того, что детерминировано начиная работу из состояния q' и обозревая первый символ слова y, автомат будет как-то двигаться лишь по слову y и при первом пересечении границы он окажется именно в состоянии q, а значит в конфигурации, соответствующей вершине $(q, 1)$. Добавим в первую долю вершины *Accept* и *Reject*, соответствующие конфигурациям принятия и отвержения автомата A, соответственно. В них будут входить дуги из второй доли по тому же принципу: на дуге из вершину $(q', 2)$, например, в вершину *Accept* напишем вес p, если p — это вероятность того, что детерминировано начиная работу, обозревая первый символ y и находясь в состоянии q', автомат достигнет принимающей конфигурации, двигаясь лишь по слову y. Для *Reject* аналогично. Также для вершин *Accept* и *Reject* добавим петли с весом 1. Заметим, что все дуги этого графа зависят лишь от слова y, т. к. описывают поведения автомата именно на этой части входного слова.

Объединим эти два графа в граф $M[x, y]$. Полученный граф будет иметь $2 * c + 3$ вершин: в первой доле c вершин, соответствующих каждому из состояний, а также вершины *Init*, *Accept* и *Reject*, во второй доле c, для каждого из состояний. Множество дуг графа $M[x, y]$ — это объединение дуг графов $M[x]$ и $M[y]$. Такой граф полностью описывает поведение автомата на слове xy. Пронумеруем вершины от 1 до $2c + 3$, начиная с первой доли и продолжая второй и составим матрицу весов M для графа $M[x, y]$, она будет иметь следующий вид:

$$\left(\begin{array}{c|c} 0 & x \\ \hline y & 0 \end{array}\right).$$

Часть матрицы, помеченная буквой x зависит лишь от слова x, часть y — от y. Каждая из строк является вектором распределения вероятностей перехода из данной конфигурации в во все остальные (представленные в графе).

2. Цепь Маркова

Если мы запишем в ряд те вершины, которые соответствуют конфигурациям, посещенным автоматом при чтении слова xy, то это будет след вычислений $K_0K_1K_2...K_M$, где K_0=*Init*, а K_M — это терминальная конфигурация, а именно *Accept* или *Reject*. Причем Каждая K_i — это случайная

величина, зависящая от K_{i-1}. Этот процесс называется цепью Маркова. Поведение цепи Маркова задает матрица смежности графа $M[x,y]$. Обозначим за $a(xy)$ вероятность того, что цепь Маркова окончится принимающим состоянием, т. е. K_M=*Accept*.

О мере близости. Обычная мера близости не подойдет для двусторонних автоматов, здесь введем новую меру.

Определение. *Назовем два числа p и p' β-близкими, для $\beta \geq 1$, если для них выполнится одно из следующих соотношений:$p = p' = 0$ или $p \neq 0$, $p' \neq 0$ и $\beta^{-1} \leq \frac{p}{p'} \leq \beta$ или, что то же самое $|\log(p) - \log(p')| \leq \beta$*

Определим аналогичную меру близости для матриц.

Определение. *Назовем две матрицы $[p_{ij}]$ и $[p'_{ij}]$ β-близкими, при $\beta \geq 1$, для каждого i и j p_{ij} и p'_{ij} β-близки.*

Из теории цепей Маркова известно, что если матрицы весов для графов $M[x,y]$ и $M[x',y]$ β-близки и имеют по m вершин, то величины $a(x'y)$ и $a(xy)$ β^{2m}-близки.

3. Двусторонние конечные детерминированные автоматы могут распознать лишь регулярные языки

Рассмотрим слово xy ему соответствует цепь Маркова M с матрицей вероятностей переходов $[p_{ij}]$. Если эта матрица строится для 2-КДА, то элементами матрицы могут быть лишь 0 или 1. В каждой строке сумма элементов должна быть равна 1, значит в каждой строке находиться одна и только одна 1.

Лемма 1. *Если два слова x и x' — ε-близки тогда и только тогда, когда матрицы весов соответствующих им графов $M[x]$ и $M[x']$, построенных по 2-КДА, совпадают.*

Определение. *Класс языков 2DFA это все языки, для которых существует 2-х сторонний КДА (2-КДА) их распознающий.*

Определение. *Пусть есть P — 2-КДА, которому соответствуют некоторый язык $L(P)$. Два слова x и x', будем называть эквивалентными относительно языка $L(P)$, если для любого слова y P принимает xy, тогда и только тогда, когда принимает слово $x'y$.*

Теорема 1. *2DFA = Reg.*

Доказательство. Рассмотрим два слова x и x', и соответствующие им $M[x]$ и $M[x']$. Если мы возьмем любое слово y, то поведение автомата на словах xy и $x'y$ полностью определяется матрицами смежности $M[x,y]$ и

$M[x', y]$. Если они совпадают, то x и x' эквивалентны. значит количество классов эквивалентности может быть не больше количества различных матриц смежности $M[x]$(ведь именно этот граф определяет элементы, графа $M[x, y]$, зависящие от x). Таких матриц конечное число, ведь в каждой ячейке могут стоять лишь 0 или 1, и размерность матрицы конечна.

Раз количество классов эквивалентности конечно, то язык, определяемый каждым из 2-КДА регулярен.

Свойство. *Если c — количество состояний 2-КДА, то c^{c+1} — количество состояний 1-КДА.*

Доказательство. В каждой строке матрицы весов графа $M[x]$ стоит только одна 1. Ее возможных положений всего c, т. к. столько вершин во второй доли, а словом x определяются дуги, которые идут именно в эту долю. Дуги из $c+1$ вершин определяются словом $x(Init$ и c — конфигурации на конце слова x), значит различных матриц, может быть всего c^{c+1}.

4. Двусторонние конечные недетерминированные автоматы могут распознать лишь регулярные языки

Определение. *Класс языков 2NFA — это все языки, для которых существует 2-х сторонний КНА (2-КНА) их распознающий.*

Определение. *Класс языков $2PFA_0$ — это все языки, для которых существует 2-х сторонний КВА с точкой сечения 0 (2-КВА$_0$) их распознающий.*

Лемма 2. *$2NFA = 2PFA_0$.*

Доказательство. Возьмем произвольное слово x и 2-КДА A. По A построим 2-КВА$_0$ A', просто на каждом шаге выбирая путь с помощью датчика случайных символов. Если слово x принимается автоматом A, значит есть путь в состояние принятия, следовательно вероятность принятия слова x автоматом A' $P_{Accept}(x) > 0$ и оно примется автоматом A'.

Если слово x не принимается автоматом A, значит нет пути в состояние принятия, следовательно вероятность принятия слова x автоматом A' $P_{Accept}(x) = 0$ и оно не примется автоматом A'. И наоборот.

Теорема 2. *$2NFA = Reg$.*

Доказательство. Докажем, что $2PFA_0 = \mathrm{Reg}$, тогда из леммы будет следовать утверждение теоремы. То, что $Reg \in 2PFA_0$ очевидно, т.к.2-КДА — частный случай 2-КВА$_0$. Докажем, что $2PFA_0 \in Reg$.

Все вероятности переходов лежат в интервале $[2^{-cn}, 1]$, а значит логарифмы от вероятностей в интервале $[-cn, 0]$. Разобьем отрезок $[-cn, 0]$ на

подинтервалы длинны ε. Два слова x и x' ε-близки, если 2^{ε}-близки соответствующие $M[x]$ и $M[x']$, а значит логарифмы их вероятностей $\log(p)$ и $\log(p')$ попадают в один подинтервал. Тогда 2^{ε}-близки $M[x,y]$ и $M[x',y]$, а вероятности достижения вершины принятия $a(xy)$ и $a(x'y)$ $2^{2(2+3)\varepsilon}$-близки. Это означает что,

$$\frac{a(xy)}{a(x'y)} \geq 2^{-2(2+3)\varepsilon}.$$

Если $x'y$ принимается, то $a(x'y) > 0$, значит

$$a(xy) \geq 2^{-2(2c+3)\varepsilon} a(x'y) > 0,$$

причем это равенство выполняется для любого ε. Отсюда следует, что любые два слова x и x' такие, что для соответствующих им $M[x]$ и $M[x']$ логарифмы их вероятностей $\log(p)$ и $\log(p')$ из $[-cn, 0]$, то эти слова эквивалентны. Значит не эквивалентными могут быть только ε не сравнимые слова, у которых матрицы весов графов $M[x]$ и $M[x']$ не совпадают по позициям нулевых компонент, а таких различных матриц конечное количество, ввиду конечности размеров матрицы весов.

Свойство. *Если c — количество состояний 2-КНА, то $2^{c(c+1)}$ — количество состояний 1-КДА, а значит различных классов эквивалентности не может превышать это число.*

Доказательство. В каждой строке матрицы весов графа $M[x]$ могут стоять 1 или 0. их можно расположить 2^c способами, т.к. столько вершин во второй доли, а словом x определяются дуги, которые идут именно в эту долю. Дуги из $+1$ вершин определяются словом $x(Init$ и c — конфигурации на конце слова $x)$, значит различных матриц, может быть всего $(2^{c+1})^c = 2^{c(c+1)}$.

5. Двусторонние конечные вероятностные автоматы могут распознать нерегулярные языки

Более подробно можно посмотреть информацию в статье Anne Condon, Bounded Error Probabilistic Finite State Automata. Приведем лишь результаты.

Количество классов эквивалентности растет как полином n^k, где n — длина слова x, а k — константа, зависящая лишь от c — количества состояний автомата и δ — на сколько изолирована точка сечения.

Языки, классы эквивалентности которых растут быстрее, не распознаются 2-КВА. Например, не распознаются языки с суперполиномиальным $n^{\log n}$ ростом числа классов.

6. Двусторонние конечные квантовые автоматы

Рассмотрим модель 2-qfa(2-KKA), с изолированной точкой сечения. Особенность этой модели в том, что количество различных состояний зависит от n — длинны слова. Пусть $c = dn$, где $d = const$. В вероятностном случае i-я строка матрицы, задающей поведение автомата, была распределением вероятностей попадания в соответствующую конфигурацию из i-й. Здесь вероятность попадания в соответствующую конфигурацию — это вектор из квадратов амплитуд, которые будут для каждого состояния при пересечении границы. А значит, говоря о близости слов, надо говорить о близости матриц, составленных из квадратов амплитуд.

Определим в каких приделах лежат элементы полученной матрицы. Любой двухсторонний вероятностный автомат с рациональными вероятностями, можно представить в виде автомата, все вероятности в котором из множества $\{0, 0.5, 1\}$. Это достигается представлением вероятности в двоичном виде и используя это организуются вероятности переходов. Здесь можно применить тот же способ. Каждый элемент матрицы переходов в квантовом автомате представим в двоичном виде. А так как $2^{-1} = (\sqrt{2})^{-2}$, $2^{-2} = (\sqrt{2})^{-4}$, $2^{-3} = (\sqrt{2})^{-6}$ и т. д., то каждое рациональное число можно разложить по степеням $\sqrt{2}$, т. е. можно рассматривать автомат, элементы матрицы переходов которого из $\{-1, -\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}, 1\}$. Тогда минимальное значение амплитуды по абсолютному значению будет, $2^{-nc/2}$, а квадрата амплитуды 2^{-nc}. Значит логарифмы всех не нулевых элементов матриц квадратов снизу ограничено величиной $-nc$, т. е. $\log p \in [-nc, 0]$, тогда длинна такого отрезка dn^2. Матрицы, которые соответствуют измерениям, не могут увеличить этот отрезок, т. к. после их применения, одни из амплитуд увеличиваются, а другие становятся равными 0.

Теорема 3. *Количество классов эквивалентности в языках, распознаваемых 2-KKA, растет как* $(\frac{d^2n^3}{\gamma} + 1)^{dn(dn+1)}$, *где* γ — *константа.*

Доказательство. Разобьем отрезок $[-cn, 0]$ на подинтервалы длинны ε. Два слова x и x' ε-близки, если 2^{ε}-близки соответствующие $M[x]$ и $M[x']$, а значит логарифмы их вероятностей $\log(p)$ и $\log(p')$ попадают в один подинтервал. Тогда 2^{ε}-близки $M[x, y]$ и $M[x', y]$, а вероятности достижения вершины принятия $a(xy)$ и $a(x'y)$ $2^{2(2+3)\varepsilon}$-близки. Это означает что,

$$\frac{a(xy)}{a(x'y)} \geq 2^{-2(2+3)\varepsilon}.$$

Если $x'y$ принимается, то $a(x'y) > \frac{1}{2} + \delta$, значит и $a(x'y) > \frac{1}{2} + \delta + \delta_1$ для некоторого не нулевого δ_1, тогда справедливо следующее

$$a(xy) \geq 2^{-2(2c+3)\varepsilon} a(x'y) > 2^{-2(2c+3)\varepsilon}(\frac{1}{2} + \delta + \delta_1).$$

Подберем ε так, чтобы слово xy принималось, т. е. $a(xy) > \frac{1}{2} + \delta$. Тогда

$$2^{-2(2c+3)\varepsilon}(\frac{1}{2} + \delta + \delta_1) > \frac{1}{2} + \delta.$$

Откуда

$$\varepsilon < -\log_2 \frac{\frac{1}{2} + \delta}{\frac{1}{2} + \delta + \delta_1} \Big/ 2(2c+3).$$

Можно сказать, что асимптотически $\varepsilon < \frac{\gamma}{c}$.

Заменим в матрицах графов $M[x]$ и $M[x']$ не нулевые вероятности на номера ε-интервалов, в которые они попадают, тогда ε-близость слов эквивалентно равенству таких матриц. В каждой ячейки могут быть числа от 0 до cn/ε, таких позиций $c(c+1)$, а значит различных матриц $(\frac{d^2n^3}{\gamma} + 1)^{dn(dn+1)} = 2^{dn(dn+1)(3\log n + \gamma_1)}$.

Рассмотрим случай, когда время работы автомата ограничивается полиномом $t(n)$. В этом случае все элементы матрицы весов графа M[x], меньшие $t(n)^{-2}$ можно заменить на 0. В худшем случае через границу автомат пройдет $t(n)$ раз, а значит в вероятность принятия такие элементы внесут вклад не больше, чем $t(n)^{-1}$, на это число можно уменьшить ошибку и тогда они не будут ни как влиять на принимаемость слова.

Таким образом все элементы p матрицы весов графа $M[x]$ находятся в интервале $[t(n)^{-2}, 1]$, а их логарифмы в интервале $[-2\log(t(n)), 0]$. Тогда количество ε-интервалов равно $\frac{2\log(t(n))}{\varepsilon} = \frac{2\log(t(n))c}{\gamma} = \frac{2\log(t(n))dn}{\gamma}$, а значит количество различных классов эквивалентности

$$(\frac{2\log(t(n))dn}{\gamma} + 1)^{dn(dn+1)} = 2^{dn(dn+1)(\log(n) + \log(\log(t(n))) + \gamma_1)}.$$

Этого достаточно, чтобы распознавать такие языки как эквивалентность или палиндром.

О РАСШИРЕНИИ ТИПОВ ИГРОВОГО ВЗАИМОДЕЙСТВИЯ В ЯЗЫКЕ ИГРОВЫХ ПРОГРАММ

Р. В. Хелемендик (Москва)

Игровая программа (ИП) представляет собой специальный граф, который описывает выигрышную стратегию при взаимодействии двух сторон. Рассматривается задача синтеза ИП для заданных условий: начальных значений переменных, набора функций (“ходов”), типа взаимодействия и цели,

записываемой формулой логики ветвящегося времени. При этом стратегия, описываемая ИП (в случае её существования), считается выигрышной, если для этой ИП выполнены все компоненты зафиксированного условия.

При исследовании вопроса о выразительных возможностях языков ИП (см. [1]) и логики ветвящегося времени (см. [2]) выяснилось, что первый язык слабее второго. А именно: не для всякой выполнимой формулы, являющейся целью в условии взаимодействия, можно подобрать начальные значения переменных, игровое взаимодействие и ходы сторон, чтобы существовала ИП, удовлетворяющая этому условию. В связи с этим в настоящей работе для языка ИП введено расширение типов игрового взаимодействия (введены тип "максимального выбора" и "вершина-выбиратель") и установлено, что при таком расширении выразительные возможности языков ИП и логики ветвящегося времени эквивалентны.

Игровые правила

Обозначим через $Y = \{y_1, \ldots, y_n\}$, $n \geq 4$, конечное множество переменных, $\overline{y} =< y_1, \ldots, y_n >$ — набор переменных $y_1, \ldots, y_n$; $\mathrm{A} = \{0, \ldots, \mathrm{k}-1\} \cup \{2, 3\}$, $k \geq 2$, — конечную область значений переменных из множества Y, $\overline{\alpha}^{\delta} =< \alpha_1^{\delta}, \ldots, \alpha_n^{\delta} >$ — набор значений этих переменных, $0 \leq \alpha_1^{\delta} \leq 2$, $0 \leq \alpha_j^{\delta} \leq 3, 2 \leq j \leq 3, 0 \leq \alpha_j^{\delta} \leq k-1, 4 \leq j \leq n$; W, B — конечные множества частичных n-мерных функций называемых, соответственно, *множествами ходов белых и чёрных*. Через F_{δ}^{w} (F_{δ}^{b}) обозначим множество функций из W (B), определённых на наборе $\overline{\alpha}^{\delta}$. Выделенный набор $\overline{\alpha}^{\delta_0}$ назовем *начальным*. Пятёрку $R = \langle Y, \mathrm{A}, \overline{\alpha}^{\delta_0}, \mathrm{W}, \mathrm{B} \rangle$ будем называть *игровыми правилами* или *R-правилами*.

Игровое взаимодействие

Игровое взаимодействие характеризует класс ИП согласно их структуре. Переменная y_1 управляет очередностью ходов белых и чёрных. Если $y_1 = 0$ ($y_1 = 1$), то ход белых (чёрных), а если $y_1 = 2$, то может быть как ход белых, так и ход чёрных. Переменная y_2 (y_3) определяет наши взаимотношения с выбором ходов белых (чёрных). Если $y_2 = 0$ ($y_3 = 0$), то это отношение "доверия", когда мы можем выбрать наиболее удобный ход белых (чёрных) с точки зрения достижения цели (см. ниже). Если $y_2 = 1$ ($y_3 = 1$), то это отношение "просчитывания", когда для достижения нашей цели придётся предусмотреть каждый из возможных ходов белых (чёрных). Если $y_2 = 2$ ($y_3 = 2$), то это отношение "максимального выбора", когда рассматривается любое подмножество возможных ходов белых (чёрных), причём каждый ход из этого множества может быть продублирован конечное число раз. Если $y_2 = 3$ ($y_3 = 3$), то возможен любой из этих вариантов. С использованием переменных y_1, y_2, y_3 теперь можно задавать игровыми правилами произвольный тип взаимодействия, в том числе и такие типы, которые управляются ходами сторон.

Игровая программа

Игровая программа (ИП), удовлетворяющая R-правилам, есть связный конечный ориентированный граф $\mathcal{P}$ с вершинами следующих видов: преобразователями, ветвителями, выбирателями и финальными вершинами. Каждая не финальная вершина является преобразователем (ветвителем, выбирателем) белых, либо чёрных.

Функционирование ИП определяется по индукции. Для каждой вершины $v_r^{\overline{\alpha}^\delta, x_r}$ этого графа нижний индекс уникален, $\overline{\alpha}^\delta$ есть набор значений переменных в этой вершине, а x_r является одним из следующих выражений, определяющих вид данной вершины.

• x_r есть $\otimes$. Тогда вершина $v_r^{\overline{\alpha}^\delta, \otimes}$ *финальная*. Она не имеет выходящих дуг.

• x_r есть f_t^{w} (f_t^{b}), где $f_t^{\mathrm{w}} \in F_\delta^{\mathrm{w}} \subseteq \mathrm{W}$ ($f_t^{\mathrm{b}} \in F_\delta^{\mathrm{b}} \subseteq \mathrm{B}$). Тогда вершина $v_r^{\overline{\alpha}^\delta, f_t^{\mathrm{w}}}$ ($v_r^{\overline{\alpha}^\delta, f_t^{\mathrm{b}}}$) называется белым (чёрным) *преобразователем*. Из этого преобразователя выходит единственная дуга, помеченная символом f_t^{w} (f_t^{b}), и эта дуга входит в некоторую вершину $v_{r'_t}^{\overline{\alpha}^{\delta'_t}, x_{r'_t}}$ со значением $\overline{\alpha}^{\delta'_t} = f_t^{\mathrm{w}}(\overline{\alpha}^\delta)$ ($\overline{\alpha}^{\delta'_t} = f_t^{\mathrm{b}}(\overline{\alpha}^\delta)$). Отметим, что в случае $|F_\delta^{\mathrm{w}}| > 1$ ($|F_\delta^{\mathrm{b}}| > 1$) в качестве функции f_t^{w} (f_t^{b}) допускается любой элемент F_δ^{w} (F_δ^{b}).

• x_r есть F_δ^{w} (F_δ^{b}), и $|F_\delta^{\mathrm{w}}| \geq 1$ ($|F_\delta^{\mathrm{b}}| \geq 1$). Тогда вершина $v_r^{\overline{\alpha}^\delta, F_\delta^{\mathrm{w}}}$ ($v_r^{\overline{\alpha}^\delta, F_\delta^{\mathrm{b}}}$) называется белым (чёрным) *ветвителем*. Тогда из этой вершины выходит $h = |F_\delta^{\mathrm{w}}|$ ($h = |F_\delta^{\mathrm{b}}|$) дуг, помеченных соответственно символами f_t^{w} (f_t^{b}), где $f_t^{\mathrm{w}} \in F_\delta^{\mathrm{w}} \subseteq \mathrm{W}$ ($f_t^{\mathrm{b}} \in F_\delta^{\mathrm{b}} \subseteq \mathrm{B}$), и эти дуги входят соответственно в вершины $v_{r'_t}^{\overline{\alpha}^{\delta'_t}, x_{r'_t}}$ со значениями $\overline{\alpha}^{\delta'_t} = f_t^{\mathrm{w}}(\overline{\alpha}^\delta)$ ($\overline{\alpha}^{\delta'_t} = f_t^{\mathrm{b}}(\overline{\alpha}^\delta)$).

• x_r есть F_τ^{w} (F_τ^{b}), и $F_\tau^{\mathrm{w}} \subseteq F_\delta^{\mathrm{w}}$, $|F_\tau^{\mathrm{w}}| \geq 1$ ($F_\tau^{\mathrm{b}} \subseteq F_\delta^{\mathrm{b}}$, $|F_\tau^{\mathrm{b}}| \geq 1$). Тогда вершина $v_r^{\overline{\alpha}^\delta, F_\tau^{\mathrm{w}}}$ ($v_r^{\overline{\alpha}^\delta, F_\tau^{\mathrm{b}}}$) называется белым (чёрным) *выбирателем*. Тогда из этой вершины выходит $h = |F_\tau^{\mathrm{w}}|$ ($h = |F_\tau^{\mathrm{b}}|$) видов дуг, помеченных соответственно символами f_t^{w} (f_t^{b}), где $f_t^{\mathrm{w}} \in F_\delta^{\mathrm{w}} \subseteq \mathrm{W}$ ($f_t^{\mathrm{b}} \in F_\delta^{\mathrm{b}} \subseteq \mathrm{B}$), и эти дуги входят соответственно в вершины $v_{r'_t}^{\overline{\alpha}^{\delta'_t}, x_{r'_t}}$ со значениями $\overline{\alpha}^{\delta'_t} = f_t^{\mathrm{w}}(\overline{\alpha}^\delta)$ ($\overline{\alpha}^{\delta'_t} = f_t^{\mathrm{b}}(\overline{\alpha}^\delta)$). При этом каждая из h видов дуг f_t^{w} (f_t^{b}) может быть продублирована конечное число раз и вести как в уже имеющуюся, так и в новую вершину, значением которых является $\overline{\alpha}^{\delta'_t}$.

Если $\alpha_1^\delta = 0$ и $F_\delta^{\mathrm{w}} = \emptyset$, или $\alpha_1^\delta = 1$ и $F_\delta^{\mathrm{b}} = \emptyset$, или $\alpha_1^\delta = 2$ и $F_\delta^{\mathrm{w}} \cup F_\delta^{\mathrm{w}} = \emptyset$, то вершина с набором $\overline{\alpha}^\delta$ является финальной: $v_r^{\overline{\alpha}^\delta, \otimes}$.

В противном случае вершина $v_{x_r}^{\overline{\alpha}^\delta, \otimes}$ финальной не является, и возможный ее вид (индекс x_r) находится по таблице 1, охватывающей все возможные комбинации значений α_1^δ, α_2^δ, α_3^δ.

Цель в ИП

Цель в ИП есть формула Θ^* логики ветвящегося времени (см. [2]), в которой пропозициональными переменными являются утверждения вида $(y_j = l)$, где $y_j \in Y$, $j \le 4$, $l \le (k-1)$.

Постановка задачи синтеза ИП

Пусть $\mathcal{U} = \langle R, \Theta^* \rangle$. Будем говорить, что ИП $\mathcal{P}_\mathcal{U}$ удовлетворяет условию $\mathcal{U}$, если она удовлетворяет R-правилам и в ней истинна формула Θ^*. Существует ли ИП $\mathcal{P}_\mathcal{U}$, удовлетворяющая условию $\mathcal{U}$? Если существует, то необходимо построить хотя бы одну ИП.

Таблица 1

α_1^δ	α_2^δ	α_3^δ	x_r
0	0	0,1,2,3	f_t^{w}
1	0,1,2,3	0	f_t^{b}
0	1	0,1,2,3	F_δ^{w}
1	0,1,2,3	1	F_δ^{b}
0	2	0,1,2,3	F_τ^{w}
1	0,1,2,3	2	F_τ^{b}
0	3	0,1,2,3	f_t^{w} или F_δ^{w} или F_τ^{w}
1	0,1,2,3	3	f_t^{b} или F_δ^{b} или F_τ^{b}
2	0	0	f_t^{w} или f_t^{b}
2	0	1	f_t^{w} или F_δ^{b}
2	0	2	f_t^{w} или F_τ^{b}
α_1^δ	α_2^δ	α_3^δ	x_r
2	1	0	F_δ^{w} или f_t^{b}
2	1	1	F_δ^{w} или F_δ^{b}
2	1	2	F_δ^{w} или F_τ^{b}
2	2	0	F_τ^{w} или f_t^{b}
2	2	1	F_τ^{w} или F_δ^{b}
2	2	2	F_τ^{w} или F_τ^{b}
2	0	3	f_t^{w} или f_t^{b} или F_δ^{b} или F_τ^{b}
2	1	3	F_δ^{w} или f_t^{b} или F_δ^{b} или F_τ^{b}
2	2	3	F_τ^{w} или f_t^{b} или F_δ^{b} или F_τ^{b}
2	3	0	f_t^{w} или F_δ^{w} или F_τ^{w} или f_t^{b}
2	3	1	f_t^{w} или F_δ^{w} или F_τ^{w} или F_δ^{b}
2	3	2	f_t^{w} или F_δ^{w} или F_τ^{w} или F_τ^{b}
2	3	3	f_t^{w} или F_δ^{w} или F_τ^{w} или f_t^{b} или F_δ^{b} или F_τ^{b}

Теоремы о соответствии

Пусть задано условие $\mathcal{U} = \langle R, \Theta^* \rangle$, $m = \lceil \log_2 k \rceil$. Введём $m(n-3)$ пропозициональных переменных $p_1, \ldots, p_{m(n-3)}$. Заменим в формуле Θ^* каждое утверждение $(y_j = l)$ на конъюнкцию m множителей $p^{\sigma_{j,l,i}}_{m(j-4)+i}$, $1 \le i \le m$, где $p^{\sigma_{j,l,i}}_{m(j-4)+i}$ есть $p_{m(j-4)+i}$, если в двоичной записи m разрядами числа l на i-м месте стоит 1 (в этом случае переменную $p_{m(j-4)+i}$ будем называть положительно входящей для утверждения $y_j = l$), и $p^{\sigma_{j,l,i}}_{m(j-4)+i}$ есть $\neg p_{m(j-4)+i}$ в противном случае. Полученную формулу Θ логики ветвящегося времени назовём *формулой, соответствующей* Θ^*.

Теорема 1. *Если существует ИП $\mathcal{P}_\mathcal{U}$, удовлетворяющая условию $\mathcal{U} = \langle R, \Theta^* \rangle$, то формула Θ, соответствующая Θ^*, выполнима.*

Пусть дана формула логики ветвящегося времени Θ, и $p_1, \ldots, p_m$ - все встречающиеся в ней различные пропозициональные переменные. Положим $Y = \langle y_1, \ldots, y_n \rangle$, $n = m + 3$, $A = \{0, 1, 2, 3\}$, $k = 2$. Заменим каждую подформулу формулы Θ с чётным (в частности, нулевым) числом отрицаний, непосредственно стоящих перед переменной p_j, на подформулу $(y_{j+3} = 1)$, а каждую подформулу с нечётным числом отрицаний, непосредственно стоящих перед переменной p_j – на подформулу $(y_{j+3} = 0)$. Полученную формулу обозначим через Θ^*. В условии $\mathcal{U} = \langle R, \Theta^* \rangle$ тройку $K = \langle Y, A, \Theta^* \rangle$ с зафиксированными и определёнными выше компонентами назовём *каркасом* (условия $\mathcal{U}$), соответствующим формуле Θ.

Теорема 2. *Если выполнимой формуле Θ соответствует каркас $K = \langle Y, A, \Theta^* \rangle$ условия $\mathcal{U}$, то возможно такое доопределение условия $\mathcal{U}$, что существует ИП $\mathcal{P}_\mathcal{U}$, удовлетворяющая этому условию.*

Из теорем 1 и 2 следует, что теперь в языках ИП и логики ветвящегося времени могут быть решены одни и те же задачи. В то же время язык ИП предоставляет более широкие средства для структуризации записи задачи в рамках следующего подхода: указание начальной ситуации; определение правил её изменения и типа взаимодействия; постановка цели.

Работа выполнена при финансовой поддержке программы фундаментальных исследований Отделения математических наук РАН “Алгебраические и комбинаторные методы математической кибернетики” (проект “Оптимальный синтез управляющих систем”).

Список литературы

1. Хелемендик Р. В. О расширении логического языка игровых программ и решении задачи синтеза. // Синтаксис и семантика логических систем: Материалы российской школы-семинара. — Иркутск, Издательство ГОУ

ВПО “Иркутский государственный педагогический университет”, 2006. С. 108–112.

2. Хелемендик Р. В. Алгоритм распознавания формул логики ветвящегося времени и эффективный алгоритм построения выводов общезначимых формул из аксиом. // Математические вопросы кибернетики. Вып. 15: Сборник статей / Под ред. О.Б.Лупанова. — М.: Физматлит, 2006. С. 217–266.

О МНОГОЯРУСНЫХ ФОРМУЛАХ

Д. Ю. Черухин (Москва)

Рассматриваются булевы схемы из функциональных элементов (СФЭ, [1]). Ветвлением вершины называется число рёбер, исходящих из этой вершины; в частности, в ветвлении учитывается число выходов, которым соответствует эта вершина (на которые "подаётся сигнал"из этой вершины). Например, если из вершины выходит 2 ребра, ведущих в другие вершины схемы и, кроме того, вершина соответствует трём выходам схемы, то её ветвление равно 5.

Вершина называется узловой, если либо она является входом схемы, либо её ветвление больше единицы. СФЭ S называется *k-ярусной* формулой, если в любом ориентированном пути в S содержится не более k узловых вершин. Другими словами, если узловые вершины можно разбить на k ярусов так, что внутри каждого яруса вершины попарно несравнимы в смысле естественного порядка в ориентированном графе.

Одноярусные формулы соответствуют обычным формулам, т. е. схемам без ветвления (могут ветвиться только входы). Сложностью k-ярусной формулы является сумма ветвлений узловых вершин. Такая мера сложности естественна для формул; в случае $k = 1$ она совпадает с числом вхождений переменных в формулу. Пусть L_B^k — мера сложности функций (операторов) в классе k-ярусных формул в конечном базисе B, $\mathcal{L}_B^k$ — соответствующая функция Шеннона [1].

Теорема 1. *В любом базисе B при $k \geqslant 2$*

$$\mathcal{L}_B^k(n) \sim \frac{2^n}{n}.$$

Теорема 1 показывает, что начиная с 2-х ярусов функция Шеннона асимптотически совпадает с аналогичной функцией для СФЭ (СФЭ можно

рассматривать как формулу с неограниченным числом ярусов). Заметим, что [1]

$$\mathcal{L}_B^1(n) \sim \frac{2^n}{\log_2 n}.$$

Пусть $F = (f_1, \ldots, f_m)$ — оператор, зависящий от двух наборов переменных: $X = (x_1, \ldots, x_k)$ и $Y = (y_1, \ldots, y_l)$. Разложим f_j в полином Жегалкина [8] по переменным X:

$$f_j = f_j^0 \oplus f_j^1 x_1 \oplus \ldots \oplus f_j^k x_k \oplus f_j',$$

где каждая из функций f_j^i зависит только от Y, f_j' — нелинейная по X часть.

Пусть $M^1, \ldots, M^k$, $M_1, \ldots, M_m$ — множества функций, зависящих от переменных Y и обладающих свойством: каждая функция f_j^i вычислима через функции из множества $M^i \cup M_j$, т. е. представима в виде $h(g_1, \ldots, g_t)$, где $\{g_1, \ldots, g_t\} \subseteq M^i \cup M_j$, $h \in P_2$. Тогда набор $(M^1, \ldots, M^k;\ M_1, \ldots, M_m)$ назовём *F-таблицей*. Через $L'(F)$ обозначим минимум по всем F-таблицам суммы $\sum\limits_i |M^i| + \sum\limits_j |M_j|$.

Теорема 2. *В любом базисе B*

$$L_B^2(F) \geqslant L'(F).$$

Следствие 1. *Пусть F_n — любой из операторов: умножение матриц, умножение многочленов, циклическая свёртка; n — число его входов. Тогда в любом базисе B*

$$L_B^2(F_n) = \Omega(n^{3/2}).$$

Теорема 2 может быть обобщена [5, 6] на класс СФЭ глубины 2 в базисе из всех булевых функций. Известные для этого класса нижние оценки вида $\Omega(n\frac{\ln^2 n}{\ln \ln n})$ следуют из результатов теории графов [10].

Пусть $F = (F_1, \ldots, F_k)$ — булев оператор, разбитый на k операторов и зависящий от набора переменных $X = (X_1, \ldots, X_k)$, разбитого на k наборов. Обозначим через $\mathcal{D}(F_i, X_j)$ множество подоператоров, полученных из F_i при всевозможных подстановках констант вместо всех переменных, не входящих в набор X_j.

Теорема 3. *Для любого базиса B существует константа c_B' такая, что для любого оператора F, существенно завясящего от всех переменных из X*

$$L_B^2(F) \geqslant c_B' \sum_{i=1}^{k} \log_2 |\mathcal{D}(F_i, X_i)|.$$

Теорема 3 является обобщением метода Нечипорука для формул [2]. Она позволяет получать нижние оценки сложности вида $\Omega(\frac{n^2}{\log n})$, например, для оператора, состоящего из одинаковых функций Нечипорука (число функций равно числу переменных).

Обозначим $\Lambda_n = x_1 \oplus \ldots \oplus x_n$. Для любого $k \geqslant 1$ введём функцию

$$\varphi_k(x) = \frac{1}{1-(1-1/x)^k}.$$

Теорема 4. [7] *Пусть B — базис, $\gamma > 1$. Тогда:*

а) если

$$L_B^1(\Lambda_n) = \mathcal{O}(n^\gamma),$$

то для любого k

$$L_B^k(\Lambda_n) = \mathcal{O}(n^{\varphi_k(\gamma)}).$$

б) если базис B обладает экспонентой сжатия (shrinkage exponent) [7, 9] γ, то для любого k

$$L_B^k(\Lambda_n) = \Omega(n^{\varphi_k(\gamma)}).$$

Теорема 4 устанавливает связь между нижними и верхними оценками сложности функции Λ_n в классе формул и соответствующими оценками в классе многоярусных формул. Заметим, что нижние оценки сложности функции Λ_n в классе формул традиционно получаются с помощью метода Субботовской [3,4] и из подобного доказательства обычно извлекается информация о нижней оценке экспоненты сжатия.

Пусть M^* — множество булевых функций, возрастающих или убывающих по каждой переменной. Для мер сложности μ_1, μ_2 обозначим через $\mu_1 \leqslant \mu_2$ отношение частичного порядка $\mu_1 = \mathcal{O}(\mu_2)$ (т. е. $\forall f \in P_2\ \mu_1(f) = \mathcal{O}(\mu_2(f))$).

Теорема 5. [7] *а) Для любого базиса $B \subseteq M^*$ существует последовательность $k_1, k_2, \ldots$ такая, что*

$$L_B^{k_1} > L_B^{k_2} > \ldots$$

б) Для базиса $B_0 = \{\&, \vee, \neg\}$

$$L_{B_0}^1 > L_{B_0}^2 > \ldots$$

в) Для каждого k существует последовательность базисов $B_1, B_2 \ldots$ такая, что

$$L_{B_1}^k > L_{B_2}^k > \ldots$$

Теорема 5 следует из теоремы 4 и известных результатов об экспоненте сжатия для различных базисов [3,9].

Теорема 6. *Для любого базиса B и любых k, l*

$$L_B^k = (L_B^l)^{\mathcal{O}(1)}.$$

Обозначим $\ln^{(s)}(x) = \ln\ln\ldots\ln(x)$, где число логарифмов равно s, $s \geqslant 0$. Скажем, что меры сложности μ_1 и μ_2 s-эквивалентны, если

$$\exists C\ \forall f \in P_2\ |\ln^{(s)}(\mu_1(f)) - \ln^{(s)}(\mu_2(f))| \leqslant C.$$

Скажем, что меры *слабо* эквивалентны, если для некоторого s они s-эквивалентны.

Заметим, что 1-эквивалентность есть совпадение по порядку (это отношение исследуется в теореме 5), 2-эквивалентность есть полиномиальная эквивалентность (как в теореме 6). Можно показать, что меры сложности многоярусных формул и контактно-вентильных схем (а также их ограничений — контактных схем, ветвящихся программ и т. д.) 3-эквивалентны. В то же время, вопрос о слабой эквивалентности этих мер с мерой сложности СФЭ является открытым.

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994), программы "Университеты России"(проект УР.04.02.528) и программы поддержки ведущих научных школ РФ (проект НШ–1807.2003.1).

Список литературы

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

2. Нечипорук Э. И. Об одной булевской функции // ДАН СССР. 1966. Т. 169, N 4. с. 765–766.

3. Перязев Н. А. Сложность представлений булевых функций формулами в немонолинейных базисах. Дискретная математика и информатика. Вып. 2. — Иркутск: Изд-во Иркут. ун-та, 1995.

4. Субботовская Б. А. О реализации линейных функций формулами в базисе $\vee, \&, -$. ДАН СССР. 1961. Т. 136, N. 3. с. 784–787.

5. Черухин Д. Ю. О схемах из функциональных элементов с ограниченной глубиной ветвления // Докл. РАН. Т. 405, N. 4. 2005. с. 467–470.

6. Черухин Д. Ю. Нижняя оценка сложности в классе схем глубины 2 без ограничений на базис // Вестн. МГУ. Сер. 1. N 4. 2005. с. 54–56.

7. Черухин Д. Ю. О схемах из функциональных элементов конечной глубины ветвления // Дискретная математика. Т. 18, вып. 4. 2006. с. 73–83.

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

9. Hastad J. The shrinkage exponent of de Morgan formulas is 2. SIAM J. Comput. 1998. V. 27. p. 48–64.

10. Radhakrishnan J. Ta-Shma A. Bounds for dispersers, extractors, and depth-two superconcentrators // SIAM J. of Discrete Mathematics. 2000. V. 13, No 1. p. 2–24.

О СЛОЖНОСТИ ФУНКЦИЙ С "МАЛЫМ ЧИСЛОМ ЕДИНИЦ" В КЛАССЕ КНФ

С. Е. Черухина (Москва)

В работе [1] для функций $f(x_1, \ldots, x_n)$ из семейства $R_{n,k}$ (обращающихся в единицу на k наборах) было доказано, что в классе формул в базисе $\{\&, \vee, \neg\}$ их сложность не превосходит $2n + k2^{k-1}$. Используя конструкцию автора работы [1], нетрудно показать, что в классе КНФ сложность будет ограничена величиной $2n + 2^{k-2}2^{2^{k-1}}$.

Применяя метод, рассмотренный в [2], верхняя оценка существенно понижается до $2n + ck^2 2^k + k2^{k-1}$. Нижняя оценка для функционала $L(n,k) = \max L(f)$ (по всем функциям из $R_{n,k}$) следует из доказываемой далее теоремы.

Тогда для небольших значений k (точнее, для $k \leqslant \log n + \frac{1}{2}\log\log n$) верно

$$2n + c_1 \frac{2^k}{\sqrt{k}} \leqslant L(n,k) \leqslant 2n + c_2 k^2 2^k.$$

В частности, для $k \leqslant \log n - 2\log\log n - \psi(n), \psi(n) \to \infty, n \to \infty$, верно

$$L(n,k) \sim 2n.$$

Мы будем рассматривать некоторую булеву функцию $f(x_1, \ldots, x_n)$, принимающую значение 1 на $k+2$ наборах. Эти наборы составляют *матрицу* M функции f. Оценим снизу сложность такой функции формулами вида КНФ.

Для удобства доказательства будем рассматривать не саму функцию f, а ее отрицание — $\bar{f}$ и реализацию $\bar{f}$ формулами ДНФ. При этом матрица M содержит наборы, на которых $\bar{f}$ равна нулю.

Определение. *Два столбца матрицы M находятся в общем положении, если в строках подматрицы, ими составляемой, встречаются все четыре возможные комбинации из 0 и 1.*

Лемма 1. *Пусть x_i — переменная функции $\bar{f}(x_1, \ldots, x_n), n \geqslant 2$, а также:*

а) расстояние между любыми двумя строками матрицы M не меньше 2;

б) столбец, соответствующий переменной x_i, находится в общем положении с любым другим столбцом из M.

Тогда в любой ДНФ для $\bar{f}$ как переменная x_i, так и ее отрицание встречаются не менее двух раз.

Доказательство. Заметим, что по крайней мере по одному разу x_i и $\bar{x}_i$ встречаются в любой ДНФ, реализующей $\bar{f}$. Действительно, в силу п. б), функция $\bar{f}$ равна 0 на некотором наборе $\tilde{\alpha}$ с $\alpha_i = 1$. На наборе $\tilde{\beta}$, отличающемся от набора $\tilde{\alpha}$ только i-й координатой ($\beta_i = 0$), в силу п. а), $\bar{f}(\tilde{\beta}) = 1$. Следовательно, функция $\bar{f}$ не возрастает по переменной x_i, а значит, $\bar{x}_i$ содержится в любой ДНФ для $\bar{f}$. Аналогично существуют наборы $\tilde{\alpha}$ с координатой $\alpha_i = 0$ и $\tilde{\beta}$ с координатой $\beta_i = 1$, $\rho(\tilde{\alpha}, \tilde{\beta}) = 1$, на которых $\bar{f}(\tilde{\alpha}) = 0$ и $\bar{f}(\tilde{\beta}) = 1$, из чего следует, что x_i также должно присутствовать в любой ДНФ для $\bar{f}$.

Далее, предположим, что

$$x_i \text{ входит в ДНФ для } \bar{f} \text{ ровно 1 раз.} \tag{1}$$

Пусть K — конъюнкция, содержащая x_i. Рассмотрим два случая:

1) $K = x_i$. Тогда при $x_i = 1$ функция $\bar{f}$ обращается в 1, следовательно, матрица M должна содержать нулевой столбец, соответствующий переменной x_i, что противоречит п. б) условия леммы.

2) $K = x_i x_j^{\sigma} \cdots$ (без ограничения общности, можем считать, что $\sigma = 1$).

Пусть $\tilde{\alpha}$ — любой набор такой, что $\alpha_i = \alpha_j = 0$. Покажем, что $\bar{f}(\tilde{\alpha}) = 1$. Предположим, что $\bar{f}(\tilde{\alpha}) = 0$. Рассмотрим набор $\tilde{\beta}$ такой, что $\rho(\tilde{\alpha}, \tilde{\beta}) = 1$, $\beta_i = 1, \beta_j = 0$. Тогда $\bar{f}(\tilde{\beta}) = 1$, т. к. из п. а) следует, что соседних нулей у $\bar{f}$ нет. Набор $\tilde{\beta}$ должен быть накрыт некоторой конъюнкцией K', причем $K' \neq K$, поскольку $K(\tilde{\beta}) = 0$. Конъюнкция K' должна содержать x_i, т. к. K' не убывает по x_i ($K'(\tilde{\alpha}) = 0, K'(\tilde{\beta}) = 1$). Но по предположению (1) K — единственная конъюнкция, содержащая x_i. Противоречие. Следовательно, $\bar{f}(\tilde{\alpha}) = 1$. Это верно для любого набора $\tilde{\alpha}$, у которого $\alpha_i = \alpha_j = 0$, поэтому в матрице M отсутствуют строки, в i-м и j-м столбцах которых стоят одновременно 0, а это противоречит тому, что i-ый и j-ый столбцы находятся в общем положении (п. б)). Итак, x_i входит в ДНФ, как минимум, два раза. Случай $\bar{x}_i$ аналогичен.

Утверждение 1. *Если в матрице M функции f в столбце, соответствующем переменной x_i, есть 0 и 1 и расстояние между любыми двумя строками не меньше 2, то переменная x_i и ее отрицание входят в любую КНФ функции f по крайней мере по одному разу.*

Доказательство следует из первой части доказательства леммы.

Теорема 1. *Для любых $n, k, k \geqslant 4$, $n \geqslant C_k^{\lfloor k/2 \rfloor}$, найдется функция от n переменных, принимающая значение 1 на $k+2$ наборах, такая, что*

$$L(f) \geqslant 2n + 2C_k^{\lfloor k/2 \rfloor} - 2.$$

Доказательство. Матрица M функции $\bar{f}$ будет устроена следующим образом. Рассмотрим $C_k^{\lfloor k/2 \rfloor}$ столбцов, представляющие из себя всевозможные наборы длины k, содержащие ровно $\lfloor k/2 \rfloor$ единиц; из них составим матрицу A. Последний (например) столбец матрицы A продублируем $n - C_k^{\lfloor k/2 \rfloor}$ раз. Эти одинаковые столбцы образуют матрицу B. Также добавим к матрицам A и B по две строки: "нулевую"и "единичную", вместе с которыми образуются новые матрицы A' и B'. Наконец, $M = (A'|B')$. Тогда любые два столбца из A' находятся в общем положении (т. к. соответствующие векторы из A несравнимы). И любой столбец из A', кроме последнего, находится в общем положении с любым другим столбцом из M. Расстояние между любыми двумя строками из M не меньше двух; это следует из того, что в матрице M, кроме двух последних строк, в качестве столбцов имеются все варианты наборов длины k, содержащие $\lfloor k/2 \rfloor$ единиц. Поэтому для всех столбцов из A', кроме последнего, применима лемма, а для остальных — утверждение. Следовательно,

$$L(f) \geqslant 4(C_k^{\lfloor k/2 \rfloor} - 1) + 2(n - C_k^{\lfloor k/2 \rfloor} + 1) = 2n + 2C_k^{\lfloor k/2 \rfloor} - 2.$$

Замечание. Для больших значений k, а именно, для k таких, что $n \leqslant C_k^{\lfloor k/2 \rfloor}$ и $k \leqslant 2^{n-1}$ можно доказать, что $L(n,k) \geqslant 4n$.

Список литературы

1. Фиников Б. И. Об одном семействе классов функций алгебры логики и их реализации в классе П-схем. ДАН СССР 115, 2, 1957, с. 247–248.

2. Черухина С. Е. О сложности функций с малым числом единиц. Труды 6 Международной конференции "Дискретные модели в теории управляющих систем" (Москва, 7-11.12.2004). Изд. отд. ф-та ВМиК МГУ, 2004, с. 95.

ОБ ЭФФЕКТИВНОЙ РЕАЛИЗАЦИИ ФУНКЦИЙ, ПОСТРОЕННЫХ ПО РЕКУРСИВНОЙ КОНСТРУКЦИИ СПЕЦИАЛЬНОГО ВИДА

С. Г. Шипунов (Москва)

Введение

Ю.В. Таранниковым была разработана рекурсивная конструкция, позволяющая строить m-устойчивые функции с нелинейностью близкой к максимально возможной для данного класса функций. Однако, основной проблемой ограничивающей возможность применения данной конструкции при создании потоковых шифраторов является нетривиальная в общем случае реализация функции, порожденных этой конструкцией. В данной работе будет представлен алгоритм, позволяющий эффективно реализовывать эти функции.

Данная статья состоит из двух частей. В первой части приводятся базовые определения и алгоритм построения рассматриваемой конструкции. Во второй части приводится разработанный нами алгоритм эффективной реализации в общем случае.

1. Базовые определения

Рассмотрим векторное пространство F_n^2 наборов длины n с компонентами из F_2 — конечного поля из двух элементов 0 и 1, операции сложения и умножения в котором вводятся как обычные операции сложения и умножения по модулю 2.

Будем говорить, что булева функция

$$f = f(x_1, x_2, ..., x_n)$$

зависит от пары переменных (x_i, x_j) квазилинейно, если $f(X') \neq f(X'')$ для любых двух наборов X' и X'', различающихся только в i-й и j-й компонентах. Пара (x_i, x_j) в этом случае называется парой квазилинейных переменных. В [1] показывается, что пара (x_i, x_j) является парой квазилинейных переменных в булевой функции

$$f = f(x_1, x_2, ..., x_n)$$

в том и только в том случае, когда f может быть представлена в виде

$$f = g(x_1, ..., x_{j-1}, x_{j+1}, ..., x_{i-1}, x_{i+1}, ..., x_n, x_i \oplus x_j) \oplus x_j \ .$$

Конструкция 1. *Пусть* $f_0, ..., f_{2^k-1}$ *булевы функции на* F_n^2. *Пусть* $\sigma_1, ..., \sigma_k$ — *двоичное представление* r.*Пусть* $C = (c_1, ..., c_k)$ *произвольный двоичный набор. Обозначим* $s = \sum_{i=1}^{i=k} c_i$. *Введем множества*

$$X = \{x_i | i = 1, ..., n\}, \quad Y = \{y_i | i = 1, ..., k\}, \quad Z = \{z_i | i = 1, ..., k\}.$$

Определим

$$F(X, Y, Z) = \bigoplus_{j=1}^{j=2^k-1} f_{\sigma_1,...,\sigma_k}(X)(y_1 \oplus c_1 z_1 \oplus \sigma_1) \ldots$$

$$\ldots (y_k \oplus c_k z_k) \oplus c_1 z_1 \oplus \ldots \oplus c_k z_k.$$

Определение. *Матрица* $B_{k_0,k,p,t} = b_{ij}$ *размера* $2^k \times p$, *состоящая из* $(*, 1, 2)$, *называется подходящей, если*:

1) *Для любых двух строк* i_1, i_2 *существует такой столбец* j, *что* $b_{i_1,j} = 1$, $b_{i_2,j} = 2$ *или* $b_{i_1,j} = 2$, $b_{i_2,j} = 1$;

2) *сумма всех элементов в любой строке не превосходит* t, $*$ *считается как* 0;

3) *число единиц в любой строке не превосходит* k_0.

Обозначим $S_{n,m,k}$ множество булевых функций, такое что для каждого $s, 0 \leq s \leq k$, множество $S_{n,m,k}$ содержит $(m + s)$ -устойчивую функцию на F_2^{n+s} , которая имеет s непересекающихся пар квазилинейных переменных.

Были введены все необходимые определения, теперь приведем теорему Ю. В. Таранникова, позволяющую строить m-устойчивые функции, для сколько угодно больших m.

Теорема 1. *При* $2p - t \leq n$, *по системе функций* S_{n,m,k_0} *и подходящей матрице* $B_{k_0,k,p,t}$ *можно построить систему функций* $S_{n+k+t,m+t,k_0}$.

Приведем только конструктивную часть доказательства. Ее можно разбить на три части.

1) Рассмотрим каждую строку матрицы $B_{k_0,k,p,t}$. Пусть рассматриваем i-ю строку и пусть в ней s единиц. Из системы функций S_{n,m,k_0} возьмем $(m + s)$-устойчивую функцию с s парами неперсекающихся квазилинейных переменных. Добавим к ней $t - s$ линейных переменных. И обозначим результат f_i'.

2) Переименуем переменные в f_i' таким образом, чтобы стоящей в матрице $B_{k_0,k,p,t}$ в i-й строке на j месте единице соответствовала пара квазилинейных переменных (x_{2j-1}, x_{2j}), а двойке соответствовала пара линейных переменных (x_{2j-1}, x_{2j}). Получим функцию f_i''.

3) К полученным функциям применим конструкцию 1 для всех $C, 0 \leq wt(C) \leq k$, и получим искомую систему функций $S_{n+k+t,m+t,k_0}$.

Важно учитывать, что приведенная конструкция рекурсивная, то есть по системе S_{n,m,k_0} после неоднократного последовательного применения теоремы с различными подходящими матрицами $B_{k_0^i,k^i,p^i,t^i}$, можно получить функции со сколько угодно высокой устойчивостью, а при правильном подборе параметров k_0, k, p, t, и со сколько угодно близкой к максимально возможной нелинейностью. Но перестановка на втором шаге чрезвычайно усложняет реализацию функций из системы, полученных с помощью последовательного применения данной теоремы для произвольной фиксированной последовательности подходящих матриц $B_{k_0^i,k^i,p^i,t^i}, 0 \le i \le n$. Далее будет предложен метод, позволяющий обойти эту проблему.

2. Об эффективной реализации конструкции

Пусть есть произвольная последовательность

$$B_{k_0^i,k^i,p^i,t^i}, 0 \le i \le N,$$

с условием $k_0^n \le k^{n-1}$, и произвольная система S_{n,m,k_0^0}. Построим с помощью последовательного применения теоремы 1 систему

$$S_{n+\sum_{i=1}^{i=N} k^i + \sum_{i=1}^{i=N} t^i, m+\sum_{i=1}^{i=N} t^i, k^N}.$$

Зафиксируем произвольным образом $s^N, 0 \le s^N \le k^N$. Рассмотрим применение третьего шага из теоремы 1 для последней матрицы $B_{k_0^N,k^N,p^N,t^N}$ и системы

$$S_{n+\sum_{i=1}^{i=N-1} k^i + \sum_{i=1}^{i=N-1} t^i, m+\sum_{i=1}^{i=N-1} t^i, k^n}.$$

В нем

$$f_s^N(X,Y,Z) = \bigoplus_{\sigma_1,\dots,\sigma_{k^N}} f''_{\sigma_1,\dots,\sigma_{k_N}}(X)(y_1^N \oplus z_1^N \oplus \sigma_1)\dots$$

$$\dots(y_s^N \oplus z_s^N \oplus \sigma_s)(y_{s+1}^N \oplus \sigma_{s+1})\dots(y_{k^N}^N \oplus \sigma_{k^N}^N) \oplus \bigoplus_{i=1}^{i=s} z_i^N.$$

Заметим, что на произвольно заданном наборе переменных Y, Z только один из множителей

$$(y_1^N \oplus z_1^N \oplus \sigma_1)\dots(y_s^N \oplus z_s^N \oplus \sigma_s)(y_{s+1}^N \oplus \sigma_{s+1})\dots(y_{k^N}^N \oplus \sigma_{k^N}^N)$$

не равен нулю, а значит можно определить индекс $\sigma_1, \dots, \sigma_{k^N}$

функции $f''_{\sigma_1,\ldots,\sigma_{k_N}}$, а именно

$$\begin{aligned}
\sigma_1 &= y_1^N \oplus z_1^N \oplus 1\\
&\ldots\ldots\ldots\ldots\\
\sigma_s &= y_s^N \oplus z_s^N \oplus 1,\\
\sigma_{s+1} &= y_{s+1}^N \oplus 1,\\
&\ldots\ldots\ldots\ldots\\
\sigma_{k^N} &= y_{k^N}^N \oplus 1.
\end{aligned}$$

А значит и номер строки матрицы $B_{k_0^N,k^N,p^N,t^N}$, согласно которой происходила перестановка во втором шаге. Так же можно вычислить линейную прибавку

$$L^N = \bigoplus_{i=1}^{i=s} z_i^N.$$

Перейдем теперь ко второму шагу. Пусть в данной строке матрицы $B_{k_0^N,k^N,p^N,t^N}$ s единиц, тогда в ней $\frac{t^N-s}{2}$ двоек и $p-\frac{t^N+s}{2}$ символов *. Зафиксируем переименование переменных следующим образом:
1) Пусть на j месте в интересующей нас i строке стоит 2 и до нее в этой строке было r_2 двоек. В первом шаге теоремы 1 было добавлено t^N-s линейных переменных, а именно $(u_1^N,\ldots,u_{t^N-s}^N)$. Переименуем

$$(u_{2r_2-1}^N, u_{2r_2}^N) \text{ в } (x_{2j-1}^N, x_{2j}^N).$$

2)Пусть на j месте в интересующей нас i строке стоит 1 и до нее в этой строке было r_1 единиц. В третьем шаге теоремы 1 для матрицы

$$B_{k_0^{N-1},k^{N-1},p^{N-1},t^{N-1}}$$

и системы

$$S_{n+\sum_{i=1}^{i=N-2}k^i+\sum_{i=1}^{i=N-2}t^i,m+\sum_{i=1}^{i=N-2}t^i,k^{N-2}}$$

было добавлено s переменных z и k^{N-1} переменных y, а именно

$$(z_1^{N-1},\ldots,z_s^{N-1}) \text{ и } (y_1^{N-1},\ldots,u_{y^{N-1}}^{N-1})$$

Из них $(z_i^{N-1}, y_i^{N-1}), 0 \le i \le s$, образуют пары квазилинейных переменных. Переименуем

$$(y_{r_1}^{N-1}, z_{r_1}^{N-1}) \text{ в } (x_{2j-1}^N, x_{2j}^N).$$

3)Переименование оставшихся переменных должно быть сделано произвольным фиксированным образом. В частности переменные $(y_{s+1}^{N-1}, ..., y_{k^{N-1}}^{N-1})$, не входящие в упомянутые ранее пары квазилинейных переменных переименовываются в какие-то $(X_{i_1}^N, ..., x_{s_{k^{N-1}-s}}^N)$.

Переименование переменных есть всего лишь подстановка вместо

$$U = (u_1^N, \ldots, u_{t^N-s}^N),$$
$$Z = (z_1^{N-1}, \ldots, z_s^{N-1}),$$
$$Y = (y_1^{N-1}, \ldots, y_{k^{N-1}}^{N-1})$$

определенных переменных из X. Вариант такой подстановки был описан ранее, поэтому по номеру строки можно определить параметр s(число пар квазилинейных переменных) и подстановку переменных вместо наборов U, Y, Z. А зная это можно перейти к третьему шагу теоремы 1 для системы

$$S_{n+\sum_{i=1}^{i=N-2} k^i + \sum_{i=1}^{i=N-2} t^i, m+\sum_{i=1}^{i=N-2} t^i, k^N}$$

и матрицы

$$B_{k_0^{N-1}, k^{N-1}, p^{N-1}, t^{N-1}}.$$

Рассмотрим первый шаг теоремы. На этом шаге нам известны значения переменных

$$U = (u_1^N, \ldots, u_{t^N-s}^N)$$

из второго шага. Остается лишь прибавить их к L^N.

Таким образом, мы перешли от вычисления функции из

$$S_{n+\sum_{i=1}^{i=N} k^i + \sum_{i=1}^{i=N} t^i, m+\sum_{i=1}^{i=N} t^i, k^N}$$

к вычислению функции из

$$S_{n+\sum_{i=1}^{i=N-1} k^i + \sum_{i=1}^{i=N-1} t^i, m+\sum_{i=1}^{i=N-1} t^i, k^{N-1}}.$$

Данный процесс можно продолжить вплоть до S_{n,m,k_0^0}. В итоге мы получили алгоритм, позволяющий эффективно вычислять функции, построенные по произвольно заданной последовательности подходящих матриц $B_{k_0^i, k^i, p^i, t^i}, 0 \leq i \leq N$, при этом на каждом шаге алгоритма вычисляется всего одна функция из 2^{k^i} возможных. И даже у этой одной функции вычисляется лишь линейная часть, а вместо нелинейной части считается номер предыдущей функции. В совокупности это обеспечивает линейную программную скорость.

Список литературы

1. Тарасников Ю. В. О корреляционно-имунных и устойчивых булевых функциях// Математические вопросы кибернетики. Вып 11.— М.: Физматлит, 2002. — С. 91–148.

ОБЩИЙ ПОДХОД К ПРОБЛЕМЕ ЭКВИВАЛЕНТНОСТИ ПРОГРАММ НА ШКАЛАХ, СВЯЗАННЫХ С ОБРАБОТКОЙ ПРЕРЫВАНИЙ

В. Л. Щербина (Москва)

Эквивалентность программ на шкалах — понятие существенно более сильное, чем функциональная эквивалентность (по сути, это эквивалентность на целом классе семантик). С одной стороны, это делает возможным строить эффективные алгоритмы, с другой — выражать характерные особенности модели вычислений. Метод критериальных систем, позволяющий устанавливать эквивалентность для некоторых шкал, требует явного построения полугруппы -критериальной системы. Универсальный способ построения критериальной системы для составной шкалы, включающей действия основной программы и действия по обработке прерываний, не известен. В данной работе предлагается подход, базирующийся на методе критериальных систем, позволяющий решать проблему эквивалентности для широкого класса шкал за полиномиальное время. Идея его состоит в том, чтобы рассматривать серии объединённых определённым образом операторов как единичные команды.

Рассмотрим конечное множество $\tilde{A}$, которое назовем алфавитом *действий*. *Операторной цепочкой* называется слово в алфавите $\tilde{A}$. Для пустой операторной цепочки будет использоваться обозначение λ.

Рассмотрим также непустое конечное множество $\mathcal{C}$, элементами которого обозначаются всевозможные комбинации значений логических условий, различаемых в описываемой модели программ.

Пропозициональная операторная программа сигнатуры $(\tilde{A}, \mathcal{C})$ задается системой переходов $\langle V, \textbf{вход}, \textbf{выход}, \textbf{тупик}, B, T\rangle$, где V — конечное множество вершин-преобразователей, **вход** — *начальная вершина*, **выход** — *заключительная вершина*, **тупик** — *вершина пустого цикла*, $B\colon V \to \tilde{A}$ — *функция привязки*, сопоставляющая каждому преобразователю программы некоторый оператор, $T\colon (V \cup \{\textbf{вход}\}) \times \mathcal{C} \to (V \cup \{\textbf{выход}, \textbf{тупик}\})$. *Размером* $|\pi|$ программы π назовем число вершин-преобразователей в ней.

Детерминированной динамической шкалой (или просто *шкалой*) сигнатуры $\tilde{A}$ назовем тройку $\mathcal{F} = \langle S, s_0, R\rangle$, состоящую из непустого множества *состояний* S, *начального состояния* $s_0, s_0 \in S$, и *функции преобразования* $R\colon S \times \tilde{A} \to S$.

Назовем шкалу *упорядоченной*, если отношение достижимости состояний является частичным порядком на S.

Для каждой операторной цепочки обозначим через $[h]$ состояние $s = R^*(s_0, h)$, где R^* — естественное расширение функции R на множество конечных последовательностей операторов. Мы ограничимся рассмотрением

только таких шкал, в которых каждое состояние достижимо из начального. Если для любой четверки операторных цепочек h_1, h_2, h_3, h_4 равенства $[h_1] = [h_3]$, $[h_2] = [h_4]$ влекут $[h_1 h_2] = [h_3 h_4]$, то шкала называется *полугрупповой*. Можно рассматривать ее как полугруппу $(S, *)$, в которой операция определяется соотношением $[h_1] * [h_2] = [h_1 h_2]$.

Детерминированной динамической моделью (или просто *моделью*) M сигнатуры $(\tilde{\mathcal{A}}, \mathcal{C})$ назовем пару $\langle \mathcal{F}, \xi \rangle$, в которой $\mathcal{F} = \langle S, s_0, R \rangle$ — шкала сигнатуры $\tilde{\mathcal{A}}$, а $\xi\colon S \to \mathcal{C}$ — *означивание* логических условий.

Пусть $\pi = \langle V, \textbf{вход}, \textbf{выход}, \textbf{тупик}, B, T \rangle$ — некотороя пропозициональная операторная программа, и $M = \langle \mathcal{F}, \xi \rangle$ — модель, базирующаяся на шкале $\mathcal{F} = \langle S, s_0, R \rangle$. Тогда последовательность четверок (конечная или бесконечная)

$$r = (v_0, a_0, s_0, \delta_0), (v_1, a_1, s_1, \delta_1), \ldots, (v_m, a_m, s_m, \delta_m), \ldots$$

называется *вычислением* программы π на модели M, если она удовлетворяет следующим требованиям:

1) $v_0 = \textbf{вход}, a_0 = \lambda, s_0$ — начальное состояние, $\delta_0 = \xi(s_0)$;

2) каждая четверка $(v_i, a_i, s_i, \delta_i), i \geqslant 1$, состоит извершины преобразователя v_i(состояния программы), оператора a_i, состояния данных s_i и логического условия δ_i;

3) для каждого i, $i \geqslant 1$, выполняются соотношения $v_i = T(v_{i-1}, \delta_{i-1})$, $a_i = B(v_i)$, $s_i = R(s_{i-1}, a_i)$, $\delta_i = \xi(s_i)$;

4) эта последовательность оканчивается четверкой $(v_m, a_m, s_m, \delta_m)$ тогда и только тогда, когда $v_m \in \{\textbf{выход}, \textbf{тупик}\}$.

Таким образом определенное вычисление будем обозначать $r(\pi, M)$. Если $r(\pi, M)$ оканчивается четверкой $(\textbf{выход}, a_m, s_m, \delta_m)$, то будем называть это вычисление *терминальным*, а состояние s_m — его *результатом*, который будем обозначать $[r(\pi, M)]$. В остальных случаях вычисление считается безрезультатным, и значение $[r(\pi, M)]$ полагается неопределенным.

Программы π' и π'' назовем *эквивалентными на шкале* $\mathcal{F}$ (и обозначим этот факт $\pi'' \sim_{\mathcal{F}} \pi''$), если для всякой модели $M = \langle \mathcal{F}, \xi \rangle$ выполняется $[r(\pi', M)] = [r(\pi'', M)]$.

Пусть фиксированы 2 шкалы: $\mathcal{F}_{\mathcal{A}} = \langle S_{\mathcal{A}}, s_{\mathcal{A}0}, R_{\mathcal{A}} \rangle$ сигнатуры $\mathcal{A}$ и $\mathcal{F}_{\mathcal{B}} = \langle S_{\mathcal{B}}, s_{\mathcal{B}0}, R_{\mathcal{B}} \rangle$ сигнатуры $\mathcal{B}$, $\mathcal{A} \cap \mathcal{B} = \emptyset$. Шкалу $intr(\mathcal{F}_{\mathcal{A}}, \mathcal{F}_{\mathcal{B}}) = \langle S, s_0, R \rangle$ сигнатуры $\tilde{\mathcal{A}} = \mathcal{A} \cup \mathcal{B}$, где $S = S_{\mathcal{A}} \times S_{\mathcal{B}}$, $s_0 = (s_{\mathcal{A}0}, s_{\mathcal{B}0})$,

$$R((s_{\mathcal{A}}, s_{\mathcal{B}}), a) = \begin{cases} (s_{\mathcal{A}}, R_{\mathcal{B}}(s_{\mathcal{B}}, a)), & a \in \mathcal{B}, \\ (R(s_{\mathcal{A}}, a), s_{\mathcal{B}0}), & a \in \mathcal{A}, \end{cases}$$

назовём *шкалой* основных действий $\mathcal{F}_{\mathcal{A}}$ *с прерываниями* $\mathcal{F}_{\mathcal{B}}$.

Выбор такого определения обусловлен изучаемым свойством обработчиков прерываний — незаметностью их действий для прикладной программы. Рассмотрим выполнение программы, работающей в вычислительной среде, в которой возможно возникновение прерываний (как засчет генерации их самой программой, так и вследствие внешних причин). На время обработки прерывания выполнение основной программы приостанавливается. Как правило, в процессе этой обработки выполняются служебные действия (перераспределение памяти, управление устройствами), не вляющие существенно на основное вычисление. Это случай успешной обработки прерывания. Но возможна ситуация, когда после завершения обработки прерывания управление не возвращается в основную программу (например, при возникновении аварийной ситуации, последствия которой невозможно исправить, нехватке ресурсов, и т.д.). Тогда результат вычисления определяется действиями, выполненными основной программой и действиями последнего цикла обработки прерываний.

В ряде случаев полиномиальный алгоритм для проблемы эквивалентности на упорядоченных шкалах можно получить методом критериальных систем с теми или иными модификациями. Основная идея состоит в том, чтобы отслеживать всевозможные совместные (на одной модели) вычисления пары программ, представляя различие в их состояниях данных в процессе выполнения как элемент особой структуры. Для учёта повторяющихся фрагментов вычисления в процессе работы алгоритма строится граф, каждая вершина которого вершины которого помечена вершинами-преобразователями программ и элементом критериальной системы. Пути в таком графе отвечают совместным вычислениям. О неэквивалентности программ свидетельствует достижимость из начальной вершины вершины, в которой обе программы завершили вычисление с различными состояниями данных. При выполнении определённых требований можно избежать рассмотрения бесконечного множества состояний во всевозможных моделях.

Пусть $\mathcal{F} = \langle S, s_0, R\rangle$ — упорядоченная полугрупповая шкала, и $\prec$ — некоторое отношение строгого частичного порядка на S, отношение достижимости. Рассмотрим некоторую полугруппу W с бинарной операцией $\circ$ и единицей e, в которой выделена подполугруппа U и пара элементов w^+, w^*. Пятерку $K = \langle W, U, w^+, w^*, \varphi\rangle$, где φ — гомоморфизм полугруппы $\mathcal{F} \times \mathcal{F}$ в полугруппу U назовем k_0 *-критериальной системой* для шкалы $\mathcal{F}$, если K и $\mathcal{F}$ удовлетворяют следующим требованиям:

1) для всякой пары состояний s', s'' из S выполняется

$$s' = s'' \Leftrightarrow w^+ \circ \varphi(\langle s', s''\rangle) \circ w^* = e;$$

2) для любых состояний $s_1, s_2, s_3, s_4 \in S$ таких, что $w^+ \circ \varphi(\langle s_1, s_2\rangle) = w^+ \circ \varphi(\langle s_3, s_4\rangle)$, выполняется

$$s_1 \prec s_2 \Leftrightarrow s_3 \prec s_4, \qquad s_1 \succ s_2 \Leftrightarrow s_3 \succ s_4,$$

3) для любого элемента $u'' \in U \circ w^*$ существует не более k_0 различных элементов $u' \in w^+ \circ U$ таких, что $u' \circ u'' = e$

Обоснование и примеры применения метода критериальных систем такого типа можно найти в [1]. Модификации метода описаны в [2, 3].

Идея общего алгоритма проверки эквивалентности на шкалах с прерываниями базируется на том, что в большинстве случаев действия по обработке прерываний не играют никакой роли, т.к. поглощаются основными действиями. Это позволяет разбить задачу на две слабо связанные между собой части. Проблема эквивалентности решается для программ, получающихся из исходных выкидыванием действий по обработке прерываний (с учётом возможности наличия серии непоглощённых операторов обработки прерываний в конце). Для корректного построения переходов в таких программах необходимо решать проблему достижимости или совместной достижимости для фрагментов исходных программ, содержащих только действия по обработке прерываний.

Будем говорить, что у программы $\pi = \langle V, \textbf{вход}, \textbf{выход}, \textbf{тупик}, B, T\rangle$ сигнатуры $(\tilde{\mathcal{A}}, \mathcal{C})$ *заданы финалы* функцией f, если каждому ребру отвечающей этой программе системы переходов, ведущему в вершину **выход**, поставлен в соответствие элемент некоторого множества (*множества финалов*) — т.е. функция f определена на множестве $\{(v, \delta) \mid v \in \{\textbf{вход}\} \cup V, \delta \in \mathcal{C}, T(v, \delta) = \textbf{выход}\}$.

Финалом результативного *вычисления* программы π на модели M назовём элемент множества финалов, отвечающий последнему шагу данного вычисления (обозначим $fin(\pi, v, M)$).

Задача поиска финалов формулируется следующим образом. Пусть дана программа $\pi = \langle V, \textbf{вход}, \textbf{выход}, \textbf{тупик}, B, T\rangle$ сигнатуры $(\tilde{\mathcal{A}}, \mathcal{C})$, у которой заданы финалы и выбрана некоторая вершина $v_0 \in \{\textbf{вход}\} \cup V$. Требуется построить множество $finals(\pi, v_0) = \bigcup_\xi \{fin(\pi, v_0, \langle \mathcal{F}, \xi\rangle)\}$, где ξ пробегает по всем функциям означивания. По определению положим $finals(\pi, \textbf{тупик}) = \{\textbf{тупик}\}$.

Задача поиска совместных финалов формулируется так. Пусть даны 2 программы $\pi_i = \langle V_i, \textbf{вход}, \textbf{выход}, \textbf{тупик}, B_i, T_i\rangle, i = 1, 2$ сигнатуры $(\tilde{\mathcal{A}}, \mathcal{C})$, у которых заданы финалы (причем множества финалов могут содержать элемент **выход** — ему придается особый статус) и выбраны некоторые вершины $v_{i0} \in \{\textbf{вход}\} \cup V_i$. Требуется построить множество $\bigcup_\xi \{t(\xi)\}$, где ξ

пробегает по всем функциям означивания, а

$$t(\xi) = \begin{cases} (\textbf{выход}, \textbf{выход}, 1), & fin(\pi_1, v_{10}, \langle \mathcal{F}, \xi \rangle) = fin(\pi_2, v_{20}, \langle \mathcal{F}, \xi \rangle) = \textbf{выход}, \\ & [r(\pi_1, v_{10}, \langle \mathcal{F}, \xi \rangle)] = [r(\pi_2, v_{20}, \langle \mathcal{F}, \xi \rangle)], \\ (\textbf{выход}, \textbf{выход}, 0), & fin(\pi_1, v_{10}, \langle \mathcal{F}, \xi \rangle) = fin(\pi_2, v_{20}, \langle \mathcal{F}, \xi \rangle) = \textbf{выход}, \\ & [r(\pi_1, v_{10}, \langle \mathcal{F}, \xi \rangle)] \neq [r(\pi_2, v_{20}, \langle \mathcal{F}, \xi \rangle)], \\ (fin(\pi_1, v_{10}, \langle \mathcal{F}, \xi \rangle), & \\ \ fin(\pi_2, v_{20}, \langle \mathcal{F}, \xi \rangle)), & \text{иначе.} \end{cases}$$

Теорема 1. *Задачи поиска финалов и поиска совместных финалов разрешимы на упорядоченной полугрупповой шкале, для которой имеется k_0 — критериальная система.*

Теорема 2. *Пусть фиксированы 2 шкалы: $\mathcal{F}_{\mathcal{B}}$ сигнатуры $\mathcal{B}$ и полугрупповая упорядоченная шкала $\mathcal{F}_{\mathcal{A}}$ сигнатуры $\mathcal{A}$. Пусть существует алгоритмы, решающие задачи поиска финалов и поиска совместных финалов для шкалы $\mathcal{F}_{\mathcal{B}}$ с временной сложностью $O(f(n))$, где n — размер входных программ. Тогда проблема эквивалентности на шкале $intr(\mathcal{F}_{\mathcal{A}}, \mathcal{F}_{\mathcal{B}})$ разрешима за время $O(n^2 f(n))$.*

Это позволяет эффективно проверять эквивалентность программ на составных шкалах, для которых не построено критериальных систем, если критериальные системы имеются для компонент таких шкал. Например, для шкалы на базе полугруппы, порожденной тождествами поглощения $[ba] = [a]$, $a \in \mathcal{A}$, $b \in \mathcal{B}$ и тождествами перестановочности $[a_1 a_2] = [a_2 a_1], (a_1, a_2) \in Comm$, где $Comm \subseteq (\mathcal{A} \times \mathcal{A}) \cup (\mathcal{B} \times \mathcal{B})$, предложенный алгоритм имеет сложность $O(n^4)$, где n — размер входных программ.

Список литературы

1. Захаров В.А. Быстрые алгоритмы разрешения эквивалентности пропозициональных операторных программ на упорядоченных полугрупповых шкалах. // Вестник Московского университета, сер. 15, Вычислительная математика и кибернетика, N 3, 1999, часть 1, с. 29–35.

2. Захаров В.А. Быстрые алгоритмы разрешения эквивалентности операторных программ на уравновешенных шкалах. // Математические вопросы кибернетики, Физматлит, 1998, вып. 7, с. 303–324.

3. Zakharov V., Zakharyaschev I. On the equivalence-checking problem for a model of programs related with multi-tape automata. // Lecture Notes in Computer Science, v. 3317, 2005, p.293–305.

НЕСУЩЕСТВОВАНИЕ ДВОИЧНЫХ КОДОВ, РАВНОМЕРНО РАСПРЕДЕЛЕННЫХ ПО ШАРАМ ПОЧТИ ВСЕХ МОЩНОСТЕЙ

М. С. Ярыкина (Москва)

Двоичные коды, равномерно распределенные по подкубам, изучались в нескольких областях математики и в приложениях, например, двоичные коды с наибольшим дуальным расстоянием, корреляционно-иммунные и устойчивые функции, ортогональные массивы. Такие коды используются для генерации псевдослучайных последовательностей, в криптографии и т. д. Равномерное распределение двоичных наборов по шарам не изучалось ранее работы [1], хотя представляется, что коды, двоичные наборы которых равномерно распределены по сферам, могут иметь некоторые полезные приложения. Например, такие коды можно использовать в качестве хеширующей функции, а также когда мы хотим, чтобы все слова на выходе связи имели примерно одинаковую вероятность декодирования.

Кодом C (множеством двоичных наборов) назовем произвольное подмножество булевого куба размерности n. *Мощностью* $|C|$ называется число двоичных наборов в нем. *Расстоянием* $d(x, y)$ между двумя наборами x и y называется число компонент, в которых эти наборы различаются. *Шаром* $S_r(x)$ с центром $x \in V^n$ радиуса r называется множество $S_r(x) = \{y \in V^n \,|\, d(x, y) \leqslant r\}$. *Весом* $wt(S_r(x), C)$ шара $S_r(x)$ для кода C называется мощность множества $S_r(x) \cap C$.

Определение. *Пусть l — натуральное. Код $C \subseteq V^n$ называется* равномерно распределенным *по шарам со степенью l (или l-РРШ кодом), если для любых $x, y \in V^n, 0 \leqslant r \leqslant n$, выполняется*

$$|wt((S_r(x), C) - wt((S_r(y), C)| \leqslant l.$$

Полное описание 1-РРШ кодов было дано в [1], в т. ч. было получено количество 1-РРШ кодов для любого n.

Утверждение 1. [1] *Пусть $C \subseteq V^n$, $|C| \leqslant 2^{n-1}$. Если C — 1-РРШ код, то выполняется один из случаев:*

$$1)\ |C| \leqslant 2; \qquad 2)\ n \leqslant 4; \qquad 3)\ n = 6, \quad |C| = 4.$$

Теорема 1. (*Коды малой мощности*) *Пусть $l \in \mathbb{N}$ и $m = m(n) \geqslant 2l + 1$. Тогда, для достаточно больших n не существует l-*РРШ *кодов мощности m при* $\frac{m}{\sqrt{n}e^{\frac{n}{4^{l+1}}}} \underset{n\to\infty}{\longrightarrow} 0$.

Доказательство полностью приведено в [2]. Идея доказательства состоит в том, что в условиях теоремы доказывается существование шаров радиуса R веса 0 и веса не менее $l+1$, где $R = \lambda(n)n$ и $\lambda(n) \to 1/2-0$.

Теорема 2. (*Коды средней мощности*) *Пусть l — фиксированное натуральное число. Тогда существует некоторое $k_0(l)$ такое, что при достаточно больших n не существует кодов, равномерно распределенных по шарам со степенью l, мощности m, удовлетворяющего неравенствам:*

$$8nl < m < \frac{2^n}{\sum\limits_{i=0}^{k_0(l)} \binom{n}{i}}.$$

Замечание. В случае $l = 2$ имеем $k_0 = 52$.

Для доказательства теоремы нам понадобятся следующие леммы.

Лемма 1. *Пусть все шары радиуса k имеют вес не более, чем l. Тогда существует шар радиуса $\left\lfloor \frac{2^l}{2^l-1} k \right\rfloor$ имеющий вес не более, чем l.*

Лемма 2. *Пусть l — фиксированное натуральное число. Тогда найдется такое k_0, что при $k > k_0$, $n \geqslant 2\frac{2^l}{2^l-1}k + 2^l + 2$ выполнено неравенство*

$$\sum_{i=0}^{\lfloor \frac{2^l}{2^l-1} k \rfloor} \binom{n}{i} > 2l \sum_{i=0}^{k+1} \binom{n}{i}.$$

Замечание. В случае $l = 2$ имеем $k_0 = 52$.

Лемма 3. *Булев куб размерности n можно покрыть (не более, чем) $4n$ шарами радиуса $R = \frac{n}{2} - 2^l - 1$ для достаточно больших n.*

Доказательство теоремы 2. Предположим, что l-РРШ код (в булевом кубе размерности n) веса m существует. Из условия следует, что существует шар радиуса $k = k_0$ веса 0. Докажем по индукции, что существует шар радиуса $k+1$ веса 0. База индукции: $k = k_0$.

Шаг индукции. Если существует шар радиуса k веса 0, то по лемме 1, существует шар радиуса $R \geqslant \left\lfloor \frac{2^l}{2^l-1} k \right\rfloor$ веса не более, чем l, поэтому любой шар радиуса R имеет вес не больше, чем $2l$.

Если $n < 2 \cdot \frac{2^l}{2^l-1}k + 2^l + 2$, то по лемме 3 весь булев куб покрываем $4n$ шарами радиуса R. Значит, вес кода не превосходит $2l + l2(4n-1)$, что противоречит условию теоремы. Если $n \geqslant 2 \cdot \frac{2^l}{2^l-1}k + 2^l + 2$, то по лемме 2

средний вес шара радиуса $k+1$ меньше, чем $\frac{1}{2l}$ среднего веса $R_C^{\frac{2^l}{2^l-1}k}$ шара радиуса не менее $\frac{2^l}{2^l-1}k$. Значит, существует шар радиуса $k+1$ веса 0.

Поскольку k растет, а n фиксированно, когда-нибудь выполнится условие $n < 2 \cdot \frac{2^l}{2^l-1}k + 2^l + 2$, то есть на каком-то шаге индукции мы придем к противоречию. Теорема доказана.

Коды большой мощности. В случае кодов большой мощности мы выделим два семейства мощностей. Для каждого семейства мощностей у нас будет свой способ доказательства.

Теорема 3. (*Первое семейство*) *Пусть* $l \in \mathbb{N}$, $s \in \mathbb{N}$, $u > 1$, c_s — *некоторая константа* (*своя для каждого* s) *и* m *такое что*

$$\frac{ul^2}{4}\frac{2^n}{\sum\limits_{i=0}^{s}\binom{n}{i}} \leqslant m \leqslant \left(\frac{n}{s^2}+c_s\right)\frac{2^n}{\sum\limits_{i=0}^{s}\binom{n}{i}}, \qquad \text{для } s \geqslant 2,$$

$$\frac{ul^2}{4}\cdot\frac{2^n}{n+1} \leqslant m \leqslant 2^{n-1}, \qquad \text{для } s = 1.$$

Тогда для достаточно больших n *не существует* l-РРШ *кодов мощности* m. *Кроме того, в случае* $s = 1$ *не существует* l-РРШ *кодов для* n, *удовлетворяющих следующим условиям:*

$$n > \frac{u}{u-1}\left(3l+1+\frac{ul^2}{4}\right), \quad n \geqslant 6l+3+\frac{ul^2}{2}.$$

Доказательство теоремы приведено в [2]. Заметим, что коды мощности m, удовлетворяющие случаю $s = 1$ — это почти все двоичные коды размерност n. Уравновешенные коды также относятся к этому случаю.

Лемма 4. *Пусть* $x_1, \ldots, x_k$ — *произвольные натуральные числа, такие, что* $x_1 + \cdots + x_k = S > 0$ *и* $\max\{x_i\} - \min\{x_i\} \leqslant l$. *Тогда*

$$\frac{S^2}{k} \leqslant x_1^2 + \cdots + x_k^2 \leqslant \frac{S^2}{k} + \frac{kl^2}{4}.$$

Теорема 4. (*Второе семейство*) *Пусть* $l \in \mathbb{N}$, $s \in \mathbb{N}$, λ_1, λ_2 — *некоторые положительные числа и* m *такое что*

$$\lambda_1\frac{2^n}{\sum\limits_{i=0}^{s}\binom{n}{i}} \leqslant m \leqslant \lambda_2\frac{2^n}{\sum\limits_{i=0}^{s}\binom{n}{i}}$$

Тогда для достаточно больших n *не существует* l-РРШ *кодов мощности* m.

Замечание. Числа λ_1 и λ_2 выбирает так, чтобы первое и второе семейства мощностей пересекались.

Доказательство. Пусть C — l-РРШ код размерности n, мощность которого равна m. Оценим число пар кодовых слов во всех шарах радиуса s двумя способами. Обозначим через V_k объем шара радиуса k.

Первый способ. Обозначим x_1, x_2, …, x_{2^n} — веса шаров радиуса s. Так как каждое кодовое слово содержится ровно в $V_s = \sum\limits_{i=0}^{s} \binom{n}{i}$ шарах радиуса s, то $S := \sum\limits_{i=0}^{2^n} x_i = mV_s$. Число пар кодовых слов в шаре радиуса s веса x_i равно $\frac{x_i(x_i-1)}{2}$, соответственно, число пар кодовых слов во всех шарах радиуса s равно $N = \sum\limits_{i=0}^{2^n} \frac{x_i(x_i-1)}{2} = \frac{1}{2}\sum\limits_{i=0}^{2^n} x_i^2 - \frac{1}{2}\sum\limits_{i=0}^{2^n} x_i$.

Поскольку C является l-РРШ кодом, то $\max\{x_i\} - \min\{x_i\} \leqslant l$. Значит, по лемме 1 и выражая S^2 через m, n и s получаем:

$$N \leqslant \frac{m^2}{2\cdot 2^n}\cdot\frac{1}{(s!)^2}\left(n^{2s} + (3s-s^2)n^{2s-1} + O(n^{2s-2})\right) - \\ - \frac{m}{2}\cdot\frac{1}{s!}\left(n^s + \frac{3s-s^2}{2}n^{s-1} + O(n^{s-2})\right) + \frac{2^n l^2}{8}.$$

Второй способ. В шарах радиуса s содержатся пары кодовых слов на расстоянии от 1 до $2s$. Мы рассмотрим шары радиуса $2s$ с центром в кодовых словах. Разобьем эти шары на сферы радиусом от 1 до $2s$, оценим вес каждой сферы, и соответственно, оценим число пар кодовых слов на расстоянии 1, 2 и так далее до $2s$ отдельно.

В дальнейшем, для более компактной записи выкладок, мы будем писать $t = x \pm 2l$ вместо двойного неравенства $x - 2l \leqslant t \leqslant x + 2l$.

Средний вес шара радиуса k равен $P_k = \frac{mV_k}{2^n}$, вес произвольного шара $S_k(x)$ равен $wt(S_k(x)) = \frac{mV_k}{2^n} \pm l$, а вес произвольной сферы ρ_k равен $wt(\rho_k) = \frac{mV_k}{2^n} - \frac{mV_{k-1}}{2^n} \pm 2l$.

Обозначим через N_k число пар двоичных наборов кода C на расстоянии k, а p_k — число шаров радиуса s, в которых одновременно содержится пара двоичных наборов на расстоянии k. Искомое число N пар кодовых слов в сумме во всех шарах радиуса s равно

$$N = \sum_{k=1}^{2s} N_k p_k = \frac{m^2}{2\cdot 2^n}\cdot\frac{1}{(s!)^2}\left(n^{2s} + \left(3s-s^2\right)n^{2s-1} + O(n^{2s-2})\right) \pm \frac{m^2}{2\cdot 2^n}\cdot 2l\cdot O(n^{s-1}).$$

Рассмотрим случай $m = \lambda\cdot\frac{2^n}{n^{s-1}}\cdot(s-1)!$. Тогда мы получаем, что оценки $N = N'$, полученная первым способом и $N = N''$, полученная вторым способом, имеют вид

$$N \leqslant N' = \frac{\lambda^2 \cdot 2^n}{2s^2}\left(n^2 + (3s - s^2)n - \frac{s}{\lambda}n + O(1)\right),$$

$$N = N'' = \frac{\lambda^2 \cdot 2^n}{2s^2}\left(n^2 + \left(3s - s^2\right)n + O(1)\right).$$

Поскольку одна оценка отличается от другой наличием слагаемого $-\frac{s}{\lambda}n$, начиная с некоторого n мы получим, что оценка N' меньше оценки N''. Противоречие. Теорема доказана.

Список литературы

1. Тарannиков Ю. В. О классе булевых функций, равномерно распределенных по шарам со степенью 1. Вестник Московского Университета. Серия 1. Математика. Механика. 1997, вып. 52, №5, стр. 18–22.

2. Ярыкина М. С. Применение оценок для сумм биномиальных коэффициентов при решении некоторых задач теории кодирования и криптографии. Математические вопросы кибернетики. Вып. 12. — М.: Физматлит, 2003. — С. 87–108.