УДК 519.714 Математика

О схемах из функциональных элементов с ограниченной глубиной ветвления

Д. Ю. Черухин

Аннотация

Рассмотрена модель булевых вычислений, промежуточная между схемами из функциональных элементов (СФЭ) и формулами, а именно, схемы с конечным числом ярусов ветвления (многоярусные схемы). Свойства данной модели двояки: с одной стороны, уже для двухярусных схем справедлив принцип параметризации — частный случай принципа локального кодирования, характерного для СФЭ; с другой стороны, в некоторых базисах при любом константном ограничении на число ярусов можно получить эффективные нижние оценки сложности функций методами, характерными для формул. В модели двухярусных схем в произвольном базисе предложен новый метод получения нижних оценок сложности операторов.

1. Основные определения. Функция вида $f\colon \{0,1\}^n \to \{0,1\}$ называется *булевой*; вектор-функцию вида $F\colon \{0,1\}^n \to \{0,1\}^m$ будем называть булевым (n,m)-*оператором.* Произвольная полная [1] система булевых функций называется *базисом.* Обозначим: $B_0 = \{\&, \vee, \neg\}$, $P_2(n) = \{f\colon \{0,1\}^n \to \{0,1\}\}$, $P_2 = \bigcup_{n \geqslant 0} P_2(n)$. Множества B_0, $P_2(n)$ при $n \geqslant 2$, P_2 являются базисами.

Схемой из функциональных элементов (*СФЭ*, [2, 1, 3]) в базисе B называется набор $S = (\Gamma, \mathbb{I}, \mathbb{O}, \psi, \rho)$, для которого выполнены условия: Γ — конечный ориентированный граф без ориентированных циклов [1] с множеством вершин V и множеством рёбер E; $\mathbb{I} \subseteq V^n$, $\mathbb{O} \subseteq V^m$ для некоторых n, m ($\mathbb{I}, \mathbb{O}$ — наборы, соответственно, *входов* и *выходов* схемы); элементы набора $\mathbb{I}$ попарно различны; $\psi\colon V \backslash V' \to B$, где V' — множество входов (ψ сопоставляет каждому *элементу*, т. е. вершине, отличной от входов, функцию из базиса B); $\rho \subseteq E^2$ — отношение полного порядка на множестве рёбер (необходимое для указания порядка следования рёбер, входящих в каждую вершину); кроме того, ни в один из входов схемы не входит ни одного ребра и число рёбер, входящих в вершину v, отличную от входов, равно арности функции $\psi(v)$.

Каждой вершине $v \in V$ поставим в соответствие функцию $f_v \in P_2(n)$, *вычисляемую* в вершине v. Пусть $\mathbb{I} = (v_1, \ldots, v_n)$. Для каждого $i = 1, \ldots, n$ положим $f_{v_i}(\tilde{x}) \equiv x_i$, где $\tilde{x} = (x_1, \ldots, x_n)$. Далее действуем по индукции, используя отсутствие ориентированных циклов. Пусть в вершину v входят рёбра $e_1, \ldots, e_k$ (записанные в порядке ρ), ведущие, соответственно, из вершин $u_1, \ldots, u_k$, для которых функции $f_{u_1}, \ldots, f_{u_k}$ уже определены. Тогда положим $f_v(\tilde{x}) \equiv \psi(v)(f_{u_1}(\tilde{x}), \ldots, f_{u_k}(\tilde{x}))$. Наконец, если $\mathbb{O} = (w_1, \ldots, w_m)$, то скажем, что схема S *вычисляет* оператор $(f_{w_1}, \ldots, f_{w_m})$.

Ветвлением вершины v называется сумма числа рёбер, выходящих из v, и числа вхождений вершины v в набор $\mathbb{O}$. Вершина v называется *узловой*, если либо v является входом, либо ветвление v больше единицы. *Глубиной ветвления* схемы S называется максимальное число узловых вершин, содержащихся в одном ориентированном пути в Γ. Схемы глубины ветвления 1 естественным образом соответствуют формулам [3]. В настоящей заметке изучаются схемы с глубиной ветвления, ограниченной заданным числом d (схемы с d *ярусами* ветвления, d-ярусные схемы).

Введём две меры сложности схем: через $L(S)$ обозначим число элементов в S, через $\mathcal{L}(S)$ — сумму ветвлений узловых вершин. Мера сложности L традиционна для СФЭ, $\mathcal{L}$ более естественна для формул; в случае конечного базиса B меры L и $\mathcal{L}$ отличаются не более чем в константу раз. Через $D(S)$ обозначим *глубину* схемы S, т. е. максимальную длину ориентированного пути в Г. Заметим, что схемам глубины ветвления d в базисе B соответствуют схемы глубины d в базисе $[B]$, состоящем из всех функций, бесповторно выразимых [4] в B.

Пусть $d \in \mathbb{N} \cup \{\infty\}$. Для произвольного булева оператора F через $L_B^d(F)$ $[\mathcal{L}_B^d(F)$, $D_B(F)]$ обозначим соответственно минимум выражения $L(S)$ $[\mathcal{L}(S)$, $D(S)]$, взятый по всем схемам S, вычисляющим оператор F и имеющим глубину ветвления, не превосходящую d (заметим, что $D_B(F)$ не зависит от d). Наконец, если $\mathcal{F} \subseteq P_2$, то через $L_B^d(\mathcal{F})$ обозначим максимум выражения $L_B^d(f)$ по всем $f \in \mathcal{F}$.

2. Асимптотические оценки сложности. Для произвольного набора $\tilde{\alpha} \in \{0,1\}^n$, $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$, обозначим $N(\tilde{\alpha}) = \sum_{i=1}^n \alpha_i 2^{n-i}$. Введём обозначения: $A_{n,k} = \{\tilde{\alpha} \in \{0,1\}^n \mid N(\tilde{\alpha}) < k\}$, $J(x) = \frac{x}{\log_2 x}$.

Теорема 1. *Пусть для каждого n дано $\mathcal{F}_n \subseteq P_2(n)$ и существуют такие числа m_n, k_n, $2^{m_n - 1} < k_n \leqslant 2^{m_n}$, и оператор F_n: $\{0,1\}^n \to A_{m_n,k_n}$, что при $n \to \infty$ выполнено:*

1) $\forall f \in \mathcal{F}_n$ $\exists g$: $\{0,1\}^{m_n} \to \{0,1\}$ $f = g \circ F_n$;

2) $D_{B_0}(F_n) = o(m_n)$;

3) $k_n \sim \log_2 |\mathcal{F}_n|$;

4) $J(\log_2 |\mathcal{F}_n|) = \omega(n)$.

Тогда $L_{B_0}^2(\mathcal{F}_n) \sim J(\log_2 |\mathcal{F}_n|)$, $n \to \infty$.

Теорема 1 даёт принцип параметризации — ослабленный вариант принципа локального кодирования, справедливого для СФЭ [5]. Нижняя оценка в теореме 1 следует из аналогичной оценки для СФЭ, верхняя строится с использованием метода Лупанова [3]. Почти вся сложность в построенной схеме сосредоточена в блоке, вычисляющем дизъюнкции, поэтому, используя технику обобщенного разложения [3], теорему 1 несложно распространить на произвольный конечный базис. Заметим также, что с увеличением глубины ветвления принцип локального кодирования справедлив в большей мере: например, в трёхярусных схемах может быть промоделирована конструкция кодирование-вычисление-декодирование.

Следствие 1. $L_{B_0}^2(P_2(n)) \sim \frac{2^n}{n}$, $n \to \infty$.

Заметим, что $L_{B_0}^{\infty}(P_2(n)) \sim \frac{2^n}{n}$, $\mathcal{L}_{B_0}^1(P_2(n)) \sim \frac{2^n}{\log_2 n}$ [3]. Обозначим через $S_{n,k}$ множество всех *k-слой* функций, т. е. функций от n переменных, равных 1, если число единиц среди аргументов больше k и равных 0, если число единиц меньше k.

Следствие 2. *Если $n \to \infty$, $k \to \infty$ и $(n-k) \to \infty$, то $L_{B_0}^2(S_{n,k}) \sim J(C_n^k)$.*

Аналогичная оценка справедлива для класса частичных функций, определённых на k-м слое. Некоторые результаты можно получить независимо от теоремы 1. Пусть $T_{n,k}$ — множество функций от n переменных, равных единице в k точках.

Теорема 2. *Если $n \to \infty$ и $\log_2 n \leqslant k \leqslant 2^{n/2}$, то $L_{B_0}^2(T_{n,k}) \asymp J(\log_2 C_{2^n}^k)$; если, дополнительно, $\frac{\log_2 k}{\log_2 n} \to \infty$, $\frac{\log_2 k}{n} \to 0$, то $L_{B_0}^2(T_{n,k}) \sim J(\log_2 C_{2^n}^k)$.*

3. Эффективные оценки сложности. Всюду далее базисы $B, B_1, B_2, \ldots$ считаем конечными. Обозначим $\Lambda_n = x_1 \oplus \ldots \oplus x_n$, $\varphi_d(x) = \frac{1}{1-(1-1/x)^d}$.

Теорема 3. *Пусть B — базис, $\gamma > 1$. Тогда, если $L_B^1(\Lambda_n) = \mathcal{O}(n^{\gamma})$, $n \to \infty$, то для любого $d < \infty$ при $n \to \infty$ выполнено $L_B^d(\Lambda_n) = \mathcal{O}(n^{\varphi_d(\gamma)})$.*

Пусть f: $\{0,1\}^n \to \{0,1\}$, $A \in \{0,1,*\}^n$. Обозначим через $|A|$ число элементов $0,1$ в наборе A, через $f|_A$ — функцию, полученную из f фиксацией тех переменных, на местах которых в наборе A стоит 0 или 1, соответствующей константой из A. Введём меру сложности L^*_B: если f тождественно равна константе или функции одного аргумента, то $L^*_B(f) = 0$, иначе $L^*_B(f) = L^1_B(f)$. Скажем, что базис B обладает *экспонентой сжатия* γ [6], если для любой $f \in P_2(n)$ при $n \to \infty$, $m \geqslant 1$, $m = o(n)$, выполнено

$$L^*_B(f) = \Omega\Big(\Big(\frac{n}{m}\Big)^\gamma\Big)\frac{1}{2^{n-m}C_n^m}\sum_{A,|A|=n-m} L^*_B(f|_A).$$

Теорема 4. *Если базис B обладает экспонентой сжатия γ, то для любого $d < \infty$ при $n \to \infty$ имеет место $L^d_B(\Lambda_n) = \Omega(n^{\varphi_d(\gamma)})$.*

Теоремы 3, 4 показывают, что оценки сложности линейной функции в классе многоярусных схем можно получить из соответствующих оценок в классе формул. Базис B назовём *обобщенно-монотонным* (*ОМ*-базисом), если любая функция из B нестрого возрастает или убывает по каждому своему аргументу. Известно [7], что экспонента сжатия базиса B больше единицы тогда и только тогда, когда B является ОМ-базисом. Таким образом, теорема 4 позволяет получать нелинейные нижние оценки для любого $d \geqslant 1$ и любого ОМ-базиса B. Доказательльство нелинейных нижних оценок при $d = 2$ в случае не ОМ-базиса, по-видимому, представляет трудность. В этом случае известны нелинейные нижние оценки для (n,n)-операторов [8, 9, 10]. Наибольшая из них имеет вид $\Omega(n\frac{\ln^2 n}{\ln\ln n})$ и следует из результатов теории графов [9].

Пусть $F = (f_1, \dots, f_m)$ и каждая из функций f_j, $1 \leqslant j \leqslant m$, зависит от двух наборов переменных: $\tilde{x} = (x_1, \dots, x_k)$ и $\tilde{y} = (y_1, \dots, y_l)$, $n = k + l$. Разложим f_j в полином Жегалкина [1] по переменным $\tilde{x}$: $f_j = f^0_j \oplus f^1_j x_1 \oplus \ldots \oplus f^k_j x_k \oplus f'_j$, где функция f^i_j, $0 \leqslant i \leqslant k$, зависит от $\tilde{y}$, f'_j — нелинейная по $\tilde{x}$ часть. Набор $(M^1, \dots, M^k;\ M_1, \dots, M_m)$ назовём *F-таблицей*, если M^i $(i = 1, \dots, k)$ и M_j $(j = 1, \dots, m)$ — множества функций от переменных $\tilde{y}$ и каждая функция f^i_j вычислима через функции из множества $M^i \cup M_j$, т. е. представима в виде $h(g_1, \dots, g_t)$, где $\{g_1, \dots, g_t\} \subseteq M^i \cup M_j$, $h \in P_2$. Через $L'(F)$ обозначим минимум (по всем F-таблицам) суммы $\sum_i |M^i| + \sum_j |M_j|$.

Теорема 5. $\mathcal{L}^2_{P_2}(F) \geqslant L'(F)$.

Пусть MMUL_n — оператор произведения двух матриц размера $q \times q$ над полем $\mathbb{Z}_2$, $k = l = m = q^2$, $n = 2q^2$.

Следствие 3. *Если B — не ОМ-базис, то $L^2_B(\mathrm{MMUL}_n) \asymp n^{3/2}$, $n \to \infty$.*

С помощью теоремы 5 также можно получить нижние оценки сложности вида $\Omega(n^{3/2})$ для операторов циклической свёртки и произведения многочленов над $\mathbb{Z}_2$.

4. Сравнение мер сложности. Мерой сложности будем называть произвольную функцию μ: $P_2 \to \mathbb{R}_+$. Обозначим $\ln^{(s)}(x) = \ln\ln\ldots\ln(x)$, где число логарифмов равно s, $s \geqslant 0$. Введём отношения *s-предшествования* $(\leqslant_s)$ и *слабого предшествования* $(\leqslant_\infty)$ мер сложности:

$$\mu_1 \leqslant_s \mu_2 \iff \exists C\ \forall f \in P_2\ \ln^{(s)}(\mu_1(f)) - \ln^{(s)}(\mu_2(f)) \leqslant C,$$
$$\mu_1 \leqslant_\infty \mu_2 \iff \exists s\ \mu_1 \leqslant_s \mu_2,$$

где неравенства рассматриваются на области определения функции $\ln^{(s)}(x)$. Отношение $\leqslant_s$ $(s \in \mathbb{Z}_+ \cup \{\infty\})$ порождает отношения строгого порядка $<_s$ и эквивалентности $\sim_s$. Отношение $\sim_1$ означает совпадение по порядку, $\sim_2$ — полиномиальную эквивалентность; если между мерами есть экспоненциальный разрыв, то они не слабо эквивалентны.

Теорема 6. *а) Для любого ОМ-базиса B существует последовательность $d_1, d_2, \ldots$ такая, что $L_B^{d_1} >_1 L_B^{d_2} >_1 \ldots$;*

б) $L_{B_0}^1 >_1 L_{B_0}^2 >_1 \ldots$;

в) $\forall d < \infty\ \exists (B_1, B_2, \ldots)\ L_{B_1}^d >_1 L_{B_2}^d >_1 \ldots$

Теорема 6 следует из теорем 3, 4, оценок экспоненты сжатия базисов [6, 11] и неравенств $L_B(\Lambda_n) = \mathcal{O}(n^2)$ [2, стр. 82], [4]. При $d = 1$ утверждение п. в) теоремы 6 было получено в [12].

Теорема 7. *Для любого B*

а) $\forall d < \infty\ \exists C\ \forall f\ L_B^1(f) \leqslant C(L_B^d(f))^d$;

б) $\exists (f_1, f_2, \ldots)\ L_B^2(f_n) = \mathcal{O}(n)$, $L_B^1(f_n) = \Omega(\frac{n^2}{\ln n})$, $n \to \infty$.

Следствие 4. *Если $d_1, d_2 < \infty$ и B_1, B_2 — базисы, то $L_{B_1}^{d_1} \sim_2 L_{B_2}^{d_2}$.*

Соотношения $L_{B_1}^1 \sim_2 L_{B_2}^1$ известны [13]. Пусть $RS(f)$ — наименьшее число контактов в контактно-вентильной схеме, вычисляющей функцию f [14]. Можно показать, что $RS \sim_3 L_{B_0}^1$. Вопрос о слабой эквивалентности мер $L_{B_0}^1$ и $L_{B_0}^\infty$, по-видимому, открыт.

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).

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

[2] Шеннон К. Э. Работы по теории информации и кибернетике. — М.: ИЛ, 1963.

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

[4] Субботовская Б. А. О сравнении базисов при реализации функций алгебры логики формулами. *ДАН СССР.* — 1963. — **149**, 4. — 784–787.

[5] Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования. *Проблемы кибернетики.* Вып. 14. — М.: Наука, 1965. — 31–110.

[6] Hastad J. The shrinkage exponent of de Morgan formulas is 2. *SIAM J. Comput.* — 1998. — **27**. — 48–64.

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

[8] Pudlak P., Savicky P. On shifting networks. *Theoretical Comput. Sci.* — 1993. — **116**. — 415–419.

[9] Radhakrishnan J., Ta-Shma A. Bounds for dispersers, extractors, and depth-two superconcentrators. *SIAM J. of Discrete Mathematics.* — 2000. — **13**, 1. — 2–24.

[10] Raz R., Shpilka A. Lower bounds for matrix product, in bounded depth circuits with arbitrary gates *SIAM J. Comput.* — 2003. — **32**, 2. — 488–513.

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

[12] Черухин Д. Ю. О сравнении булевых базисов. *Докл. РАН.* — 1999. — **367**, 6. — 742–743.

[13] Spira Ph. M. On time-hardware complexity tradeoffs for Boolean functions. — *Proc. of 4-th Hawaii Internat. Symb. on System Sciences.* — 1971. —525–527.

[14] Окольнишникова Е. А. О сложности ветвящихся программ. — *Математические вопросы кибернетики.* Вып. 10. — М.: Наука, 2001. — 69–82.