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-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*

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

и глубины

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

В частности,

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

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

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

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*

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

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 константа, 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.

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

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

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

Значения r, $w(1),\dots,w(k)$ 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 $M_{\Sigma'}$:

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

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 $m(H)n^{L-1} \leq m(G_L) \leq m(H)n^{L-1} + \frac{n^L-n}{n-1}$, 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: $k(H) \leq k(G_L) \leq k(H)\frac{n^L-n}{n-1}$.*

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.