УДК 519.714

О схемах из функциональных элементов конечной глубины ветвления / Д. Ю. Черухин

В работе введено понятие глубины ветвления схемы из функциональных элементов и рассмотрены классы схем, имеющие глубину ветвления, ограниченную константой. В данных классах схем и различных базисах получены верхние и нижние оценки сложности линейной булевой функции. Построены бесконечно убывающие последовательности мер сложности при фиксированном базисе и растущей глубине ветвления и при фиксированной глубине ветвления и меняющемся базисе.

Ключевые слова: булева функция, схема из функциональных элементов, сложность, глубина.

Keywords: Boolean function, combinational circuit, complexity, depth.

О схемах из функциональных элементов конечной глубины ветвления

Д. Ю. Черухин

Базисом будем называть конечную полную систему булевых функций. Определения схемы из функциональных элементов (СФЭ) и формулы в базисе B можно найти, например, в [1]. Скажем, что вершина v схемы S обладает *ветвлением*, если функция, вычисленная в вершине v, используется в дальнейшем вычислении не менее двух раз, а именно, либо вершине v соответствуют не менее двух выходов схемы, либо v является выходом схемы и существует хотя бы одно ребро, выходящее из v, либо из v выходит не менее чем два ребра. Вершину v назовём *узловой*, если либо v является входом схемы, либо v обладает ветвлением.

Глубиной ветвления схемы S называется наибольшее число узловых вершин, содержащихся в одном ориентированном пути в схеме S. Таким образом, глубина ветвления формул равна 1 (заметим, что если не считать входы узловыми вершинами, то глубина ветвления бесповторных [2] формул равна нулю; однако такое определение в некотором смысле неудобно), глубина ветвления схем из функциональных элементов неограничена. В данной работе рассмотрены классы схем, в которых глубина ветвления ограничена константой.

При реализации почти всех булевых функций рассматриваемые классы схем (если глубина ветвления ограничена числом, не меньшим 2) ведут себя подобно схемам из функциональных элементов (а именно, имеют тот же порядок роста функции Шеннона). В настоящей работе показано, что при реализации отдельных функций, например, линейной функции, данные классы схем более напоминают формулы, а именно, и верхние (Теорема 1) и нижние (Теорема 2) оценки сложности извлекаются из соответствующих методов оценки сложности формул.

При получении нижних оценок сложности используется традиционный метод "забивания" переменных, впервые использованный Субботовской [3] для базиса $\{\&, \vee, \neg\}$, и распространённый затем на класс обобщенно-монотонных базисов, т. е. базисов, в которых линейная функция имеет нелинейную сложность [4–7]; метод забивания известен также как метод сжатия формул (shrinkage) под действием случайной подстановки [7,8]. Вопрос о том, применимы ли к схемам ограниченной глубины ветвления аналоги других методов получения нижних оценок сложности формул [9], остаётся открытым.

Скажем, что мера сложности L_1 булевых функций *предшествует* [2] мере сложности L_2 ($L_1 \leqslant L_2$), если $L_1(f) = \mathcal{O}(L_2(f))$ при $\mathrm{nes}(f) \to \infty$, где $\mathrm{nes}(f)$ — число существенных переменных функции f (здесь и далее асимптотические соотношения понимаются в смысле теории предела по базе). Для каждого базиса B и числа $k \geqslant 1$ мы введём меру сложности L_B^k, соответствующую классу схем в базисе B, глубина ветвления которых не превосходит k. Мы построим (Теорема 3) бесконечные последовательности вида $L_B^{k_1} > L_B^{k_2} > \dots$ для каждого обобщенно-монотонного базиса B и вида $L_{B_1}^k > L_{B_2}^k > \dots$ для каждого $k \geqslant 2$; при $k = 1$ такие последовательности известны (например, [6]). Кроме того, используя улучшенную технику сжатия формул в базисе $B_0 = \{\&, \vee, \neg\}$ [8], покажем (Теорема 4), что $L_{B_0}^1 > L_{B_0}^2 > \dots$

Стоит отметить связь глубины ветвления с глубиной в обычном смысле, т. е. наибольшей из длин ориентированных путей в схеме. Схемы глубины ветвления k в базисе B можно рассматривать как схемы глубины k над бесконечным базисом, состоящим из всех функций, бесповторно выразимых [2] в базисе B. Вопрос о сравнении мер сложности одной и той же модели схем с разными константными ограничениями на глубину был впервые исследован в работе [10]: для класса монотонных формул было показано, что при увеличении глубины на единицу мера сложности строго уменьшается.

В настоящее время имеется достаточно много работ по нижним оценкам сложности схем ограниченной глубины; в некоторых из них получены экспоненциальные нижние оценки сложности [9]. В отличие от многих классов схем ограниченной глубины рассматриваемые в данной работе классы являются "сильными", так как они не слабее класса формул в полном базисе, традиционно считающегося "сильным": наибольшие известные нижние оценки сложности формул не превосходят полинома от числа переменных.

Сложностью схемы S будем считать число рёбер, выходящих из узловых вершин; сложность будем обозначать через $L(S)$. Нетрудно показать, что данная мера сложности отличается не более чем в константу раз от традиционной меры сложности СФЭ — числа элементов; в то же время рассматриваемая мера сложности является традиционной для формул (число рёбер, исходящих из входов формулы, равно числу вхождений в формулу символов переменных). Обозначим через $L_B^k(f)$ сложность булевой функции f в классе СФЭ в базисе B, глубина ветвления которых не превосходит k. В частности, $L_B^1(f)$ — сложность функции f в классе формул в базисе B.

Обозначим $\Lambda_n = x_1 \oplus \ldots \oplus x_n$. Для любого целого $k \geqslant 1$ введём функцию

$$\varphi_k(x) = \frac{1}{1-(1-1/x)^k}.$$

Заметим, что если $x > 1$, то $\varphi_1(x) = x$ и последовательность $\varphi_1(x), \varphi_2(x)$, $\ldots$, монотонно убывая, стремится к числу 1.

Теорема 1. *Пусть B — базис, $\gamma > 1$. Тогда, если*

$$L_B^1(\Lambda_n) = \mathcal{O}(n^\gamma), \quad n \to \infty,$$

то для любого k

$$L_B^k(\Lambda_n) = \mathcal{O}(n^{\varphi_k(\gamma)}), \quad n \to \infty.$$

Доказательство. На первом шаге объединим переменные в группы (которые будем называть 1-группами) примерно по n_1 переменных в каждой (числа n_1, $n_2, \ldots, n_{k-1}$ выберем позже). Сумму переменных в каждой 1-группе реализуем формулой сложности $\mathcal{O}(n_1^\gamma)$. Общая сложность построенных формул есть $\mathcal{O}(n_1^\gamma \cdot \frac{n}{n_1})$. На втором шаге объединим 1-группы в более крупные 2-группы, а именно, каждую 2-группу образуем примерно из n_2 1-групп. Реализуем сумму переменных в каждой 2-группе формулой, используя в качестве входов этой формулы ранее вычисленные суммы для 1-групп. Общая сложность построенных формул на втором шаге есть $\mathcal{O}(n_2^\gamma \cdot \frac{n}{n_1 n_2})$.

Подобным образом действуем и дальше. На k-м шаге объединим все n переменных в одну k-группу и вычислим их сумму, опираясь на суммы переменных в $(k-1)$-группах. Пусть n_k — число $(k-1)$-групп, тогда

$$n_1 n_2 \cdot \ldots \cdot n_k \sim n. \qquad (1)$$

Сложность формулы, построенной на k-м шаге есть $\mathcal{O}(n_k^\gamma) = \mathcal{O}(n_k^\gamma \cdot \frac{n}{n_1 n_2 \ldots n_k})$. Построенная нами схема имеет глубину ветвления k и реализует функцию Λ_n, поэтому

$$L_B^k(\Lambda_n) = \mathcal{O}\Big(\sum_{i=1}^{k} n_i^\gamma \cdot \frac{n}{n_1 \ldots n_i}\Big). \qquad (2)$$

Выберем числа $n_1, \ldots, n_{k-1}$ так, чтобы слагаемые в сумме (2) были примерно равны. После несложных выкладок получим условия

$$n_{i+1} \sim n_i^\alpha, \text{ где } \alpha = \frac{\gamma}{\gamma - 1}, \quad i = 1, \ldots, k-1.$$

Подставим их в (1):

$$n \sim n_1 \cdot n_1^\alpha \cdot \ldots \cdot n_1^{\alpha^{k-1}} = n_1^{\frac{\alpha^k - 1}{\alpha - 1}}.$$

Выразив отсюда n_1, подставим его в (2):

$$L_B^k(\Lambda_n) = \mathcal{O}\Big(k \cdot n_1^\gamma \frac{n}{n_1}\Big) = \mathcal{O}(n_1^{\gamma-1} n) = \mathcal{O}\Big(n^{\frac{\alpha-1}{\alpha^k-1}(\gamma-1)+1}\Big). \qquad (3)$$

Наконец, преобразуем показатель степени в последней формуле выкладки (3):

$$\frac{\alpha - 1}{\alpha^k - 1}(\gamma - 1) + 1 = \frac{(\frac{\gamma}{\gamma-1} - 1)(\gamma - 1)}{\alpha^k - 1} + 1 = \frac{1}{\alpha^k - 1} + 1 = \frac{1}{1 - (1/\alpha)^k} = \varphi_k(\gamma).$$

Теорема 1 доказана.

Подстановкой констант называется функция, сопоставляющая некоторым переменным константы из множества $\{0, 1\}$. Если f — функция, A — подстановка констант, то через $f|_A$ обозначим функцию, полученную из f фиксацией переменных, входящих в область определения подстановки A, соответствующими константами; через $|A|$ обозначим мощность множества определения подстановки A. Введём меру сложности функций L_B^*: если f тождественно равна константе, переменной или отрицанию переменной, то $L_B^*(f) = 0$, иначе $L_B^*(f) = L_B^1(f)$.

Пусть f — функция от n переменных, $0 \leqslant m \leqslant n$. Тогда обозначим

$$L_B^*(f; m) = \frac{1}{2^{n-m} C_n^m} \sum_{A, |A| = n-m} L^*(f|_A)$$

(здесь и далее сумма берётся по подстановкам A, область определения которых содержится в множестве переменных функции f). Другими словами, $L^*_B(f;m)$ — сложность случайной подфункции от m переменных функции f. Скажем, что базис B обладает *экспонентой сжатия* γ, если при $n = \mathrm{nes}(f) \to \infty$, $m \geqslant 1$, $m = o(n)$, выполнено

$$L^*_B(f) = \Omega\Big(\Big(\frac{n}{m}\Big)^{\gamma}\Big) L^*_B(f;m). \tag{4}$$

Теорема 2. *Пусть базис B обладает экспонентой сжатия γ, $\gamma > 1$. Тогда для любого k*

$$L^k_B(\Lambda_n) = \Omega(n^{\varphi_k(\gamma)}), \quad n \to \infty.$$

Доказательство. Проведём индукцию по k. Базис индукции, $k = 1$, следует из (4), если положить $m = 2$.

Индуктивный переход: $k - 1 \mapsto k$. Пусть S — схема минимальной сложности для функции Λ_n в классе схем глубины ветвления, не большей k. Пусть V — множество узловых вершин схемы S, отличных от входов. Если $V = \varnothing$, то схема S является формулой и доказываемое утверждение следует из базиса индукции и неравенства $\varphi_k(\gamma) < \gamma$.

Рассмотрим случай $V \neq \varnothing$. Вершину $v \in V$ назовём *минимальной в* V, если не существует вершины $v' \in V$, $v' \neq v$, такой, что из v' в v ведёт некоторый ориентированный путь. Пусть $V' = \{v_1, \ldots , v_r\}$ — множество всех минимальных в V вершин. Пусть также f_i — функция, вычисляемая в вершине v_i, $1 \leqslant i \leqslant r$ (f_i зависит от входных переменных схемы S). Тогда часть схемы S, предшествующая вершине v_i, т. е. часть, в которой вычисляется функция f_i, является формулой; обозначим её через F_i. Формулы $F_1, \ldots , F_r$ не содержат общих вершин, за исключением входов, и минимальны, поэтому

$$L(S) \geqslant \sum_{i=1}^{r} L(F_i) = \sum_{i=1}^{r} L^1_B(f_i). \tag{5}$$

Если

$$\sum_{i=1}^{r} L^1_B(f_i) \geqslant n^{\varphi_k(\gamma)}, \tag{6}$$

то, в силу (5), теорема доказана. Если же (6) не выполнено, то с учётом (4) для некоторой константы C при $m \geqslant 1$, $m = o(n)$ имеем

$$n^{\varphi_k(\gamma)} > \sum_{i=1}^{r} L_B^1(f_i) \geqslant \sum_{i=1}^{r} L_B^*(f_i) \geqslant C\left(\frac{n}{m}\right)^{\gamma} \sum_{i=1}^{r} L_B^*(f_i; m) =$$
$$= C\left(\frac{n}{m}\right)^{\gamma} \frac{1}{2^{n-m} C_n^m} \sum_{A, |A| = n-m} \sum_{i=1}^{r} L_B^*(f_i|_A).$$

Существует такая подстановка констант A, $|A| = n - m$, что

$$n^{\varphi_k(\gamma)} > C\left(\frac{n}{m}\right)^{\gamma} \sum_{i=1}^{r} L_B^*(f_i|_A). \tag{7}$$

Положим $m = Dn^{\alpha}$, где α удовлетворяет условию

$$\varphi_k(\gamma) - \gamma(1-\alpha) = \alpha, \tag{8}$$

D определим ниже. Перепишем (7) в виде

$$\sum_{i=1}^{r} L_B^*(f_i|_A) < \frac{D^{\gamma}}{C} n^{\varphi_k(\gamma) - \gamma(1-\alpha)} = \frac{D^{\gamma}}{C} n^{\alpha} = \frac{D^{\gamma-1}}{C} m.$$

Константу D выберем так, чтобы выполнялось

$$\sum_{i=1}^{r} L_B^*(f_i|_A) < \frac{m}{2}. \tag{9}$$

Пусть M — множество переменных, каждая из которых существенна хотя бы для одной из функций $f_i|_A$, существенно зависящих не менее, чем от двух переменных. В силу (9) имеем $|M| < m/2$. Пусть A' — подстановка констант, определённая на множестве M. Тогда каждая из функций $f_i|_{A \cup A'}$ тождественно равна либо константе, либо переменной, либо отрицанию переменной. Осуществим подстановку констант $A \cup A'$ в схему S и проведём естественные упрощения, в частности, если функция $f_i|_{A \cup A'}$ равна переменной, то отождествим вершину v_i с соответствующим входом, если $f_i|_{A \cup A'}$ равна отрицанию переменной, то поступим аналогично, но предварительно пронесём отрицание через вершину v_i (возможно, увеличив число элементов отрицания, что не влияет на сложность); наконец, если функция $f_i|_{A\cup A'}$ тождественно равна константе, то вершину v_i удалим, осуществив дальнейшие подстановки этой константы.

В результате получим схему S', реализующую линейную функцию (или её отрицание) от не менее чем $m/2$ переменных. В схеме S' каждая из вершин, входящих в множество V', либо отсутствует, либо совпадает с одним из входов. Заметим, что любой ориентированный путь Π в исходной схеме S, содержащий ровно k узловых вершин, содержит хотя бы одну из вершин множества V'. (Действительно, пусть v — первая узловая вершина пути Π, отличная от входов. Тогда существует вершина $v' \in V'$, предшествующая вершине v. Заменив в Π начальный отрезок так, чтобы путь проходил через вершину v', получим путь, содержащий больше k узловых вершин. Противоречие.) Кроме того, каждая узловая вершина схемы S' является узловой для схемы S. Поэтому глубина ветвления схемы S' не превосходит $k-1$.

Применив предположение индукции, получим (заметив также, что сложности функции и её отрицания равны)

$$L(S) \geqslant L(S') \geqslant L_B^{k-1}(\Lambda_{m/2}) = \Omega((m/2)^{\varphi_{k-1}(\gamma)}) = \Omega(n^{\alpha\varphi_{k-1}(\gamma)}). \tag{10}$$

Выразив α из (8), преобразуем показатель степени в (10):

$$\alpha\varphi_{k-1}(\gamma) = \frac{\gamma - \varphi_k(\gamma)}{\gamma - 1} \cdot \varphi_{k-1}(\gamma). \tag{11}$$

Покажем, что последнее выражение в (11) равно $\varphi_k(\gamma)$, что равносильно следующему

$$\varphi_k(\gamma) = \frac{\gamma \cdot \varphi_{k-1}(\gamma)}{\varphi_{k-1}(\gamma) + \gamma - 1}. \tag{12}$$

Воспользовавшись равенством $\varphi_k(\gamma) = \frac{\gamma^k}{\gamma^k - (\gamma-1)^k}$, получим

$$\frac{\gamma \cdot \varphi_{k-1}(\gamma)}{\varphi_{k-1}(\gamma) + \gamma - 1} = \frac{\gamma \cdot \frac{\gamma^{k-1}}{\gamma^{k-1} - (\gamma-1)^{k-1}}}{\frac{\gamma^{k-1}}{\gamma^{k-1} - (\gamma-1)^{k-1}} + \gamma - 1} =$$
$$= \frac{\gamma^k}{\gamma^{k-1} + (\gamma - 1)(\gamma^{k-1} - (\gamma-1)^{k-1})} = \frac{\gamma^k}{\gamma^k - (\gamma-1)^k} = \varphi_k(\gamma).$$

Равенство (12), а вместе с ним и теорема 2, доказаны.

Функция f называется *обобщенно-монотонной*, если f по каждому своему аргументу либо не возрастает, либо не убывает. Базис, состоящий только из обобщенно-монотонных функций, называется обобщенно-монотонным. *Порядком* базиса B называется наибольшее число аргументов у функций из B.

Лемма 1. *Обобщенно-монотонный базис B порядка k обладает экспонентой сжатия $\gamma = \frac{3k-3}{3k-4}$.*

Доказательство. Будем использовать терминологию и результаты работы [11]. Заметим, что базис B можно считать нормальным (т. е. содержащим вместе с каждой функцией все её подфункции). В [11] введена мера сложности формул P: $P(F) = L(F) + M(F)$, где $M(F)$ — сумма весов функций, входящих в формулу; вес функции от l аргументов равен $\frac{l-2}{2}$ при $l \geqslant 2$ и 0 при $l \leqslant 1$. Для приведённой формулы F справедливо неравенство [11, Лемма 1]

$$L(F) \geqslant \frac{2k-2}{3k-4}P(F). \tag{13}$$

Через $F\restriction_A$ будем обозначать минимальную (с точки зрения меры P) приведённую формулу, являющуюся упрощением формулы $F|_A$, полученной, в свою очередь, действием подстановки констант A на формулу F.

В [11, Лемма 2] фактически доказано неравенство [11, (5)], а именно, для любых приведённой формулы F и переменной y справедливо

$$P(F) - \frac{P(F\restriction_{y=0}) + P(F\restriction_{y=1})}{2} \geqslant \frac{3}{2}L_y(F), \tag{14}$$

где $L_y(F)$ — число вхождений в F символов переменной y. Просуммировав (14) по всем n переменным формулы F, разделив на n и применив (13), получим

$$P(F) - \frac{1}{2n}\sum_{A,|A|=1} P(F\restriction_A) \geqslant \frac{3}{2n}L(F) \geqslant \frac{3k-3}{(3k-4)n}P(F) = \frac{\gamma}{n}P(F).$$

Отсюда следует

$$P(F) \geqslant \frac{1}{1-\gamma/n}\cdot\frac{1}{2n}\sum_{A,|A|=1} P(F\restriction_A). \qquad (15).$$

Введём меру сложности функций P_B^*, положив $P_B^*(f) = P_B(f)$, если $\mathrm{nes}(f) \geqslant 2$ и $P_B^*(f) = 0$ в противном случае. Тогда для любой функции f от n аргументов справедливо

$$P_B^*(f) \geqslant \frac{1}{1-\gamma/n} \cdot \frac{1}{2n} \sum_{A,|A|=1} P_B^*(f|_A). \tag{16}$$

Действительно, если $\mathrm{nes}(f) \leqslant 1$, то (16) следует из определения меры P_B^*, а если $\mathrm{nes}(f) \geqslant 2$, то (16) следует из (15), если в качестве F взять приведённый вид минимальной формулы (в смысле меры P) для функции f. Применив неравенство (16) итеративно $n-m$ раз и считая, что функция $f|_A$ не зависит от тех переменных, вместо которых были подставлены константы, получим

$$P_B^*(f) \geqslant \Big(\prod_{i=m+1}^{n} \frac{1}{1-\gamma/i} \Big) \frac{1}{2^{n-m} C_n^m} \sum_{A,|A|=n-m} P_B^*(f|_A). \tag{17}$$

Оценим произведение в (17):

$$\prod_{i=m+1}^{n} \frac{1}{1-\gamma/i} = \exp\Big\{ - \sum_{i=m+1}^{n} \ln\big(1 - \frac{\gamma}{i}\big) \Big\} \geqslant \exp\Big\{ \sum_{i=m+1}^{n} \frac{\gamma}{i} \Big\} \asymp$$
$$\asymp \exp\big\{\gamma(\ln n - \ln m)\big\} = \Big(\frac{n}{m}\Big)^{\gamma}.$$

Поставив данную оценку в (17), с учётом соотношения $P_B^*(f) \asymp L_B^*(f)$ получим требуемое неравенство (4). Лемма 1 доказана.

Теорема 3. а) *Для любого обобщенно-монотонного базиса B существует последовательность чисел $k_1, k_2, \ldots$ такая, что $L_B^{k_1} > L_B^{k_2} > \ldots$*

б) *Для любого $k = 1, 2, \ldots$ существует последовательность базисов B_1, $B_2, \ldots$ такая, что $L_{B_1}^k > L_{B_2}^k > \ldots$*

Доказательство. а) Положим $k_1 = 1$. Пусть k_i уже определено; определим k_{i+1}. Согласно лемме 1, базис B обладает экспонентой сжатия $\gamma > 1$. Поэтому, в силу теоремы 2, имеем

$$L_B^{k_i}(\Lambda_n) = \Omega(n^{\varphi_{k_i}(\gamma)}). \tag{18}$$

Последовательность $\varphi_1(2), \varphi_2(2), \ldots$ стремится к единице, следовательно, найдётся такое l, что $\varphi_l(2) < \varphi_{k_i}(\gamma)$. Положим $k_{i+1} = l$. Известно [9], что

$L^1_{B_0}(\Lambda_n) = \mathcal{O}(n^2)$. Отсюда и из неравенства $L^1_B \leqslant L^1_{B_0}$, справедливого для любого базиса B [2], следует $L^1_B(\Lambda_n) = \mathcal{O}(n^2)$. Тогда, в силу теоремы 1 и (18), имеем

$$L_B^{k_{i+1}}(\Lambda_n) = \mathcal{O}(n^{\varphi_{k_{i+1}}(2)}) = o(n^{\varphi_{k_i}(\gamma)}) = o(L_B^{k_i}(\Lambda_n)),$$

а значит, $L_B^{k_{i+1}} \not\geqslant L_B^{k_i}$. Наконец, неравенство $L_B^{k_{i+1}} \leqslant L_B^{k_i}$ справедливо в силу того, что класс схем с бо́льшим ограничением на глубину вложен в класс схем с меньшим ограничением.

б) Так же, как в работе [6], введём функцию

$$f_s(x_1, \dots, x_s, y_1, \dots, y_s) = \begin{cases} 1, & \text{если } \sum\limits_{i=1}^{s}(x_i + y_i) > s, \\ x_1 \oplus \ldots \oplus x_s, & \text{если } \sum\limits_{i=1}^{s}(x_i + y_i) = s, \\ 0, & \text{если } \sum\limits_{i=1}^{s}(x_i + y_i) < s \end{cases}$$

и образуем базис $B'_s = B_0 \cup \{f_s\}$, который, очевидно, является обобщенно-монотонным.

В силу тождества

$$f_s(x_1, \dots, x_s, \bar{x}_1, \dots, \bar{x}_s) \equiv \Lambda_s$$

несложно предложить метод построения формул для функции Λ_n, дающий при $s \geqslant 2$ оценку

$$L^1_{B'_s}(\Lambda_n) = \mathcal{O}(n^{\log_s(2s)}). \tag{19}$$

А именно, множество переменных нужно разбить на s примерно равных групп, каждую группу на s подгрупп и т. д. Если реализованы суммы переменных в каждой из подгрупп, то сумму переменных в группе можно реализовать, подставив построенные формулы (каждую — по два раза) вместо аргументов функции f_s. Таким образом, при увеличении числа переменных в s раз сложность формулы увеличивается примерно в $2s$ раз. Отсюда следует (19).

Построим последовательность чисел $s_1, s_2, \ldots$ и в качестве B_i возьмём базис B'_{s_i}, $i = 1, 2, \ldots$ Положим $s_1 = 2$. Далее, пусть число s_i определено; выберем s_{i+1}. В силу леммы 1 и теоремы 2 для некоторого числа $\gamma_i > 1$ выполнено

$$L^k_{B_i}(\Lambda_n) = \Omega(n^{\varphi_k(\gamma_i)}). \tag{20}$$

В качестве s_{i+1} возьмём такое число s, для которого $\varphi_k(\log_s(2s)) < \varphi_k(\gamma_i)$. Тогда в силу (19) и (20) и теоремы 1

$$L^k_{B_{i+1}}(\Lambda_n) = \mathcal{O}(n^{\varphi_k(\log_{s_{i+1}}(2s_{i+1}))}) = o(n^{\varphi_k(\gamma_i)}) = o(L^k_{B_i}(\Lambda_n)),$$

а значит, $L^k_{B_{i+1}} \not\geqslant L^k_{B_i}$. Неравенство $L^k_{B_{i+1}} \leqslant L^k_{B_i}$ следует из того, что при $s < s'$ функция f_s может быть получена из $f_{s'}$ подстановкой констант вместо некоторых переменных.

Теорема 3 доказана.

Лемма 2. *Для любого γ, $1 < \gamma < 2$, базис B_0 обладает экспонентой сжатия γ.*

Доказательство. Воспользуемся обозначениями и результатами работы [8]. Пусть f — функция от n переменных, $m = o(n)$, $p = \frac{2m}{n}$, $q = \frac{2p}{1-p}$. Рассмотрим случайную подстановку констант R_p: переменные независимо друг от друга получают значения $0, 1$ с одной и той же вероятностью $\frac{1-p}{2}$ и не получают значение с вероятностью p. Пусть $L^2(f)$ — мат. ожидание случайной величины $L(f|_{R_p})$ при условии $L(f|_{R_p}) \geqslant 2$; обозначим $L = L^1_{B_0}(f)$. Тогда [8, Lemma 7.2]

$$L^2(f) \leqslant \begin{cases} 30q^2 L(\log L)^{3/2}, & \text{если } q \leqslant \frac{1}{2\sqrt{L\log L}}, \\ 200q^2 L(\log \frac{1}{q})^{3/2}, & \text{если } \frac{1}{2} \geqslant q \geqslant \frac{1}{4\sqrt{L\log L}} \end{cases} \tag{21}$$

(здесь и далее $\log$ означает логарифм по основанию 2).

Из условия первого случая неравенства (21) следует $\log L = \mathcal{O}(\log \frac{1}{q})$, поэтому, объединяя оба случая (21) в один и используя цепочку соотношений $q \asymp p \asymp \frac{m}{n} = o(1)$, получим

$$L^2(f) = \mathcal{O}(q^2 \log^{3/2} \frac{1}{q})L = \mathcal{O}(q^\gamma)L.$$

Если, дополнительно, $\mathrm{nes}(f) \geqslant 2$, то

$$L^*_{B_0}(f) = L = \Omega\Big(\Big(\frac{1}{q}\Big)^\gamma\Big)L^2(f) = \Omega\Big(\Big(\frac{n}{m}\Big)^\gamma\Big)L^2(f). \tag{22}$$

Введём обозначения:

$$\Phi_i = p^i(1-p)^{n-i}C^i_n, \qquad \Psi_s = \sum_{i=0}^{s} \Phi_i.$$

Запишем вероятностное определение величины $L^2(f)$ в виде конечной суммы и оценим её:

$$L^2(f) = \sum_{i=0}^{n} p^i \Big(\frac{1-p}{2}\Big)^{n-i} \sum_{A,|A|=n-i} L^*_{B_0}(f|_A) = \sum_{i=0}^{n} p^i (1-p)^{n-i} C_n^i L^*_{B_0}(f;i) =$$

$$= \sum_{i=0}^{n} \Phi_i L^*_{B_0}(f;i) \geqslant \sum_{i=m}^{n} \Phi_i L^*_{B_0}(f;m) = (1-\Psi_{m-1}) L^*_{B_0}(f;m). \qquad (23)$$

Заметим, что при $i \leqslant p(n+1)$ (а значит, при $i \leqslant m$), выполнено

$$\frac{\Phi_i}{\Phi_{i-1}} = \frac{p}{1-p} \cdot \frac{n-i+1}{i} \geqslant 1.$$

Тогда, используя формулу Стирлинга $n! \asymp (n/e)^{n+0,5}$, при $n \to \infty$, $m = o(n)$, $m \to \infty$ получим

$$\Psi_{m-1} \leqslant m\Phi_m \asymp m\Big(\frac{2m}{n}\Big)^m \Big(\frac{n-2m}{n}\Big)^{n-m} \frac{(n/e)^{n+0,5}}{(m/e)^{m+0,5}((n-m)/e)^{n-m+0,5}} \asymp$$
$$\asymp 2^m \Big(\frac{n-2m}{n-m}\Big)^{n-m} \sqrt{m} = 2^m \Big(1 - \frac{m}{n-m}\Big)^{n-m} \sqrt{m} \sim \Big(\frac{2}{e}\Big)^m \sqrt{m}.$$

Таким образом, Ψ_{m-1} ограничено бесконечно малой величиной, зависящей только от m, а значит, существует такое m_0, что при $m \geqslant m_0$ выполнено $\Psi_{m-1} \leqslant 1/2$. Тогда из (22) и (23) следует, что требуемое неравенство (4) выполнено при $m \geqslant m_0$. Наконец, уменьшив константу в правой части (4) и воспользовавшись неравенством $L^*_{B_0}(f;m_0) \geqslant L^*_{B_0}(f;m)$ при $m \leqslant m_0$, добъёмся того, чтобы (4) было выполнено при $1 \leqslant m \leqslant m_0$. Лемма 2 доказана.

Теорема 4. *Справедливы неравенства* $L^1_{B_0} > L^2_{B_0} > \dots$

Доказательство. Из теорем 1, 2, леммы 2, оценки $L^1_{B_0}(\Lambda_n) = \mathcal{O}(n^2)$ [9] и непрерывности по x функции $\varphi_k(x)$ в точке $x = 2$ следует, что для любого k и любой константы $c > 0$ выполнено

$$L^k_{B_0}(\Lambda_n) = \Omega(n^{\varphi_k(2)-c}), \qquad L^k_{B_0}(\Lambda_n) = \mathcal{O}(n^{\varphi_k(2)}).$$

Тогда в силу строгого убывания последовательности $\varphi_1(2), \varphi_2(2), \dots$ имеем

$$L^{k+1}_{B_0}(\Lambda_n) = o(L^k_{B_0}(\Lambda_n)), \quad k = 1, 2, \dots$$

Неравенства $L_{B_0}^{k+1} \leqslant L_{B_0}^{k}$, $k = 1, 2, \ldots$ очевидны. Теорема 4 доказана.

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994), программы "Университеты России" (проект УР.04.02.528) и программы поддержки ведущих научных школ РФ (проект НШ–1807.2003.1).

Литература

1. Лупанов О. Б. *Асимптотические оценки сложности управляющих систем.* Изд-во МГУ, Москва, 1984.

2. Субботовская Б. А. О сравнении базисов при реализации функций алгебры логики формулами. *ДАН СССР* (1963) **149**, N 4, 784–787.

3 Субботовская Б. А. О реализации линейных функций формулами в базисе $\vee, \&, -$. *ДАН СССР* (1961) **136**, N 3, 784–787.

4. Мучник Б. А. Оценка сложности реализации линейной функции в некоторых базисах. *Кибернетика* (1970), N 4, 29–38.

5. Перязев Н. А. Сложность представлений булевых функций формулами в немонолинейных базисах. *Дискретная математика и информатика. Вып. 2.* Изд-во Иркут. ун-та, Икрутск, 1995.

6. Черухин Д. Ю. О сложности реализации линейной функции формулами в конечных булевых базисах. *Дискретная математика* (2000) **12**, вып. 1, 135–144.

7. Chockler H., Zwick U. Which bases admit non-trivial shrinkage of formulae? *Computational complexity* (2001) **10**, No 1, pp. 28–40.

8. Hastad J. The shrinkage exponent of de Morgan formulas is 2. *SIAM J. Comput* (1998) **27**, pp. 48–64.

9. Нигматуллин Р. Г. *Сложность булевых функций.* Наука, Москва, 1991.

10. Лупанов О. Б. О влиянии глубины формул на их сложность. *Кибернетика* (1970), N 2, 46–49.

11. Черухин Д. Ю. Сверхквадратичные нижние оценки сложности формул в некоторых базисах. *Дискретный анализ и исследование операций. Сер. 1* (2000) **7**, N 2, 86–95.