УДК 519.714

О СХЕМАХ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ С ДВУМЯ ЯРУСАМИ ВЕТВЛЕНИЯ

Д. Ю. Черухин

Рассмотрен класс схем, промежуточный между СФЭ и формулами, а именно, состоящий из схем, в которых ветвлением обладают только некоторые, попарно несравнимые элементы. В данном классе получен порядок роста функции Шеннона и предложены методы доказательства нижних оценок сложности операторов. В частности, получена почти квадратичная эффективная нижняя оценка.

1. Введение

В работе изучается некоторый подкласс схем из функциональных элементов (СФЭ) [1]. Предполагается, что используемая система элементарных функций (базис) является конечной и полной в множестве всех булевых функций. Скажем, что выход функционального элемента (или вход схемы) обладает *ветвлением*, если сигнал с данного выхода (или входа) подаётся либо не менее чем на два входа других элементов (возможно, на входы одного и того же элемента), либо хотя бы на один вход другого элемента и хотя бы на один выход схемы, либо не менее чем на два выхода схемы.

Формулы можно определить как СФЭ, в которых только входы могут обладать ветвлением. Таким образом, формулы можно назвать схемами с одним ярусом ветвления. Определим более широкий класс схем — СФЭ с двумя ярусами ветвления (аналогично можно определить СФЭ с k ярусами ветвления, $k \geqslant 3$). Скажем, что элемент E_1 предшествует элементу E_2, если в схеме существует ориентированный путь, ведущий от E_1 к E_2. СФЭ называется схемой с 2-*мя ярусами ветвления*, если любые два различных элемента, обладающих ветвлением, несравнимы, т. е. ни один из них не предшествует другому; при этом входы не считаются элементами, они также могут обладать ветвлением.

В связи с данным определением возникает естественный вопрос: какова "сила" введённого класса с точки зрения сложности; похож ли он больше на СФЭ или на формулы? Ответ на этот вопрос неоднозначен. С одной стороны, по порядку роста функции Шеннона класс СФЭ с 2-мя ярусами ветвления больше похож на класс СФЭ (см. теорему 1). С другой стороны, при реализации конкретных функций рассматриваемый класс более напоминает класс формул.

Например, если базис является обобщенно-мототонным (о.-м.), т. е. каждая его функция возрастает или убывает по каждой своей переменной, то на схемы с ограниченным числом ярусов ветвления можно распространить метод Субботовской [3] (в его вероятностном варианте) и получить степенные нижние оценки сложности линейной функции $x_1 \oplus \ldots \oplus x_n$. В частности, сложность линейной функции в классе двухярусных схем в базисе $\{\&, \vee, \neg\}$ допускает оценку $n^{4/3-o(1)}$. Следствием этого является различие базисов с точки зрения сложности, имеющее место для формул [4] и не имеющее места в случае СФЭ.

В случае двухярусных схем в не о.-м. базисе ни одной эффективной нелинейной нижней оценки сложности функций неизвестно. Для этого случая известны нижние оценки сложности (n, n)-операторов. Один из методов их доказательства основан на теоретико-графовой технике (см., например, [6]). Суть метода такова. Пусть любая схема для данного оператора содержит граф специального вида, например, суперконцентратор [7, 8] или определённый его подграф. Известно, что число рёбер в (n, n)-суперконцентраторе глубины 2 нелинейно по n [7]. Следовательно, сложность данного оператора нелинейна. Описанным методом можно получать оценки, не превосходящие $n \log_2^{2-o(1)} n$ [7].

В данной работе предложены два других метода оценки сложности операторов. Первый из них сводит задачу получения нижних оценок к задаче оценки информационных характеристик некоторой функциональной таблицы. В редуцированной задаче отсутствует графовая структура, что делает её более обозримой. Первым методом доказана невысокая нижняя оценка сложности оператора сдвига (теорема 2). Более высокая оценка сложности оператора сдвига получена теоретико-графовым методом в [6]. Видоизменив оператор и упростив (и вместе с тем сузив) наш метод, можно получить оценку сложности вида $\Omega(n^{3/2})$ [5]. Отметим, что этот метод может быть легко перенесён на более сильный класс схем глубины 2 в базисе из всех булевых функций.

Второй метод (теорема 3) возник из дальнейшего анализа узкого варианта первого метода и в окончательном виде приобрёл черты обобщения метода Нечипорука для формул [2], что ещё раз подчёркивает близость двухярусных схем к формулам. Во втором методе используется специфика двухярусных схем. Существенно то, на первом ярусе вычисляются формулы в конечном базисе, а не произвольные булевы функции. Данный метод позволяет получить нижнюю оценку вида $n^{2-o(1)}$.

Интерес к классу двухярусных схем возник в связи с проблемой получения нелинейных нижних оценок сложности СФЭ [3]. Один из возможных подходов к данной проблеме был предложен Вэльянтом. Подход основан на теореме 5.1 из [8]; он состоит в совместном оценивании сложности и глубины схемы, при этом СФЭ произвольной структуры редуцируется к СФЭ с двумя ярусами ветвления, иссследование которой является проблемной частью подхода (в процессе редукции возможно существенное увеличение сложности).

2. Оценка функции Шеннона

Пусть B — базис, т. е. конечная полная система булевых функций, K — класс схем (один из: "Ф" — формулы, "C" — СФЭ, "C_2" — СФЭ с 2-мя ярусами ветвления). Обозначим через $L(S)$ сложность схемы S, т. е. число её элементов; через $L_B^K(f)$ — сложность функции (или оператора) f при реализации схемами класса K над базисом B. Положим $L_B^K(n) = \max L_B^K(f)$, где максимум берётся по всем функциям $f(x_1, \dots, x_n)$. Известно [1], что

$$L_B^{\Phi}(n) \asymp \frac{2^n}{\log_2 n}, \qquad L_B^C(n) \asymp \frac{2^n}{n}.$$

Теорема 1. *В любом базисе B*

$$L_B^{C_2}(n) \asymp \frac{2^n}{n}.$$

Доказательство. Нижняя оценка следует из очевидного неравенства $L_B^C(n) \leqslant L_B^{C_2}(n)$. Верхняя извлекается из метода Шеннона (см. [1]). Заметим, что верхнюю оценку достаточно доказать для базиса $B_0 = \{\&, \vee, \neg\}$. Действительно, функции из базиса B_0 бесповторно выражаются в любом базисе [3], поэтому при переходе от базиса B_0 к произвольному базису B сложность схемы увеличится не более чем в константу раз (при замене элемента его бесповторным выражением через другие элементы новых ветвлений не возникает).

Пусть k — параметр, $m = \lfloor \frac{n-k}{2} \rfloor$. Для произвольной функции $f(x_1, \dots, x_n)$ справедливо представление

$$f(x_1, \dots, x_n) = \bigvee_{\sigma_1, \dots, \sigma_{n-k}} x_1^{\sigma_1} \cdot \ldots \cdot x_m^{\sigma_m} \,\&\, x_{m+1}^{\sigma_{m+1}} \cdot \ldots \cdot x_{n-k}^{\sigma_{n-k}} \,\&$$

$$\& \, f(\sigma_1, \dots, \sigma_{n-k}, x_{n-k+1}, \dots, x_n). \quad (1)$$

Функции $x_1^{\sigma_1} \cdot \ldots \cdot x_m^{\sigma_m}$, $x_{m+1}^{\sigma_{m+1}} \cdot \ldots \cdot x_{n-k}^{\sigma_{n-k}}$, $f(\sigma_1, \dots, \sigma_{n-k}, x_{n-k+1}, \dots, x_n)$ назовём функциями *второго яруса*. Каждую из них реализуем формулой. Элементы, на выходах которых реализованы функции второго яруса, составляют второй ярус ветвления нашей схемы. Функция f вычисляется (в соответствии с представлением (1)) как формула, переменными в которой являются функции второго яруса.

Для вычисления всех функций вида $x_1^{\sigma_1}\cdot\ldots\cdot x_m^{\sigma_m}$ достаточно $2^m(2m-1)$ элементов; для функций $x_{m+1}^{\sigma_{m+1}}\cdot\ldots\cdot x_{n-k}^{\sigma_{n-k}}$ требуется $2^{m+1}(2m+1)$ элементов; всевозможные функции от переменных $x_{n-k+1},\ldots,x_n$ можно вычислить со сложностью $2^{2^k}\cdot\mathcal{O}\bigl(\frac{2^k}{\log_2 k}\bigr)$. Наконец, для вычисления функции f, если уже вычислены функции второго яруса, достаточно $3\cdot 2^{n-k}$ элементов.

Положим $k=\lfloor\log_2(n-2\log_2 n)\rfloor$. Тогда сложность всей схемы не превосходит

$$2\cdot 2^{m+1}(2m+1)+2^{2^k}\cdot\mathcal{O}\Bigl(\frac{2^k}{\log_2 k}\Bigr)+3\cdot 2^{n-k}=$$
$$=\mathcal{O}\Bigl(2^{n/2}\cdot n\Bigr)+\mathcal{O}\Bigl(\frac{2^n}{n^2}\cdot\frac{n}{\log_2\log_2 n}\Bigr)+\mathcal{O}\Bigl(\frac{2^n}{n}\Bigr)=\mathcal{O}\Bigl(\frac{2^n}{n}\Bigr).$$

Теорема 1 доказана.

3. Вспомогательные утверждения

Теореме 2 предпошлём ряд вспомогательных понятий и утверждений.

Пусть $\tilde y_1,\ldots,\tilde y_n$, $\tilde z_1,\ldots,\tilde z_n$ — наборы переменных (возможно, содержащие одинаковые переменные), $Y=(\tilde y_1,\ldots,\tilde y_n)$, $Z=(\tilde z_1,\ldots,\tilde z_n)$, $F=(f_{i,j})$ — матрица размера $n\times n$, состоящая из булевых функций, причём для любых i,j, $1\leqslant i\leqslant n$, $1\leqslant j\leqslant n$, функция $f_{i,j}$ зависит только от переменных из наборов $\tilde y_i$ и $\tilde z_j$. Тогда набор $\mathcal{F}=(Y,Z,F)$ назовём *локальной функциональной таблицей размера* n (сокращённо — n-*таблицей*).

Пусть $M=(m_{i,j})$ — матрица из нулей и единиц размера $n\times n$. Матрицу M назовём *псевдодиагональной*, если не существует двух единиц, стоящих в одной строке или одном столбце матрицы M. Множество матриц $R=\{M_1,\ldots,M_k\}$ размера $n\times n$, состоящих из нулей и единиц, назовём *диагональным разбиением размера* n *и мощности* k (сокращённо — (n,k)-*разбиением*), если каждая матрица $M_t\in R$ $(1\leqslant t\leqslant k)$ псевдодиагональна и для любых i,j существует единственная матрица $M_{t(i,j)}\in R$ такая, что на пересечении её i-й строки и j-го столбца стоит единица.

Скажем, что n-таблица $\mathcal{F}$ *вычисляет* матрицу M размера $n\times n$, если существуют такие наборы значений $\tilde\alpha_1,\ldots,\tilde\alpha_n$, $\tilde\beta_1,\ldots,\tilde\beta_n$ переменных из наборов, соответственно, $\tilde y_1,\ldots,\tilde y_n$, $\tilde z_1,\ldots,\tilde z_n$, что $\forall i,j$ $f_{i,j}(\tilde\alpha_i,\tilde\beta_j)=m_{i,j}$. Скажем, что таблица $\mathcal{F}$ *распознаёт* (n,k)-разбиение R, если $\mathcal{F}$ вычисляет каждую матрицу, входящую в R.

Обозначим через $c(n,k)$ минимальное число c, для которого существует n-таблица $\mathcal{F}$, такая, что число переменных в каждом из наборов $\tilde{y}_1, \dots, \tilde{y}_n, \tilde{z}_1, \dots, \tilde{z}_n$ не превосходит c и $\mathcal{F}$ распознаёт некоторое (n,k)-разбиение. Нашей ближайшей целью является доказательство утверждения $c(n,n) \to \infty$, $n \to \infty$. По-видимому, полученную нами нижнюю оценку для $c(n,n)$ можно существенно улучшить, что приведёт к улучшению итоговой нижней оценки сложности булевого оператора.

Скажем, что n-таблица $\mathcal{F}$ является *равномерной* и имеет *мощность* c, если в каждом из наборов $\tilde{y}_1, \dots, \tilde{y}_n, \tilde{z}_1, \dots, \tilde{z}_n$ содержится ровно c переменных. Пару наборов констант $(\tilde{\alpha}, \tilde{\beta})$ (каждый из которых имеет длину c) назовём *нулевой парой* таблицы $\mathcal{F}$, если $\forall i, j\ f_{i,j}(\tilde{\alpha}, \tilde{\beta}) = 0$.

Подтаблицей таблицы $\mathcal{F}$ называется таблица, полученная из $\mathcal{F}$ удалением некоторых строк и столбцов и перестановкой оставшихся (операции удаления и перестановки производятся синхронно в матрице F и наборах Y, Z, связанных, соответственно, со строками и столбцами матрицы F). Единичной называется матрица, в которой на главной диагонали стоят единицы, а в остальных позициях — нули; единичная матрица размера $n \times n$ обозначается E_n. Определим функцию $\theta(x)$:

$$\theta(x) = \begin{cases} x, & x \geqslant 1; \\ 0, & x < 1. \end{cases}$$

Утверждение 1. *Пусть равномерная n-таблица $\mathcal{F}$ мощности c вычисляет матрицу E_n и имеет N нулевых пар. Тогда найдётся n'-таблица $\mathcal{F}'$, являющаяся подтаблицей таблицы $\mathcal{F}$ и имеющая $(N+1)$ нулевых пар, причём*

$$n' \geqslant \theta\Big(\frac{n}{3(4^c - N)}\Big).$$

Доказательство. Существует ровно 4^c пар наборов констант $(\tilde{\alpha}, \tilde{\beta})$, в которых $\tilde{\alpha}$ и $\tilde{\beta}$ имеют длину c; из них N пар являются нулевыми для таблицы $\mathcal{F}$. Для любого i $(1 \leqslant i \leqslant n)$ существует пара наборов $(\tilde{\alpha}_i, \tilde{\beta}_i)$ такая, что $f_{i,i}(\tilde{\alpha}_i, \tilde{\beta}_i) = 1$. Ни одна из пар $(\tilde{\alpha}_i, \tilde{\beta}_i)$, $1 \leqslant i \leqslant n$, не является нулевой для таблицы $\mathcal{F}$. Пусть $(\tilde{\alpha}', \tilde{\beta}')$ — та пара, которая повторяется среди пар $(\tilde{\alpha}_i, \tilde{\beta}_i)$, $1 \leqslant i \leqslant n$, наибольшее число раз. Обозначим через I множество тех индексов i, для которых $(\tilde{\alpha}', \tilde{\beta}') = (\tilde{\alpha}_i, \tilde{\beta}_i)$. Тогда

$$|I| \geqslant \frac{n}{4^c - N}. \tag{2}$$

Выделим из таблицы $\mathcal{F}$ подтаблицу $\mathcal{F}^*$, содержащую те и только те строки и столбцы, номера которых входят в множество I. Заметим, что таблица $\mathcal{F}^*$

вычисляет матрицу $E_{|I|}$, при этом наборы переменных $\tilde{y}_1, \dots, \tilde{y}_n$ принимают один и тот же набор значений — $\tilde{\alpha}'$; аналогично, наборы $\tilde{z}_1, \dots, \tilde{z}_n$ принимают набор значений $\tilde{\beta}'$. В матрице $E_{|I|}$ выделим максимальную квадратную подматрицу M', состоящую только из нулей; размер матрицы M' не меньше, чем $\lfloor |I|/2 \rfloor$. Искомую таблицу $\mathcal{F}'$ образуем из тех строк и столбцов таблицы $\mathcal{F}^*$, которые соответствуют строкам и столбцам подматрицы M' матрицы $E_{|I|}$.

Заметим, что все нулевые пары таблицы $\mathcal{F}$ являются нулевыми для таблицы $\mathcal{F}'$. Кроме того, пара $(\tilde{\alpha}', \tilde{\beta}')$ является нулевой для $\mathcal{F}'$, но не является нулевой для $\mathcal{F}$. Таким образом, число нулевых пар таблицы $\mathcal{F}'$ не меньше $N + 1$. Вместе с тем (используя (2) и неравенство $\lfloor x/2 \rfloor \geqslant \theta(x/3)$, справедливое для целых $x \geqslant 0$),

$$n' \geqslant \left\lfloor \frac{|I|}{2} \right\rfloor \geqslant \theta\Big(\frac{|I|}{3}\Big) \geqslant \theta\Big(\frac{n}{3(4^c - N)}\Big).$$

Утверждение 1 доказано.

Утверждение 2. *Пусть равномерная n-таблица $\mathcal{F}$ мощности c распознаёт (n,k)-разбиение R. Тогда существуют n'-таблица $\mathcal{F}'$, являющаяся подтаблицей таблицы $\mathcal{F}$, и (n',k)-разбиение R', распознаваемое таблицей $\mathcal{F}'$, такие, что R' содержит матрицу $E_{n'}$ и*

$$n' \geqslant \frac{n^2}{k}.$$

Доказательство. Действительно, матрицы, входящие в разбиение R, содержат в сумме n^2 единиц, следовательно, найдётся матрица $M \in R$, содержащая не менее n^2/k единиц. Из матрицы M можно получить единичную матрицу с помощью удаления нулевых строк и столбцов и перестановки оставшихся. Проделав те же операции удаления и перестановки с таблицей $\mathcal{F}$ и всеми матрицами разбиения R, получим требуемые $\mathcal{F}'$ и R'. Утверждение 2 доказано.

Утверждение 3. *Пусть равномерная n-таблица $\mathcal{F}$ мощности c распознаёт (n,k)-разбиение R и пусть $N \leqslant 4^c$. Тогда существуют n_N-таблица $\mathcal{F}_N$, являющаяся подтаблицей таблицы $\mathcal{F}$, и (n_N,k)-разбиение R_N, распознаваемое таблицей $\mathcal{F}_N$, такие, что $\mathcal{F}_N$ содержит N нулевых пар и*

$$n_N \geqslant \theta\Big(\frac{n^{2^N}}{(3k \cdot 4^c)^{2^N - 1}}\Big). \tag{3}$$

Доказательство. Проведём индукцию по N.

Базис индукции: $N = 0$. Неравенство (3) имеет вид $n_N \geqslant n$, т. е. достаточно положить $\mathcal{F}_N = \mathcal{F}$, $R_N = R$.

Индуктивный переход: $N \to N+1$. Пусть $\mathcal{F}_N$ и R_N уже построены. В силу утв. 2 существуют подтаблица $\mathcal{F}'_N$ таблицы $\mathcal{F}_N$ и (n'_N, k)-разбиение R_N, распознаваемое таблицей $\mathcal{F}_N$, такие, что

$$n'_N \geqslant \frac{n_N^2}{k}. \tag{4}$$

Кроме того, $\mathcal{F}'_N$ вычисляет матрицу $E_{n'_N}$, содержащуюся в R'_N. Поэтому, в силу утв. 1 существует подтаблица таблицы $\mathcal{F}'_N$, содержащая не менее $(N+1)$ нулевых пар. Обозначим её через $\mathcal{F}_{N+1}$, определив n_{N+1} и R_{N+1} соответствующим образом. Имеем

$$n_{N+1} \geqslant \theta\Big(\frac{n'_N}{3(4^c - N)}\Big) \geqslant \theta\Big(\frac{n'_N}{3 \cdot 4^c}\Big). \tag{5}$$

Объединив выкладки (3)–(5) с учётом соотношений $\theta(x)^2 = \theta(x^2)$, $\theta(x)/y \geqslant \theta(x/y)$ и $\theta(\theta(x)) = x$, справедливых при $x \geqslant 0$, $y \geqslant 1$, получим

$$n_{N+1} \geqslant \theta\Big(\frac{n'_N}{3 \cdot 4^c}\Big) \geqslant \theta\Big(\frac{n_N^2}{3k \cdot 4^c}\Big) \geqslant$$
$$\geqslant \theta\bigg(\frac{1}{3k \cdot 4^c} \cdot \theta\Big(\frac{n^{2^N}}{(3k \cdot 4^c)^{2^N - 1}}\Big)^2\bigg) \geqslant \theta\bigg(\frac{n^{2^{N+1}}}{(3k \cdot 4^c)^{2^{N+1}-1}}\bigg).$$

Утверждение 3 доказано.

Лемма 1.

$$c(n, n) = \Omega(\log_2 \log_2 \log_2 n), \qquad n \to \infty.$$

Доказательство. Пусть $c = c(n, n)$. Рассмотрим n-таблицу $\mathcal{F}$ и распознаваемое ею (n, n)-разбиение R, такие, что для любого i длина любого из наборов $\tilde{y}_i, \tilde{z}_i$ не превосходит c. Дополним некоторые из наборов $\tilde{y}_1, \ldots, \tilde{y}_n, \tilde{z}_1, \ldots, \tilde{z}_n$ фиктивными переменными так, чтобы таблица $\mathcal{F}$ стала равномерной таблицей мощности c.

Положим $N = 4^c$. Согласно утв. 3 существует подтаблица $\mathcal{F}_N$ и разбиение R_N, для которых выполнено (3) при $n = k$. Тогда

$$n_N \geqslant \theta\Big(\frac{n}{(3N)^{2^N - 1}}\Big). \tag{6}$$

Если аргумент функции θ в (6) не меньше единицы, то $n_N \geqslant 1$. В этом случае мы получаем противоречие: с одной стороны любая пара наборов $(\tilde{\alpha}, \tilde{\beta})$ является нулевой для $\mathcal{F}_N$ (так как $N = 4^c$), а с другой стороны в разбиении R_N существует матрица, вычислимая таблицей $\mathcal{F}_N$ и содержащая хотя бы одну единицу.

Таким образом,

$$n < (3N)^{2^N - 1} \leqslant 2^{2^N \log_2(3N)} = 2^{2^{N + \log_2 \log_2(3N)}}.$$

Следовательно,

$$N \sim N + \log_2 \log_2(3N) \geqslant \log_2 \log_2 n.$$

В свою очередь, $c = \frac{1}{2}\log_2 N$. Окончательно имеем

$$c(n,n) = c = \Omega(\log_2 \log_2 \log_2 n).$$

Лемма 1 доказана.

Обозначим через $c'(n,k)$ минимальное число c, для которого существует n-таблица $\mathcal{F}$ такая, что $\mathcal{F}$ распознаёт некоторое (n,k)-разбиение и

$$\sum_{i=1}^{n} (|\tilde{y}_i| + |\tilde{z}_i|) \leqslant cn, \tag{7}$$

где $|\tilde{y}|$ обозначает число переменных в наборе $\tilde{y}$.

Утверждение 4. *Для любых n, k*

$$c'(n,k) \geqslant \frac{1}{2} c\Big(\frac{n}{2}, k\Big).$$

Доказательство. Пусть $c = c'(n,k)$. Рассмотрим n-таблицу $\mathcal{F}$ (распознающую некоторое (n,k)-разбиение), для которой выполнено (7). В силу (7) среди наборов $\tilde{y}_1, \ldots, \tilde{y}_n, \tilde{z}_1, \ldots, \tilde{z}_n$ существует не более $n/2$ наборов, в каждом из которых содержится больше, чем $2c$ переменных. Следовательно, из наборов $\tilde{y}_1, \ldots, \tilde{y}_n$ можно выбрать $n/2$ наборов, содержащих не более, чем $2c$ переменных; аналогичное верно и для наборов $\tilde{z}_1, \ldots, \tilde{z}_n$.

Из строк и столбцов таблицы $\mathcal{F}$, соответствующих выбранным наборам, образуем $n/2$-таблицу $\mathcal{F}'$. Она распознаёт, очевидно, некоторое $(n/2, k)$-разбиение и число переменных в каждом из наборов вида $\tilde{y}_i, \tilde{z}_i$ таблицы $\mathcal{F}'$ не превосходит $2c$. По определению числа $c(n,k)$ имеем

$$2c'(n,k) = 2c \geqslant c\Big(\frac{n}{2}, k\Big).$$

Утверждение 4 доказано.

4. Оценка сложности оператора сдвига

Теперь перейдём к получению нижней оценки сложности.

Для фиксированного числа n определим функцию $r(i,t)$ (где i,t — целые, $1 \leqslant i \leqslant n$, $0 \leqslant t \leqslant n-1$), положив $r(i,t)$ равным такому числу j из отрезка $[1,\dots,n]$, что $j \equiv i+t \pmod{n}$. Оператором *сдвига* (точнее, оператором *циклического сдвига влево*, сокращённо — RCL) назовём оператор

$$\mathrm{RCL}_n : (x_1,\dots,x_n,\ y_1,\dots,y_m) \mapsto (z_1,\dots,z_n)$$

такой, что $m = \lceil \log_2 n \rceil$ и

$$\forall j \quad z_j = x_{r(j,t)}, \quad \text{где } t = \sum_{s=1}^{m} y_s 2^{m-s}.$$

Лемма 2. *В любом базисе B*

$$L_B^{C_2}(\mathrm{RCL}_n) = \Omega(nc'(n,n)), \qquad n \to \infty.$$

Доказательство. Докажем лемму в случае базиса B, состоящего из всех двуместных булевых функций; для произвольного B лемма доказывается аналогично. Рассмотрим СФЭ с двумя ярусами ветвления, реализующую оператор RCL_n и имеющую минимальную сложность. Добавив в неё лишние элементы и увеличив сложность не более, чем в константу раз, можно получить схему S следующего (*строго двухярусного*) вида: существуют элементы $E_1,\dots,E_p$ (элементы *второго яруса*) такие, что

а) любой элемент, обладающий ветвлением, входит в их число;

б) выход ни одного из элементов $E_1,\dots,E_p$ не является выходом схемы;

в) любой ориентированный путь, ведущий от входа к выходу схемы, содержит хотя бы один (и, очевидно, только один) из элементов $E_1,\dots,E_p$.

Введём некоторые обозначения. Обозначим через $F_1,\dots,F_n$ элементы, выходы которых являются, соответственно, выходами $z_1,\dots,z_n$ схемы S. Далее, пусть Γ_l $(1 \leqslant l \leqslant p)$ — подсхема схемы S, состоящая из всех элементов, предшествующих E_l (включая E_l); g_l — функция от переменных $x_1,\dots,x_n,y_1,\dots,y_m$, вычисляемая на выходе элемента E_l; G_l — множество индексов i таких, что при вычислении функции g_l схемой Γ_l используется переменная x_i.

Аналогично, пусть X_j $(1 \leqslant j \leqslant n)$ — подсхема схемы S, состоящая из всех элементов, предшествующих F_j, но не предшествующих ни одному из элементов второго яруса (входами схемы X_j являются выходы некоторых элементов второго яруса); h_j — функция от переменных $x_1,\dots,x_n,y_1,\dots,y_m$, вычисляемая на выходе элемента F_j; H_j — множество индексов l таких, что при вычислении функции h_l схемой X_j используется выход элемента E_l.

По построению схемы S подсхемы $\Gamma_1,\dots,\Gamma_p,X_1,\dots,X_n$ не пересекаются и в объединении дают всю схему S. Заметим, что если в некоторой схеме S' используется k входов, то $L(S')\geqslant k-1$ (в случае произвольного базиса B это неравенство выполнено с точностью до умножения на константу); если при этом $L(S')\geqslant 1$, то $L(S')\geqslant k/2$. Каждая из схем $\Gamma_1,\dots,\Gamma_p,X_1,\dots,X_n$ содержит хотя бы один элемент, поэтому

$$L(S)=\sum_{l=1}^{p}L(\Gamma_l)+\sum_{j=1}^{n}L(X_j)\geqslant\frac{1}{2}\Big(\sum_{l=1}^{p}|G_l|+\sum_{j=1}^{n}|H_j|\Big). \tag{8}$$

Обозначим через G'_i $(1\leqslant i\leqslant n)$ множество индексов l таких, что переменная x_i используется при вычислении функции g_l схемой Γ_l. Тогда

$$\sum_{i=1}^{n}|G'_i|=\sum_{l=1}^{p}|G_l|. \tag{9}$$

Для обоснования (9) можно использовать матрицу $M'=(m'_{i,l})$ размера $n\times p$, состоящую из нулей и единиц, в которой $m'_{i,l}=1$ тогда и только тогда, когда переменная x_i используется при вычислении функции g_l схемой Γ_l. Правая и левая части равенства (9) содержат подсчитанное разными способами (по строкам и по столбцам) число единиц в матрице M'.

Далее, построим n-таблицу $\mathcal{F}$. Каждой функции f, зависящей только от переменных $y_1,\dots,y_m$, сопоставим новую переменную u_f. Наборы $\tilde y_1,\dots,\tilde y_n$, $\tilde z_1,\dots,\tilde z_n$ таблицы $\mathcal{F}$ образуем из переменных вида u_f. Каждой паре (i,j), $1\leqslant i,j\leqslant n$, сопоставим одну из переменных вида u_f, которую обозначим через $u_{i,j}$. Булеву функцию $f_{i,j}$ определим как функцию, для которой выполнено тождество

$$u_{i,j}\equiv f_{i,j}(\tilde y_i,\tilde z_j), \tag{10}$$

в котором переменные вида u_f заменены на соответствующие им функции от переменных $y_1,\dots,y_m$. При этом мы покажем, что функция, соответствующая переменной $u_{i,j}$, вычислима через функции, соответствующие переменным из наборов $\tilde y_i,\tilde z_j$ (здесь и далее мы говорим, что функция f^* *вычислима* через функции $f_1^*,\dots,f_k^*$, если существует такая булева функция F, что справедливо тождество $f^*\equiv F(f_1^*,\dots,f_k^*)$).

Произвольную функцию f от переменных $x_1, \dots, x_n, y_1, \dots, y_m$ можно *разложить в полином* (Жегалкина) по переменным $x_1, \dots, x_n$, т. е. представить в виде (нас интересует линейная часть)

$$f = f^0 \oplus f^1 x_1 \oplus \ldots \oplus f^n x_n \oplus f', \tag{11}$$

где каждая из функций $f^0, \dots, f^n$ зависит только от переменных $y_1 \dots, y_m$ и f' — полином Жегалкина, в котором каждое слагаемое содержит хотя бы две из переменных $x_1, \dots, x_n$. Разложим таким образом функции g_l $(1 \leqslant l \leqslant p)$ и h_j $(1 \leqslant j \leqslant n)$:

$$g_l = g_l^0 \oplus g_l^1 x_1 \oplus \ldots \oplus g_l^n x_n \oplus g_l',$$

$$h_j = h_j^0 \oplus h_j^1 x_1 \oplus \ldots \oplus h_j^n x_n \oplus h_j'.$$

Набор $\tilde{y}_i$ $(1 \leqslant i \leqslant n)$ образуем из всех переменных вида u_f, соответствующих функциям g_l^i, $l \in G_i'$; набор $\tilde{z}_j$ $(1 \leqslant j \leqslant n)$ — из всех переменных, соответствующих функциям g_l^0, $l \in H_j$. Сразу же заметим (с учётом (8) и (9)), что

$$L(S) \geqslant \frac{1}{2} \sum_{i=1}^{n} (|G_i'| + |H_i|) = \frac{1}{2} \sum_{i=1}^{n} (|\tilde{y}_i| + |\tilde{z}_i|). \tag{12}$$

Для любых i, j в качестве $u_{i,j}$ возьмём переменную, соответствующую функции h_j^i.

Покажем, что функцию h_j^i можно вычислить через функции из множества $\{g_l^0, g_l^i \mid l \in H_j\}$. Действительно, любая булева функция может быть представлена в виде суперпозиции сложения (по модулю 2), умножения (конъюнкции) и прибавления единицы. Если аргументы и результат каждой из этих операций разложить в полином по $x_1, \dots, x_n$, то можно заметить, что свободный член результата (т. е. f^0 в представлении (11)) вычисляется через свободные члены аргументов, а коэффициент при переменной x_i (т. е. f^i в (11)) — через свободные члены и коэффициенты при x_i аргументов. Таким образом коэффициент при x_i (т. е. g_j^i) суперпозиции функций вычисляется через свободные члены (g_l^0) и коэффициенты при x_i (т. е. g_l^j) тех функций второго яруса, которые используются для вычисления h_j (другими словами, функций из множества $\{g_l \mid l \in H_j\}$).

Далее, заметим, что если при вычислении функции g_l не используется переменная x_i (т. е. $l \notin G_i'$), то $g_l^i = 0$, следовательно, функцию g_l^i можно исключить из множества функций, используемых для вычисления h_j^i (считаем, что для вычисления констант не нужно аргументов). Итак, функция h_j^i, соответствующая переменной $u_{i,j}$, может быть вычислена через функции из множества

$V_{i,j} = \{g_l^0 \mid l \in H_j\} \cup \{g_l^i \mid l \in G_i'\}$. Заметим, что наборы $\tilde{y}_i$ и $\tilde{z}_j$ составлены из переменных вида u_f, соответствующих функциям из множества $V_{i,j}$. Таким образом, функция $f_{i,j}$ определена корректно (см. (10)); n-таблица $\mathcal{F}$ построена.

Рассмотрим теперь (n,n)-разложение $R = \{M^1, \ldots, M^n\}$, в котором матрица $M^t = (m_{i,j}^t)$, $1 \leqslant t \leqslant n$, определена следующим образом:

$$\forall i,j \quad m_{i,j}^t = 1 \iff i = r(j,t).$$

Покажем, что таблица $\mathcal{F}$ распознаёт разбиение R, т. е. для любого t, $1 \leqslant t \leqslant n$, таблица $\mathcal{F}$ вычисляет матрицу M^t.

Зафиксируем t. Существуют такие константы $\alpha_1, \ldots, \alpha_m$, что $\sum\limits_{s=1}^{m} \alpha_s 2^{m-s} = t$. Для произвольной функции f обозначим через $f|_A$ результат подстановки в функцию f констант $\alpha_1, \ldots, \alpha_m$ вместо переменных $y_1, \ldots, y_m$ соответственно. Заметим, что если функцию $f|_A$ представить в виде (11), то коэффициенты полученного разложения можно получить из соответствующих коэффициентов разложения функции f действием подстановки A, т. е. $(f|_A)^i = (f^i)|_A$. Поэтому коэффициент при переменной x_i в разложении функции $h_j|_A$ (который мы обозначим через $(h_j|A)^i$) равен константе $h_j^i|_A$. С другой стороны, коэффициент $(h_j|A)^i$ можно найти явно из определения оператора RCL_n. А именно, имеет место равенство $h_j|_A = x_{r(j,t)}$, $1 \leqslant j \leqslant n$, откуда (с учётом определения матрицы M^t) следует

$$(h_j|_A)^i = 1 \iff i = r(j,t) \iff m_{i,j}^t = 1.$$

Таким образом,

$$h_j^i|_A = (h_j|_A)^i = m_{i,j}^t. \tag{13}$$

При действии подстановки A каждая функция f, зависящая только от переменных $y_1, \ldots, y_m$, принимает некоторое значение. Это значение припишем переменной u_f. В частности, для любых i,j всем переменным из наборов $\tilde{y}_i, \tilde{z}_j$ и переменной $u_{i,j}$ приписаны значения; при этом сохраняют силу тождества (10). Наконец, заметим, что значение, приписанное переменной $u_{i,j}$, равно $h_j^i|_A$, т. е. (в силу (13)) $m_{i,j}^t$. Итак, при некоторых значениях переменных из наборов $\tilde{y}_1, \ldots, \tilde{y}_n, \tilde{z}_1, \ldots, \tilde{z}_n$ каждая функция $f_{i,j}$, применённая к значениям своих переменных, даёт результат $m_{i,j}^t$. Это и означает, что таблица $\mathcal{F}$ вычисляет матрицу M^t.

Обозначим $c = 2L(S)/n$. Тогда неравенство (12) примет вид (7). По определению величины $c'(n,n)$ имеем $c \geqslant c'(n,n)$. Окончательно получим

$$L_B^{C_2}(\mathrm{RCL}_n) = \Omega(L(S)) = \Omega(cn) = \Omega(nc'(n,n)).$$

Лемма 2 доказана.

Теорема 2. *В произвольном базисе B*

$$L_B^{C_2}(\mathrm{RCL}_n) = \Omega(n \log_2 \log_2 \log_2 n), \qquad n \to \infty.$$

Теорема 2 следует из лемм 1, 2 и утверждения 4.

5. Почти квадратичная нижняя оценка сложности

Пусть $\tilde{f}$: $\{0,1\}^n \to \{0,1\}^m$ — булев оператор, $\tilde{f} = (f_1, \ldots, f_m)$. Далее, пусть $\tilde{x}$ — набор переменных оператора $\tilde{f}$ и $\tilde{x}$ разбит на непересекающиеся наборы: $\tilde{x} = (\tilde{x}^1, \ldots, \tilde{x}^k)$. Обозначим через $\mathcal{D}(\tilde{f}, \tilde{x}^i)$ $(i = 1, \ldots, k)$ множество подоператоров, полученных из оператора $\tilde{f}$ при всевозможных подстановках констант вместо всех его переменных, за исключением тех, которые входят в набор $\tilde{x}^i$. Положим $I(\tilde{f}, \tilde{x}^i) = \log_2 |\mathcal{D}(\tilde{f}, \tilde{x}^i)|$.

В случае $m = 1$ известна следующая оценка сложности (метод Нечипорука, [2, 3]). Пусть каждый из наборов $\tilde{x}^i$ содержит хотя бы одну существенную переменную функции f. Тогда для любого базиса B существует константа c_B такая, что для любой функции f выполнено

$$L_B^{\Phi}(f) \geqslant c_B \sum_{i=1}^{k} I(f, \tilde{x}^i). \tag{14}$$

Заметим, что если f не равна тождественно константе и набор $\tilde{x}^i$ не содержит существенных для f переменных, то $\tilde{x}^i$ не даёт вклада в левую часть (14), но даёт вклад 1 в сумму в правой части. Поэтому для достаточно большого числа фиктивных наборов $\tilde{x}^i$ неравенство (14) не выполнено.

Пусть теперь m произвольно и оператор $\tilde{f}$ разбит на k операторов: $f = (\tilde{f}^1, \ldots, \tilde{f}^k)$, а именно, каждая из функций $f_1, \ldots, f_m$ отнесена ровно к одному из наборов $\tilde{f}^1, \ldots, \tilde{f}^k$. Будем считать, что каждая переменная из $\tilde{x}$ существенна для оператора $\tilde{f}$.

Теорема 3. *Для любого базиса B существует константа c'_B такая, что для любого оператора $\tilde{f}$ выполнено*

$$L_B^{C_2}(\tilde{f}) \geqslant c'_B \sum_{i=1}^{k} I(\tilde{f}^i, \tilde{x}^i).$$

Доказательство. Мы будем использовать некоторые понятия и обозначения из доказательства леммы 2. Рассмотрим строго двухярусную схему S минимальной сложности, реализующую оператор $\tilde{f}$. Пусть $E_1, \ldots, E_p$ — элементы второго яруса, $F_1, \ldots, F_m$ — элементы, подаваемые на выходы схемы; Γ_l

$(1 \leqslant l \leqslant p)$ и X_j $(1 \leqslant j \leqslant m)$ — части схемы, расположенные, соответственно, на первом и втором ярусе и оканчивающиеся, соответственно, элементами E_l и F_j; g_l и h_j — функции от переменных $\tilde{x}$, вычисляемые на выходах, соответственно, элементов E_l и F_j.

Обозначим через G_l $(1 \leqslant l \leqslant p)$ множество индексов i таких, что хотя бы одна из переменных набора $\tilde{x}^i$ существенна для функции g_l. Положим $G'_i = \{l \mid i \in G_l\}$, $i = 1, \ldots, k$. Через H_i $(1 \leqslant i \leqslant k)$ обозначим множество тех индексов l, для которых функция g_l используется при вычислении хотя бы одной функции из набора $\tilde{f}^i$. Наконец, через H'_j $(1 \leqslant j \leqslant m)$ обозначим множество тех l, что g_l используется при вычислении функции f_j. Схема Γ_l является формулой, поэтому из (14) следует

$$L(\Gamma_l) \geqslant L_B^{\Phi}(g_l) \geqslant c_B \sum_{i\colon i \in G_l} I(g_l, \tilde{x}^i). \tag{15}$$

Рассмотрим произвольный оператор $\tilde{f}' \in \mathcal{D}(\tilde{f}^i, \tilde{x}^i)$. Ему соответствует некоторая подстановка констант вместо переменных, не входящих в $\tilde{x}^i$. Осуществив эту же подстановку в функции $(g_l)_{l \in H_i}$, мы получим набор их подфункций $(g'_l)_{l \in H_i}$, $g'_l \in \mathcal{D}(g_l, \tilde{x}^i)$. Указанное соответствие $\tilde{f}' \mapsto (g'_l)_{l \in H_i}$ инъективно: из двух равных наборов подфункций, производя одни и те же вычисления, мы получим равные подоператоры оператора $\tilde{f}$. Таким образом,

$$|\mathcal{D}(\tilde{f}^i, \tilde{x}^i)| \leqslant \prod_{l \in H_i} |\mathcal{D}(g_l, \tilde{x}^i)|.$$

Следовательно,

$$I(\tilde{f}^i, \tilde{x}^i) \leqslant \sum_{l \in H_i} I(g_l, \tilde{x}^i). \tag{16}$$

Заметим, что если $l \notin G'_i$, т. е. $i \notin G_l$, то функция g_l существенно не зависит ни от одной переменной из $\tilde{x}^i$. Тогда множество $\mathcal{D}(g_l, \tilde{x}^i)$ состоит только из констант. Следовательно, $I(g_l, \tilde{x}^i) \leqslant 1$, а значит,

$$\sum_{l \in H_i \setminus G'_i} I(g_l, \tilde{x}^i) \leqslant |H_i|. \tag{17}$$

Заметим также (что мы уже делали при доказательстве леммы 2), что для некоторой константы c''_B выполнено

$$|H'_j| \leqslant c''_B L(X_j). \tag{18}$$

Наконец, объединив выкладки (15)–(18), получим

$$\sum_{i=1}^{k} I(\tilde{f}^i, \tilde{x}^i) \leqslant \sum_{i,l:\, l\in H_i} I(g_l, \tilde{x}^i) = \sum_{i,l:\, l\in H_i \cap G_i'} I(g_l, \tilde{x}^i) + \sum_{i,l:\, l\in H_i \setminus G_i'} I(g_l, \tilde{x}^i) \leqslant$$

$$\leqslant \sum_{i,l:\, l\in G_i'} I(g_l, \tilde{x}^i) + \sum_{i=1}^{k} |H_i| \leqslant \sum_{l,i:\, i\in G_l} I(g_l, \tilde{x}^i) + \sum_{j=1}^{m} |H_j'| \leqslant$$

$$\leqslant \frac{1}{c_B} \sum_{l=1}^{p} L(\Gamma_l) + c_B'' \sum_{j=1}^{m} L(X_j) \leqslant \frac{1}{c_B'} L(S)$$

для некоторой константы c_B'. Теорема 3 доказана.

Определим оператор MMA_n *многократного доступа к памяти.* Пусть r — натуральное число, $n = 2^r$, $m = [n/r]$. Обозначим через $N(\tilde{\alpha})$ номер набора α. Если $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_r)$, то $N(\tilde{\alpha}) = \sum_{i=1}^{r} \alpha_i 2^{n-i}$. Пусть наборы $(x_1, \ldots, x_n)$, $\tilde{y}^1, \ldots, \tilde{y}^m$ состоят из попарно различных переменных и в каждом из наборов $\tilde{y}^i$ $(1 \leqslant i \leqslant m)$ содержится r переменных. Положим

$$\mathrm{MMA}_n : (x_1, \ldots, x_n,\ \tilde{y}^1, \ldots, \tilde{y}^m) \mapsto (x_{N(\tilde{y}^1)}, \ldots, x_{N(\tilde{y}^m)}).$$

Пусть f_i — i-я компонента оператора MMA_n. Среди подфункций функции f_i, зависящих только от переменных $\tilde{y}^i$, встречаются всевозможные функции от переменных $\tilde{y}^i$. Действительно, значение подфункции на произвольном наборе $\tilde{\alpha}$ равно константе, подставленной вместо переменной $x_{N(\tilde{\alpha})}$. Таким образом, $|\mathcal{D}(f_i, \tilde{y}^i)| = 2^{2^r} = 2^n$, а значит, $I(f_i, \tilde{y}^i) = n$. Применив теорему 3, получим

$$L_B^{C_2}(\mathrm{MMA}_n) \geqslant c_B' \sum_{i=1}^{m} I(f_i, \tilde{y}^i) = c_B' mn = \Omega\Big(\frac{n^2}{\log_2 n}\Big).$$

Работа выполнена при финансовой поддержке Фонда Президента РФ поддержки научных школ (проект НШ–1807.2003.01) и при частичной финансовой поддержке РФФИ (проект 05–01–00994).

Литература

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Из-во МГУ, 1984. — 138 с.

2. Нечипорук Э. И. Об одной булевской функции // ДАН СССР. — 1966. — Т. 169, N 4. — С. 765–766.

3. Нигматуллин Р. Г. Сложность булевых функций. — М.: Наука, 1991. — 240 с.

4. Субботовская Б. А. О сравнении базисов при реализации функций алгебры логики формулами // ДАН СССР. — 1963. — Т. 149, N 4. — С. 784–787.

5. Черухин Д. Ю. Нижняя оценка сложности в классе схем глубины 2 без ограничений на базис // Вестник Московского университета. Серия 1. Математика. Механика. — 2005. — N 4. — С. 54–56.

6. Pudlak P., Savicky P. On shifting networks // Theoretical Comput. Sci. — 1993. — V. 116. — P. 415–419.

7. Radhakrishnan J. Ta-Shma A. Bounds for dispersers, extractors, and depth-two superconcentrators // SIAM J. of Discrete Mathematics. — 2000. — V. 13, No 1. — P. 2–24.

8. Valiant L. G. Graph-theoretic arguments in low-level complexity // Lecture Notes in Computer Science, V. 53. — 1977. — P. 162–176.

мех.-мат. факультет МГУ, Воробьёвы горы, Москва, 119992, Россия
E-mail address: cherukhin@rambler.ru