УДК 519.714

НИЖНЯЯ ОЦЕНКА СЛОЖНОСТИ В КЛАССЕ СХЕМ ГЛУБИНЫ 2 БЕЗ ОГРАНИЧЕНИЙ НА БАЗИС

Д. Ю. Черухин

Рассмотрены схемы из функциональных элементов глубины 2 в базисе, состоящем из всех булевых функций. Получена нижняя оценка сложности $\Omega(n^{3/2})$ для эффективно заданного (n,n)-оператора.

Трудности, возникшие на пути получения высоких нижних оценок сложности схем из функциональных элементов, привели многих исследователей к рассмотрению схем с ограничениями [1]. Одним из возможных ограничений является ограничение на глубину схемы. Под глубиной будем понимать длину максимального ориентированного пути, соединяющего некоторый вход с некоторым выходом схемы.

Вэльянт предложил [2] ограничить глубину величиной $O(\log n)$ и получить в этом классе схем нелинейную нижнюю оценку сложности, т. е. доказать, что либо сложность некоторого (эффективно заданного) оператора нелинейна, либо его глубина нелогарифмична (проблема до сих пор не решена). В качестве подхода к решению данной проблемы Вэльянт предложил редукцию, сводящую схемы глубины $O(\log n)$ к схемам глубины 2: из достаточно высокой нижней оценки для схем глубины 2 специального вида следует нелинейная нижняя оценка для схем глубины $O(\log n)$.

В данной заметке мы рассмотрим класс K_2 схем глубины 2 в базисе P_2, состоящем из всех булевых функций. Весом элемента является число его входов, сложность схемы определяется как сумма весов элементов. Схема, полученная в результате редукции Вэльянта, принадлежит классу K_2, таким образом, представляет интерес исследование класса K_2. В классе K_2 сложность отдельной булевой функции равна числу её существенных переменных; нетривиальность состоит в оценке сложности операторов. Наибольшая возможная сложность оператора ограничена величиной $O(n^2)$.

Нелинейные нижние оценки сложности в классе K_2 извлекаются из теоретико-графовых рассуждений [3–6]. Например, для некоторого (n,n)-оператора F доказано, что любая схема, вычисляющая F, содержит n-суперконцентратор (граф специального вида, [3,5,7,8]). Отсюда следует, что сложность оператора F не меньше наименьшей сложности (числа рёбер) суперконцентратора. Существуют суперконцентраторы сложности $O(n)$ [7] и, одновременно, глубины $O(\log n)$ [8]. Если же ограничиться глубиной 2, то наименьшая сложность суперконцентратора нелинейна [3] и равна [5]

$$\Theta\Big(n\frac{\log^2 n}{\log\log n}\Big). \tag{1}$$

В работах [4,6] использовалось теоретико-графовое свойство, более слабое, чем наличие суперконцентратора. Таким образом, известные нижние оценки сложности в классе K_2 не превосходят величины (1). В данной заметке получена нижняя оценка сложности вида $\Omega(n^{3/2})$.

Отметим, что в ряде работ были доказаны высокие (в том числе экспоненциальные) нижние оценки сложности в классе схем ограниченной глубины при наличии ограничений на базис [1].

Пусть $\tilde{x} = (x_1, \ldots, x_n)$, $\tilde{y} = (y_1, \ldots, y_n)$, $\tilde{z} = (z_1, \ldots, z_n)$. Рассмотрим оператор *циклической свёртки* $\mathrm{CCONV}_n \colon (\tilde{x}, \tilde{y}) \mapsto \tilde{z}$, где

$$z_j = \bigoplus_{i+k\equiv j \,(\mathrm{mod}\, n)} x_i y_k, \qquad j = 1, \ldots, n. \tag{2}$$

Через $L_2(F)$ будем обозначать сложность оператора F в классе K_2.

Теорема 1.

$$L_2(\mathrm{CCONV}_n) = \Omega(n^{3/2}), \quad n \to \infty.$$

Доказательство. Рассмотрим схему S из класса K_2, вычисляющую оператор CCONV_n и имеющую минимальную сложность. Увеличив сложность схемы S не более чем в 2 раза, можно получить схему S', в которой любой ориентированный путь, соединяющий произвольные вход и выход, имеет длину 2. Обозначим через $w_1, \ldots, w_p$ все вершины схемы S', находящиеся на расстоянии 1 от входов. Пусть $g_l(\tilde{x}, \tilde{y})$, $1 \leqslant l \leqslant p$, — функция, вычисляемая в вершине w_l, а $h_j(\tilde{x}, \tilde{y})$, $1 \leqslant j \leqslant n$, — функция, вычислимая на j-м выходе схемы.

Произвольную функцию $f(\tilde{x}, \tilde{y})$ можно разложить в *полином Жегалкина по переменным* $\tilde{x}$, а именно, единственным образом представить в виде

$$f(\tilde{x}, \tilde{y}) \equiv f^0(\tilde{y}) \oplus f^1(\tilde{y})x_1 \oplus \ldots \oplus f^n(\tilde{y})x_n \oplus f'(\tilde{x}, \tilde{y}), \tag{3}$$

где каждое слагаемое функции f' содержит хотя бы две из переменных $\tilde{x}$. Для произвольной функции $f(\tilde{x}, \tilde{y})$ будем обозначать через f^i $(0 \leqslant i \leqslant n)$ соответствующую функцию из (3).

Будем говорить, что функция φ *вычислима* через функции $\varphi_1, \ldots, \varphi_s$, если для некоторой функции F выполнено тождество

$$\varphi(\tilde{y}) \equiv F(\varphi_1(\tilde{y}), \ldots, \varphi_s(\tilde{y})).$$

Обозначим через G_i $[H_j]$ множество индексов l таких, что i-й вход [j-й выход] схемы S' соединён ребром с вершиной w_l $(1 \leqslant i, j \leqslant n)$. Функция h_j^i вычислима через функции из множества $\{g_l^i, g_l^0 \mid l \in H_j\}$. Действительно, любая булева функция представима полиномом над $\mathbb{Z}_2$, а коэффициент при переменной x_i результата сложения или умножения функций можно выразить через коэффициенты при переменной x_i и свободные члены операндов. Далее, если $l \notin G_i$, то функция g_l не зависит от переменной x_i, следовательно, $g_l^i \equiv 0$. Тогда h_j^i можно вычислить через функции из множества $U_i \cup V_j$, где

$$U_i = \{g_l^i \mid l \in G_i\}, \quad V_j = \{g_l^0 \mid l \in H_j\}.$$

Для упрощения доказательства будем считать, что $n = m^2$. Введём множества индексов

$$X_t = \{tm - m + 1, \ldots, tm\}, \quad Z_t = \{t, t + m, \ldots, t + m^2 - m\}, \quad t = 1, \ldots, m.$$

Очевидно, $X_1 \sqcup \ldots \sqcup X_m = Z_1 \sqcup \ldots \sqcup Z_m = \{1, \ldots, n\}$. В силу определения (2) и единственности разложения (3) имеем

$$h_j^i \equiv y_k, \quad \text{где } k \equiv j - i \pmod{n}. \tag{4}$$

Заметим, что если индекс i пробегает множество X_t, а индекс j — множество Z_t, то индекс k, вычисляемый через i, j согласно (4), пробегает все числа от 1 до n. Таким образом, множество

$$Q_t = \{h_j^i \mid i \in X_t,\ j \in Z_t\}$$

содержит функции, равные всем переменным из набора $\tilde{y}$. Следовательно, через функции из Q_t может быть вычислена любая функция от переменных $\tilde{y}$.

В свою очередь, множество функций Q_t может быть вычислено через множество

$$R_t = \Big(\bigcup_{i\in X_t} U_i\Big) \cup \Big(\bigcup_{j\in Z_t} V_j\Big).$$

Отсюда следует, что $|R_t| \geqslant n$. Действительно, каждая функция $\varphi \in R_t$ порождает на своей области определения $\{0,1\}^n$ отношение эквивалентности с классами $\varphi^{-1}(0)$ и $\varphi^{-1}(1)$. Пересечение отношений, соответствующих функциям из R_t содержит не более, чем $2^{|R_t|}$ классов эквивалентности. Если $|R_t| < n$, то найдутся два набора $\tilde{\alpha}, \tilde{\beta} \in \{0,1\}^n$ принадлежащие одному классу. Тогда равенство $\varphi(\tilde{\alpha}) = \varphi(\tilde{\beta})$ верно для любой функции $\varphi \in R_t$, а значит, и для любой функции, вычислимой через множество R_t. Но через R_t можно вычислить произвольную функцию от переменных $\tilde{y}$. Противоречие.

Итак, для любого t имеем

$$n \leqslant |R_t| \leqslant \sum_{i\in X_t} |U_i| + \sum_{j\in Z_t} |V_j| \leqslant \sum_{i\in X_t} |G_i| + \sum_{j\in Z_t} |H_j|.$$

Суммируя по всем t, и учитывая, что сложность схемы равна числу рёбер, получим

$$nm \leqslant \sum_t \Big(\sum_{i\in X_t} |G_i| + \sum_{j\in Z_t} |H_j|\Big) = \sum_{i=1}^{n} |G_i| + \sum_{j=1}^{n} |H_j| = L(S').$$

Теорема доказана.

Аналогичными рассуждениями можно получить оценку $\Omega(n^{3/2})$ для обычной свёртки, т. е. оператора, выражающего коэффициенты произведения многочленов из $\mathbb{Z}_2[x]$ через коэффициенты сомножителей. Также можно получить оценку $\Omega(n^3)$ для оператора произведения матриц размера $n \times n$.

Исследование выполнено при финансовой поддержке программы поддержки ведущих научных школ РФ (проект НШ–1807.2003.01). программы "Университеты России" (проект УР 04.03.061) и РФФИ (проект 02–01–00985).

СПИСОК ЛИТЕРАТУРЫ

1. *Нигматуллин Р.Г.* Сложность булевых функций. М.: Наука, 1991.
2. *Valiant L.* Graph-theoretic arguments in low-level complexity // Lecture Notes in Computer Science. 1977. **53**. 162–176.
3. *Pippenger N.* Superconcentrators of depth 2 // J. of Computer and System Sciences. 1982. **24**. 82–90.
4. *Pudlak P., Savicky P.* On shifting networks // Theoretical Comput. Sci. 1993. **116**. 415–419
5. *Radhakrishnan J., Ta-Shma A.* Tight bounds for depth-two superconcentrators // Proc. 38-th FOCS. 1997. 585–594.
6. *Raz R., Shpilka A.* Lower bounds for matrix product, in bounded depth circuits with arbitrary gates // SIAM J. Comput. 2003. **32(2)**. 488–513.
7. *Valiant L.* Graph-theoretic properties in computational complexity // J. of Computer and System Sciences. 1976. **13**. 278–285.
8. *Pippenger N.* Superconcentrators // SIAM J. Comput. 1977. 298–304.