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

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

МАТЕРИАЛЫ IX МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

Москва,
16–21 сентября 2013 г.

Москва 2013

МАТЕРИАЛЫ IX МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

(Москва, 16–21 сентября 2013 г.)

Москва 2013

М34
УДК 519.7

Издание осуществлено при поддержке Российского фонда фундаментальных исследований по проекту 13–01–06831

М34 Материалы IX молодежной научной школы по дискретной математике и ее приложениям (Москва, 16–21 сентября 2013 г.). Под редакцией А. В. Чашкина. — М.: Изд-во ИПМ РАН, 2013. — 130 с.

Сборник содержит материалы IX молодежной научной школы по дискретной математике и ее приложениям, проходившей в Москве с 16 по 21 сентября 2013 г. при поддержке Российского фонда фундаментальных исследований (проект 13–01–06831). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание

МАТЕРИАЛЫ
IX МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ
И ЕЕ ПРИЛОЖЕНИЯМ
(Москва, 16–21 сентября 2013 г.)

Под общей редакцией А. В. ЧАШКИНА

Редакционная группа:
Ю. В. Бородина, Е. Е. Трифонова, А. Д. Яшунский

Ответственный за выпуск *О. С. Дудакова*

СОДЕРЖАНИЕ

ВОССТАНОВЛЕНИЕ ИЗОБРАЖЕНИЯ ПО ЕГО КОДУ

П. Г. Агниашвили (Москва)

Введение

Среди множества подходов к распознаванию образов рассматривается дискретно-геометрический подход [2]. При данном подходе одной из ключевых характеристик изображения является его код. По своему смыслу код должен отражать определенную общность в восприятии изображений. В данной работе таким общим признаком является a'-эквивалентность изображений (аффинная эквивалентность с сохранением нумерации точек). Код строится таким образом, чтобы быть одинаковым для a'-эквивалентных изображений. Кроме того, если изображения не являются a'-эквивалентными, их коды также должны быть различны — только тогда можно говорить о коде, характеризующем данный признак и никакой другой.

В первом разделе вводятся основные понятия, среди которых код и μ-код. По сути, μ-код — это модификация кода, вносящая в него знак. Эта особенность позволяет μ-коду в точности соответствовать классу a'-эквивалентных изображений (лемма 3), что, вообще говоря, не верно для кода: можно привести пример двух изображений, не являющихся a'-эквивалентными, но имеющих один и тот же код.

Возникает задача о нахождении класса изображений, для которых возможно однозначное восстановление по коду с точностью до a'-эквивалентности. Данному вопросу посвящен второй раздел (теорема 1), в котором вводится класс допустимых изображений. Критерий допустимости (теорема 2) решает вопрос о допустимости вырожденных изображений (лежащих в двух непересекающихся гиперплоскостях). Если изображение не является допустимым, то можно говорить о числе эквивалентных изображений, т. е. имеющих одинаковый код. В работе приведена оценка для числа эквивалентных изображений (теорема 3).

В третьем разделе рассматривается более конструктивный вопрос: алгоритм восстановления изображения по его коду. Основная идея заключается в расстановке знаков для элементов кода с целью получения μ-кода. Непосредственный перебор всех расстановок знаков и проверка их корректности приводит к алгоритму, временна́я сложность которого растет экспоненциально с ростом числа точек в изображении. С учетом того, что изображения могут содержать большое число точек, такой алгоритм не является эффективным. В то же время существует алгоритм, решающий данную задачу за линейное время по отношению к числу точек (теорема 4).

1. Основные понятия

Изображением в $\mathbb{R}^n$, $n \geqslant 2$, называется конечное множество индексированных точек, не лежащих в одной гиперплоскости и занумерованных индексами $1, \ldots, k$ в случае k точек, $k \in \mathbb{N}$. Для изображения A через $|A|$ будем обозначать число точек в изображении, а через $\mathbb{N}_{|A|} = \{1, \ldots, |A|\}$ — множество индексов у точек изображения. Два изображения A_1 и A_2, состоящие из одинакового числа точек ($|A_1| = |A_2|$), называются *a'-эквивалентными*, если существует аффинное преобразование, при котором каждая точка из A_1 с индексом $p \in \mathbb{N}_{|A_1|}$ отображается в точку из A_2 с тем же индексом $p \in \mathbb{N}_{|A_2|}$.

Рассмотрим изображение A. Введем произвольную аффинную систему координат в $\mathbb{R}^n$, и пусть $(x_1^p, \ldots, x_n^p)$ — координаты точки с индексом $p \in \mathbb{N}_{|A|}$ в этой системе координат. Определим для двух произвольных наборов индексов $p_1, \ldots, p_{n+1} \in \mathbb{N}_{|A|}$ и $q_1, \ldots, q_{n+1} \in \mathbb{N}_{|A|}$ индексированное число $\mu_{q_1 \ldots q_{n+1}}^{p_1 \ldots p_{n+1}}$ по формуле:

$$\mu_{q_1 \ldots q_{n+1}}^{p_1 \ldots p_{n+1}} = \begin{vmatrix} x_1^{p_1} & \cdots & x_n^{p_1} & 1 \\ \vdots & \ddots & \vdots & \vdots \\ x_1^{p_{n+1}} & \cdots & x_n^{p_{n+1}} & 1 \end{vmatrix} \Bigg/ \begin{vmatrix} x_1^{q_1} & \cdots & x_n^{q_1} & 1 \\ \vdots & \ddots & \vdots & \vdots \\ x_1^{q_{n+1}} & \cdots & x_n^{q_{n+1}} & 1 \end{vmatrix}$$

Здесь в случае равенства знаменателя нулю полагаем, что значение $\mu_{q_1 \ldots q_{n+1}}^{p_1 \ldots p_{n+1}}$ не определено, и используем запись $\mu_{q_1 \ldots q_{n+1}}^{p_1 \ldots p_{n+1}} = \infty$. Для краткости обозначаем наборы индексов заглавной буквой, например, $P = (p_1, \ldots, p_{n+1})$, и пишем в таком случае $P \in \mathbb{N}_{|A|}^{n+1}$. Для индексированных чисел вида $\mu_{q_1 \ldots q_{n+1}}^{p_1 \ldots p_{n+1}}$ получаем короткое обозначение μ_Q^P, а наборы индексов P и Q называем *верхним* и *нижним наборами* соответственно. Перестановка индексов в верхнем или нижнем наборах может привести к изменению знака числа μ_Q^P, но не изменяет его абсолютного значения.

Множество индексированных чисел $\mu\text{-}T_A = \{\mu_Q^P \mid P, Q \in \mathbb{N}_{|A|}^{n+1}\}$ называется *μ-кодом* изображения A. Положим $\rho_Q^P = |\mu_Q^P|$ и назовем *кодом* изображения A множество индексированных чисел $T_A = \{\rho_Q^P \mid P, Q \in \mathbb{N}_{|A|}^{n+1}\}$. Таким образом, код является, по сути, μ-кодом без знака.

Пусть для некоторого набора индексов $S = (s_1, \ldots, s_{n+1}) \in \mathbb{N}_{|A|}^{n+1}$ выполняется условие $\mu_S^P \neq \infty$. Обозначим через μ_j^p элемент μ-кода, у которого нижний набор является набором S, а верхний набор есть $(s_1, \ldots, s_{j-1}, p, s_{j+1}, \ldots, s_{n+1})$, т. е. j-й индекс набора S замещен индексом p. Набор индексов S называется *симплексным набором*. Множество $\{\mu_j^p | p \in \mathbb{N}_{|A|}, j \in \mathbb{N}_{n+1}\}$ называется *ключевым подмножеством μ-кода* $\mu\text{-}T_A$ относительно симплексного набора S. Аналогично случаю μ-кода вводятся понятия элемента кода, симплексного набора индексов и ключевого подмножества кода.

Лемма 1 [1]. *Для любого индекса $p \in \mathbb{N}_{|A|}$ выполняется соотношение*:

$$\mu_1^p + \ldots + \mu_{n+1}^p = 1. \tag{1}$$

Лемма 2 [1]. *Для любых наборов индексов* $P = (p_1, \ldots, p_{n+1}) \in \mathbb{N}_{|A|}^{n+1}$, $Q = (q_1, \ldots, q_{n+1}) \in \mathbb{N}_{|A|}^{n+1}$ *верна следующая формула*:

$$\mu_Q^P = \frac{\begin{vmatrix} \mu_1^{p_1} & \cdots & \mu_{n+1}^{p_1} \\ \vdots & \ddots & \vdots \\ \mu_1^{p_{n+1}} & \cdots & \mu_{n+1}^{p_{n+1}} \end{vmatrix}}{\begin{vmatrix} \mu_1^{q_1} & \cdots & \mu_{n+1}^{q_1} \\ \vdots & \ddots & \vdots \\ \mu_1^{q_{n+1}} & \cdots & \mu_{n+1}^{q_{n+1}} \end{vmatrix}} \tag{2}$$

Здесь в случае равенства знаменателя нулю полагаем $\mu_Q^P = \infty$.

Лемма 3 [1]. *Каждому классу a'-эквивалентных изображений соответствует единственный* μ*-код, являющийся* μ*-кодом для каждого изображения из класса. Данное соответствие является биекцией.*

2. Класс допустимых изображений

Рассмотрим произвольную аффинную систему координат в $\mathbb{R}^n$, $n \geqslant 2$. Пусть $M = \{\mathbf{x}^{p_1}, \ldots, \mathbf{x}^{p_m}\}$ — некоторое множество точек. Аффинная оболочка множества M, т. е. множество $\{\alpha_1\mathbf{x}^{p_1} + \ldots + \alpha_m\mathbf{x}^{p_m} \mid \sum\limits_{i=1}^{m} \alpha_i = 1\}$ называется *гранью* $<M>$.

Как известно, для любой точки $\mathbf{x}^a \in <M>$ множество $<M> - \mathbf{x}^a$ является линейным пространством. *Размерностью* грани $<M>$ называется число, на единицу большее размерности пространства $<M> - \mathbf{x}^a$. Под размерностью множества M будем понимать размерность соответствующей грани $<M>$, и потому в обоих случаях будем использовать обозначение $\dim(M)$.

Изображение A называется *допустимым*, если для любых двух непересекающихся граней $< A_1 >$ и $< A_2 >$, содержащих все точки изображения A, выполняется соотношение $\dim(A) = \dim(A_1) + \dim(A_2)$. Очевидно, любое изображение, a'-эквивалентное допустимому изображению, также является допустимым. Это замечание позволяет говорить о допустимости целого класса a'-эквивалентных изображений.

Теорема 1 [1]. *Код определяет единственный класс a'-эквивалентных изображений тогда и только тогда, когда класс является допустимым.*

Изображение A называется *вырожденным*, если существуют две непустые непересекающиеся грани $< A_1 >$ и $< A_2 >$, содержащие все точки изображения A. В противном случае изображение называется *невырожденным*.

Множества $A_1, \ldots, A_k$ называются *независимыми*, если их грани попарно не пересекаются.

Теорема 2. *Изображение A является допустимым тогда и только тогда, когда для некоторого $k \in \mathbb{N}$ существуют независимые невырожденные изображения $A_1, \ldots, A_k$, такие что $A = A_1 \cup \ldots \cup A_k$ и $\dim(A) = \sum\limits_{i=1}^{k} \dim(A_i)$.*

Если изображение не является допустимым, то существуют отличные от данного изображения, имеющие такой же код. Такие изображения называются *эквивалентными*. Обозначим через $C(A)$ число изображений, эквивалентных изображению A. Положим $C(d) = \max\limits_{A:\, \dim(A)=d} C(A)$, $d \geqslant 3$. Имеет место

Теорема 3. *При любом натуральном $d \geqslant 3$ верна оценка*

$$2^{d-2} \leqslant C(d) \leqslant 2^{d-1}.$$

Таким образом, данному коду может соответствовать большое число изображений. Возникает вопрос о нахождении всех таких изображений по коду.

3. Алгоритм восстановления изображения по его коду

Рассмотрим изображение A в $\mathbb{R}^n$, $n \geqslant 2$. Пусть $\{\rho_j^p \mid p \in \mathbb{N}_{|A|}, j \in \mathbb{N}_{n+1}\}$ — ключевое подмножество кода T_A относительно некоторого симплексного набора индексов S, а $T^\rho = (t_{pj})$ — матрица размера $|A| \times (n+1)$, определенная соотношением $t_{pj} = \rho_j^p$, $p \in \mathbb{N}_{|A|}$, $j \in \mathbb{N}_{n+1}$. Для произвольной матрицы $T = (t_{ij})$ с элементами из $\mathbb{R}$ через $M(T)$ обозначим класс всех матриц $A = (a_{ij})$ того же размера, для которых $|a_{ij}| = |t_{ij}|$.

Произвольная матрица $T^\mu \in M(T^\rho)$ называется *матрицей кода T_A* относительно симплексного набора индексов S. Элементы матрицы кода T^μ обозначаем через μ_j^p. Матрица кода называется *правильной*, если для каждой ее строки $(\mu_1^p, \ldots, \mu_{n+1}^p)$ выполняется соотношение (1) и для любых двух наборов индексов $P, Q \in \mathbb{N}_{|A|}^{n+1}$ выполняется соотношение $|\mu_Q^P| = \rho_Q^P$, где число μ_Q^P определяется формулой (2).

Лемма 4. *Каждый класс a'-эквивалентных изображений соответствует единственной правильной матрице кода T^μ, совпадающей с ключевым подмножеством μ-кода каждого изображения класса (при фиксированном симплексном наборе). Данное соответствие является биекцией.*

Данная лемма позволяет сформулировать задачу о восстановлении изображения с точностью до a'-эквивалентности по его коду в следующем виде:

Для изображения A известен его код T_A и некоторый симплексный набор индексов S. Требуется найти все правильные матрицы кода T_A относительно симплексного набора S.

Заметим, что данную задачу можно решить очевидным способом: перебрать все матрицы кода $T^\mu \in M(T^\rho)$, проверяя для каждой из них условия

правильной матрицы кода. Но такой способ оказывается неэффективным с вычислительной точки зрения, так как для числа N матриц кода верна оценка $2^{|A|} \leqslant N \leqslant 2^{(n+1)|A|}$, и потому прямой перебор приводит к экспоненциальной сложности по отношению к числу точек в изображении. В этой связи актуальна

Теорема 4. *Для каждого $n \geqslant 2$ существует алгоритм со следующими свойствами:*

1. *Входные данные алгоритма: пара (T_A, S), где T_A — код произвольного изображения A в $\mathbb{R}^n$, и S — произвольный симплексный набор кода T_A. Выходные данные алгоритма: все правильные матрицы кода T_A относительно симплексного набора S и только они.*

2. *Существует реализация алгоритма с временно́й сложностью $C(n)|A|$, где $C(n) = O(n4^n)$.*

Список литературы

1. Агниашвили П. Г. Однозначность восстановления изображения по его коду в n-мерном случае // Интеллектуальные системы. — 2011. — Т. 15, вып. 1-4. — С. 293–332.
2. Козлов В. Н. Элементы математической теории зрительного восприятия. — М.: Издательство Центра прикладных исследований при механико-математическом факультете МГУ, 2001.

ВЕРХНЯЯ ОЦЕНКА НЕНАДЕЖНОСТИ СХЕМ В БАЗИСЕ, СОСТОЯЩЕМ ИЗ ФУНКЦИИ ВЕББА

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

Введение

В современной математике и технике теория синтеза схем из ненадежных функциональных элементов занимает важное место. Стоит отметить, что доминирующее положение занимают схемы, функционирующие на основе двухзначной логики. Однако сложность решаемых задач, а, следовательно, и технических устройств, постоянно возрастает. Уже подходят к своему пределу многие технологические возможности, такие как увеличение плотности элементов на схемах, повышение рабочей частоты. Применение многозначной логики является одним из путей решения названных проблем.

К многозначным логикам, к их математическому аппарату как к источнику математических моделей, обладающих большими потенциальными возможностями, обращались неоднократно [1, 2]. В работе [3] построен функционально полный в P_3 базис, в котором на компромиссной основе согласованы математические и технические требования и интересы, и рассмотрены некоторые аспекты синтеза электронных схем в этом базисе.

Определенный интерес представляет исследование надежности функционирования схем в полном базисе из трехзначных функций. Стоит отметить, что многозначный синтез имеет ряд особенностей, и вопрос повышения надежности схем, реализующих функции трехзначной логики, является к настоящему моменту плохо изученным. В этой работе предложен метод синтеза надежных схем в полном базисе, состоящем из функции Вебба $V_3(x_1, x_2) = \max(x_1, x_2) + 1 (\mathrm{mod}\ 3)$.

Постановка задачи

Пусть $n \geqslant 1$, а P_3 — множество всех функций трехзначной логики, т. е. функций $f(x_1, ..., x_n) : \{0, 1, 2\}^n \to \{0, 1, 2\}$. Рассмотрим реализацию функций из множества P_3 схемами из ненадежных функциональных элементов в базисе, состоящем из функции Вебба $V_3(x_1, x_2) = \max(x_1, x_2) + 1 (\mathrm{mod}\ 3)$. Полнота этого множества в P_3 проверена, например, в книге [4].

Будем считать, что схема из ненадежных элементов реализует функцию $f(\tilde{x})$, $\tilde{x} = (x_1, ..., x_n)$, если при поступлении на входы схемы набора $\tilde{a}$ при отсутствии неисправностей в схеме на ее выходе появляется значение $f(\tilde{a})$.

Предположим, что каждый элемент базиса на любом входном наборе $\widehat{a}$ ($\widehat{a} = (a_1, a_2)$) таком, что $f(\widehat{a}) = \tau$, с вероятностью ε, $\varepsilon \in (0, 1/4]$, выдает значение $\tau + 1 (\mathrm{mod}\ 3)$ и с вероятностью ε выдает значение $\tau + 2 (\mathrm{mod}\ 3)$. Все элементы схемы переходят в неисправные состояния независимо друг от друга.

Пусть схема S реализует функцию $f(\tilde{x})$. Обозначим через $P_i(S, \tilde{a})$ вероятность появления значения i ($i \in \{0, 1, 2\}$) на выходе схемы S при входном наборе $\tilde{a}$, а через $P_{f(\tilde{a}) \neq \tau}(S, \tilde{a})$ — вероятность появления ошибки на выходе схемы S при входном наборе $\tilde{a}$, на котором $f(\tilde{a}) = \tau$. Ясно, что $P_{f(\tilde{a}) \neq \tau}(S, \tilde{a}) = P_{\tau+1}(S, \tilde{a}) + P_{\tau+2}(S, \tilde{a})$.

Например, если входной набор $\tilde{a}$ схемы S такой, что $f(\tilde{a}) = 0$ (т. е. при отсутствии неисправностей в схеме S на ее выходе появляется значение 0), то вероятность ошибки на этом наборе равна $P_{f(\tilde{a}) \neq 0}(S, \tilde{a}) = P_1(S, \tilde{a}) + P_2(S, \tilde{a})$. Обозначим через α максимальную вероятность ошибки на всех таких наборах $\tilde{a}$, что $f(\tilde{a}) = 0$. В дальнейшем будем писать $\alpha = \max\limits_{\tilde{a}, f(\tilde{a})=0} \{P_{f(\tilde{a}) \neq 0}(S, \tilde{a})\}$.

Если входной набор $\tilde{a}$ схемы S такой, что $f(\tilde{a}) = 1$ (т. е. при отсутствии неисправностей в схеме S на выходе схемы появляется значение 1, то вероятность ошибки на этом наборе равна $P_{f(\tilde{a}) \neq 1}(S, \tilde{a}) = P_0(S, \tilde{a}) + P_2(S, \tilde{a})$. Обозначим $\beta = \max\limits_{\tilde{a}, f(\tilde{a})=1} \{P_{f(\tilde{a}) \neq 1}(S, \tilde{a})\}$.

Если входной набор $\tilde{a}$ схемы S такой, что $f(\tilde{a}) = 2$ (т. е. при отсутствии неисправностей в схеме S на выходе схемы появляется значение 2), то вероятность ошибки на этом наборе равна $P_{f(\tilde{a})\neq 2}(S,\tilde{a}) = P_0(S,\tilde{a}) + P_1(S,\tilde{a})$. Обозначим $\gamma = \max\limits_{\tilde{a}, f(\tilde{a})=2}\{P_{f(\tilde{a})\neq 2}(S,\tilde{a})\}$.

Ненадежностью схемы S будем называть число $P(S) = \max\{\alpha,\beta,\gamma\}$.

Замечание. Очевидно, что $\alpha \leqslant P(S)$; $\beta \leqslant P(S)$; $\gamma \leqslant P(S)$.

Функционирование базисного элемента E с приписанной ему функцией Вебба $V_3(x_1,x_2) = \max(x_1,x_2)+1 (\mathrm{mod}\ 3)$ можно описать таблицей 1.

Таблица 1

x_1	x_2	$V_3(x_1,x_2)$	p_0	p_1	p_2
0	0	1	ε	$1-2\varepsilon$	ε
0	1	2	ε	ε	$1-2\varepsilon$
0	2	0	$1-2\varepsilon$	ε	ε
1	0	2	ε	ε	$1-2\varepsilon$
1	1	2	ε	ε	$1-2\varepsilon$
1	2	0	$1-2\varepsilon$	ε	ε
2	0	0	$1-2\varepsilon$	ε	ε
2	1	0	$1-2\varepsilon$	ε	ε
2	2	0	$1-2\varepsilon$	ε	ε

Замечание. Очевидно, что ненадежность $P(E)$ базисного элемента E равна 2ε (т. е. $P(E) = 2\varepsilon$), а надежность элемента E равна $1-2\varepsilon$.

Формулировки основных теорем

Пусть f — произвольная функция из P_3, а S — любая схема, реализующая функцию f. Покажем, каким образом по схеме S построить схему, которая реализует ту же функцию f, но, возможно (при некоторых условиях на $P(S)$), более надежно. Для этого возьмем два экземпляра схемы S и соединим их выходы со входами базисного элемента E. Новую схему обозначим $\psi(S)$. Затем возьмем два экземпляра схемы $\psi(S)$ и другой базисный элемент E. Соединим выходы схем $\psi(S)$ со входами этого базисного элемента. Получим схему $\psi(\psi(S)) = \psi^2(S)$. Наконец, возьмем два экземпляра схем $\psi^2(S)$ и третий базисный элемент. Соединим выходы схем $\psi^2(S)$ со входами базисного элемента. Получим схему $\psi^3(S)$, которая при некоторых условиях на $P(S)$ функционирует с большей надежностью, чем исходная схема S.

Теорема 1. *Пусть f — произвольная функция из P_3, S — любая схема, реализующая f, а $P(S)$ — ненадежность схемы S. Тогда схема $\psi^3(S)$ реализует функцию f с ненадежностью*

$$P(\psi^3(S)) \leqslant \max\{8\varepsilon+4P^2(S)+(3\varepsilon+2P^2(S))^2, 6\varepsilon+8(\varepsilon+P(S))^2, 2\varepsilon+25(\varepsilon+P(S))^2\}.$$

Доказательство проводится непосредственным вычислением вероятности ошибок на выходе схемы $\psi^3(S)$ с помощью формулы полной вероятности.

С помощью теоремы 1 доказывается теорема 2.

Теорема 2. *При любом $n \in \mathbb{N}$ любую функцию $f(x_1, ..., x_n)$ можно реализовать такой схемой C, что при всех $\varepsilon \in (0, 1/(4(198 \cdot 3^n + 5n - 344)^2))$ верно неравенство*

$$P(C) \leqslant 8\varepsilon + 266\varepsilon^2.$$

Таким образом, из теоремы 2 следует, что при любом $n \in \mathbb{N}$ любую функцию $f(x_1, ..., x_n) \in P_3$ можно реализовать схемой, ненадежность которой при $n \to \infty$ и $\varepsilon \leqslant 1/(4(198 \cdot 3^n + 5n - 344)^2)$ асимптотически при $\varepsilon \to 0$ не больше 8ε.

Цель дальнейших исследований — получение нетривиальных нижних оценок ненадежности схем.

Работа выполнена при финансовой поддержке РФФИ, проекты 12-01-31340 и 11-01-00212.

Список литературы

1. Виноградов Ю.А., Иорданский М.А. Машинный анализ схем ЭВМ // Проблемы кибернетики, вып. 24. — М.: Наука, 1972. — С. 147–160.
2. Моделирующие системы с многозначными гибридным кодированием // Сб. науч. трудов под ред. М.А. Ракова — Киев: Наукова думка, 1980. — 192 с.
3. Виноградов Ю.А. О синтезе трехзначных схем // Математические вопросы кибернетики, вып.3. — М.: Наука, 1991. — С. 187–198.
4. Яблонский С.В. Введение в дискретную математику. — Учеб. пособие для вузов. — М.: Высш. шк., 2001. — 384 с.

О НАДЕЖНОСТИ СХЕМ В БАЗИСЕ $\{\overline{x\&y}\}$ ПРИ КОНСТАНТНЫХ НЕИСПРАВНОСТЯХ НА ВХОДАХ ЭЛЕМЕНТОВ

М. А. Алехина, В. В. Курышева (Пенза)

Впервые задачу синтеза надежных схем из ненадежных элементов рассматривал Дж. фон Нейман [1]. Он предполагал, что все элементы схемы независимо друг от друга с вероятностью ε, $\varepsilon \in (0, 1/2)$, подвержены инверсным неисправностям, когда функциональный элемент с приписанной ему булевой функцией e в неисправном состоянии реализует функцию $\bar{e}$. С помощью итерационного метода Дж. фон Нейман установил, что при $\varepsilon \leqslant 1/6$ произвольную булеву функцию можно реализовать схемой, вероятность ошибки на выходе

которой при любом входном наборе значений переменных не превосходит $c\varepsilon$, где c — некоторая константа, зависящая от базиса. С ростом числа итераций сложность схемы увеличивается экспоненциально.

Схема из ненадежных элементов характеризуется двумя важными параметрами: вероятностью ошибки на выходе схемы (ненадежностью) и сложностью схемы. Оптимизации сложности схем уделялось главное внимание в работах С. И. Ортюкова [2], Д. Улига [3] и некоторых других авторов. Задача построения схем, функционирующих с наименьшей (или близкой к наименьшей) вероятностью ошибки решалась М. А. Алехиной [4] в предположении, что все элементы схемы независимо друг от друга переходят в неисправные состояния либо только типа 0 на входах (выходах), либо только типа 1 на входах (выходах).

В этой работе рассматривается задача построения асимптотически оптимальных по надежности схем в базисе $\{\overline{x\&y}\}$, причем в отличие от работы [4] каждый элемент схемы независимо от других элементов схемы может переходить или в неисправное состояние типа 0 на входе, или в неисправное состояние типа 1 на входе. Такие неисправности элементов рассматриваются впервые, ранее не исследовались. Введем необходимые понятия и определения.

Будем считать, что схема из ненадежных функциональных элементов реализует функцию $f(x_1, ..., x_n)$ $(n \geqslant 1)$, если при поступлении на входы схемы набора $\tilde{a} = (a_1, ..., a_n)$ при отсутствии неисправностей в схеме на ее выходе появляется значение $f(\tilde{a})$. Предполагается, что в каждый такт работы схемы на любом входе любого из ее элементов независимым образом могут происходить константные неисправности либо типа 0 с вероятностью ε_0, либо типа 1 с вероятностью ε_1 (но не одновременно). Будем предполагать, что $\varepsilon_0 \in (0, 1/4)$ и $\varepsilon_1 \in (0, 1/2)$.

Неисправности типа 0 *на входах элементов* характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию $x|y$, а в неисправном — поступающий на его вход нуль не искажается, а поступающая на его вход единица с вероятностью ε_0 может превратиться в нуль. *Неисправности типа* 1 *на входах элементов* определяются аналогично. т. е. в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию $x|y$, а в неисправном — поступающая на его вход единица не искажается, а поступающий на его вход нуль с вероятностью ε_1 может превратиться в единицу. Учитывая характер рассматриваемых неисправностей, вычислим вероятности появления ошибок на выходе базисного элемента E при всех входных наборах этого элемента:

$P_0(E, (00)) = \varepsilon_1^2$, $P_0(E, (01)) = P_0(E, (10)) = \varepsilon_1$, $P_1(E, (11)) = 2\varepsilon_0 - \varepsilon_0^2$.

Пусть $P_{\overline{f(\tilde{a})}}(S, \tilde{a})$ — вероятность появления $\overline{f(\tilde{a})}$ на выходе схемы S, реализующей булеву функцию $f(\tilde{x})$, при входном наборе $\tilde{a}$. *Ненадежность* $P(S)$ схемы S определяется как максимальное из чисел $P_{\overline{f(\tilde{a})}}(S, \tilde{a})$ (максимум бе-

рется по всем входным наборам $\tilde{a}$ схемы S), т. е. $P(S) = \max\{P_{\overline{f(\tilde{a})}}(S, \tilde{a})\}$. *Надежность* схемы S равна $1 - P(S)$.

Очевидно, ненадежность базисного элемента E равна $\max\{2\varepsilon_0 - \varepsilon_0^2, \varepsilon_1\}$. Обозначим ее через ε, т. е. $\varepsilon = \max\{2\varepsilon_0 - \varepsilon_0^2, \varepsilon_1\}$, тогда надежность базисного элемента E равна $1 - \varepsilon$.

Пусть $P_{\varepsilon_0,\varepsilon_1}(f) = \inf P(S)$, где инфимум берется по всем схемам S из ненадежных элементов, реализующим функцию f.

Схема A из ненадежных элементов, реализующая функцию f, называется *асимптотически оптимальной по надежности*, если $P(A) \sim P_{\varepsilon_0,\varepsilon_1}(f)$ при $\varepsilon_0 \to 0, \varepsilon_1 \to 0$.

Справедлива теорема 1.

Теорема 1. *Любую булеву функцию f можно реализовать такой схемой B, что ее ненадежность $P(B) \leqslant 2\varepsilon_0 + 2\varepsilon_1^2 + 48\varepsilon^2$ при всех $\varepsilon \in (0, \epsilon]$, где* $\epsilon = \min\{1/160,\ (\sqrt{2(2\varepsilon_0 + (2\varepsilon_0 - \varepsilon_1)^2)} - 4\varepsilon_0)/8\}$.

Пусть $h(\tilde{x}), \tilde{x} = (x_1, ..., x_n)$, — произвольная булева функция, а $K(n)$ — множество булевых функций вида $f(\tilde{x}) = (\bar{x}_i \vee h(\tilde{x}))^a$, где $n \in \{1, ..., n\}, a \in \{0, 1\}$. Обозначим через K множество $\bigcup\limits_{n=1}^{\infty} K(n)$.

Теорема 2. *Пусть функция $f \notin K$, и S — любая схема, реализующая f. Тогда $P(S) \geqslant 2\varepsilon_0 + 2\varepsilon_1^2 - 5\varepsilon_0^2 - 4\varepsilon_0\varepsilon_1 - 4\varepsilon_1^3 - 4\varepsilon_0\varepsilon_1^2 - \varepsilon_0^4$ при всех $\varepsilon \in (0, 1/8]$.*

Из теоремы 2 следует, что любая схема, удовлетворяющая условиям теоремы 1 и реализующая булеву функцию $f \notin K$, является асимптотически оптимальной по надежности и функционирует с ненадежностью, асимптотически равной $2\varepsilon_0 + 2\varepsilon_1^2$ при $\varepsilon_0, \varepsilon_1 \to 0$.

Нетрудно проверить, что число функций в классе $K(n)$ не больше $2n2^{2^{n-1}}$, что мало по сравнению с общим числом 2^{2^n} булевых функций от n переменных. Поэтому почти все булевы функции в рассматриваемом базисе можно реализовать асимптотически оптимальными по надежности схемами, функционирующими с ненадежностью, асимптотически равной $2\varepsilon_0 + 2\varepsilon_1^2$ при $\varepsilon_0, \varepsilon_1 \to 0$.

Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 11–01–00212).

Список литературы

1. фон Нейман Дж. Вероятностная логика и синтез надежных организмов из ненадежных компонент // Автоматы. М.: ИЛ, 1956. — С. 68–139.
2. Ортюков С. И. Об избыточности реализации булевых функций схемами из ненадежных элементов // Труды семинара по дискретной математике и ее приложениям (Москва, 27 — 29 января 1987 г.). — М.: Изд-во МГУ, 1989. — С. 166–168.

3. Uhlig D. Reliable networks from unreliable gates with almost minimal comlexity // Fundamentals of Computation Theory. Intern. conf. FCT'87 (Kazan, June 1987). — Proc. Berlin: Springer-Verl., 1987. — P. 462–469. (Lecture Notes in Comput. Sci.; V. 278).
4. Алехина М. А. Синтез асимптотически оптимальных по надежности схем из ненадежных элементов (монография). — Пенза: Информационно-издательский центр ПГУ, 2006. — 156 с.

ТОЧНАЯ СВЕРХЭКСПОНЕНЦИАЛЬНАЯ ОЦЕНКА СЛОЖНОСТИ ДЛЯ ОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ

А. А. Андреев (Москва)

Рассматривается задача о реализации функций многозначной логики формулами [1]. Известно, что в двузначной логике сложность реализации функций формулами над конечными системами имеет не более чем экспоненциальный порядок роста от числа переменных [2, 3]. В работе [4] приводится пример последовательности функций 5-значной логики, сложность которых в классе формул над некоторой конечной системой превосходит $2^{C_n^{n/2}}$, где n — число переменных. В работе [5] аналогичный результат получен для последовательности функций 4-значной логики. В работе автора [6] приводится последовательность $f_n(x_1, \ldots, x_n)$ функций из P_{10}, сложность которых в классе формул над некоторой конечной системой превосходит 2^{3^n}.

В настоящей работе приводится пример последовательностей функций из P_k, сложность которых превосходит $2^{(k-3)^n}$. Кроме того, приводится точная формула для сложности реализации этих функций. В частности, этот пример позволяет привести последовательность функций из P_6, сложность которых в классе формул над некоторой конечной системой превосходит 2^{3^n}.

Обозначим через P_k множество всех функций k-значной логики, $k \geqslant 4$. Обозначим через E^n $(n \geqslant 1)$ множество всех наборов $(\alpha_1, \ldots, \alpha_n)$, таких, что $\alpha_1, \ldots, \alpha_n \in E_k = \{0, 1, \ldots, k-1\}$, а через H_n — множество всех наборов из E^n, состоящих только из символов $3, \ldots, k-1$, причем тройки есть обязательно. Определим функции $\lambda(x, y)$, $\mu(x, y, z)$, $\varphi_m(x, y)$ $(m \in \{3, \ldots, k-1\})$ и $f_n(y, x_1, \ldots x_n)$ из P_k следующим образом. Положим

$$\lambda(x,y) = \begin{cases} 0, & \text{если } x = 0,\ y = 2; \\ 1, & \text{если } x = 1 \text{ или } x = 0,\ y = 3; \\ 2 & \text{в остальных случаях;} \end{cases}$$

$$\mu(x,y,z)=\begin{cases}\lambda(x,z), & \text{если } x=y;\\ 2 & \text{в противном случае;}\end{cases}$$

$$\varphi_m(x,y)=\begin{cases}3, & \text{если } x=3,\ y=m;\\ 2 & \text{в остальных случаях;}\end{cases}$$

$$f_n(y,x_1,\ldots,x_n)=\begin{cases}0, & \text{если } y=0,\ (x_1,\ldots x_n)\notin H_n;\\ 1, & \text{если } y=1 \text{ или } y=0,\ (x_1,\ldots x_n)\in H_n;\\ 2 & \text{в остальных случаях.}\end{cases}$$

Положим $\mathfrak{B}=\{\mu,\varphi_3,\ldots,\varphi_{k-1},2\}$, $\mathfrak{A}=\mathfrak{B}\cup\{\lambda\}$. Имеет место следующее утверждение.

Теорема. *При всех $n\geqslant 1$, $k\geqslant 4$ для последовательности f_n функций k-значной логики имеет место равенство*

$$L_{\mathfrak{B}}(f_n)=(n+1)\cdot 2^{n((k-3)^n-(k-4)^n)}-n.$$

Из этой теоремы (при $k=6$) получаем

Следствие. *При всех $n\geqslant 1$ для последовательности f_n функций 6-значной логики имеет место равенство*

$$L_{\mathfrak{B}}(f_n)=(n+1)\cdot 2^{n(3^n-2^n)}-n.$$

Следует отметить, что это следствие является усилением результата упомянутой выше работы [6].

При доказательстве теоремы ключевым фактом является следующее утверждение.

Лемма. *Пусть Φ — произвольная формула над $\mathfrak{A}$, реализующая функцию $f_n(y,x_1,\ldots,x_n)$ из P_k и имеющая вид*

$$\Phi=\lambda(\lambda(\ldots\lambda(\lambda(y,Z_1),Z_2),\ldots),Z_N),$$

где $Z_1,\ldots,Z_N$ — формулы над $\mathfrak{A}$, $k\geqslant 4$, n и N — натуральные. Пусть $L(\Phi)=L_{\mathfrak{A}}(f_n)$. Тогда

$$N\geqslant(k-3)^n-(k-4)^n,$$

и для всех $i=1,\ldots,N$ выполняются неравенства

$$L(Z_i)\geqslant n.$$

Работа выполнена при финансовой поддержке РФФИ (проект №11–01–00508) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.
2. Угольников А. Б. О глубине формул в неполных базисах // Математические вопросы кибернетики, вып. 1. — М.: Наука, 1988. — С. 242–245.
3. Угольников А. Б. О глубине и сложности формул, реализующих функции из замкнутых классов // Доклад АН СССР — 1988. — Т. 298, № 6. — С. 1341–1344.
4. Угольников А. Б. О сложности реализации формулами одной последовательности функций многозначной логики // Математические вопросы кибернетики. — вып. 2. — 1989. — С. 174–176.
5. Угольников А. Б. О сложности реализации формулами одной последовательности функций 4-значной логики //Вестник Московского университета — сер. 1. Математика. Механика. — 2004, № 3. — С. 52–55.
6. Андреев А. А. Об одной последовательности функций многозначной логики // Вестник Московского университета — сер. 1. Математика. Механика. — 2011, № 6. — С. 3–7.

ДИСКРЕТНЫЕ ДИНАМИЧЕСКИЕ СИСТЕМЫ ЦИРКУЛЯНТНОГО ТИПА С ПОРОГОВЫМИ ФУНКЦИЯМИ В ВЕРШИНАХ

Ц. Ч.-Д. Батуева (Новосибирск)

Введение

Пусть даны $n \geqslant 3$ и $\{d_1, d_2, \ldots, d_k\} \subseteq \{0, 1, \ldots, n-1\}$. *Циркулянтом* принято называть ориентированный граф $G_{n;d_1,d_2,\ldots,d_k}$ с множеством вершин $\{0, 1, \ldots, n-1\}$ и дуг $\{\overrightarrow{ij} \mid j - i \equiv d_r \pmod n), r = 1, 2, \ldots, k\}$ [3].

В работе [2] была введена следующая общая модель дискретной динамической системы циркулянтного типа.

В каждый момент времени вершины циркулянта $G_{n;d_1,d_2,\ldots,d_k}$ помечены элементами $v_0, v_1, \ldots, v_{n-1}$ из конечного поля F_q порядка q. Будем называть набор $\widetilde{v} = (v_0, v_1, \ldots, v_{n-1}) \in F_q^n$ *состоянием системы*. В следующий момент времени состояние системы пересчитывается под действием отображения

$$A_{f,q} : F_q^n \to F_q^n,$$

где $f = (f_0, f_1, \ldots, f_{n-1})$ и каждая вершина приобретает новую метку, равную значению функции $f_i : F_q^k \to F_q$, аргументами которой являются значения старых меток в тех вершинах, дуги которых входят в вершину i.

Функциональным графом $G_{f,q}$ называется, ориентированный граф, вершинами которого являются элементы из F_q^n, а дуги соединяют вершины $\widetilde{v}$ и $\widetilde{u}$, если $A_{f,q}(\widetilde{v}) = \widetilde{u}$.

Состояние системы $\widetilde{u}$ называется *рабочим*, если существует состояние $\widetilde{v}$ такое, что $A_{f,q}(\widetilde{v}) = \widetilde{u}$. В противном случае состояние называется *истоком*.

Определенная таким образом дискретная динамическая система является моделью регуляторного контура генной сети. Стационарные состояния соответствуют устойчивым состояниям в организме, характеризующимся постоянством концентрации веществ. Циклы описывают периодические незатухающие колебания концентраций определенных групп веществ.

В данной работе рассматривается структура функционального графа в случае, когда отображение $A_f : F_2^n \to F_2^n$, все функции f_i равны между собой, $k < n$ и каждому состоянию системы $\widetilde{v}$ ставится в соответствие состояние $\widetilde{u}$ тогда и только тогда, когда

$$u_i = f_0(v_{i-k \pmod n}, v_{i-(k-1) \pmod n}, \ldots, v_{i-1 \pmod n}),$$

где $i = 0, 1, \ldots, n-1$.

Далее примем обозначение $A_{f_0,q}$ вместо $A_{f,q}$, где $f = (f_0, f_0, \ldots, f_0)$. Функциональный граф также будем обозначать $G_{f_0,q}$.

Пороговой функцией называется функция, которая представима в виде

$$f(x_1, \ldots, x_k) = \begin{cases} 1, & \text{если } \sum\limits_{i=1}^{k} a_i x_i > T, \\ 0, & \text{иначе,} \end{cases}$$

где a_i — вес аргумента x_i, T — порог функции f, $a_i, T \in \mathbb{R}$.

Данная работа посвящена описанию свойств функционального графа $P_{f,2}$, где f — пороговая функция, а именно, — описанию неподвижных точек и некоторых истоков, получению оценок длины максимальной цепочки.

1. Неподвижные точки

Пусть $f : F_q^k \to F_q$. Построим ориентированный граф $P_{f,q}$, вершинами которого являются элементы поля F_q^k, причем дуга идет из вершины $(v_0, v_1, \ldots, v_{k-1})$ в вершину $(v_1, v_2, \ldots, v_k)$ тогда и только тогда, когда $f(v_0, \ldots, v_{k-1}) = v_k$.

Пусть n кратно l. Тогда состояние $(v_0, v_1, \ldots, v_{n-1})$, где $v_i = v_{i+l}$ для $i = 0, 1, \ldots, n-l-1$ будем обозначать через $(v_0, v_1, \ldots, v_{l-1})^{n/l}$.

Теорема 1. *Состояние* $\widetilde{v} = (v_0, v_1, \ldots, v_{l-1})^{n/l}$ *с минимальным периодом* l *является неподвижной точкой отображения* $A_{f,q}$ *тогда и только тогда, когда граф* $P_{f,q}$ *содержит простой цикл* $\widetilde{u}^0, \ldots, \widetilde{u}^{l-1}$, *где вершины*

$$\widetilde{u}^i = (v_i, v_{i+1 \pmod l}, \ldots, v_{i+k-1 \pmod l})$$

для $i = 0, 1, \ldots, l-1$.

2. Свойства функционального графа $P_{f,2}$

Следующая теорема дает описание всех истоков функционального графа $P_{f,2}$ для функции с единственной единицей.

Теорема 2. *Пусть f — булева функция от k переменных и существует единственное $\widetilde{\alpha} \in F_2^k$, что $f(\widetilde{\alpha}) = 1$, а минимальный период слова $\widetilde{\alpha}$ равен p.*

1. *Состояние, содержащее подслово $10^{s-1}1$, является истоком, если выполнено $1 \leqslant s \leqslant k-1$ и $s \neq p$.*

2. *Состояние, содержащее подслово $10^{k-1}1$, является истоком, если выполнено $k = tp$ и $t \geqslant 2$.*

3. *Других истоков нет.*

Основываясь на этих результатах, получено описание неподвижных точек, некоторых истоков и циклов для пороговых функций от не более трех переменных, причем существенно зависящих от всех своих переменных. Также получены оценки на длины максимальных цепей.

Список литературы

1. Евдокимов А. А., Лиховидова Е. О. Дискретная модель генной сети циркулянтного типа с пороговыми функциями // Вестник томского государственного университета. — 2008. — Т. 2(3). — С. 18–21.
2. Евдокимов А. А., Пережогин А. Л. Дискретные динамические системы циркулянтного типа с линейными функциями в вершинах сети // Дискретный анализ и исследование операций. — 2011. — Т. 18, вып 3. — С. 39–48.
3. Харари Ф. Теория графов. — М.: УРСС, 2003.

СЛОЖНОСТЬ И СТРУКТУРА МИНИМАЛЬНЫХ СХЕМ ИЗ КЛАССА BDD ДЛЯ НЕКОТОРЫХ СИММЕТРИЧЕСКИХ ФУНКЦИЙ АЛГЕБРЫ ЛОГИКИ

Е. М. Богомолова (Москва)

Введение

Цель работы — построение минимальных BDD (двоичных решающих диаграмм) для некоторых симметрических функций алгебры логики, нахождение их сложности и описание структуры.

Доказано, что сложность реализации симметричной монотонной функции с порогом 2 от n переменных в классе BDD равна $2n-2$, а сложность реализации элементарных симметрических функций с рабочими числами 1 и $n-1$ от n переменных в классе BDD равна $2n-1$. При этом было установлено, что для данных функций минимальные BDD единственны с точностью до перестановки переменных и могут быть получены методом каскадов.

1. Основные понятия[1] и некоторые предшествующие результаты

Напомним, что BDD Σ от булевых переменных (БП) $x_1, x_2, \dots x_n$ — это ориентированный ациклический граф с одним истоком — входом Σ и двумя стоками — выходами Σ, один из которых помечен символом 0, а другой — символом 1. При этом каждая вершина Σ за исключением выходов, помечена одной из БП набора $x = (x_1, x_2, \dots x_n)$ и имеет две исходящих дуги с пометками 0 и 1. Будем считать, как обычно, что указанная BDD Σ реализует функцию алгебры логики (ФАЛ) $f(x)$ такую, что $f(\alpha) = \sigma$ (здесь α — набор значений БП x, а $\sigma \in B$), тогда и только тогда, когда из входа Σ в выход Σ с пометкой σ идет цепь, в которой пометка любой дуги равна значению БП, приписанной ее начальной вершине, на наборе α.

Напомним также (см., например, [3]), что BDD Σ от БП $x = (x_1, x_2, \dots x_n)$, реализующая ФАЛ $f(x)$, структурно изоморфна и функционально эквивалентна контактной схеме из ориентированных контактов (ОКС) S с тем же самым множеством вершин, входов, выходов и дуг. Единственное формальное различие между Σ и S заключается в том, что любая вершина v BDD Σ, имеющая пометку x_i, $1 \leqslant i \leqslant n$, теряет ее при переходе от Σ к S, а дуги с пометками 0 и 1, исходящие из v, заменяются при этом ориентированными контактами с пометками $\overline{x}_i$ и x_i соответственно.

Указанную ОКС S будем называть контактной моделью BDD Σ и будем обозначать ее через $\hat{\Sigma}$. Заметим, что в ОКС $\hat{\Sigma}$ ФАЛ проводимости от входа к выходу с пометкой σ, $\sigma \in B$, равна $f^{\sigma}(x)$. Те ОКС, которые являются моделями BDD, будем называть каскадными ОКС, так как они тесно связаны с контактными схемами (КС) каскадного типа (см. [3]).

Под сложностью BDD (КС или ОКС) будем понимать, как обычно, число отличных от выходов вершин (соответственно число контактов) в ней. Далее будем обозначать сложность BDD Σ как $\mathcal{L}(\Sigma)$, а сложность КС или ОКС S как $L(S)$. При этом, очевидно, $\mathcal{L}(\Sigma) = 2L(\hat{\Sigma})$. Определим сложность $\mathcal{L}(f)$ (соответственно $L(f)$) ФАЛ f как минимальную из сложностей реализующих ее BDD (соответственно КС), а ту схему, на которой она достигается, будем считать минимальной BDD (соответственно КС).

Симметрической функцией от переменных $x = (x_1, x_2, \dots, x_n)$ с множеством рабочих чисел $I, I \subseteq [0, n]$, будем называть функцию, принимающую значение 1 только на тех наборах значений БП x, число единиц в которых

[1] Понятия, не определяемые в данной работе, могут быть найдены, например, в [3].

принадлежит I, и будем обозначать ее через s_n^I. При этом те ФАЛ s_n^I, для которых $|I| = 1$, считаются элементарными симметрическими ФАЛ.

Сложность реализации в классе КС как произвольных, так и некоторых специальных или конкретных симметрических ФАЛ, в частности, линейных ФАЛ $l_n = x_1 \oplus x_2 \oplus \ldots \oplus x_n$, $\overline{l}_n = x_1 \oplus x_2 \oplus \ldots \oplus x_n \oplus 1$, а также монотонной симметрической ФАЛ с порогом 2, т. е. ФАЛ $s_n^{\overline{2,n}}$, изучалась в ряде работ (см., например, [1, 2, 4, 5, 8]). При этом в некоторых случаях [4, 5] удалось не только установить сложность исследуемых ФАЛ, но и описать структуру минимальных схем. Так, из [4] следует, в частности, что $\mathcal{L}(l_n) = \mathcal{L}(\overline{l}_n) = 2n-2$ и что соответствующая минимальная BDD единственна с точностью до изоморфизма и перестановки БП.

2. Описание минимальных BDD для монотонных симметрических функций с порогом 2

Сферической функцией от n БП называется функция, принимающая значение 0 на всех наборах с одной единицей, значение 1 — на всех наборах с двумя единицами и произвольные значения — на всех остальных наборах.

В работах [4, 5] (см. также [9]) фактически доказано следующее утверждение.

Лемма 1. *Если $f(x_1, x_2, \ldots, x_n)$ — сферическая* ФАЛ, *то в реализующей ее* КС *или* ОКС Σ *для каждого i, $i \in [1, n]$, имеется контакт с пометкой x_i, причем для всех переменных кроме, может быть, двух, такие контакты встречаются в схеме дважды. При этом множество первых замыкающих контактов проводящих цепей, идущих от входа Σ к ее выходу, не пересекается с аналогичным множеством последних замыкающих контактов, и в каждом из них отсутствуют контакты не более чем одной* БП.

Из данной леммы следует нижняя оценка сложности $\mathcal{L}(s_n^{\overline{2,n}}) \geqslant 2n - 2$. Эта сложность достигается при построении BDD методом каскадов, а значит $\mathcal{L}(s_n^{\overline{2,n}}) = 2n - 2$.

Рассмотрим далее ОКС $\hat{\Sigma}$ с выходом v и входами v_0 и v_1, которая моделирует минимальную BDD, реализующую ФАЛ $s_n^{\overline{2,n}}$. Заметим, что в любой цепи из v в v_1 в схеме $\hat{\Sigma}$ последний замыкающий контакт входит непосредственно в v_1, иначе схему либо можно минимизировать, либо она проводит на нулевом наборе.

Также заметим, что если в схеме $\hat{\Sigma}$ контакт, помеченный x_i, единственен, является последним в какой-либо цепи из v в v_1 и исходит из вершины u, то контакт, помеченный $\overline{x}_i$ и исходящий из u, входит непосредственно в v_0. Действительно, в противном случае существует цепь, ведущая из u в v_0 и состоящая более чем из одного контакта. Но такая цепь, согласно предыдущим рассуждениям, не может присутствовать в $\hat{\Sigma}$.

Далее, не ограничивая общности, будем считать, что замыкающий контакт с пометкой x_n единственен и является последним в любой цепи.

Если в схеме $\hat{\Sigma}$ в вершину непосредственно входит замыкающий контакт, исходящий из истока v, то в нее входит ровно один контакт. В противном случае можно построить цепь, ведущую из истока v в v_1 и состоящую только из одного замыкающего контакта.

И последнее, что стоит заметить перед формулировкой теоремы, — если в схеме $\hat{\Sigma}$ из v исходят замыкающий и размыкающий контакты, помеченные x_1 и $\overline{x}_1$, то в данной схеме больше не существует контактов, помеченных этой переменной и ее отрицанием, иначе чтобы получить из $\hat{\Sigma}$ схему, реализующую $s^{\overline{2,n-1}}(x_2, x_3, \ldots, x_n)$, достаточно переименовать в ней исток и убрать 6 дуг. Сложность полученной схемы будет меньше минимальной, а значит предположение не верно.

Теорема 1. *Для любого $n, n \geqslant 3$, справедливо равенство*

$$\mathcal{L}(s_n^{\overline{2,n}}) = 2n - 2,$$

причем соответствующая минимальная BDD *единственна с точностью до перестановки переменных.*

Теорема доказывается индукцией по количеству переменных. Для функции $s^2(x_{n-1}, x_n)$ утверждение теоремы очевидно, а минимальная схема для функции $s^{\overline{2,n}}(x_1, x_2, \ldots, x_n)$ получается из минимальной схемы для функции $s^{\overline{2,n-1}}(x_1, x_2, \ldots, x_{n-1})$ единственным образом, что следует из предыдущих рассуждений.

3. Описание минимальных BDD для элементарных симметрических функций с рабочими числами 1 и $n-1$

Очевидно, что если Σ — ОКС, структурно моделирующая BDD для s_n^1, то схема Σ', получающаяся из Σ при помощи замены всех замыкающих контактов на размыкающие, а всех размыкающих на замыкающие, реализует функцию s_n^{n-1}.

Пусть Σ — каскадная ОКС, структурно моделирующая некоторую минимальную BDD для элементарной симметрической функции с рабочим числом 1 от n переменных, v — ее вход, v_1 — выход, на котором реализуется эта функция, v_0 — выход, на котором реализуется ее отрицание.

Лемма 2. $\mathcal{L}(s_n^1) = \mathcal{L}(s_n^{n-1}) = 2n-1$. *При этом в* ОКС Σ, *структурно моделирующей минимальную* BDD ФАЛ s_n^1, *существует такой номер $j \in [1, n]$, для которого x_j и $\overline{x}_j$ встречаются один раз и исходят из истока схемы, а для любого $i \in [1, n]$, $i \neq j$ контакты с пометками x_i и $\overline{x}_i$ встречаются в Σ по два раза.*

Действительно, если предположить, что существует единственная пара контактов, помеченная какой-либо переменной и исходящая не из истока схемы, то через вершину, из которой они исходят, будут проходить все проводя-

щие в v_1 цепи. Но в случае реализации ${s_n}^1$ минимальной схемой это невозможно.

Теперь перейдем к структуре схемы.

Если в Σ контакт h_i, помеченный x_i, является первым (последним) замыкающим контактом в цепи, проводящей из v в v_0, он не является последним (первым) замыкающим ни в одной другой цепи, проводящей из v в v_0, иначе бы существовала цепь, проводящая на наборе с одной единицей.

Пусть в Σ замыкающий контакт, исходящий из v и помеченный x_1, входит в вершину u_1, а размыкающий — в u_0. Если перенаправить замыкающий контакт, исходящий из u_1 (не ограничивая общности, будем считать, что он помечен x_2) в v_0, полученная схема будет эквивалентна исходной, так как от противного можно доказать, что все цепи из входа в выходы, которым принадлежит замыкающий контакт, исходящий из u_1, входят в v_0.

Если в Σ существует контакт h из вершины u, не являющейся истоком, в вершину u_1, то его можно перенаправить в v_0, получив при этом схему, эквивалентную исходной. В обратном случае существует цепь из v в v_0, проходящая через размыкающий контакт, смежный с h, и проводящая на наборе с одной единицей, что противоречит условию.

Теперь рассмотрим полную ОКС Σ_k с входом w и выходами w_1 и w_0, построенную для s_n^1 методом каскадов (см., например, [3]), при котором разложение происходит сначала по x_1, потом по x_2 и т.д. до x_n, причем в w_1 реализуется s_n^1, а в w_0 — ее отрицание. Пусть в цепи из истока в w_0, состоящей из размыкающих контактов, каждая вершина, из которой исходят размыкающий и замыкающий контакты, помеченные x_i, обозначена s_i (легко видеть, что вершины в этой цепи расположены так: $s_2, s_3, \dots s_n$). Пусть в цепи из истока в w_1, состоящей из замыкающего контакта, помеченного x_1, и размыкающих контактов, t_i — вершина, из которой исходят размыкающий и замыкающий контакты, помеченные x_i (легко видеть, что вершины в этой цепи расположены так: $t_2, t_3, \dots t_n$).

В Σ_k, построенной методом каскадов для s_n^1, замыкающий контакт, исходящий из t_2 не может быть никуда перенаправлен, так чтобы получилась схема, эквивалентная исходной. Действительно, если контакт может быть перенаправлен в вершины w_0, w_1, t_i, при $i > 3$ или в s_i, будут существовать цепи из истоков в стоки, проводящие на наборах, на которых схема не может проводить.

Более того, в Σ_k любой контакт, входящий в w_0, не может быть никуда перенаправлен, чтобы получилась схема, эквивалентная исходной, так как данный контакт может быть либо замыкающим и исходить из t_i, либо размыкающим и исходить из s_n. В обоих случаях перенаправление невозможно, потому что либо образуется цикл, либо схема начинает проводить не на тех наборах.

Теорема 2. *Для любого* $n, n \geqslant 2$, *справедливо равенство*

$$\mathcal{L}(s_n^1) = \mathcal{L}(s_n^{n-1}) = 2n - 1,$$

причем соответствующие минимальные BDD *единственны с точностью до перестановки переменных.*

Доказательство теоремы ведется индукцией по числу переменных. Для s_2^1 это верно, а минимальная BDD для s_n^1 приводима к минимальной BDD для $s_{n-1}^1(x_2, x_3 \dots x_n)$, причем восстановить минимальную BDD для s_n^1 из минимальной BDD для $s_{n-1}^1(x_2, x_3 \dots x_n)$ можно единственным образом.

Список литературы

1. Гринчук М. И. О сложности реализации симметрических булевых функций контактными схемами // Математические вопросы кибернетики. — 1991. — Вып. 3. — М.: Наука. — С. 77–104.
2. Красулина Е. Г. О сложности реализации монотонных симметрических функций алгебры логики контактными схемами // Математические вопросы кибернетики. — 1988. — Вып. 1. — М.: Наука. — С. 140–167.
3. Ложкин С. А. Лекции по основам кибернетики. — М.: МАКС-Пресс, 2005.
4. Ложкин С. А. Об одном методе получения линейных нижних оценок сложности контактных схем и некоторых минимальных схемах для линейных функций // Сборник трудов семинара по дискретной математике и ее приложениям. — М.: Изд-во Механико-Математического факультета МГУ. — 1997. — С. 113–115.
5. Ложкин С. А. Об одном методе получения линейных нижних оценок сложности контактных схем и о структуре минимальных схем для некоторых функций // Межвузовский сборник научных трудов. — 1993. — Вып. 18. — С. 110–112.
6. Лупанов О. Б. К вопросу о реализации симметрических функций алгебры логики контактными схемами // Проблемы кибернетики. — 1965. — Вып. 15. — М.: Наука. — С. 85–99.
7. Нигматуллин Р. Г. Сложность булевых функций. — М.: Наука, 1991.
8. Попов Е. А. О сложности и структуре контактных схем, близких к минимальным, для элементарных симметрических функций // Вестник Московского Университета. Серия 15. Вычислительная математика и кибернетика. — 2008. — Вып. 3. — С. 39–46.
9. Яблонский С. В. Элементы математической кибернетики. — М.: Высшая школа, 2007.

НИЖНЯЯ ОЦЕНКА ДЛИНЫ ПОЛНОГО ПРОВЕРЯЮЩЕГО ТЕСТА В БАЗИСЕ $\{x|y\}$

Ю. В. Бородина (Москва)

Будем рассматривать схемы из функциональных элементов [1, 2] в некотором конечном базисе B. В качестве неисправностей предполагаем константные неисправности типа „1" на выходах элементов (при переходе в неисправное состояние элемент выдает значение 1 независимо от входных данных).

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

Функция, реализуемая на выходе схемы при наличии в схеме неисправного элемента, называется *функцией неисправности*. Всякое множество T входных наборов схемы S называется *полным проверяющим тестом* для этой схемы, если для любой функции неисправности $g(\tilde{x})$, не равной тождественно $f(\tilde{x})$, в T найдется хотя бы один такой набор $\tilde{\sigma}$, что $f(\tilde{\sigma}) \neq g(\tilde{\sigma})$ [3, 4]. Число наборов, составляющих этот тест, называется *длиной* теста.

Введем обозначения [3, 4]: $D(T)$ — длина теста T; $D(S) = \min D(T)$, где минимум берется по всем полным проверяющим тестам T для схемы S; $D(f, B) = \min D(S)$, где минимум берется по всем схемам S в данном базисе B, реализующим функцию f; $D(n, B) = \max D(f, B)$; где максимум берется по всем булевым функциям f от n переменных. Функция $D(n, B)$ называется *функцией Шеннона* длины полного проверяющего теста для базиса B.

В работе [5] было показано, что $D(n, \{\&, \vee, {}^-\}) = 2$ для всех $n \geqslant 2$. Возникает естественный вопрос: верно ли, что для всякого конечного базиса B $D(n, B) \leqslant C(B)$, где $C(B)$— константа, не зависящая от n? Оказывается, это не так.

Теорема. *Для всякого $n \geqslant 2$ имеет место равенство*

$$D(x_1 \vee x_2 \vee \cdots \vee x_n, \{|\}) = n + 1$$

(*здесь* $|$ *обозначает штрих Шеффера*).

Следствие. $D(n, \{|\}) \geqslant n + 1$, *при* $n \geqslant 2$.

Работа выполнена при финансовой поддержке программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем») и РФФИ (проект № 11-07-00311).

Список литературы

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

2. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2002.
3. Яблонский С. В. Некоторые вопросы надежности и контроля управляющих систем// Математические вопросы кибернетики. — 1988. — Вып. 1. — С. 5–25.
4. Редькин Н. П. Надежность и диагностика схем. — М.: МГУ, 1992.
5. Бородина Ю. В. О синтезе легкотестируемых схем в случае однотипных константных неисправностей на выходах элементов// Вестник Московского университета. — Серия 15. Вычислительная математика и кибернетика. — 2008. — №1. — С. 40–44.

ФУНКЦИОНИРОВАНИЕ ДИСКРЕТНЫХ МОДЕЛЕЙ ГЕННЫХ СЕТЕЙ ЦИРКУЛЯНТНОГО ТИПА С ПОРОГОВЫМИ ФУНКЦИЯМИ

И. С. Быков (Новосибирск)

1. Постановка задачи

Одним из процессов, поведение которых могут моделировать дискретные динамические системы, является функционирование *генных сетей*.

Генной сетью называют множество химических веществ внутри биологической клетки. Эти химические вещества взаимодействуют между собой, вступая в химические реакции, продуктом которых вновь являются химические соединения клетки. Таким образом, количественный и качественный химический состав клетки с течением времени изменяется.

Взаимодействие химических веществ внутри клетки задается с помощью *графа-носителя*. Пусть внутри клетки проходит химическая реакция, в которую вступает вещество X, а продуктом реакции является вещество Y:

$$X + \ldots \to Y + \ldots$$

Тогда можно говорить, что вещество X в некотором смысле «влияет» на вещество Y. Это влияние и отражается в графе-носителе.

Определение. Граф-носитель — ориентированный граф $G(V, D)$, каждой вершине которого сопоставляется химическое вещество. $(V(X), V(Y)) \in D(G)$, если в результате реакции с участием вещества X может получиться вещество Y (вещество X «влияет» на вещество Y).

Сопоставим каждой вершине значение s и функцию f. Значение s вершины — это количество соответствующего химического вещества, а функция f

задает правило, согласно которому это количество изменится в следующей момент времени. Аргументами функций данной вершины являются значения s вершин, дуги из которых ведут в данную, т. е. для данного графа-носителя G множество

$$\{s(X) \mid (X, Y) \in D(G)\},$$

является множеством аргументов функции f вершины Y.

Определение. *Состоянием* системы является кортеж $(s_0, s_1, \ldots, s_{n-1})$, где s_i — значение i-ой вершины. Множество всех состояний будем обозначать Ω.

Таким образом, граф-носитель и множество функций f_i всех вершин задают отображение A, действующее на множестве всех состояний.

Определение. Ориентированный граф $H = G(V, D)$, где

$$V = \Omega, \quad D = \{(S_1, S_2) | S_1, S_2 \in \Omega; A(S_1) = S_2\},$$

называют *графом состояний*.

В качестве графа-носителя будем рассматривать *граф-циркулянт*.

Определение. Граф-циркулянт — ориентированный граф $G_{n,k}$ с множеством вершин $V = \{0, 1, \ldots, n-1\}$, и множеством дуг

$$D = \{(i, j) |\ i, j \in V, i \neq j\, (i - j) \bmod n \leqslant k\},$$

В каждой вершине задано значение s_i из $\mathbb{Z}_p = \{0, \ldots, p-1\}$. Таким образом, $\Omega = \mathbb{Z}_p^n$. Параметр p будем называть *значностью*.

В каждой вершине v_i обобщенного графа-циркулянта задана следующая *пороговая функция* f с параметром $T \in \mathbb{Z}$: пусть $S = (s_0, s_1, \ldots, s_{n-1})$, тогда $A(S) = S' = (s'_0, s'_1, \ldots, s'_{n-1})$, где

$$s'_i = f(s_{i+1}, s_{i+2}, \ldots, s_{i+k}) = \begin{cases} s_i + 1, & \text{если } \sum\limits_{j=1}^{k} s_{i+j} < T \text{ и } s_i < p - 1; \\ s_i - 1, & \text{если } \sum\limits_{j=1}^{k} s_{i+j} \geqslant T \text{ и } s_i > 0; \\ s_i, & \text{иначе.} \end{cases}$$

(Здесь и далее арифметические операции в индексах выполняются по модулю n). В дальнейшем будем рассматривать пороговые значения удовлетворяющие неравенству $1 \leqslant T \leqslant k \cdot (p-1)$. В противном случае функционирование системы тривиально.

В работе исследуется задача анализа функционирования: определение качественных характеристик графа состояний по данным параметрам системы p, n, k, T. К таким характеристикам относятся циклы графа состояний и, в частности, неподвижные точки (циклы единичной длины).

2. Неподвижные точки

Лемма 1. *Пусть* $p = 2$. *Если состояние* $S = (s_0, s_1, \ldots, s_{n-1})$ — *неподвижная точка системы с параметрами* n,k,T, *то* $s_i = s_{i+r\cdot \text{НОД}(n,k+1)}$ *для любых* $i \in \mathbb{Z}_n$ *и* $r \in \mathbb{Z}_+$.

Теорема 1. *Пусть система задана параметрами* p, n, k, T. *Тогда неподвижные точки в системе существуют в том и только том случае, когда выполняется каждое из трех условий*:

1. $\text{НОД}(n, k+1) > 1$,
2. $k + 1 - \frac{k+1}{\text{НОД}(n,k+1)} \geqslant \lceil \frac{T}{p-1} \rceil$,
3. $\frac{k+1}{\text{НОД}(n,k+1)}$ *нацело делит* $\lceil \frac{T}{p-1} \rceil$.

Доказательство. Очевидно, что каждая компонента неподвижной точки принимает значение 0 или $p-1$. Отсюда следует, что случай произвольного значения p эквивалентен случаю $p = 2$ и порогового значения $\lceil \frac{T}{p-1} \rceil$.

Необходимость. Пусть S — неподвижная точка.

1. Если $\text{НОД}(n, k+1) = 1$, то по лемме 1 $S = (\widetilde{0})$ или $S = (\widetilde{1})$. Противоречие, так как $(\widetilde{0})$ и $(\widetilde{1})$ не являются неподвижными точками.

2. Пусть $k+1-\frac{k+1}{\text{НОД}(n,k+1)} < \lceil \frac{T}{p-1} \rceil$ и существует хотя бы одно i, что $s_i = 0$. Тогда по лемме 1 S имеет вид:

$$(\ldots, 0, \underbrace{\overbrace{\ldots,0}^{\text{НОД}(n,k+1)}, \overbrace{\ldots,0}^{\text{НОД}(n,k+1)}, \ldots, \overbrace{\ldots,0}^{\text{НОД(n,k+1)}}}_{k+1}, \ldots)$$

   Отсюда следует, что $\sum_{j=1}^{k} s_{i+j} \leqslant k + 1 - \frac{k+1}{\text{НОД}(n,k+1)} < \lceil \frac{T}{p-1} \rceil$, а это означает, что $s_i \neq s'_i = 1$. Противоречие.

3. Пусть $\frac{k+1}{\text{НОД}(n,k+1)}$ не делит нацело $\lceil \frac{T}{p-1} \rceil$. Существует хотя бы одно i, что $s_i = 0$. Обозначим $k' = \frac{k+1}{\text{НОД}(n,k+1)}$. Тогда, в силу того, что k' не делит нацело $\lceil \frac{T}{p-1} \rceil$, существуют такие t, q из $\overline{0, k'-1}$, что

$$\sum_{j=t\cdot \text{НОД}(n,k+1)+1}^{(t+1)\cdot \text{НОД}(n,k+1)} s_{i+j} \neq \sum_{j=q\cdot \text{НОД}(n,k+1)+1}^{(q+1)\cdot \text{НОД}(n,k+1)} s_{i+j}.$$

   Отсюда следует, что $\exists\ 1 \leqslant r < \text{НОД}(n, k+1)$ такое, что $s_{i_q} \neq s_{i_t}$, где

$$i_q = i + q \cdot \text{НОД}(n, k+1) + r; \quad i_t = i + t \cdot \text{НОД}(n, k+1) + r.$$

   Очевидно $|i_t - i_q|$ кратно $\text{НОД}(n, k+1)$, тогда по лемме: $s_{i_q} = s_{i_t}$. Противоречие.

Достаточность. Пусть выполнены все три условия. Построим неподвижную точку. Обозначим

$$T_k = \frac{\lceil \frac{T}{p-1} \rceil \cdot \text{НОД}(n, k+1)}{k+1}.$$

Рассмотрим состояние

$$S = (\overbrace{0, \dots, 0}^{\text{НОД}(n,k+1)-T_k}, \overbrace{p-1, \dots, p-1}^{T_k}, \overbrace{0, \dots, 0}^{\text{НОД}(n,k+1)-T_k}, \dots, \overbrace{p-1, \dots, p-1}^{T_k}).$$

Легко показать, что S — неподвижная точка. Теорема доказана.

Теорема 2. *Пусть система задана параметрами p, n, k, T, которые удовлетворяют условию существования неподвижных точек. Тогда количество неподвижных точек равно*

$$\binom{\text{НОД}(n, k+1)}{T_k}, \text{ где } T_k = \frac{\lceil \frac{T}{p-1} \rceil \cdot \text{НОД}(n, k+1)}{k+1}.$$

3. Циклы

Определение. *Блоком* состояния S называется максимальная по включению последовательность таких компонент $s_i, s_{i+1}, \dots, s_{i+l-1}$, что выполнены равенства $s_i = s_{i+1} = \dots = s_{i+l-1}$. Число l называется размером или длиной блока.

Обозначим множество циклических сдвигов состояния S через $U(S)$. Если состояние из $U(S)$ можно представить в виде

$$0^{l_0}\ 1^{l_1}\ 0^{l_2}\ 1^{l_3} \dots 0^{l_{b(S)-2}}\ 1^{l_{b(S)-1}},$$

то число $b(S)$ будем называть количеством блоков состояния S.

Для $S = (0, 0, \dots, 0)$ и $S = (1, 1, \dots, 1)$ положим $b(S) = 1$.

Лемма 2. *Выполняется неравенство $b(A(S)) \leqslant b(S)$.*

Доказательство. Покажем, что если $s'_i \neq s'_{i+1}$, то $s_{i+1} = s'_{i+1}$.

Пусть $s'_i = 0$, а $s'_{i+1} = 1$. Тогда

$$\sum_{j=1}^{k} s_{i+j} \geqslant T;\ \sum_{j=1}^{k} s_{(i+1)+j} = \sum_{j=2}^{k+1} s_{i+j} < T.$$

Следовательно $s_{i+1} = 1$. Аналогично для $s'_i = 1$.

Получили $s_{i+1} = s'_{i+1}$. Обозначим $J(S') = \{i \mid s'_{i-1} \neq s'_i = 1\}$ — множество индексов начал блоков из единиц в состоянии S'. Теперь покажем, что s_{i_1} и s_{i_2} лежат в различных блоках состояния S для любых различных i_1, i_2 из $J(S')$.

Действительно, для любых различных индексов i_1, i_2 из $J(S')$ существует индекс j, лежащий между ними, такой, что j — начало блока из нулей. Следовательно $s_j = 0$, откуда следует, что s_{i_1} и s_{i_2} лежат в различных блоках состояния S.

Получили что мощность множества $J(S')$ не превосходит количества блоков из единиц в S, а так как мощность множества $J(S')$ равна количеству блоков из единиц в S', то можно заключить, что $b(S') \leqslant b(S)$ для любого S из Ω. Лемма доказана.

Следствие 1. *Если $A^{r'}(S) = S$ для некоторого $r' \in \mathbb{Z}_+$, то $b(S) = b(A^r(S))$ для любого $r \in \mathbb{Z}_+$.*

Теорема 3. *Пусть S лежит в цикле графа состояний, а длина любого блока любого состояния этого цикла не меньше k, тогда $A^2(S) \in U(S)$.*

Доказательство. Возьмем два последовательных блока B_1 и B_2 в состоянии S. Пусть блок B_1 кончается на позиции c, а блок B_2 - на позиции d. Тогда длина блока B_2 равна $d - c$. Обозначим $S' = A(S) = (s'_0, s'_1, \ldots, s'_{n-1})$, и $S'' = A^2(S) = (s''_0, s''_1, \ldots, s''_{n-1})$.

Пусть B_1 — блок из нулей, а B_2 — блок из единиц. Рассмотрим блок B_2 и покажем, что $s'_{d-T} = 0$, а $s'_{d-T+1} = 1$. Действительно:

$$\sum_{j=1}^{k} s_{d-T+j} = \sum_{j=1}^{T} s_{d-T+j} + \sum_{j=T+1}^{k} s_{d-T+j} = T + \sum_{j=T+1}^{k} s_{d-T+j} \geqslant T.$$

Значит $s'_{d-T} = 0$. Аналогично для s'_{d-T+1}:

$$\sum_{j=1}^{k} s_{d-T+1+j} = \sum_{j=1}^{T-1} s_{d-T+1+j} + \sum_{j=T}^{k} s_{d-T+1+j} = T - 1 + \sum_{j=T}^{k} s_{d-T+1+j}.$$

В силу того, что длина любого блока S не меньше k:

$$\sum_{j=T+1}^{k} s_{d-T+1+j} = 0.$$

Аналогично, рассмотрев блок B_1, можно показать, что $s'_{c-k+T-1} = 1$, а $s'_{c-k+T} = 0$.

Теперь обозначим $c' = c - k + T - 1$ и $d' = d - T$, соответственно блок из единиц, заканчивающийся на c' обозначим B'_1, а блок из нулей, заканчивающийся на d' — B'_2. Теперь, проделав ту же самую операцию для блоков B'_1 и B'_2, получим, что $s''_{c'-T} = 0$, $s''_{c'-T+1} = 1$, $s''_{d'-k+T-1} = 1$, $s''_{d'-k+T} = 0$. Рассмотрим блок из единиц в S'' начинающийся с

$$c' - T + 1 = (c - k + T - 1) - T + 1 = c - k$$

и заканчивающийся на

$$d' - k + T - 1 = (d - T) - k + T - 1 = d - k - 1.$$

Получили, что блок B_2 сместился на $k+1$ позицию влево в состоянии S''.

Так как каждый блок из единиц состояния S сместился на $k+1$ позицию влево в состоянии S'', а количество блоков не изменилось, то каждый блок из нулей состояния S тоже сместился на $k+1$ позицию влево в состоянии S''.

Имеем, что каждый блок в состоянии S смещается на $k+1$ позицию влево в состоянии S''. Это и значит, что $S'' \in U(S)$. Теорема доказана.

Анализ экспериментальных результатов приводит к предположению об обобщении теоремы 3:

Гипотеза. *Если S лежит в цикле графа состояний, то $A^2(S) \in U(S)$.*

Список литературы

1. Евдокимов А. А., Лиховидова Е. О. Дискретная модель генной сети циркулянтного типа с пороговыми функциями // Вестник ТГУ. — 2008. — С. 18–21.

СООТВЕТСТВИЕ МЕЖДУ APN-ФУНКЦИЯМИ И СПЕЦИАЛЬНЫМИ БУЛЕВЫМИ ФУНКЦИЯМИ

А. А. Городилова (Новосибирск)

Введение

В работе рассматриваются криптографические векторные булевы функции. Векторная функция, например, задает S-блок — основное нелинейное преобразование блочного шифра. От свойств таких компонент существенное зависит криптографическая стойкость криптосистем.

Приведем формальные определения. *Булевой функцией* от n переменных называется любое отображение $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$. *Весом Хэмминга* $wt(f)$ булевой функции f называется количество единиц в векторе ее значений. *Векторной булевой функцией* F называется любое отображение $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$. Векторную функцию можно рассматривать как набор из m координатных булевых функций от n переменных, т. е. $F = (f_1, \ldots, f_m)$.

Рассматриваемое в данной работе криптографическое свойство было определено в 1994 году в [1]. Векторная функция F называется *δ-дифференциально равномерной*, если для любых векторов $a \neq 0$, b уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более δ решений. Чем меньше значение δ, тем привлекательнее

использовать δ-дифференциально равномерные векторные булевы функции в блочных шифрах для обеспечения стойкости к дифференциальному виду криптоанализа.

Далее рассматриваем только случай $n = m$. В этом случае минимальное возможное δ равно двум. Действительно, если x_0 — решение уравнения $F(x) \oplus F(x \oplus a) = b$, тогда $x_0 \oplus a$ также является решением. APN-*функцией* (Almost Perfect Nonlinear) называется 2-дифференциально равномерная векторная функция. В работе [2] приведен обзор по известным APN-функциям.

Несмотря на достаточно простую формулировку указанного свойства, в области APN-функций остается большое количество открытых вопросов. Прежде всего, это построение новых APN-функций. Все известные конструкции найдены с помощью алгебраического представления, когда функция рассматривается как функция на элементами конечного поля. Однако таких конструкций очень мало.

Рассматриваются смежные вопросы — оценки количества и классификация APN-функций. В работе [3] исследованы следующие отношения эквивалентности. Пусть F и F' — векторные булевы функции. F и F' называются *EA-эквивалентными*, если существуют аффинные перестановки L_1 и L_2, аффинная функция L, что $F' = L_1 \circ F' \circ L_2 \oplus L$. Функции F и F' называются *CCZ-эквивалентными*, если графы $G_F = \{(x, F(x));\ x \in \mathbb{Z}_2^n\}$ и $G_{F'} = \{(x, F'(x));\ x \in \mathbb{Z}_2^n\}$ аффинно эквивалентны. В той же работе показано, что такие преобразования сохраняют свойство функции быть APN-функцией. Кроме того, EA-эквивалентность сильнее CCZ-эквивалентность. Но количество классов эквивалентности и их мощность в общем случае неизвестны.

1. γ-эквивалентность APN-функций

В данной работе предложена новая классификация APN-функций. Опишем подробнее. Пусть $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$. Для F и любого вектора $a \neq 0$ определяется множество

$$B_a(F) = \{F(x) \oplus F(x \oplus a) \mid x \in \mathbb{Z}_2^n\}.$$

Для F строится булева функция γ_F от $2n$ переменных следующим образом:

$$\gamma_F(a, b) = \begin{cases} 1, & \text{если } a \neq 0 \text{ и } b \in B_a(F); \\ 0, & \text{иначе.} \end{cases}$$

Известно, что F является APN-функцией тогда и только тогда, когда $wt(\gamma_F) = 2^{2n-1} - 2^{n-1}$.

Пусть $F, F' : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$. Введем определение.

Определение. Функции F и F' назовем *γ-эквивалентными*, если выполнено равенство $\gamma_F = \gamma_{F'}$.

Нетрудно убедиться, что γ-эквивалентность является отношением эквивалентности на множестве всех векторных булевых функций. Следовательно, множество функций распадается на непересекающиеся классы.

Получены следующие результаты.

Теорема 1. *Пусть F — APN-функция от n переменных. Тогда все функции $F_{c,d}(x) = F(x \oplus c) \oplus d$, где $c, d \in \mathbb{Z}_2^n$, являются APN-функциями, γ-эквивалентными F. Кроме того, все функции $F_{c,d}$ попарно различны.*

Теорема 2. *Пусть γ — булева функция от $2n$ переменных, $\gamma = \gamma_F$ для некоторой APN-функция F от n переменных. Тогда существует не более 2^{2n} APN-функций с такой γ.*

Следствие 1. *В каждом классе γ-эквивалентности APN-функций от n переменных ровно 2^{2n} различных функций.*

Таким образом, γ-эквивалентность устанавливает определенное соответствие между всеми APN-функциями и специальными булевыми функциями от удвоенного числа переменных.

2. Итеративная конструкция APN-функций

В работе предложена итеративная конструкция APN-функций от $n+1$ переменных из двух APN-функции и двух булевых функций от n переменных. Доказана следующая теорема.

Теорема 3. *Пусть F и G — APN-функции от n переменных, f и g — булевы функции от n переменных. Пусть S — векторная булева функция от $n+1$ переменных, определенная как*

$$S(x, x_{n+1}) = ((x_{n+1} \oplus 1)F(x) \oplus x_{n+1}G(x),\ (x_{n+1} \oplus 1)f(x) \oplus x_{n+1}g(x)),$$

где $x \in \mathbb{Z}_2^n$, $x_{n+1} \in \mathbb{Z}_2$. Тогда S — APN-функция, если выполнено условие:
$(*)$ для всех $x, y, a \in \mathbb{Z}_2^n$, $a \neq 0$, таких, что $F(x) \oplus F(x \oplus a) = G(y) \oplus G(y \oplus a)$, выполняется $f(x) \oplus f(x \oplus a) \neq g(y) \oplus g(y \oplus a)$.

Следствие 2. *Пусть F и G — APN-функции от n переменных, f и g — булевы функции от n переменных, удовлетворяющие условию $(*)$ из теоремы 3. Тогда функции $F'(x) = F(x \oplus c') \oplus d'$, $G'(x) = G(x \oplus c'') \oplus d''$, $f' = f(x \oplus c') \oplus d_1$, $g'(x) = g(x \oplus c'') \oplus d_2$ удовлетворяют условию $(*)$ для любых $c', c'', d', d'' \in \mathbb{Z}_2^n$, $d_1, d_2 \in \mathbb{Z}_2$.*

Данное следствие показывает, что если найдена некоторая подходящая четверка функций F, G, f, g, то вместо F и G можно брать и γ-эквивалентные им. Открытым остается вопрос, как выбрать APN-функции F, G и булевы функции f, g, которые бы удовлетворяли условию $(*)$ из теоремы 3. Можно сформулировать гипотезу.

Гипотеза. Для любой APN-функции F от n переменных найдутся APN-функция G и булевы функции f, g от n переменных, удовлетворяющие условию $(*)$.

Вычислительная проверка гипотезы при малых n:
• от $n = 1$ к $n = 2$: гипотеза верна, причём данной конструкцией порождаются все 192 APN-функции от 2-х переменных;
• от $n = 2$ к $n = 3$: гипотеза верна, причём данной конструкцией порождаются 589824 APN-функции из всех 668128 APN-функций от 3-х переменных;
• от $n = 3$ к $n = 4$: весь перебор не реализован, выборочная проверка подтверждает гипотезу.

Список литературы

1. Nyberg K. Differentially uniform mappings for cryptography // Eurocrypt 1993, Lecture Notes in Computer Science. — 1994. — V. 765, — P. 55–64.
2. Тужилин М. Э. Почти совершенные нелинейные функции // Прикладная дискретная математика. — 2009. — № 3. — С. 14–20.
3. Carlet C., Charpin P., Zinoviev V. Codes, bent functions and permutations suitable for DES-like cryptosystems // Designs, Codes and Cryptoraphy. — 1998. — V. 15(2). — P. 125–156.

О СХОДИМОСТИ ВЕТВЯЩИХСЯ ЦЕПНЫХ ДРОБЕЙ С ЦЕЛЫМИ ЭЛЕМЕНТАМИ

Д. В. Грибанов (Нижний Новгород)

Введение

В данной работе рассматривается скорость сходимости ветвящихся цепных дробей с натуральными элементами. В работе [2] показано, что любая такая дробь сходится, также показано как организовать сходимость к любому алгебраическому числу. Но в работе [2] не рассматривается вопрос о скорости сходимости. Хотя многие вопросы о скорости сходимости ветвящихся цепных дробей решены в [1], данная работа имеет смысл, так как рассматривается скорость сходимости частного случая ветвящихся цепных дробей. То есть возможно получение оценок лучших чем в [1].

Пусть дана система уравнений:

$$\begin{cases} T^{(1)} = \dfrac{a^{(1)}}{c_0^{(1)} + \sum\limits_{i=1}^{d} c_i^{(1)} T^{(i)}} \\ \dots \\ T^{(d)} = \dfrac{a^{(d)}}{c_0^{(d)} + \sum\limits_{i=1}^{d} c_i^{(d)} T^{(i)}} \end{cases} \tag{1}$$

$$\text{где } d \in \mathbb{N},\ a^{(k)} \in \mathbb{N},\ c_0^{(k)} \in \mathbb{N},\ c_i^{(k)} \in \mathbb{Z}_+ \text{ для } j,\ k \in \overline{1,\ d}. \tag{2}$$

В [2] показано, что (1) при условиях (2) имеет единственное решение.

Определение ([2]). Каждое $T^{(k)}$ называется *периодической ветвящейся цепной дробью с натуральными элементами и степенью ветвления* d .

Далее вместо слов *периодическая ветвящаяся цепная дробь с натуральными элементами* будем использовать сокращение ПВЦД.

Рассмотрим рекуррентную формулу:

$$T_n^{(k)} = \frac{a^{(k)}}{c_0^{(k)} + \sum\limits_{i=1}^{d} c_i^{(k)} T_{n-1}^{(i)}}, \quad \text{где } T_1^{(k)} = \frac{a^{(k)}}{c_0^{(k)}}. \tag{3}$$

Определение ([2]). $T_n^{(k)}$ является *n-ой подходящей* ПВЦД *для* $T^{(k)}$.

В [2] показано, что $T_n^{(k)}$ является частным случаем определения подходящей дроби для ветвящейся дроби из [1], а также, что $\lim\limits_{n\to\infty} T_n^{(k)} = T^{(k)}$.

Также рассмотрим $Q_n^{(k)} = \dfrac{a^{(k)}}{T_n^{(k)}}$. Очевидно $\{Q_n^{(k)}\}$ сходится.

$$Q_n^{(k)} = c_0^{(k)} + \sum_{i=1}^{d} \frac{c_i^{(k)} a^{(i)}}{Q_{n-1}^{(i)}}, \quad \text{Где } Q_1^{(k)} = \frac{a^{(k)}}{T_1^{(k)}} = c_0^{(k)}. \tag{4}$$

Результаты работы

Теорема 1. *Пусть* $m > n$. *Тогда*

$$T_m^{(i_0)} - T_n^{(i_0)} = (-1)^n \frac{a^{(i_0)}}{Q_m^{(i_0)} Q_n^{(i_0)}} \sum_{(i_1,\, i_2,\, \ldots,\, i_n)=\bar{1}}^{(i_1,\, i_2,\, \ldots,\, i_n)=\bar{d}} \frac{c_{i_n}^{(i_{n-1})} a^{(i_n)}}{Q_{m-n}^{(i_n)}} \prod_{s=1}^{n-1} \frac{c_{i_s}^{(i_{s-1})} a^{(i_s)}}{Q_{m-s}^{(i_s)} Q_{n-s}^{(i_s)}} = \tag{5}$$

$$= (-1)^n \frac{a^{(i_0)}}{Q_m^{(i_0)} Q_m^{(i_0)}} \sum_{(i_1,\, i_2,\, \ldots,\, i_n)=\bar{1}}^{(i_1,\, i_2,\, \ldots,\, i_n)=\bar{d}} \frac{\prod\limits_{s=1}^{n} c_{i_s}^{(i_{s-1})} a^{(i_s)}}{\prod\limits_{s=1}^{n} Q_{m-s}^{(i_s)} \prod\limits_{s=1}^{n-1} Q_{n-s}^{(i_s)}} = \tag{6}$$

$$= (-1)^n \frac{a^{(i_0)}}{Q_m^{(i_0)} Q_n^{(i_0)}} \sum_{i_1=1}^{d} \frac{c_{i_1}^{(i_0)} a^{(i_1)}}{Q_{m-1}^{(i_1)} Q_{n-1}^{(i_1)}} \left(\sum_{i_2=1}^{d} \frac{c_{i_2}^{(i_1)} a^{(i_2)}}{Q_{m-2}^{(i_2)} Q_{n-2}^{(i_2)}} \cdots \right.$$

$$\left. \cdots \left(\sum_{i_{n-1}=1}^{d} \frac{c_{i_{n-1}}^{(i_{n-2})} a^{(i_{n-1})}}{Q_{m-n+1}^{(i_{n-1})} Q_1^{(i_{n-1})}} \left(\sum_{i_n=1}^{d} \frac{c_{i_n}^{(i_{n-1})} a^{(i_n)}}{Q_{m-n}^{(i_n)}} \right) \right) \right). \tag{7}$$

Доказательство. Доказательство (6) копирует доказательство более общей формулы в [1], но мы проведем его заново, чтобы не было путаницы с различными системами обозначений. Равенство (7) является следствием (6) и не является частным случаем общей формулы из [1].

$$Q_m^{(i_0)} - Q_n^{(i_0)} = \sum_{i=1}^{d} \frac{c_i^{(i_0)} a^{(i)}}{Q_{m-1}^{(i)}} - \sum_{i=1}^{d} \frac{c_i^{(i_0)} a^{(i)}}{Q_{n-1}^{(i)}} = (-1) \sum_{i_1=1}^{d} \frac{c_{i_1}^{(i_0)} a^{(i_1)} (Q_{m-1}^{(i_1)} - Q_{n-1}^{(i_1)})}{Q_{m-1}^{(i_1)} Q_{n-1}^{(i_1)}} =$$

$$= (-1)^2 \sum_{i_1=1}^{d} \sum_{i_2=1}^{d} \frac{c_{i_1}^{(i_0)} c_{i_2}^{(i_1)} a^{(i_1)} a^{(i_2)} (Q_{m-2}^{(i_2)} - Q_{n-2}^{(i_2)})}{Q_{m-1}^{(i_1)} Q_{m-2}^{(i_2)} Q_{n-1}^{(i_1)} Q_{n-2}^{(i_2)}}, \text{ при } n > 2.$$

Используя $Q_m^{(k)} - Q_1^{(k)} = \sum\limits_{i=1}^{d} \dfrac{c_i^{(k)} a^{(i)}}{Q_{m-1}^{(i)}}$, раскрываем рекуррентность выше:

$$Q_m^{(i_0)} - Q_n^{(i_0)} = (-1)^{n-1} \sum_{(i_1, i_2, \ldots, i_{n-1}) = \bar{1}}^{(i_1, i_2, \ldots, i_{n-1}) = \bar{d}} \prod_{s=1}^{n-1} \frac{c_{i_s}^{(i_{s-1})} a^{(i_s)} (Q_{m-n+1}^{(i_s)} - Q_1^{(i_s)})}{Q_{m-s}^{(i_s)} Q_{n-s}^{(i_s)}} =$$

$$= (-1)^{n-1} \sum_{(i_1, i_2, \ldots, i_{n-1}) = \bar{1}}^{(i_1, i_2, \ldots, i_{n-1}) = \bar{d}} \frac{c_{i_n}^{(i_{n-1})} a^{(i_n)}}{Q_{m-n}^{(i_n)}} \prod_{s=1}^{n-1} \frac{c_{i_s}^{(i_{s-1})} a^{(i_s)}}{Q_{m-s}^{(i_s)} Q_{n-s}^{(i_s)}} =$$

$$= (-1)^{n-1} \sum_{(i_1, i_2, \ldots, i_n) = \bar{1}}^{(i_1, i_2, \ldots, i_n) = \bar{d}} \frac{\prod_{s=1}^{n} c_{i_s}^{(i_{s-1})} a^{(i_s)}}{\prod_{s=1}^{n} Q_{m-s}^{(i_s)} \prod_{s=1}^{n-1} Q_{n-s}^{(i_s)}}.$$

Теперь будем выносить по одному множителю за знак одной из сумм, так чтобы зависимые части оказались в глубине формулы. Рассматриваемое выражение равно:

$$(-1)^{n-1} \sum_{(i_1, i_2, \ldots, i_{n-1}) = \bar{1}}^{(i_1, i_2, \ldots, i_{n-1}) = \bar{d}} \prod_{s=1}^{n-1} \frac{c_{i_s}^{(i_{s-1})} a^{(i_s)}}{Q_{m-s}^{(i_s)} Q_{n-s}^{(i_s)}} \left(\sum_{i_n=1}^{d} \frac{c_{i_n}^{(i_{n-1})} a^{(i_n)}}{Q_{m-n}^{(i_n)}} \right) =$$

$$= (-1)^{n-1} \sum_{i_1=1}^{d} \frac{c_{i_1}^{(i_0)} a^{(i_1)}}{Q_{m-1}^{(i_1)} Q_{n-1}^{(i_1)}} \left(\sum_{i_2=1}^{d} \frac{c_{i_2}^{(i_1)} a^{(i_2)}}{Q_{m-2}^{(i_2)} Q_{n-2}^{(i_2)}} \cdots \right.$$

$$\left. \cdots \left(\sum_{i_{n-1}=1}^{d} \frac{c_{i_{n-1}}^{(i_{n-2})} a^{(i_{n-1})}}{Q_{m-n+1}^{(i_{n-1})} Q_1^{(i_{n-1})}} \left(\sum_{i_n=1}^{d} \frac{c_{i_n}^{(i_{n-1})} a^{(i_n)}}{Q_{m-n}^{(i_n)}} \right) \right) \right).$$

Так как $T_m^{(i_0)} - T_n^{(i_0)} = (-1) \dfrac{a^{(i_0)} (Q_m^{(i_0)} - Q_n^{(i_0)})}{Q_m^{(i_0)} Q_n^{(i_0)}}$, получаем искомые формулы.

Будем обозначать $\beta^{(k)} = \sum\limits_{i=1}^{d} c_i^{(k)} a^{(i)}$, $\beta^{(max)} = \max\{b^{(k)}\}$, $\beta^{(min)} = \min\{b^{(k)}\}$, $\Delta_\beta = \beta^{(max)} - \beta^{(min)}$.

Теорема 2. *При $n > n_0$ имеет место*

$$|T_{n+1}^{(k)} - T_n^{(k)}| \leqslant C_1((\beta^{(max)} + (\Delta_\beta - 1)^2 \frac{1 + \sqrt{1 + 4\frac{\beta^{(max)}}{(\Delta_\beta - 1)^2}}}{2})^{-1} \beta^{(max)})^{n-1}.$$

Доказательство. Если $T^{(k)} = \dfrac{a^{(k)}}{c_0^{(k)} + \sum\limits_{i=1}^{d} c_i^{(k)} T^{(i)}}$, то рассмотрим ПВЦД $\hat{T}^{(k)} = \dfrac{a^{(k)}}{1 + \sum_{i=1}^{d} c_i^{(k)} \hat{T}^{(i)}}$, полученную из $T^{(k)}$ заменой $c_0^{(k)} = 1$.

Нетрудно видеть, что верна следующая

Лемма 1. $T_{n+1}^{(k)} - T_n^{(k)} \leqslant \hat{T}_{n+1}^{(k)} - \hat{T}_n^{(k)}$.

В связи с леммой 1, далее будем рассматривать ПВЦД, у которых $c_0^{(k)} = 1$ для всех $k \in \overline{1, d}$. Тогда $Q_n^{(k)} = 1 + \sum\limits_{i=1}^{d} \dfrac{c_i^{(k)} a^{(i)}}{Q_{n-1}^{(i)}}$.

Лемма 2.

$$\eta^{(min)} \leqslant Q_n^{(k)} \leqslant \eta^{(max)}, \text{ где } \eta^{(min)} = \frac{-(\Delta_\beta - 1) + \sqrt{(\Delta_\beta - 1)^2 + 4\beta^{(max)}}}{2},$$

$$\eta^{(max)} = \frac{(\Delta_\beta + 1) + \sqrt{(\Delta_\beta + 1)^2 + \beta^{(min)}}}{2}.$$

Доказательство. Рассмотрим:

$$\eta_n^{(min)} = 1 + \frac{\beta^{(min)}}{\eta_{n-1}^{(max)}}, \quad \eta_n^{(max)} = 1 + \frac{\beta^{(max)}}{\eta_{n-1}^{(min)}}, \text{ где } \eta_1^{(min)} = \eta_1^{(max)} = 1.$$

Докажем по индукции, что

$$\eta_n^{(min)} \leqslant Q_n^{(k)} \leqslant \eta_n^{(max)}. \tag{8}$$

Основание индукции очевидно. Индуктивный переход:

$$\eta_n^{(min)} = 1 + \frac{\beta^{(min)}}{\eta_{n-1}^{(max)}} \leqslant 1 + \sum_{i=1}^{d} \frac{c_i^{(k)} a^{(i)}}{\eta_{n-1}^{(max)}} \leqslant Q_n^{(k)} = 1 + \sum_{i=1}^{d} \frac{c_i^{(k)} a^{(i)}}{Q_{n-1}^{(i)}} \leqslant$$

$$\leqslant 1 + \sum_{i=1}^{d} \frac{c_i^{(k)} a^{(i)}}{\eta_{n-1}^{(min)}} \leqslant 1 + \frac{\beta^{(max)}}{\eta_{n-1}^{(min)}} = \eta_n^{(max)}.$$

Теперь покажем, что $|\eta_n^{(min)}| \leqslant +\infty$ и $|\eta_n^{(max)}| \leqslant +\infty$.

Рассмотрим систему:

$$\begin{cases} \eta^{(min)} - 1 = \dfrac{\beta^{(min)}}{1 + (\eta^{(max)} - 1)} \\ \eta^{(max)} - 1 = \dfrac{\beta^{(max)}}{1 + (\eta^{(min)} - 1)} \end{cases} \tag{9}$$

Данная система является частным случаем (1) с условиями (2), а значит по [2] имеет единственное решение. Пусть $\eta_n^{(min)}$ и $\eta_n^{(max)}$ — подходящие дроби для (9).

Таким образом, имеем: $\lim\limits_{n\to\infty} \eta_n^{(min)} = \eta^{(min)}$, $\lim\limits_{n\to\infty} \eta_n^{(max)} = \eta^{(max)}$.

Используя (8), получаем: $\eta^{(min)} \leqslant Q_n^{(k)} \leqslant \eta^{(max)}$.

Первая часть леммы 2 доказана. Теперь найдем значения $\eta^{(min)}$ и $\eta^{(max)}$. Из (9) получаем, что

$$\eta^{(max)} - \eta^{(min)} = \Delta_\beta \tag{10}$$

Подстановкой в (9) получаем уравнение:

$$\eta^{(min)^2} + (\Delta_\beta - 1)\eta^{(min)} - \beta^{(max)} = 0\,, \quad D = (\Delta_\beta - 1)^2 + 4\beta^{(max)} \geqslant 0,$$

из которого с учетом $\eta^{(min)} \geqslant 0$ выражается $\eta^{(min)}$. Далее $\eta^{(max)} = \Delta_\beta - \eta^{(min)}$, что доказывает лемму (2).

Лемма 3. $\beta^{(max)} + (\Delta_\beta - 1)^2\eta^{(min)} \leqslant Q_{n+1}^{(k)}Q_n^{(k)} \leqslant \beta^{(min)} + (\Delta_\beta + 1)^2\eta^{(max)}$.

Доказательство. Имеет место $\eta_{n+1}^{(min)}\eta_n^{(min)} \leqslant Q_{n+1}^{(k)}Q_n^{(k)} \leqslant \eta_{n+1}^{(max)}\eta_n^{(max)}$. Используя (10), получаем:

$$\eta_{n+1}^{(max)}\eta_n^{(min)} - \Delta_\beta\eta_n^{(min)} \leqslant Q_{n+1}^{(k)}Q_n^{(k)} \leqslant \eta_{n+1}^{(min)}\eta_n^{(max)} + \Delta_\beta\eta_n^{(max)}.$$

Но $\eta_{n+1}^{(max)}\eta_n^{(min)} = (1 + \dfrac{\beta^{(max)}}{\eta_n^{(min)}})\eta_n^{(min)} = \eta_n^{(min)} + \beta^{(max)}$

и $\eta_{n+1}^{(min)}\eta_n^{(max)} = (1 + \dfrac{\beta^{(min)}}{\eta_n^{(max)}})\eta_n^{(max)} = \eta_n^{(max)} + \beta^{(min)}$.

Отсюда получаем:

$$\beta^{(max)} + (\Delta_\beta - 1)^2\eta_n^{(min)} \leqslant Q_{n+1}^{(k)}Q_n^{(k)} \leqslant \beta^{(min)} + (\Delta_\beta + 1)^2\eta_n^{(max)}.$$

Приняв во внимание лемму 3, воспользуемся формулой (7). Обозначим левую часть неравенства леммы 3 за A. В (7) будем оценивать $Q_{n+1}^{(k)}Q_n^{(k)}$ значениями A, а одиночные вхождения $Q_n^{(k)}$ значениями $\eta^{(min)}$. После каждой

оценки знаменателя, просуммируем числитель, получив значение некоторого $\beta^{(k)}$. Оценим $\beta^{(k)}$ как $\beta^{(max)}$.

Итого имеем:

$$|T_{n+1}^{(i_0)} - T_n^{(i_0)}| \leqslant \frac{a^{(i_0)}{\beta^{(max)}}^n}{A^{n-1}{\eta^{(min)}}^3}.$$

Подставляя значения A и $\eta^{(min)}$, получаем утверждение теоремы 2.

Следствие. *Оценка теоремы 2 достижима, если выбрать коэффициенты так, чтобы* $\Delta_\beta = 0$.

Приведем пример, на котором оценка достигается:

$$\begin{cases} T^{(1)} = \dfrac{2}{1 + 3T^{(1)} + T^{(2)}} \\ T^{(2)} = \dfrac{4}{1 + T^{(1)} + 2T^{(2)}} \end{cases}.$$

Автор благодарит В. Н. Шевченко и В. А. Калягина за неоценимую помощь в написании работы.

Список литературы

1. Скоробогатько В. Я. Теория ветвящихся цепных дробей и её применение в вычислительной математике. — М.: Наука, 1983.
2. Закиров Н. Р. О представлении произвольного алгебраического числа периодической ветвящейся цепной дробью // Математические вопросы кибернетики. — 2006. — Вып. 15. — С. 65–78.
3. Марченков С. С. Конечные автоматы и периодические разложения действительных чисел // Математические вопросы кибернетики. — 1999. — Вып. 8. — С. 304–311.

ПЕРЕХОДНЫЕ ЯВЛЕНИЯ В СТОХАСТИЧЕСКИХ КС-ЯЗЫКАХ С ОДНИМ НЕТЕРМИНАЛЬНЫМ СИМВОЛОМ

О. В. Дурандин (Нижний Новгород)

Введение

Рассматриваются переходные явления для стохастических КС-грамматик с одним нетерминальным символом. Переходные явления возникают в случае, когда перронов корень r матрицы первых моментов грамматики близок к 1.

Для рассматриваемого случая исследуются свойства деревьев вывода высоты, большей t, при $t \to \infty$. Для таких деревьев найдена асимптотика математического ожидания числа вершин, помеченных нетерминалами, на ярусе t, дисперсии числа нетерминальных символов на ярусе t и вероятности продолжения. Выявлены особенности в свойствах деревьев вывода при переходе от докритического ($r < 1$) к критическому случаю ($r = 1$).

1. Основные определения и понятия

Определение. *Стохастической* КС-*грамматикой* называется система $G =< V_N, V_T, R, S >$, где V_N — конечное множество нетерминальных символов (нетерминалов); V_T — конечное множество терминальных символов (терминалов); S — аксиома грамматики, $S \in V_N$; R — конечное множество правил, представимое в следующем виде : $R = \cup_{i=1}^{k} R_i$, где k — мощность V_N и $R_i = \{r_{i1}, \ldots, r_{i,n_i}\}$. Каждое правило r_{ij} имеет следующий вид:

$$r_{ij} : A_i \xrightarrow{p_{ij}} \beta_{ij}, \qquad j = 1, \ldots, n_i$$

где $A_i \in V_N$, $\beta_{ij} \in (V_N \cup V_T)^*$ и p_{ij} — вероятность применения правила r_{ij} (вероятность правила), причём $0 < p_{ij} \leqslant 1$, $\sum\limits_{j=1}^{n_i} p_{ij} = 1$.

Для $\alpha, \gamma \in (V_N \cup V_T)^*$ будем говорить, что γ непосредственно выводимо из α (обозначать $\alpha \Rightarrow \gamma$), если существуют $\alpha_1, \alpha_2 \in (V_N \cup V_T)^*$, для которых $\alpha = \alpha_1 A_i \alpha_2$, $\gamma = \alpha_1 \beta_{ij} \alpha_2$ и в грамматике имеется правило $A_i \xrightarrow{p_{ij}} \beta_{ij}$.

Через $\Rightarrow_*$ обозначим рефлексивное транзитивное замыкание отношения $\Rightarrow$. Множество слов $L_G = \{\alpha : S \Rightarrow_* \alpha, \alpha \in V_T^*\}$ образует КС-язык, порожденный грамматикой G. Каждому слову α КС-языка соответствует последовательность правил грамматики (вывод), с помощью которой α выводится из аксиомы S.

Левым выводом слова α называется вывод, при котором каждое правило в процессе вывода слова α из аксиомы S применяется к самому левому нетерминальному символу в слове. Последовательность правил в левом выводе обозначим как $\omega(\alpha)$.

Для вывода существует полезное представление в виде дерева вывода. Процедуру построения дерева можно описать следующим образом.

Корень дерева вывода помечается аксиомой S. Пусть при выводе слова α на очередном шаге построения в процессе левого вывода применяется правило $A \to b_{i1} b_{i2} \ldots b_{im}$, где $b_{il} \in V_N \cup V_T (l = 1, \ldots, m)$. Тогда из самой левой вершины-листа дерева, помеченной символом A (при обходе листьев дерева слева направо), проводится m дуг в вершины следующего яруса, которые помечаются слева направо символами $b_{i1} b_{i2} \ldots b_{im}$ соответственно. После построения дуг и вершин для всех правил грамматики в выводе слова языка листья дерева помечаются терминальными символами и само слово получается при обходе листьев дерева слева направо.

Ярусы дерева нумеруются следующим образом. Корень дерева располагается на нулевом ярусе. Вершины дерева, смежные с корнем, образуют первый ярус и т.д. Таким образом, дуги, выходящие из вершин j-го яруса, ведут к вершинам $(j+1)$-го яруса. *Высотой дерева* называется максимальная длина пути от корня к листу, или номер последнего яруса.

Пусть $\alpha \in L_G, \omega = r_{i_1 j_1} r_{i_2 j_2} \dots r_{i_n j_n}$ — некоторый вывод слова $\alpha \in L_G$, а d — соответствующее этому слову дерево вывода. Вероятность дерева вывода d определим, как $p(d) = p_{i_1 j_1} p_{i_2 j_2} \dots p_{i_n j_n}$. Будем обозначать $D(L_G)$ множество всех деревьев вывода для слов из L_G. Стохастическая КС-грамматика называется согласованной, если $\sum\limits_{d \in D(L_G)} p(d) = 1$.

В работе рассматриваются согласованные стохастические КС-грамматики с одним нетерминалом.

Введем понятие производящей функции. Для грамматики с одним нетерминалом производящая функция $F(s)$ строится по множеству правил R. При рассмотрении грамматик с одним нетерминалом, правила грамматики можно записать в виде: $S \xrightarrow{p_j} \beta_j$. Для каждого правила $S \xrightarrow{p_j} \beta_j$ (где $S \in V_N, \beta_j \in (V_N \cup V_T)^*$ и $\sum\limits_{j=0}^{n} p_j = 1$) выписываются слагаемые $p_j s^l$, где l — число вхождений нетерминального символа S в правую часть правила. Тогда $F(s) = \sum\limits_{j=1}^{n} p_j s^l$.

Примем, что $F(1; s) = F(s)$, тогда $F(t; s)$ определяется следующим образом: $F(t+1; s) = F(t; F(s))$.

Первым факториальным моментом назовем величину $A(t) = \frac{\partial F(t;s)}{\partial s}|_{s=1}$. Примем обозначение $r = A(1)$. Для случая одного нетерминала величина A является перроновым корнем матрицы первых моментов [2].

Положим $B = \frac{\partial^2 F(s)}{\partial s^2}|_{s=1}$.

Процесс порождения слов стохастического КС-языка можно описать как ветвящийся процесс [3].

Для стохастических КС-грамматик известна следующая классификация (в зависимости от значения величины r):

- *докритический случай*, если $r < 1$;
- *критический случай*, если $r = 1$.

2. Переходные явления

Переходными называются явления, возникающие при $r < 1, r \to 1, t \to \infty$, т. е. асимптотические свойства процессов, близких к критическим.

Пусть $\mu(t)$ — число вершин в дереве вывода на ярусе t, помеченных нетерминалами.

Утверждение 1. *Математическое ожидание числа нетерминалов* $\mu(t)$ *определяется формулой* $M\mu(t) = A(t) = r^t$.

Это утверждение получается интерпретацией результатов из [1]. Поскольку, в данном случае рассматриваются все деревья вывода, в том числе и те, высота которых не превосходит t, полезно рассмотреть *условное математическое ожидание* для деревьев вывода, высота которых больше t.

Обозначим $Q(t)$ вероятность того, что дерево вывода имеет высоту большую, чем t. Назовем эту величину *вероятностью продолжения.*

Утверждение [1]. *Асимптотика вероятности продолжения при* $t \to \infty$ *определяется формулой:*

$$Q(t) \sim \begin{cases} \frac{r^t}{1+\frac{B}{2}\frac{r^t-1}{r-1}}, & \text{при } r < 1 \text{ (докритический случай);} \\ \frac{1}{1+\frac{Bt}{2}}, & \text{при } r = 1 \text{ (критический случай).} \end{cases}$$

Утверждение 2. *Условное математическое ожидание числа нетерминалов на ярусе* t *в дереве вывода при* $t \to \infty$

$$\{M\mu(t) \mid Q(t) > 0\} \sim \begin{cases} 1 + \frac{B}{2}\frac{r^t-1}{r-1}, & \text{при } r < 1; \\ 1 + \frac{Bt}{2}, & \text{при } r = 1. \end{cases}$$

Утверждение 3. *Условное математическое ожидание числа нетерминалов на ярусе* t *в дереве вывода, при условиях* $r < 1, r \to 1, t \to \infty$

$$\{M\mu(t) \mid Q(t) > 0\} = \frac{M\mu(t)}{Q(t)} \sim 1 + \frac{B}{2}\sum_{i=0}^{t-1} r^i.$$

Для переходных явлений можно получить более точные асимптотические оценки. Обозначим $r = 1 - \varepsilon$. Имеет место следующее утверждение:

Утверждение 4. *Условное математическое ожидание числа нетерминалов на ярусе* t *в дереве вывода, при условиях* $\varepsilon > 0, \varepsilon \to 0, t \to \infty$

$$\{M\mu(t) \mid Q(t) > 0\} = \frac{M\mu(t)}{Q(t)} \sim 1 + \frac{B}{2\varepsilon}.$$

Следующее утверждение устанавливает верхнюю оценку величины B, вне зависимости от вероятностей правил грамматики.

Утверждение 5. $B < l_{max}^2$, *где* l_{max} — *максимальное число нетерминалов в правых частях правил.*

Из утверждений 4 и 5 видно, что $\{M\mu(t) \mid Q(t) > 0\} = 1 + \frac{B}{2\varepsilon} \to \infty$ и можно сделать вывод, что число нетерминалов на ярусе t (при $t \to \infty$) ограничено константой, которая неограниченно растет при $\varepsilon \to 0$.

Дисперсия числа нетерминальных символов на ярусе t характеризует «ветвистость» дерева, и определяется правилами грамматики, в правой части которых содержится более одного нетерминала. Из [1] известна асимптотика для дисперсии на ярусе t (при $t \to \infty$):

$$D\mu(t) = \begin{cases} \frac{B+r-r^2}{r(r-1)} r^t, & \text{если } r < 1; \\ Bt, & \text{если } r = 1. \end{cases}$$

Исключая деревья вывода высоты не превосходящей t, можно получить *условную дисперсию* для числа нетерминалов в дереве вывода.

Утверждение 6. *Условная дисперсия числа нетерминальных символов в дереве вывода на ярусе t, при условиях $t \to \infty, \varepsilon > 0, \varepsilon \to 0$*

$$\{D\mu(t) \mid Q(t) > 0\} = \frac{D\mu(t)}{Q(t)} \sim \frac{B^2}{\varepsilon^2}.$$

Итак, условная дисперсия для деревьев вывода высоты большей чем t при переходном явлении ограничена константой, стремящейся к бесконечности при $\varepsilon \to 0$.

Рассмотрим соотношение вероятностей правил при переходных явлениях. Правило КС-грамматики называется заключительным, если в его правой части отсутствуют нетерминальные символы.

Пусть P_0 — множество заключительных правил, а P_1 — множество незаключительных правил вывода. Из условия согласованности КС-грамматики следует, что $\sum\limits_{j=1}^{n} p_j = \sum\limits_{P_1} p_j + \sum\limits_{P_0} p_j = 1$.

Утверждение 7. *При возникновении переходных явлений выполняется соотношение $\sum\limits_{j \in P_1} p_j(l_j - 1) \to \sum\limits_{j \in P_0} p_j$ для вероятностей правил грамматики (здесь l_j — число нетерминалов в правой части j-го правила).*

3. Переходные явления в языках Дика с произвольным числом скобок

Проиллюстрируем полученные результаты на примере языка Дика.

Языком Дика (Dyck language) над $2n$ буквами называется КС-язык над алфавитом $\{a_1, b_1, a_2, b_2, \ldots, a_n, b_n\}$, порождаемый грамматикой со следующим

множеством правил:

$$\begin{cases} S \xrightarrow{p_0} \lambda, \\ S \xrightarrow{p_1} a_1 S b_1 S, \\ S \xrightarrow{p_2} a_2 S b_2 S, \\ \dots \\ S \xrightarrow{p_n} a_n S b_n S, \end{cases}$$

при условии $\sum\limits_{i=0}^{n} p_i = 1$.

Словами языка являются последовательности правильно вложенных скобок n типов (если считать символ a_i левой скобкой i типа, а b_i соответствующей правой скобкой). Производящая функция, соответствующая грамматике языка Дика, имеет вид $F(s) = (\sum\limits_{i=1}^{n} p_i)s^2 + p_0$. Отметим, что $r = 2(1 - p_0)$ и $B = 2(1 - p_0)$. Нетрудно заметить, что переходные явления в языках Дика возникают при $p_0 \to \frac{1}{2}$.

Асимптотика вероятности продолжения дерева вывода для слов языка Дика (с n типами скобок) на t ярусе:

$$Q(t) \sim \begin{cases} \frac{2p_0 - 1}{p_0}(2(1 - p_0))^t, & \text{при } p_0 \to \frac{1}{2}; \\ \frac{1}{1 + \frac{t}{2}}, & \text{при } p_0 = \frac{1}{2}. \end{cases}$$

Условное математическое ожидание для $\mu(t)$:

$$\{M\mu(t) \mid Q(t) > 0\} = \frac{M\mu(t)}{Q(t)} = 1 + (1 - p_0) \sum_{k=0}^{t-1} (2(1 - p_0))^k.$$

С ростом t число нетерминальных символов увеличивается, что обеспечивает сильное ветвление дерева вывода языка Дика.

Условная дисперсия обобщенных языков Дика:

$$\{D\mu(t) \mid Q(t) > 0\} = (1 + \frac{1}{1 - 2(1 - p_0)})(1 + (1 - p_0) \sum_{k=0}^{t-1} (2(1 - p_0))^k).$$

Таким образом, можно увидеть, что условная дисперсия при переходном явлении ($p_0 \to \frac{1}{2}$) стремится к бесконечности.

Список литературы

1. Севастьянов Б. А. Ветвящиеся процессы. — М.: Наука, 1971.
2. Жильцова Л. П. — Закономерности применения правил грамматики в выводах слов стохастического контекстно-свободного языка // Математические вопросы кибернетики. — 2000. — Вып. 9. — С. 101–126.
3. Фу К. Структурные методы в распознавании образов. — М.: Мир, 1977.

О k-ПОРОГОВЫХ ФУНКЦИЯХ

Е. М. Замараева (Нижний Новгород)

Введение

Функция f, отображающая множество $E_n^d = \{0, 1, \ldots, n-1\}^d, n \geqslant 2, d \geqslant 1$, в $\{0, 1\}$, называется *пороговой*, если существуют такие вещественные числа $a_0, a_1, \ldots, a_d$, что

$$M_1(f) = \big\{x \in E_n^d : f(x) = 1\big\} = \left\{x \in E_n^d : \sum_{j=1}^{d} a_j x_j \leqslant a_0\right\},$$

при этом неравенство $\sum\limits_{j=1}^{d} a_j x_j \leqslant a_0$ называется *пороговым*.

Функция f, отображающая множество $E_n^d = \{0, 1, \ldots, n-1\}^d, n \geqslant 2, d \geqslant 1$, в $\{0, 1\}$, называется *k-пороговой*, $k \geqslant 1$, если существуют такие вещественные числа $a_{10}, a_{11}, \ldots, a_{kd}$, что

$$M_1(f) = \left\{x \in E_n^d : \sum_{j=1}^{d} a_{ij} x_j \leqslant a_{i0} \text{ для } i = 1, \ldots, k\right\}, \tag{1}$$

при этом неравенства $\sum\limits_{j=1}^{d} a_{ij} x_j \leqslant a_{i0}$ для $i = 1, \ldots, k$ называются *пороговыми*. Если имеет место (1), то будем говорить, что k-пороговая функция *задана* этой системой линейных неравенств.

Обозначим через $\mathfrak{T}(n, d, k)$ — множество всех k-пороговых функций, заданных на множестве E_n^d.

Многие задачи, решаемые для пороговых функций, актуальны и для k-пороговых функций. К ним относится задача *расшифровки* функции, под которой понимается восстановление значений заранее не известной функции f из заданного класса C с помощью последовательных обращений к оракулу. *Оракул* — это процедура, возвращающая значение функции в заданной точке. *Оракульной сложностью* расшифровки в классе C называют минимальное количество обращений к оракулу, необходимое для восстановления любой функции из этого класса.

В рамках задачи расшифровки появляется интерес к изучению разрешающего множества функции. *Разрешающим множеством* функции f из заданного класса C называется множество точек T такое, что если для некоторой функции $g \in C, f(x) = g(x)$ для всех $x \in T$, то f и g тождественны. Разре-

шающее множество T называется *тупиковым*, если никакое его собственное подмножество не является разрешающим.

Точка x для некоторой функции f из класса C называется *существенной*, если существует некая функция $h \in C$, совпадающая с f на всей области определения за исключением точки $x : f(x) \neq h(x)$. Очевидно, что в любое разрешающее множество функции должны входить все ее существенные точки. Известно [1], что тупиковое разрешающее множество пороговой функции представлет собой множество всех ее существенных точек.

В работе предприняты первые шаги по характеризации разрешающего множества k-пороговых функций, приведены некоторые необходимые и достаточные условия для множества, чтобы быть разрешающим для заданной k-пороговой функции f, показана неединственность тупикового разрешающего множества для k-пороговой функции в общем случае.

1. Разрешающее множество k-пороговых функций

Для произвольной пороговой функции $f \in \mathfrak{T}(n, d)$ запишем систему неравенств относительно коэффициентов некоторого порогового неравенства $a_0, a_1, \ldots, a_d$, с помощью которого может быть задана f:

$$\begin{cases} \sum\limits_{j=1}^{d} a_j x_j \leqslant a_0 & \text{для всех } (x_1, \ldots, x_d) \in M_1(f), \\ \sum\limits_{j=1}^{d} a_j x_j > a_0 & \text{для всех } (x_1, \ldots, x_d) \in M_0(f). \end{cases} \tag{2}$$

Любой подсистеме, эквивалентной системе (2), соответствует разрешающее множество — множество точек, чьи координаты являются коэффициентами в неравенствах подсистемы. Показано, что минимальная подсистема, эквивалентная системе (2), никакая собственная подсистема которой не будет эквивалентна (2), единственна, отсюда следует единственность тупикового разрешающего множества для пороговых функций (см. [2]).

Система, аналогичная (2), для k-пороговой функции имеет более сложную структуру и состоит из неравенств и совокупностей неравенств:

$$\begin{cases} \sum\limits_{j=1}^{d} a_{ij} x_j \leqslant a_{i0} & \text{для всех } (x_1, \ldots, x_d) \in M_1(f), i = 1, \ldots, k, \\ \left[\begin{array}{l} \sum\limits_{j=1}^{d} a_{1j} x_j > a_{10} \\ \vdots \\ \sum\limits_{j=1}^{d} a_{kj} x_j > a_{k0} \end{array} \right. & \text{для всех } (x_1, \ldots, x_d) \in M_0(f). \end{cases} \tag{3}$$

Система (3) состоит из $k\,|M_1(f)|$ неравенств и $|M_0(f)|$ совокупностей из k неравенств.

Эта система эквивалентна совокупности из $|M_0(f)|^k$ систем неравенств. Для каждого элемента l из множества $\{1,\dots,k\}^{|M_0(f)|}$ совокупность будет содержать систему:

$$\begin{cases} \sum\limits_{j=1}^{d} a_{ij}x_j \leqslant a_{i0} & \text{для всех } (x_1,\dots,x_d) \in M_1(f), i = 1,\dots,k, \\ \sum\limits_{j=1}^{d} a_{l_{x^j}}x_j > a_{l_{x^0}} & \text{для всех } (x_1,\dots,x_d) \in M_0(f). \end{cases} \tag{4}$$

Полученная совокупность состоит из систем, часть из которых могут быть несовместны. Любое решение совместной системы (4) из совокупности будет давать коэффициенты для пороговых неравенств заданной функции.

Назовем неравенство из системы (4) 1-*неравенством*, если коэффициентами неравенства являются координаты точки, в которой функция принимает значение 1, и 0-*неравенством* в обратном случае. 0-неравенство, которое не выполняется для заданной функции, назовем *ложным*. Обозначим через $S(f)$ множество всех существенных точек k-пороговой функции f.

Выведем некоторые свойства разрешающего множества k-пороговой функции относительно совокупности систем (4).

Утверждение 1. *Для каждой совместной системы типа* (4) *точки, соответствующие* 1*-неравенствам из минимальной подсистемы, эквивалентной заданной системе, являются существенными.*

Доказательство. Рассмотрим точку $x \in E_n^d, f(x) = 1$, такую, что для некоторой системы (4) минимальная подсистема, эквивалентная системе, содержит 1-неравенство, соответствующее x. Так как 1-неравенство входит в минимальную подсистему, эквивалентную системе (4), значит найдется множество $\{a_{ij} : i = 1,\dots,k, j = 0,\dots,d\}$, такое, что выполняются все неравенства, соответствующие точкам из $E_n^d \setminus \{x\}$, и не выполняется хотя бы одно из неравенств, соответствующих точке x. Из этого следует, что $\{a_{ij}\}$ задает k-пороговую функцию g, различающуюся с f только в точке x, а значит x является существенной точкой.

Утверждение 2. *Для каждой совместной системы типа* (4) *существенными являются все точки* $x' \in M_0(f)$*, соответствующие* 0*-неравенствам из минимальной подсистемы, эквивалентной заданной системе, такие, что система следующего вида совместна*:

$$\begin{cases} \sum\limits_{j=1}^{d} a_{ij}x_j \leqslant a_{i0} & \textit{для всех } (x_1,\dots,x_d) \in M_1(f), i = 1,\dots,k, \\ \sum\limits_{j=1}^{d} a_{l_{x^j}}x_j > a_{l_{x^0}} & \textit{для всех } (x_1,\dots,x_d) \in M_0(f), \\ \sum\limits_{j=1}^{d} a_{ij}x'_j \leqslant a_{i0}, & i = 1,\dots,k, i \neq l_{x'}. \end{cases} \tag{5}$$

Доказательство. Так как 0-неравенство в системе, соответствующее x', входит в минимальную подсистему, эквивалентную заданной, и заданная система совместна, значит, совместна и система следующего вида:

$$\begin{cases} \sum\limits_{j=1}^{d} a_{ij}x_j \leqslant a_{i0} & \text{для всех } (x_1,\ldots,x_d) \in M_1(f), i = 1,\ldots,k, \\ \sum\limits_{j=1}^{d} a_{l_x j}x_j > a_{l_x 0} & \text{для всех } (x_1,\ldots,x_d) \in M_0(f) \setminus \{x'\}, \\ \sum\limits_{j=1}^{d} a_{l_{x'} j}x'_j \leqslant a_{l_{x'} 0} \end{cases} \tag{6}$$

Вместе совместность систем (5) и (6) ведут к совместности системы:

$$\begin{cases} \sum\limits_{j=1}^{d} a_{ij}x_j \leqslant a_{i0} & \text{для всех } (x_1,\ldots,x_d) \in M_1(f) \cup x', i = 1,\ldots,k, \\ \sum\limits_{j=1}^{d} a_{l_x j}x_j > a_{l_x 0} & \text{для всех } (x_1,\ldots,x_d) \in M_0(f) \setminus \{x'\}. \end{cases} \tag{7}$$

Совместность системы (7) приводит нас к тому, что существует k-пороговая функция g, различающаяся с f только в точке x', а это значит, что точка x' — существенная.

Утверждение 3. *Если некоторая система, образованная одним из возможных наборов неравенств, соответствующих точкам некоторого разрешающего множества T, не входит ни в одну совместную систему типа* (4), *то она несовместна.*

Доказательство. Рассмотрим некоторую систему, образованную одним из возможных наборов неравенств, соответствующих точкам разрешающего множества T. Пусть она совместна, тогда существует некоторая k-пороговая функция g, коэффициенты пороговых неравенств которой удовлетворяют всем неравенствам этой системы, и совпадающая с функцией f в точках разрешающего множества T. Но из того, что все возможные системы типа (4), включающие выбранную систему, несовместны, следует, что не найдется коэффициентов пороговых неравенств для f, удовлетворяющих этой системе. Следовательно $f \neq g$, и это противоречит тому, что их значения совпадают на разрешающем множестве T.

Утверждение 4. *Множество точек, содержащее все точки из утверждений 1, 2 и удовлетворяющее утверждению 3, является разрешающим.*

Замечание 1. В отличие от пороговых функций в общем случае тупиковое разрешающее множество k-пороговой функции не единственно и может не ограничиваться существенными точками.

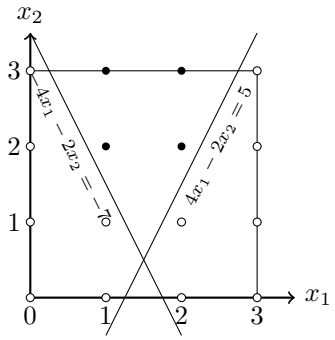
Пример. Рассмотрим 2-пороговую функцию из класса $\mathfrak{T}(4,2,2)$, принимающую значение 1 на множестве точек:

$$M_1(f) = \{(1,2),(1,3),(2,2),(2,3)\}.$$

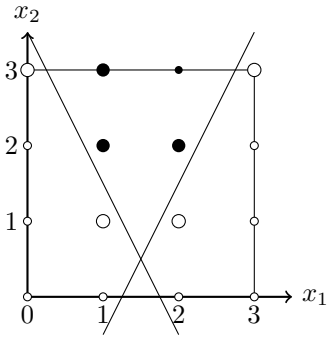
Эта функция может быть задана системой из 2 неравенств

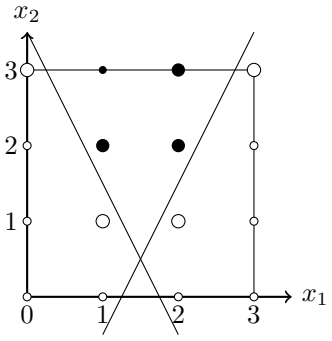
$$\begin{cases} -4x_1 - 2x_2 \leqslant -7, \\ 4x_1 - 2x_2 \leqslant 5, \end{cases}$$

и проиллюстрирована следующим образом:



Множество существенных точек $S(f) = \{(1,1),(1,2),(2,1),(2,2),(0,3),(3,3)\}$, при этом функция имеет 2 тупиковых разрешающих множества: $S(f) \cup \{(1,3)\}$ и $S(f) \cup \{(2,3)\}$. Ниже тупиковые разрешающие множества обведены большими кружками.





Список литературы

1. Anthony M., Brightwell G., Shawe-Taylor J. On specifying boolean functions by labelled examples // Discrete Applied Mathematics. — 1995. — V. 61, I. 1 — P. 1–25.

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

О РАДИУСЕ ПОКРЫТИЯ ЛИНЕЙНЫХ КОДОВ, ПОРОЖДЕННЫХ АФФИННЫМИ ГЕОМЕТРИЯМИ НАД ПОЛЕМ ПОРЯДКА 4

М. Э. Коваленко (Москва)

Введение и основные определения

Аффинная геометрия $\mathbb{EG}(n, p^s)$ — аффинное пространство $\mathbb{F}_{p^s}^n$, т. е. точки — это вектора из $\mathbb{F}_{p^s}^n$, прямые — это одномерные подпространства $\mathbb{F}_{p^s}^n$ и их смежные классы (по операции сложения векторов), d-мерные плоскости — d-мерные подпространства $\mathbb{F}_{p^s}^n$ и их смежные классы.

Определение. *Матрицей инцидентности* аффинной геометрии называется матрица M, строки и столбцы которой сопоставлены прямым и точкам аффинной геометрии соответственно, а элемент в пересечении строки b и столбца p равен 1, если точка лежит на соответствующей прямой, и 0 иначе.

Рассмотрим матрицу инцидентности $\mathbb{EG}(2, 4^h)$, а точнее строки этой матрицы как двоичные векторы. Тогда эти векторы порождают линейное подпространство $\mathbb{C}_h \subset \mathbb{F}_2^{4^h}$. По определению $\mathbb{C}_h$ является линейным кодом в пространстве размерности 4^h.

Назовем *расстоянием* между двумя векторами из $\mathbb{F}_2^{4^h}$ количество координат, в которых они отличаются. Тогда для каждого вектора пространства $\mathbb{F}_2^{4^h}$, не лежащего в $\mathbb{C}_h$, можно выбрать минимальное расстояние среди всех расстояний от него до каждого из векторов $\mathbb{C}_h$. Максимум из всех этих расстояний для векторов $\mathbb{F}_2^{4^h}$, не лежащих в $\mathbb{C}_h$, обозначим за $r(\mathbb{C}_h)$ и назовем *радиусом покрытия* линейного кода. А для векторов самого $\mathbb{C}_h$ выберем минимальное расстояние между двумя различными векторами и назовем его *кодовым расстоянием*. Более подробно с приведенными понятиями можно ознакомиться, например, в [1].

В рамках данной работы исследуется вопрос нахождения точного значения радиуса покрытия указанных кодов, а именно доказывается, что для любой размерности кода радиус покрытия кода равен 4.

Приведем некоторые свойства выбранных кодов, необходимые для дальнейшей работы.

Лемма 1. *В коде $\mathbb{C}_h$ нет векторов нечетного веса, более того, нет и векторов веса 2.*

Доказательство. Первая часть леммы очевидна поскольку, в силу строения порождающей матрицы, базис подпространства составляют вектора веса 4, пересекающиеся не более, чем по одному элементу. Докажем вторую часть.

Предположим, что в коде лежит вектор веса два, выбираем соответствующую пару точек из $\mathbb{F}_4^h$, а у этих двух точек координату, по которой они отличаются. Пусть это координата y_i и $y_{i,1} = \alpha$, а $y_{i,2} = \beta$, тогда красим гиперплоскость $\{y_i = \alpha\}$ в красный цвет, а $\{y_i = \beta\}$ — в синий. Из оставшихся двух гиперплоскостей еще одну красим в синий, и оставшуюся в красный. Итак, по фиксированной координате покрасили половину в красный, половину в синий цвет.

Любая прямая или целиком лежит в одной из этих полуплоскостей или же пересекает все 4, а, значит, содержит четное число точек каждого цвета. Таким образом, прибавление блоков не изменит четности количества точек каждого цвета, входящих в наш набор, т. е. не существует линейной комбинации прямых нашего $\mathbb{F}_4^h$, которая давала бы какую-либо пару точек.

Замечание. Поскольку в выбранном коде лежит нулевой вектор и не лежат вектора веса два, то кодовое расстояние данного кода равняется 4.

1. Совокупность всех подмножеств $\mathbb{F}_4^h$ как векторное пространство над $\mathbb{F}_2$

Рассмотрим совокупность всех подмножеств $\mathbb{F}_4^h$ как векторное пространство над $\mathbb{F}_2$ с операцией симметрической разности. Обозначим это векторное пространство за $\mathcal{A}(h)$, а за $x_i(a)$ i-ю координату элемента $a \in A \in \mathcal{A}(h)$ или, что то же самое, $a \in \mathbb{F}_4^h$.

Замечание. В пространстве $\mathcal{A}(h)$ выберем базис из одноточечных множеств e_j: $x_i(e_j) = \delta_{ij}$.

Здесь и далее подразумевается, что поле $\mathbb{F}_4$ реализовано в виде факторалгебры $\mathbb{F}_2[x]\Big/\{x^2 + x + 1\}$.

Далее выберем в $\mathcal{A}(h)$ все такие подмножества с четным числом элементов, что покоординатная сумма всех элементов каждого подмножества равна 0. Обозначим совокупность выбранных подмножеств

$$\mathcal{A}_0(h) = \{A \in \mathcal{A}(h) \mid \forall i \sum_{a \in A} x_i(a) = 0\}.$$

Под суммой здесь понимается сумма над $\mathbb{F}_4$.

Лемма 2. *Множество $\mathcal{A}_0(h)$ является подпространством $\mathcal{A}(h)$.*

Доказательство. Очевидно, что операция симметрической разности сохраняет четность количества точек во множестве. Далее рассмотрим $A_1 + A_2$, где $A_1, A_2 \in \mathcal{A}_0(h)$, тогда $\sum\limits_{a \in A_1 + A_2} x_i(a) = \sum\limits_{a \in A_1} x_i(a) + \sum\limits_{a \in A_2} x_i(a) = 0 + 0 = 0$, так как пространство над полем характеристики 2. Таким образом, симметрическая разность не выводит за подпространство.

Посчитаем размерность выбранного подпространства.

Лемма 3. *Для любого* $h \in \mathbb{N}$ *верно* $|\mathcal{A}_0(h)| = 2^{2^{2h}-2h}$.

Доказательство. Каждый из $a \in \mathbb{F}_4^h, a = (x_1 + Xy_1, \ldots, x_n + Xy_n)$ представим в виде $a = (x_1, y_1, \ldots, x_n, y_n)$, тогда всего множеств $A \subseteq \mathbb{F}_4^h$ будет ровно $2^{\left|\mathbb{F}_4^h\right|}$. Множеств, у которых $\sum\limits_{a \in A} x_1(a) = 0$ ровно половина (у второй половины сумма равна 1), т. е. $\frac{2^{\left|\mathbb{F}_4^h\right|}}{2}$. Далее — тех множеств, у которых одновременно $\sum\limits_{a \in A} x_1(a) = 0$ и $\sum\limits_{a \in A} y_1(a) = 0$, будет ровно $\frac{2^{\left|\mathbb{F}_4^h\right|}}{2^2}$. Поскольку все пары x_i, y_j линейно независимы, то, продолжая подобные рассуждения, получим, что $\#A = \frac{2^{\left|\mathbb{F}_4^h\right|}}{2^{2h}}$, а значит, $|\mathcal{A}_0(h)| = 2^{2^{2h}-2h}$.

Поскольку подпространство над полем характеристики 2, то можно посчитать размерность $|\mathcal{A}_0(h)|$.

Следствие 1. *Для любого* $h \in \mathbb{N}$ *верно* $\dim \mathcal{A}_0(h) = 2^{2h} - 2h$.

Теперь обозначим за $\mathcal{A}_0^4(h) = \{A \in \mathcal{A}(h), |A| = 4 \mid \forall i \sum\limits_{a \in A} x_i(a) = 0\}$ все подмножества из четырех элементов такие, что покоординатная сумма всех элементов подмножества равна 0, а за $\mathbb{B}_0(h)$ — все прямые. Заметим, что $<\mathbb{B}_0(h)>$ является подпространством $<\mathcal{A}_0^4(h)>$.

Лемма 4. *Для любого* $h \in \mathbb{N}$ *выполняется* $<\mathcal{A}_0^4(h)> = \mathcal{A}_0(h)$.

Доказательство. Построим выражение любого множества $\mathcal{A}_0(h)$ через множества $\mathcal{A}_0^4(h)$: рассмотрим элемент $A \in \mathcal{A}_0(h) : A \neq \varnothing, |A| \geqslant 4$, поскольку множества из двух элементов будут удовлетворять условию принадлежности $\mathcal{A}_0(h)$, только если состоят из двух одинаковых точек. Тогда выберем любые 3 точки $a, b, c \in A$ и рассмотрим $A' = A \triangle \{a, b, c, a + b + c\}$, где $x_i(a+b+c) = x_i(a)+x_i(b)+x_i(c)$, сумма над $\mathbb{F}_4$. Заметим, что A и A' выражаются множествами $\mathcal{A}_0^4(h)$ одновременно и при этом $|A'| < |A|$. Тогда получился спуск по весу, соответственно, продолжаем этот спуск к $A'', A''', \ldots, A^{(n)}, \ldots$ до тех пор, пока не станет $\left|A^{(n)}\right| \leqslant 4$.

Таким образом, в $\mathcal{A}_0^4(h)$ можно выбрать порождающую систему из $2^{2h} - 2h$ множеств.

Лемма 5. *Если одна четверка* $\mathcal{A}_0^4(h)\backslash\mathbb{B}_0(h)$ *порождается прямыми* $\mathbb{B}_0(h)$, *то все четверки* $\mathcal{A}_0^4(h)\backslash\mathbb{B}_0(h)$ *порождаются прямыми* $\mathbb{B}_0(h)$.

Замечание. Лемму также можно сформулировать следующим образом: или все четверки $\mathcal{A}_0^4(h)\setminus\mathbb{B}_0(h)$ порождаются прямыми $\mathbb{B}_0(h)$, или никакая четверка $\mathcal{A}_0^4(h)\backslash\mathbb{B}_0(h)$ не выражается через прямые $\mathbb{B}_0(h)$.

Доказательство. Пусть какое-либо множество A из $\mathcal{A}_0^4(h)\backslash\mathbb{B}_0(h)$ выражается через прямые $\mathbb{B}_0(h)$. Рассмотрим любую четверку $\mathcal{A}_0^4(h)\backslash\mathbb{B}_0(h)$ и три пары прямых, проходящие через пары точек выбранной четверки, в силу строения четверок среди этих пар прямых ни в одной паре нет пересечения. Выберем любые два направления из трех пар параллельных прямых, образующих A, и аффинными преобразованиями переведем эти направления в направления $x_1 = (1, 0, \ldots, 0)$ и $x_2 = (0, 1, 0, \ldots, 0)$. Таким образом, выбранная четверка перейдет во множество $\{(0, \ldots, 0), (0, 1, 0, \ldots, 0), (1, 0, 0, \ldots, 0), (1, 1, 0, \ldots)\}$. Поскольку любую четверку $\mathcal{A}_0^4(h)\backslash\mathbb{B}_0(h)$ можно эквивалентными аффинными преобразованиями перевести в четверку $\{(0, \ldots, 0), (0, 1, 0, \ldots, 0), (1, 0, 0, \ldots, 0), (1, 1, 0, \ldots)\}$, то из того, что какая-либо четверка $\mathcal{A}_0^4(h)\backslash\mathbb{B}_0(h)$ выражается через прямые $\mathbb{B}_0(h)$ следует, что любая другая четверка $\mathcal{A}_0^4(h)\backslash\mathbb{B}_0(h)$ выражается через прямые $\mathbb{B}_0(h)$.

Дальнейшей целью будет показать, что на расстоянии 0 до $\mathbb{B}_0(h)$ в $\mathbb{F}_4^h$ не могут лежать четверки $\mathcal{A}_0^4(h)\backslash\mathbb{B}_0(h)$. Для этого из лемм 4 и 5 можно сделать важное следствие:

Следствие 2. *В* $\mathcal{A}_0(h)$ *не существует базиса из прямых* $\mathbb{B}_0(h)$, *если и только если никакая четверка* $\mathcal{A}_0^4(h)\backslash\mathbb{B}_0(h)$ *не порождается блоками* $\mathbb{B}_0(h)$.

В [2] приводится точное значение размерности пространства $<\mathbb{B}_0(h)>$.

Теорема о базисе $\mathbb{B}_0(h)$ [2]. *В* $\mathbb{B}_0(h)$ *существует базис из* $2^{2h} - h^2 - h - 1$ *элементов, т. е. в* $\mathbb{F}_4^h$ *выполнено* $\dim <\mathbb{B}_0(h)> = 2^{2h} - h^2 - h - 1$.

Таким образом, любая достаточно большая система прямых $\mathbb{B}_0(h)$ линейно зависима в $\mathbb{F}_h^4$. Тогда по теореме о базисе $\mathbb{B}_0(h)$ и следствию 1 в $\mathcal{A}_0(h)$ не существует базиса из прямых $\mathbb{B}_0(h)$, тогда по следствию 2 никакая четверка $\mathcal{A}_0^4(h)\backslash\mathbb{B}_0(h)$ не выражается через прямые $\mathbb{B}_0(h)$. Следовательно, множества $\mathcal{A}_0^4(h)\backslash\mathbb{B}_0(h)$ не могут лежать на расстоянии 0 до $\mathbb{B}_0(h)$ в $\mathbb{F}^{4^h}$.

Более того, по лемме 1 множества $\mathcal{A}_0^4(h)\backslash\mathbb{B}_0(h)$ не могут лежать и на расстоянии 2 до $\mathbb{B}_0(h)$ в $\mathbb{F}^{4^h}$. Тогда любая четверка $\mathcal{A}_0^4(h)\backslash\mathbb{B}_0(h)$ обязана лежать на расстоянии 4. Непосредственной проверкой несложно убедиться, что никакие другие четверки не лежат на расстоянии, большем 2. Таким образом доказана теорема:

Теорема 1. *Для любого* h *для любого* $F \in \mathcal{A}_0^4(h)\setminus\mathbb{B}_0(h)$ *множество* F *лежит на расстоянии* 4 *до* $<\mathbb{B}_0(h)>$, *причем никакие другие четверки не лежат на расстоянии, большем* 2, *до* $<\mathbb{B}_0(h)>$.

2. Радиус покрытия $r(\mathbb{C}_h)$, где $\mathbb{C}_h$ — код, порожденный $\mathbb{EG}(2, 4^h)$

Итак, в предыдущем разделе было фактически показано, что для вектора из $\mathbb{F}_2^{4^h}$, соответствующего четверке $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$, с ростом h сохраняется расстояние от него до кода.

Теперь докажем лемму, необходимую для указания верхней оценки на радиус покрытия кода.

Лемма 6. *Если в $\mathbb{F}_4^h$ множество из R точек лежит на расстоянии R от $<\mathbb{B}_0(h)>$, то любое его S-элементное подмножество лежит на расстоянии S от $<\mathbb{B}_0(h)>$.*

Доказательство. Очевидно, что расстояние, большее чем S, ни для какого S-элементного подмножества достигаться не может. Предположим, для какого-то S-элементного подмножества можно построить линейную комбинацию блоков, такую что на ней достигается расстояние, меньшее S. Тогда дополнение этого подмножества из $R - S$ элементов в любом случае лежит от $< \mathbb{B}_0(h) >$ на расстоянии не большем, чем $R - S$. Но тогда для всего R-элементного множества есть линейная комбинация, на которой достигается расстояние, меньшее R. Противоречие.

Теорема 2. *Для любого R-элементного подмножества, $R > 4$, в $\mathbb{F}_4^h$ его расстояние до $<\mathbb{B}_0(h)>$ не превосходит 4.*

Доказательство. Поскольку $R > 4$, то в R есть как минимум 5 точек $\{a, b, c, d_1, d_2\}$. Из теоремы 1 известно, что на расстоянии 4 от $<\mathbb{B}_0(h)>$ могут лежать только четверки $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$, а, значит, $a+b+c+d_1 = a+b+c+d_2 = 0$. Следовательно, $d_1 = d_2$. Противоречие.

Переформулируя эту теорему для кода $\mathbb{C}_h$, получим важное следствие:

Следствие 3. *Пусть $\mathbb{C}_h$ — код, порожденный строками матрицы инцидентности $\mathbb{EG}(2, 4^h)$, тогда $r(\mathbb{C}_h) \leqslant 4$.*

Доказательство. Предположим, что существует вектор в $\mathbb{F}_2^{4^h}$, который лежит от $\mathbb{C}_h$ на расстоянии, большем 4. Поскольку 0 лежит в коде, то можно считать, что вес выбранного вектора больше или равен 5. Тогда рассмотрим соответствующее этому вектору множество элементов $\mathbb{F}_4^h$, по предположению в нем не менее 5 элементов. Но по теореме 2 расстояние от этого множества до $<\mathbb{B}_0(h)>$ не может превосходить 4, поэтому существует линейная комбинация блоков, а, значит, и линейная комбинация векторов в $\mathbb{F}_2^{4^h}$, приближающая выбранное множество и соответствующий вектор на расстояние, не превосходящее 4. Противоречие.

В свою очередь в теореме 1 фактически показано, что на векторах $\mathbb{F}_2^{4^h}$, соответствующих четверкам $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$, достигается верхняя оценка из следствия 3. Таким образом, доказана следующая теорема:

Теорема о радиусе покрытия. *Пусть* $h \in \mathbb{N}$ *и* $\mathbb{C}_h$ *— код, порожденный строками матрицы инцидентности* $\mathbb{EG}(2, 4^h)$. *Тогда* $r(\mathbb{C}_h) = 4$.

Список литературы

1. Тарannиков Ю. В. Комбинаторные свойства дискретных структур и приложения к криптологии. — М.: МЦНМО, 2011.
2. Коваленко М. Э., Урбанович Т. А. О ранге матриц инцидентности точек и прямых конечных аффинных и проективных геометрий над полем порядка 4. Препринт, 2013.

ОБ АФФИННОСТИ БУЛЕВЫХ ФУНКЦИЙ НА АФФИННЫХ ПОДПРОСТРАНСТВАХ

Н. А. Коломеец (Новосибирск)

В данной работе рассматривается свойство булевых функций, связанное с аффинностью на аффинных подпространствах.

Введем необходимые определения. Отображение $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется *булевой функцией* от n переменных. *Алгебраической степенью* или просто *степенью* булевой функции называется степень ее алгебраической нормальной формы (полинома Жегалкина). Булева функция называется *аффинной*, если ее алгебраическая степень не больше 1 и *квадратичной*, если ее степень равна 2. Множество $a \oplus D = \{a \oplus d \ : \ d \in D\}, a \in \mathbb{Z}_2^n, D \subseteq \mathbb{Z}_2^n$, называется *сдвигом* множества D. *Аффинное подпространство* — сдвиг линейного подпространства. Через Ind_D обозначим характеристическую функцию множества $D \subseteq \mathbb{Z}_2^n$. Через $\langle u, v\rangle$ обозначим скалярное произведение векторов u и v. Булева функция f от n переменных *аффинна на множестве* $D \subseteq \mathbb{Z}_2^n$, если существуют $a \in \mathbb{Z}_2^n$, $c \in \mathbb{Z}_2$, такие что верно $f|_D(x) = \langle a, x\rangle \oplus c$. Под *расстоянием* между двумя булевыми функциями подразумевается *расстояние Хэмминга* между их векторами значений.

Все квадратичные булевы функции обладают следующим свойством.

Утверждение 1. *Пусть* f *— квадратичная булева функция от* n *переменных. Тогда для любого аффинного подпространства* L *верно: если* f *аффинна на* L, *то* f *также аффинна на любом сдвиге* L.

Доказательство следует из неравенства $\deg(f(x) \oplus f(x \oplus s)) \leqslant 1$, верного для любого $s \in \mathbb{Z}_2^n$.

Отметим, что не для всех квадратичных функций существует хотя бы одно аффинное подпространство размерности большей, чем $\lceil n/2 \rceil$, на котором функция аффинна. Например, если f является бент-функцией (n четно), то

не существует подпространств размерности $n/2+1$ и больше, на которых f аффинна. Бент-функция — это булева функция от четного числа переменных, максимально удаленная от множества всех аффинных функций. Понятие бент-функций ввел О. Ротхаус [3]. Бент-функции представляют интерес в криптографии и теории кодирования, поскольку имеют в этих областях множество различных приложений. Тем не менее, до сих пор существует большое число нерешенных проблем, связанных с бент-функциями (например, см. [5, 6]).

Внесем ограничение на размерность подпространств в условие утверждения 1.

Утверждение 2. *Пусть f — квадратичная булева функция от n переменных. Тогда для любого аффинного подпространства L размерности $\lceil n/2 \rceil$ верно: если f аффинна на L, то f аффинна на любом сдвиге L.*

Если f является бент-функцией, то по всем подпространствам размерности $n/2$, на которых она аффинна, можно построить все бент-функции, которые находятся на расстоянии $2^{n/2}$ от f.

Утверждение 3 [4]. *Пусть f — бент-функция от n переменных, n четно, и $L \subseteq \mathbb{Z}_2^n$, $|L| = 2^{n/2}$. Тогда $f(x) \oplus Ind_L(x)$ является бент-функцией тогда и только тогда, когда L является аффинным подпространством и f на нем аффинна.*

Конструкцию $f(x) \oplus Ind_L(x)$ можно также найти в монографии [5]. Приведем связанное определение, изначально предложенное Х. Доббертином для функций от четного числа переменных, а затем обобщенное П. Шарпин.

Определение ([1, 2])**.** Булева функция f от n переменных называется нормальной (слабо нормальной), если существует подпространство L размерности $\lceil \frac{n}{2} \rceil$, на котором f является константой (аффинна).

Следующая теорема показывает, для каких функций справедливо утверждение 2.

Теорема. *Пусть f — булева функция от n переменных и для любого аффинного подпространства L размерности $\lceil \frac{n}{2} \rceil$ верно: если f аффинна на L, то f аффинна на любом сдвиге L. Тогда f либо аффинна, либо квадратична, либо не является слабо нормальной.*

Отметим, что случай, когда f является бент-функцией, наиболее интересен.

Список литературы

1. Charpin P. Normal Boolean functions // Journal of Complexity. — 2004. — V. 20. — P. 245–265.

2. Dobbertin H. Construction of bent functions and balanced Boolean functions with high nonlinearity // Fast Software Encryption, Lecture Notes in Computer Science. — 1994. — V. 1008. — P. 61–74.
3. Rothaus O. On bent functions // J. Combin. Theory. Ser. A. — 1976. — V. 20., N. 3 — P. 300–305.
4. Коломеец Н. А., Павлов А. В. Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. — 2009. Т. 4. — С. 5–20.
5. Логачев О.А., Сальников А.А., Ященко В.В. Boolean functions in coding theory and cryptology. M.: MCNMO, 2004. 470 p. ISBN 5-94057-117-4.
6. Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения. Saarbrucken: LAP LAMBERT Academic Publishing, 2011. 180 с. ISBN: 978-3-8433-0904-2.

О СЛОЖНОСТИ БУЛЕВЫХ ФОРМУЛ В БАЗИСАХ ИЗ ЭЛЕМЕНТОВ С ПРЯМЫМИ И ИТЕРАТИВНЫМИ ВХОДАМИ

В. А. Коноводов (Москва)

Пусть $X = \{x_1, x_2, \ldots\}$ и $Y = \{y_1, y_2, \ldots\}$ — счетные множества булевых переменных, причем переменные из X (из Y) будем называть *прямыми* (соответственно *итеративными*). Для каждого множества переменных Z обозначим через $P_2(Z)$ множество всех функций алгебры логики (в дальнейшем — просто функций), зависящих от переменных из Z.

Пусть $B \subset P_2(X \cup Y)$ — некоторое конечное множество базисных функций. Будем рассматривать одновыходные схемы из функциональных элементов (в дальнейшем будем называть их просто схемами) над базисом B (см., например, [1]), в которых:

1. Прямые входы любого элемента либо присоединяются к входам схемы, либо являются константными входами (вход называется константным, если вместо него в базисный элемент подставлена константа 0 или 1).

2. Итеративные входы любого элемента либо присоединяются к выходам других элементов, либо присоединяются к входам схемы, либо являются константными входами.

3. Неконстантным входам схемы сопоставлены некоторые переменные из множества X.

Как обычно, формулами считаются те схемы, которые не содержат ветвлений выходов элементов.

Систему функций B будем называть *полной*, если для любой функции f, $f \in P_2(X)$, существует формула над B указанного вида, реализующая f.

Критерий полноты произвольной системы функций был получен в работе [2].

Каждому элементу $\mathcal{E}$ базиса B поставим в соответствие его вес $\rho(\mathcal{E}) > 0$. Сложностью $L_B(\mathcal{F})$ формулы $\mathcal{F}$ в этом базисе назовем сумму весов всех входящих в нее элементов. Функцией Шеннона $L_B(n)$ для сложности формул в базисе B, как обычно, называется максимальное значение $L_B(f)$ среди всех функций f, $f \in P_2(\{x_1, \ldots, x_n\})$, где $L_B(f)$ — минимальная сложность формулы из рассматриваемого класса, реализующей функцию f.

Функция Шеннона $L_B^C(n)$ для сложности схем определяется аналогично.

Формулы в стандартных базисах

Пусть B_0 — стандартный базис, состоящий из функциональных элементов $\&$, $\vee$ и $\neg$ веса 1, которые реализуют функции $y_1 \cdot y_2$, $y_1 \vee y_2$ и $\bar{y}_1$, соответственно. Известно (см., например, [1, 3]), что[1]

$$L_{B_0}(n) = \frac{2^n}{\log n}\left(1 \pm O\left(\frac{1}{\log n}\right)\right)$$

(здесь и далее все логарифмы рассматриваются по основанию 2).

Из критерия полноты [2] вытекает, что следующие итеративные модификации стандартного базиса B_0:

$$\{y_1 \& y_2, x_1 \vee x_2, \bar{x}_1\},$$
$$\{y_1 \& y_2, y_1 \vee x_1, \bar{x}_1\},$$
$$\{y_1 \& x_1, y_1 \vee x_1, \bar{x}_1\},$$
$$\{y_1 \& x_1, y_1 \vee x_1, \bar{y}_1\}$$

и двойственные к ним, не являются полными.

Рассмотрим теперь полные итеративные модификации стандартного базиса. Будем считать, что если два входа некоторого элемента итеративные, и в базисе есть другие элементы с прямыми входами, то вес такого элемента равен 2, а веса элементов с прямыми переменными равны 1. В противном случае все элементы в некотором смысле «равноценны», и их веса будем считать равными 1.

Теорема. *Пусть*

$$B_1 = \{y_1 \& y_2, x_1 \vee x_2, \bar{y}_1\}, \text{ и } B_2 = \{y_1 \& y_2, y_1 \vee x_1, \bar{y}_1\},$$

[1] Для числовых функций $g(n)$ и $h(n)$ натурального аргумента n запись $h(n) = O(g(n))$ означает, как обычно, что отношение $|h(n)/g(n)|$ ограничено сверху. Запись $h(n) = \Theta(g(n))$ означает, что $h(n) = O(g(n))$ и $g(n) = O(h(n))$.

где вес элементов, реализующих конъюнкцию, равен 2, *а веса остальных элементов равны* 1. *Тогда при растущем значении натурального аргумента* n *справедливы следующие оценки соответствующих функций Шеннона для сложности формул*:

$$L_{B_1}(n) = \frac{3}{2} \cdot \frac{2^n}{\log n} \left(1 + \frac{\frac{1}{2}\log\log n \pm O(1)}{\log n}\right),$$

$$L_{B_2}(n) = \frac{2^n}{\log n} \left(1 + \frac{\log\log n \pm O(1)}{\log n}\right).$$

Данное утверждение справедливо также для базисов, двойственных к приведенным.

Оценки такого рода являются оценками высокой степени точности, устанавливающими не только асимптотику функции Шеннона, но и асимптотику первого остаточного члена ее асимптотического разложения.

Аналогичным образом подобные оценки могут быть получены для базисов B_1' и B_2', отличающихся от B_1 и B_2 тем, что функциональные элементы, имеющие вес 2, имеют произвольный вес, строго больший 1.

Порядок роста функции Шеннона в различных базисах

В [4] установлено, что функция Шеннона $L_B^C(n)$ для сложности схем в произвольном полном базисе B имеет «стандартный» порядок роста $2^n/n$. Кроме того, в [4] указано, что в случае формул порядок роста $L_B(n)$ не более, чем 2^n, и не менее, чем $2^n/\log n$.

Пусть A — произвольное конечное множество функций, $A \subseteq P_2(X \cup Y)$. Обозначим через $[A]$ множество тех функций, которые можно получить из элементов множества A в результате применения следующих операций суперпозиции:

1. Переименование (с отождествлением) прямых переменных.
2. Переименование (с отождествлением) итеративных переменных.
3. Подстановка констант 0, 1 вместо переменных.
4. Замена итеративных переменных прямыми переменными.
5. Подстановка одной функции вместо итеративной переменной другой функции.

Обозначим $\delta(A) = [A] \cap P_2(Y)$. Тогда $\delta(A)$ является «обычным» замкнутым классом [5] в $P_2(Y)$, содержащим константы.

Утверждение 1. *Пусть B — система базисных функций, для которой $\delta(B)$ совпадает с классом всех монотонных функций от переменных Y. Тогда при растущем значении натурального аргумента n*

$$L_B(n) = \Theta\left(\frac{2^n}{\log n}\right).$$

Для каждого натурального числа k определим функции

$$\mu_k = \mu_k(x_1, \ldots, x_k, y_0, \ldots, y_{2^k-1}) = \bigvee_{\sigma_1,\ldots,\sigma_k \in \{0,1\}} x_1^{\sigma_1} \cdots x_k^{\sigma_k} \cdot y_{\nu(\sigma_1,\ldots,\sigma_k)},$$

$$h_k = (\bar{x}_1 \vee \ldots \vee \bar{x}_k) \cdot y_1 \vee x_1 \cdots x_k \cdot y_2 = \mu_k(x_1, \ldots, x_k, y_1, \ldots, y_1, y_2),$$

где $x^0 = \bar{x}$, $x^1 = x$, а $\nu(\sigma_1, \ldots, \sigma_k)$ — натуральное число, двоичная запись которого совпадает с $(\sigma_1, \ldots, \sigma_k)$. Функция μ_k называется мультиплексорной функцией порядка k.

Утверждение 2. *Для любого натурального k при растущем значении натурального аргумента n выполняются соотношения*

$$L_{\{\mu_k\}}(n) = \Theta(2^n), \quad L_{\{h_k\}}(n) = \Theta(2^n).$$

Работа выполнена при поддержке РФФИ, проект № 12-01-00964-а.

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Издательство МГУ, 1984.
2. Ложкин С. А. О полноте и замкнутых классах функций алгебры логики с прямыми и итеративными переменными // Вестн. Моск. ун-та, сер. 15: Вычислит. матем. и киберн. — 1999, — № 3. — С. 35-–41.
3. Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов. // Математические вопросы кибернетики. — 1996. — Вып. 6. —М.: Физматлит. — С. 189–213.
4. Ложкин С. А. О сложности реализации функций алгебры логики схемами и формулами, построенными из функциональных элементов с прямыми и итеративными переменными // Труды III международной конференции «Дискретные модели в теории управляющих систем» Красновидово'98 (22–27 июня 1998 г.) — М.: Диалог-МГУ, 1998. — С. 72–73.
5. Яблонский С. В. Введение в дискретную математику. — М., 1986.

О ГЛУБИНЕ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ ПРИ РЕАЛИЗАЦИИ СХЕМАМИ НАД ПРОИЗВОЛЬНЫМ БЕСКОНЕЧНЫМ БАЗИСОМ

А. В. Кочергин (Москва)

Введение

Изучается поведение функции Шеннона $D_B(n)$ глубины схем из функциональных элементов над произвольным бесконечным полным базисом B. Устанавливается, что при любом фиксированном $k \geqslant 2$ для любого бесконечного полного базиса B функций k-значной логики либо существует такая константа $\alpha \geqslant 1$, что $D_B(n) = \alpha$ при всех достаточно больших n, либо существует такая константа $\beta > 0$, что при $n \to \infty$ выполняется $D_B(n) \sim \beta \log_2 n$.

1. Основные понятия. Постановка задачи

Изучается глубина функций k-значной ($k \geqslant 2$) логики при реализации схемами из функциональных элементов над произвольным бесконечным базисом. Под *базисом* понимается произвольное функционально полное множество функций k-значной логики, т. е. такое, что его замыкание относительно операции суперпозиции совпадает с множеством всех функций k-значной логики. Базис будем называть *бесконечным*, если для любого натурального числа m существует функция из этого базиса, существенно зависящая более чем от m переменных. В противном случае базис будем называть *конечным*. Под *глубиной схемы* понимается максимальное число функциональных элементов в ориентированных цепях, ведущих от какого-либо входа схемы к ее выходу. Под глубиной функции f над базисом B, обозначаемой через $D_B(f)$, будем понимать минимальную глубину схем, реализующих функцию f над базисом B. Для произвольного базиса B функций k-значной логики стандартным образом определяется функция $D_B(n)$ Шеннона глубины: при любом натуральном n ее значение задается соотношением $D_B(n) = \max D_B(f)$, где максимум берется по всем функциям k-значной логики f, зависящим от n переменных. Более подробно эти и другие определения см. в [1, 2].

В [1] установлено, что для любого конечного базиса B булевых функций (функций двузначной логики) существует такая константа $\alpha > 0$, что при $n \to \infty$ выполняется соотношение $D_B(n) \sim \alpha n$. В [3] этот результат распространен на случай функций k-значной логики. Показано, что для любого конечного базиса B функций k-значной логики ($k \geqslant 3$) существует такая константа $\beta > 0$, что при $n \to \infty$ выполняется соотношение $D_B(n) \sim \beta n$. В [4] установлено, что в случае двузначной логики для любого бесконечного базиса B порядок роста функции Шеннона глубины $D_B(n)$ равен либо 1, либо $\log_2 n$. В [5, 6] этот результат усилен: доказано, что для любого бесконечного бази-

са булевых функций B либо существует такая константа a, $1 \leqslant a \leqslant 6$, что $D_B(n) = a$ при всех достаточно больших n, либо существует такая целочисленная константа $b \geqslant 2$, что $\log_b n \leqslant D_B(n) \leqslant \log_b n + 5$ при всех n. В [7] результат работы [4] распространен на случай функций k-значной логики. Показано, что при любом фиксированном $k \geqslant 2$ для любого бесконечного базиса B функций k-значной логики либо существует такая константа $\zeta \geqslant 1$, что $D_B(n) = \zeta$ при всех достаточно больших n, либо существуют такие константы η, γ, δ, где $\eta > 0$, что $\eta \log_2 n \leqslant D_B(n) \leqslant \gamma \log_2 n + \delta$ при всех n.

Основным результатом данной работы является следующее утверждение.

Теорема. *При любом фиксированном $k \geqslant 2$ для любого бесконечного полного базиса B функций k-значной логики либо существует такая константа $\alpha \geqslant 1$, что $D_B(n) = \alpha$ при всех достаточно больших n, либо существует такая константа $\beta > 0$, что при $n \to \infty$ имеет место соотношение $D_B(n) \sim \beta \log_2 n$.*

В [8] показано, что при любом простом p всякую булеву функцию f от n переменных можно представить, и притом единственным образом, в виде многочлена

$$f(x_1, \ldots, x_n) \equiv a_0 + \sum_{s=1}^{n} \sum_{1 \leqslant i_1 < \ldots < i_s \leqslant n} a_{i_1 \ldots i_s} x_{i_1} \ldots x_{i_s} \pmod{p}$$

с коэффициентами $a_0, a_{i_1 \ldots i_s}$ из множества $\{0, 1, \ldots, p-1\}$. Представление булевой функции f в указанном виде называется ее *p-представлением*. Наибольшее из таких чисел s, что $a_{i_1 \ldots i_s} \neq 0$, называется *$p$-степенью* булевой функции f и обозначается через $\deg_p f$; если все $a_{i_1 \ldots i_s} = 0$, то p-степень функции f полагается равной нулю. Для любого множества булевых функций A обозначим через $\deg_p A$ максимум из p-степеней входящих в множество A функций, если он существует. В противном случае положим $\deg_p A = \infty$. Подробнее эти определения см. в [5].

Для произвольного целого числа x, $0 \leqslant x \leqslant k-1$, запишем двоичное представление в виде

$$x = y_1(x) + 2y_2(x) + \ldots + 2^{r-1} y_r(x),$$

где $r = \lceil \log_2 k \rceil$, $y_j(x) \in \{0, 1\}$. Будем рассматривать функции $y_j(x)$, выражающие разряды двоичного представления числа x, как одноместные функции k-значной логики, принимающие значения 0 и 1.

Сохраняя терминологию из [7], для любого простого p и для любой функции k-значной логики $f = f(x_1, x_2, \ldots, x_n)$ обозначим через $\mathrm{gdeg}_p f$ *обобщенную p-степень* функции f, определяемую следующим образом:

$$\mathrm{gdeg}_p f = \max_{1 \leqslant j \leqslant r} \min_{g_j^f} \deg_p g_j^f(t_1^1, \ldots, t_r^1, t_1^2, \ldots, t_r^2, \ldots, t_1^n, \ldots, t_r^n),$$

где при каждом j минимум берется по всем булевым функциям

$$g_j^f(t_1^1,\dots,t_r^1,t_1^2,\dots,t_r^2,\dots,t_1^n,\dots,t_r^n)$$

от nr переменных, удовлетворяющим условию

$$g_j^f(y_1(x_1),\dots,y_r(x_1),\dots,y_1(x_n),\dots,y_r(x_n)) = y_j(f(x_1,x_2,\dots,x_n)).$$

При любом простом p для любого множества A функций k-значной логики обозначим через $\mathrm{gdeg}_p A$ максимум из обобщенных p-степеней входящих в множество A функций, если он существует. В противном случае положим $\mathrm{gdeg}_p A = \infty$. В [7] установлено, что для любого простого p и любого бесконечного базиса B функций k-значной логики имеет место неравенство $\mathrm{gdeg}_p B > 1$.

Обозначим через $A_{1,B}$ базис булевых функций, состоящий из двуместной дизъюнкции, отрицания и всевозможных булевых функций вида g_j^f, где $1 \leqslant j \leqslant r$, а f — функция k-значной логики из базиса B. Легко видеть, что $A_{1,B}$ — бесконечный базис булевых функций. Кроме того, для любого простого p выполняется равенство $\mathrm{gdeg}_p B = \deg_p A_{1,B}$. В [5] установлено, что для любого бесконечного базиса A булевых функций либо $\deg_q A = \infty$ при любом простом q, либо существует единственное p, такое, что $\deg_p A < \infty$. Поэтому справедлива лемма.

Лемма 1. *Для любого бесконечного базиса B функций k-значной логики либо $\mathrm{gdeg}_q B = \infty$ при любом простом q, либо существует единственное p, такое, что $\mathrm{gdeg}_p B < \infty$.*

Если бесконечный базис B функций k-значной логики при некотором (и единственном) p удовлетворяет неравенству $\mathrm{gdeg}_p B < \infty$, то будем говорить, что базис B является базисом *конечной характеристики p*. Если же при всех простых q справедливо соотношение $\mathrm{gdeg}_q B = \infty$, то будем говорить, что базис B является базисом *бесконечной характеристики*. В некоторых случаях для удобства базисы конечной характеристики p будем также называть просто базисами *конечной характеристики*.

В случае базисов бесконечной характеристики справедливо следующее утверждение.

Лемма 2 [7]. *Пусть B — бесконечный базис функций k-значной логики, такой, что $\mathrm{gdeg}_q B = \infty$ для любого простого q. Тогда существует такая константа $\alpha \geqslant 1$, что $D_B(n) = \alpha$ при всех достаточно больших n.*

2. Базисы конечной характеристики

Рассмотрим произвольный бесконечный базис B функций k-значной логики, удовлетворяющий следующему условию: для некоторого простого p выполняется неравенство $\mathrm{gdeg}_p B < \infty$. Для любого целого неотрицательного d

через $M_{p,B}(d)$ обозначим максимум из обобщенных p-степеней функций, реализуемых над базисом B схемами глубины не более d (нетрудно показать корректность такого определения: для любого натурального d имеет место неравенство $M_{p,B}(d) < \infty$). Легко видеть, что при любом натуральном d справедливы соотношения

$$M_{p,B}(d) \geqslant M_{p,B}(1) = \operatorname{gdeg}_p B > 1.$$

Лемма 3. *Для любых натуральных m и l справедливо неравенство*

$$M_{p,B}(m+l) \leqslant M_{p,B}(m) M_{p,B}(l).$$

Сформулируем известный факт из математического анализа (см., например, [9]).

Лемма 4. *Пусть $\{a_n\}$ — такая последовательность неотрицательных чисел, что для любых натуральных чисел m и l выполняется неравенство $a_{m+l} \leqslant a_m + a_l$. Тогда существует предел $\lim\limits_{n\to\infty} \frac{a_n}{n}$.*

Из лемм 3–4 вытекает следующее утверждение.

Лемма 5. *Последовательность $\{a_d\}$, где*

$$a_d = \frac{\log_2 M_{p,B}(d)}{d},\ d = 1, 2, 3, \ldots,$$

при $d \to \infty$ имеет предел.

Положим

$$\kappa_B = \lim_{d\to\infty} \frac{\log_2 M_{p,B}(d)}{d}.$$

Лемма 6. *Величина κ_B удовлетворяет неравенству $\kappa_B > 0$.*

Лемма 7. *Для любого натурального n существует функция k-значной логики $w_n = w_n(x_1, \ldots, x_n)$, удовлетворяющая условию $\operatorname{gdeg}_p w_n \geqslant n$.*

Лемма 8. *Для любого натурального d и произвольной функции k-значной логики f справедливо неравенство*

$$\operatorname{gdeg}_p f \leqslant M_{p,B}(d)^{\left\lceil \frac{D_B(f)}{d} \right\rceil}.$$

Используя утверждения лемм 5–8, можно установить справедливость следующего утверждения.

Лемма 9. *Для любого $\varepsilon \geqslant 0$ при всех достаточно больших n справедливо неравенство*

$$D_B(n) \geqslant \left(\kappa_B^{-1} - \varepsilon\right) \log_2 n.$$

Лемма 10. *Существует такая константа d_5, что для любых функций k-значной логики f и ψ, удовлетворяющих условию $\mathrm{gdeg}_p\psi \leqslant \mathrm{gdeg}_p f$, выполняется неравенство $D_B(\psi) \leqslant D_B(f) + d_5$.*

С помощью леммы 10, можно показать справедливость следующего факта.

Лемма 11. *При $n \to \infty$ выполняется соотношение*

$$D_B(n) \leqslant \kappa_B^{-1} \log_2(n) + o(\log_2(n)).$$

Из лемм 9 и 11 следует, что если для произвольного бесконечного базиса B при некотором простом p выполняется неравенство $\mathrm{gdeg}_p B < \infty$, то имеет место соотношение $D_B(n) \sim \beta \log_2 n$, где $\beta = \kappa_B^{-1}$.

Отсюда и из леммы 2 непосредственно вытекает утверждение теоремы.

Автор выражает благодарность О. М. Касим-Заде за постановку задачи, всестороннее внимание к работе и ценные замечания.

Работа выполнена при финансовой поддержке РФФИ (проект 11–01–00508) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Лупанов О. Б. О схемах из функциональных элементов с задержками // Проблемы кибернетики. Вып. 23. М.: Наука. — 1970. — С. 1–11.
2. Сэвидж Дж. Э. Сложность вычислений. — М.: Факториал, 1998.
3. Кочергин А. В. О глубине функций k-значной логики в конечных базисах // Вестн. Моск. ун-та. Сер. 1. Матем. Механ. — 2013. — № 1. — С. 56–59.
4. Касим-Заде О. М. О глубине булевых функций при реализации схемами над произвольным базисом // Вестн. Моск. ун-та. Сер. 1. Матем. Механ. — 2007. — № 1. — С. 18–21.
5. Касим-Заде О. М. О глубине булевых функций над произвольным бесконечным базисом // Дискретный анализ и исследование операций. Сер. 1. — 2007. — Т. 14, № 1. — С. 45–69.
6. Касим-Заде О. М. О глубине булевых функций при реализации схемами над произвольным бесконечным базисом // Вестн. Моск. ун-та. Сер. 1. Матем. Механ. — 2012. — № 6. — С. 55–57.
7. Кочергин А. В. О глубине функций k-значной логики в бесконечных базисах // Вестн. Моск. ун-та. Сер. 1. Матем. Механ. — 2011. — № 1. — С. 22–26.
8. Smolensky R. Algebraic methods in the theory of lower bounds for Boolean circuit complexity // Proc. 19th Annual ACM Symposium on Theory of Computing (1987). — N. Y.: ACM, 1987. — P. 77–82.

9. Полиа Г., Сеге Г. Задачи и теоремы из анализа. Часть первая. Издание третье. — М.: Наука, 1978.

О СЛОЖНОСТИ OBDD БУЛЕВЫХ ФУНКЦИЙ НЕКОТОРЫХ ВИДОВ

А. О. Красиков (Москва)

Введение

В настоящей заметке получены оценки сложности OBDD для функций некоторых видов. Также получены порядки переменных функций, при которых достигаются эти оценки.

Основные определения

Определение. *Двоичная разрешающая диаграмма* (BDD) — это корневой ориентированный ациклический граф, вершины которого разбиты на два класса: терминальные вершины и нетерминальные вершины. Каждая нетерминальная вершина v помечена переменной $var(v)$ и имеет две вершины-последователя: $low(v)$ и $high(v)$. Каждая терминальная вершина v помечена $value(v)$ — либо 0, либо 1. Всякая двоичная разрешающая диаграмма B с корнем в вершине v определяет булеву функцию $f_v(x_1, \ldots, x_n)$ следующего вида:

1. Если v — терминальная вершина, то считаем, что
   (a) если $value(v) = 1$, то $f_v(x_1, \ldots, x_n) = 1$,
   (b) если $value(v) = 0$, то $f_v(x_1, \ldots, x_n) = 0$.
2. В случае, когда v — нетерминальная вершина и $var(v) = x_i$,

$$f_v(x_1, \ldots, x_n) = (\overline{x_i} f_{low(v)}(x_1, \ldots, x_n)) \vee (x_i f_{high(v)}(x_1, \ldots, x_n)).$$

Определение. *Порядком переменных* $(x_1, \ldots, x_n)$ называется их перестановка $t(x_1, \ldots, x_n) = (x_{i_1}, \ldots, x_{i_n})$. Через $t(x_i)$ будем обозначать номер переменной x_i в порядке t.

Определение. OBDD — двоичная разрешающая диаграмма со следующими ограничениями на структуру:

1. По каждому пути из корня в терминальную вершину переменные должны следовать в одном и том же порядке;

2. В диаграмме не должно быть изоморфных поддеревьев или избыточных вершин.

Определение. Пусть $f = f(x_1, \ldots, x_n)$, $t(x_1, \ldots, x_n)$ — порядок переменных $(x_1, \ldots, x_n)$. Тогда сложность $L_t(f)$ OBDD, реализующей функцию $f(x_1, \ldots, x_n)$ при порядке переменных $t(x_1, \ldots, x_n)$ — это число нетерминальных вершин в OBDD; через $L(f)$ будем обозначать $\min\limits_t L_t(f)$; через $L_t(f, x)$ будем обозначать число вершин в OBDD с пометкой x при порядке переменных t.

Известные оценки

Верхняя оценка сложности BDD (в худшем случае) [1] равна $(1+o(1))2^n/n$. Для OBDD верхняя оценка сложности (в худшем случае) [2]: $(2 + o(1))2^n/n$. Для симметрических функций OBDD имеют линейную сложность; для функций, представляющих целочисленное сложение, — линейную; для функций, представляющих целочисленное умножение, — экспоненциальную [3].

1. Класс функций, имеющих ДНФ с независимыми слагаемыми

Посредством $var(K)$, будем обозначать множество переменных, входящих в элементарную конъюнкцию K.

Определение 1. Будем говорить, что функция $f(x_1, \ldots, x_n)$ имеет ДНФ

$$A = x_{1_1} \ldots x_{1_{k_1}} \vee \ldots \vee x_{r_1} \ldots x_{r_{k_r}} = K_1 \vee \ldots \vee K_r$$

с *независимыми слагаемыми*, если $\forall i \neq j \ var(K_i) \cap var(K_j) = \varnothing$.

Определение 2. Пусть $f(x_1, \ldots, x_n)$ имеет ДНФ $D(f) = K_1 \vee \ldots \vee K_r$ с независимыми слагаемыми. Тогда порядок $t(x_1, \ldots, x_n)$ будем называть *несмешивающим*, если он представим в виде:

$$(X_{i_1}, \ldots, X_{i_r}),$$

где $X_i = var(K_i)$. В противном случае порядок будем называть *смешивающим*.

В работе доказана следующая теорема:

Теорема 1. *Пусть $f(x_1, \ldots, x_n)$ имеет* ДНФ *с независимыми слагаемыми, k — число существенных переменных функции f. Тогда при несмешивающем порядке $t(x_1, \ldots, x_n)$ $L_t(f) = k$, при смешивающем $L_t(f) > k$.*

Следствие. *Для класса функций, имеющих* ДНФ *с независимыми слагаемыми, несмешивающие порядки, и только они являются оптимальными по сложности.*

2. Класс дизъюнктивно разложимых функций

Определение 3. Пусть $f = f(x_1, \ldots, x_n)$, $D(f)$ — ее ДНФ. Тогда *графом пересечений* ДНФ $D(f)$ будем называть граф следующей структуры:

1. Существует взаимно-однозначное соответствие между вершинами графа и конъюнкциями $D(f)$;

2. Между вершинами графа проходит ребро в том, и только в том случае, когда соответствующие им конъюнкции имеют общие переменные.

Пусть $G(f)$ — граф пересечений ДНФ некоторой булевой функции f, C — его подграф. Множеству вершин графа C соответствует множество элементарных конъюнкций. Тогда посредством $var(C)$ будем обозначать множество переменных, входящих в эти конъюнкции; *функцией, соответствующей* C, будем называть дизъюнкцию всех этих конъюнкций.

Определение 4. Будем говорить, что функция $f(x_1, \ldots, x_n)$ *дизъюнктивно разложима*, если для некоторой ее ДНФ $D(f)$ граф пересечений $D(f)$ имеет более одной компоненты связности. Соответствующую ДНФ будем называть *разложимой* ДНФ функции f.

Определение 5. Пусть $f(x_1, \ldots, x_n)$ — дизъюнктивно разложимая функция, $D(f)$ — ее разложимая ДНФ, $G(f)$ — граф пересечений этой ДНФ, $C_1, \ldots, C_r$ — компоненты связности этого графа. Тогда порядок $t(x_1, \ldots, x_n)$ будем называть *несмешивающим* для функции $f(x_1, \ldots, x_n)$, если он представим в виде

$$(X_{i_1}, \ldots, X_{i_r}),$$

где $X_i = var(C_i)$. В противном случае порядок будем называть *смешивающим*.

Определение 6. *Проекцией* порядка переменных $t(x_1, \ldots, x_n)$ на множество $\{x_{i_1}, \ldots, x_{i_r}\} \subseteq \{x_1, \ldots, x_n\}$ будем называть такой порядок $t'(x_{i_1}, \ldots, x_{i_r})$ что $t'(x) < t'(y)$ тогда и только тогда, когда $t(x) < t(y)$.

Была доказана следующая теорема:

Теорема 2. *Пусть $f(x_1, \ldots, x_n)$ — дизъюнктивно разложимая функция; $D(f)$ — соответствующая разложимая* ДНФ*; $C_1, \ldots, C_r$ — компоненты связности графа пересечений $D(f)$, $f_1, \ldots, f_r$ — соответствующие им функции; $t(x_1, \ldots, x_n)$ — порядок переменных. Тогда, если порядок t — несмешивающий, то*

$$L_t(f) = \sum_{i=1}^{r} L_t(f_i);$$

если t — смешивающий, то

$$L_t(f) \geqslant L_{t'}(f),$$

а если f к тому же монотонная функция, то

$$L_t(f) > L_{t'}(f),$$

где $t' = (t'_{i_1}, \ldots, t'_{i_r})$, а t'_i — проекция t на множество $var(C_i)$.

Аналогично можно ввести понятие *конъюнктивно разложимая функция*, и для таких функций будет верна теорема, аналогичная теореме 2.

Список литературы

1. Breitbart Y., Hunt III H., Rosenkrantz D. On the Size of Binary Decision Diagrams Representing Boolean Functions // Theoret. Computer Sci. — 1995. — V. 145. — P. 45–69.
2. Heh-Tyan Liaw, Chen-Shang Lin On the OBDD-Representation of General Boolean Functions // IEEE Trans. Computers. — 1992. — V. 41, №. 6. — P. 661–664.
3. Bryant R. E. Symbolic Boolean Manipulation with Ordered Binary Decision Diagrams // ACM Computing Surveys. — 1992. — V. 24, №. 3.

О ЧИСЛЕ ЭЛЕМЕНТОВ СХЕМЫ, РЕАЛИЗУЮЩЕЙ ОБОБЩЕННУЮ МЕДИАНУ В ПОЛНОМ БАЗИСЕ С ФУНКЦИЕЙ $x_1 \oplus x_2 \oplus a$

А. Е. Лакомкина (Пенза)

Рассматривается реализация булевых функций схемами из ненадежных элементов в полном конечном базисе $B = \{e_1, e_2, ..., e_m\}$ $(m \in \mathbf{N})$, содержащем либо $x_1 \oplus x_2$, либо $x_1 \oplus x_2 \oplus 1$.

Булеву функцию вида $x_1^{\sigma_1}x_2^{\sigma_2} \vee x_1^{\sigma_1}x_3^{\sigma_3} \vee x_2^{\sigma_2}x_3^{\sigma_3}$ $(\sigma_i \in \{0,1\}, i \in \{1,2,3\})$ будем называть *обобщенной медианой*.

Пусть G — множество булевых функций от переменных x_1, x_2, x_3, каждая из которых конгруэнтна некоторой обобщенной медиане. Очевидно, что $x_1x_2 \vee x_1x_3 \vee x_2x_3 \in G$.

Обозначим через N_g минимальное число надежных элементов, необходимое для реализации функции $g \in G$ в базисе B схемой; и пусть $N_G = \min N_g$, где минимум берется по всем функциям $g \in G$.

Булевы функции вида $x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_0$ $(a_i \in \{0,1\}, i \in \{0,1,2,3\})$, как и в работе [1], будем называть *особенными*.

Лемма 1 [1]. *Из всякой нелинейной и неособенной функции от трех или более переменных подстановкой переменных можно получить либо особенную функцию, либо нелинейную функцию двух переменных.*

Из леммы 1 следует, что для всякой нелинейной функции f_L имеет место один из вариантов:

либо f_L является особенной функцией;

либо f_L — функция двух переменных;

либо из неособенной функции $f_L(x_1, x_2, ..., x_n)$ $(n \geqslant 3)$ подстановкой переменных можно получить особенную функцию;

либо из неособенной функции $f_L(x_1, x_2, ..., x_n)$ $(n \geqslant 3)$ отождествлением переменных можно получить нелинейную функцию двух переменных.

Таким образом, получаем очевидное следствие.

Следствие 1. *Из всякой нелинейной функции f_L подстановкой переменных можно получить функцию, равную либо некоторой особенной функции: $\varphi(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_0$, либо некоторой нелинейной функции двух переменных: $\psi(x_1, x_2) = x_1x_2 \oplus a_1x_1 \oplus a_2x_2 \oplus a_0$, $(a_i \in \{0, 1\}, i \in \{0, 1, 2, 3\})$.*

Теорема 1. *Если полный конечный базис содержит функцию $x_1 \oplus x_2$ или $x_1 \oplus x_2 \oplus 1$, то $N_G \leqslant 4$.*

Доказательство. Пусть B — произвольный полный конечный базис. Поскольку базис B — полный, в нем содержится нелинейная функция f_L. Из функции f_L (см. лемму 1 и следствие 1) подстановкой переменных можно получить функцию, равную либо

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

либо

$$\psi(x_1, x_2) = x_1x_2 \oplus a_1x_1 \oplus a_2x_2 \oplus a_0, \quad a_i \in \{0, 1\}, i \in \{0, 1, 2, 3\}.$$

1. Пусть $\varphi(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_0$.

1.1. Если функция $\varphi(x_1, x_2, x_3)$ конгруэнтна функции

$$x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a_4(x_2 \oplus x_3) \oplus a_0,$$

то $\varphi(x_1, x_2, x_3) = x_1^{\overline{a}_0 \oplus a_4} \cdot x_2^{\overline{a}_0} \oplus x_1^{\overline{a}_0 \oplus a_4} \cdot x_3^{\overline{a}_0} \oplus x_2^{\overline{a}_0} \cdot x_3^{\overline{a}_0}$, т. е. $\varphi(x_1, x_2, x_3) \in G$. В этом случае $N_G = 1$.

1.2. Если функция $\varphi(x_1, x_2, x_3)$ конгруэнтна функции

$$x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3 \oplus a_4(x_1 \oplus x_2) \oplus a_0,$$

то, отождествляя x_1 и x_2, получим функцию $\varphi(x_1, x_1, x_3) = x_1 \oplus x_3 \oplus a_0$. Моделируя формулу $\varphi_2(\varphi_2(x_1, x_2, x_3), \varphi_2(x_1, x_2, x_3), x_3)$, построим схему S_g из двух элементов. Нетрудно проверить, что

$$\varphi_2(\varphi_2(x_1, x_2, x_3), \varphi_2(x_1, x_2, x_3), x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a_4 \cdot (x_1 \oplus x_2) \in G.$$

Таким образом, $N_G \leqslant 2$.

2. Пусть $\psi(x_1, x_2) = x_1x_2 \oplus a_1x_1 \oplus a_2x_2 \oplus a_0$, т. е. функция $\psi(x_1, x_2)$ конгруэнтна одной из функций $\overline{x}_1 \cdot \overline{x}_2$, $\overline{x}_1 \vee \overline{x}_2$, $\overline{x}_1 \cdot x_2$, $\overline{x}_1 \vee x_2$, $x_1 \cdot x_2$, $x_1 \vee x_2$. По условию базис B содержит линейную функцию $l(x_1, x_2) = x_1 \oplus x_2 \oplus a, (a \in \{0, 1\})$. Рассмотрим возможные варианты.

2.1. Предположим, что из базисных функций подстановкой переменных можно получить функцию $\overline{x}_1 \cdot \overline{x}_2$. Тогда моделируя формулу $l(\overline{l(x_1, x_2)} \cdot l(x_1, x_3), x_1)$, построим схему из четырех элементов, реализующую функцию

$$(x_1 \oplus x_2 \oplus \overline{a}) \cdot (x_1 \oplus x_3 \oplus \overline{a}) \oplus x_1 \oplus a = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus \overline{a} \cdot (x_2 \oplus x_3) \oplus 1$$

из множества G, т. е. $N_G \leqslant 4$.

2.2. Предположим, что из базисных функций подстановкой переменных можно получить функцию $\overline{x}_1 \vee \overline{x}_2$. Моделируя формулу $l(\overline{l(x_1, x_2)} \vee \overline{l(x_1, x_3)}, x_1)$, построим схему из четырех элементов, реализующую функцию

$$(\overline{x_1 \oplus x_2 \oplus a} \vee \overline{x_1 \oplus x_3 \oplus a} \oplus x_1 \oplus a = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a \cdot (x_2 \oplus x_3) \oplus 1$$

из множества G, т. е. $N_G \leqslant 4$.

2.3. Предположим, что из базисных функций подстановкой переменных можно получить функцию $\overline{x}_1 \cdot x_2$. Тогда моделируя формулу $l(\overline{l(x_1, x_2)} \cdot l(x_1, x_3), x_i)$ ($i = 2$, если $a = 1; i = 3$, если $a = 0$), построим схему из четырех элементов, реализующую функцию

$$(x_1 \oplus x_2 \oplus \overline{a}) \cdot (x_1 \oplus x_3 \oplus a) \oplus x_i \oplus a = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a$$

из множества G, т. е. $N_G \leqslant 4$.

2.4. Предположим, что из базисных функций подстановкой переменных можно получить функцию $\overline{x}_1 \vee x_2$. Моделируя формулу $l(\overline{l(x_1, x_2)} \vee l(x_1, x_3), x_i)$ ($i = 3$, если $a = 1$; $i = 2$, если $a = 0$), построим схему из четырех элементов, реализующую функцию

$$((x_1 \oplus x_2 \oplus \overline{a}) \vee (x_1 \oplus x_3 \oplus a)) \oplus x_i \oplus a = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus \overline{a}$$

из множества G, т. е. $N_G \leqslant 4$.

2.5. Предположим, что из базисных функций подстановкой переменных можно получить функцию $x_1 \cdot x_2$. Тогда моделируя формулу $l(l(x_1, x_2) \cdot l(x_1, x_3), x_1)$, построим схему из четырех элементов, реализующую функцию

$$(x_1 \oplus x_2 \oplus a) \cdot (x_1 \oplus x_3 \oplus a) \oplus x_1 \oplus a = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a \cdot (x_2 \oplus x_3) \oplus a$$

из множества G, т. е. $N_G \leqslant 4$.

2.6. Предположим, что из базисных функций подстановкой переменных можно получить функцию $x_1 \vee x_2$. Моделируя формулу $l(l(x_1, x_2) \vee l(x_1, x_3), x1)$, построим схему из четырех элементов, реализующую функцию

$$((x_1 \oplus x_2 \oplus a) \vee (x_1 \oplus x_2 \oplus a)) \oplus x_1 \oplus a = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus \overline{a}(x_2 \oplus x_3),$$

из множества G, т. е. $N_G \leqslant 4$.

Таким образом, во всех рассмотренных случаях $N_G \leqslant 4$.

Теорема 1 доказана.

Вывод: в любом полном конечном базисе, содержащем функцию $x_1 \oplus x_2$ или $x_1 \oplus x_2 \oplus 1$, хотя бы одну из функций множества G можно реализовать схемой, используя не более четырех элементов.

Список литературы

1. Редькин Н. П. О полных проверяющих тестах // Математические вопросы кибернетики. — Вып. 2. — М.: Наука, 1989. — С. 198–222.

О ПОСТРОЕНИИ МАТРИЦ ДЕ БРЕЙНА

Д. А. Макаров (Москва)

В данной работе рассмотрены некоторые способы построения матриц, в которых по содержимому подматрицы фиксированного размера можно однозначно определить ее местоположение в матрице.

Основные определения

Определение. $\{a_t\}$ будем называть *последовательностью де Брейна* [1], если: $a_t \in B$, где B — конечное множество мощности c (для удобства будем считать, что $B = \{1, \ldots, c\}$); существует такое n, что для любого i выполнено $a_i = a_{i+c^n}$; наборы $a_i, a_{i+1}, \ldots, a_{i+n-1}$ и $a_j, a_{j+1}, \ldots, a_{j+n-1}$ различны при любых i, j таких, что $|i - j| < c^n$.

Число n будем называть размером *окна* последовательности, а $\{a_t\}$ — последовательностью де Брейна с окном размера n.

Определение. *Окном* размера $n \times m$ в матрице $\{a_{rs}\}$ из N строк и M столбцов будем называть подматрицу из n идущих подряд строк и m идущих подряд столбцов:

$$\begin{pmatrix} a_{i,j} & a_{i,j+1} & \ldots & a_{i,j+m-1} \\ a_{i+1,j} & a_{i+1,j+1} & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ a_{i+n-1,j} & \ldots & \ldots & a_{i+n-1,j+m-1} \end{pmatrix},$$

где $i \leqslant N - n$ и $j \leqslant M - m$.

Определение. Матрицу A с элементами из множества B мощности c будем называть *субдебрейновой с окном* $n \times m$, если все окна $n \times m$ в матрице A различны, и *матрицей де Брейна с окном* $n \times m$, если кроме того число различных окон $n \times m$ в точности равно c^{nm}.

Ранее в качестве двумерного обобщения последовательностей де Брейна рассматривались торы де Брейна (см., например, [2]). Торы де Брейна соответствуют матрицам де Брейна специального вида.

Очевидно, что размер матрицы де Брейна не может быть произвольным, однако субдебрейнова матрица может быть любого размера. Таким образом возникает задача построения субдебрейновой матрицы заданного размера с заданным размером окна, используя множество B по возможности меньшего размера. Из определений субдебрейновой матрицы вытекает неравенство, дающее нижнюю оценку мощности множества B:

$$c \geqslant \sqrt[nm]{(N - n + 1)(M - m + 1)}.$$

Так как все окна в матрице де Брейна и субдебрейновой матрице различны, по заданному содержимому окну можно однозначно определить местоположение в матрице. Далее, помимо собственно построения матриц де Брейна (субдебрейновых матриц), мы будем строить для них алгоритмы, решающие задачу поиска местоположения.

Приведем пример субдебрейновой матрицы с окном 2×2:

$$\begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 2 & 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Для такой матрицы мощность множества B превышает приведенную ранее нижнюю оценку.

Матрица $1 \times M$ с окном 1×2

Построим матрицу де Брейна размера $1 \times M$ с окном 1×2 (фактически, начальный отрезок некоторой последовательности де Брейна с окном размера 2), так, чтобы задача поиска местоположения решалась с помощью константного (не зависящего от M) числа арифметических операций.

Будем строить последовательность $\{a_t\}$ явно. Выделим в множестве B элемент, например 1, который будем называть *закрывающим*. Положим $a_0 = 1$, $a_1 = 1$. Возьмем элемент $2 \in B$ и добавим в последовательность элементы $2, 2$. Зафиксируем элемент $2 \in B$ и добавим в последовательность всевозможные комбинации этого элемента с элементами из B, значения которых больше фиксированного (для удобства будем перебирать комбинации в порядке

возрастания значений элементов из множества B). Когда элементы, значение которых больше чем у фиксированного, закончатся, добавим в последовательность закрывающий элемент 1. Получим последовательность:

$$1, 1, 2, 2, 3, 2, \ldots, c-1, 2, c, 2, 1.$$

Повторим те же действия для элемента $3 \in B$, затем для элемента $4 \in B$ и т.д. Таким образом на k-ом шаге получаем последовательность:

$$\ldots, k-1, c, k-1, 1, k, k, k+1, k, k+2, k, \ldots, k, c, k, 1.$$

На последнем шаге получаем:

$$\ldots, c-1, c, c-1, 1, c, c, 1$$

Из образованного таким образом фрагмента последовательности получается матрица де Брейна с c^2+1 столбцами.

Решением задачи поиска местоположения будет номер столбца, в котором начинается искомое окно. Пусть e — номер столбца, а $(i\,j)$ — искомое окно. В зависимости от значений элементов i и j выберем одну из формул (1), приведенных ниже, и определим e:

$$\begin{array}{ll} j = 1: & e = 2ci - 2c - i^2 + 2i; \\ i = 1, j > 1: & e = 2cj - j^2 + 4j - 4c - 2; \\ 1 < i < j: & e = 2ci - i^2 + 2i - 4c + 2j - 2; \\ 1 < j \leqslant i: & e = 2cj - j^2 + 2j - 4c + 2i - 1. \end{array} \qquad (1)$$

Матрица размером $N \times M$ с окном размера $N \times 2$

Сведем построение такой матрицы к предыдущему случаю. Пусть задано множество $B = \{0, 1, \ldots, c-1\}$. Образуем новое множество $B' = \{1, 2, \ldots, c^N\}$. К множеству B' применим алгоритм, приведенный ранее. Из каждого элемента полученной матрицы вычтем 1.

Заменим каждый элемент на столбец высоты N, подставляя вместо чисел их c-ичные представления, записанные в виде столбца. Для определенности будем считать, что первый элемент столбца это старший разряд c-ичного числа. Получим матрицу размера $N \times (c^{2N}+1)$.

Преобразуем алгоритм поиска местоположения. Пусть окно имеет вид:

$$\begin{pmatrix} a_{N-1} & b_{N-1} \\ \vdots & \vdots \\ a_0 & b_0 \end{pmatrix}.$$

Поставим в соответствие столбцам из окна числа по правилу: $a = \sum\limits_{k=0}^{N-1} a_k c^k + 1$, $b = \sum\limits_{k=0}^{N-1} b_k c^k + 1$. Для полученного окна $(a\,b)$ ищем номер столбца e по формулам (1), заменяя c на c^N.

Матрица размером $3 \times M$ с окном размера 2×2

Построим теперь субдебрейновы матрицы размера $3 \times M$ с окном 2×2. Пусть множество $B = \{0, 1, \ldots, c-1\}$. Рассмотрим пары элементов из B в виде столбцов $\binom{a}{b}$ и образуем новое множество B' из тех пар элементов, для которых выполнено неравенство $a \leqslant b$. Мощность множества B' равна $Q + c$, где $Q = \frac{c(c-1)}{2}$ — количество столбцов вида $\binom{a}{b}$ с $a < b$, а c — количество пар из двух одинаковых элементов.

Сопоставим элементам множества B' числа от 1 до $Q+c$. Пусть $\binom{a}{b} \in B'$, тогда:

1. Если $a = b = 0$, сопоставим столбцу число 1.
2. Если $a = b \neq 0$, сопоставим столбцу число $Q + a$.
3. Если $a < b$, сопоставим столбцу число $(c - 1.5)a - 0.5a^2 + b + 1$.

Полученные числа образуют множество $B'' = \{1, 2, ..., Q + c\}$.

Для множества B'' применим алгоритм построения матриц де Брейна $1 \times M$. В полученной матрице проведем обратную замену — заменим числа на столбцы, соответствующие этим числам. В новой матрице скопируем первую строчку в третью.

При $M \leqslant 0.25c^4 + 0.5c^3 - 0.75c^2 + 1$ первые M столбцов полученной таким образом матрицы будут образовывать субдебрейнову матрицу.

Преобразуем задачу поиска местоположения. Пусть e — номер столбца матрицы, в котором находится левый столбец искомого окна, g — номер строки матрицы, в которой находится первая строчка искомого окна. Пусть искомое окно имеет вид $\begin{pmatrix} u & w \\ v & y \end{pmatrix}$.

Проверим неравенства $u \leqslant v$ и $w \leqslant y$. Из выполнения обоих неравенств вытекает $g = 1$, в противном случае $g = 2$. Если окно находится во второй строке, поменяем в нем местами первую и вторую строчки. С помощью формул, полученных для перехода от множества B' к множеству B'', получаем два числа, соответствующих столбцам в окне. Для этих чисел применим формулы для поиска местоположения в матрице де Брейна $1 \times M$ с окном 1×2. Полученное число будет равно e — номеру столбца, в котором находится окно.

Автор выражает благодарность А. Д. Яшунскому за полезные обсуждения и внимание к работе.

Список литературы

1. de Bruijn N. G. A combinatorial problem // Koninklijke Nederlandse Akademie v. Wetenschappen. —1946. —V. 49. — P. 758–764.

2. Hurlbert G., Isaak G. On the de Bruijn torus problem // Journal of Combinatorial Theory. —1993. — Series A 64 (1). — P. 50–62.

О НИЖНЕЙ ОЦЕНКЕ СТОИМОСТИ КОДИРОВАНИЯ ДЛЯ СТОХАСТИЧЕСКОЙ КС-ГРАММАТИКИ, ИМЕЮЩЕЙ ВИД «ЦЕПОЧКИ», В КРИТИЧЕСКОМ СЛУЧАЕ

И. М. Мартынов (Нижний Новгород)

Введение

При передаче и хранении информации часто возникает необходимость кодирования данных таким образом, чтобы обеспечить наибольшую степень сжатия. Сжатие данных может быть достигнуто использованием статистических данных, таких как частоты появления букв в сообщениях. Если, кроме этого, учитывать структурные свойства языка сообщений, можно дополнительно увеличить эффективность сжатия.

Для учета структурных и вероятностных свойств источника сообщений предлагается описывать его стохастической КС-грамматикой. Рассматриваются грамматики с матрицей первых моментов A специального вида в критическом случае, когда перронов корень матрицы A равен 1. Для таких грамматик исследуется множество деревьев вывода фиксированной высоты, оценивается энтропия множества слов, порожденных такими деревьями, а также стоимость кодирования.

1. Основные определения

Стохастической контекстно-свободной грамматикой [1] называется система $G =< V_T, V_N, R, s >$, где V_T и V_N — конечные множества терминальных и нетерминальных символов (терминалов и нетерминалов) соответственно, $s \in V_N$ — аксиома, $R = \bigcup\limits_{i=1}^{k} R_i$, где k — мощность алфавита V_N, и R_i — множество *правил вывода* вида

$$r_{ij} : A_i \xrightarrow{p_{ij}} \beta_{ij}, \qquad j = 1, \ldots, n_i,$$

где $A_i \in V_N$, $\beta_{ij} \in (V_N \cup V_T)^*$ и p_{ij} — вероятности правил вывода, удовлетворяющие условиям:

$$0 < p_{ij} \leqslant 1, \qquad \sum_{j=1}^{n_i} p_{ij} = 1.$$

Правило вывода $A_i \to \beta_{ij}$ может быть применено к слову из алфавита $V \cup T$ путем замены некоторого нетерминала A_i в этом слове на β_{ij}. Если слово α может быть получено из аксиомы s последовательным применением правил грамматики, говорят, что грамматика порождает слово α. Множество слов, порождаемых грамматикой G, образует язык $L(G)$. Говорят, что грамматика G задает язык L.

Процесс порождения слова в стохастической КС-грамматике можно описать с помощью дерева вывода [2]. Оно строится следующим образом. Вначале корень дерева помечается аксиомой грамматики. Далее, на каждом шаге к некоторому листу дерева, помеченному некоторым нетерминалом A_i, применяется правило из R_i в соответствии с распределением вероятностей p_{ij} $(1 \leqslant j \leqslant n_i)$ правил вывода на этом множестве. Буквы слова, стоящего в правой части правила вывода, присоединяются к выбранному листу в качестве потомков, слева направо. Этот процесс повторяется до тех пор, пока в дереве вывода остаются листья, помеченные нетерминальными символами. Слово α, образованное нетерминалами, помечающими листья полученного дерева, соответствует этому дереву вывода.

Вероятность $p(d)$ дерева вывода d определяется как произведение вероятностей всех правил вывода, примененных при построении дерева. Вероятность $p(\alpha)$ слова α из V_T^* определяется как сумма вероятностей $p(d)$ всех деревьев вывода d, соответствующих данному слову. Если каждому слову, порожденному грамматикой, соответствует единственное дерево вывода, такую грамматику называют *грамматикой с однозначным выводом.*

По стохастической КС-грамматике строится матрица $A = (a_j^i)$ первых моментов. Ее элемент a_j^i определяется как $\sum\limits_{k=1}^{n_i} p_{ik} s_{ik}^j$, где величина s_{ik}^j равна числу нетерминальных символов A_j в правой части правила r_{ik}. Перронов корень [3] матрицы A обозначим через r.

Будем говорить, что нетерминал A_j непосредственно выводится из нетерминала A_i (и обозначать $A_i \to A_j$), если в грамматике существует правило вида $A_i \xrightarrow{p_{ij}} \alpha_1 A_j \alpha_2$, где $\alpha_1, \alpha_2 \in (V_T \cup V_N)^*$. Рефлексивное транзитивное замыкание отношения $\to$ обозначим $\to_*$.

Классом нетерминалов назовем максимальное по включению подмножество $K \subseteq V_N$ такое, что $A_i \to_* A_j$ для любых $A_i, A_j \in K$. Для различных классов нетерминалов K_1 и K_2 будем говорить, что класс K_2 непосредственно следует за классом K_1 (и обозначать $K_1 \prec K_2$), если существуют $A_1 \in K_1$ и $A_2 \in K_2$, такие, что $A_1 \to A_2$. Рефлексивное транзитивное замыкание отношения $\prec$ обозначим через $\prec_*$.

Пусть $\mathcal{K} = \{K_1, K_2, \ldots, K_m\}$ — множество классов нетерминалов грамматики, $m \geqslant 2$. Будем полагать, что классы нетерминалов пронумерованы таким образом, что $K_i \prec_* K_j$ тогда и только тогда, когда $i < j$.

Будем говорить, что грамматика имеет вид «цепочки», если ее матрица первых моментов A имеет вид

$$\begin{pmatrix} A_{11} & A_{12} & 0 & \cdots & 0 & 0 \\ 0 & A_{22} & A_{23} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & A_{m-1,m-1} & A_{m-1,m} \\ 0 & 0 & 0 & \cdots & 0 & A_{m,m} \end{pmatrix} \tag{1}$$

Один класс нетерминалов представлен в матрице множеством подряд идущих строк и соответствующим множеством столбцов с теми же номерами. Для класса K_i квадратная подматрица, образованная соответствующими строками и столбцами, обозначается через A_{ii}. Подматрица A_{ij} является нулевой, если $K_i \not\prec K_j$. Блоки, расположенные ниже главной диагонали, нулевые в силу упорядоченности классов.

Для грамматики с матрицей первых моментов вида (1) классы нетерминалов образуют линейный порядок по отношению $\prec$:

$$K_1 \prec K_2 \prec \ldots \prec K_i \prec \ldots \prec K_m.$$

Для каждого класса K_i матрица A_{ii} неразложима. Без ограничения общности будем считать, что она строго положительна и непериодична. Обозначим через r_i перронов корень матрицы A_{ii}. Для неразложимой матрицы перронов корень является вещественным и простым. Очевидно, $r = \max\limits_i \{r_i\}$.

2. Полученные результаты

Пусть $J = \{i_1, i_2, \ldots, i_l\}$ — множество всех номеров i_j классов, для которых $r_{i_j} = 1$.

Рассмотрим подцепочку классов

$$K_j \prec K_{j+1} \prec \ldots \prec K_m,$$

такую что $j \in J$, и $i \notin J$ для любого $i > j$. Обозначим через $I = \{j, j+1, \ldots, m\}$ множество индексов классов этой подцепочки.

Будем также обозначать через D^t множество деревьев вывода высоты t, которые могут быть получены при выводе слов в грамматике. Множество слов, соответствующих таким деревьям вывода, обозначим L^t.

Тогда верна следующая теорема:

Теорема 1. *Энтропия множества деревьев вывода D^t выражается формулой*

$$H(D^t) \sim \sum_{i \in I} \sum_{j=1}^{n_i} d_i H(R_i) \cdot t^2,$$

где $H(R_i) = \sum\limits_{j=1}^{n_i} p_{ij} \log p_{ij}$ *— энтропия множества* R_i*, и* $d_i > 0$ *— некоторые вычислимые константы.*

Энтропия $H(D^t)$ имеет асимптотику t^2, причем константа при t^2 определяется нетерминалами из наиболее удаленного от начала цепочки критического класса, а также классами следующими за ним.

Через f^* обозначим кодирование языка L^t, минимизирующее величину

$$M_t(f) = \sum_{\alpha \in L^t} p_t(\alpha) \cdot |f(\alpha)|\,,$$

где f — схема кодирования и $p_t(\alpha)$ — условная вероятность слова α при $\alpha \in L^t$. Будем также предполагать, что рассматриваемая грамматика является грамматикой с однозначным выводом. Тогда верна следующая теорема:

Теорема 2. *Пусть матрица* A *первых моментов грамматики имеет вид* (1) *и ее перронов корень* $r = 1$*. Тогда стоимость* $C(L, f)$ *любого кодирования* f *языка* L*, порождаемого этой грамматикой, удовлетворяет неравенству*

$$C(L, f) \geqslant C^*(L),$$

где

$$C^*(L) = \frac{\sum\limits_{i \in I} d_i H(R_i)}{\sum\limits_{i \in I} d_i L(R_i)},$$

где, в свою очередь, $H(R_i) = -\sum\limits_{j=1}^{n_i} p_{ij} \log p_{ij}$*,* $L(R_i) = \sum\limits_{j=1}^{n_i} l_{ij} p_{ij}$*,* l_{ij} *— число терминальных символов в правой части правила* r_{ij}*, и* $d_i > 0$ *— некоторые вычислимые константы.*

Список литературы

1. Фу К. Структурные методы в распознавании образов. — М.: Мир, 1977.
2. Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции. Том 1. — М.: Мир, 1978.
3. Гантмахер Ф. Р. Теория матриц. — 5-е изд. — М.: ФИЗМАТЛИТ, 2010.

О БАЗИРУЕМОСТИ ЗАМКНУТЫХ КЛАССОВ ФУНКЦИЙ ТРЕХЗНАЧНОЙ ЛОГИКИ, ПОРОЖДЕННЫХ СИММЕТРИЧЕСКИМИ ФУНКЦИЯМИ С ОГРАНИЧЕННЫМ ЧИСЛОМ СЛОЕВ

А. В. Михайлович (Москва)

Рассматриваются замкнутые классы функций трехзначной логики, порожденные немонотонными симметрическими функциями с ограниченным числом слоев. Известно [1], что все замкнутые классы булевых функций имеют конечный базис. В [2] показано, что при всех $k \geqslant 3$ в P_k существуют как замкнутые классы со счетным базисом, так и классы, не имеющие базиса. В [3, 4] рассмотрены некоторые семейства замкнутых классов, порождающие системы которых содержат немонотонные симметрические функции; для них приведены критерии базируемости и конечной порожденности. В данной работе рассматриваются семейства классов, порожденных симметрическими функциями с ограниченным числом слоев. При этом критерий базируемости остается прежним, а критерий конечной порожденности меняется. Все необходимые определения можно найти в [3–5].

Обозначим через R множество всех функций трехзначной логики, принимающих значения только из множества $\{0, 1\}$ и равных нулю на единичном наборе и на всех наборах, содержащих хотя бы одну нулевую компоненту. Функции f и g из R называются *конгруэнтными*, если одна из них получается из другой переименованием переменных без отождествления. Пусть Φ — некоторая формула над R. Множество всех функций, символы которых содержатся в формуле Φ, обозначим через $\Theta(\Phi)$. Пусть $f(x_1, \ldots, x_n) \in R$. Будем обозначать через N_f множество всех наборов из E_3^n, на которых функция f принимает значение 1. Множество всех наборов из E_3^n, которые получаются друг из друга перестановкой компонент, называется *слоем*. Функцию $f(x_1, \ldots, x_n)$ из R будем называть *симметрической*, если для любого слоя $\mathcal{L} \subseteq E_3^n$ и любых двух наборов $\widetilde{\alpha}$, $\widetilde{\beta}$ из $\mathcal{L}$ выполняется равенство $f(\widetilde{\alpha}) = f(\widetilde{\beta})$. Функцию $f(x_1, \ldots, x_n)$ из R будем называть *m-слойной симметрической функцией*, если существует m различных слоев $\mathcal{L}_1, \ldots, \mathcal{L}_m$, $m \geqslant 1$, таких, что $N_f = \mathcal{L}_1 \cup \ldots \cup \mathcal{L}_m$. Функцию из R будем называть *монотонной*, если она монотонна относительно порядка $0 < 1 < 2$ на множестве E_3. Множество всех немонотонных m-слойных симметрических функций обозначим через NS^m. Множество всех немонотонных симметрических функций обозначим через NS. Положим $\mathrm{NS}^{(m)} = \cup \mathrm{NS}^i$, где объединение берется по всем i, $1 \leqslant i \leqslant m$.

Пусть $f, g \in \mathrm{NS}^{(m)}$, $m \geqslant 1$, $A \subseteq R$. Будем говорить, что функция f не превосходит функцию g относительно $\preceq_A$, если $f \in [\{g\} \cup A]$. Будем говорить, что функции f и g эквивалентны относительно A (обозначение $f \sim_A g$),

если $[\{f\} \cup A] = [\{g\} \cup A]$. Если $A = \varnothing$, то индекс будем опускать. Зафиксируем множество A. Множество $H \subset \mathrm{NS}^{(m)} \backslash [A]$ называется *цепью*, если любые два элемента множества H сравнимы относительно порядка $\preceq_A$. Пусть $G \subseteq \mathrm{NS}^{(m)} \backslash [A]$. Цепь $H \subseteq G$ называется *максимальной цепью* множества G, если для любой цепи $H_1 \subset \mathrm{NS}^{(m)} \backslash [A]$, такой, что $H \subseteq H_1$ и $H \neq H_1$, цепь H_1 не является подмножеством множества G. Функция $f \in H$ называется *верхней гранью* цепи H, если для любой функции $g \in H$ выполняется неравенство $g \preceq_A f$. Цепь называется *ограниченной*, если она имеет верхнюю грань.

Лемма 1. *Пусть* $f(x_1, \ldots, x_n) \in \mathrm{NS}^l$, $l \geqslant 1$, Φ — *формула над* NS, *реализующая функцию* f, *а* Φ_1 — *подформула формулы* Φ, *имеющая вид* $g(\mathcal{B}_1, \ldots, \mathcal{B}_m)$, *где* $\mathcal{B}_1, \ldots, \mathcal{B}_m$ — *формулы над* NS, $g \in \mathrm{NS}^r$, $r \leqslant l$. *Тогда среди формул* $\mathcal{B}_1, \ldots, \mathcal{B}_m$ *есть символы переменных, причем символ каждой переменной из множества* $\{x_1, \ldots, x_n\}$ *встречается одинаковое число раз.*

Доказательство леммы аналогично доказательству утверждения 1 из [3].

Следствие 1. *Пусть* $f(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_m) \in \mathrm{NS}^l$, $l \geqslant 1$, Φ *и* Ψ — *формулы над* NS, *реализующие функции* f *и* g *соответственно. Пусть существуют подформулы* Φ_1 *и* Ψ_1 *формул* Φ *и* Ψ, *имеющие вид* $g(\mathcal{B}_1, \ldots, \mathcal{B}_m)$ *и* $f(\mathcal{C}_1, \ldots, \mathcal{C}_n)$ *соответственно, где* $\mathcal{B}_1, \ldots, \mathcal{B}_m$, $\mathcal{C}_1, \ldots, \mathcal{C}_n$ — *формулы над* NS. *Тогда функции* f *и* g *конгруэнтны, а формулы* Φ_1 *и* Ψ_1 — *простые.*

Теорема 1 [3]. *Пусть* G — *произвольное множество попарно неконгруэнтных функций из* NS^1, $F = [G]$. *Тогда справедливы следующие утверждения.*

1. *Класс* F *имеет конечный базис тогда и только тогда, когда множество* G *содержит конечное число функций.*

2. *Класс* F *имеет счетный базис тогда и только тогда, когда* G *содержит счетное число функций и каждая функция, принадлежащая* G, *содержится в некоторой ограниченной максимальной цепи множества* G *относительно порядка* $\preceq$.

3. *Класс* F *не имеет базиса тогда и только тогда, когда найдется функция* $h \in G$, *такая, что* h *не лежит ни в какой ограниченной максимальной цепи множества* G *относительно порядка* $\preceq$.

Лемма 2 [4]. *Если множество* F *содержит счетное число попарно неконгруэнтных немонотонных симметрических функций и* $F \subseteq R$, *то класс* $G = [F]$ *не имеет конечного базиса.*

Лемма 3. *Пусть* $G \subseteq \mathrm{NS}^{(k)}$, $G^l = G \cap \mathrm{NS}^l$, $H^l = G \backslash \mathrm{NS}^{(l)}$, $1 \leqslant l \leqslant k$, $F = [G]$. *Пусть класс* F *имеет базис* $\mathfrak{A}$. *Тогда существует множество* $\mathfrak{A}^l \subseteq \mathfrak{A}$, *которое является базисом класса* $[H^l]$.

Доказательство леммы основано на том, что любая формула над R, реализующая l-слойную функцию, не содержит символов функций, принимающих значение 1 на меньшем числе слоев.

Лемма 4. *Пусть* $G \subseteq \mathrm{NS}^{(k)}$, $G^l = G \cap \mathrm{NS}^l$, $H^l = G \backslash \mathrm{NS}^{(l)}$, $1 \leqslant l \leqslant k$. *Пусть класс* $[H^l]$ *имеет базис. Тогда класс* $[H^{l-1}]$ *имеет базис тогда и только тогда, когда каждая функция множества* $G^l \backslash [H^l]$ *содержится в ограниченной максимальной цепи множества* $G^l \backslash [H^l]$ *относительно порядка* $\preceq_{H^l}$.

Доказательство. Обозначим через $\mathfrak{B}$ множество верхних граней множества $G^l \backslash [H^l]$ относительно порядка $\preceq_{H^l}$.

Необходимость. Пусть класс H^{l-1} имеет базис $\mathfrak{A}$. Для каждой функции f из $\mathfrak{A}$ зафиксируем формулу Υ_f над G, реализующую функцию f. Пусть Φ — произвольная формула над $\mathfrak{A}$. Заменим в формуле Φ каждую из функций базиса $\mathfrak{A}$ на соответствующую ей подформулу над G. Полученную формулу над G обозначим через $\pi(\Phi)$. В силу леммы 3 класс $[H^l]$ имеет базис $\mathfrak{A}^l \subseteq \mathfrak{A}$.

Пусть $f(x_1, \ldots, x_n) \in \mathfrak{A} \backslash \mathfrak{A}^l$. Тогда существует функция g из $\Theta(\Upsilon_f) \backslash [H^l]$. Пусть $g \notin \mathfrak{B}$. Тогда существует функция $g' \in G^l \backslash [H^l]$, такая, что $g \preceq_{H^l} g'$, $g \not\sim_{H^l} g'$. Покажем тогда, что $g' \in [\mathfrak{A} \backslash \{f\}]$. В самом деле, если $g' \notin [\mathfrak{A} \backslash \{f\}]$, то существует формула Ψ над $\mathfrak{A}$, реализующая функцию g' и содержащая подформулу, имеющую вид $f(\mathcal{B}_1, \ldots, \mathcal{B}_n)$, где $\mathcal{B}_1, \ldots, \mathcal{B}_n$ — формулы над $\mathfrak{A}$. Тогда формула $\pi(\Psi)$ над H^{l-1} реализует функцию g' и содержит подформулу, имеющую вид $g(\mathcal{C}_1, \ldots, \mathcal{C}_m)$, где $\mathcal{C}_1, \ldots, \mathcal{C}_m$ — формулы над H^{l-1}. В силу следствия 1 функции g и g' являются конгруэнтными. Получили противоречие. Следовательно, $g' \in [\mathfrak{A} \backslash \{f\}]$.

Нетрудно показать, что существует функция $h \in \Theta(\Upsilon_f) \cap \mathfrak{B}$, для которой выполняется соотношение $h \notin [\mathfrak{A} \backslash \{f\}]$. Кроме того, используя следствие 1, получаем, что формула Υ_f содержит простую подформулу, имеющую вид $h(x_{i_1}, \ldots, x_{i_m})$.

Рассмотрим функцию $g(x_1, \ldots, x_n)$ из $G^l \backslash [H^l]$. Пусть Φ — формула над $\mathfrak{A}$, реализующая функцию g. Рассмотрим два случая.

Пусть формула $\pi(\Phi)$ содержит простую подформулу $h(x_{i_1}, \ldots, x_{i_m})$, такую, что $h \in \mathfrak{B}$. В силу леммы 1 существует $q \in \mathbb{N}$, такое, что среди $x_{i_1}, \ldots, x_{i_m}$ каждая переменная из $\{x_1, \ldots, x_n\}$ встречается q раз. Нетрудно видеть, что тогда выполняется равенство $g(x_1, \ldots, x_n) = h(x_1^q, \ldots, x_n^q)$.

Пусть теперь формула $\pi(\Phi)$ не содержит простых подформул, которые являются формулами над $\mathfrak{B}$. Предположим, что все простые подформулы формулы $\pi(\Phi)$ являются формулами над $G^l \backslash ([H^l] \cup \mathfrak{B})$. Тогда существует функция f из $\mathfrak{A} \backslash \mathfrak{A}^l$, такая, что все простые подформулы формулы Υ_f являются формулами над $G^l \backslash ([H^l] \cup \mathfrak{B})$. Это противоречит доказанному выше. Следовательно, существует простая подформула формулы $\pi(\Phi)$, которая является формулой над H^l. Обозначим эту формулу через Ψ. Пусть f — некоторая функция из $\Theta(\Phi) \backslash \mathfrak{A}^l$, а $h(x_{i_1}, \ldots, x_{i_s})$ — простая подформула формулы Υ_f, причем $h \in \mathfrak{B}$. Тогда существует подформула Φ_1 формулы $\pi(\Phi)$, имеющая

вид $h(\mathcal{B}_1, \ldots, \mathcal{B}_m)$. В силу леммы 1 существует число q из $\mathbb{N}$, такое, что среди формул $\mathcal{B}_1, \ldots, \mathcal{B}_m$ каждая переменная из $\{x_1, \ldots, x_n\}$ встречается q раз. Без ограничения общности будем считать, что $\mathcal{B}_1, \ldots, \mathcal{B}_{qn}$ — символы переменных, а $\mathcal{B}_{qn+1}, \ldots, \mathcal{B}_m$— нетривиальные формулы. Нетрудно видеть, что тогда

$$g(x_1, \ldots, x_n) = h(x_1^q, \ldots, x_n^q, \underbrace{\Psi, \ldots, \Psi}_{m-qn}).$$

Таким образом получаем, что любая функция g из $G^l \backslash [H^l]$ содержится в ограниченной максимальной цепи множества $G^l \backslash [H^l]$ относительно $\preceq_{H^l}$.

Достаточность. Пусть $\mathfrak{A}^l$ — базис класса $[H^l]$. Покажем, что множество $\mathfrak{A}^l \cup \mathfrak{B}$ является базисом класса $[H^{l-1}]$. Нетрудно видеть, что $[H^{l-1}] = [\mathfrak{A}^l \cup \mathfrak{B}]$. Покажем, что для любой функции f из $\mathfrak{A}^l \cup \mathfrak{B}$ выполняется соотношение $f \notin [(\mathfrak{A}^l \cup \mathfrak{B}) \backslash \{f\}]$. Предположим, что $f \in [(\mathfrak{A}^l \cup \mathfrak{B}) \backslash \{f\}]$. Рассмотрим два случая.

Пусть $f \in \mathfrak{A}^l$. В силу леммы 3 функция f содержится в $[\mathfrak{A}^l \backslash \{f\}]$. Это противоречит тому, что множество $\mathfrak{A}^l$ является базисом класса $[H^l]$. Следовательно, $f \notin [(\mathfrak{A}^l \cup \mathfrak{B}) \backslash \{f\}]$.

Пусть теперь $f(x_1, \ldots, x_n) \in \mathfrak{B}$. Пусть Φ — формула над $(\mathfrak{A}^l \cup \mathfrak{B}) \backslash \{f\}$, реализующая функцию f. Рассмотрим два подслучая. Пусть формула Φ содержит простую подформулу $g(x_{i_1}, \ldots, x_{i_m})$, такую, что $g \in \mathfrak{B}$. В силу леммы 1 существует $q \in \mathbb{N}$, такое, что среди $x_{i_1}, \ldots, x_{i_m}$ каждая переменная из $\{x_1, \ldots, x_n\}$ встречается q раз. Нетрудно видеть, что тогда выполняется равенство $f(x_1, \ldots, x_n) = g(x_1^q, \ldots, x_n^q)$. Таким образом, существует функция $g \in \mathfrak{B} \backslash \{f\}$, такая, что $f \in [\{g\}]$. А значит, функция f не является верхней гранью. Получили противоречие.

Пусть теперь формула Φ содержит простую подформулу Φ_1, которая является формулой над $\mathfrak{A}^l$. Поскольку $f \notin [\mathfrak{A}^l]$, то существует подформула Φ_1 формулы $\pi(\Phi)$, имеющая вид $h(\mathcal{B}_1, \ldots, \mathcal{B}_m)$, где $h \in \mathfrak{B}$, а $\mathcal{B}_1, \ldots, \mathcal{B}_m$ — формулы над $(\mathfrak{A}^l \cup \mathfrak{B}) \backslash \{f\}$. В силу леммы 1 существует число q из $\mathbb{N}$, такое, что среди $\mathcal{B}_1, \ldots, \mathcal{B}_m$ каждая переменная из $\{x_1, \ldots, x_n\}$ встречается q раз. Без ограничения общности будем считать, что $\mathcal{B}_1, \ldots, \mathcal{B}_{qn}$ — символы переменных, а $\mathcal{B}_{qn+1}, \ldots, \mathcal{B}_m$— нетривиальные формулы. Нетрудно видеть, что тогда

$$f(x_1, \ldots, x_n) = h(x_1^q, \ldots, x_n^q, \underbrace{\Psi, \ldots, \Psi}_{m-qn}).$$

Следовательно, существует функция $h \in \mathfrak{B} \backslash \{f\}$, такая, что $f \in [\{h\} \cup \mathfrak{A}^l]$. А значит, функция f не является верхней гранью. Получили противоречие. Следовательно, $f \notin [(\mathfrak{A}^l \cup \mathfrak{B}) \backslash \{f\}]$. А значит, класс $[H^{l-1}]$ имеет базис.

Теорема 2. *Пусть G — множество попарно неконгруэнтных функций из $\mathrm{NS}^{(k)}$, $G^l = G \cap \mathrm{NS}^l$, $H^l = G \backslash \mathrm{NS}^{(l)}$, $1 \leqslant l \leqslant k$, $F = [G]$. Тогда выполняются следующие условия.*

1. *Класс F имеет конечный базис тогда и только тогда, когда множество G конечно.*

2. *Класс F имеет счетный базис тогда и только тогда, когда G содержит счетное число функций и для любого l, $1 \leqslant l \leqslant k$, каждая функция множества $G^l \backslash [H^l]$ содержится в ограниченной максимальной цепи множества $G^l \backslash [H^l]$ относительно порядка $\preceq_{H^l}$.*

3. *Класс F не имеет базиса тогда и только тогда, когда существует m, $1 \leqslant m \leqslant k$, и существует функция $h \in G^m \backslash [H^m]$, которая не содержится ни в какой ограниченной максимальной цепи множества $G^m \backslash [H^m]$ относительно порядка $\preceq_{H^m}$.*

Доказательство. 1. Необходимость следует из леммы 2. Достаточность очевидна.

2. Необходимость. Пусть класс F имеет базис $\mathfrak{A}$. В силу леммы 3 для любого l, $1 < l \leqslant k$, существуют множества $\mathfrak{A}^l \subseteq \mathfrak{A}$ и $\mathfrak{A}^{l-1} \subseteq \mathfrak{A}$, которые являются базисами классов H^l и H^{l-1} соответственно. В силу леммы 4 получаем, что каждая функция множества $G^l \backslash [H^l]$ содержится в ограниченной максимальной цепи множества $G^l \backslash [H^l]$ относительно порядка $\preceq_{H^l}$.

Доказательство достаточности будем вести индукцией по l от k до 1. База индукции. Рассмотрим множество G^k. Поскольку $H^k = \varnothing$, то порядок $\preceq_{H^k}$ совпадает с порядком $\preceq$. В силу теоремы 1 класс $[G^k]$ имеет базис. Отметим, что $G^k = H^{k-1}$. Следовательно, класс $[H^{k-1}]$ имеет базис.

Пусть теперь класс H^l имеет базис, $0 < l < k$. Покажем, что класс H^{l-1} имеет базис. По условию каждая функция множества $G^l \backslash [H^l]$ содержится в ограниченной максимальной цепи множества $G^l \backslash [H^l]$ относительно порядка $\preceq_{H^l}$. В силу леммы 4 класс $[H^{l-1}]$ имеет базис.

3. Доказательство пункта 3 следует из пунктов 1 и 2.

Список литературы

1. Post E. L. The two-valued iterative systems of mathematical logic. // Annals of Math. Studies. — Princeton Univ. Press, 1941. — 122 p.
2. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса. // ДАН СССР. — 1959. — 127, № 1. — С. 44–46.
3. Михайлович А. В. О замкнутых классах трехзначной логики, порожденных симметрическими функциями // Вестн. Моск. ун-та. Матем. Механ. — 2008. — № 4. — С. 54–57.
4. Михайлович А. В. О свойствах замкнутых классов функций трехзначной логики, порожденных симметрическими функциями // Материалы X Международного семинара «Дискретная математика и ее приложения» (Москва, 1–6 февраля 2010 г.). — Москва: Изд-во механико-математического факультета МГУ, 2010. — С. 193–196.

5. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2001. — 384 с.

О ДИАГНОСТИЧЕСКИХ ТЕСТАХ ОТНОСИТЕЛЬНО СЛИПАНИЙ ПЕРЕМЕННЫХ В БУЛЕВЫХ ФУНКЦИЯХ

Е. В. Морозов (Москва)

Введение

Будем говорить, что в булевой функции $f(x_1, \ldots, x_n)$ произошло Ф-*слипание* переменных $x_{i_1}, \ldots, x_{i_k}$, если вместо исходной функции реализуется булева функция, полученная из нее подстановкой вместо каждой из переменных $x_{i_1}, \ldots, x_{i_k}$ функции $\varphi(x_{i_1}, \ldots, x_{i_k})$, где функция $\varphi \in \Phi$, φ будем также называть *функцией слипания*. Через $\Psi = \Psi_{n,f,\Phi}$ обозначим множество функций, в которое входит $f(x_1, \ldots, x_n)$ и всевозможные булевы функции, получающиеся из $f(x_1, \ldots, x_n)$ в результате Ф-слипаний. Ф-слипаний называется k-кратным, если слипаются ровно k переменных. Множество наборов T назовем *диагностическим тестом для функции* $f(x_1, \ldots, x_n)$, если для любой пары неравных функций из Ψ в T найдется набор, на котором эти функции принимают разные значения. Традиционным образом введем *функцию Шеннона длины диагностического теста относительно* Ф-*слипаний переменных* $L_\Phi(n)$, как максимум по всем булевым функциям длины минимального диагностического теста относительно Ф-слипаний. В качестве множества Φ будем рассматривать: $\Phi_\vee$, содержащее все функции вида $g(x_1, \ldots, x_k) = x_1 \vee x_2 \vee \ldots x_k$; Φ_{lin}, содержащее все функции вида $g(x_1, \ldots, x_k) = x_1 \oplus x_2 \oplus \ldots \oplus x_k \oplus \sigma$. Соответствующие множества функций неисправности будем обозначать через $\Psi_\vee, \Psi_{lin}$, а соответствующие функции Шеннона — $L_{\Phi_\vee}(n)$, $L_{\Phi_{lin}}(n)$. Также будем рассматривать Ф-слипания кратности, не выше k, тогда: $\Phi^k = \{g(x_1, \ldots, x_i) \mid g(x_1, \ldots, x_i) \in \Phi, i \leqslant k\}$. Тогда множество функций неисправности обозначим через Ψ_{Φ^k}, а функцию Шеннона — через $L_{\Phi^k}(n)$.

Теорема 1. *Пусть* Φ *— такое множество функций, что для любого* k *найдется* $g(y_1, \ldots, y_k) \in \Phi$. *Тогда для функции Шеннона* $L_\Phi(n)$ *при некоторой положительной константе* C_1 *справедлива нижняя оценка* $L_\Phi(n) \gtrsim C_1 \frac{2^{\frac{n}{2}}}{\sqrt[4]{n}}$.

Доказательство. Заметим, что если в некоторой элементарной конъюнкции $x_1^{\sigma_1} x_2^{\sigma_2} \ldots x_m^{\sigma_m}$ произошло слипание, в котором участвуют переменные

x_i, x_j такие, что $\sigma_i \neq \sigma_j$, то данная конъюнкция обратится в ноль, поскольку вместо переменных, входящих к конъюнкцию с разными степенями, будет подставлена одна и та же величина. Воспользуемся данным наблюдением и построим функцию, схожую использованной Носковым [1] для константных неисправностей. Сначала будем предполагать, что для любого k найдется $g(y_1, \ldots, y_k) \in \Phi$, не равная тождественному нулю. Опишем функцию, на которой достигается нижняя оценка:

$$h(x_1, \ldots, x_n) = \bigvee_{\sigma_2+\sigma_3+\ldots+\sigma_m=\left\lceil \frac{m}{2} \right\rceil - 1} x_1 x_2^{\sigma_2} \ldots x_m^{\sigma_m} x_{m+1}^{\delta_1(\tilde{\sigma^m})} \ldots x_n^{\delta_{n-m}(\tilde{\sigma^m})},$$

причем разным векторам $\tilde{\sigma}$ соответствуют разные вектора $\tilde{\delta}(\tilde{\sigma})$. Найдем m, при котором число слагаемых в описанной ДНФ будет близко к максимальному.

Число всевозможных векторов $\tilde{\sigma}$, равное $C_{m-1}^{\left\lceil \frac{m}{2} \right\rceil - 1}$, тем больше, чем больше m. Число всевозможных векторов $\tilde{\delta}$ равно 2^{n-m}, при этом должно выполняться неравенство $2^{n-m} \geqslant C_{m-1}^{\left\lceil \frac{m}{2} \right\rceil - 1}$. Используя известное асимптотическое равенство для биномиальных коэффициентов при $m \to \infty$ получаем: $2^{n-m} \geqslant a \frac{2^{m-1}}{\sqrt{\frac{\pi m}{2}}}$, где a — некоторая константа.

Разделим на обе части неравенства на 2^{m-1}, прологарифмируем и получим неравенство $n - 2m + 1 \geqslant \log \frac{1}{\sqrt{\frac{\pi m}{2}}}$. Представим m в виде $\frac{n}{2} + t$, тогда $2t - 1 \leqslant \log \sqrt{\frac{n}{2} + t} - \log \sqrt{\frac{\pi}{2}}$. Учтем, что $t \leqslant \frac{n}{2}$, отбросим последнее слагаемое, тогда получим, что $t \leqslant \frac{1}{2} \log n + \frac{1}{2}$. Отсюда следует, что $2t - 1 \leqslant \log \sqrt{\frac{n}{2} + \frac{1}{2} \log n + \frac{1}{2}} - \log \sqrt{\frac{\pi}{2}}$. При $t = \frac{1}{4} \log n - 1$ данное неравенство верно, максимально допустимое t асимптотически не превышает выбранное значение. Итак, положим $m = \left\lfloor \frac{n}{2} + \frac{1}{4} \log n \right\rfloor - 1$.

Тождественный нуль получается из $h(x_1, \ldots, x_n)$ слипанием всех переменных. Чтобы получить требуемую оценку, достаточно оценить снизу мощность множества наборов, отличающего нуль от других функций неисправности.

Предположим, что произошло слипание некоторых $\left\lceil \frac{m}{2} \right\rceil - 1$ переменных из $x_2, \ldots, x_m$ и переменной x_1, а функция слипания — некоторая отличная от нуля функция. Во всех слагаемых выбранной ДНФ, кроме одного, степени хотя бы двух неисправных переменных различны, следовательно только одно слагаемое может быть не равно тождественному нулю. В то же время данное слагаемое не равно нулю только при $x_{m+1} = \delta'_1, \ldots, x_n = \delta'_{n-m}$, где вектор значений $\tilde{\delta}$ соответствует выбранному вектору $\tilde{\sigma}$. Поскольку среди функций слипания есть ненулевая функция, функция неисправности так же будет ненулевой.

Значит, наборы, на которых функции неисправности, получающиеся при слипании разных m переменных из $x_2, \ldots, x_m$ и переменной x_1, отличны от

нуля, не пересекаются. Тогда, чтобы отличить каждую из выбранных функций неисправности от тождественного нуля, потребуется столько же булевых наборов, сколько имеется функций неисправности. Их число равно $C_{m-1}^{\lceil \frac{m}{2} \rceil - 1}$. Заменяем m на $\lfloor \frac{n}{2} + \frac{1}{4}\log n - 1 \rfloor$, снова воспользуемся асимптотическим равенством для биномиальных коэффициентов, получаем требуемую оценку. Переходя к пределу в последнем выражении, учитывая, что в $P_2(n)$ есть ненулевая функция при любом числе переменных, получаем необходимую оценку.

Если же при каком-то n в множестве Φ не будет необходимой отличной от нуля функции, рассуждая двойственным образом, получаем нужную оценку.

Введем несколько обозначений. Через $f^{g(x_{i_1},\ldots,x_{i_k})}_{x_{i_1},\ldots,x_{i_k}}(x_1,\ldots,x_n)$ будем обозначать функцию неисправности, получающуюся из $f(x_1,\ldots,x_n)$ в результате слипания переменных $x_{i_1},\ldots,x_{i_k}$ с функцией слипания $g(x_{i_1},\ldots,x_{i_k})$. Для набор $\tilde{\alpha}$ через $|\tilde{\alpha}|$ обозначим число единиц в данном наборе.

Теорема 2. *Для функции Шеннона $L_{\Phi_\vee}(n)$ при некоторой положительной константе C_2 справедлива нижняя оценка $L_{\Phi_\vee}(n) \gtrsim C_2 \frac{2^n}{\sqrt{n}}$.*

Доказательство. В нижеследующих рассуждениях будем говорить, что набор $\tilde{\alpha}$ *переходит* в набор $\tilde{\beta}$ в результате слипания переменных $x_{i_1},\ldots,x_{i_p}$, если $\beta_j = \alpha_{i_1} \vee \alpha_{i_2} \vee \ldots \vee \alpha_{i_p}$ при $j \in \{i_1,\ldots,i_p\}$ и $\beta_j = \alpha_j$ в противном случае.

Рассмотрим сначала нечетное n. Тогда $\lceil \frac{n}{2} \rceil = \lfloor \frac{n}{2} \rfloor + 1$. Возьмем функцию $h(x_1,\ldots,x_n)$, равную единице на всех наборах $\tilde{\alpha}$, для которых $|\tilde{\alpha}| = \lfloor \frac{n}{2} \rfloor$ и нулю на всех остальных. Сузим класс возможных неисправностей до слипаний кратности $\lceil \frac{n}{2} \rceil$. В результате дизъюнктивного слипания переменных набор $\tilde{\beta}$ переходит в набор $\tilde{\beta}'$ так, что $|\tilde{\beta}'| \geqslant |\tilde{\beta}|$. Поэтому если $|\tilde{\beta}| \geqslant \lceil \frac{n}{2} \rceil$, то на наборе $\tilde{\beta}$ значение любой из возможных функций неисправности равно нулю. Если $|\tilde{\beta}| < \lfloor \frac{n}{2} \rfloor$ и в слипании участвуют только переменные, на местах которых в наборе $\tilde{\beta}$ стоит ноль, данный набор не изменится и значение функции неисправности будет равно нулю. Если же в слипании участвует хотя бы одна переменная, значение которой на наборе $\tilde{\beta}$ равно единице, то он перейдет в некоторый набор $\tilde{\beta}'$, для которого верно $|\tilde{\beta}'| \geqslant \lceil \frac{n}{2} \rceil$, в силу того, что кратность рассматриваемых слипаний равна $\lceil \frac{n}{2} \rceil$. Поэтому значение функций неисправности также будет равно нулю. Таким образом получается, что функции могут различаться только на наборах $\tilde{\alpha} : |\tilde{\alpha}| = \lfloor \frac{n}{2} \rfloor$.

Пусть $X' = \{x_{i_1},\ldots,x_{i_{\lceil \frac{n}{2} \rceil}}\}$, $X'' = \{x_{j_1},\ldots,x_{j_{\lceil \frac{n}{2} \rceil}}\}$, и пусть $h^{X'}_{x_{i_1} \vee \ldots \vee x_{i_{\lceil \frac{n}{2} \rceil}}}$ и $h^{X''}_{x_{j_1} \vee \ldots \vee x_{j_{\lceil \frac{n}{2} \rceil}}}$ — две различные функции неисправности.

Заметим, что если в наборе $\tilde{\alpha}$ есть хотя бы одна единица в позициях, соответствующих переменным из X' и хотя бы одна единица в позициях, соответствующих переменных из X'', то обе функции будут равны нулю на данном наборе в силу кратности рассматриваемых слипаний. Тогда функции могут отличаться от нуля только на наборах, у которых в позициях $i_1,\ldots,i_{\lceil \frac{n}{2} \rceil}$ или

$j_1, \ldots, j_{\lceil \frac{n}{2} \rceil}$ стоят все нули. Поскольку рассматриваются только наборы, в которых ровно $\lfloor \frac{n}{2} \rfloor$ единиц, получаем, что данные функции могут различаться всего на двух наборах.

Пусть в тест не входят некоторые два набора $\tilde{\alpha'}$ и $\tilde{\alpha''}$, для которых $|\tilde{\alpha'}| = |\tilde{\alpha''}| = \lfloor \frac{n}{2} \rfloor$. Тогда слипание переменных, соответствующее нулям в наборе $\tilde{\alpha'}$, и слипание переменных, соответствующее нулям в наборе $\tilde{\alpha''}$, неразличимы.

Отсюда следует, что в тест входит не менее, чем $C_n^{\lfloor \frac{n}{2} \rfloor} - 1$ наборов. Оценив данное выражение снизу и устремив n к бесконечности, получаем неравенство: $L_{\Phi_\vee}(n) \geqslant C_n^{\lfloor \frac{n}{2} \rfloor} - 1 > C_{n-1}^{\frac{n-1}{2}} \sim \frac{2^{n-1}}{\sqrt{\pi \frac{n-1}{2}}} \sim \frac{1}{\sqrt{2\pi}} \frac{2^n}{\sqrt{n}}$. Для четных n, рассматривая функцию $h(x_1, \ldots, x_n)$, равную единицу только на наборах $\tilde{\alpha} : |\tilde{\alpha}| = \frac{n}{2} - 1$, и слипания кратности $\frac{n}{2} + 1$, аналогично получаем нижнюю оценку длины теста: $L_{\Phi_\vee}(n) \geqslant C_n^{\frac{n}{2}-1} - 1 > C_{n-2}^{\frac{n}{2}-1} \sim \frac{2^{n-2}}{\sqrt{\pi \frac{n-1}{2}}} \sim \frac{1}{2\sqrt{2\pi}} \frac{2^n}{\sqrt{n}}$.

Теперь без доказательства сформулируем теорему о верхней оценке для линейных слипаний:

Теорема 3. *Для функции Шеннона $L_{\Phi_{lin}}(n)$ справедлива верхняя оценка $L_{\Phi_{lin}}(n) \lesssim 2^{0.773n}$.*

Работа выполнена при поддержке гранта РФФИ № 12-01-00964-а.

Список литературы

1. Носков В. Н. Диагностические тесты для входов для логических устройств // Дискретный анализ. — 1974. — Вып. 26. — Новосибирск. ИМ СО АН СССР. — С. 72–83.

КРИТЕРИЙ ПОРОЖДЕНИЯ НЕКОТОРЫХ МНОЖЕСТВ МОНОТОННЫХ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ

Д. Ю. Панин (Москва)

Рассматривается некоторый класс функций многозначной логики, монотонных относительно частичного порядка специального вида. В работе получен критерий порождения всех двухместных функций из рассматриваемого множества (см. также [1–3]). Подобные вопросы возникают при исследовании свойств предполных классов монотонных функций, не имеющих конечных порождающих систем [4–7].

Пусть P — произвольное частично упорядоченное множество. Будем обозначать через M^P множество всех функций, монотонных относительно P.

Пусть $n \geqslant 1$. Положим $Q_n = \{0, a_1, b_1, \ldots, a_n, b_n, 1\}$, $Q = Q_n$, $Q^0 = Q \setminus \{1\}$, $Q^1 = Q \setminus \{0\}$, $a_0 = b_0 = 0$, $a_{n+1} = b_{n+1} = 1$. Положим $\Delta_i = \{a_i, b_i\}$, где $0 \leqslant i \leqslant n+1$.

Введем на элементах множества Q отношение частичного порядка $\leqslant$ следующим образом:

1) $\varepsilon_i \leqslant \varepsilon_j$ для всех $\varepsilon_i, \varepsilon_j$, таких, что $\varepsilon_i \in \Delta_i$, $\varepsilon_j \in \Delta_j$, $0 \leqslant i < j \leqslant n+1$,

2) $\varepsilon \leqslant \varepsilon$ для всех $\varepsilon \in Q$,

3) других сравнимых элементов нет.

Пусть $1 \leqslant i \leqslant n$, $\mathcal{T} \subseteq Q$. Будем обозначать через $M_i^{\mathcal{T}}(n)$ множество всех функций $f(x_1, \ldots, x_n)$ из множества M^Q, таких, что для любого набора $(\delta_1, \ldots, \delta_n)$ из $\mathcal{T}^n$ выполнено равенство $f(\delta_1, \ldots, \delta_n) = \delta_i$.

Положим $\mathcal{U} = \{0, 1\}$, $\mathcal{V} = Q \setminus \mathcal{U}$. Определим множества $\mathfrak{M}_i(n)$, $\mathfrak{M}_e(n)$ и $\mathfrak{M}_e$ следующим образом. Положим

$$\mathfrak{M}_i(n) = M_i^{\mathcal{V}}(n) \cap M_i^{\mathcal{U}}(n), \quad \mathfrak{M}_e(n) = \bigcup_{i=1}^{n} \mathfrak{M}_i(n), \quad \mathfrak{M}_e = \bigcup_{n \geqslant 1} \mathfrak{M}_e(n).$$

Будем обозначать через $F_{\leqslant}$ множество всех одноместных функций $f(x)$ из множества M^{Q^0}, таких, что $f(\delta) \leqslant \delta$ для всех $\delta \in Q^0$. Будем обозначать через $F_{\geqslant}$ множество всех одноместных функций $f(x)$ из множества M^{Q^1}, таких, что $\delta \leqslant f(\delta)$ для всех $\delta \in Q^1$.

Определим отображения $\varrho_0 : \mathfrak{M}_e(2) \to F_{\leqslant}$ и $\varrho_1 : \mathfrak{M}_e(2) \to F_{\geqslant}$. Функции $f(x_1, x_2)$ из множества $\mathfrak{M}_e(2)$ сопоставим функцию $\varrho_0(f)(x)$ из множества $F_{\leqslant}$ (соответственно функцию $\varrho_1(f)(x)$ из множества $F_{\geqslant}$) следующим образом. Пусть $\delta \in Q^0$, $\varepsilon \in Q^1$. Положим

$$\varrho_0(f)(\delta) = \begin{cases} f(\delta, 0), & \text{если } f \in \mathfrak{M}_1(2); \\ f(0, \delta), & \text{если } f \in \mathfrak{M}_2(2). \end{cases}$$

$$\varrho_1(f)(\varepsilon) = \begin{cases} f(\varepsilon, 1), & \text{если } f \in \mathfrak{M}_1(2); \\ f(1, \varepsilon), & \text{если } f \in \mathfrak{M}_2(2). \end{cases}$$

Определим отображение $\varrho : \mathfrak{M}_e(2) \to F_{\leqslant} \times F_{\geqslant}$. Пусть $f \in \mathfrak{M}_e(2)$, положим

$$\varrho(f) = (\varrho_0(f), \varrho_1(f)).$$

Пусть $\Omega \subseteq Q$. Положим

$$S_\Omega = \{f \in F_{\leqslant} \mid f(\delta) = \delta \text{ для всех } \delta \in \Omega\},$$

$$N_\Omega = \{f \in F_\leqslant \mid f(\delta) \neq \delta \text{ для всех } \delta \in \Omega\}.$$

Цепью длины m, $1 \leqslant m \leqslant n+1$, будем называть последовательность элементов $(\omega_0, \omega_1, \omega_2, \ldots, \omega_{m-1})$, принадлежащих множеству Q, таких, что для всех $i = 0, \ldots, m-1$, выполняется соотношение $\omega_i \in \Delta_i$.

Будем обозначать через G_2 множество всех функций g из $F_\leqslant$, для которых найдутся номер k, $2 \leqslant k \leqslant n-1$, и цепь Ω длины $k-1$, такие, что выполнены следующие условия:

$$g \in S_\Omega, \quad g \in N_{\Delta_n}, \quad g(\Delta_k) = \Delta_{k-1}, \quad g(\Delta_{k+1}) = \Delta_k.$$

Пусть $\Omega = (\omega_0, \ldots, \omega_k)$ — цепь длины $k+1$, где $0 \leqslant k \leqslant n$. Определим функцию φ_Ω, положив

$$\varphi_\Omega(\delta) = \begin{cases} \delta, & \text{если } \delta \in \Delta_i, \text{ где } k+1 \leqslant i \leqslant n; \\ w_i, & \text{если } \delta = w_i, \text{ где } 0 \leqslant i \leqslant k; \\ w_{i-1}, & \text{если } \delta = c(w_i), \text{ где } 1 \leqslant i \leqslant k. \end{cases}$$

Пусть $\Omega = (\omega_0, \ldots, \omega_{n-1})$ — цепь длины n. Определим функции $g^a_\Omega, g^b_\Omega, g_\Omega$ следующим образом. Положим $g^a_\Omega = \varphi_{\Omega \cup \{a_n\}}$, $g^b_\Omega = \varphi_{\Omega \cup \{b_n\}}$,

$$g_\Omega(\delta) = \begin{cases} \varphi_\Omega(\delta), & \text{если } \delta \in Q_{n-1}; \\ w_{n-1}, & \text{если } \delta \in \Delta_n. \end{cases}$$

Определим семейство $\mathfrak{G}$ множеств функций из F следующим образом. Семейство $\mathfrak{G}$ состоит из всех множеств $A \subseteq F$, таких, что для каждой цепи Ω длины n выполнено по крайней мере одно из следующих двух условий:

$$g_\Omega \in A, \quad \{g^a_\Omega, g^b_\Omega\} \subseteq A.$$

Определим множества Z^a, Z^b следующим образом. Положим

$$Z^a = \{f \in F_\leqslant \mid f(a_n) \leqslant f(b_n)\},$$

$$Z^b = \{f \in F_\leqslant \mid f(b_n) \leqslant f(a_n)\}.$$

Определим отображение $\theta : Q^1 \to Q^0$, положив: $\theta(1) = 0$, $\theta(a_i) = a_{n+1-i}$, $\theta(b_i) = b_{n+1-i}$, $i = 1, \ldots, n$. Очевидно, что θ — взаимно-однозначное соответствие.

Определим отображение $\zeta : F_\geqslant \to F_\leqslant$. Пусть $f \in F_\geqslant$. Положим

$$\zeta(f) = \theta^{-1} \circ f \circ \theta.$$

Функцию $\zeta(f)$ будем также называть *двойственной* (относительно θ) к f и обозначать через f^*. Пусть $A \subseteq F_\geqslant$. Множество $\zeta(A)$ будем называть *двойственным* к A и обозначать через A^*.

Пусть $G \subseteq F$. Будем говорить, что множество G *хорошее*, если найдется множество $A \in \mathfrak{G}$, такое, что $A \subseteq G$, и выполнены соотношения

$$G_2 \subseteq G, \quad G \nsubseteq Z^a, \quad G \nsubseteq Z^b.$$

Имеет место следующий критерий порождения множества $\mathfrak{M}_e(2)$.

Теорема. *Пусть $A \subseteq \mathfrak{M}_e(2)$. Тогда соотношение $\mathfrak{M}_e(2) \subseteq [A]$ выполняется тогда и только тогда, когда выполнены следующие условия*

1) *для каждого $\alpha \in \Delta_1$ и для каждого $\delta \in \mathcal{V}$, множество $\varrho(A)$ содержит элемент (f_0, f_1), такой, что $f_0(\alpha) = \alpha$ и $f_1(\delta) \neq \delta$;*

2) *для каждого $\alpha \in \Delta_n$ и для каждого $\delta \in \mathcal{V}$, множество $\varrho(A)$ содержит элемент (f_0, f_1), такой, что $f_0(\delta) \neq \delta$ и $f_1(\alpha) = \alpha$;*

3) *множества $\varrho_0(A)$ и $\varrho_1(A)^*$ являются хорошими.*

Список литературы

1. Панин Д. Ю. О порождении одноместных монотонных функций многозначной логики // Вестник Московского университета. Математика. Механика. — 2010. — № 6. — С. 52–55.
2. Панин Д. Ю. О некоторых свойствах одноместных монотонных функций многозначной логики // Проблемы теоретической кибернетики: Мат-лы XVI Междунар. конф. (Н. Новгород, 20–25 июня 2011 г.). Изд-во Нижегородского ун-та. — 2011. — С. 349–352.
3. Панин Д. Ю. Критерии полноты для некоторых классов монотонных одноместных функций в P_k // Вестник Московского университета. Математика. Механика. — 2013. — № 3. — С. 57–61.
4. Tardos G. A not finitely generated maximal clone of monotone operations // Order. — 1986. — № 3. — P. 211–218.
5. Lau D. Function algebras on finite sets: a basic course on many-valued logic and clone theory (Springer monographs in mathematics). Secaucus, N.J.: Springer-Verlag New York Inc. — 2006.
6. Дудакова О. С. О конечной порожденности предполных классов монотонных функций многозначной логики // Математические вопросы кибернетики. М.: Физматлит. — 2008. — Вып. 17. — С. 13–104.
7. Дудакова О. С. О классах функций k-значной логики, монотонных относительно множеств ширины два // Вестник Московского университета. Математика. Механика. — 2008. — № 1. — С. 31–37.

ОБ ОСОБЕННОСТЯХ СПЕЦИАЛЬНОЙ ОПЕРАЦИИ СУПЕРПОЗИЦИИ В МНОГОЗНАЧНОЙ ЛОГИКЕ

Д. К. Подолько (Москва)

Известно [1], что семейство классов функций k-значной логики, замкнутых относительно операции суперпозиции, континуально при $k \geqslant 3$. Поэтому для классификации семейства таких классов в ряде работ рассматриваются различные усиления операции суперпозиции (см., например, [2–5]).

В настоящей работе используется аналогичный подход — на основе кодирования функций многозначной логики в двоичной системе счисления определяется специальная операция суперпозиции. Показывается что семейство классов функций k-значной логики, содержащих только функции, принимающие не более двух значений, и замкнутых относительно рассматриваемой операции суперпозиции, является континуальным, но при добавлении к ней еще и операции введения несущественной переменной, становится счетным.

Пусть $k \geqslant 2$. Через E_k обозначим множество $\{0, 1, \ldots, k-1\}$, а через E_k^n, $n \geqslant 1$ — множество всех n-местных наборов, компоненты которых принадлежат E_k. Через P_k обозначим множество всех функций k-значной логики.

Далее будем считать, что $k = 2^m$, $m > 1$. Все числа из E_k запишем в двоичной системе счисления. Таким образом каждому числу α из E_k биективно сопоставляется двоичный вектор $\langle \alpha_1, \ldots, \alpha_m \rangle$ (обозначение $\widehat{\alpha}$). Переменной x, принимающей значения из E_k, поставим в соответствие вектор-переменную $\langle x_1, \ldots, x_m \rangle$ (обозначение $\widehat{x}$), принимающую значения из E_2^m, таким образом, что значению α переменной x сопоставляется значение $\widehat{\alpha}$ вектор-переменной $\widehat{x}$. И, наконец, каждой n-местной функции $F(x^1, \ldots, x^n)$ из P_k сопоставим вектор mn-местных булевых функций $\langle f_1, \ldots, f_m \rangle (\widehat{x}^1, \ldots, \widehat{x}^n)$. Его будем также обозначать через $\widehat{F}(\widehat{x}^1, \ldots, \widehat{x}^n)$ или просто $\widehat{F}$. Назовем такие представления *двоичным представлением числа α, переменной x* и *функции F* соответственно. Переменные $x_1, \ldots, x_m$ назовем *компонентами* вектор-переменной $\widehat{x}$ и переменной x, а функции $f_1, \ldots, f_m$ — *компонентами* вектор-функции $\widehat{F}$ и функции F. Множество всех компонент F будем обозначать через $b(F)$.

Пусть $\omega \in S_{mp}$, $p \geqslant 1$, т. е. ω — перестановка множества $\{1, 2, \ldots, mp\}$. Тогда отображение $\omega^{(mp)} : E_2^{mp} \to E_2^{mp}$, задаваемое функцией

$$\omega^{(mp)}(x_1, \ldots, x_{mp}) = (x_{\omega(1)}, \ldots, x_{\omega(mp)}),$$

будем называть *двоичной перестановкой порядка mp*.

Пусть $x^1, \ldots, x^p$, $p \geqslant 1$ — переменные, принимающие значения из множества E_k. Вектор $(\widehat{x}^1, \ldots, \widehat{x}^p)$, компоненты которого являются двоичными представлениями переменных $x^1, \ldots, x^p$, можно рассматривать как вектор-переменную, принимающую значения из E_2^{mp}. Поэтому если $\omega^{(mp)}$ — двоичная

перестановка порядка mp, то имеет место соотношение:

$$\omega^{(mp)}(\widehat{x}^1,\dots,\widehat{x}^p)=\Big(\langle x_{\omega(1)},\dots,x_{\omega(m)}\rangle,\dots,\langle x_{\omega(m(p-1)+1)},\dots,x_{\omega(mp)}\rangle\Big),$$

где $\widehat{x}^i=\langle x_{m(i-1)+1},\dots,x_{mi}\rangle$ для $i=1,\dots,p$.

Пусть $\mathcal{A}\subseteq P_k$. Введем понятие *вектор-формулы над* $\mathcal{A}$.

1. Пусть x — переменная. Тогда выражение $\widehat{x}$ назовем *вектор-формулой над* $\mathcal{A}$. Такие вектор-формулы будем называть *тривиальными*.

2. Пусть $F\in\mathcal{A}$, F зависит от p переменных, $\Phi_1,\dots,\Phi_p$ — вектор-формулы над $\mathcal{A}$, а $\omega^{(mp)}$ — двоичная перестановка порядка mp. Тогда выражение $\widehat{F}\Big(\omega^{(mp)}\big(\Phi_1,\dots,\Phi_p\big)\Big)$ назовем *вектор-формулой над* $\mathcal{A}$.

Пусть Φ — вектор-формула над $\mathcal{A}$, а $\{\widehat{x}^1,\dots,\widehat{x}^n\}$ — множество всех тривиальных вектор-формул, содержащихся в Φ. Тогда будем обозначать вектор-формулу Φ через $\Phi(\widehat{x}_1,\dots,\widehat{x}_n)$ и говорить, что она зависит от вектор-переменных $\widehat{x}^1,\dots,\widehat{x}^n$. Значение $\Phi(\widehat{\alpha}^1,\dots,\widehat{\alpha}^n)$ вектор-формулы $\Phi(\widehat{x}^1,\dots,\widehat{x}^n)$ для каждого набора $(\widehat{\alpha}^1,\dots,\widehat{\alpha}^n)$ из E_2^{mn} определяется стандартным образом.

Будем говорить, что функция $F(x^1,\dots,x^n)$ *реализуется* вектор-формулой $\Phi(\widehat{x}^1,\dots,\widehat{x}^n)$ над $\mathcal{A}$, если для всех наборов $(\widehat{\alpha}^1,\dots,\widehat{\alpha}^n)$ из E_2^{mn} верно соотношение $\Phi(\widehat{\alpha}^1,\dots,\widehat{\alpha}^n)=\widehat{F}(\widehat{\alpha}^1,\dots,\widehat{\alpha}^n)$. Если при этом вектор-формула $\Phi(\widehat{x}^1,\dots,\widehat{x}^n)$ не является тривиальной, то будем говорить, что функция F получена при помощи *операции двоичной S-суперпозиции* из функций системы $\mathcal{A}$. Несложно показать, что операция двоичной S-суперпозиции является усилением операции суперпозиции.

Множество всех функций k-значной логики, которые можно получить из функций системы $\mathcal{A}$ при помощи операции двоичной S-суперпозиции, будем называть S_0-*замыканием множества* $\mathcal{A}$ (обозначение $[\mathcal{A}]_{S_0}$). Множество $\mathcal{A}$ будем называть S_0-*замкнутым*, если выполняется равенство $\mathcal{A}=[\mathcal{A}]_{S_0}$.

Через $\widehat{P_{k,2}}$ обозначим множество всех функций k-значной логики, которые принимают не более двух значений. Покажем, что семейство всех S_0-замкнутых классов функций из $\widehat{P_{k,2}}$ имеет мощность континуума. Для этого определим множества $R_n\subseteq E_k^n$ и $\widehat{R}_n\subseteq E_2^{mn}$ для всех $n\geqslant 2$. Положим $R_n=\big\{(1,k-1,\dots,k-1),(k-1,1,k-1,\dots,k-1),\dots,(k-1,k-1,\dots,k-1,1)\big\}$ и $\widehat{R}^n=\big\{(\widehat{\alpha}^1,\dots,\widehat{\alpha}^n)\,|\,(\alpha^1,\dots,\alpha^n)\in R_n\big\}$. Определим n-местную функцию χ_n из P_k как характеристическую функцию множества R_n:

$$\chi_n(x^1,\dots,x^n)=\begin{cases}1, \text{ если } (x^1,\dots,x^n)\in R_n;\\ 0, \text{ в противном случае.}\end{cases}$$

Положим также $\mathcal{W}=\bigcup\limits_{n=2}^{\infty}\{\chi_n\}$. Имеет место следующее утверждение.

Лемма 1. *Пусть $n\geqslant 2$. Тогда верно соотношение $\chi_n\notin\big[\mathcal{W}\backslash\{\chi_n\}\big]_{S_0}$.*

Доказательство. Доказательство данной леммы основано на методе, который используется при доказательства теоремы о континуальности семейства классов функций из P_k, замкнутых относительно операции суперпозиции (см., например, [6]).

Предположим, что $\chi_n \in \left[\mathcal{W}\backslash\{\chi_n\}\right]_{S_0}$. Тогда χ_n реализуется нетривиальной вектор-формулой Φ над $\mathcal{W}\backslash\{\chi_n\}$. Без ограничения общности будем считать, что Φ зависит только от вектор-переменных $\widehat{x}^1, \ldots, \widehat{x}^n$. Поэтому Φ имеет вид:

$$\widehat{\chi_p}\Big(\omega^{(mp)}\big(\Phi_1(\widehat{x}^1, \ldots, \widehat{x}^n), \ldots, \Phi_p(\widehat{x}^1, \ldots, \widehat{x}^n)\big)\Big),$$

где $\Phi_1, \ldots, \Phi_p$ — некоторые вектор-формулы над $\mathcal{W}\backslash\{\chi_n\}$, а $\omega^{(mp)}$ — двоичная перестановка порядка mp, $p \geqslant 2$, $p \neq n$.

Рассмотрим произвольный набор $(\alpha^1, \ldots, \alpha^n)$ из R_n. Так как вектор-формула Φ реализует функцию χ_n, то выполнено $\Phi(\widehat{\alpha}^1, \ldots, \widehat{\alpha}^n) = \widehat{1}$. Следовательно, набор $\Big(\omega^{(mp)}\big(\Phi_1(\widehat{\alpha}^1, \ldots, \widehat{\alpha}^n), \ldots, \Phi_p(\widehat{\alpha}^1, \ldots, \widehat{\alpha}^n)\big)\Big)$ должен содержаться в $\widehat{R}_p$, а поскольку $\omega^{(mp)}$ сохраняет количество нулевых компонент в наборе, на котором она действует, то в наборе $\big(\Phi_1(\widehat{\alpha}^1, \ldots, \widehat{\alpha}^n), \ldots, \Phi_p(\widehat{\alpha}^1, \ldots, \widehat{\alpha}^n)\big)$ должен быть ровно $m-1$ нуль. Покажем, что это не так. Для этого рассмотрим три случая.

1. Среди вектор-формул $\Phi_1, \ldots, \Phi_p$ имеются хотя бы две нетривиальные вектор-формулы. Каждая из таких вектор-формул реализует функцию, которая принимает только значения из множества $\{0, 1\}$, а следовательно в ее двоичное представление входит как минимум $m-1$ нулевая компонента.

2. Среди вектор-формул $\Phi_1, \ldots, \Phi_p$ имеется только одна нетривиальная. Так как $p \geqslant 2$, то среди данных вектор-формул имеется хотя бы одна тривиальная. Без ограничения общности будем считать, что это вектор-формула $\widehat{x}^1$.

3. Все вектор-формулы $\Phi_1, \ldots, \Phi_p$ являются тривиальными. Поскольку все переменные функции χ_n существенные, то среди рассматриваемых вектор-формул должна содержаться каждая из вектор-формул $\widehat{x}^i$, $i = 1, \ldots, n$. Следовательно, $p > n$ и среди вектор-формул $\Phi_1, \ldots, \Phi_p$ найдутся хотя бы две одинаковые вектор-формулы. Без ограничения общности будем считать, что они равны вектор-формуле $\widehat{x}^1$.

В каждом из трех случаев рассмотрим набор $(1, k-1, \ldots, k-1)$ из R_n, который обозначим через $(\alpha^1, \ldots, \alpha^n)$. Набор $\big(\Phi_1(\widehat{\alpha}^1, \ldots, \widehat{\alpha}^n), \ldots, \Phi_p(\widehat{\alpha}^1, \ldots, \widehat{\alpha}^n)\big)$ содержит как минимум $2m-2$ нулевые компоненты: по $m-1$ от каждой нетривиальной вектор-формулы (для случаев 1 и 2) и по $m-1$ от каждой вектор-формулы $\widehat{x}^1$ (для случаев 2 и 3). Данное утверждение противоречит описанному выше необходимому условию. Лемма доказана.

Теорема 1. *Пусть $k = 2^m$, $m > 1$. Тогда $\widehat{P_{k,2}}$ содержит континуальное семейство различных S_0-замкнутых классов.*

Доказательство теоремы проводится с использованием леммы 1 аналогично доказательству теоремы о континуальности семейства классов функций из

P_k, замкнутых относительно операции суперпозиции (см., например, [6]).

Теперь рассмотрим усиление оператора S_0-замыкания. Пусть $\mathcal{A} \subseteq P_k$. Множество всех функций, которые можно получить из $\mathcal{A}$ при помощи операций двоичной S-суперпозиции и введения несущественной переменной, будем называть *S-замыканием множества $\mathcal{A}$* (обозначение $[\mathcal{A}]_S$). Множество $\mathcal{A}$ будем называть *S-замкнутым*, если верно равенство $\mathcal{A} = [\mathcal{A}]_S$. Множество $B(\mathcal{A}) = \big[\bigcup\limits_{F \in \mathcal{A}} b(F)\big]$, где через $[\mathcal{B}]$ обозначается замыкание множества $\mathcal{B}$ булевых функций относительно операций суперпозиции и введения несущественной переменной, будем называть *булевым замыканием множества $\mathcal{A}$*.

Следующая лемма устанавливает эквивалентность понятия S-замыкания и понятия β-замыкания, введенного в работе [7].

Лемма 2. *Пусть $\mathcal{A} \subseteq P_k$. Тогда выполняется соотношение $[\mathcal{A}]_S = [\mathcal{A}]_\beta$.*

Доказательство. Рассмотрим произвольную функцию $H \in [\mathcal{A}]_\beta$. Она реализуется некоторой вектор-формулой Φ над $\mathcal{A}$ (в определениях из [7]), которая имеет вид:

$$\langle f_1(\varphi_1, \varphi_2, \ldots, \varphi_{mn}), \ldots, f_m(\varphi_1, \varphi_2, \ldots, \varphi_{mn})\rangle,$$

где $\langle f_1, \ldots, f_m\rangle = \widehat{F}$, F содержится в $\mathcal{A}$, либо получена из функций системы $\mathcal{A}$ при помощи операции введения несущественной переменной, $\varphi_1, \ldots, \varphi_{mn}$ — компоненты некоторых вектор-формул над $\mathcal{A}$ (в определениях из [7]). Тогда двоичное представление функции H имеет вид:

$$\langle f_1, \ldots, f_m\rangle(\langle h_1, \ldots, h_m\rangle, \ldots, \langle h_{m(n-1)+1}, \ldots, h_{mn}\rangle),$$

где h_i — функция, реализуемая φ_i (в определениях из [7]), $i = 1, \ldots, mn$.

Покажем, что $H \in [\mathcal{A}]_S$. Доказательство будем вести индукцией по глубине реализации функций $h_1, \ldots, h_{mn}$ над множеством функций $\bigcup\limits_{F \in \mathcal{A}} b(F)$.

Пусть глубина реализации каждой из функций $h_1, \ldots, h_{mn}$ равна нулю. Это означает, что h_i является компонентой $x_{j_i}^{a_i}$ переменной x^{a_i}, где $1 \leqslant j_i \leqslant m$, $a_i \geqslant 1$, $i = 1, \ldots, mn$. Рассмотрим mn-местную функцию F' из P_k, полученную из функции F путем добавления $(m-1)n$ несущественных переменных и вектор-формулу $\widehat{F}'\big(\omega^{(m^2n)}\big(\widehat{x}^{a_1}, \ldots, \widehat{x}^{a_{mn}}\big)\big)$, где ω — некоторая перестановка множества $\{1, \ldots, m^2n\}$, которая переставляет число $m(i-1)+j_i$ на место i для всех $i = 1, \ldots, mn$. Очевидно, что данная вектор-формула реализует H.

Предположим, что лемма доказана, если глубина реализации каждой функции h_i меньше d, $i = 1, \ldots, mn$. Докажем утверждение для глубины d.

Рассмотрим функцию h_i для каждого $i = 1, \ldots, mn$. Если она является компонентой $x_{j_i}^{a_i}$ переменной x^{a_i}, $1 \leqslant j_i \leqslant m$, $a_i \geqslant 1$, то определим вектор-формулу Φ_i над $\mathcal{A}$, равную $\widehat{x}^{a_i}$. Если $h_i \in B(\mathcal{A})$, то $h_i = f_{j_i}^{a_i}(g_{i,1}, \ldots, g_{i,mn_i})$, где $f_{j_i}^{a_i}$ — компонента функции F^{a_i} из $\mathcal{A}$, зависящей от n_i переменных, $1 \leqslant j_i \leqslant m$, $a_i \geqslant 1$, а функция $g_{i,t}$ либо содержится в $B(\mathcal{A})$, либо является компонентой

переменной, и имеет глубину реализации не более $d-1$, $t=1,\ldots,mn_i$. По предположению индукции функция, соответствующая двоичному представлению

$$\langle f_1^{a_i},\ldots,f_m^{a_i}\rangle(\langle g_{i,1},\ldots,g_{i,m}\rangle,\ldots,\langle g_{i,m(n_i-1)+1},\ldots,g_{i,mn_i}\rangle),$$

лежит в $[\mathcal{A}]_S$ и реализуется некоторой вектор-формулой Φ_i над $\mathcal{A}$.

Снова рассмотрим вектор-формулу $\widehat{F'}\Big(\omega^{(m^2n)}\big(\Phi_1,\ldots,\Phi_{mn}\big)\Big)$, где ω — некоторая перестановка множества $\{1,\ldots,m^2n\}$, которая для всех $i=1,\ldots,mn$ переставляет число $m(i-1)+j_i$ на место i. Очевидно, что данная вектор-формула реализует H, а следовательно верно соотношение $[\mathcal{A}]_\beta\subseteq[\mathcal{A}]_S$.

Рассмотрим теперь произвольную функцию $H\in[\mathcal{A}]_S$. Она реализуется некоторой вектор-формулой Φ над $\mathcal{A}$, которая имеет вид:

$$\widehat{F}\Big(\omega^{(mn)}\big(\Phi_1,\ldots,\Phi_n\big)\Big),$$

где функция F содержится в $\mathcal{A}$, либо получена из функций системы $\mathcal{A}$ при помощи операции введения несущественной переменной, $\Phi_1,\ldots,\Phi_n$ — вектор-формулы над $\mathcal{A}$, а $\omega^{(mn)}$ — двоичная перестановка порядка mn. Обозначим через $F_1\ldots,F_n$ функции, реализуемые вектор-формулами $\Phi_1,\ldots,\Phi_n$, а через $\langle h_1,\ldots,h_m\rangle$, $\langle h_{m+1},\ldots,h_{2m}\rangle,\ldots,\langle h_{m(n-1)+1},\ldots,h_{mn}\rangle$ — их двоичные представления соответственно. Функция h_i либо содержится в $B(\mathcal{A})$, либо является компонентой некоторой вектор-переменной, а значит, реализуется компонентой некоторой вектор-формулы над $\mathcal{A}$ (в определениях из [7]), $i=1,\ldots,mn$. Обозначим эту компоненту через φ_i, а $\omega(i)$ — через ω_i, $i=1,\ldots,mn$. Рассмотрим вектор-формулу над $\mathcal{A}$ (в определениях из [7]), имеющую вид:

$$\langle f_1(\varphi_{\omega_1},\varphi_{\omega_2},\ldots,\varphi_{\omega_{mn}}),\ldots,f_m(\varphi_{\omega_1},\varphi_{\omega_2},\ldots,\varphi_{\omega_{mn}})\rangle.$$

Очевидно, что данная вектор-формула реализует функцию H (в определениях из [7]) и $H\in[\mathcal{A}]_\beta$. Лемма доказана.

Теорема 2. *Пусть $k=2^m, m>1$. Тогда $\widehat{P_{k,2}}$ содержит счетное семейство различных S-замкнутых классов.*

Данное утверждение следует из леммы 2 и теоремы из [7] о счетности семейства всех β-замкнутых классов функций из $\widehat{P_{k,2}}$.

Таким образом показано, что операция двоичной S-суперпозиции не является достаточно сильной, чтобы при помощи нее получить семейство всех замкнутых классов функций из $\widehat{P_{k,2}}$ счетной или конечной мощности. Однако добавление к ней операции введения несущественной переменной сужает семейство всех замкнутых классов таких функций до счетного.

Работа выполнена при финансовой поддержке РФФИ (проект №11–01–00508) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза

управляющих систем»).

Список литературы

1. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // Докл. АН СССР. — 1959. — Т. 127, № 1. — С. 44–46.
2. Нгуен Ван Хоа. О семействах замкнутых классов k-значной логики, сохраняемых всеми автоморфизмами // Дискретная математика. — 1993. — Т. 5, вып. 4. — С. 87–108.
3. Марченков С. С. S-классификация функций многозначной логики // Дискретная математика. — 1997. — Т. 9, вып. 3. — С. 125–152.
4. Тарасова О. С. Классы функций k-значной логики, замкнутые относительно операций суперпозиции и перестановок // Математические вопросы кибернетики. Выпуск 13: Сборник статей. — М.: Физматлит, 2004. — С. 59–112.
5. Акулов Я. В. О полноте систем функций для классов расширенной суперпозиции // Вестник МГУ. Серия 1. Математика. Механика. — 2011. — № 1. — С. 36–41.
6. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2001.
7. Подолько Д. К. О классах функций, замкнутых относительно специальной операции суперпозиции // Вестник МГУ. Серия 1. Математика. Механика. — 2013. — № 6.

ОБ ОЦЕНКАХ СЛОЖНОСТИ СХЕМ В ОДНОМ БЕСКОНЕЧНОМ БАЗИСЕ

О. В. Подольская (Москва)

В работе рассматривается задача о сложности реализации булевых функций схемами из функциональных элементов в бесконечном полном базисе, который состоит из всевозможных булевых функций, принимающих единичное значение лишь на попарно несравнимых наборах. Известны нижние оценки порядка $\sqrt{n}$ для сложности реализации линейной функции, функции голосования и почти всех булевых функций от n переменных. Установлена верхняя оценка n для сложности реализации произвольной булевой функции от n переменных.

Булеву функцию, принимающую единичное значение лишь на попарно несравнимых наборах, будем называть *антицепной*, а совокупность всех антицепных функций от любого числа переменных будем обозначать через AC. Антицепными являются, например, функции $\overline{x}$, $x\&y$, а также $x+y$ (сложение

по модулю 2). В частности, из полноты системы $\{\overline{x}, x\&y\}$ следует, что AC образует полный базис.

Будем изучать схемы, в которых функциональным элементам приписаны функции из AC. Определим *сложность схемы* как количество элементов в ней, а *сложность булевой функции* f как наименьшее количество элементов, достаточное для реализации этой функции схемой в базисе AC. Через $L(n)$ обозначим наибольшую величину сложности функций от n переменных. Функция $L(n)$ натурального аргумента n называется *функцией Шеннона*. С этими и другими понятиями, которые используются в работе, подробнее можно ознакомиться в [1].

Линейной функцией от n переменных будем называть булеву функцию, принимающую единичное значение лишь на тех наборах, в которых число единиц нечетно. *Функцией голосования* от n переменных назовем булеву функцию, которая принимает значение единица на тех и только тех наборах, в которых число единиц не меньше $n/2$.

Будем говорить, что некоторое свойство выполняется для *почти всех* булевых функций от n переменных, если отношение числа функций, для которых свойство выполнено, к общему числу функций от n переменных стремится к единице при $n \longrightarrow \infty$.

Сложность реализации булевых функции схемами в базисе AC изучалась ранее в работах [2–4]. В частности, в [3] была доказана нижняя оценка порядка $(n/\ln n)^{1/2}$ сложности схемы для линейной функции от n переменных. В [4] эта оценка была улучшена, и было показано, что для реализации линейной функции, функции голосования и почти всех функций от n переменных схемами в базисе AC требуется по порядку не менее $\sqrt{n}$ элементов при $n \to \infty$. Отсюда вытекает нижняя оценка функции Шеннона $L(n) \geqslant c \cdot \sqrt{n}$ для всех достаточно больших n и некоторой положительной константы c.

В [2] указана верхняя оценка функции Шеннона $L(n) \leqslant n+1$. Автору данной работы удалось улучшить эту оценку, доказав следующее утверждение.

Теорема. *Для всех n имеет место верхняя оценка функции Шеннона* $L(n) \leqslant n$.

Приведем коротко основные идеи доказательства. Для произвольной булевой функции f от n переменных сначала покажем, как можно построить схему сложности не более $n+2$, а затем поясним, как ее сложность может быть уменьшена. Для краткости будем использовать следующие обозначения для наборов длины n: $(0,0,\ldots,0) = \widetilde{0}$, $(1,1,\ldots,1) = \widetilde{1}$, $(x_1, x_2, \ldots, x_n) = \widetilde{x}$.

Для всякой булевой функции f от n переменных зададим функции от n переменных $h_0^f, \ldots, h_n^f$, полагая для всякого $t \in \{0, 1, \ldots, n\}$

$$h_t^f(\widetilde{x}) = 1 \Leftrightarrow \begin{cases} \sum\limits_{k=1}^{n} x_k = t \\ f(\widetilde{x}) = 1. \end{cases}$$

Заметим, что каждая из функций h_t^f принадлежит классу AC.

Определим функцию $g(y_1, \ldots, y_{n+1})$ следующим образом: положим ее равной единице на наборах, в которых ровно одна единица, а на остальных наборах равной нулю. Ясно, что g принадлежит классу AC. Нетрудно видеть, что

$$g(h_0^f(\widetilde{x}), \ldots, h_n^f(\widetilde{x})) = f(\widetilde{x}). \tag{1}$$

Таким образом, можно построить схему сложности не более $n+2$ для произвольной булевой функции от n переменных (см. рис. 1).

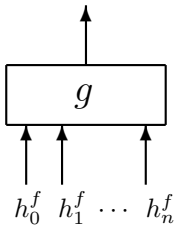


Рис. 1

Далее, чтобы уменьшить полученную верхнюю оценку, будем использовать два приема. Первый из них основан на следующем соображении: заметим, что если $f(\widetilde{0}) = 0$, то из схемы, построенной выше (рис. 1), можно удалить элемент, реализующий функцию h_0^f, а если $f(\widetilde{1}) = 0$, то может быть удален элемент, соответствующий функции h_n^f. Действительно, в обоих случаях эти элементы реализуют константу 0. При этом в обоих случаях мы получаем схему сложности не более $n+1$. Если же $f(\widetilde{1}) = f(\widetilde{0}) = 1$, то пользуясь указанными выше замечаниями, построим схему для $\overline{f}$ сложности не более n, а затем подадим выход схемы на элемент отрицания, и получим схему для f сложности не более $n+1$. Таким образом, для произвольной булевой функции от n переменных можем получить схему сложности не более $n+1$.

Опишем теперь второй прием, с помощью которого можно уменьшить сложность схемы еще на единицу. Идея состоит в том, что можно эффективнее использовать элемент схемы, соответствующий функции g (в схеме сложности не более $n+1$), подав на него дополнительно входные переменные $x_1, \ldots, x_n$. Покажем это для частного случая функции f, такой что $f(\widetilde{1}) = 1, f(\widetilde{0}) = 0$. В этом случае реализуем функцию f следующим образом:

$$f(\widetilde{x}) = g'(h_1^f, \ldots, h_{n-1}^f, x_1, \ldots, x_n), \tag{2}$$

где $g'(y_1, \ldots, y_{n-1}, x_1, \ldots, x_n,)$ — функция от $2n-1$ переменной, которая принимает единичное значение на следующих наборах:

$$\text{(I)} \begin{cases} \exists j, \text{ такой что } y_j = 1, \\ \forall i \neq j : y_i = 0, \\ \sum\limits_{k=1}^{n} x_k = j, \\ f(x_1, \ldots, x_n) = 1, \end{cases} \qquad \text{(II)} \begin{cases} \forall\, i \;\; y_i = 0, \\ \forall\, i \;\; x_i = 1. \end{cases}$$

Равенство (2) нетрудно проверить прямым перебором возможных значений входных наборов.

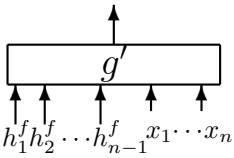


Рис. 2

Соответствующая схема (рис. 2) имеет сложность n.

Остальные три случая, в зависимости от значений $f(\widetilde{0})$ и $f(\widetilde{1})$, рассматриваются аналогично путем комбинирования описанных выше приемов (причем в случае $f(\widetilde{0}) = f(\widetilde{1}) = 0$ можем получить схему сложности не более $n-1$). Таким образом устанавливается верхняя оценка n сложности произвольной булевой функции от n переменных.

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во Московского университета, 1984.
2. Касим-Заде О. М. О сложности схем в одном бесконечном базисе // Вестник Московского университета, Сер. 1. Математика. Механика. — 1994. — № 6. — С. 40–44.
3. Касим-Заде О. М. О сложности реализации булевых функций схемами в одном бесконечном базисе // Дискретный анализ и исследование операций. — 1995. — Т.2, № 1. — С. 7–20.
4. Подольская О. В. О нижних оценках сложности схем в базисе антицепных функций // Вестник Московского университета, Сер. 1. Математика. Механика. — 2013. — № 2. — С. 17–23.

ВЕРХНИЕ ОЦЕНКИ СЛОЖНОСТИ И ГЛУБИНЫ ФОРМУЛ ДЛЯ СИММЕТРИЧЕСКИХ БУЛЕВЫХ ФУНКЦИЙ

И. С. Сергеев (Москва)

Введение

В настоящей заметке рассматриваются сложность и глубина реализации оператора C_n подсчета числа единиц в булевом наборе длины n, а также класса S_n симметрических булевых функций n переменных формулами. Получены конкретные верхние оценки в случае формул над стандартным базисом $B_0 = \{\vee, \wedge, {}^-\}$ и базисом B_2 всех двуместных булевых функций.

Понятия формулы, глубины и сложности разъясняются в [2]. Глубину и сложность реализации булевого оператора f формулами над базисом B обозначим через $D_B(f)$ и $L_B(f)$ соответственно.

Известные методы [2–4, 6, 7] сводят реализацию симметрических функций к реализации оператора $C_n(x_1, \dots, x_n) = (C_{n,m-1}, \dots, C_{n,0})$, вычисляющего арифметическую сумму $x_1 + \dots + x_n$ булевых переменных $x_1, \dots, x_n$, где $m = \lceil \log_2(n+1) \rceil$ (функция $C_{n,i}$ вычисляет i-й разряд суммы).

Отметим, что первые нетривиальные верхние оценки глубины и сложности оператора C_n и класса S_n (над базисом B_0) получены В. М. Храпченко [3, 4]. Метод синтеза с тех пор не претерпел принципиальных изменений, хотя и был обогащен новыми идеями, см. [6, 7].

Оператор C_n реализуется методом компрессоров, см., например, [3, 4]. Двоичный (k,l)-компрессор ширины 1 — это схема, реализующая булев оператор $(x_1,\ldots,x_k)\to(y_1,\ldots,y_l)$ по правилу $\sum 2^{a_i}x_i=\sum 2^{b_j}y_j$, где $k>l$, а $a_i,b_j\in\mathbb{Z}$. (k,l)-компрессор произвольной ширины строится из параллельных копий компрессоров ширины 1 — он преобразует k многоразрядных чисел в l чисел, сохраняя сумму. Из компрессоров собирается сохраняющая сумму схема преобразования n чисел в l чисел.

Наилучшие известные оценки глубины и сложности оператора C_n получены путем конструирования подходящих компрессоров и оптимального размещения их в схеме[1]: $D_{B_0}(C_n)\lesssim 4,93\log_2 n$, $D_{B_2}(C_n)\lesssim 3,44\log_2 n$ ([7] со ссылкой на [5]); $L_{B_0}(C_n)\preceq n^{4,57}$, $L_{B_2}(C_n)\preceq n^{3,13}$ [7].

Для класса S_n и базиса $B\in\{B_0,\,B_2\}$ оценки выводятся из соотношений:

$$D_B(S_n)\lesssim\max_{0\leqslant i<m}\{D_B(C_{n,i})+m-i\},\qquad L_B(S_n)\preceq\sum_{i=0}^{m-1}2^{m-i}L_B(C_{n,i}),$$

см. [3, 6] (произвольная симметрическая функция рассматривается как функция компонент оператора C_n и реализуется методом разложения по переменным).

Известные верхние оценки:

$$L_{B_0}(S_n)\preceq n^{4,85},\quad L_{B_2}(S_n)\preceq n^{3,30},\quad D_{B_2}(S_n)\lesssim 3,81\log_2 n,$$

см. [6]; несколько лучшие оценки вытекают из [7].

Результаты

Новое соображение состоит в том, чтобы вычислять сумму $\sigma=x_1+\ldots+x_n$ из остатков $\sigma_2=(\sigma \bmod 2^k)$ и $\sigma_3=(\sigma \bmod 3^l)$ при помощи китайской теоремы. Каждый остаток вычисляется методом компрессоров. Число σ_2 просто состоит из младших k компонент оператора C_n. Остаток σ_3 вычисляется в троичной системе счисления при помощи троичных компрессоров. Существенно используется то, что младшие разряды суммы в методе компрессоров могут быть вычислены проще, чем старшие.

Обозначим через $C_n^{(3)}(x_1,\ldots,x_n)=\left(C_{n,m-1}^{(3)},\ldots,C_{n,0}^{(3)}\right)$, $m=\lceil\log_3(n+1)\rceil$, булев $(n,2m)$-оператор вычисления арифметической суммы булевых переменных $x_1,\ldots,x_n$ в троичной системе счисления. Компонента $C_{n,i}^{(3)}$ является 2-битным кодом соответствующей цифры из троичной записи числа.

[1] Знак $\lesssim$ обозначает асимптотическое неравенство; знаки $\preceq$, $\prec$ — соответственно нестрогое и строгое неравенства по порядку.

Лемма. *Пусть* $2^k \cdot 3^l > n$. *Для любого полного конечного базиса* B *справедливо*

$$D_B(C_n) \leqslant D_B\left(C_{n,k-1}, \ldots, C_{n,0}, C^{(3)}_{n,l-1}, \ldots, C^{(3)}_{n,0}\right) + O\left(\log^2 \log n\right),$$

$$L_B(C_n) \preceq 2^{O\left(\log^2 \log n\right)} \left(\sum_{i=0}^{k-1} L_B(C_{n,i}) + \sum_{i=0}^{l-1} L_B\left(C^{(3)}_{n,i}\right)\right).$$

Доказательство. Второе соотношение следует из первого ввиду очевидного неравенства $\log L_B(f) \preceq D_B(f)$. Докажем соотношение для глубины.

Методом Шенхаге (см. [1, гл. 14]) $O(\log n)$-разрядное число σ_3 преобразуется из троичного представления в двоичное с глубиной $O(\log^2 \log n)$. Далее вычисление σ, исходя из σ_2 и σ_3, выполняется согласно формуле

$$\sigma = \sigma_2 + 2^k \left(\tau \left(\sigma_3 - \sigma_2\right) \bmod 3^l\right),$$

где τ определяется из сравнения $\tau 2^k \equiv 1 \mod 3^l$. Вычисление по указанной формуле сводится к нескольким умножениям, сложениям, вычитаниям и делению с остатком $O(\log n)$-разрядных чисел, поэтому может быть выполнено с глубиной $O(\log \log n)$.

Используя простейшие троичные $(4, 2)$-компрессоры, модификации двоичных компрессоров из работ [3, 5, 7], метод [6] и лемму, можно получить следующие оценки.

Теорема 1.

$$D_{B_0}(C_n) \lesssim 4,87 \log_2 n, \qquad D_{B_2}(C_n) \lesssim 3,34 \log_2 n,$$
$$L_{B_0}(C_n) \preceq n^{4,47}, \qquad L_{B_2}(C_n) \preceq n^{3,03}.$$

Как следствие, такие же оценки справедливы для функции голосования от n переменных и других монотонных симметрических функций, см., например, [3]. В качестве еще одного следствия можно получить оценки глубины оператора M_n умножения n-разрядных чисел, используя соотношение $D_B(M_n) \lesssim D_B(C_n) + \log_2 n$, где $B \in \{B_0, B_2\}$, см. [4].

Произвольную симметрическую функцию можно представить как функцию разрядов числа σ_2 и кода числа σ_3 и далее реализовать методом разложения по переменным. Предварительно число σ_3 переписывается в системе счисления с основанием 3^β, где $1 \prec \beta \prec \log n$, а цифры кодируются обычным двоичным представлением. В итоге получаются следующие оценки.

Теорема 2.

$$D_{B_0}(S_n) \lesssim 4,88 \log_2 n, \qquad D_{B_2}(S_n) \lesssim 3,34 \log_2 n,$$
$$L_{B_0}(S_n) \preceq n^{4,48}, \qquad L_{B_2}(S_n) \preceq n^{3,04}.$$

Работа выполнена при финансовой поддержке РФФИ, проекты 11–01–00508 и 11–01–00792–а, и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Гашков С. Б. Занимательная компьютерная арифметика. Быстрые алгоритмы операций с числами и многочленами. — М.: Либроком, 2012.
2. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.
3. Храпченко В. М. О сложности реализации симметрических функций формулами // Мат. заметки — 1972. — Т. 11(1). — С. 109–120.
4. Храпченко В. М. Некоторые оценки для времени умножения // Проблемы кибернетики. Вып. 33. — М.: Наука, 1978. — С. 221–227.
5. Grove E. Proofs with potential. Ph.D. Thesis. — U.C. Berkeley, 1993.
6. Paterson M. S., Pippenger N., Zwick U. Faster circuits and shorter formulae for multiple addition, multiplication and symmetric Boolean functions // Proc. 31st IEEE Symp. Found. Comput. Sci. — 1990. — P. 642–650.
7. Paterson M., Zwick U. Shallow circuits and concise formulae for multiple addition and multiplication // Comput. Complexity. — 1993. — V. 3. — P. 262–291.

О РАСПОЗНАВАНИИ ПОДОБИЯ НАД КОЛЬЦОМ ЦЕЛЫХ ЧИСЕЛ МАТРИЦ ТРЕТЬЕГО ПОРЯДКА, ИМЕЮЩИХ ПРИВОДИМЫЙ ХАРАКТЕРИСТИЧЕСКИЙ МНОГОЧЛЕН

С. В. Сидоров (Нижний Новгород)

Понятие подобных матриц над некоторым полем является классическим в линейной алгебре и легко обобщается на произвольное коммутативное кольцо с единицей, в частности, на кольцо целых чисел $\mathbf{Z}$. Введем необходимые определения.

Определение 1. Матрица $A \in \mathbf{Z}^{n\times n}$ *подобна* матрице $B \in \mathbf{Z}^{n\times n}$ над полем рациональных чисел $\mathbf{Q}$, если существует такая матрица $X \in \mathbf{Q}^{n\times n}$, что $AX = XB$ и $\det X \neq 0$.

Определение 2. Матрица $A \in \mathbf{Z}^{n\times n}$ *подобна* матрице $B \in \mathbf{Z}^{n\times n}$ над кольцом целых чисел $\mathbf{Z}$, если существует такая матрица $X \in \mathbf{Z}^{n\times n}$, что $AX = XB$

и $\det X \in \{-1, 1\}$. Матрица X называется матрицей, трансформирующей A в B.

Одним из необходимых условий условия подобия матриц является равенство их характеристических многочленов. Здесь будем рассматривать матрицы третьего порядка, имеющие приводимый над $\mathbf{Z}$ характеристический многочлен вида

$$d(\lambda) = (\lambda - \alpha)(\lambda^2 + p\lambda + q), \tag{1}$$

где $\alpha \in \mathbf{Z}$ и $\lambda^2 + p\lambda + q$ неприводим над $\mathbf{Z}$. Пусть матрица $A \in \mathbf{Z}^{3\times 3}$ имеет характеристический многочлен вида (1). Тогда A подобна над полем рациональных чисел $\mathbf{Q}$ блочно-диагональной матрице Фробениуса $F = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & -p & -q \\ 0 & 1 & 0 \end{pmatrix}$. При этом над $\mathbf{Z}$ матрица A подобна блочной матрице $\left(\begin{array}{c|c} \alpha & a \\ \hline 0 & A' \end{array}\right)$, где $a^\top \in \mathbf{Z}^2$, $A' \in \mathbf{Z}^{2\times 2}$ и характеристический многочлен матрицы A' равен $\lambda^2 + p\lambda + q$.

Выясним, при каких условиях матрицы

$$A = \left(\begin{array}{c|c} \alpha & a \\ \hline 0 & A' \end{array}\right), B = \left(\begin{array}{c|c} \alpha & b \\ \hline 0 & B' \end{array}\right) \tag{2}$$

подобны над $\mathbf{Z}$. Если они подобны, то найдется такая матрица $S = \left(\begin{array}{c|c} t & u \\ \hline v & S' \end{array}\right)$, что $AS = SB$ и $\det S \in \{-1, 1\}$. Поскольку

$$AS = \left(\begin{array}{c|c} \alpha t + av & \alpha u + aS' \\ \hline A'v & A'S' \end{array}\right) = \left(\begin{array}{c|c} \alpha t & tb + uB' \\ \hline \alpha v & vb + S'B' \end{array}\right) = SB, \tag{3}$$

то $A'v = \alpha v$. Отсюда следует, что $v = 0$, так как характеристический многочлен матрицы A' неприводим над $\mathbf{Z}$, и матрица A' не имеет целых собственных чисел. Следовательно, $t, \det S' \in \{1, -1\}$. Итак, $S = \left(\begin{array}{c|c} \pm 1 & u \\ \hline 0 & S' \end{array}\right)$. Из (3) также следует, что $A'S' = S'B'$, $u(B' - \alpha E) = aS' \pm b$. Тем самым доказано следующее утверждение.

Утверждение 1. *Матрицы вида* (2) *подобны над* $\mathbf{Z}$ *тогда и только тогда, когда выполняются два условия:*
1) A' *и* B' *подобны над* $\mathbf{Z}$*;*
2) *существует такая матрица* S' (*трансформирующая* A' *в* B')*, что вектор* $u = (aS' \pm b)(B' - \alpha E)^{-1}$ *является целочисленным.*

Выясним, как проверить эти условия. Рассмотрим множество матриц $M = \{S \in \mathbf{Z}^{2\times 2} \mid A'S = SB'\}$, которое является подмодулем в $\mathbf{Z}^{2\times 2}$. Известно, что размерность этого модуля равна 2. Пусть T_1 и T_2 — базис $\Lambda_{A',B'}$,

тогда любую матрицу из M можно представить в виде $xT_1 + yT_2$ для некоторых целых x и y. Для того, чтобы матрицы A' и B' были подобны над $\mathbf{Z}$ необходимо и достаточно разрешимости в целых числах диофантова уравнения $f(x,y) = \det(xT_1 + yT_2) = a'x^2 + b'xy + c'y^2 = \pm 1$. Пусть $D = b'^2 - 4a'c'$ — дискриминант квадратичной формы $f(x,y)$. Тогда дискриминант d характеристического многочлена $g(\lambda) = \det(A' - \lambda E) = \det(B' - \lambda E)$ равен $d = Dh^2$ для некоторого $h \in \mathbf{Z}$ (см., например, [1]). Поскольку d не является полным квадратом в силу неприводимости $g(\lambda)$, то и D не является полным квадратом. Возможны два случая: 1) $f(x,y)$ — знакоопределенная квадратичная форма (если $D < 0$); 2) $f(x,y)$ — неопределенная квадратичная форма (если $D > 0$). Еще Гауссом и Лагранжем рассматривалась задача нахождения целочисленных решений уравнения $a'x^2 + b'xy + c'y^2 = \pm 1$. Если оно не имеет целочисленных решений, то матрицы вида (2) не подобны над $\mathbf{Z}$. В противном случае нужно проверить выполнение второго условия утверждения 1.

Если $D < 0$, то уравнение $f(x,y) = \pm 1$ имеет конечное число решений, либо не имеет решений, следовательно, число матриц, трансформирующих A' в B', конечно. Поэтому проверку второго условия утверждения 1 можно осуществить перебором.

Если $D > 0$, то уравнение $f(x,y) = \pm 1$ либо не имеет решений, либо имеет счетное множество решений (x_n, y_n). При этом любое решение уравнения $f(x,y) = \pm 1$ можно получить, зная его минимальное положительное решение (x_0, y_0) и минимальное положительное решение (x', y') уравнения Пелля $x^2 - Dy^2 = \pm 1$. А именно, если обозначить $Q = \begin{pmatrix} x' - b'y' & -2c'y' \\ 2a'y' & x' + b'y' \end{pmatrix}$, то $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = Q^n \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$, $n \in \mathbf{Z}$, $\det Q \in \{\pm 1\}$. Таким образом, любая матрица, трансформирующая A' в B', имеет вид

$$S_n = x_n T_1 + y_n T_2, \ n \in \mathbf{Z} \tag{4}$$

Осталось проверить, существует ли такое n, что вектор $u = (aS_n \pm b)(B' - \alpha E)^{-1}$ является целочисленным. Это условие равносильно системе сравнений

$$(aS_n \pm b)(B' - \alpha E)^* \equiv 0 \pmod{\Delta},$$

где $\Delta = |\det(B' - \alpha E)|$, $(B' - \alpha E)^*$ — присоединенная матрица для $B' - \alpha E$. Заметим, что достаточно рассматривать $0 \leqslant n \leqslant 2\Delta - 1$. Действительно, множество матриц $G = \{Q^n \pmod{\Delta} | n \in \mathbf{Z}\}$ по модулю Δ образует циклическую группу. Так как $\det Q \in \{-1, 1\}$, то $Q^n = tQ + E$ или $Q^n = tQ - E$ для некоторого целого t. Следовательно,

$$|G| \leqslant 2\Delta.$$

Итак, второе условие утверждения 1 можно проверить за конечное число шагов. Таким образом, имеет место следующая теорема.

Теорема. *Матрицы вида* (2) *подобны над* $\mathbf{Z}$ *тогда и только тогда, когда выполняются условия*:
1) A' *и* B' *подобны над* $\mathbf{Z}$;
2) *существует такая матрица* S_n *вида* (4), $0 \leqslant n \leqslant 2\Delta - 1$, *что вектор* u, *равный* $(aS_n \pm b)(B' - \alpha E)^{-1}$, *является целочисленным.*

Утверждение 2. *Пусть характеристический многочлен матрицы* A' *равен* $\lambda^2 + p\lambda + q$. *Тогда матрица* $A_1 = \left(\begin{array}{c|c} \alpha & a \\ \hline 0 & A' \end{array}\right)$ *подобна над* $\mathbf{Z}$ *матрице* $A_2 = \left(\begin{array}{c|c} \alpha & r \\ \hline 0 & A' \end{array}\right)$, *где* $a = (a_1, a_2)$, $r = (r_1, r_2)$, r_i — *остаток от деления* a_i *на* $\Delta = |\alpha^2 + p\alpha + q|$, $i = 1, 2$.

Доказательство. Положим $S = \left(\begin{array}{c|c} 1 & q \\ \hline 0 & E \end{array}\right)$, где вектор $q \in \mathbf{Z}^2$ является решением системы линейных уравнений $a - r = q(A' - \alpha E)$. Тогда $A_1 S = S A_2$, $\det S = 1$. Утверждение доказано.

Поскольку число классов подобия матриц второго порядка, имеющих неприводимый характеристический многочлен, конечно (см., например, [1]), то верно следующее утверждение.

Утверждение 3. *Число классов подобия матриц третьего порядка, имеющих характеристический многочлен вида* (1), *конечно.*

Работа выполнена при поддержке ФЦП «Научные и научно-педагогические кадры инновационной России», соглашение №14.B37.21.0393.

Список литературы

1. Шевченко В. Н., Сидоров С. В. О подобии матриц второго порядка над кольцом целых чисел // Известия ВУЗ. Математика. — 2006. — № 4. —С. 57–64.

ПЕРМАНЕНТЫ МНОГОМЕРНЫХ МАТРИЦ

А. А. Тараненко (Новосибирск)

Введение

Пусть A — матрица порядка n, $A = (a_{ij})_{i,j=1}^n$. *Перманентом* матрицы A называется величина

$$\mathrm{per} A = \sum_{\sigma \in S_n} \prod_{i=1}^n a_{i\sigma i}.$$

Матрица A называется *неотрицательной*, если $a_{ij} \geqslant 0$ для любых значений $i, j \in \{1, \ldots, n\}$. Неотрицательная матрица A называется *дважды стохастической*, если $\sum\limits_{j=1}^{n} a_{ij} = 1$ для любых $i \in \{1, \ldots, n\}$ и $\sum\limits_{i=1}^{n} a_{ij} = 1$ для любых $j \in \{1, \ldots, n\}$. Обозначим через J_n — матрицу порядка n, каждый элемент которой равен $1/n$.

В 1926 году Ван дер Варденом была выдвинута гипотеза, что перманент любой дважды стохастической матрицы порядка n не меньше, чем $\frac{n!}{n^n}$, причем равенство достигается только на матрице J_n. Эта гипотеза была доказана Г. П. Егорычевым [6] и Д. И. Фаликманом [9]. Также, Минк сделал предположение, что перманент (0,1)-матриц порядка n не превосходит $\prod\limits_{i=1}^{n} r_i!^{1/r_i}$, где r_i есть количество единиц в i-ой строке матрицы. Данное утверждение было доказано в разное время Брэгманом [1], Шривером [4] и Рамакришнаном [3].

Понятие перманента можно обобщить на матрицы произвольной размерности. Тогда число замощений регулярного графа выражается через многомерный перманент некоторой неотрицательной матрицы, в частности, как многомерный перманент выражается число 1-совершенных кодов [5].

Латинским квадратом порядка n называется такая таблица чисел $n \times n$, что каждое число встречается в каждой строке и каждом столбце ровно один раз. *Трансверсалью* латинского квадрата порядка n называется набор из n элементов такой, что в любой строке или столбце лежит ровно один выбранный элемент, и значения всех элементов различны. Обозначим через $T(n)$ максимальное число трансверсалей по всем латинским квадратам порядка n.

В работе [2] показано, что $b_1^n \leqslant T(n) \leqslant b_2^n \sqrt{n} n!$, где $b_1 \approx 1,719$ и $b_2 \approx 0,614$. При $n \to \infty$ правую часть неравенства можно переписать в виде $T(n) \leqslant n^n e^{-cn+o(n)}$, где $c \approx 1,48$.

1. Определения

Пусть $n, d \in \mathbb{N}$ и пусть $I = \{(\alpha_1 \ldots \alpha_d) : \alpha_i \in \{1, \ldots, n\}\}$ — множество индексов. Будем называть *d-мерной матрицей A порядка n* массив чисел $(a_\alpha)_{\alpha \in I}$, $a_\alpha \in \mathbb{R}$.

Пусть $k \in \{0, \ldots, d\}$. *k-мерной гранью* матрицы A называется множество ее элементов, у которых зафиксированы значения $d - k$ координат, а остальные k координат пробегают все n значений. Произвольную $(d-1)$-мерную грань будем называть *гипергранью*. Обозначим через $L^k(A)$ множество всех k-мерных граней матрицы A.

Для d-мерной матрицы A порядка n и $\alpha \in I$ *минором элемента a_α* называется d-мерная матрица $(A|\alpha)$ порядка $n-1$, которая получается из A вычеркиванием всех таких элементов a_β, что для некоторого $i \in \{1, \ldots, d\}$ выполняется $\alpha_i = \beta_i$.

Неотрицательная матрица A называется *полистохастической*, если сумма элементов в любой ее одномерной грани равна единице. Назовем *нормой*

функцию w, которая сопоставляет матрице (или некоторой ее части) сумму всех ее элементов.

Для d-мерной матрицы A порядка n обозначим через $D(A)$ — множество всех ее диагоналей

$$D(A) = \{(a_{\alpha_1}, \ldots, a_{\alpha_n}) | a_{\alpha_i} \in A, \forall i \neq j \ \rho(\alpha_i, \alpha_j) = d\},$$

где ρ — расстояние Хэмминга.

Перманентом матрицы A называется величина

$$\mathrm{per}A = \sum_{p \in D} \prod_{a_\alpha \in p} a_\alpha.$$

Каждому латинскому квадрату порядка n можно поставить в соответствие трехмерную (0,1)-матрицу по следующему правилу: элемент латинского квадрата с координатами (i, j) равен k тогда и только тогда, когда $a_{ijk} = 1$. Заметим, что перманент построенной матрицы будет равен числу трансверсалей соответствующего ей латинского квадрата.

Пусть $n, d \in \mathbb{N},\ d \geqslant 3,\ \gamma \in \mathbb{R},\ 0 \leqslant \gamma \leqslant n^{d-2}$. Введем множество d-мерных матриц порядка n

$$M^d_{n,\gamma} = \left\{ (a_\alpha)_{\alpha \in I} | a_\alpha \geqslant 0, \sum_{\alpha \in I} a_\alpha = \gamma n, \forall l \in L^1(A) \ \sum_{a_\alpha \in l} a_\alpha \leqslant 1 \right\}.$$

Обозначим

$$P^d_n(\gamma) = \max_{A \in M^d_{n,\gamma}} \mathrm{per}A,$$

а также

$$\varphi^d_n(\gamma) = \frac{\ln P^d_n(\gamma)}{n} - \ln \gamma + d - 1, \text{ т. е. } P^d_n(\gamma) = \gamma^n e^{-(d-1)n + \varphi^d_n(\gamma) n}.$$

2. Свойства функций $P^d_n(\gamma)$ и $\varphi^d_n(\gamma)$

1. $P^d_n(\gamma)$ и $\varphi^d_n(\gamma)$ непрерывны по γ в силу непрерывности перманента и непрерывности изменения множества $M^d_{n,\gamma}$.

2. $P^d_n(\gamma)$ и $\varphi^d_n(\gamma)$ дифференцируемы слева для любого $\gamma \in (0, n^{d-2}]$.

3. Для любых $n, d \in \mathbb{N},\ d \geqslant 3,\ \gamma \in \mathbb{R},\ 0 \leqslant \gamma \leqslant n^{d-2}$ верно $0 \leqslant \varphi^d_n(\gamma) \leqslant d-1$.

4. Пусть $n, d \in \mathbb{N},\ d \geqslant 3,\ \gamma \in \mathbb{R},\ 0 < \gamma < n^{d-2}$ и обозначим через $J^d_{n,\gamma}$ d-мерную матрицу порядка n, каждый элемент которой равен γ / n^{d-1}. Тогда $\mathrm{per}J^d_{n,\gamma} < P^d_n(\gamma)$.

5. Для фиксированных n и d функция $\varphi^d_n(\gamma)$ невозрастает.

3. Локальный экстремум многомерного перманента

Несложно показать [7], что матрица J_n будет точкой локального минимума перманента в классе дважды стохастических матриц. Аналогичными методами можно доказать, что равномерная матрица является точкой локального экстремума перманента в классе полистохастических матриц любой размерности. Для этого потребуется следующая лемма.

Лемма 1. *Пусть A — некоторая d-мерная полистохастическая матрица порядка n. Тогда норма минора $(A|\alpha)$ равна*

$$\sum_{j=0}^{d-1}(-1)^j C_d^j n^{d-j-1} + (-1)^d a_\alpha.$$

Обозначим через J_n^d d-мерную матрицу порядка n, каждый элемент которой равен $1/n$. Тогда верна следующая теорема.

Теорема 1. *J_n^d — точка экстремума для функции перманента на множестве d-мерных полистохастических матриц порядка n, причем при четном d на J_n^d перманент имеет локальный минимум, при нечетном — локальный максимум.*

4. Дифференциальное неравенство на функцию $P_n^d(\gamma)$

Для функции $P_n^d(\gamma)$ можно доказать дифференциальное неравенство, из которого может быть получена оценка на саму функцию. Для этого необходимы две вспомогательные леммы.

Лемма 2. *Пусть $n, d \in \mathbb{N}$, $d \geqslant 3$, $\gamma \in \mathbb{R}$, $1 \leqslant \gamma \leqslant n^{d-2}$ и пусть $A \in M_{n,\gamma}^d$ — матрица, для которой* $\mathrm{per}A > 0$. *Тогда существует такой элемент матрицы $a_\alpha > 0$, что норма соответствующего ему минора $(A|\alpha)$ не превосходит величины $\gamma\left(n - d + C_d^2 \frac{n^{d-3}}{\gamma}\right)$:*

$$w(A|\alpha) \leqslant \gamma\left(n - d + C_d^2 \frac{n^{d-3}}{\gamma}\right).$$

Следующее утверждение позволяет связать перманент произвольной матрицы с перманентами матриц меньшего порядка и меньшим значением γ.

Лемма 3. *Пусть $n, d \in \mathbb{N}$, $d \geqslant 3$, $\gamma \in \mathbb{R}$, $dn^{d-3} \leqslant \gamma \leqslant n^{d-2}$ и пусть $A \in M_{n,\gamma}^d$ — матрица, для которой* $\mathrm{per}A > 0$. *Тогда для достаточно малых $\varepsilon > 0$ существует семейство матриц $A^\varepsilon \in M_{n,\gamma-\varepsilon}^d$ и матрица $B \in M_{n-1,\gamma_B}^d$, где $\gamma - \frac{dn^{d-2}-\gamma}{n-1} \leqslant \gamma_B \leqslant \gamma\left(1 - \frac{d-1-C_d^2 n^{d-3}/\gamma}{n-1}\right)$, такие, что*

$$\mathrm{per}A = \mathrm{per}A^\varepsilon + \varepsilon n \mathrm{per}B.$$

Используя приведенные леммы, можно получить дифференциальное неравенство на $P_n^d(\gamma)$.

Утверждение 1. *Пусть* $n, d \in \mathbb{N},\ d \geqslant 3,\ \gamma \in \mathbb{R},\ dn^{d-3} \leqslant \gamma \leqslant n^{d-2}$. *Тогда* $P_n^d(\gamma)$ *удовлетворяет неравенству*

$$\frac{dP_n^d(\gamma)}{d\gamma} \leqslant nP_{n-1}^d(\tilde{\gamma})$$

для некоторого $\tilde{\gamma}$ *из интервала* $\left[\gamma - \frac{dn^{d-2}-\gamma}{n-1}, \gamma\left(1 - \frac{d-1-C_d^2 n^{d-3}/\gamma}{n-1}\right)\right]$.

5. Асимптотическая верхняя оценка перманентов многомерных матриц

Теорема 2. *Пусть* $d \geqslant 3$. *Тогда для любого* $\delta \in (0, 1]$ *максимум перманента* d*-мерных матриц из множества* $M_{n,\gamma}^d$ *при* $\gamma = n^{d-3+\delta}$ *и* $n \to \infty$ *равен* $\gamma^n e^{-(d-1)n+o(n)}$:

$$P_n^d(\gamma) = \gamma^n e^{-(d-1)n+o(n)}.$$

Из теоремы 2 следует асимптотическая верхняя оценка числа трансверсалей латинских квадратов

$$T(n) \leqslant P_n^3(n) = n^n e^{-2n+o(n)},$$

которая является улучшением оценки, полученной в [2].

Пусть $\delta, \varepsilon \in (0, 1]$ — произвольные. Рассмотрим функцию

$$F_n^d(\gamma) = \gamma^n e^{-n\left(d-2+\frac{\ln(\gamma/n^{d-3})}{\delta \ln n}\right)(1-\varepsilon)}.$$

Идея доказательства теоремы 2 заключается в том, чтобы показать, что $F_n^d(\gamma)$ мажорирует $P_n^d(\gamma)$ для всех достаточно больших n и $\gamma \in \Delta$, где Δ — некоторый промежуток вида $[g^d(n), n^{d-3+\delta}]$. Для этого нужно доказать, что, при подходящем разбиении Δ на два промежутка Δ_1 и Δ_2, функция F является мажорантой при $\gamma \in \Delta_1$ и что производная F не меньше, чем производная P при $\gamma \in \Delta_2$ для всех достаточно больших n. Кроме того, для доказательства теоремы 2 необходимо следующее утверждение, являющееся следствием [4].

Утверждение 2. *Пусть* A *— неотрицательная двумерная матрица порядка* n, *каждый элемент которой не превосходит единицы, и пусть выполнено* $\sum\limits_{i,j=1}^{n} a_{ij} = \gamma n$. *Тогда*

$$\mathrm{per}A \leqslant \lceil\gamma\rceil!^{\frac{n}{\lceil\gamma\rceil}}.$$

Список литературы

1. Bregman L. M. Some properties of nonnegative matrices and their permanents // Soviet Math. Dokl. — 1973. — 14. — P. 945–949.
2. McKay B. D., McLeod J. C., Wanless I. M. The number of transversals in a Latin square. // Des Codes Crypt — 2006. — 40. — P. 269–284.
3. Radhakrishnan J. An entropy proof of Bregman's theorem // Journal of combinatorial theory. — 1997. — Series A 77. — P. 161–164.
4. Schrijver A. A short proof of Minc's conjecture // Journal of combinatorial theory. — 1978. — Series A 25. — P. 80–83.
5. Августинович С. В. Многомерные перманенты в задачах перечисления // Дискретный анализ и исследование операций. — 2008. — Т. 15, № 5. — С. 3–5.
6. Егорычев Г. П. Решение проблемы Ван дер Вардена для перманентов // Сибирский математический журнал. — 1981. — Т. 22, № 6. — С. 65-71.
7. Минк Х. Перманенты. — М.: Мир, 1982.
8. Тараненко А. А. Верхняя оценка числа трансверсалей латинского квадрата // Материалы 51-й международной научной студенческой конференции «Студент и научно-технический прогресс», математика (Новосибирск, 12-18 апреля 2013 г.). — Новосибирск: Редакционно-издательский центр НГУ — 2013. — С. 236.
9. Фаликман Д. И. Доказательство гипотезы Ван дер Вардена о перманенте дважды стохастической матрицы // Матем. заметки. — 1981. — Т. 29, вып. 6. — С. 931-938.

О ВОССТАНОВЛЕНИИ БАЗ ДАННЫХ ДЛЯ НЕКОТОРЫХ ФОРМУЛ-ОГРАНИЧЕНИЙ СПЕЦИАЛЬНОГО ВИДА

Е. Е. Трифонова (Москва)

Введение

В настоящий момент наблюдается большой интерес к базам данных с большими объемами информации, поступающей из множественных источников. Для таких баз данных часта ситуация, когда возникают противоречия, т. е. об одних и тех же вещах содержится разная (противоречащая друг другу) информация. Существуют различные способы работы с возникающими противоречиями [2]. Рассматриваемая в настоящей работе модель наиболее близка к модели, рассматриваемой в [1].

1. Основные определения

Схемой базы данных будем называть совокупность $\langle \mathbb{P}, \Phi \rangle$, где $\mathbb{P}$ — конечное множество предикатов, Φ — формула-ограничение. *Базой данных* D назовем совокупность $D = \langle \mathbb{T}, \Phi \rangle$, где $\mathbb{T}$ — множество таблиц. При этом каждому предикату P из $\mathbb{P}$ ставится в соответствие таблица T из $\mathbb{T}$, которая определяет значение истинности предиката. Элементом таблицы является *кортеж*. $X = X(D)$ — множество всех кортежей базы данных D, $X = \bigcup\limits_{T \in \mathbb{T}} X_T$. *Вспомогательным предикатом* $g(x_1, x_2)$ будем называть конструкцию вида

$$g(x_1, x_2) = f_i(x_1) \mathcal{R} f_j(x_2),$$

где $f_i, f_j \in F$, $F : X \to \mathbb{N}$, $\mathcal{R}$ — одно из отношений $<, >, \leqslant, \geqslant, \neq, =$.

Будем обозначать как G множество всевозможных вспомогательных предикатов. *Вспомогательным условием* будем называть выражение

$$h(x_1, \ldots, x_n) = g_1(x_{i_1}, x_{j_1}) \Diamond g_2(x_{i_2}, x_{j_2}) \Diamond \ldots \Diamond g_k(x_{i_k}, x_{j_k}),$$

где $i_1, \ldots, i_k, j_1, \ldots, j_k \in \{1, \ldots, n\}, g_1, g_2, \ldots, g_k \in G$, $\Diamond$ — место размещения логических операторов & и $\vee$.

Тогда формула-ограничение Φ — это замкнутая формула на языке первого порядка, записанная с использованием связок $\vee$, &, $\neg$, $\to$, предикатов из $\mathbb{P}$ и из G. Если Φ истинна на множестве X, то будем говорить, что база данных D — *непротиворечивая*. Если Φ ложна на множестве X, то будем говорить, что в D *содержатся противоречия*.

Восстановлением Q для базы данных D будем называть базу данных, для которой выполняется следующее:

1. Схемы баз данных Q и D совпадают.
2. Каждый кортеж из таблицы Q содержится в соответствующей таблице D.
3. База данных Q — непротиворечивая.
4. Добавление к Q любого кортежа из D, который в Q не содержится, в соответствующую таблицу приводит к тому, что в Q возникают противоречия.

Будем называть *наилучшим восстановлением* — восстановление, содержащее наибольшее число кортежей среди всех восстановлений для рассматриваемой базы данных. Наилучших восстановлений может быть несколько.

2. Разбиение формул-ограничений на подклассы

Рассмотрим следующие виды формул:

$$\forall x(P(x) \to h(x)) \tag{I}$$

$$\forall x_1 \forall x_2(P(x_1)\&P(x_2) \to h(x_1, x_2)) \tag{II}$$

$$\forall x_1 \exists x_2(P_1(x_1) \to P_2(x_2)\&h_1(x_1, x_2) \vee h_2(x_1)) \tag{III}$$

Назовем классом A множество конечных формул, построенных из формул вида (I), (II), (III), соединенных &. Тогда ограничения, которые накладываются на базы данных в базовой версии SQL, могут быть записаны с помощью формул, принадлежащих классу A, см. [3].

Разобьем все формулы, выразимые в классе A, на следующие подклассы:

1. конъюнкция одного вида формул (первый подкласс):
   (I) & (I) & ... & (I);
   (II) & (II) & ... & (II);
   (III) & (III) & ... & (III);
2. конъюнкция двух видов формул (второй подкласс):
   (I) & ... & (I) & (II) & ... & (II);
   (II) & ... & (II) & (III) & ... & (III);
   (I) & ... & (I) & (III) & ... & (III);
3. конъюнкция трех видов формул (третий подкласс):
   (I) & ... & (I) & (II) & ... & (II) & (III) & ... & (III).

Под конъюнкцией одного вида формул и записью (I) & (I) & ... & (I) будем подразумевать, что вся формула имеет вид:

$$\forall x_1(P_1(x_1) \to h_1(x_1))\&\forall x_2(P_2(x_2) \to h_2(x_2))\& \ldots \&$$

$$\&\forall x_{k-1}(P_{k-1}(x_{k-1}) \to h_{k-1}(x_{k-1}))\&\forall x_k(P_k(x_k) \to h_k(x_k)). \tag{1}$$

Для конъюнкций других видов формул в рамках первого подкласса подобное сокращенное обозначение будет расшифровываться аналогичным образом.

Под конъюнкцией двух видов формул (I) & ... & (I) & (II) & ... & (II) будем подразумевать, что вся формула имеет вид:

$$\forall x_1(P_1(x_1) \to h_1(x_1))\& \ldots \&\forall x_k(P_k(x_k) \to h_1(x_k))\&$$

$$\&\forall x_{k+1}\forall x_{k+2}(P_{k+1}(x_{k+1})\&P_{k+1}(x_{k+2}) \to h_{k+1}(x_{k+1}, x_{k+2}))\& \ldots \&$$

$$\&\forall x_{k+2m-1}\forall x_{k+2m}(P_{k+m}(x_{k+2m-1})\&$$

$$\&P_{k+m}(x_{k+2m}) \to h_{k+m}(x_{k+2m-1}, x_{k+2m})). \quad (2)$$

Для конъюнкций других видов формул в рамках второго подкласса подобное сокращенное обозначение будет расшифровываться аналогичным образом, так же как и для конъюнкции трех видов формул (третий подкласс).

3. Восстановления для первого подкласса формул

Для первого подкласса формул для построения наилучших восстановлений справедливы следующие утверждения.

Утверждение 1. *Пусть* $D = \langle \mathbb{T}, \Phi \rangle$, $P_1, \ldots, P_n \in \mathbb{P}$ *и* $T_1, \ldots, T_n$ — *соответствующие им таблицы,*

$$\Phi = (\mathrm{I})\&(\mathrm{I})\& \ldots \&(\mathrm{I}),$$

и в базе данных D *содержатся противоречия.*

Тогда существует единственное восстановление для D. *Оно будет являться наилучшим.*

Графом противоречий будем называть гиперграф (т. е. граф, у которого ребро может соединять более чем две вершины), вершинами которого являются кортежи, а ребрами соединены те кортежи, которые не могут совместно присутствовать ни в одном восстановлении.

Утверждение 2. *Пусть* $D = \langle \mathbb{T}, \Phi \rangle$, $P_1, \ldots, P_n \in \mathbb{P}$ *и* $T_1, \ldots, T_n$ — *соответствующие им таблицы,*

$$\Phi = (\mathrm{II})\&(\mathrm{II})\& \ldots \&(\mathrm{II}),$$

и в базе данных D *содержатся противоречия.*

Тогда для D *может существовать несколько наилучших восстановлений. Задача поиска наилучшего восстановления сводится к поиску максимального независимого множества для графа противоречий.*

Утверждение 3. *Пусть* $D = \langle \mathbb{T}, \Phi \rangle$, $P_1, \ldots, P_n \in \mathbb{P}$ *и* $T_1, \ldots, T_n$ — *соответствующие им таблицы,*

$$\Phi = (\mathrm{III})\&(\mathrm{III})\& \ldots \&(\mathrm{III}),$$

и в базе данных D *содержатся противоречия.*

Тогда для D *существует одно восстановление, наилучшее.*

4. Восстановления для второго подкласса формул

Для второго подкласса формул для построения наилучших восстановлений справедливы следующие утверждения.

Утверждение 4. *Пусть* $D = \langle \mathbb{T}, \Phi \rangle$, $P_1, \ldots, P_n \in \mathbb{P}$ *и* $T_1, \ldots, T_n$ — *соответствующие им таблицы,*

$$\Phi = (\mathrm{I}) \& \ldots \& (\mathrm{I}) \& (\mathrm{II}) \& \ldots \& (\mathrm{II}),$$

и в базе данных D *содержатся противоречия.*

Тогда может быть несколько наилучших восстановлений для D. *Сначала строим наилучшее восстановление для части* (I) & ... & (I) *формулы* (*т. е. для базы данных* $\langle \mathbb{T}, (\mathrm{I}) \& \ldots \& (\mathrm{I}) \rangle$), *а затем находим множество наилучших восстановлений для части* (II) & ... & (II) (*т. е. для базы данных* $\langle \mathbb{T}', (\mathrm{II}) \& \ldots \& (\mathrm{II}) \rangle$, *где* $\mathbb{T}'$ — *таблицы базы данных* D *после проведения первой операции*).

Утверждение 5. *Пусть* $D = \langle \mathbb{T}, \Phi \rangle$, $P_1, \ldots, P_n \in \mathbb{P}$ *и* $T_1, \ldots, T_n$ — *соответствующие им таблицы,*

$$\Phi = (\mathrm{I}) \& \ldots \& (\mathrm{I}) \& (\mathrm{III}) \& \ldots \& (\mathrm{III}),$$

и в базе данных D *содержатся противоречия.*

Тогда для D *существует только одно восстановление, наилучшее. Сначала строим наилучшее восстановление для части* (I) & ... & (I) *формулы* (*т. е. для базы данных* $\langle \mathbb{T}, (\mathrm{I}) \& \ldots \& (\mathrm{I}) \rangle$), *а затем для части* (III) & ... & (III) (*т. е. для базы данных* $\langle \mathbb{T}', (\mathrm{III}) \& \ldots \& (\mathrm{III}) \rangle$, *где* $\mathbb{T}'$ — *таблицы базы данных* D *после проведения первой операции*).

Утверждение 6. *Пусть* $D = \langle \mathbb{T}, \Phi \rangle$, $P_1, \ldots, P_n \in \mathbb{P}$ *и* $T_1, \ldots, T_n$ — *соответствующие им таблицы,*

$$\Phi = (\mathrm{II}) \& \ldots \& (\mathrm{II}) \& (\mathrm{III}) \& \ldots \& (\mathrm{III}),$$

и в базе данных D *содержатся противоречия. Кроме этого, для формулы* Φ *выполняется следующее: предикаты из части формулы* (II) & ... & (II) *не используются на вторых местах* (*в качестве второго предиката*) *части формулы* (III) & ... & (III).

Тогда может быть несколько наилучших восстановлений для D. *Сначала строим наилучшее восстановление для части* (III) & ... & (III) (*т. е. для базы данных* $\langle \mathbb{T}, (\mathrm{III}) \& \ldots \& (\mathrm{III}) \rangle$) *формулы, а затем для части* (II) & ... & (II) (*т. е. для базы данных* $\langle \mathbb{T}', (\mathrm{II}) \& \ldots \& (\mathrm{II}) \rangle$, *где* $\mathbb{T}'$ — *таблицы базы данных* D *после проведения первой операции*).

Работа выполнена при финансовой поддержке РФФИ (грант 11-07-00311) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Chomicki, J., Marchinkowski, J. Minimal-change integrity maintenance using tuple deletion. // Inf. Comput. — 2005. — V. 197(1–2). — P. 90–121.
2. Motro A. Sources of Uncertainty, Imprecision and Inconsistency in Information Systems. // Uncertainty Management in Information Systems: From Needs to Solutions / Motro A., Smets P. Eds. — Kluwer Academic Publishers, 1996. — Ch. 2. — P. 9–34.
3. Трифонова Е.Е. О представлении ограничений, записанных с помощью SQL, для построения восстановлений баз данных // Материалы VIII молодежной школы по дискретной математике и ее приложениям (Москва, 24-29 октября 2011 г.) — 2011. — Ч. II. — С. 30–35.
4. Трифонова Е.Е. О построении восстановлений баз данных для некоторых классов формул-ограничений // Вестник Нижегородского университета им. Н.И.Лобачевского. — 2012. — № 5(2). —С. 214–218.

О РЕКУРСИВНЫХ КОНСТРУКЦИЯХ ПЛАТОВИДНЫХ УСТОЙЧИВЫХ БУЛЕВЫХ ФУНКЦИЙ

Е. В. Хинко (Москва)

Введение

Вопрос корреляционной иммунности и устойчивости булевых функций имеет большое криптографическое значение и поднимается в работах многих авторов. Например, в работах [3] и [5] затрагивается проблема устойчивости функций при максимальных значениях нелинейности, а в работах [4] и [6] построены соответствующие конструкции функций.

В работе [1] Ю. В. Тарannиковым построены рекурсивные конструкции устойчивых функций с высокой нелинейностью, имеющие пары квазилинейных покрывающих переменных.

В представленной работе рассматривается вопрос порождения платовидных функций в рекурсивных конструкциях с шагом 3 и строятся конструкции, обеспечивающие рост устойчивости функций. К схожей теме уже обращался К. В. Захаров, исследовавший в работе [2] рекурсивные конструкции бент-функций (являются подмножеством платовидных) с шагом 2 переменных. Целью проделанной работы было найти и рассмотреть все возможные конструкции, обеспечивающие рост устойчивости на 1, 2 или 3 при шаге переменных 3, и изучить их свойства. В результате была проведена классификация

возможных конструкций в зависимости от значений и соотношений коэффициентов порождающих функций, конструкции, в тех случаях, где они есть, были найдены и проанализированы.

1. Основные определения и факты

Пусть f — произвольная булева функция от n переменных.

Определение 1. *Коффициентом Уолша* называется величина

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

где $< x, u >$ — стандартное скалярное произведение наборов.

Определение 2. Булева функция $f : V_n \to F_n^2$ называется *платовидной*, если $W_f(u) \in \{0, \pm 2^c\}\ \forall u \in V_n$.

Определение 3. Булева функция $f : V_n \to F_n^2$ называется *корреляционно-иммунной* порядка m, если $W_f(u) = 0\ \forall u : 1 \leqslant wt(u) \leqslant m$. Будем записывать это как $f \in CI(m)$.

Определение 4. Булева функция $f : V_n \to F_n^2$ называется *m-устойчивой*, если $f \in CI(m)$ и f уравновешена.

Определение 5. Функция f зависит от x_i и x_j *квазилинейно*, если для любых двух наборов x' и x'' длины n, различающихся только в i-й и j-й компонентах, выполнено $f(x') \neq f(x'')$.

Утверждение (равенство Парсеваля). $\sum\limits_{u \in V_n} W_f^2(u) = 4^n$.

2. Постановка задачи

Рассмотрим 8 булевых платовидных m-устойчивых функций $f_n^{i_j}$, $j \in \overline{1,8}$, от n переменных с одинаковым порядком платовидности. Некоторые из этих функций могут совпадать с точностью до отрицания. Мы хотим добавить три переменные и найти условия, при которых новые функции от $n+3$ переменных будут сохранять свойство платовидности (возможно с другим, но одинаковым порядком) и иметь больший порядок устойчивости, чем у исходных функций.

Запишем кратко:

$$\left(f_{n+3}^s = \sigma_{s1} g_{s1} \quad |\sigma_{s2} g_{s3} \quad |\sigma_{s3} g_{s3} \quad |\sigma_{s4} g_{s4} \quad |\sigma_{s5} g_{s5} \quad |\sigma_{s6} g_{s6} \quad |\sigma_{s7} g_{s7} \quad |\sigma_{s8} g_{s8}\right),$$

где $s = \overline{1,8}$, $\sigma_{ij} g_{ij} = \begin{cases} f_n^{a_{ij}}, \sigma_{ij} = 1 \\ \overline{f_n^{a_{ij}}}, \sigma_{ij} = -1 \end{cases}$.

3. Краткий обзор хода работы и полученные результаты

Из равенства Парсеваля следует, что число ненулевых коэффициентов Уолша у каждой из порождающих функций $f_n^{i_j}$, $j \in \overline{1,8}$, равно 4^{n-c}. Из этого легко видеть, что порядок платовидности у новых функций от $n+3$ переменных может быть равен $c+2$ или $c+3$.

Непосредственно проверяется, что коэффициенты Уолша преобразуются в соответствии с приведенной ниже матрицей, т. е. каждый коэффициент функции от $n+3$ переменных — линейная комбинация с коэффициентами ± 1 коэффициентов Уолша функций $f_n^{i_j}$, $j \in \overline{1,8}$.

$$\begin{pmatrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - \end{pmatrix} \tag{1}$$

Эта матрица называется *матрицей Адамара—Сильвестра* порядка 8.

Были последовательно рассмотрены три случая увеличения устойчивости функций на 3, 2 и 1, и для каждого из них подслучаи (увеличение коэффициентов Уолша в 8 и 4 раза) и подподслучаи.

Результат исследования кратко приведен в следующей теореме:

Теорема. *Соотношение*

$$f_{n+3}^s = \sigma_{s1} f_n^{i_1} | \sigma_{s2} f_n^{i_2} | \sigma_{s3} f_n^{i_3} | \sigma_{s4} f_n^{i_4} | \sigma_{s5} f_n^{i_5} | \sigma_{s6} f_n^{i_6} | \sigma_{s7} f_n^{i_7} | \sigma_{s8} f_n^{i_8}$$

1) *обеспечивает рост устойчивости на 3 с сохранением платовидности, если все функции* $f_n^{i_j}$, $j \in \overline{1,8}$, *совпадают с точностью до отрицания. При этом*:

- *новая функция одна,*

- *знаки* σ_{ij} *равны* (*здесь и далее с точностью до умножения всех на* -1) *соответствующим знакам* $sgn(W_{f_n^i}(u))$ *в 8-й строке матрицы* (1),

- *коэффициенты Уолша новых функций* f_{n+3}^s *по модулю в 8 раз больше коэффициентов Уолша порождающих функций* $f_n^{i_j}$, $j \in \overline{1,8}$,

- *данной конструкции соответствует добавление трех линейных переменных.*

2) *обеспечивает рост устойчивости на 2 с сохранением платовидности, если*

а) или все функции $f_n^{i_j}$, $j \in \overline{1,8}$, *совпадают с точностью до отрицания*:

- *новых функций четыре,*

- *знаки* σ_{sj} *равны соответствующим знакам* $sgn(W_{f_n^i}(u))$ *в 4-й, 6-й, 7-й или 8-й строках матрицы* (1),

- *коэффициенты Уолша новых функций* f_{n+3}^s *по модулю в 8 раз больше коэффициентов Уолша порождающих функций* $f_n^{i_j}$, $j \in \overline{1,8}$,

- *данной конструкции соответствует добавление трех линейных или двух линейных и одной фиктивной переменной в зависимости от строки из* σ_{sj}.

б) или порождающие функции $f_n^{i_j}$, $j \in \overline{1,8}$, *разбиваются на два подмножества из четырех совпадающих, удовлетворяющие условиям* α *и* β. *При этом*:

- *новых функций две, возможно рекурсивное применение,*

- *строки из* σ_{sj} *равны соответствующим знакам* $sgn(W_{f_n^i}(u))$ *в паре из 4-й, 6-й, 7-й или 8-й строк матрицы* (1) *в зависимости от подмножеств,*

- *ненулевые коэффициенты Уолша функций одного подмножества приходятся на нулевые коэффициенты Уолша функций другого и наоборот,*

- *коэффициенты Уолша новых функций* f_{n+3}^s *в 4 раза больше коэффициентов Уолша порождающих функций* $f_n^{i_j}$, $j \in \overline{1,8}$,

- *данной конструкции соответствует добавление пары квазилинейных и одной линейной переменной для одной из функций и трех линейных для второй.*

в) или порождающие функции $f_n^{i_j}$, $j \in \overline{1,8}$, *разбиваются четыре подмножества из двух совпадающих. При этом*:

- *новых функций можно получить четыре на одном шаге.*

- *строки из* σ_{sj} *равны соответствующим знакам* $sgn(W_{f_n^i}(u))$ *в 4-й, 6-й, 7-й или 8-й строках матрицы* (1),

- *коэффициенты Уолша новой функции* f_{n+3}^s *в 4 раза больше коэффициентов Уолша порождающих функций* $f_n^{i_j}$, $j \in \overline{1,8}$.

г) или порождающие функции $f_n^{i_j}$, $j \in \overline{1,8}$, *различны. При этом:*

- *новых функций можно получить четыре на одном шаге.*

- *строка из* σ_{sj} *равна соответствующим знакам* $sgn(W_{f_n^i}(u))$ *в 4,6,7 или 8 строках матрицы* (1),

- *коэффициенты Уолша новой функции* f_{n+3}^s *в 4 раза больше коэффициентов Уолша порождающих функций* $f_n^{i_j}$, $j \in \overline{1,8}$.

3) *обеспечивает рост устойчивости на 1 с сохранением платовидности, если*

а) или все функции $f_n^{i_j}$, $j \in \overline{1,8}$, *совпадают с точностью до отрицания*:

- *новых функций семь,*

- *знаки* σ_{sj} *равны соответствующим знакам* $sgn(W_{f_n^i}(u))$ *в строках матрицы* (1) (*кроме первой*).

- *коэффициенты Уолша новых функций* f_{n+3}^s *по модулю в 8 раз больше коэффициентов Уолша порождающих функций* $f_n^{i_j}$, $j \in \overline{1,8}$,

- данной конструкции соответствует добавление трех линейных или двух линейных и одной фиктивной или одной линейной и двух фиктивных переменных в зависимости от строки из σ_{sj}.

б) или все функции $f_n^{i_j}$, $j \in \overline{1,8}$, *совпадают с точностью до отрицания*:

- новых функций четыре,

- коэффициенты Уолша новых функций f_{n+3}^s *по модулю в 4 раза больше коэффициентов Уолша порождающих функций* $f_n^{i_j}$, $j \in \overline{1,8}$,

- конструкции соответствует добавление слагаемых второй степени.

в) или порождающие функции $f_n^{i_j}$, $j \in \overline{1,8}$, *разбиваются на два подмножества из четырех совпадающих, удовлетворяющие условиям* α *и* β. *При этом*:

- новых функций две, возможно рекурсивное применение,

- строки из σ_{sj} *равны соответствующим знакам* $sgn(W_{f_n^i}(u))$ *в паре 4 из выбираемого произвольно подмножества строк матрицы* (1) (*кроме первой*) *в зависимости от подмножеств,*

- ненулевые коэффициенты Уолша функций одного подмножества приходятся на нулевые коэффициенты Уолша функций другого и наоборот,

- коэффициенты Уолша новых функций f_{n+3}^s *в 4 раза больше коэффициентов Уолша порождающих функций* $f_n^{i_j}$, $j \in \overline{1,8}$,

- данной конструкции соответствует либо добавление пары линейных и одной фиктивной, либо трех линейных, либо пары квазилинейных и одной линейной переменной.

г) или порождающие функции $f_n^{i_j}$, $j \in \overline{1,8}$, *разбиваются на четыре подмножества из 2 совпадающих. При этом*:

- новых функций можно получить четыре на одном шаге,

- строки из σ_{sj} *равны соответствующим знакам* $sgn(W_{f_n^i}(u))$ *в 4 из выбираемого произвольно подмножества строк матрицы* (1) (*кроме первой*),

- коэффициенты Уолша новой функции f_{n+3}^s *в 4 раза больше коэффициентов Уолша порождающих функций* $f_n^{i_j}$, $j \in \overline{1,8}$.

д) или порождающие функции $f_n^{i_j}$, $j \in \overline{1,8}$, *различны. При этом*:

- новых функций можно получить восемь на одном шаге,

- строка из σ_{sj} *равна соответствующим знакам* $sgn(W_{f_n^i}(u))$ *в 4 из выбираемого произвольно подмножества строк матрицы* (1) *(кроме первой),*

- коэффициенты Уолша новой функции f_{n+3}^s *в 4 раза больше коэффициентов Уолша порождающих функций* $f_n^{i_j}$, $j \in \overline{1,8}$.

Условия α) и β):

α) В обоих подмножествах из четырех порождающих функций $f_n^{i_j}$, $j \in \overline{1,8}$, в каждой из половин i_1, i_2, i_3, i_4 и i_5, i_6, i_7, i_8 должно быть четное число функций.

β) Если оба подмножества из четырех порождающих функций $f_n^{i_j}$, $j \in \overline{1,8}$, содержат по две функции в каждой из половин i_1, i_2, i_3, i_4 и i_5, i_6, i_7, i_8, то в

обоих подмножествах в каждой из половин функции должны располагаться на симметричных или совпадающих местах с функциями другой половины.

Отметим, что некоторые из этих конструкций (1, 2а, 2б, 3а, 3б, 3в) были в разных смыслах известны ранее, а некоторые (2в, 2г, 3г, 3д) являются новыми.

Список литературы

1. Тарасников Ю. В. О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. — 2002. — Вып. 11. — С. 91–148.
2. Захаров К. В. О порождении бент-функций рекурсивными конструкциями. — Дипломная работа. Москва, 2008.
3. Fedorova M., Tarannikov Yu. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices // Progress in Cryptology — Indocrypt 2001, Chennai, India, December 16-20, 2001, Proceedings, Lecture Notes in Computer Science. — V. 2247. — Springer-Verlag, 2001. — P. 254–256.
4. Pasalic E., Maitra S., Johansson T., Sarkar P. New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity // WCC2001 International Workshop on Coding and Cryptography, Paris, January 8-12, 2001, Electronic Notes in Discrete Mathematics. — V.6. — Elsever Science. — 2001.
5. Tarannikov Yu. On resilient Boolean functions with maximal possible nonlinearity // Proceeding of Indocrypt 2000, Lecture Notes in Computer Science. — V. 1977. — Springer-Verlag, 2000. — P. 19–30.
6. Tarannikov Yu. New constructions of resilient Boolean functions with maximal nonlinearity // Fast Software Encryption. 8th International Workshop, FSE 2001, Yokohama, Japan, April 2–4, 2001 . Revised Papers, Lecture Notes in Computer Science. — V. 2355. — 2002. — P. 66–77.

ОЦЕНКИ ЧИСЛА ОБЛАСТЕЙ В РАЗБИЕНИЯХ ПЛОСКОСТИ НАБОРАМИ ПСЕВДОПРЯМЫХ

И. Н. Шнурников (Москва)

Введение

Псевдопрямой на вещественной проективной плоскости назовем замкнутую гладкую кривую без самопересечений, не ограничивающую диска (т. е. уходящую на бесконечность в представлении проективной плоскости в виде аффинной плоскости с бесконечно удаленными точками). Набором псевдопрямых назовем конечное множество из $n \geqslant 3$ псевдопрямых на проективной

плоскости, таких, что любые две из них пересекаются трансверсально в единственной точке, при этом все псевдопрямые не проходят через одну точку. Через t_i обозначим число точек пересечения, принадлежащих i псевдопрямым для $1 < i < n$. Через f обозначим число областей проективных плоскости, разделенной набором псевдопрямых. Эйлерова характеристика проективной плоскости приводит к соотношению

$$f = 1 + \sum_{i \geqslant 2} (i-1) t_i.$$

Интерес представляют возможные значения чисел t_i и соотношения между ними, см. обзоры П. Брасса и др. и Н. Нилакантана [1, 2].

Гипотеза Г. А. Дирака [3] утверждает, что $t_2 \geqslant \left[\frac{n}{2}\right]$, известен также пример с $t_2 = \frac{n}{2}$ для четных чисел $n \geqslant 6$. Дж. Сцима и Е. Т. Сойер [4] доказали неравенство $t_2 \geqslant \frac{6}{13} n$ при $n \geqslant 8$. Б. Грин и Т. Тао [5], использовав методы аддитивной комбинаторики, доказали гипотезу Дирака для достаточно больших n.

П. Эрдеш и Г.Б. Пурди [6] в 1978 г. доказали неравенство

$$\max\{t_2, t_3\} \geqslant n - 1 \quad \text{при} \quad n \geqslant 25,$$

и доказали, что если $t_2 < n - 1$, то $t_3 > cn^2$ для некоторой положительной константы c. Имеет место неравенство Э. Мельхиора [7]:

$$t_2 \geqslant 3 + \sum_{i \geqslant 4} (i-3) t_i$$

и неравенство Ф. Хирцебруха [8]:

$$t_2 + 0,75 t_3 \geqslant n + \sum_{i \geqslant 5} (2i - 9)\, t_i$$

при условии $t_{n-1} = t_{n-2} = 0$. Известно также неравенство с похожими коэффициентами [9]:

$$t_2 + 1,5 t_3 \geqslant 8 + \sum_{i \geqslant 4} (2i - 7,5)\, t_i$$

при условии $t_{n-1} = t_{n-2} = 0$.

Множество всех возможных значений числа f при заданном числе псевдопрямых n описано Н. Мартиновым [10]:

Теорема. *Нетривиальный набор из n псевдопрямых на проективной плоскости делит последнюю на f областей тогда и только тогда, когда существует целое число k, $1 \leqslant k \leqslant n-2$, такое, что*

$$(n-k)(k+1) + C_k^2 - \min\left\{n-k, C_k^2\right\} \leqslant f \leqslant (n-k)(k+1) + C_k^2.$$

В доказательстве теоремы Мартинова ключевую роль играли нижние оценки числа f, зависящие от чисел n и m, где m — максимальное число псевдопрямых, пересекающихся в одной точке. Такие оценки можно получать, используя соотношения между числами t_i. Цель настоящей работы — получить еще одну нижнюю оценку числа f и указать, при каких условиях она сильнее ранее известных.

1. Оценки числа областей

Под (n, m, f) конфигурацией будем иметь в виду набор из n псевдопрямых на проективной плоскости с максимальной кратностью точек пересечения m, причем дополнение к их объединению состоит из f областей.

Теорема 1. *Для (n, m, f) конфигураций псевдопрямых выполнено*

$$f \geqslant 1 + \frac{n(n-1)}{m} + \frac{m-2}{m}(t_2 + \ldots + t_{m-1}).$$

Доказательство. Из эйлеровой характеристики проективной плоскости следует

$$f = 1 + \sum_{i=2}^{m}(i-1)t_i.$$

Число пар псевдопрямых равно

$$\frac{n(n-1)}{2} = \sum_{i=2}^{m}\frac{i(i-1)}{2}t_i.$$

Умножим равенство числа пар на $\frac{2}{m}$ и выделим сумму:

$$\frac{n(n-1)}{m} = \sum_{i=2}^{m}\frac{i(i-1)}{m}t_i = \sum_{i=2}^{m}(i-1)t_i - \sum_{i=2}^{m}\left(i - 1 - \frac{i(i-1)}{m}\right)t_i.$$

Множители в последней сумме равны

$$i - 1 - \frac{i(i-1)}{m} = \frac{(i-1)(m-i)}{m} \geqslant \frac{m-2}{m} \quad \text{при} \quad 2 \leqslant i \leqslant m-1.$$

Поэтому

$$\frac{n(n-1)}{m} \leqslant \sum_{i=2}^{m}(i-1)t_i - \frac{m-2}{m}(t_2 + \ldots + t_{m-1})$$

и

$$f \geqslant 1 + \frac{n(n-1)}{m} + \frac{m-2}{m}(t_2 + \ldots + t_{m-1}).$$

Теорема 2. *При $m \geqslant 4$ и $n \geqslant m+1$ для (n, f, m) конфигураций псевдопрямых выполнено*

$$f \geqslant 2\left(\frac{n^2 + (m^2 - 2m - 1)n - m^3 + 3m^2}{3m - 1}\right).$$

Доказательство. Пусть O — точка пересечения псевдопрямых $l_1, \ldots, l_m$, обозначенных в порядке следования. Псевдопрямые $l_1, \ldots, l_m$ без учета остальных псевдопрямых набора делят проективную плоскость на m областей. Обозначим через D_i область между псевдопрямыми l_i и l_{i+1}, считая $l_{m+1} = l_1$. Каждая из оставшихся $n-m$ псевдопрямых $l_{m+1}, \ldots, l_n$ пересекает область D_i по простой дуге. Выберем максимальное по количеству множество M_i дуг области D_i, попарно не пересекающихся во внутренних точках. Обозначим через a_i число дуг множества M_i. Объединение дуг множество отрезков образует граф без циклов (т. е. лес — несвязное объединение деревьев). Действительно, через точку O и через долю можно провести мысленную псевдопрямую и упорядочить отрезки подмножества по порядку (любому из двух, считая от точки O) следования их точек пересечения с мысленной псевдопрямой. Тогда оба конца первого по порядку отрезка предполагаемого цикла суть концы двух других отрезков цикла, располагающихся по одну сторону доли от первого отрезка и, следовательно, пересекающихся во внутренней точке. В графе без циклов число ребер не превосходит уменьшенного на единицу числа вершин. Вершины графа располагаются на псевдопрямых l_i и l_{i+1}, поэтому $a_i + 1$ не превосходит числа точек пересечения псевдопрямых l_i и l_{i+1} с оставшимися $(n - m)$ псевдопрямыми. За c_j для $j = 2, \ldots, m$ обозначим количество точек пересечения кратности j, расположенных на псевдопрямых $l_1, \ldots, l_m$, кроме точки O. Итак,

$$m + \sum_{i=1}^{m} a_i \leqslant 2 \sum_{j=2}^{m} c_j. \tag{1}$$

Каждая из $n - m - a_i$ дуг, не вошедших в множество M_i, пересекает хотя бы одну из его дуг во внутренней точке. Поэтому $n - m - a_i$ не превосходит суммы (по точкам пересечения псевдопрямых, расположенных строго внутри области D_i) уменьшенных на единицу кратностей, т. е.

$$n - m - a_i \leqslant \sum_{j=2}^{m} t_j^i (j - 1), \tag{2}$$

где через t_j^i обозначено количество точек пересечения кратности j в области D_i. Тогда

$$f = \sum_{i=1}^{m} \sum_{j=2}^{m} t_j^i (j - 1) + \sum_{j=2}^{m} c_j (j - 1) + m, \tag{3}$$

так как $c_j + \sum\limits_{i=1}^{m} t_j^i$ — это количество точек пересечения на плоскости $\mathbb{RP}^2$ кратности j, отличных от точки O. Заметим, что

$$\sum_{j=2}^{m} c_j(j-1) = m(n-m), \tag{4}$$

так как каждая из оставшихся псевдопрямых пересекается с каждой из m псевдопрямых $l_1 \ldots, l_m$. Из равенств (3) и (4) следует:

$$f - m(n-m+1) = \sum_{i=1}^{m}\sum_{j=2}^{m} t_j^i(j-1). \tag{5}$$

Сложим неравенства (2) по всем $i = 1, \ldots, m$ и сложим с (1):

$$m(n-m+1) \leqslant \sum_{i=1}^{m}\sum_{j=2}^{m} t_j^i(j-1) + 2(c_2 + \ldots + c_m). \tag{6}$$

Подставим в (6) равенство (5) и выразим f :

$$f \geqslant 2m(n-m+1) - 2(c_2 + \ldots + c_m). \tag{7}$$

Обозначим через s сумму $c_2 + \ldots + c_{m-1}$. Из равенства (4) и неравенства

$$c_2 + 2c_3 + \ldots + (m-2)c_{m-1} \geqslant s$$

имеем:

$$c_m \leqslant \frac{m(n-m) - s}{m-1}. \tag{8}$$

Подставим (8) в (7), используя сумму s:

$$f \geqslant \frac{2m(n-m)(m-2)}{m-1} + 2m - 2s\frac{m-2}{m-1}. \tag{9}$$

По теореме 1 верно неравенство

$$f \geqslant 1 + \frac{n(n-1)}{m} + \frac{m-2}{m}s. \tag{10}$$

Умножим неравенство (9) на $m-1$, неравенство (10) на $2m$ и сложим:

$$(3m-1)f \geqslant 2m(n-m)(m-2) + 2m^2 + 2n(n-1).$$

Отсюда получаем требуемое неравенство.

Замечание. Найдем все пары чисел (n, m) с $m \geqslant 4$ и $n \geqslant m+1$, при которых теорема 2 сильнее неравенства из [11, теорема 1]. Сравним правые части соответствующих неравенств на числа областей f:

$$\frac{n^2+(m^2-2m-1)n-m^3+3m^2}{3m-1} > \frac{n^2-n+2m}{m+3} \Leftrightarrow$$
$$\Leftrightarrow (m-2)(n-m-1)(2n-m^2-m) < 0.$$

Следовательно, при $m+1 < n < \frac{m^2+m}{2}$ теорема 2 сильнее неравенства из [11].

Список литературы

1. Brass P., Mozer W., Pach J. Incidence and Arrangement Problems // Research Problems in Discrete Geometry. — Springer, 2005. — P. 289–324.
2. Nilakantan N. Extremal Problems Related to the Sylvester-Gallai Theorem // Combinatorial and Computational Geometry, ed. by J. E. Goodman, J.Pach, E. Welzl. — Cambridge University Press, 2005. — P. 479–494.
3. Dirac G. A. Collinearity properties of sets of points // Quart. J. Math., Oxford Ser. — V. 2, N. 2. — 1951. — P. 221–227.
4. Csima J., Sawyer E. T. There exist $\frac{6n}{13}$ ordinary points // Discrete Comput. Geom. — V. 9. — 1993. — P. 187–202.
5. Green B., Tao T. On sets defining few ordinary lines // http://arxiv.org/abs/1208.4714, — 2012.
6. Erdos P., Purdy G. B. Some combinatorial problems in the plane // J. Combinatorial Theory Ser. A. — V. 25. — 1978. — P. 205–210.
7. Melchior E. Über Vielseite der Projektiven Ebene // Deutsche Mathematik. — V. 5. — 1940. — P. 461–475.
8. Hirzebruch F. Singularities of algebraic surfaces and characteristic numbers // Contemporary Math. — V. 58. — 1986. — P. 141–155.
9. Шнурников И. Н. Распределение количества компонент связности дополнения к наборам замкнутых геодезических. Дисс. МГУ, Москва, 2013.
10. Martinov N. Classification of arrangements by the number of their cells // Discrete and Comput. Geometry. — V. 9, №1. — 1993. — P. 39–46.
11. Шнурников И. Н. На сколько областей делят плоскость n прямых, среди которых не более $n-k$ коллинеарных? // Вестник Московского Университета. Серия 1. Математика, механика. — 2010. — № 5. — С. 32–36.

ОБ ОДНОМ СЕМЕЙСТВЕ РАСПРЕДЕЛЕНИЙ ВЕРОЯТНОСТЕЙ, ПОРОЖДАЕМОМ БЕСПОВТОРНЫМИ ФОРМУЛАМИ НАД КОНЕЧНЫМИ ПОЛЯМИ

А. Д. Яшунский (Москва)

Рассмотрим конечное поле Z_k из k элементов. Операции умножения и сложения над Z_k будем обозначать $\times$ и $+$, соответственно. Для удобства будем обозначать элементы поля $0, 1, 2, \ldots, k-1$, причем 0 обозначает нулевой элемент поля. Мультипликативную группу поля $Z_k \setminus \{0\}$ будем обозначать Z_k^*.

Определим *формулу над полем* Z_k индуктивно: во-первых, переменные x_i являются формулами; во-вторых, если Φ и Ψ — формулы, то $(\Phi+\Psi)$ и $(\Phi\times\Psi)$ также являются формулами. Формула называется *бесповторной*, если все входящие в нее переменные различны. Далее будут рассматриваться только бесповторные формулы, причём формулы, различающиеся только наименованием переменных будут отождествляться. Для удобства будем считать, что для образования бесповторных формул $(\Phi+\Psi)$ и $(\Phi\times\Psi)$ бесповторные формулы Φ и Ψ выбираются с непересекающимися множествами переменных.

Пусть Φ — некоторая бесповторная формула над Z_k, подставим вместо ее переменных независимые одинаково распределенные случайные величины над полем Z_k с распределением π. Значение формулы Φ само будет случайной величиной: ее распределение обозначим $P(\Phi)$, понимая под $P_i(\Phi)$ вероятность того, что Φ принимает значение $i \in Z_k$.

Распределение переменных $P(x_i) = \pi$ будем называть *начальным*. Несложно заметить, что для распределения $P((\Phi + \Psi))$ имеют место соотношения

$$P_i((\Phi + \Psi)) = \sum_{j \in Z_k} P_{i-j}(\Phi) P_j(\Psi),$$

а для распределения $P((\Phi \times \Psi))$ — соотношение

$$P_0((\Phi \times \Psi)) = P_0(\Phi) + P_0(\Psi) - P_0(\Phi) P_0(\Psi)$$

и для $i \in Z_k^*$:

$$P_i((\Phi \times \Psi)) = \sum_{j \in Z_k^*} P_{ij^{-1}}(\Phi) P_j(\Psi).$$

Покажем, что, если начальное распределение не имеет нулевых компонент, над полем Z_k можно построить семейство распределений с достаточно произвольными вероятностями нулевого элемента и вероятностями ненулевых элементов сколь угодно близкими друг к другу.

Лемма. *Пусть для начального распределения π выполнено $\pi_i > 0$ при всех $i \in Z_k$. Тогда для любого $\varepsilon > 0$ и любого $\delta > 0$ существует такая бесповторная формула F над Z_k, что $P_0(F) > 1 - \varepsilon$ и*

$$\max_{i \in Z_k^*} P_i(F) - \min_{i \in Z_k^*} P_i(F) < (1 - P_0(F))\delta.$$

Доказательство. Образуем последовательность бесповторных формул, полагая $F_0 = x$, $F_{n+1} = (F_n \times F_n)$. Несложно заметить, что выполнено равенство $1 - P_0(F_{n+1}) = (1 - P_0(F_n))^2$, из которого следует: $1 - P_0(F_n) = (1 - \pi_0)^{2^n}$. Из этого соотношения непосредственно вытекает, что для любого $\varepsilon > 0$ для достаточно больших n имеет место $P_0(F_n) > 1 - \varepsilon$.

Рассмотрим теперь величины $P_i(F_n)$ при $i \in Z_k^*$. Они могут быть выражены через условные вероятности:

$$P_i(F_n) = \mathcal{P}\{F_n = i\} = \mathcal{P}\{F_n = i | F_n \neq 0\}\mathcal{P}\{F_n \neq 0\} = \\ = \mathcal{P}\{F_n = i | F_n \neq 0\}(1 - P_0(F_n)).$$

Из свойств операции умножения в Z_k вытекает, что значения условных вероятностей $\mathcal{P}\{F_n = i | F_n \neq 0\}$ в точности совпадают с вероятностями, получающимися при преобразовании начального распределения $\mathcal{P}\{F_0 = i | F_0 \neq 0\}$ бесповторными формулами F_n над группой Z_k^*. В силу известных свойств преобразований распределений вероятностей бесповторными формулами над квазигруппами [1], найдётся такое $\alpha > 0$, что

$$\max_{i \in Z_k^*} \mathcal{P}\{F_n = i | F_n \neq 0\} - \min_{i \in Z_k^*} \mathcal{P}\{F_n = i | F_n \neq 0\} < \alpha^n.$$

Следовательно, для достаточно больших n выполнено

$$\max_{i \in Z_k^*} \mathcal{P}\{F_n = i | F_n \neq 0\} - \min_{i \in Z_k^*} \mathcal{P}\{F_n = i | F_n \neq 0\} < \delta,$$

откуда легко вытекает утверждение леммы.

Теорема. *Пусть для начального распределения π выполнено $\pi_i > 0$ при всех $i \in Z_k$. Тогда для любого $a \in [1/k, 1]$, любого $\varepsilon > 0$ и любого $\delta > 0$ существует такая бесповторная формула G над Z_k, что $|P_0(G) - a| < \varepsilon$ и*

$$\max_{i \in Z_k^*} P_i(G) - \min_{i \in Z_k^*} P_i(G) < \delta.$$

Доказательство. Пусть $\varepsilon > 0$ задано, рассмотрим произвольное $\delta' > 0$. По приведенной выше лемме существует такая бесповторная формула F над Z_k, что $P_0(F) > 1 - \varepsilon$ и $\max\limits_{i \in Z_k^*} P_i(F) - \min\limits_{i \in Z_k^*} P_i(F) < (1 - P_0(F))\delta'$. Заметим, что тогда $P_i(F) \leqslant (1 - P_0(F))\left(\frac{1}{k-1} + \delta'\right)$ для $i \in Z_k^*$.

Образуем последовательность бесповторных формул G_n, полагая $G_0 = F$, $G_{n+1} = (G_n + F)$. Покажем, что выполнено $0 < P_0(G_n) - P_0(G_{n+1}) < \varepsilon$ при условии, что $P_0(G_n) > \frac{1}{k} + \delta'$. В силу определения формул G_n и выбора формулы F:

$$P_0(G_n) - P_0(G_{n+1}) = P_0(G_n) - P_0(G_n)P_0(F) - \sum_{j \in Z_k^*} P_j(G_n)P_{0-j}(F) \leqslant$$
$$\leqslant P_0(G_n)(1 - P_0(F)) < \varepsilon.$$

Одновременно, в силу оценки для $P_i(F)$ при $i \in Z_k^*$:

$$P_0(G_n) - P_0(G_{n+1}) = P_0(G_n)(1 - P_0(F)) - \sum_{j \in Z_k^*} P_j(G_n)P_{0-j}(F) >$$
$$> P_0(G_n)(1 - P_0(F)) - \left(\frac{1}{k-1} + \delta'\right)(1 - P_0(F)) \sum_{j \in Z_k^*} P_j(G_n) =$$
$$= (1 - P_0(F)) \left(1 - (1 - P_0(G_n)) \left(1 + \frac{1}{k-1} + \delta'\right)\right).$$

В силу предположения $P_0(G_n) > \frac{1}{k} + \delta'$ имеем $1 - P_0(G_n) < 1 - \frac{1}{k} - \delta'$, откуда

$$(1 - P_0(G_n)) \left(1 + \frac{1}{k-1} + \delta'\right) < \left(1 - \frac{1}{k} - \delta'\right) \left(1 + \frac{1}{k-1} + \delta'\right) < 1,$$

что влечёт неравенство $P_0(G_n) - P_0(G_{n+1}) > 0$.

Обозначим $\delta_n = \max\limits_{i \in Z_k^*} P_i(G_n) - \min\limits_{i \in Z_k^*} P_i(G_n)$. Для произвольных $i_1, i_2 \in Z_k^*$, $i_1 \neq i_2$ рассмотрим величину $|P_{i_1}(G_{n+1}) - P_{i_2}(G_{n+1})|$:

$$|P_{i_1}(G_{n+1}) - P_{i_2}(G_{n+1})| = \left| \sum_{j \in Z_k} P_{i_1 - j}(G_n)P_j(F) - \sum_{j \in Z_k} P_{i_2 - j}(G_n)P_j(F) \right| \leqslant$$
$$\leqslant |P_{i_1}(F) - P_{i_2}(F)|P_0(G_n) + \sum_{j \neq i_1, i_2} |P_{i_1 - j}(G_n) - P_{i_2 - j}(G_n)|P_j(F) \leqslant$$
$$\leqslant |P_{i_1}(F) - P_{i_2}(F)|P_0(G_n) + \delta_n \sum_{j \neq i_1, i_2} P_j(F) \leqslant \delta_0 + (1 - \min_{i \in Z_k^*} P_i(F))\delta_n.$$

В силу произвольности i_1 и i_2 получаем, что $\delta_{n+1} \leqslant \delta_0 + (1 - \min\limits_{i \in Z_k^*} P_i(F))\delta_n$, откуда легко следует $\delta_n \leqslant \frac{\delta_0}{\min\limits_{i \in Z_k^*} P_i(F)}$. Заметим, что в силу выбора формулы F, имеет место $\delta_0 < \delta'\varepsilon$ и

$$\min_{i \in Z_k^*} P_i(F) > \left(\frac{1}{k-1} - \delta'\right)(1 - P_0(F)) > \left(\frac{1}{k-1} - \delta'\right)\varepsilon.$$

Следовательно, при всех n выполнено $\delta_n < \frac{\delta'}{\frac{1}{k-1}-\delta'}$. Для достаточно малых δ' (а именно, $\delta' \leqslant \frac{1}{2(k-1)}$) получаем, что $\delta_n < 2(k-1)\delta'$.

По заданным $\varepsilon > 0$ и $\delta > 0$ выберем теперь $\delta' = \min\{\varepsilon, \frac{1}{2(k-1)}, \frac{\delta}{2(k-1)}\}$. В силу полученных выше соотношений, найдётся такой номер N, что выполнено $\left|P_0(G_N) - \frac{1}{k}\right| < \varepsilon$, причём $P_0(G_0), P_0(G_1), \ldots, P_0(G_N)$ образуют монотонно невозрастающую последовательность, в которой разность двух идущих подряд элементов не превышает ε. Вместе с тем, для всех формул G_n, $n = 0, 1, \ldots, N$ имеет место неравенство

$$\max_{i \in Z_k^*} P_i(G_n) - \min_{i \in Z_k^*} P_i(G_n) < \delta.$$

Отсюда легко следует утверждение теоремы.

Отметим, что все приведенные рассуждения в действительности выполняются не только для конечных полей, а для конечных алгебраических структур образованных следующим образом: в качестве Z_k^* возьмем произвольную квазигруппу порядка $k-1$ с операцией умножения $\times$, дополнив ее элементом 0, полагая $0 \times z = z \times 0 = 0 \times 0 = 0$ для всех $z \in Z_k^*$. На полученном множестве $Z_k = Z_k^* \cup \{0\}$ зададим квазигрупповую операцию $+$ так, чтобы $0 \in Z_k$ был ее нейтральным элементом, т. е. $0 + z = z + 0 = z$ для всех $z \in Z_k$.

Автор выражает благодарность О. М. Касим-Заде за полезные обсуждения и внимание к работе. Работа выполнена при финансовой поддержке программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем») и РФФИ (проект №11–01–00508).

Список литературы

1. Яшунский А. Д. О квазигрупповых свертках распределений вероятностей // Материалы VIII молодежной научной школы по дискретной математике и ее приложениям (Москва 24–29 октября 2011 г.). Ч. II. Под ред. А. В. Чашкина. — 2011. — С. 54–56.