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

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

ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ

СБОРНИК ЛЕКЦИЙ

VII

Москва 2013

Институт прикладной математики им. М. В. Келдыша
Российской Академии Наук
Московский государственный университет им. М.В. Ломоносова
Механико-математический факультет

ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ

СБОРНИК ЛЕКЦИЙ МОЛОДЕЖНЫХ НАУЧНЫХ ШКОЛ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

VII

Москва 2013

М34
УДК 519.7

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

М34 Дискретная математика и ее приложения: Сборник лекций молодежных научных школ по дискретной математике и ее приложениям. Выпуск VII. Под редакцией А. В. Чашкина. — М.: Изд-во ИПМ РАН, 2013. — 56 с.

Седьмой выпуск лекций содержит лекции, прочитанные на IX молодежной научной школе по дискретной математике и ее приложениям, проходившей в Москве в ИПМ им. М. В. Келдыша РАН 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

ДИСКРЕТНАЯ МАТЕМАТИКА
И ЕЕ ПРИЛОЖЕНИЯ
Сборник лекций
Выпуск VII

Под общей редакцией А. В. ЧАШКИНА

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

Ответственный за выпуск *О. С. Дудакова*

СЛОЖНОСТЬ РАСШИФРОВКИ ПОРОГОВЫХ ФУНКЦИЙ

Н. Ю. Золотых

Нижегородский государственный университет им. Н. И. Лобачевского, Нижний Новгород, пр. Гагарина, д. 23

e-mail: zolotykh@vmk.unn.ru

Предлагается обзор основных результатов, касающихся задачи расшифровки пороговой функции многозначной логики: строение и мощность наименьшего разрешающего множества, сложность расшифровки и др. Лекция является переработанным вариантом статьи [1].

1. Определения и предварительные результаты

Пусть $E_k^n = \{0, 1, \ldots, k-1\}^n$, $k \geqslant 2$, $n \geqslant 1$. Обозначим $\mathcal{F}(n, k)$ множество всех функций $f : E_k^n \to \{0, 1\}$, в частности, $\mathcal{F}(n, 2)$ — множество всех булевых функций n переменных. Рассмотрим некоторый класс $\mathcal{F}' \subseteq \mathcal{F}(n, k)$. Под *расшифровкой* функции в классе $\mathcal{F}'$ понимают восстановление значений заранее не известной функции f из известного класса $\mathcal{F}'$ с помощью обращений к оракулу этой функции. Под *оракулом* функции f понимают некоторую процедуру, которая по заданному $x \in E_k^n$ возвращает $f(x)$.

По-видимому, впервые задача расшифровки рассматривалась В. К. Коробковым и Т. Л. Резником [2–4] для класса монотонных булевых функций. Сложность расшифровки монотонных булевых функций установил Ж. Ансель [5]. Оптимальный по числу вопросов и используемой памяти алгоритм расшифровки предложил Н. А. Соколов [6]. Задачу расшифровки монотонных функций многозначной логики рассматривали В. К. Коробков [7], В. Б. Алексеев [8], А. В. Сержантов [9] и др. М. В. Горяинов и А. А. Сапоженко [10] предложили алгоритм расшифровки монотонных функций на частично упорядоченных множествах. Другие сведения о монотонных функциях и задаче расшифровки монотонных функций приведены в обзоре А. Д. Коршунова [11]. Рассматриваются задачи расшифровки функций из других классов (А. А. Вороненко, В. В. Осокин, Э. Э. Гасанов и др.). Задача интенсивно изучается в рамках теории тестов [12] и вычислительной теории машинного обучения (Computational Learning Theory) [13].

Для функции $f \in \mathcal{F}(n, k)$ обозначим

$$M_\nu(f) = \{x \in E_k^n : \ f(x) = \nu\}, \qquad \nu = 0, 1.$$

Функция $f \in \mathcal{F}(n,k)$ называется *пороговой*, если существуют вещественные числа $a_0, a_1, \ldots, a_n$, такие, что

$$M_0(f) = \left\{ x \in E_k^n : \sum_{j=1}^{n} a_j x_j \leqslant a_0 \right\},$$

при этом неравенство

$$\sum_{j=1}^{n} a_j x_j \leqslant a_0 \tag{1}$$

называется *пороговым*. Очевидно, его коэффициенты можно сделать целыми. Обозначим $\mathcal{T}(n,k)$ множество всех пороговых функций, заданных на E_k^n, т. е. множество пороговых функций k-значной логики n переменных. В частности, $\mathcal{T}(n,2)$ — множество всех булевых пороговых функций n переменных.

Задачу расшифровки пороговых функций, по-видимому, первым рассматривал В. Н. Шевченко [14]. В случае пороговых функций уточним термин «расшифровка»: под *расшифровкой пороговой функции* будем понимать алгоритм поиска коэффициентов порогового неравенства заранее не известной функции f с помощью обращений к ее оракулу.

Задача расшифровки пороговых функций тесно связана с проблемой оценки числа таких функций. Заметим, что задача оценки числа пороговых функция является весьма сложной. До сих пор не известна асимптотика числа пороговых булевых функций. Из результатов Л. Шлефли [15] о числе открытых областей, получаемых при разбиении n-мерного пространства K гиперплоскостями, легко получить верхнюю оценку:

$$|\mathcal{T}(n,2)| < 2\sum_{j=0}^{n} \left(\begin{array}{c} 2^n - 1 \\ j \end{array} \right) < 2^{n^2}.$$

С. Яджима и Т. Ибараки [16] получили первую нетривиальную нижнюю оценку:

$$|\mathcal{T}(n,2)| > 2^{n^2/2}.$$

Ю. А. Зуев [17, 18] доказал, что

$$|\mathcal{T}(n,2)| > 2^{n^2(1-10/\ln n)},$$

тем самым установив асимптотику логарифма числа булевых пороговых функций:

$$\log_2 |\mathcal{T}(n,2)| \sim n^2, \qquad n \to \infty. \tag{2}$$

При доказательстве асимптотики использовался один комбинаторно-вероятностный результат о (± 1)-матрицах, полученный А. М. Одлыжко [19]. Другой

подход к получению асимптотического равенства (2), также использующий лемму Одлыжко, предложил А. А. Ирматов [20].

Обстоятельный обзор результатов по пороговым булевым функциям и пороговым представлениям булевых функций содержится в [21].

Для числа пороговых функций k-значной логики А. А. Ирматов и Ж. Д. Ковиянич [22] получили нижнюю оценку:

$$|\mathcal{T}(n,k)| \geqslant \frac{1}{2}\left(\begin{array}{c} k^n \\ \lfloor n-4-2n/\log_k n \rfloor \end{array}\right) |\mathcal{T}(\lfloor 2n/\log_k n + 4 \rfloor,\, k)|,$$

справделивую для достаточно больших n. Отсюда и из оценки Шлефли получается асимптотика логарифма числа таких функций:

$$\log_2 |\mathcal{T}(n,k)| \sim n^2 \log_2 k, \qquad n \to \infty.$$

Для пороговых функций k-значной логик двух переменных в [23] получена оценка:

$$|\mathcal{T}(2,k)| = \frac{6k^4}{\pi^2} + O(k^3 \log k), \qquad k \to \infty.$$

Пусть $\mathcal{A}$ — алгоритм расшифровки в классе $\mathcal{F}' \subseteq \mathcal{F}(n,k)$. Обозначим через $\tau(\mathcal{A}, f)$ число обращений к оракулу при расшифровке функции $f \in \mathcal{F}'$.

Оракульной сложностью алгоритма $\mathcal{A}$ называется

$$\tau(\mathcal{A}) = \max_{f \in \mathcal{F}'} \tau(\mathcal{A}, f).$$

Оракульной сложностью расшифровки в классе $\mathcal{F}'$ называется

$$\tau(\mathcal{F}') = \min_{\mathcal{A}} \tau(\mathcal{A}) = \min_{\mathcal{A}} \max_{f \in \mathcal{F}'} \tau(\mathcal{A}, f).$$

Множество $T \subseteq E_k^n$ называется *разрешающим* (также используется термин *проверочный тест*) для $f \in \mathcal{F}'$ относительно класса $\mathcal{F}'$, если для любой функции $g \in \mathcal{F}'$, $f \neq g$, найдется по крайней мере одна точка $z \in T$, такая, что $g(z) \neq f(z)$. Понятие разрешающего множества введено В. К. Коробковым и Т. Л. Резником [2] в контексте монотонных булевых функций. Разрешающее множество, никакое собственное подмножество которого не является разрешающим для f, называется *тупиковым*. Разрешающее множество функции f минимальной мощности называется ее *наименьшим* разрешающим множеством.

Точка $z \in E_k^n$ называется *существенной* для функции $f \in \mathcal{F}'$ относительно класса $\mathcal{F}'$, если найдется функция $g \in \mathcal{F}'$, такая, что $f(z) \neq g(z)$, $f(x) = g(x)$ для всех $x \in E_k^n \setminus \{z\}$. При этом f и g называются *соседними* функциями.

Легко видеть, что множество всех существенных точек для заданной функции f включено в любое ее разрешающее множество. Обратное включение в общем случае не имеет места.

Рассмотрим два примера. Если $\mathcal{F}'$ — класс монотонных функций n переменных, то для любой функции $f \in \mathcal{F}'$ ее тупиковое разрешающее множество единственно, совпадает со множеством существенных точек и состоит из верхних нулей и нижних единиц функции [2, 8].

Если $\mathcal{F}'$ — класс самодвойственных булевых функций n переменных, то легко видеть, что произвольная функция $f \in \mathcal{F}'$ обладает $2^{2^{n-1}}$ тупиковыми разрешающими множествами (каждое мощности 2^{n-1}) и не имеет существенных точек.

Пусть $\sigma(f, \mathcal{F}')$ — мощность наименьшего разрешающего множества для функции $f \in \mathcal{F}'$ относительно класса $\mathcal{F}'$. *Длиной обучения* в классе $\mathcal{F}'$ называется

$$\sigma(\mathcal{F}') = \max_{f \in \mathcal{F}'} \sigma(f, \mathcal{F}').$$

Нетрудно видеть, что

$$\sigma(f, \mathcal{F}') = \min_{\mathcal{A}} \tau(\mathcal{A}, f),$$

поэтому

$$\sigma(\mathcal{F}') = \max_{f \in \mathcal{F}'} \min_{\mathcal{A}} \tau(\mathcal{A}, f).$$

Нетрудно видеть, что для любого класса $\mathcal{F}'$

$$\sigma(\mathcal{F}') \leqslant \tau(\mathcal{F}').$$

Под *средней мощностью наименьшего разрешающего множества* в классе $\mathcal{F}'$ понимаем величину

$$\overline{\sigma}(\mathcal{F}') = \frac{1}{|\mathcal{F}'|} \sum_{f \in \mathcal{F}'} \sigma(f, \mathcal{F}').$$

Если P — полиэдр (выпуклое многогранное множество) в $\mathbf{R}^n$, то обозначим $\operatorname{Vert} P$ множество его вершин. Если $X \subseteq \mathbf{R}^n$, то обозначим $\operatorname{Conv} X$ — выпуклую оболочку множества X, а $\operatorname{Cone} X$ — коническую оболочку этого множества (множество всех неотрицательных линейных комбинаций).

2. Характеризация разрешающего множества и оценки длины обучения пороговой функции

Обозначим

$$\tau(n, k) = \tau\big(\mathcal{T}(n, k)\big), \quad \sigma(n, k) = \sigma\big(\mathcal{T}(n, k)\big), \quad \overline{\sigma}(n, k) = \overline{\sigma}\big(\mathcal{T}(n, k)\big).$$

Легко видеть, что для функции $f \in \mathcal{T}(n, 2)$, тождественно равной 0 или 1,

$$\sigma\big(f, \mathcal{T}(n, k)\big) = |E_2^n| = 2^n,$$

поэтому

$$\tau(n,k) \geqslant \sigma(n,k) \geqslant \tau(n,2) = \sigma(n,2) = 2^n.$$

Итак, $\tau(n,k)$ и $\sigma(n,k)$ зависят от n экспоненциально, поэтому далее в первую очередь нас будет интересовать асимптотика величин $\tau(n,k)$ и $\sigma(n,k)$ при стремлении $k \to \infty$ и фиксированном n.

Следующее построение хорошо известно в пороговой логике. С каждой функцией $f \in \mathcal{T}(n,k)$ в пространстве коэффициентов $a_0, a_1, \ldots, a_n$ свяжем так называемый *конус* $C(f)$ *разделяющих функционалов*, заданный как множество решений следующей системы:

$$\begin{cases} \sum\limits_{j=1}^{n} a_j x_j \leqslant a_0 & \text{при всех} \quad (x_1, \ldots, x_n) \in M_0(f); \\ \sum\limits_{j=1}^{n} a_j x_j > a_0 & \text{при всех} \quad (x_1, \ldots, x_n) \in M_1(f). \end{cases} \tag{3}$$

Пусть $T_\nu \subseteq M_\nu(f)$ $(\nu = 0, 1)$. Рассмотрим подсистему системы (3):

$$\begin{cases} \sum\limits_{j=1}^{n} a_j x_j \leqslant a_0 & \text{при всех} \quad (x_1, \ldots, x_n) \in T_0; \\ \sum\limits_{j=1}^{n} a_j x_j > a_0 & \text{при всех} \quad (x_1, \ldots, x_n) \in T_1. \end{cases} \tag{4}$$

Утверждение. *Для того, чтобы множество* $T = T_0 \cup T_1$, $T_\nu \subseteq M_\nu(f)$ $(\nu = 0, 1)$ *было разрешающим для* $f \in \mathcal{T}(n,k)$, *необходимо и достаточно, чтобы система неравенств* (3) *была эквивалентна системе неравенств* (4).

Можно доказать, что в системе (3) найдется минимальная подсистема, эквивалентная всей системе:

$$\begin{cases} \sum\limits_{j=1}^{n} a_j x_j \leqslant a_0 & \text{при всех} \quad (x_1, \ldots, x_n) \in T_0(f); \\ \sum\limits_{j=1}^{n} a_j x_j > a_0 & \text{при всех} \quad (x_1, \ldots, x_n) \in T_1(f). \end{cases}$$

Следствие 1. *Для любой* $f \in \mathcal{T}(n,k)$ *множество* $T = T_0 \cup T_1$, *где* $T_\nu \subseteq M_\nu(n,k)$ $(\nu = 0, 1)$, *является тупиковым разрешающим тогда и только тогда, когда* $T_\nu = T_\nu(f)$ $(\nu = 0, 1)$.

Таким образом, $\sigma(n,k)$ можно интерпретировать как максимальное число соседних пороговых функций, а $\overline{\sigma}(n,k)$ — их среднее число.

Следствие 2. *Для любой* $f \in \mathcal{T}(n,k)$ *существует единственное тупиковое разрешающее множество* $T(f) = T_0(f) \cup T_1(f)$, *совпадающее с множеством всех существенных точек функции* f.

Теорема 1 [24]. *Для любой функции* $f \in \mathcal{T}(n,k)$

$$T_\nu(f) \subseteq \operatorname{Vert}\operatorname{Conv} M_\nu(f) \qquad (\nu = 0,1).$$

Оценивая $|\operatorname{Vert}\operatorname{Conv} M_\nu(f)|$ сверху, В. Н. Шевченко [24] доказал, что

$$\sigma(n,k) \leqslant 2^n \log_2^n(k+1).$$

Более точную (при фиксированном n) оценку получил Т. Хегедюш [25] на основе результатов [26] о числе вершин в неявно заданных целочисленных полиэдрах:

$$\sigma(n,k) = O(\log_2^{n-1} k), \qquad k \to \infty.$$

Полиэдр называется *целочисленным*, если все его вершины целые. Рассмотрим полиэдр $P = \{x \in \mathbf{R}^n : \ Ax \leqslant a_0\}$, где $A \in \mathbf{Z}^{m\times n}$, $a_0 \in \mathbf{Z}^m$, и целочисленный полиэдр $P_{\mathbf{Z}} = \operatorname{Conv}(P \cap \mathbf{Z}^n)$. Проблемой получения оценок $|\operatorname{Vert} P_{\mathbf{Z}}|$ занимались В.Н. Шевченко, С.И. Веселов, А. Ю. Чирков, А. С. Хейес, Д. К. Ларман, И. Барани, Р. Хоу, Л. Ловаш, У. Кук, М. Хартманн, Р. Каннан, К. МакДиармид и др. (см. обзор работ в [27]).

Полное описание структуры разрешающего множества дает следующая

Теорема 2 [28, 29]. *Для любой функции* $f \in \mathcal{T}(n,k)$

$$T_0(f) = T_1(g) = \bigcup_{a,\, a_0} \operatorname{Vert}\operatorname{Conv} \left\{ x = (x_1, x_2, \ldots, x_n) \in E_k^n : \ \sum_{j=1}^n a_j x_j = a_0 \right\},$$

где $g = 1 - f$ *и объединение берется по всем* $a = (a_1, a_2, \ldots, a_n)$, a_0, *таким, что неравенство* (1) *является пороговым для функции* f.

На ее основе для $\sigma(n,k)$ получена первая нетривиальная оценка снизу.

Теорема 3 [28, 29]. *При любом фиксированном* $n \geqslant 2$

$$\sigma(n,k) = \Omega(\log_2^{n-2} k), \qquad k \to \infty.$$

Прогресс на пути построения более точных верхних и нижних оценок для величины $\sigma(n,k)$ происходил за счет использования новых результатов о числе вершин в неявно заданных целочисленных полиэдрах.

В частности, в [30] получена двусторонняя оценка:

$$\frac{\Big(\frac{1}{2}\log k - n - 3 - (n-1)\log(n-2)\Big)^{n-2}}{4(n-1)3^{n-1}(n-2)^{n-2}\Big((n-2)!\Big)^2} \leqslant \sigma(n,k) \leqslant$$

$$\leqslant 2n\log(2n)\Big(1 + \log(k+1)\Big)^{n-1}.$$

Долгое время существовала гипотеза $\sigma(n,k) = \Theta(\log_2^{n-2} k)$ (для любого фиксированного $n \geqslant 2$ и $k \to \infty$). Гипотеза доказана в [1], см. также [31]. При доказательстве используется новая характеризация [32] тупикового разрешающего множества пороговой функции.

Обозначим $K(f) = \operatorname{Cone}\big(M_1(f) - M_0(f)\big)$, $F_0(f) = \operatorname{Conv} M_0(f) - K(f)$, $F_1(f) = \operatorname{Conv} M_1(f) + K(f)$.

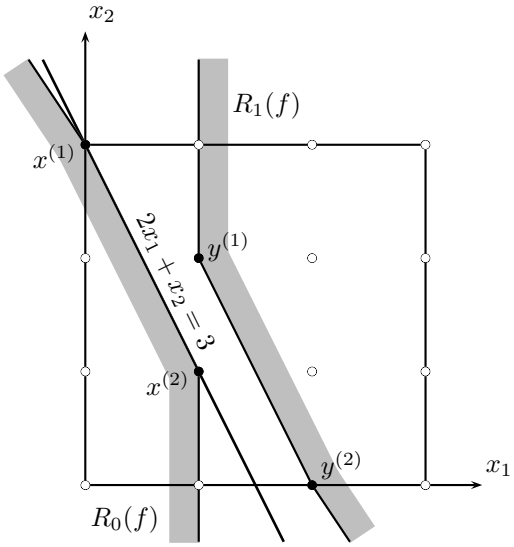

Рис. 1

Теорема 4 [32]. *Пусть* $f \in \mathcal{T}(n,k)$, *тогда* $T_\nu(f) = \operatorname{Vert} F_\nu(f)$ $(\nu = 0,1)$.

Следствие [32]. *Пусть* $f \in \mathcal{T}(n,k)$, $x, y \in T_\nu(f)$ $(\nu = 0,1)$, $x \neq y$. *Тогда*

$$2x - y \notin F_0(f) \cup F_1(f). \tag{5}$$

На рис. 1 изображены множества $F_0(f)$ и $F_1(f)$ для функция $f \in \mathcal{T}(2,4)$, заданной пороговым неравенством $2x_1 + x_2 \leqslant 3$. Наименьшее разрешающее множество образуют точки

$$x^{(1)} = (0,3), \quad x^{(2)} = (1,1), \quad y^{(1)} = (1,2), \quad y^{(2)} = (2,0).$$

В рассматриваемом случае имеем $K(f) = \operatorname{Cone}\{r^{(1)}, r^{(2)}\}$,

$$F_0(f) = \operatorname{Cone}\{x^{(1)}, x^{(2)}\} - K(f), \quad F_1(f) = \operatorname{Cone}\{y^{(1)}, y^{(2)}\} + K(f),$$

$$T_0(f) = \operatorname{Vert} F_0(f) = \left\{x^{(1)}, x^{(2)}\right\}, \qquad T_1(f) = \operatorname{Vert} F_0(f) = \left\{y^{(1)}, y^{(2)}\right\},$$

где $r^{(1)} = y^{(2)} - x^{(1)} = (3, -2)$, $r^{(2)} = y^{(1)} - x^{(2)} = (0, 1)$.

Условие (5) близко к *свойству разделенности*, введенному В. Н. Шевченко в [33] в связи с исследованием задачи о числе вершин неявно заданных целочисленных полиэдров. Обозначим $\mathbf{Z}_+$ множество неотрицательных целых чисел. Говорят, что множество $G \subset \mathbf{Z}_+^n$ обладает *свойством разделенности* [33], если из условий $x, y \in G$, $x \neq y$ следует $2x - y \notin \mathbf{Z}_+^n$.

Лемма [33]. *Пусть множество $G \subset \mathbf{Z}_+^n$ обладает свойством разделенности и для каждого $x = (x_1, x_2, \ldots, x_n) \in G$ выполнено $\alpha_i \leqslant x_j \leqslant \beta_j$ $(j = 1, \ldots, n-1)$, где $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$, $\beta_1, \beta_2, \ldots, \beta_{n-1}$ — неотрицательные числа, тогда*

$$|G| \leqslant \prod_{j=1}^{n-1} \left\lfloor 1 + \log_2 \frac{\beta_j + 2}{\alpha_j + 1} \right\rfloor.$$

Развивая соответствующий аппарат, удается доказать следующий результат.

Теорема 5 [1]. *Для любого фиксированного $n \geqslant 2$*

$$\sigma(n, k) = O(\log_2^{n-2} k), \qquad k \to \infty.$$

Из теорем 3, 5 получаем, что для любого фиксированного $n \geqslant 2$

$$\sigma(n, k) = \Theta(\log_2^{n-2} k), \qquad k \to \infty.$$

Приведем один результат о средней мощности наименьшего разрешающего множества пороговой функции. М. Энтони, Г. Брайтуэлл, Д. Коэн, Дж. Шоу-Тейлор [34] показали, что

$$\overline{\sigma}(n, 2) \leqslant n^2.$$

Этот результат можно обобщить (см. [35]) на случай пороговых функций k-значной логики:

$$\overline{\sigma}(n, k) \leqslant n^2 \log_2 k.$$

3. Длина обучения пороговой функции двух переменных

Возможные значения мощности наименьшего разрешающего множества пороговой функции, зависящей от двух переменных, суть 3 и 4. Таким образом, справедлива

Теорема 6 [28, 36]. *Для любого $k \geqslant 2$*

$$\sigma(2, k) = 4.$$

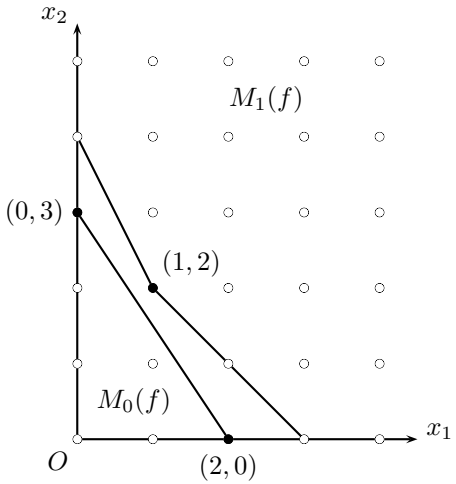

Рис. 2

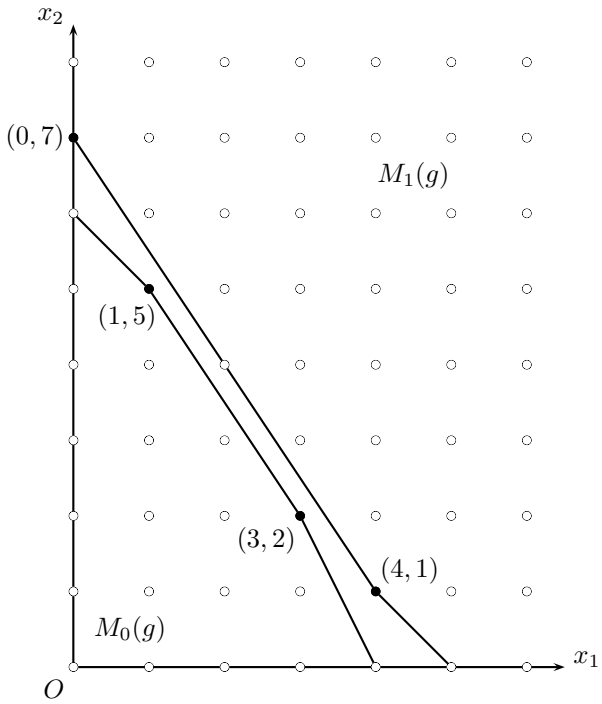

Рис. 3

Рассмотрим функцию $f \in \mathcal{T}(2,k)$ (для произвольного $k \geqslant 5$), определяемую пороговым неравенством $3x_1 + 2x_2 \leqslant 6$. В этом случае (см. рис. 2) множество $T(f)$ содержит 3 точки: $(2,0)$, $(0,3)$, $(1,2)$. Точка $(0,4)$, например, не принадлежит $T(f)$, так как никакая опорная к $\operatorname{Conv} M_1(f)$ прямая, проходящая через $(0,4)$, не является разделяющей для $M_0(f)$, $M_1(f)$.

Для функции $g \in \mathcal{T}(2,k)$, $k \geqslant 8$, определяемой пороговым неравенством $3x_1 + 2x_2 \leqslant 13$, разрешающее множество $T(g)$ состоит из 4 точек: $(3,2)$, $(1,5)$, $(4,1)$, $(0,7)$ (см. рис. 3).

Более того, среднее значение мощности наименьшего разрешающего множества пороговой функции двух переменных асимптотически равно 7/2.

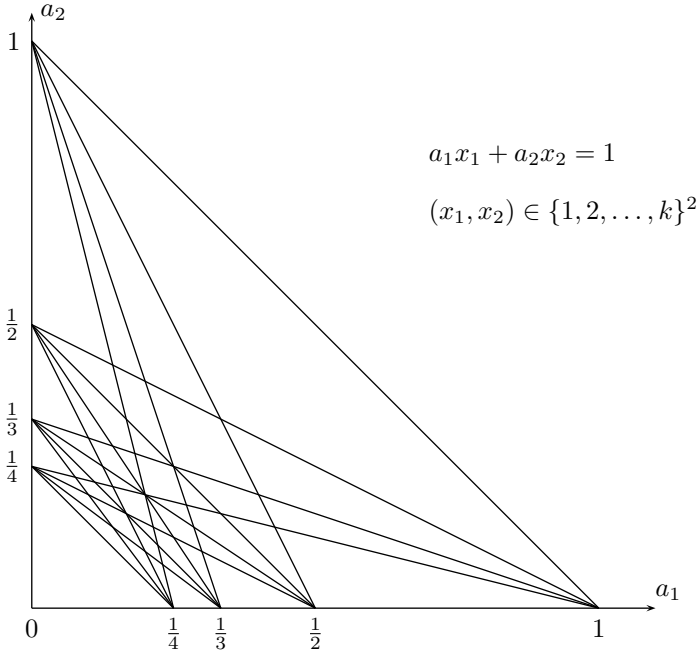

Рис. 4

Теорема 7 [37].

$$\overline{\sigma}(2,k) = \frac{7}{2} + O\left(\frac{1}{k}\right), \qquad k \to \infty.$$

Отсюда получаем интересное геометрическое

Следствие. *Среди ограниченных областей, получаемых при разбиении плоскости параметров a_1, a_2 всеми прямыми $a_1x_1 + a_2x_2 = 1$, где (x_1, x_2)*

принадлежит множеству $\{0,1,\ldots,k-1\}^2$*, встречаются только треугольники и четырехугольники, причем их количества асимптотически равны.*

Аналогичный результат получается, если разбивать плоскость параметров a_1, a_2 прямыми $a_1x_1+a_2x_2=1$, где $(x_1,x_2)\in\{1,2,\ldots,k\}^2$ и т. п. В частности, на рис. 4 представлено разбиение указанными прямыми первой четверти плоскости.

4. Алгоритмы расшифровки пороговых функций

В. Н. Шевченко [14] предложил для расшифровки пороговых функций алгоритм $\mathcal{A}_0$, у которого при любом фиксированном n величина $\tau(\mathcal{A}_0)$ ограничена полиномом от $\log k$. Т.Хегедюш [25] показал, что

$$\tau(\mathcal{A}_0)=O\Big(\log^{\lfloor n/2\rfloor(n-1)+n}k\Big).$$

Н. Ю. Золотых, В. Н. Шевченко [38] и Т. Хегедюш [39] построили алгоритм $\mathcal{A}_1$, для которого $\tau(\mathcal{A}_1)=O(\log^n k)$. Из теоремы 4 следует, что $\tau(\mathcal{A}_1)=O(\log^{n-1}k)$.

Более того, применяя результаты М. Ю. Мошкова [40, 41] в теории тестов, можно построить (ср. [39]) алгоритм $\mathcal{A}'$, для которого

$$\tau(\mathcal{A}')=O\left(\frac{\log^{n-1}k}{\log\log k}\right),\qquad k\to\infty.$$

Итак, справедлива

Теорема 8.

$$\tau(n,k)=O\left(\frac{\log^{n-1}k}{\log\log k}\right),\quad \tau(n,k)\geqslant\sigma(n,k)=\Omega(\log^{n-2}k),\quad k\to\infty.$$

Для $n=2$ в [28, 42] построен алгоритм $\mathcal{A}$, для которого

$$\tau(\mathcal{A})\leqslant 6\log(k-1)+4.$$

Работа выполнена в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2007–2013 годы», госконтракт 11.519.11.4015.

Литература

1. Золотых Н. Ю., Чирков А. Ю. Сложность расшифровки пороговых функций многозначной логики // Материалы XI Международного семинара «Дискретная математика и ее приложения», посвященного 80-летию со дня рождения академика О. Б. Лупанова (18–23 июня 2012 г.) / Под редакцией О.М. Касим-Заде. — М.: Изд-во механико-матем. факультета МГУ. — 2012. — С. 63–77.

2. Коробков В. К., Резник Т. Л. О некоторых алгоритмах вычисления монотонных функций алгебры логики // Доклады АН СССР. — 1962. — V. 147, № 5. — С. 1022–1025.

3. Коробков В. К. Оценка числа монотонных функций алгебры логики и сложности алгоритма отыскания разрешающего множества для произвольной монотонной функции алгебры логики // Доклады АН СССР. — 1963. — V. 150, № 4. — С. 744–747.

4. Коробков В. К. О монотонных функциях алгебры логики // Проблемы кибернетики. Вып. 13. — М.: Наука, 1965. — С. 5–28.

5. Hansel G. Sur le nombre des fonctions booléennes monotones de n variables // C. R. Acad. Sci. — Paris, 1966. — V. 262, № 20. — P. 1088–1090.

6. Соколов Н. А. Оптимальная расшифровка монотонных булевых функций // Журн. вычисл. математики и матем. физики. — 1987. — V. 27, № 12. — С. 1878–1887.

7. Коробков В. К. Некоторые обобщения задачи «расшифровки» монотонных функций алгебры логики // Дискретный анализ. Сб. тр. Вып. 5. — Новосибирск: изд-во Ин-та матем. СО АН СССР, 1965. — С. 19–25.

8. Алексеев В. Б. О расшифровке некоторых классов монотонных многозначных функций // Журн. вычисл. математики и матем. физики. — 1976. — V. 16, № 1. — С. 189–198.

9. Сержантов А. В. Оптимальный алгоритм расшифровки некоторых классов монотонных функций // Журн. вычисл. математики и матем. физики. — 1983. — V. 23, № 1. — С. 206–212.

10. Горяинов М. В., Сапоженко А. А. О расшифровке монотонных функций на частично упорядоченных множествах // Дискретный анализ и исследование операций. — 1995. — Т. 2, № 3. — С. 79–80.

11. Коршунов А. Д. Монотонные булевы функции // Успехи матем. наук. — 2003. — Т. 58, № 5. — С. 5–108.

12. Чегис И. А., Яблонский С. В. Логические способы контроля работы электрических схем // Тр. Матем. ин-та АН СССР. — 1958. — Т. 51. — С. 270–360.

13. Angluin D. Queries and concept learning // Machine Learning. — 1988. — V. 2, № 4. — P. 319–342.

14. Шевченко В. Н. О расшифровке пороговых функции многозначной логики // Комбинаторно-алгебраические методы в прикл. матем. — Горький: Горьковский гос. ун-т, 1987. — С. 155–163.

15. Schläfli L. Gesammelte mathematisce Abhanglugen. Band 1. — Basel: Verlag Birkhäuzer, 1950.

16. Yajima S., Ibaraki T. A lower bound of the number of threshold functions // IEEE Trans. on Electronic Comput. — 1965. — V. 14, № 6. — P. 929–929.

17. Зуев Ю. А. Асимптотика логарифма числа пороговых функций алгебры логики // Доклады АН СССР. — 1989. — Т. 306, № 3. — С. 528–530.

18. Зуев Ю. А. Комбинаторно-вероятностные и геометрические методы в пороговой логике // Дискретная математика. — 1991. — Т. 3, № 2. — С. 47–57.

19. Odlyzko A. M. On subspaces spanned by random selection of ± 1 vectors // J. Combin. Theory, A. — 1988. — V. 47, № 1. — С. 124–133.

20. Ирматов А. А. О числе пороговых функций // Дискретная математика. — 1993. — Т. 5, № 3. — С. 40–43.

21. Зуев Ю. А. Пороговые функции и пороговые представления булевых функций // Матем. вопросы кибернетики. Вып. 5. — М.: Физматлит, 1994. — С. 5–61.

22. Ирматов А. А., Ковиянич Ж. Д. Об асимптотике логарифма числа пороговых функций k-значной логики // Дискретная математика. — 1998. — Т. 10, № 3. — С. 35–56.

23. Koplowitz J., Lindenbaum M., Bruckstein A. M. The number of digital straight lines on an $N \times N$ grid // IEEE Trans. Inform. Theory. — 1990. — V. 36. — P. 192–197.

24. Шевченко В. Н. О некоторых функциях многозначной логики, связанных с целочисленным программированием // Методы дискретного анализа в теории графов и схем. Вып. 42. — Новосибирск: Ин-т матем. СО АН СССР, 1985. — С. 99–108.

25. Hegedüs T. Geometrical concept learning and convex polytopes // Proc. 7th Ann. ACM Conf. on Computational Learning Theory. — New York: ACM Press, 1994. — P. 228–236.

26. Cook W., Hartmann M., Kannan R., McDiarmid C. On integer points in polyhedra // Combinatorica. — 1992. — V. 12, No 1. — P. 27–37.

27. Веселов С. И., Чирков А. Ю. Оценки числа вершин целых полиэдров // Дискретный анализ и исследование операций. Серия 2. — 2007. — Т. 14, № 2. — С. 14–31.

28. Шевченко В. Н., Золотых Н. Ю. О сложности расшифровки пороговых функций k-значной логики // Доклады Академии наук. — 1998. — Т. 362, № 5. — С. 606–608.

29. Золотых Н. Ю., Шевченко В. Н. О нижней оценке сложности расшифровки пороговых функций k-значной логики // Журн. вычисл. матем. и матем. физики. — 1999. — Т. 39, № 2. — С. 346–352.

30. Золотых Н. Ю. Оценки мощности минимального разрешающего множества пороговой функции многозначной логики // Матем. вопросы кибернетики. Вып. 17. — М.: Физматлит, 2008. — С. 159–168.

31. Chirkov A. Yu., Zolotykh N. Yu. On the number of irreducible points in polyhedra. arXiv:1306.4289. — 2013.

32. Золотых Н. Ю., Чирков А. Ю. О верхней оценке мощности минимального разрешающего множества пороговой функции // Дискретный анализ и исследование операций. — 2012. — Т. 19, №5. — С. 35–46.

33. Шевченко В. Н. О числе крайних точек в целочисленном программировании // Кибернетика. — 1981. — № 2. — С. 133–134.

34. Antony M., Brightwell G., Shawe-Taylor J. On exact specification by labelled examples // Discrete Applied Mathematics. — 1995. — V. 61, № 1. — С. 1–25.

35. Вировлянская М. А., Золотых Н. Ю. Верхняя оценка средней мощности минимального разрешающего множества пороговой функции многозначной логики // Вестник Нижегород. гос. ун-та им. Н. И. Лобачевского. Матем. моделирование и оптимальное управление. — Нижний Новгород.: изд-во ННГУ, 2003. — С. 238–246.

36. Золотых Н. Ю. О сложности расшифровки пороговых функций, зависящих от двух переменных // Материалы XI Межгосударственной школы-семинара «Синтез и сложность управляющих систем». Часть I. — М.: Изд-во Центра прикладных исследований при механико-матем. ф-те МГУ, 2001. — С. 74–79.

37. Alekseyev M. A., Basova M. G., Zolotykh N. Yu. The average cardinality of the minimal teaching set of a threshold function on a two-dimensional rectangular grid. arXiv:1307.1058. — 2013.

38. Золотых Н. Ю., Шевченко В. Н. Расшифровка пороговых функций k-значной логики // Дискретный анализ и иссл. операций. — 1995. — Т. 2, № 3. — С. 18–23.

39. Hegedüs T. Generalized teaching dimensions and the query complexity of learning // Proc. 8th Ann. ACM Conf. on Computational Learning Theory (COLT'95). — New York: ACM Press, 1995. — P. 108–117.

40. Мошков М. Ю. Об условных тестах // Доклады АН СССР. — 1982. — Т. 265, № 3. — С. 550–552.

41. Мошков М. Ю. Условные тесты // Проблемы кибернетики. Вып. 40. — М.: Наука, 1983. — С. 131–170.

42. Золотых Н. Ю. Пороговые функции, зависящие от двух переменных: сложность расшифровки и мощность разрешающего множества // Материалы четвертой молодежной научной школы по дискретной математике и ее приложениям. — М.: Изд-во механико-матем. факультета МГУ, 2000. — С. 48–54.

СВОЙСТВА ЦЕЛОЧИСЛЕННЫХ ПАСКАЛЬ-ФУНКЦИЙ, ДОКАЗУЕМЫЕ НА ОСНОВЕ АРИФМЕТИКИ ПО МОДУЛЮ 2^{16}

Н. К. Косовский

Санкт-Петербургский государственный университет,
Санкт-Петербург, Университетская наб., д. 7/9

e-mail: kosov@nk1022.spb.edu

Введение

В рамках конечно-дискретной математики ниже предлагаются математические модели целочисленных вычислений по модулю N, особенно при $N = 2^{16}$, характерного для IBM-совместимых персональных компьютеров. Эти модели более точно отражают практику использования компьютеров. Вводятся РАМ (равнодоступная адресная машина), РАСП (равнодоступная адресная машина с хранимой программой) и паскаль-программы, использующие арифметические операции по модулю N с остатками из сегмента $[-[N/2], [N/2] - 1 + (N \mod 2)]$.

Описывается язык индексных логик первого порядка, позволяющий сформулировать математические свойства таких всюду применимых паскаль-программ. Доказывается P-SPACE-полнота задачи проверки тождественной истинности в таких логиках, содержащих арифметические операции по модулю N. Устанавливается, что размера памяти $2s+2$ достаточно для вычисления продолжения посредством любой наперед заданной константой РАСП-программы по модулю N с памятью s до всюду применимой.

1. Исходные определения

Всегда завершаемость (иначе говоря, всюду применимость) программы является важным аспектом дружественной программы. Поэтому будем рассматривать всегда завершаемые целочисленные паскаль-функции и паскаль-предикаты, использующие арифметические операции по модулю N с остатками из упомянутого выше сегмента. Такие паскаль-функции и паскаль--предикаты можно рассматривать как присваивающие значения соответствующего типа своему имени.

Использование в этом случае традиционной для языка паскаль записи вызова функции или предиката в выражении (в дальнейшем используется тер-

мин «индексный терм») не требует уточнения способа вычисления выражения. В случае же использования незавершаемого выражения, обозначенного знаком ? , при одной интерпретации имеет место равенство $?*0=0$ (при параллельном вычислении значений всех подвыражений) или равенство $?*0=?$ (при последовательном вычислении значений всех подвыражений).

В работе [1] определены РАМ и РАСП как модели целочисленных вычислений, использующие один (по существу, динамический) линейный массив для записи целых чисел произвольной длины.

Определим понятия РАМ и РАСП *по модулю* N, использующие арифметические операции по модулю N с остатками, принадлежащими сегменту $[-[N/2], [N/2]-1+(N \mod 2)]$. Здесь $[N/2]$ — целая часть от деления N на 2, $(N \mod 2)$ — остаток от деления N на 2. Последовательность таких остатков от деления на N является целым числом, записанным по основанию N с цифрами из сегмента $[-[N/2], [N/2]-1+(N \mod 2)]$. Предлагается использовать один массив целых чисел из этого же сегмента, но произвольной размерности (одномерный, двухмерный, ...), одной и той же для каждой программы. Длина массива по каждому измерению не превосходит N. При этом исходные данные располагаются в первых измерениях для РАМ и РАСП, а программа для РАСП вместе со счетчиком команд располагается в последних измерениях. Кроме того, счетчик команд находится в самых последних измерениях массива. Признаком конца данных (и начала программы для РАСП, а также начала счетчика команд) может служить дополнительное измерение, использующее в качестве двух границ своего измерения только одну и ту же константу, например, единицу.

Таким образом, в массиве любой РАМ- и РАСП-программы по модулю N может быть только конечное число элементов, но это число не может быть ограничено сверху (из-за возможно растущего числа измерений массивов в последовательности как РАМ-, так и РАСП-программ).

Для использования традиционного обозначения элемента массива в выражениях языка паскаль недостаточно логики первого порядка. Поэтому понятие формулы такой логики с вызовами паскаль-функций и паскаль-предикатов из конечной сигнатуры расширяется до понятия индексной формулы.

Прежде всего, вводится понятие *индексного терма*, определение которого получается из определения терма (см., например, [2]) с помощью замены слова «терм» на слова «индексный терм» и добавления в определение индексного терма следующей дополнительной конструкции: индексным термом является любая переменная для массива, за которой следует последовательность разделенных запятой индексных термов, заключенная в квадратные скобки. *Постоянным индексным термом* называется индексный терм, не содержащий предметных переменных или массивов. Таким образом разрешается исполь-

зовать элементы массивов с одним и тем же для РАМ и РАСП по модулю N числом измерений и с разным числом измерений для паскаль-программ по модулю N.

Определение понятия *индексной атомарной формулы* получается из определения понятия атомарной формулы путем замены слова «терм» на слова «индексный терм». Определение понятия *индексной формулы первого порядка в конечной сигнатуре* получается из определения понятия формулы первого порядка в той же сигнатуре путем замены слов «атомарная формула» на слова «индексная атомарная формула» и добавления возможности использования кванторов не только по элементам массивов, но и по самим массивам и их подмассивам с явным указанием диапазонов границ каждого измерения. Речь идет о диапазонах вида $t1..t2$, где $t1$ и $t2$ — постоянные индексные термы. В случае, когда $t1 = t2$, вместо диапазона $t1..t1$ разрешается использовать постоянный индексный терм $t1$. Это расширяет возможности языка паскаль, предоставленные при описании в нем массивов, поскольку вместо диапазона может находиться один постоянный индексный терм вместо его повторного указания через две последовательные точки (..) .

По существу, понятие предметной переменной, используемое в логике первого порядка, расширяется на элемент массива с постоянными индексами. Последние могут находиться непосредственно вслед за квантором, иметь свободные и связанные вхождения в индексную формулу первого порядка. Поэтому необходимо сначала доопределить естественным образом понятие *области действия вхождения квантора* как индексной подформулы, начинающейся с этого вхождения квантора, и доопределить понятие связанного вхождения элемента массива, самого массива и любого его подмассива. Элемент t массива с постоянными индексами входит *связанно*, если он находится в области действия вхождения квантора, непосредственно вслед за которым выписано имя этого, содержащего t, массива или подмассива с указанием постоянных диапазонов, или элементов в каждом измерении этого массива. Вхождение элемента массива, не являющееся связанным называется *свободным*.

Аналогично может быть определено понятие тождественно истинной индексной формулы в конечной сигнатуре по модулю N с учетом интерпретации паскаль-функций и паскаль-предикатов, вычислимых по модулю N с остатками из сегмента $[-[N/2], [N/2] - 1 + (N \mod 2)]$.

Корректность тела всегда завершаемой паскаль-функции описывается с помощью триад Хора вида $\{A\}S\{B\}$, где A и B — условия, а S — паскаль-программа. Она может быть записана в виде $A \Rightarrow [B]^{\overline{x}}_{\overline{S1}(\overline{x})}$, где $\overline{S1}$ — список имен глобальных переменных программы S. Здесь $[B]^{\overline{x}}_{\overline{S1}(\overline{x})}$ – результат подстановки в B вместо всех свободных вхождений переменных списка $\overline{x}$ соответствующих индексных термов из списка $\overline{S1}(\overline{x})$. При этом оба списка должны иметь одинаковое число своих членов. Здесь имена глобальных переменных

программы S рассматриваются как имена паскаль-функций, вычисляющих их значения в результате работы паскаль-программы S от аргументов $\overline{x}$.

Если включить все эти паскаль-функции в сигнатуру индексной логики первого порядка, то в ее языке можно записать утверждения о корректности паскаль-программы S по используемому модулю N. Сказанное свидетельствует о широких возможностях введенных индексных логик первого порядка в конечных сигнатурах из функций и предикатов, вычисляющих выбранные целочисленные остатки по используемому модулю.

2. Основные результаты

Чисто логический вариант следующей теоремы был сформулирован в [3]. Определение понятия P-SPACE-полноты задачи можно найти в [1].

Теорема 1. *Каковы бы ни были натуральное число* N (*при* $N \geqslant 2$) *и содержащая* $\{+, -, *, <\}$ *конечная сигнатура всегда применимых функций и предикатов по модулю* N *с носителем из всех целых чисел сегмента* $[-[N/2], [N/2] - 1 + (N \mod 2)]$, *задача принадлежности множеству всех тождественно истинных индексных формул первого порядка является* P-SPACE-*полной.*

Доказательство основывается на P-SPACE-полноте задачи КВАНТОРНАЯ БУЛЕВА ФОРМУЛА (QBF) [1] по проверке тождественной истинности кванторых булевых формул и на доказательстве возможности проверки тождественной истинности индексных формул упомянутого в теореме вида алгоритмом из P-SPACE.

Особый интерес вызывают модули из последовательности $\{2^{2^m}\}$. В случае $m = 0$ индексная логика первого порядка по модулю 2 в сигнатуре, содержащей $\{+, *, <\}$, по существу является формулой QBF. При каждом натуральном числе m носитель индексной логики первого порядка по модулю $2^{2^{m+1}}$ представляет собой множество всех пар пар из остатков по модулю 2^{2^m}. Начиная с $m = 4$, несколько таких модулей достаточно широко используются в компьютерах.

Отметим, что предикат равенства коротко записывается в такой сигнатуре при любом m.

$$x = y \Leftrightarrow \neg(x < y) \ \& \ \neg(y < x)$$

Замена строгого неравенства в сигнатуре на равенство в ней приводит при больших m к значительной длине записи формулы, выражающей предикат строгого неравенства.

Следующая теорема представляет собой более красивую модификацию теоремы из [4].

Теорема 2. *Каковы бы ни были натуральные числа s и N (при $N \geqslant 2$) проблема применимости* РАСП*-программы по модулю N, использующей массив из s элементов, может быть доопределена одной и той же заранее заданной константой до* РАСП*-программы, использующей массив из $2s+2$ элементов.*

Доказательство основано на том, что РАСП-программа по модулю N, использующая массив из s элементов и совершившая N^s+1 шагов, обязательно зацикливается. Дело в том, что количество различных вариантов содержимого памяти размера s не превосходит N^s. Следовательно, если число шагов больше N^s, то РАСП-программа по модулю N зацикливается.

Поэтому для доказательства теоремы достаточно переписать программу, после выполнения каждого шага исходной РАСП-программы вставляя прибавление единицы в дополнительный подмассив из $s+1$ элементов и проверку отличия от $-[N/2]$ в первом элементе дополнительного подмассива. Еще один элемент массива используется для хранения заранее выбранной константы.

Поскольку можно построить РАСП-интерпретатор паскаль-программ по модулю N (не содержащих файлов, рекурсивных функций и рекурсивных процедур), использующих суммарно не более s переменных и элементов массива в процессе вычисления, то можно доопределить такую паскаль-программу по модулю N до всюду применимой.

Пусть f_0 и f_1 — всюду применимые продолжения посредством нуля и единицы соответственно паскаль-функции f. Тогда $!f(x) \Leftrightarrow f_0(x) = f_1(x)$. Здесь запись $!f(x)$ означает завершаемость работы паскаль-функции f над x. Аналогично для паскаль-предиката Q имеем $!Q(x) \Leftrightarrow (Q_{true}(x) \Leftrightarrow Q_{false}(x))$.

Таким образом, теорема 1 позволяет описывать математические свойства нерекурсивных паскаль-функций и паскаль-предикатов, иногда не завершающих свою работу. В этом случае их можно заменить всегда завершаемыми продолжениями, полученными на основе теоремы 2.

Теорема 3. *Каково бы ни было натуральное число N (при $N \geqslant 2$), проблемы применимости как* РАМ*-, так и* РАСП*-программ по модулю N являются* P-SPACE*-полными.*

P-SPACE-полнота рассматриваемой в теореме проблемы вытекает из возможности решения проблемы QBF с помощью как РАМ-, так и РАСП-программ по модулю N, которые могут быть построены за число шагов, не превосходящее полинома от длины записи исходных данных, а также с помощью конструкции, использованной в теореме 2.

Литература

1. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. — М.: Мир, 1979.

2. Косовский Н. К. Элементы математической логики и ее приложения к теории субрекурсивных алгоритмов. — Л.: Изд. Ленинградского университета, 1981.

3. Косовский Н. К. Pspace-полнота предикатных логик конечного порядка над конечной областью // Смирновские чтения. 3 Международная конференция. М., 2001. — С. 44.

4. Косовский Н. К., Фам Тхань Лам. Оценка памяти, необходимой для исключения бесконечного зацикливания в Паскаль-программах, выполняемых на компьютере // Материалы XVI Международной школы-семинара «Синтез и сложность управляющих систем» (СПб, 26–30 июня 2006 г.) Изд-во мех-мат ф-та МГУ, М., 2006. — С. 53–54.

ТЕОРИЯ ВЕНТИЛЬНЫХ СХЕМ (СОВРЕМЕННОЕ СОСТОЯНИЕ)

В. В. Кочергин

**МГУ имени М. В. Ломоносова,
Москва, Ленинские горы**

e-mail: vvkoch@yandex.ru

Введение

Теорию схем можно подразделить по мощности применяемых средств на несколько уровней: теория вентильных схем, теория контактных схем, теория схем из функциональных элементов, теория автоматов с памятью. При этом конструкции одного уровня могут (в той или иной степени) быть промоделированы во всех высших уровнях. Поэтому результаты вентильного уровня, несущего наибольшую топологическую нагрузку, имеют принципиальную — общекибернетическую — значимость.

В литературе по синтезу и сложности управляющих систем под вентильными схемами в зависимости от исследуемых задач могут пониматься несколько разные объекты, которые условно можно разделить на классические вентильные схемы [19, 21, 36], реализующие булевы матрицы, а также на вентильные схемы с кратными путями (или графы с предписанным числом путей) [39] (см. также [17]), реализующие целочисленные неотрицательные матрицы. В последнее время более активно изучается второй вариант вентильных схем, имеющий тесную связь с задачами экономного вычисления систем одночленов (см., например, [38]). Однако, результаты из теории классических вентильных схем занимают особое место в теории сложности, Кроме того, они и сейчас находят применение при решении различных задачах (см., например. [5, 30, 33]). В частности, в основе асимптотически точной верхней оценки сложности для задач Р. Беллмана и Д. Кнута [4] о сложности вычисления одночлена общего вида от нескольких переменных и сложности вычисления набора степеней, соответственно, лежит как раз технически тяжелый результат относительно сложности реализации булевых матриц ступенчатого вида классическими вентильными схемами специального типа — об этом подробнее будет сказано ниже. Кроме того, методы исследований для случая реализации булевых матриц и случая реализации целочисленных неотрицательных матриц достаточно близки. Поэтому в лекции кроме описания последних достижений в задаче о сложности реализации целочисленных неотрицательных матриц вентильны-

ми схемами, дается обзор результатов по теории классических вентильных схем. Этот обзор касательно результатов, полученных до середины 70-х годов прошлого века, опирается на обзор О. Б. Лупанова [21].

1. Классические вентильные схемы

Напомним определение классической вентильной схемы [19] или, более точно, классическое определение вентильной схемы.

В наиболее общем (для классического случая) виде [21] *вентильная схема* определяется как ориентированный граф, в котором выделено некоторое множество вершин — множество полюсов — и эти вершины занумерованы. С каждой вентильной схемой S связывается матрица из нулей и единиц $A = (a_{ij})$ — *матрица проводимостей* ($a_{ij} = 1$ тогда и только тогда, когда в схеме S имеется ориентированный путь из полюса с номером i в полюс с номером j). Очевидно, что матрица проводимостей любой вентильной схемы является транзитивной.

Важным классом вентильных схем [19, 25, 27] являются такие, в которых полюса разбиты на два подмножества: «входные» с номерами $P = \{1, 2, \ldots, p\}$ и «выходные» — с номерами $Q = \{p+1, p+2, \ldots, p+q\}$ и на матрицу проводимостей наложено дополнительное ограничение: $a_{ij} = 0$, если $i \neq j$ и либо $i \in P$, $j \in P$, либо $i \in Q$, $j \in Q$, либо $i \in Q$, $j \in P$. В этом случае система проводимостей полностью определяется подматрицей данной матрицы, имеющей p строк и q столбцов; ее обычно и называют матрицей проводимостей.

Заметим, что без ограничения общности можно считать, что в вентильной схеме нет ориентированных циклов (без изменения матрицы проводимостей этот ориентированный цикл можно заменить на одну вершину).

Теперь дадим эквивалентное определение вентильной схемы, которое и будем, как правило, использовать в дальнейшем.

Пусть $A = (a_{ij})$ — булева (двоичная) матрица размера $p \times q$. *Вентильной схемой, реализующей матрицу* A, называется ориентированный граф S без ориентированных циклов в котором:

1) выделено p вершин — входных полюсов и q вершин — выходных полюсов;

2) нет ориентированных путей от одного входа к другому, от одного выхода к другому, от выхода к входу;

3) для любой пары (i, j), $1 \leqslant i \leqslant p$, $1 \leqslant j \leqslant q$, ориентированный путь от i-го входа к j-му выходу существует тогда и только тогда, когда $a_{ij} = 1$.

Через $L_{BC}(S)$ будем обозначать *сложность вентильной схемы* S, т. е. число ребер (вентилей) схемы S (в литературе по вентильным схемам сложность также иногда обозначается буквами B и C). *Сложность* $L_{BC}(A)$ *реализации булевой матрицы* A *вентильными схемами* определяется следующим образом: $L_{BC}(A) = \min L_{BC}(S)$, где минимум берется по всем вентильным схемам,

реализующим матрицу A. Функция Шеннона $L_{BC}(p,q)$ сложности реализации булевых матриц вентильными схемами вводится стандартным образом как минимальное число вентилей, достаточное для реализации любой булевой матрицы с p строками и q столбцами, т. е. $L_{BC}(p,q) = \max L_{BC}(A)$, где максимум берется по всем булевым матрицам размера $p \times q$.

Аналогичным образом определяется и функция Шеннона $L^{(r)}_{BC}(p,q)$ сложности реализации булевых матриц вентильными схемами глубины r (*глубина схемы* — максимальная длина цепи от входа к выходу).

Во множестве всех вентильных схем выделим важный для приложений специальный класс — вентильные схемы, в которых число путей от произвольного входа до произвольного выхода равно либо 0, либо 1 (см., например, [36]).

Пусть $A = (a_{ij})$ — булева (двоичная) матрица размера $p \times q$. Ориентированный граф (без петель и кратных ребер) S будем называть 0-1-*вентильной схемой, реализующей матрицу* A, если:

1) в S выделено p вершин — входных полюсов и q вершин — выходных полюсов;

2) в S нет ориентированных путей от одного входа к другому, от одного выхода к другому, от выхода к входу;

3) для любой пары (i,j), $1 \leqslant i \leqslant p$, $1 \leqslant j \leqslant q$, число ориентированных путей от i-го входа к j-му выходу равно a_{ij}.

Обозначим через $L_{01}(S)$ *сложность* 0-1-*вентильной схемы* S, т. е. число ребер (вентилей) схемы S. Определим *сложность* $L_{01}(A)$ *реализации булевой матрицы* A 0-1-*вентильными схемами*, положив $L_{01}(A) = \min L_{01}(S)$, где минимум берется по всем 0-1-вентильным схемам, реализующим матрицу A.

Таким образом, определение 0-1-вентильной схемы несколько отличается от классического определения вентильной схемы — в п. 3 определения в случае, когда $a_{ij} = 1$, накладывается более сильное условие: вместо существования пути от i-го входа к j-му выходу требуется существование и единственность такого пути.

Очевидно, что все введенные меры сложности булевых матриц при реализации вентильными схемами различных типов обладают свойством двойственности, т. е. сложность исходной матрицы и транспонированной к ней совпадают — для построения схемы, реализующей транспонированную матрицу, достаточно в исходной схеме поменять направления всех вентилей.

Помимо только что обсужденных равенств

$$L_{BC}(A) = L_{BC}(A^T), \quad L^{(r)}_{BC}(A) = L^{(r)}_{BC}(A^T), \quad L_{01}(A) = L_{01}(A^T)$$

отметим следующие простые соотношения:

$$L_{BC}(A) \leqslant L_{01}(A), \quad L_{BC}(p,q) \leqslant L_{01}(p,q).$$

Кроме того, для вентильных схем глубины 1 выполняются равенства

$$L^{(1)}_{BC}(A) = \|A\|, \quad L^{(1)}_{BC}(p,q) = pq,$$

где $\|A\|$ означает число единиц в матрице A. Тем самым задача о сложности реализации матриц вентильными схемами глубины 1 является тривиальной. Однако уже для схем глубины 2 задача оказалась значительно более содержательной.

В 1956 г. О. Б. Лупановым [19] предложен асимптотически наилучший (будем считать, что значения p и q являются функциями некоторого натурального параметра n и имеются в виду асимптотические соотношения при $n \to \infty$) метод построения вентильных схем глубины 2, который в дальнейшем лег в основу асимптотически оптимальных методов синтеза «более сильных» классов управляющих систем (контактных схем, схем из функциональных элементов, автоматов и т. д. — см., например, [20, 22]):

Теорема 1 [19]. *Пусть выполнены условия*

а) $p \to \infty$;

б) $p \leqslant q$;

в) $\frac{\log q}{p} \to 0$.

Тогда

$$L^{(2)}_{BC}(p,q) \sim \frac{pq}{\log q}.$$

Следствие 1. *В условиях теоремы* 1

$$\frac{pq}{\log(pq)} \lesssim L_{BC}(p,q) \lesssim \frac{pq}{\log q}.$$

Следствие 2. *В условиях теоремы* 1

$$\frac{pq}{\log(pq)} \lesssim L_{01}(p,q) \lesssim \frac{pq}{\log q}.$$

Следствие 3. *В условиях теоремы* 1 *при дополнительном условии*

$г_0$) $\frac{\log p}{\log q} \to 0$

выполняются соотношения

$$L_{BC}(p,q) \sim L_{01}(p,q) \sim L^{(2)}_{BC}(p,q) \sim \frac{pq}{\log q}.$$

Уточнение оценок для величины $L_{BC}(p,q)$ было получено Э. И. Нечипоруком [25, 27].

Теорема 2 [25,27]. *Пусть выполнены условия а) и б) теоремы* 1, *а также условие*

г$_c$) $\lim \frac{\log p}{\log q} = \frac{\mu}{\mu(\varrho-1)+\varrho}$, *где* μ *и* ϱ *— целые числа, большие нуля.*

Тогда

$$L_{BC}(p,q) \sim L_{01}(p,q) \sim L^{(3)}_{BC}(p,q) \sim \frac{pq}{\log(pq)}.$$

Замечание. *Условие г$_c$) включает важный для приложений случай, когда величины* p *и* q *имеют одинаковый порядок роста.*

Окончательное асимптотически точное решение (при естественном условии, что число полюсов существенно меньше сложности) было получено Н. Пиппенджером [36, 39] в 1976 г.

Теорема 3 [36, 39]. *Пусть выполнены условия теоремы* 1. *Тогда*

$$L_{BC}(p,q) \sim L_{01}(p,q) \sim \frac{pq}{\log(pq)}.$$

Отметим, что конструкция из верхней оценки теоремы 3 требует растущей глубины вентильной схемы. Вопрос о том, достаточно ли вентильных схем ограниченной глубины для получения асимптотической верхней оценки вида $\frac{pq}{\log(pq)}$, остается до сих пор открытым.

Случай, когда не выполняется условие в) из теоремы 1 (т. е. число полюсов сравнимо со сложностью) был исследован В. А. Орловым [29].

Теорема 4 [29]. *Пусть* k *— произвольное фиксированное целое число. Тогда*

$$L^{(2)}_{BC}(\lfloor k \log q \rfloor, q) \sim (k+1)q.$$

Теорема 5 [29]. *Пусть выполнены условия*

а$'$) $q \to \infty$,

в$_\alpha$) $\lim \frac{p}{\log q} = \alpha$, *причем* $\alpha > 1$, α *— не целое число.*

Тогда

$$L^{(2)}_{BC}(p,q) \sim \lfloor \alpha + 1 \rfloor q.$$

Теорема 6 [29]. *Пусть* $q \geqslant p2^{p-1} - p$. *Тогда*

$$L^{(2)}_{BC}(p,q) = p2^{p-1} - p + q.$$

Теорема 7 [29]. *Пусть выполнено условие а), а также условия*

в$_1$) $\lim \frac{p}{\log q} = 1$,

д) $q \geqslant p2^{p-1} - p$.

Тогда

$$L^{(2)}_{BC}(p,q) \sim 2q.$$

Теорема 8 [29]. *Пусть выполнены условия а) и $в_1$), а также условие*
∂^-) $q \leqslant 2(2^p - p - 1)$.

Тогда

$$L_{BC}(p,q) \sim L^{(2)}_{BC}(p,q) \sim 2q.$$

Теорема 9 [29]. *Пусть выполнено условие а), а также условие*
∂^+) $q \geqslant 2(2^p - p - 1)$.

Тогда

$$L_{BC}(p,q) \sim L^{(2)}_{BC}(p,q) \sim 2 \cdot 2^p + q.$$

Наряду с задачей о реализации произвольных булевых матриц (заданных размеров) исследовались вопросы о сложности реализации матриц из специальных классов.

Положим $L^{(r)}_{BC}(p,q,\alpha) = \max L^{(r)}_{BC}(A)$, где максимум берется по всем булевым матрицам из p строк и q столбцов, имеющих αpq единичных элементов. Введем обозначения

$$\alpha^* = \min(\alpha, 1-\alpha), \quad H(\alpha) = \alpha \log \frac{1}{\alpha} + (1-\alpha)\log\frac{1}{(1-\alpha)}.$$

Э. И. Нечипорук доказал следующие утверждения.

Теорема 10 [25, 27]. *Пусть выполнено условие б), а также условия*
a_α) $\alpha p \to \infty$;
$e_{\alpha,\varrho}$) $\frac{\log q}{\log \frac{1}{\alpha}} \to \varrho$, ϱ *— целое,* $\varrho > 0$;
$ж_{\alpha,\varrho}$) $q\alpha^\varrho \to \infty$.

Тогда

$$L^{(2)}_{BC}(p,q,\alpha) \sim \frac{\alpha pq}{\varrho}.$$

Теорема 11 [24, 27]. *Пусть выполнены условия а) и б), а также условия*
$в_\alpha$) $H(\alpha)\frac{p}{\log q} \to \infty$;
e_∞) $\frac{\log q}{\log \frac{1}{\alpha^*}} \to \infty$.

Тогда

$$L^{(2)}_{BC}(p,q,\alpha) \sim H(\alpha)\frac{pq}{\log q}.$$

Теорема 12 [27]. *Пусть выполнены условия а) $в_\alpha$) и e_∞), а также условие*
$г_1$) $\log p \sim \log q$.

Тогда

$$L^{(3)}_{BC}(p,q,\alpha) \sim H(\alpha)\frac{pq}{\log(pq)}.$$

Важное место в теории вентильных схем занимает тесно связанная, например, с построением самокорректирующихся схем задача о сложности реализации не всюду определенных (недоопределенных) матриц — матриц, элементами которых могут быть не только нули и единицы, но и символы $*$ (символ $*$ соответствует неопределенному элементу). Доопределением не всюду определенной матрицы является полностью определенная матрица, все элементы которой совпадают с соответствующими определенными элементами исходной матрицы. Под сложностью не всюду определенной матрицы понимается минимальная сложность ее доопределений.

Положим $L^{(r)}_{BC}(\gamma; p, q) = \max L^{(r)}_{BC}(A)$, где максимум берется по всем не всюду определенным матрицам из p строк и q столбцов, имеющих γpq определенных элементов и $(1-\gamma)pq$ символов $*$.

Э. И. Нечипорук получил следующий результат.

Теорема 13 [26, 27]. *Пусть выполнены условия а) и б), а также условия*

$в^{\gamma}$) $\frac{\gamma p}{\log q} \to \infty$;

$е^{\gamma}$) $\frac{\log q}{\log \frac{1}{\gamma}} \to \infty$.

Тогда

$$L^{(2)}_{BC}(\gamma; p, q) \sim \gamma \frac{pq}{\log q}.$$

В некотором смысле окончательное (при естественном ограничении, что число полюсов существенно меньше сложности) асимптотически точное решение задачи о сложности реализации не всюду определенных матриц вентильными схемами глубины 2 было предложено А. Е. Андреевым в 1987 г.

Теорема 14 [3]. *Пусть выполнено условие б), а также условия*

$а^{\gamma}$) $\gamma q \to \infty$;

$в^{\gamma}_{а}$) $\frac{\gamma p}{\log(\gamma q)} \to \infty$.

Тогда

$$L^{(2)}_{BC}(\gamma; p, q) \sim \frac{\gamma pq}{\log(\gamma q)}.$$

Вместе с задачами о сложности реализации произвольных матриц и матриц из специальных классов значительное внимание привлекает задача о сложности реализации конкретных матриц. Во многом это связано с тем, что для вентильных схем в отличие от большинства модельных объектов управляющих систем удается получать нетривиальные (существенно превышающие линейные относительно числа полюсов и даже сравнимые с мощностными) нижние оценки для «индивидуальных последовательностей» матриц.

Э. И. Нечипоруком исследовалась [28] сложность реализации следующей последовательности булевых матриц. Пусть r — простое число и $n = r^2$. Обозначим через $F_{a,b}$ квадратную булеву матрицу порядка r, получающуюся из

диагональной матрицы циклическим сдвигом ее столбцов на $ab \pmod r$ позиций. Из этих блоков образуем квадратную матрицу F_n порядка n:

$$F_n = \{F_{a,b}\}_{a,b=0,1,\ldots,r-1}.$$

Теорема 15 [28]. *Всякая минимальная вентильная схема, реализующая матрицу F_n, состоит из $n^{3/2}$ вентилей, т. е. $L_{BC}(F_n) = n^{3/2}$.*

Несколько позже аналогичные результаты были получены Е. Ламаньей и Дж. Севиджем [35], а также Р. Тарьяном [41, 42] (для матриц Адамара).

В обзоре по вентильным схемам О. Б. Лупанова [21] (в котором отражены все перечисленные выше результаты, за исключением теорем 3 и 14) были поставлены три задачи.

1. Получить асимптотическое выражение для роста функции Шеннона $L_{BC}(p, q)$ в случае, когда величины $\log p$ и $\log q$ имеют одинаковый порядок роста.

2. Получить асимптотическую формулу для функции Шеннона $L_{BC}(n)$ в случае вентильных схем, реализующих произвольные транзитивные квадратные булевы матрицы порядка n (в которых не выделены специально входы и выходы).

3. Построить «эффективно» последовательность квадратных булевых матриц порядка n, которые реализуются лишь со сложностью, существенно большей, чем $n^{3/2}$.

Первая из этих задач, как уже говорилось, решена Н. Пиппенджером [36, 39] — см. теорему 3.

Вторую задачу решил в 1985 г. А. Е. Андреев [1].

Теорема 16 [1]. *При $n \to \infty$ имеет место соотношение*

$$L_{BC}(n) \sim \frac{n^2}{8 \log n}.$$

Продвижения в решении третьей задачи оказались связаны с построением семейств (k, l)-редких матриц (у которых никакие k строк не имеют l общих единиц, т. е. без единичных подматриц размера $k \times l$) — подробнее см., например, [5, 7]. Построение $(2, 2)$-редких матриц с числом единиц порядка $n^{3/2}$ привело [28, 35, 41] к получению нижней оценки сложности реализации этих матриц вентильными схемами, равной по порядку $n^{3/2}$, построение $(3, 3)$-редких матриц с числом единиц порядка $n^{5/3}$ — к получению [23, 37] нижней оценки сложности реализации этих матриц вентильными схемами, равной по порядку $n^{5/3}$. В 1985 г. А. Е. Андреев [2] для любого t построил пример $(O_t(1), O_t(1))$-редкой $n \times n$-матрицы с числом единиц порядка$n^{2-1/t}$ и получил для этой

матрицы нижние оценки порядка $n^{2-1/t}$ для сложности ее реализации вентильными схемами. Последний результат несколько усилен в работах [31, 34]. Тем самым для конкретных последовательностей матриц удается доказать нижние оценки, рост которых несильно отличается от роста функции Шеннона сложности реализации булевых матриц вентильными схемами.

Возвращаясь к задаче о сложности реализации вентильными схемами матриц из специальных классов, отметим, что сам факт существования достаточно плотных (с достаточно большим общим числом единиц) редких матриц может давать высокие нижние оценки, но, конечно, неконструктивные. В этом направлении для класса циклических (циркулянтных) булевых матриц, являющегося значительно более узким, нежели класс всех булевых матриц (так как циклическая матрица полностью определяется первой строкой — остальные строки получаются из нее соответствующими сдвигами), М. И. Гринчуком [6] получены нижние оценки сложности реализации вентильными схемами, близкие к значениям для класса всех булевых матриц.

Теорема 17 [6]. *Существует последовательность $\{C_n\}$ циклических булевых матриц порядка n, такая что для некоторых положительных c_1 и c_2 при всех достаточно больших n выполняются неравенства*

$$L_{BC}(C_n) \geqslant c_1 \frac{n^2}{\log^{12} n}, \quad L^{(2)}_{BC}(C_n) \geqslant c_2 \frac{n^2}{\log^{10} n}.$$

В работе [7] этот результат несколько усилен — доказано существование циклических матриц сложности по порядку не менее $\frac{n^2}{\log^5 n}$ при реализации произвольными вентильными схемами и по порядку не менее $\frac{n^2}{\log^4 n}$ — при реализации вентильными схемами глубины 2.

Теперь остановимся на задаче о сложности реализации вентильными схемами матриц с заданной площадью информационной части.

Пусть по-прежнему $A = (a_{ij})$ — булева матрица размера $p \times q$. Для $j = 1, 2, \ldots, q$ обозначим через p_j наибольший номер среди ненулевых элементов j-го столбца матрицы A. Таким образом,

$$p_j = \max\{i \mid a_{ij} \neq 0\}, \quad j = 1, 2, \ldots, q.$$

Положим

$$\mathcal{S}(A) = \sum_{j=1}^{q} p_j.$$

Величину $\mathcal{S}(\mathcal{A})$ будем называть *информационной площадью матрицы A*.

Отметим, что, вообще говоря, величина информационной площади матрицы не инвариантна относительно операции транспонирования матрицы. Кроме того, очевидно, что в матрице A среди pq элементов не менее $pq - \mathcal{S}(\mathcal{A})$ элементов нулевые.

Введем функцию Шеннона сложности реализации булевых матриц размера $p \times q$ с информационной площадью $\mathcal{S}$:

$$L_{BC}(p, q; \mathcal{S}) = \max L_{BC}(A),$$

где максимум берется по всем матрицам размера $p \times q$ с информационной площадью $\mathcal{S}$.

Аналогично определяется и функция Шеннона $L_{01}(p, q; \mathcal{S})$.

С использованием теоремы 3 установлен следующий факт.

Теорема 18 [9, 10]. *Пусть выполнено условие*

$в_{\mathcal{S}}$) $\frac{(p+q)\log \mathcal{S}}{\mathcal{S}} \to 0$;

Тогда

$$L_{01}(p, q; \mathcal{S}) \sim L_{BC}(p, q; \mathcal{S}) \sim \frac{\mathcal{S}}{\log \mathcal{S}}.$$

На использовании теоремы 18 основано асимптотически точное решение двух известных задач. Первая из них поставлена в 1963 г. Р. Беллманом [32] (для частного случая) и в 1964 г. Е. Страусом [40] (в общем виде) и заключается в нахождении для произвольного одночлена $x_1^{a_1} x_2^{a_2} \dots x_q^{a_q}$ его сложности $l(x_1^{a_1} x_2^{a_2} \dots x_q^{a_q})$ вычисления — минимального числа умножений, достаточного для вычисления по переменным $x_1, \dots, x_q$ одночлена $x_1^{a_1} x_2^{a_2} \dots x_q^{a_q}$. Вторая поставлена в 1969 г. Д. Кнутом [8, разд. 4.6.3., упр. 32] и состоит в нахождении сложности $l(x^{a_1}, x^{a_2}, \dots, x^{a_p})$ вычисления набора из p степеней одной переменной, определяемой аналогично.

В работе [4] на основе теоремы 18 установлены такие верхние оценки в задачах Беллмана — Страуса и Кнута (эти оценки уточнены в [12]): для любой последовательности наборов натуральных чисел $\big(n_1(s), n_2(s), \dots, n_{m(s)}(s)\big)$, $s = 1, 2, \dots$, удовлетворяющей условию $\sum\limits_{i=1}^{m(s)} n_i(s) \to \infty$, выполняются неравенства

$$l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) \leqslant l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}) \leqslant$$
$$\leqslant \log \max_{1 \leqslant i \leqslant m} n_i + \frac{\log N}{\log \log N} \left(1 + O\left(\left(\frac{\log \log \log N}{\log \log N}\right)^{1/2}\right)\right) + O(m),$$

где $N = n_1 n_2 \dots n_m$.

В статье [11] установлено, что указанные верхние оценки для почти всех наборов $\big(n_1(s), n_2(s), \dots, n_{m(s)}(s)\big)$ асимптотически неулучшаемы.

2. Вентильные схемы с кратными путями

Н. Пиппенджер, завершивший исследования О. Б. Лупанова и Э. И. Нечипорука по нахождению асимптотики роста функции Шеннона сложности ре-

ализации булевых матриц вентильными схемами, обобщил этот результат на естественным образом возникающую, например, в задаче о сложности вычисления систем одночленов [38], следующую модификацию классических вентильных схем.

Пусть $A = (a_{ij})$ — целочисленная матрица размера $p \times q$ с неотрицательными элементами. Ориентированный граф S без ориентированных циклов будем называть *вентильной схемой с кратными путями* (или *вентильной схемой с предписанным числом путей*), *реализующей матрицу* A, если: в S выделено p вершин — входных полюсов и q вершин — выходных полюсов; в S нет ориентированных путей от одного входа к другому, от одного выхода к другому, от выхода к входу; для любой пары (i, j), $1 \leqslant i \leqslant p$, $1 \leqslant j \leqslant q$, число ориентированных путей от i-го входа к j-му выходу равно в точности a_{ij}. Аналогично случаю классических вентильных схем, через $L^{kp}_{BC}(S)$ обозначим число ребер (вентилей) схемы S и положим $L^{kp}_{BC}(A) = \min L^{kp}_{BC}(S)$, где минимум берется по всем схемам, реализующим матрицу A.

Для функции Шеннона, определяемой равенством $L^{kp}_{BC}(p, q, K) = L^{kp}_{BC}(A)$, где максимум берется по всем матрицам размера $p \times q$ с неотрицательными целыми элементами, не превосходящими K, Н. Пиппенджером при слабых ограничениях установлена при $pq \log(K + 1) \to \infty$ асимптотика роста.

Теорема 19. *Пусть выполняется условие* $pq \log(K + 1) \to \infty$. *Тогда*

$$L^{kp}_{BC}(p, q, K) = 3 \min(p,\, q) \log_3 K + \\ + \frac{pq \log_2(K + 1)}{\log_2(pq \log(K + 1))}(1 + o(1)) + O(\max(p,\, q)).$$

Этот результат сформулирован в [39], а его доказательство можно восстановить, объединив доказательства из [39] и [38].

Тем самым для обеих модификаций вентильных схем при слабых ограничениях на число полюсов (входов и выходов) установлена асимптотика роста функций Шеннона и предложен метод синтеза вентильных схем, дающий для почти всех матриц асимптотически минимальную верхнюю оценку. Однако при попытках получения асимптотически точных оценок сложности индивидуальных последовательностей матриц при реализации классическими схемами возникают стандартные трудности с доказательством нижних оценок, в той или иной степени близких к «мощностной», которые удается так или иначе преодолеть лишь в некоторых случаях (см., например, [2, 23, 28, 35, 41]). При реализации матриц вентильными схемами с кратным числом путей ситуация, вообще говоря, не такая — в наиболее естественном и интересном случае, когда размеры матриц ограничены (или очень слабо растут), слагаемое, соответствующее мощностным соображениям, дает не основной по порядку вклад

в рост функции Шеннона. Это дает надежду получать асимптотически точные нижние оценки для индивидуальных последовательностей (матриц). И в этом направлении получены значительные продвижения, переходя к которым далее под вентильными схемами условимся понимать вентильные схемы с кратным числом путей.

Лемма [17]. *Пусть k вершинам вентильной схемы S, приписаны наборы $(a_{11}, a_{12}, \ldots, a_{1k})$, $(a_{21}, a_{22}, \ldots, a_{2k})$, $\ldots (a_{k1}, a_{k2}, \ldots, a_{kk})$, задаваемые матрицей $A = (a_{ij})$ размера $k \times k$, Тогда*

$$3^{L_{BC}^{kp}(S)} \geqslant |\det A|^3.$$

Доказательство. Будем вести доказательство индукцией по числу вершин схемы, в которые входит хотя бы один вентиль. Для схемы, не содержащей ни одного вентиля, утверждение леммы очевидно.

В схеме S среди k выбранных вершин обозначим через v_k ту, вершину, от которой к другим выделенным вершинам не ведут пути (хотя бы одна такая вершина всегда найдется в силу ацикличности вентильной схемы). Пусть в вершину v_k ведут r вентилей. Вершины, из которых выходят эти вентили, обозначим соответственно через $v_k^{(1)}, v_k^{(2)}, \ldots, v_k^{(r)}$. Пусть этим вершинам приписаны наборы $(a_{k1}^{(i)}, a_{k2}^{(i)}, \ldots, a_{kk}^{(i)})$, $i = 1, 2, \ldots, r$. Тогда набор $(a_{k1}, a_{k2}, \ldots, a_{kk})$ есть покомпонентная сумма наборов $(a_{k1}^{(i)}, a_{k2}^{(i)}, \ldots, a_{kk}^{(i)})$, $i = 1, 2, \ldots, r$. Матрицу, получающуюся из матрицы A путем замены строки $(a_{k1}, a_{k2}, \ldots, a_{kk})$ на строку $(a_{k1}^{(i)}, a_{k2}^{(i)}, \ldots, a_{kk}^{(i)})$, обозначим через $A^{(i)}$. Схему, получающуюся из схемы S путем выбрасывания вершины v_k и всех вентилей, входящих в v_k, обозначим через S'. Применяя предположение индукции, имеем:

$$|\det A| = \left|\sum_{i=1}^{r} \det A^{(i)}\right| \leqslant \sum_{i=1}^{r} \left|\det A^{(i)}\right| \leqslant$$

$$\leqslant r\left(3^{L_{BC}^{kp}(S')}\right)^{1/3} = r\left(3^{L_{BC}^{kp}(S)-r}\right)^{1/3} \leqslant \left(3^{L_{BC}^{kp}(S)}\frac{r^3}{3^r}\right)^{1/3} \leqslant \left(3^{L_{BC}^{kp}(S)}\right)^{1/3}.$$

Лемма доказана.

Положим

$$D(A) = \max_{k:\ 1\leqslant k\leqslant \min(p,q)} \left(\max_{(i_1,\ldots,i_k;\, j_1,\ldots,j_k)} |\det A(i_1, i_2, \ldots, i_k;\, j_1, j_2, \ldots, j_k)|\right).$$

Таким образом, $D(A)$ — это максимум абсолютных величин миноров матрицы A, где максимум берется по всем минорам.

Из леммы непосредственно выводится

Теорема 20. *Для любой ненулевой целочисленной матрицы A с неотрицательными элементами справедливо неравенство*

$$L_{BC}^{kp}(A) \geqslant 3\log_3 D(A).$$

Оказывается, что нижняя оценка из теоремы 20 является хорошей базой для исследования асимптотического поведения сложности индивидуальных последовательностей матриц фиксированного размера, что подтверждает следующая

Теорема 21. *Для произвольного натурального m и произвольной последовательности матриц $\{A_n\}$ с неотрицательными элементами, каждая из которых имеет размер либо $2 \times q_n$, где $q_n \leqslant m$, либо $p_n \times 2$, где $p_n \leqslant m$, либо 3×3, при условии $D(A_n) \to \infty$ выполняется соотношение*

$$L_{BC}^{kp}(A_n) \sim 3\log_3 D(A_n).$$

Доказательство верхней оценки этой теоремы в идейном плане не сильно отличается от доказательства верхних оценок сложности вычисления систем одночленов (см., например, работы [13–15]) и технически достаточно тяжелое: например, доказательство верхней оценки в случае матриц размера 3×3 занимает примерно 70 страниц. Частичное разъяснение природы трудностей, возникающих при доказательстве верхней оценки теоремы 2 дает следующий факт. Казалось бы логично вытекающее из теоремы 21 предположение о том, что, возможно, при всех фиксированных значениях p и q для матриц размера $p \times q$ величина $L_{BC}^{kp}(A)$ асимптотически растет как $3\log_3 D(A)$, оказывается неверным уже для квадратных матриц порядка 4.

Обозначим через $A(t, n)$ матрицу размера $2t \times 2t$, определяемую следующим образом. Первой строкой матрицы $A(t, n)$ является набор длины $2t$, первая половина разрядов которого равна n, а вторая половина — 0. Остальные $2t-1$ строки матрицы $A(t, n)$ получаются из первой строки последовательным циклическим сдвигом на один разряд вправо. Тогда элементы a_{ij} матрицы $A(t, n)$ задаются равенствами

$$a_{ij} = \begin{cases} n, & \text{если } 0 \leqslant j - i \leqslant t - 1 \text{ или } j - i \leqslant -(t + 1); \\ 0, & \text{если } j - i \geqslant t \text{ или } -t \leqslant j - i \leqslant -1, \end{cases}$$

$i = 1, 2, \ldots, 2t$, $j = 1, 2, \ldots, 2t$.

Для примера выпишем матрицу $A(t,n)$ при $t=3$:

$$A(3,n)=\begin{pmatrix} n & n & n & 0 & 0 & 0\\ 0 & n & n & n & 0 & 0\\ 0 & 0 & n & n & n & 0\\ 0 & 0 & 0 & n & n & n\\ n & 0 & 0 & 0 & n & n\\ n & n & 0 & 0 & 0 & n \end{pmatrix}.$$

Теорема 22. *При условии* $t=o(\log n)$ *справедливо асимптотическое равенство*

$$L_{BC}^{kp}(A(t,n))\sim 6t\log_3 n.$$

Доказательство этой теоремы очень похоже на доказательство теоремы 1 из [16].

Следствием теоремы 22 является такое утверждение: при выполнении условия $t\leqslant\frac{\log n}{\log\log n}$ имеет место соотношение $L_{BC}^{kp}\sim\frac{6t}{t+1}\log_3 D(A(t,n))$. Таким образом, приведен пример последовательности матриц размера $2t\times 2t$, для которой устанавливаемую теоремой 20 нижнюю оценку можно усилить асимптотически в $2t/(t+1)$ раз.

Теперь перейдем к задаче о сложности реализации недоопределенных матриц вентильными схемами с кратными путями. Пусть $A=(a_{ij})$ — матрица, элементами которой являются целые неотрицательные числа и элементы $*$ (символ $*$ соответствует неопределенному элементу).

Такую матрицу так же как и в булевом случае будем называть *невсюду определенной* или *недоопределенной* (отметим, что формально полностью определенные матрицы являются частным случаем недоопределенных).

Матрица $B=(b_{ij})$ называется *доопределением* матрицы $A=(a_{ij})$ такого же размера, если в матрице B все элементы определены (нет символов $*$), и для любого определенного элемента a_{ij} матрицы A справедливо равенство $a_{ij}=b_{ij}$.

Пусть A — недоопределенная матрица, в которой все определенные элементы целочисленны и неотрицательны. Положим

$$L_{BC}^{kp}(A)=\inf L_{BC}^{kp}(B),$$

где инфимум берется по всем доопределениям B матрицы A до целочисленной матрицы с неотрицательными элементами.

Очевидно, что инфимум достигается.

Без ограничения общности можно считать, что в матрицах нет ни строк, ни столбцов, полностью состоящих из нулей и символов $*$.

Теперь рассмотрим случай, когда матрица состоит либо из двух строк, либо из двух столбцов. Без ограничения общности будем считать, что $A = (a_{ij})$ — недоопределенная матрица размера $p \times 2$.

Обозначим через $A_o = A_o(A)$ полностью определенную (возможно пустую) матрицу, получающуюся из матрицы A путем вычеркивания неполностью определенных строк. Положим $d_0(A) = D(A_o)$ если матрица A_o непустая, и $d_0(A) = 1$ в случае отсутствия полностью определенных строк в матрице A.

Выделим три подмножества множества $\{1, 2, \ldots, p\}$ номеров строк матрицы A. Через I_1 обозначим множество номеров таких строк, в которых первый элемент является определенным, а второй элемент — символ $*$, через I_2 — множество номеров таких строк, в которых первый элемент является символом $*$, а второй элемент — определенный, и, наконец, через J — множество номеров строк, оба элемента которых являются определенными.

Положим

$$d_1(A) = \frac{\max\left(\max\limits_{i \in I_1}\{a_{i1}\}, 1\right)}{\max\left(\max\limits_{j \in J}\{a_{j1}\}, 1\right)}, \quad d_2(A) = \frac{\max\left(\max\limits_{i \in I_2}\{a_{i2}\}, 1\right)}{\max\left(\max\limits_{j \in J}\{a_{j2}\}, 1\right)}.$$

Здесь максимумы в числителях (по i) берутся по всем определенным элементам, стоящим в неполностью определенных строках (т. е. в строках, в которых второй элемент — символ $*$), а максимумы в знаменателях (по j) берутся по всем определенным элементам, стоящим в полностью определенных строках.

Теперь положим

$$D^*(A) = d_0(A) \max\{d_1(A), d_2(A), 1\}.$$

Теорема 23 [18]. *Для произвольной последовательности недоопределенных матриц $A_n = \big(a_{ij}(n)\big)$, $n = 1, 2, \ldots$, фиксированного размера $p \times 2$, все определенные элементы которых неотрицательны, при условии $\sum a_{ij}(n) \to \infty$ (сумма берется по всем определенным элементам матрицы A_n) выполняется соотношение*

$$L_{BC}^{kp}(A_n) \sim 3 \log_3 D^*(A_n).$$

Работа выполнена при финансовой поддержке РФФИ (проект 11–01–00508).

Литература

1. Андреев А. Е. О сложности реализации транзитивных отношений вентильными схемами // Физическое и математическое моделирование дискретных систем. — М.: МЭИ, 1985. — № 56. — С. 11–21.

2. Андреев А. Е. Об одном семействе булевых матриц // Вестник Московского университета. Сер. 1. Математика. Механика. — 1986. — № 2. — С. 97–100.

3. Андреев А. Е. О сложности реализации вентильными схемами недоопределенных матриц // Математические заметки. — 1987. — Т. 41, № 1. — С. 77–86.

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

5. Гашков С. Б., Сергеев И. С. О сложности линейных булевых операторов с редкими матрицам // Дискретный анализ и исследование операций. — 2010. — Т. 17, № 3. — С.3–18.

6. Гринчук М. И. О сложности реализации циклических булевых матриц вентильными схемами // Известия ВУЗов. Математика. — 1988. — № 7. — 39–43.

7. Гринчук М. И., Сергеев И. С. Редкие циркулянтные матрицы и нижние оценки сложности некоторых булевых операторов // Дискретный анализ и исследование операций. — 2011. — Т. 18, № 5. — С.38–53.

8. Кнут Д. Е. Искусство программирования для ЭВМ, т. 2. 1-е издание. — М.: Мир, 1977.

9. Кочергин В. В. О сложности вычислений в конечных абелевых группах // ДАН СССР. — 1991. — Т. 317, № 2. — С. 291–294.

10. Кочергин В. В. О сложности вычислений в конечных абелевых группах // Математические вопросы кибернетики, вып. 4. — М.: Наука, 1992. — С. 178–217.

11. Кочергин В. В. О сложности вычислений одночленов и наборов степеней // Дискретный анализ. — Новосибирск: Издательство Института математики СО РАН, 1994. — (Тр./РАН. Сиб. отделение. Ин-т математики; Т. 27) — С. 94–107.

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

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

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

15. Кочергин В. В. О сложности вычисления системы из трех одночленов от трех переменных // Математические вопросы кибернетики, вып. 15. — М.: Физматлит, 2006. — С. 79–155.

16. Кочергин В. В. Об одном соотношении двух мер сложности вычисления систем одночленов // Вестник Московского университета. Сер. 1. Математика. Механика. — 2009, № 4. — С. 8–13.

17. Кочергин В. В. О сложности вентильных схем с кратным числом путей // Материалы XVIII Международной школы-семинара «Синтез и сложность управляющих систем» имени академика О. Б. Лупанова (Пенза, 28 сентября – 03 октября 2009 г.). — М.: Изд-во механико-математического факультета МГУ, 2009. — С. 51–56.

18. Кочергин В. В. О реализации недоопределенных матриц из двух столбцов вентильными схемами с кратными путями // Вестник Нижегородского университета им. Н. И. Лобачевского. — 2012. — Вып. 5, часть 2. — С. 111–116.

19. Лупанов О. Б. О вентильных и контактно-вентильных схемах // Доклады АН СССР. — 1956. — Т. 111, № 6. — С. 1171–1174.

20. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики, вып. 10. — М.: Физматгиз, 1963. — С. 63–97.

21. Лупанов О. Б. О вентильных схемах // Acta Cybernetica. — 1980. — V. 4, № 4. — P. 311–315.

22. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во Московского университета, 1984.

23. Мельхорн К. Некоторые замечания, касающиеся булевых сумм // Кибернетический сборник. Вып. 18. — М.: Мир, 1981. — С. 39–45.

24. Нечипорук Э. И. О синтезе вентильных схем // Проблемы кибернетики, вып. 9. — М.: Физматгиз, 1963. — С. 37–44.

25. Нечипорук Э. И. О вентильных схемах // Доклады АН СССР. — 1963. — Т. 148, № 1. — С. 50–53.

26. Нечипорук Э. И. О сложности вентильных схем, реализующих булевские матрицы с неопределенными элементами // Доклады АН СССР. — 1965. — Т. 163, № 1. — С. 40–42.

27. Нечипорук Э. И. О топологических принципах самокорректирования // Проблемы кибернетики, вып. 21. — М.: Наука, 1969. — С. 5–102.

28. Нечипорук Э. И. Об одной булевской матрице // Проблемы кибернетики, вып. 21. — М.: Наука, 1969. — С. 237–240.

29. Орлов В. А. Реализация «узких» матриц вентильными схемами // Проблемы кибернетики, вып. 22. — М.: Наука, 1970. — С. 45–52.

30. Чашкин А. В. О сложности булевых матриц, графов и соответствующих им булевых функций // Дискретная математика. — 1994. — Т. 6, вып. 2. — С. 44–73.

31. Alon N., Rónyai L., Szabó T. Norm-graphs: variations and applications // J. Combinat. Theory. Ser. B. — 1999. — V. 76, № 3. — P. 280–290.

32. Bellman R. E. Addition chains of vectors (Advanced problem 5125) // Amer. Math. Monthly. — 1963. — V. 70. — P. 765.

33. Jukna S., Sergeev S. Complexity of linear Boollean operators // Foundations and Trends in Theoretical Computer Science. — В печати.

34. Kóllar J., Rónyai L., Szabó T. Norm-graphs and bipartite Turán numbers // Combinatorica. — 1996. — V. 16, № 3. — P. 399–406.

35. Lamagna E. A., Savage J. E. Computational complexity of some monotone functions // Proc. 15th SWAT Conference. — Long Beach: IEEE Comput. Soc. Press, 1974. — P. 140–144.

36. Pippenger N. On evaluation of powers and related problems // Proc. 17^{th} Ann. IEEE Symp. on Found. of Computer Sci. (Houston, TX, 25–27 Oct. 1976.) — P. 258–263.

37. Pippenger N. On another Boolean matrix // Theoretical Computer Science. — 1980. — V. 11, I. 1. — P. 49–56.

38. Pippenger N. On evaluation of powers and monomials // SIAM J. Comput. — 1980. — V. 9, N 2. — P. 230–250.

39. Pippenger N. The mimimum number of edges in graphs with prescribed paths // Math. Systems Theory. — 1979. — V. 12, № 4. — P. 325–346.

40. Straus E. G. Addition chains of vectors // Amer. Math. Monthly. — 1964. — V. 71. — P. 806–808.

41. Tarjan T. G. Complexity of lattice-configurations // Studia Sci. Math. Hungar. — 1975. — V. 10. — P. 203–211.

42. Tarjan T. G. Complexity of monotone networks for computing conjunctionns // Ann. Discrete Math. — 1978. — № 2. — P. 121–133.

ПОЛУЧЕНИЕ НИЖНИХ ОЦЕНОК СЛОЖНОСТИ СХЕМ МЕТОДОМ ЗАМЕНЫ БАЗИСОВ

Н. П. Редькин

**МГУ им. М. В. Ломоносова,
Москва**

e-mail: npredkin@yandex.ru

1. Введение

Фундаментальной проблемой математической кибернетики является построение оптимальных — в том или ином смысле — управляющих систем и, в частности, построение минимальных схем из функциональных элементов [1] для конкретных булевых функций. При построении минимальных схем обычно приходится решать две задачи: вначале строить подходящие достаточно простые схемы, а затем доказывать минимальность (иногда хотя бы в асимптотике или даже по порядку) этих схем. Первую задачу во многих случаях, представляющих научный и практический интерес, удается решить довольно быстро и легко. Для доказательства утверждений о минимальности, в том числе и об асимптотической минимальности схем из функциональных элементов для конкретных булевых функций требуется получать достаточно хорошие нижние оценки сложности схем, реализующих заданные функции. Получение таких оценок почти всегда вызывает затруднения, иногда весьма значительные; исключения составляют разве что тривиальные случаи типа нахождения сложности реализации конъюнкции $x_1 \& \ldots \& x_n$ схемами в базисах, содержащих $x \& y$.

Известные к настоящему времени способы получения нижних оценок сложности схем для конкретных булевых функций зачастую предполагают достаточно простые базисы, как правило, содержащие лишь одно- и двухвходовые элементы. Возьмем, скажем, метод «забивания» переменных на входах схем булевыми константами. Этот метод позволил, например, установить сложность реализации линейных булевых функций схемами в базисах $\{x \& y,\ x \vee y,\ \overline{x}\}$, $\{x \& y,\ \overline{x}\}$, $\{x \vee y,\ \overline{x}\}$ [2]. Основан он на использовании следующих простых свойств схем в базисе $\{x \& y,\ x \vee y,\ \overline{x}\}$ (а также и в базисах $\{x \& y,\ \overline{x}\}$, $\{x \vee y,\ \overline{x}\}$).

Свойство 1. Пусть в схеме S имеются $n+2$ входов, на которые подаются переменные $x_1, x_2, \ldots, x_n$ и булевы константы 0 и 1. Если на вход какого-либо элемента схемы S подается булева константа (т. е. тождественный нуль или

тождественная единица), то этот элемент можно удалить из схемы так, что реализуемая этой схемой функция не изменится.

Свойство 2. Пусть в схеме S имеются $n+2$ входов, на которые подаются переменные x_1, x_2, ..., x_n и булевы константы 0 и 1. Тогда если какой-либо элемент схемы S реализует булеву константу, то этот элемент можно удалить из схемы S так, что реализуемая схемой функция не изменится.

Заметим, что изменение соединений элементов в схеме (после того как некоторые элементы будут удалены) всюду считается возможным. Возможно также использование и других (тоже, как правило, достаточно простых) свойств схем.

Представим теперь, что рассматриваются схемы в базисе $\{x_1 \& \ldots \& x_l, x_1 \vee \cdots \vee x_l, \overline{x}\}$, где $l \geqslant 3$. Очевидно, что схемы в этом базисе по-прежнему обладают вторым свойством, но вот первое свойство в каких-то случаях может и не выполняться (например, если на один вход трехвходового конъюнктора подается константа 1, а на два других входа подаются x и y). В результате получение нужной нижней оценки сложности схем «стандартным» методом забивания переменных будет затруднено или даже вообще окажется невозможным. Но оказывается, что полученные нижние оценки схем в простых базисах (скажем, из двухвходовых элементов) можно эффективно использовать для получения аналогичных оценок для схем в более сложных базисах. Суть рассматриваемого подхода к получению новых оценок сложности заключается в замене одного («сложного») базиса другим (более «простым») базисом.

Пусть B — произвольный базис с положительными весами элементов, а S — схема в базисе B. Как обычно, сумму весов всех элементов S будем считать *сложностью схемы* S, а обозначать эту величину будем через $L_B(S)$. Для произвольной реализуемой в базисе B булевой функции f положим $L_B(f) = \min L_B(S)$, где минимум берется по всем схемам в базисе B, реализующим f. Число $L_B(f)$ задает (по определению) *сложность реализации* функции f схемами в базисе B; схему S в базисе B, реализующую булеву функцию f, будем считать *минимальной*, если $L_B(S) = L_B(f)$.

Пусть имеются два произвольных конечных базиса B, B^*, и базис B содержит элементы E_1, ..., E_a с весами $P(E_1)$, ..., $P(E_a)$, а базис B^* содержит элементы E_1^*, ..., E_b^* с весами $P(E_1^*)$, ..., $P(E_b^*)$ соответственно. Пусть элементам E_1, ..., E_a приписаны (реализуемые этими элементами) функции φ_1, ..., φ_a, а элементам E_1^*, ..., E_b^* — функции φ_1^*, ..., φ_b^*.

Справедливо следующее утверждение о соотношении сложностей реализации одной и той же булевой функции схемами из функциональных элементов в разных базисах.

Теорема 1. *Пусть булева функция f реализуема схемой в базисе B и схемой в базисе B^*, а функции из B^* реализуемы схемами в базисе B и выпол-*

няются неравенства

$$L_B(\varphi_i^*) \leqslant P(E_i^*), \quad 1 \leqslant i \leqslant b. \tag{1}$$

Тогда выполняется и неравенство

$$L_{B^*}(f) \geqslant L_B(f). \tag{2}$$

Доказательство. Пусть задана произвольная булева функция f, реализуемая схемами в базисах B и B^*. Построим для нее минимальную схему S^* в базисе B^*, для которой выполняется условие

$$L_{B^*}(S^*) = L_{B^*}(f). \tag{3}$$

Воспользуемся условием теоремы и все функции $\varphi_1^*, \ldots, \varphi_b^*$ реализуем минимальными схемами (блоками) $S_1, \ldots, S_b$, построенными в базисе B; из (1) для сложностей блоков $S_1, \ldots, S_b$ следуют оценки

$$L_B(S_i) \leqslant P(E_i^*), \quad 1 \leqslant i \leqslant b. \tag{4}$$

Все элементы в схеме S^* заменим отвечающими им блоками (элемент E_i^* заменяется при этом блоком S_i, $1 \leqslant i \leqslant b$). В результате такой замены вместо схемы S^* в базисе B^* получим некоторую схему S в базисе B, реализующую прежнюю функцию f. Из (3) и (4) получаем $L_{B^*}(f) \geqslant L_B(S)$, а это означает, что неравенство (2) выполняется. Теорема доказана.

Покажем теперь на конкретных примерах, как с использованием теоремы 1 можно находить точные или асимптотически точные значения сложности реализации индивидуальных булевых функций схемами в базисах из многовходовых элементов.

2. Оценка сложности для монотонных симметрических пороговых функций

Рассмотрим базис B^*, содержащий элементы E_1^*, E_2^*, E_3^*, реализующие соответственно функции $\varphi_1^* = x_1 \,\&\, \ldots \,\&\, x_l$, $\varphi_2^* = x_1 \vee \cdots \vee x_l$, $\varphi_3^* = \overline{x}$, где l — некоторое заданное натуральное число не меньше трех, а вес каждого элемента равен единице (т. е. сложность схем будет определяться числом элементов в них). В этом базисе для сложности реализации функции $f_2^n(\tilde{x}) = \bigvee\limits_{1 \leqslant i < j \leqslant n} x_i x_j$ справедлива следующая теорема.

Теорема 2. *Выполняется асимптотическое равенство*

$$L_{B^*}(f_2^n) \sim \frac{2n}{l-1}.$$

Доказательство. Верхнюю оценку $L_{B^*}(f_2^n) \lesssim \frac{2n}{l-1}$ получим, воспользовавшись конструкцией М. И. Гринчука из [3], основанной на представлении функции f_2^n в виде

$$f_2^n(x_1, \ldots, x_n) = f_2^m(a_1, \ldots, a_m) \vee f_2^m(b_1, \ldots, b_m), \tag{5}$$

где $m = \lceil \sqrt{n} \rceil$, а каждое a_i и каждое b_i представляет собой дизъюнкцию не более чем m переменных из множества $\{x_1, \ldots, x_n\}$. Каждое a_i и b_i вычисляется с использованием цепочки не более чем из $\frac{m}{l-1}$ дизъюнкторов E_2^*; всего l-входовых дизъюнкторов потребуется для этого, как нетрудно заметить, асимптотически не более чем $\frac{2n}{l-1}$ штук. После этого на «достройку» схемы, вычисляющей f_2^n в соответствии с представлением (5), потребуется по порядку не более чем $\sqrt{n}$ элементов (см. первый раздел из [3]). В итоге получается схема, реализующая функцию f_2^n и содержащая асимптотически не более чем $\frac{2n}{l-1}$ элементов.

Нижнюю оценку получим заменой базиса B^* новым базисом B, содержащим двухвходовые конъюнктор и дизъюнктор и (одновходовый) инвертор. Вес каждого элемента из B положим равным $\frac{1}{l-1}$; в таком случае условия (неравенства) (1) теоремы 1 будут выполнены.

Согласно теореме 1 из [3] общее число двухвходовых конъюнкторов, двухвходовых дизъюнкторов и инверторов в любой схеме для f_2^n не меньше чем $2n - 3$; отсюда следует, что сложность любой схемы для f_2^n в базисе B не меньше чем $\frac{2n-3}{l-1}$, т. е.

$$L_B(f_2^n) \geqslant \frac{2n-3}{l-1}. \tag{6}$$

Применяя теорему 1 из неравенств (2) и (6) получаем

$$L_{B^*}(f_2^n) \gtrsim \frac{2n}{l-1}.$$

Теорема доказана.

3. Оценка сложности булевых функций с малым числом единиц

Рассмотрим класс булевых функций $F_{n,k}$, состоящий из всех тех булевых функций от n переменных, каждая из которых обращается в единицу ровно на k наборах значений переменных. Для класса $F_{n,k}$ Б. И. Фиников установил [4], что если $k = O(\log n)$, то все функции из $F_{n,k}$ реализуемы в классе схем из функциональных элементов (в любом конечном функционально полном базисе) с линейной по n сложностью. Асимптотику для сложности реализации почти всех булевых функций из $F_{n,k}$ в случаях, когда $\log n = o(\min\{k, 2^n - k\})$, нашел О. Б. Лупанов [5]; относительно базиса в [5] предполагается лишь то,

что он конечный и функционально полный, а положительные веса элементов базиса могут назначаться произвольно. Автором [6] найдена асимптотика сложности реализации каждой функции из $F_{n,k}$ в случае, когда выполняется условие

$$1 \leqslant k \leqslant \log n - c \log\log n, \tag{7}$$

где c — произвольная бóльшая единицы константа, а базис B содержит элементы, реализующие все булевы функции от двух переменных x и y, кроме двух линейных функций $x \oplus y$ и $x \oplus y \oplus 1$ (знак $\oplus$ означает сложение по модулю 2); вес каждого элемента предполагается равным единице.

В рассматриваемом ниже примере предполагается, что условие (7) выполняется, а базис B^* содержит 2^{l+1} элементов, реализующих конъюнкции $x_1^{\sigma_1} \,\&\, \ldots \,\&\, x_l^{\sigma_l}$ и дизъюнкции $x_1^{\sigma_1} \vee \cdots \vee x_l^{\sigma_l}$ для всех булевых наборов $(\sigma_1, \ldots, \sigma_l)$ длины l, где l — заданное натуральное число не меньшее трех; вес каждого элемента полагается равным единице (т. е. сложность схемы определяется числом элементов в ней).

Напомним некоторые определения из [6]. Пусть $f(x_1, \ldots, x_n)$ — произвольная булева функция из $F_{n,k}$, обращающаяся в единицу на наборах $\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_k$, где $\tilde{\sigma}_i = (\sigma_{i,1}, \ldots, \sigma_{i,n})$, $i = 1, \ldots, k$. Функции f сопоставим $(k \times n)$-матрицу M_f, строками которой являются наборы $\tilde{\sigma}_1$, …, $\tilde{\sigma}_k$, а j-й столбец отвечает переменной x_j, $j = 1, \ldots, n$. Столбцы матрицы M_f разобъем на группы одинаковых между собой столбцов; через $M_{\tilde{\tau}}$ обозначим группу столбцов (т. е. подматрицу матрицы M_f, составленную из столбцов), равных $\tilde{\tau}$ (для каких-то $\tilde{\tau}$ группы $M_{\tilde{\tau}}$ могут оказаться пустыми). Непустую группу столбцов $M_{\tilde{\tau}}$ считаем *сильной*, если она содержит не менее двух столбцов $\tilde{\tau}$ и в этих столбцах имеются как нули, так и единицы; переменные, отвечающие столбцам из сильной группы, также считаем *сильными*. Число сильных переменных функции f обозначим через $m(f)$.

Теорема 3. *Пусть среди переменных функции $f(x_1, \ldots, x_n)$, $f \in F_{n,k}$, имеется m_n сильных переменных, а для последовательности $\{k_n\}$ при всех достаточно больших n выполнено условие* (7):

$$1 \leqslant k_n \leqslant \log n - c \log\log n,$$

где c — какая-нибудь бóльшая единицы константа. Тогда

$$L_{B^*}\big(f(x_1, \ldots, x_n)\big) \sim \frac{n + m_n}{l - 1}.$$

Доказательство. Верхняя оценка получается конструктивно путем незначительной модификации схемы S, представленной в разделе 5 из [6]. В данном случае схему S будем строить с использованием формулы (7) из [6] следующим образом.

По формуле $F_{2,1}$ из [6] построим схему S_1 (реализующую ту же функцию f_1, что и формула $F_{2,1}$) из [6] из $2\left\lceil\frac{i_1-1}{l-1}\right\rceil+1$ элементов, в которой с помощью $\left\lceil\frac{i_1-1}{l-1}\right\rceil$ штук l-входовых конъюнкторов $x_1\,\&\ldots\&\,x_l$ реализуется конъюнкция $x_1\,\&\ldots\&x_{i_1}$, с помощью $\left\lceil\frac{i_1-1}{l-1}\right\rceil$ элементов $\overline{x_1}\,\&\,\overline{x_2}\,\&\ldots\&\,\overline{x_l}$ и $x_1\,\&\,\overline{x_2}\,\&\ldots\&\,\overline{x_l}$ реализуется конъюнкция $\overline{x_1}\,\&\ldots\&\,\overline{x_{i_1}}$, а на выходе дизъюнктора $x_1\vee x_2\vee\cdots\vee x_2$ (его роль играет элемент $x_1\vee x_2\vee\cdots\vee x_l$ с отождествленными 2-м, …, l-м входами) получается требуемая функция f_1.

Аналогичным образом по формулам $F_{2,2}$, …, $F_{2,r}$ из [6] строятся схемы S_2, …, S_r, реализующие функции f_2, …, f_r. Все вместе схемы S_1, …, S_r содержат $2\left\lceil\frac{i_1-1}{l-1}\right\rceil+2\left\lceil\frac{i_2-i_1-1}{l-1}\right\rceil+\cdots+2\left\lceil\frac{i_r-i_{r-1}-1}{l-1}\right\rceil$ элементов; последняя сумма, как не трудно заметить, не превосходит $\frac{2m}{l-1}+2r$.

По формуле $F_{2,r+1}$ из [6] построим схему S_{r+1} из $\left\lceil\frac{j_s}{l-1}\right\rceil$ элементов конъюнкции $x_1\,\&\ldots\&\,x_l$, реализующую ту же функцию, что и $F_{2,r+1}$. Схема S_{r+2} из $\left\lceil\frac{j_t-j_s-1}{l-1}\right\rceil$ элементов $\overline{x_1}\,\&\ldots\&\,\overline{x_l}$ и $x_1\,\&\,\overline{x_2}\,\&\ldots\&\,\overline{x_l}$ отвечает формуле $F_{2,r+2}$ из [6] и реализует ту же функцию f_{r+2}, что и формула $F_{2,r+2}$.

Формула $F'_{2,r+3}$ реализует f_{r+3} и представляет собой дизъюнктивную нормальную форму из k конъюнкций, каждая из которых содержит $r+n-i_r-j_t$ переменных. Формуле $F'_{2,r+3}$ сопоставим схему S_{r+3}, реализующую f_{r+3} и содержащую k цепочек, реализующих конъюнкции из $F'_{2,r+3}$, и $\left\lceil\frac{k-1}{l-1}\right\rceil$ элементов $x_1\vee\cdots\vee x_l$, осуществляющих сложение (логическое) конъюнкций в $F'_{2,r+3}$; каждая цепочка составляется из $\left\lceil\frac{r+n-i_r-j_t-1}{l-1}\right\rceil$ подходящих элементов $x_1^{\sigma_1}\,\&\ldots\&\,x_l^{\sigma_l}$. Всего в S_{r+3} окажется $k\left\lceil\frac{r+n-i_r-j_t-1}{l-1}\right\rceil+\left\lceil\frac{k-1}{l-1}\right\rceil$ элементов. Для умножения функций f_1, …, f_{r+3}, которые реализуются на выходах схем $S_1,\ldots,S_{r+3}$, достаточно взять цепочку S_{r+4} из $\left\lceil\frac{r+2}{l-1}\right\rceil$ элементов $x_1\,\&\ldots\&\,x_l$; в итоге получим схему S, реализующую f.

Для сложности полученной схемы S справедлива оценка

$$L_{B^*}(S)\leqslant\sum_{a=1}^{r+4}L_{B^*}(S_a)\leqslant\frac{2m}{l-1}+2r+\left\lceil\frac{j_s}{l-1}\right\rceil+$$
$$+\left\lceil\frac{j_t-j_s-1}{l-1}\right\rceil+k\left\lceil\frac{r+n-i_r-j_t-1}{l-1}\right\rceil+\left\lceil\frac{k-1}{l-1}\right\rceil+\left\lceil\frac{r+2}{l-1}\right\rceil.$$

Отсюда, учитывая неравенство (7) (условие теоремы), соотношение (5) из [6] и равенство $i_r=m$, получаем верхнюю оценку для $L_{B^*}(S)$ (а значит, и для $L_{B^*}(f)$)

$$L_{B^*}(S)\lesssim\frac{n+m}{l-1}.$$

Нижнюю оценку, как и в предыдущем примере, получим при переходе от базиса B^* к новому базису B, который содержит двухвходовые элементы, реализующие все булевы функции от двух переменных x и y, кроме двух

линейных функций ($x \oplus y$ и $x \oplus y \oplus 1$). Вес каждого элемента из B положим равным $\frac{1}{l-1}$; как нетрудно заметить, условия (1) теоремы 1 будут выполнены.

Согласно теореме 1 из [6], общее число элементов из B в любой схеме, реализующей функцию $f(x_1, \ldots, x_n)$ из $F_{n,k}$ с m сильными переменными, асимптотически не меньше $n + m$. Поэтому по теореме 1 сложность любой схемы для f в базисе B^* асимптотически не меньше чем $\frac{n+m}{l-1}$. Теорема доказана.

4. Об одном семействе классов булевых функций и их сложности реализации

Пусть l, m, n — натуральные параметры, удовлетворяющие условиям: а) $l \geqslant 3$; б) $m \leqslant n$; в) остаток от деления $m-1$ на $l-1$ не превосходит $\frac{l}{2}-1$. Обозначим через $F_{n,2}^{l,m}$ множество всех тех булевых функций из $F_{n,2}$, каждая из которых имеет m сильных переменных и при заданном $l \geqslant 3$ для параметров l, m, n выполняются условия а), б) и в).

Пусть $B = \{\varphi_1, \ldots, \varphi_8\}$ — множество из восьми булевых функций, каждая из которых есть либо конъюнкция $x^\alpha \,\&\, y^\beta$, либо дизъюнкция $x^\alpha \vee y^\beta$, где $\alpha, \beta \in \{0, 1\}$. При заданном натуральном l ($l \geqslant 3$) через B^* обозначим множество всех тех булевых функций, каждая из которых существенно зависит ровно от l переменных x_1, …, x_l и может быть реализована формулой над B сложности $l - 1$; под сложностью формулы Φ над B понимается число функциональных символов из B в формуле Φ [7].

Будем рассматривать теперь схемы из функциональных элементов в базисе B^* и найдем сложность реализации функций из $F_{n,2}^{l,m}$ схемами из функциональных элементов в базисе B^*, полагая вес каждого элемента из B^* равным единице.

Теорема 4. *Пусть* $f(\tilde{x}) \in F_{n,2}^{l,m}$ *и для параметров* l, m, n *выполняются условия* а), б) *и* в). *Тогда*

$$L_{B^*}(f) = \left\lceil \frac{n + m - 1}{l - 1} \right\rceil.$$

Доказательство. Верхнюю оценку получим конструктивно. Без ограничения общности можем предполагать, что сильными переменными заданной функции $f(\tilde{x})$ являются $x_1, \ldots, x_m$ (этого, во всяком случае, можно добиться подходящей нумерацией переменных). В таком случае в соответствии с определением класса $F_{n,2}^{l,m}$ функцию f можно представить в виде

$$f(\tilde{x}) = \left(x_1^{\sigma_1} \ldots x_m^{\sigma_m} \vee x_1^{\overline{\sigma_1}} \ldots x_m^{\overline{\sigma_m}}\right) x_{m+1}^{\sigma_{m+1}} \ldots x_n^{\sigma_n}. \tag{8}$$

Опираясь на представление (8), построим и схему S для f. Вначале возьмем две цепочки Z_1 и Z_2 из элементов базиса B^*, содержащие по p элементов каждая, где $p = \left\lfloor \frac{m-1}{l-1} \right\rfloor$, и реализующие соответственно конъюнкции

$K_1 = x_1^{\sigma_1} \dots x_{p(l-1)+1}^{\sigma_{p(l-1)+1}}$ и $K_2 = x_1^{\overline{\sigma_1}} \dots x_{p(l-1)+1}^{\overline{\sigma}_{p(l-1)+1}}$ (если окажется $p = 0$, то цепочки Z_1 и Z_2 в S будут отсутствовать). Добавим к Z_1, Z_2 элемент E, реализующий

$$\varphi = \left(K_1 x_{p(l-1)+2}^{\sigma_{p(l-2)+2}} \,\&\, \dots \,\&\, x_m^{\sigma_m} \vee K_2 x_{p(l-1)+2}^{\overline{\sigma}_{p(l-2)+2}} \,\&\, \dots \,\&\, x_m^{\overline{\sigma}_m}\right) \,\&\, x_{m+1}^{\sigma_{m+1}} \dots x_{m+q}^{\sigma_{m+q}},$$

где $q = \min\left\{n - m, l - 2(m - p(l-1))\right\}$ (если $n = m$, то множитель $x_{m+1}^{\sigma_{m+1}} \dots x_{m+q}^{\sigma_{m+q}}$ в формуле для φ отсутствует).

Заметим, что указанное (формально) значение параметра q на самом деле — по построению схемы — определяется следующим образом. На входы элемента E подаются конъюнкция K_1 (с выхода цепочки Z_1), переменные $x_{p(l-1)+2}, \dots, x_m$ (со входов схемы), конъюнкция K_2 и снова переменные $x_{p(l-1)+2}, \dots, x_m$ — в соответствии с формулой для φ; до этого момента возможность указанного подсоединения элемента E гарантируется условиями а)–в), которым удовлетворяют параметры l, m, n. Далее, если у элемента E еще остаются незадействованные входы, то на них подаются переменные $x_{m+1}, \dots, x_{m+q}$. Может оказаться, что на очередной вход элемента E уже будет подана последняя переменная x_n, а у элемента E все еще остаются незадействованные входы $v_1, \dots, v_t$. Тогда на эти входы $v_1, \dots, v_t$ дополнительно подается одна и та же последняя переменная x_n, а в формуле для φ в соответствующем месте (по соседству с $x_n^{\sigma_n}$) еще t раз повторяется множитель $x_n^{\sigma_n}$. При подаче последней переменной x_n на входы элемента E построение схемы S на этом заканчивается; нетрудно заметить, что в этом случае S содержит не более $\left\lceil \frac{n+m-1}{l-1} \right\rceil$ элементов.

Рассмотрим другой случай, когда все входы элемента E оказываются задействованными, последней на вход элемента E подана переменная x_{m+q}, $q \geqslant 0$, но $m + q < n$. В этом случае схема дополняется цепочкой Z из последовательно соединенных элементов $E_1, \dots, E_h$. Один вход элемента E_1 соединяется с выходом элемента E, а на остальные входы элемента E_1 подаются переменные $x_{m+q+1}, \dots, x_{m+q+l-1}$. Один вход элемента E_2 соединяется с выходом элемента E_1, а на остальные входы подаются $x_{m+q+l}, \dots, x_{m+q+2l-2}$, и т. д. Наконец, один вход элемента E_h соединяется с выходом элемента E_{h-1}, а на остальные входы элемента E_h подаются переменные $x_{m+q+(h-1)(l-1)+1} \cdots$ $\dots, x_n$; при этом хотя бы одна переменная на вход элемента E_h подается, а переменная x_n, возможно, подается на несколько входов (чтобы все входы нижнего в цепочке элемента оказались задействованными). Опять же нетрудно убедиться, что и в этом случае сложность построенной схемы S не будет превышать $\left\lceil \frac{n+m-1}{l-1} \right\rceil$. Таким образом, верхняя оценка установлена.

Нижнюю оценку получим при переходе от базиса B^* к базису B. Вес каждого элемента из B положим равным $\frac{1}{l-1}$; в этом случае из определения базиса B^* видно, что условия (1) теоремы 1 будут выполнены.

Согласно теореме 3 из [6] любая схема над B, реализующая функцию $f(\tilde{x})$ из $F_{n,2}^{l,m}$, содержит не менее чем $n + m - 1$ элементов, т. е. выполняется нера-

венство

$$L_B(f) \geqslant \frac{n+m-1}{l-1}.$$

Отсюда и из соотношения (2) теоремы 1 следует неравенство

$$L_{B^*}(f) \geqslant \frac{n+m-1}{l-1},$$

из которого с учетом целочисленности $L_{B^*}(f)$ окончательно получаем

$$L_{B^*}(f) \geqslant \left\lceil \frac{n+m-1}{l-1} \right\rceil.$$

Теорема полностью доказана.

5. Самокорректирующиеся схемы

Затруднения, связанные с доказательством подходящих нижних оценок сложности схем, только возрастают при переходе к самокорректирующимся схемам [8, 9]. Предлагаемый здесь метод получения нижних оценок основан на замене заданного, быть может, достаточно сложного базиса на другой, существенно (в том или ином смысле) более простой базис.[1] Обязательным условием успешного применения этого метода является наличие (или возможность получения) достаточно хороших нижних оценок сложности схем в простых базисах.

Заметим, что некоторые идеи, касающиеся подходящей «модификации» изначально заданного базиса использовались еще в работах [2, 10] при доказательстве минимальности обычных (несамокорректирующихся) схем для индивидуальных булевых функций (в [2] исходный базис фактически дополнялся элементами с нулевыми весами, реализующими булевы константы, а в [10] базис дополнялся инвертором с относительно небольшим весом). Ниже суть предполагаемого метода излагается в рафинированном, достаточно общем виде, но вместе с тем и без излишних, на наш взгляд, усложнений и обобщений, которые можно сделать, и притом достаточно просто, по различным направлениям.

Будем рассматривать схемы в базисе B, содержащем надежные и ненадежные функциональные элементы. Всякий надежный элемент имеет неотрицательный вес и реализует некоторую приписанную ему функцию из B. Всякий ненадежный элемент также имеет неотрицательный вес и в исправном состоянии реализует некоторую приписанную ему функцию из B, а в неисправном состоянии — некоторую фиксированную для всех ненадежных элементов схемы булеву константу δ ($\delta \in \{0, 1\}$).

[1] Можно усмотреть, на наш взгляд, отдаленную аналогию этого метода с заменой переменной при интегрировании.

Схема в базисе B называется *k-самокорректирующейся относительно неисправностей типа δ* (на выходах элементов), если при переходе в неисправное состояние не более чем k любых ненадежных элементов она реализует ту же функцию, что и при исправном состоянии всех ее элементов (все неисправные элементы в схеме реализуют константу δ). Сумма весов всех элементов схемы считается *сложностью* этой схемы. *Сложность реализации* булевой функции — это наименьшая из сложностей схем (в заданном базисе и в заданном классе схем), реализующих эту функцию при исправном состоянии всех ее элементов. Сложность схемы S обозначим через $L^B(S)$, а сложность реализации функции f схемами в базисе B, k-самокорректирующимися относительно неисправностей типа δ, — через $L^B_{k,\delta}(f)$. Если сложность k-самокорректирующейся относительно неисправностей типа δ схемы в базисе B, реализующей функцию $f(x_1,\ldots,x_n)$, равна (или асимптотически — по n — равна) $L^B_{k,\delta}\big(f(x_1,\ldots,x_n)\big)$, то такая схема является *минимальной* (соответственно *асимптотически минимальной*).

Пусть имеются два произвольных конечных базиса: $A = \{\varphi_1,\ldots,\varphi_a\}$ и $B = \{\psi_1,\ldots,\psi_b\}$. Первому базису отвечают надежные элементы $D_1,\ldots,D_a$ с весами $P(D_1),\ldots,P(D_a)$, реализующие соответственно функции $\varphi_1,\ldots,\varphi_a$, и ненадежные элементы E_1, $\ldots$, E_a с весами $P(E_1)$, $\ldots$, $P(E_a)$, реализующие (в исправном состоянии) те же самые функции φ_1, $\ldots$, φ_a; веса элементов удовлетворяют неравенствам $P(D_i) \geqslant P(E_i) \geqslant 0$, $i = 1,\ldots,a$. Аналогичным образом, второму базису отвечают надежные элементы $F_1,\ldots,F_b$ с весами $P(F_1),\ldots,P(F_b)$, ненадежные элементы $G_1,\ldots,G_b$, обладающие весами $P(G_1),\ldots,P(G_b)$; как надежные, так и ненадежные элементы реализуют функции ψ_1, $\ldots$, ψ_b и веса элементов удовлетворяют неравенствам $P(F_i) \geqslant P(G_i) \geqslant 0$, $i = 1,\ldots,b$.

Базис A *согласован* с базисом B, если для каждого надежного элемента F_i базиса B существует подсхема (блок) F_i^* из надежных элементов базиса A и для каждого ненадежного элемента G_i существует подсхема G_i^* из элементов базиса A такие, что выполняются следующие условия согласования:

1. Подсхема F_i^* реализует функцию ψ_i и $L^A(F_i^*) \leqslant P(F_i)$.

2. Подсхема G_i^* реализует (при исправном состоянии всех ее ненадежных элементов) функцию ψ_i и $L^A(G_i^*) \leqslant P(G_i)$.

3. При наличии в подсхеме G_i^* не более чем k неисправных элементов значение на выходе этой подсхемы на любом входном наборе (значений переменных) $\tilde{\pi} = (\pi_1,\ldots,\pi_{r_i})$ равно либо $\psi_i(\tilde{\pi})$, либо δ $(i = 1,\ldots,b)$.

Заметим, что отношение согласованности базиса A с базисом B может и не быть симметричным.

Теорема 5. *Пусть базис B согласован с базисом B^*, а f — произвольная булева функция. Тогда*

$$L^{B^*}_{k,\delta}(f) \geqslant L^{B}_{k,\delta}(f).$$

Доказательство. Пусть f — произвольная булева функция, а S^* — минимальная k-самокорректирующаяся схема из функциональных элементов в базисе B^*, реализующая функцию f; для S^* по определению минимальной схемы выполняется соотношение

$$L^{B^*}(S^*) = L^{B^*}_{k,\delta}(f). \tag{9}$$

Зафиксируем какие-нибудь блоки $F^*_1, \ldots, F^*_b$ и $G^*_1, \ldots, G^*_b$, удовлетворяющие условиям согласованности базиса B с базисом B^*. Каждый надежный элемент F_i в схеме S^* заменим соответствующим ему блоком F^*_i. Входы очередного блока F^*_i соединяем с теми вершинами схемы S^*, с которыми были соединены соответствующие входы заменяемого элемента F_i; выход блока F^*_i соединяем с теми вершинами схемы, с которыми был соединен выход элемента F_i. Аналогичным образом и все ненадежные элементы G_i в схеме S^* заменим на соответствующие им блоки G^*_i $(i = 1, \ldots, b)$. В итоге получим некоторую схему S в базисе B, которая в исправном состоянии, очевидно, реализует заданную функцию f.

Пусть в схеме S оказываются неисправными какие-то k', $k' \leqslant k$, элементов, на входы этой схемы подается какой-то набор (значений переменных) $\tilde{\sigma}$, а выдает схема некоторое значение ε. Блоки, из которых построена схема S, взаимно не пересекаются и потому в рассматриваемом случае неисправные элементы могут оказаться не более чем в k' блоках, а неправильные значения могут оказаться на выходах каких-то h блоков $G^*_{i_1}, \ldots, G^*_{i_h}$, где $h \leqslant k'$; значение на выходе блока считаем неправильным, если оно отличается от того значения, которое было бы на выходе блока при исправном состоянии всех его элементов. Пусть G^* — какой-то блок с неправильным значением на выходе; из третьего условия согласованности базисов следует, что это неправильное значение на выходе блока G^* равно δ. Но в таком случае значение на выходе схемы S, очевидно, должно совпадать со значением на выходе схемы S^*, в которой неисправны элементы $G_{i_1}, \ldots, G_{i_h}$ (прообразы блоков $G^*_{i_1}, \ldots, G^*_{i_h}$). Схема S^* — k-самокорректирующаяся, $h \leqslant k' \leqslant k$ и потому на выходе этой схемы будет $f(\tilde{\sigma})$. Но если $\varepsilon = f(\tilde{\sigma})$, то это означает, что и схема S — k-самокорректирующаяся и для нее выполняется неравенство

$$L^{B}(S) \geqslant L^{B}_{k,\delta}(f). \tag{10}$$

Из первых двух условий согласованности базисов следует неравенство

$$L^{B}(S) \leqslant L^{B^*}(S^*),$$

из которого с учетом (9) и (10) окончательно получаем

$$L^{B^*}_{k,\delta}(f) \geqslant L^{B}_{k,\delta}(f).$$

Теорема доказана.

Приведем примеры эффективного использования теоремы 5 для получения новых нижних оценок сложности самокорректирующихся схем.

6. Оценки сложности k-самокорректирующихся схем для симметрических пороговых функций

В работе [11] получены асимптотически точные оценки сложности k-самокорректирующихся схем в базисах $B_0 = \{x\,\&\,y,\ x\vee y,\ \overline{x}\}$ и $B_1 = \{x\,\&\,y,\ x\vee y\}$ для монотонных симметрических пороговых функций, заданных соотношением $f^n_2(x_1,\ldots,x_n) = \bigvee\limits_{1\leqslant i<j\leqslant n} x_ix_j$, в случае однотипных константных неисправностей типа δ, $\delta\in\{0,\,1\}$, на выходах элементов. В этой работе предполагалось, что вес каждого надежного элемента базиса B_0 (а также и базиса B_1) равен p, а вес каждого ненадежного элемента равен 1, и были установлены следующие асимптотики.

Для схем в базисе B_0 при любом натуральном фиксированном k, любом фиксированном $\delta\in\{0,\,1\}$ и $p\geqslant k{+}1$ выполняется асимптотическое равенство

$$L^{B_0}_{k,\delta}(f^n_2) \sim (k{+}2)n. \tag{11}$$

Для схем в базисе B_1 при неисправностях типа 0 и $p>0$ получена асимптотика

$$L^{B_1}_{k,0}(f^n_2) \sim n\,\min\{2p, k{+}2\}. \tag{12}$$

Используя теорему 5 и оценки (11) и (12), получим асимптотически точные оценки сложности реализации функции f^n_2 k-самокорректирующимися схемами в базисах, содержащих l-входовые ($l\geqslant 3$) конъюнкторы и дизъюнкторы.

Пусть $B^* = \{x_1\,\&\,\ldots\,\&\,x_l,\ x_1\vee\cdots\vee x_l,\ \overline{x}\}$, вес каждого надежного элемента базиса B^* равен p, $p\geqslant k{+}1$, а вес каждого ненадежного элемента равен 1. В качестве неисправностей возьмем для определенности однотипные константные неисправности типа 0 на выходах элементов (случай неисправностей типа 1 рассматривается аналогично, но только с учетом леммы 4 из [11]).

Теорема 6. *Для базиса B^* и последовательности булевых функций f^n_2, $n=2,3,\ldots,$ выполняется равенство*

$$L^{B^*}_{k,0}(f^n_2) \sim \frac{(k+2)n}{l-1}.$$

Доказательство. Верхняя оценка для $L^{B^*}_{k,0}(f^n_2)$ получается конструктивно, почти так же, как и верхняя оценка в [11]. Единственное существенное отличие, влияющее на асимптотическую оценку, будет заключаться в том, что при построении подсхем $S_{i,1}$ (см. [11], с. 67) будут использоваться цепочки не из двухвходовых, а из l-входовых ненадежных дизъюнкторов, вследствие чего главным членом в итоговой мажоранте для сложности схемы S^* окажется не величина $(k{+}2)n$, а $\frac{(k+2)n}{l-1}$ и искомая верхняя оценка приобретет нужный вид.

Для доказательства нижней оценки возьмем базис $B = \{x \,\&\, y,\ x \vee y,\ \overline{x}\}$. Положим вес каждого надежного элемента базиса B равным $\frac{p}{l-1}$, а вес каждого ненадежного элемента равным $\frac{1}{l-1}$. Согласованность базиса B с базисом B^* становится очевидной, если в качестве соответствующих блоков в базисе B, отвечающих элементам базиса B^*, взять цепочку из $l{-}1$ двухвходовых конъюнкторов (базиса B) для l-входового конъюнктора (базиса B^*) и цепочку из $l{-}1$ двухвходовых дизъюнкторов для l-входового дизъюнктора (заметим, что третье условие согласованности для блока, реализующего дизъюнкцию переменных $x_1 \vee \cdots \vee x_l$, выполняется в силу монотонности дизъюнкции и булевых констант).

Для базиса B нижняя оценка

$$L^{B}_{k,0}(f^n_2) \gtrsim \frac{(k+2)n}{l-1} \tag{13}$$

доказывается точно так же, как и нижняя оценка для $L^{B_0}_{k,0}(f^n_2)$ в [11] (можно получить оценку (13) и опираясь на соотношение (11)). Из теоремы 5 и соотношения (13) получаем искомую нижнюю оценку

$$L^{B^*}_{k,0}(f^n_2) \gtrsim \frac{(k+2)n}{l-1}.$$

Теорема доказана.

Возьмем теперь монотонный базис $B^*_1 = \{x_1 \,\&\, \ldots \,\&\, x_l,\ x_1 \vee \cdots \vee x_l\}$ и положим вес каждого надежного элемента равным p, $p \geqslant 1$, а вес каждого ненадежного элемента равным 1. В качестве неисправностей здесь будем предполагать только однотипные константные неисправности типа 0 на выходах элементов.

Теорема 7. *Для базиса B^*_1 и последовательности булевых функций f^n_2, $n = 1, 2, \ldots$, выполняется соотношение*

$$L^{B^*_1}_{k,0}(f^n_2) \sim \frac{n \min\{2p,\, k{+}2\}}{l-1}.$$

Доказательство. Верхнюю оценку получим конструктивно. Если выполнено неравенство $k{+}2 \geqslant 2p$, то схему для f_2^n построим из надежных l-входовых конъюнкторов и дизъюнкторов точно так же, как это делалось в [3] при получении верхней оценки сложности реализации функции f_2^n обычными схемами (см. [3], с. 42); можно взять и схему из доказательства верхней оценки в предыдущей теореме, полагая только в данном случае $k = 0$ — ведь схему из одних только надежных элементов формально можно считать k-самокорректирующейся. Сложность построенной схемы окажется асимптотически не больше $\frac{2pn}{l-1}$. Если $2p > k{+}2$, то можно просто воспользоваться верхней оценкой, полученной при доказательстве теоремы 6; обратим внимание на то, что эта оценка была получена с использованием k-самокорректирующихся схем, содержащих только конъюнкторы и дизъюнкторы.

Нижнюю оценку получим с использованием теоремы 5. Для этого возьмем базис $B_1 = \{x \,\&\, y,\ x \vee y\}$ и у этого базиса положим веса надежных элементов равными $\frac{p}{l-1}$, а веса ненадежных элементов равными $\frac{1}{l-1}$. Базис B_1 отличается от базиса B из предыдущего примера лишь отсутствием в нем инверсии; условия согласованности базиса B_1 с базисом B_1^* выполняются. Кроме того, рассматриваемый здесь базис B_1 отличается от одноименного базиса B_1 из [11] лишь уменьшенными в $l{-}1$ раз весами всех элементов; из этого факта и теоремы 2 из [11] получаем неравенство

$$L_{k,0}^{B_1}(f_2^n) \gtrsim \frac{n \min\{2p,\ k{+}2\}}{l-1} \tag{14}$$

(это неравенство можно вывести и непосредственно, фактически повторяя рассуждения при доказательстве нижней оценки теоремы 2 из [11]). Остается воспользоваться теоремой 5, позволяющей и для рассматриваемого базиса B_1^* с использованием (14) моментально получить требуемую нижнюю оценку. Теорема доказана.

Замечание. Основная теорема 5 и особенно представленные примеры ее использования в чем-то достаточно конкретизированы. Вместе с тем (и об этом уже говорилось ранее) возможны изменения как в исходном утверждении, т. е. в основной теореме, так и в постановках конкретных задач, решаемых с использованием этой теоремы. Например, надежная и ненадежная части одного и того же базиса могут не совпадать (в этом случае множество функций, реализуемых надежными элементами, не совпадает с множеством функций, реализуемых ненадежными элементами); в отличие от приведенных примеров в каких-то случаях веса у разных элементов одного и того же базиса (как у надежных, так и ненадежных) могут различаться; в схемах могут возникать другие неисправности, скажем, константные неисправности произвольного типа [9] на выходах элементов, неисправности на входах элементов,

инверсные неисправности. Нетрудно заметить, что и в этих случаях можно воспользоваться основной теоремой 5 или подходящей ее модификацией.

Литература

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

2. Редькин Н. П. Доказательство минимальности некоторых схем из функциональных элементов // Проблемы кибернетики. — 1970. — Вып. 23. — С. 83–101.

3. Гринчук М. И. О монотонной сложности пороговых функций // Методы дискретного анализа в теории графов и сложности. — Вып. 52. — Новосибирск, 1992. —С. 41–48.

4. Фиников Б. И. Об одном семействе классов функций алгебры логики и их реализации в класса П-схем // Доклады АН СССР. — 1957. — Т. 115, № 2. — С. 247–248.

5. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. — 1965. — Вып. 14. — С. 31–110.

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

7. Редькин Н. П. Дискретная математика. — М.: Физматлит, 2009.

8. Яблонский С. В. Элементы математической кибернетики. — М.: Высшая школа, 2007.

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

10. Редькин Н. П. О минимальной реализации линейной функции схемой из функциональных элементов // Кибернетика. — 1971. — № 6. — С. 31–38.

11. Редькин Н. П. Асимптотически минимальные самокорректирующиеся схемы для одной последовательности булевых функций // Дискретный анализ и исследования операций. — 1996. — Т. 3, № 2. — С. 62–79.

СОДЕРЖАНИЕ