# О МНОГОЯРУСНЫХ ФОРМУЛАХ

**Д. Ю. Черухин**

Рассматриваются булевы схемы из функциональных элементов (СФЭ, [1]). Ветвлением вершины называется число рёбер, исходящих из этой вершины; в частности, в ветвлении учитывается число выходов, которым соответствует эта вершина (на которые "подаётся сигнал" из этой вершины). Например, если из вершины выходит 2 ребра, ведущих в другие вершины схемы и, кроме того, вершина соответствует трём выходам схемы, то её ветвление равно 5.

Вершина называется узловой, если либо она является входом схемы, либо её ветвление больше единицы. СФЭ $S$ называется *$k$-ярусной* формулой, если в любом ориентированном пути в $S$ содержится не более $k$ узловых вершин. Другими словами, если узловые вершины можно разбить на $k$ ярусов так, что внутри каждого яруса вершины попарно несравнимы в смысле естественного порядка в ориентированном графе.

Одноярусные формулы соответствуют обычным формулам, т. е. схемам без ветвления (могут ветвиться только входы). Сложностью $k$-ярусной формулы является сумма ветвлений узловых вершин. Такая мера сложности естественна для формул; в случае $k = 1$ она совпадает с числом вхождений переменных в формулу. Пусть $L_B^k$ — мера сложности функций (операторов) в классе $k$-ярусных формул в конечном базисе $B$, $\mathcal{L}_B^k$ — соответствующая функция Шеннона [1].

**Теорема 1.** В любом базисе $B$ при $k \geqslant 2$

$$\mathcal{L}_B^k(n) \sim \frac{2^n}{n}.$$

Теорема 1 показывает, что начиная с 2-х ярусов функция Шеннона асимптотически совпадает с аналогичной функцией для СФЭ (СФЭ можно рассматривать как формулу с неограниченным числом ярусов). Заметим, что [1]

$$\mathcal{L}_B^1(n) \sim \frac{2^n}{\log_2 n}.$$

Пусть $F = (f_1, \ldots, f_m)$ — оператор, зависящий от двух наборов переменных: $X = (x_1, \ldots, x_k)$ и $Y = (y_1, \ldots, y_l)$. Разложим $f_j$ в полином Жегалкина [8] по переменным $X$:

$$f_j = f_j^0 \oplus f_j^1 x_1 \oplus \ldots \oplus f_j^k x_k \oplus f_j',$$

где каждая из функций $f_j^i$ зависит только от $Y$, $f_j'$ — нелинейная по $X$ часть.

Пусть $M^1, \ldots, M^k,\ M_1, \ldots, M_m$ — множества функций, зависящих от переменных $Y$ и обладающих свойством: каждая функция $f_j^i$ вычислима через функции из множества $M^i \cup M_j$, т. е. представима в виде $h(g_1, \ldots, g_t)$, где $\{g_1, \ldots, g_t\} \subseteq M^i \cup M_j$, $h \in P_2$. Тогда набор $(M^1, \ldots, M^k;\ M_1, \ldots, M_m)$ назовём *$F$-таблицей.* Через $L'(F)$ обозначим минимум по всем $F$-таблицам суммы $\sum\limits_i |M^i| + \sum\limits_j |M_j|$.

**Теорема 2.** В любом базисе $B$

$$L_B^2(F) \geqslant L'(F).$$

**Следствие.** Пусть $F_n$ — любой из операторов: умножение матриц, умножение многочленов, циклическая свёртка; $n$ — число его входов. Тогда в любом базисе $B$

$$L_B^2(F_n) = \Omega(n^{3/2}).$$

Теорема 2 может быть обобщена [5,6] на класс СФЭ глубины 2 в базисе из всех булевых функций. Известные для этого класса нижние оценки вида $\Omega(n\frac{\ln^2 n}{\ln\ln n})$ следуют из результатов теории графов [10].

Пусть $F = (F_1, \ldots, F_k)$ — булев оператор, разбитый на $k$ операторов и зависящий от набора переменных $X = (X_1, \ldots, X_k)$, разбитого на $k$ наборов. Обозначим через $\mathcal{D}(F_i, X_j)$ множество подоператоров, полученных из $F_i$ при всевозможных подстановках констант вместо всех переменных, не входящих в набор $X_j$.

**Теорема 3.** Для любого базиса $B$ существует константа $c'_B$ такая, что для любого оператора $F$, существенно завясящего от всех переменных из $X$

$$L_B^2(F) \geqslant c'_B \sum_{i=1}^{k} \log_2 |\mathcal{D}(F_i, X_i)|.$$

Теорема 3 является обобщением метода Нечипорука для формул [2]. Она позволяет получать нижние оценки сложности вида $\Omega(\frac{n^2}{\log n})$, например, для оператора, состоящего из одинаковых функций Нечипорука (число функций равно числу переменных).

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

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

**Теорема 4.** [7] Пусть $B$ — базис, $\gamma > 1$. Тогда:

а) если

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

то для любого $k$

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

б) если базис $B$ обладает экспонентой сжатия (shrinkage exponent) [7,9] $\gamma$, то для любого $k$

$$L_B^k(\Lambda_n) = \Omega(n^{\varphi_k(\gamma)}).$$

Теорема 4 устанавливает связь между нижними и верхними оценками сложности функции $\Lambda_n$ в классе формул и соответствующими оценками в классе многоярусных формул. Заметим, что нижние оценки сложности функции $\Lambda_n$ в классе формул традиционно получаются с помощью метода Субботовской [3,4] и из подобного доказательства обычно извлекается информация о нижней оценке экспоненты сжатия.

Пусть $M^*$ — множество булевых функций, возрастающих или убывающих по каждой переменной. Для мер сложности $\mu_1$, $\mu_2$ обозначим через $\mu_1 \leqslant \mu_2$ отношение частичного порядка $\mu_1 = \mathcal{O}(\mu_2)$ (т. е. $\forall f \in P_2\ \mu_1(f) = \mathcal{O}(\mu_2(f))$).

**Теорема 5.** [7] а) Для любого базиса $B \subseteq M^*$ существует последовательность $k_1, k_2, \ldots$ такая, что

$$L_B^{k_1} > L_B^{k_2} > \ldots$$

б) Для базиса $B_0 = \{\&, \vee, \neg\}$

$$L_{B_0}^1 > L_{B_0}^2 > \ldots$$

в) Для каждого $k$ существует последовательность базисов $B_1, B_2 \ldots$ такая, что

$$L_{B_1}^k > L_{B_2}^k > \ldots$$

Теорема 5 следует из теоремы 4 и известных результатов об экспоненте сжатия для различных базисов [3,9].

**Теорема 6.** Для любого базиса $B$ и любых $k, l$

$$L_B^k = (L_B^l)^{\mathcal{O}(1)}.$$

Обозначим $\ln^{(s)}(x) = \ln\ln\ldots\ln(x)$, где число логарифмов равно $s$, $s \geqslant 0$. Скажем, что меры сложности $\mu_1$ и $\mu_2$ $s$-эквивалентны, если

$$\exists C\ \forall f \in P_2\ |\ln^{(s)}(\mu_1(f)) - \ln^{(s)}(\mu_2(f))| \leqslant C.$$

Скажем, что меры *слабо* эквивалентны, если для некоторого $s$ они $s$-эквивалентны.

Заметим, что 1-эквивалентность есть совпадение по порядку (это отношение исследуется в теореме 5), 2-эквивалентность есть полиномиальная эквивалентность (как в теореме 6). Можно показать, что меры сложности многоярусных формул и контактно-вентильных схем (а также их ограничений — контактных схем, ветвящихся программ и т. д.) 3-эквивалентны. В то же время, вопрос о слабой эквивалентности этих мер с мерой сложности СФЭ является открытым.

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).

## Список литературы

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

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

[3] Перязев Н. А. Сложность представлений булевых функций формулами в немонолинейных базисах. Дискретная математика и информатика. Вып. 2. — Иркутск: Изд-во Иркут. ун-та, 1995.

[4] Субботовская Б. А. О реализации линейных функций формулами в базисе $\vee, \&, -$. ДАН СССР. 1961. Т. 136, N. 3. с. 784–787.

[5] Черухин Д. Ю. О схемах из функциональных элементов с ограниченной глубиной ветвления // Докл. РАН. Т. 405, N. 4. 2005. с. 467–470.

[6] Черухин Д. Ю. Нижняя оценка сложности в классе схем глубины 2 без ограничений на базис // Вестн. МГУ. Сер. 1. N 4. 2005. с. 54–56.

[7] Черухин Д. Ю. О схемах из функциональных элементов конечной глубины ветвления // Дискретная математика. Т. 18, вып. 4. 2006. с. 73–83.

[8] Яблонский С. В. Введение в дискретную математику. М.: Наука, 1986.

[9] Hastad J. The shrinkage exponent of de Morgan formulas is 2. SIAM J. Comput. 1998. V. 27. p. 48–64.

[10] 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.