МЕТОД НЕЧИПОРУКА ДЛЯ ДВУХЯРУСНЫХ СХЕМ

Д.Ю. Черухин[1]

[1]МГУ, мехмат, ЛВМ, Ленинские горы, 119992 Москва, Россия d.cherukhin@mail.ru

Работа относится к области получения высоких нижних оценок сложности для явно заданных булевых функций. Исследуется подкласс схем из функциональных элементов (СФЭ, [1]) — схемы с конечным числом ярусов ветвления [2]. Вершина схемы обладает ветвлением, если она является входом или результат вычисления в ней используется в дальнейшем более одного раза. Схема имеет k ярусов ветвления (является k-СФЭ), если любой ориентированный путь в ней содержит не более k вершин, обладающих ветвлением. Сложность СФЭ есть число элементов; меру сложности для k-СФЭ в базисе B обозначим через L_B^k.

Класс k-СФЭ интересен тем, что он является промежуточным между формулами и СФЭ. С одной стороны, при $k \geqslant 2$, асимптотика сложности почти всех функций совпадает с асимптотикой для СФЭ (1-СФЭ являются формулами). С другой стороны, на класс k-СФЭ можно распространить некоторые методы получения нижних оценок, характерные для формул.

Если базис содержит только функции, монотонные или антимонотонные по каждой переменной, то, обобщая метод Субботовской, для любого k можно получить нижнюю оценку вида n^{1+c} для функции $x_1 \oplus \ldots \oplus x_n$ [3]. Если базис не обладает данным свойством, то при $k \geqslant 2$ нелинейные нижние оценки для функций неизвестны. В данной работе, в случае $k = 2$ и произвольного конечного базиса B, предложен метод получения нижних оценок вида $n^{2-o(1)}$ для булевых операторов, являющийся обобщением метода Нечипорука [4] для формул. Ранее в данной модели автором была получена нижняя оценка $n^{3/2}$ [2]. Наибольшая известная оценка до результатов автора — $n \log^2 n / \log\log n$ [5].

Пусть $\tilde{f}\colon \{0,1\}^n \to \{0,1\}^m$ — булев оператор, множества его входов и выходов разбиты на p частей: $\tilde{x} = (\tilde{x}^1, \ldots, \tilde{x}^p)$, $\tilde{f} = (\tilde{f}^1, \ldots, \tilde{f}^p)$, и каждый из наборов $\tilde{x}^i$ содержит хотя бы одну существенную переменную для $\tilde{f}$. Обозначим через $\mathcal{D}(\tilde{f}, \tilde{x}^i)$ множество подоператоров, полученных из оператора $\tilde{f}$ при всевозможных подстановках констант вместо всех его переменных, не входящих в набор $\tilde{x}^i$. Положим $I(\tilde{f}, \tilde{x}^i) = \log_2 |\mathcal{D}(\tilde{f}, \tilde{x}^i)|$. При $m = 1$ существует такая константа c_B, что для любой функции f выполнено (метод Нечипорука):

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

Теорема. *Существует такая константа c'_B, что для любого оператора $\tilde{f}$ выполнено*

$$L_B^2(\tilde{f}) \geqslant c'_B \sum_{i=1}^{p} I(\tilde{f}^i, \tilde{x}^i).$$

Доказательство. Рассмотрим 2-СФЭ S минимальной сложности, реализующую оператор $\tilde{f}$. Пусть $g_1, \ldots, g_q$ — элементы, обладающие ветвлением, отличные от входов; $f_1, \ldots, f_m$ — выходы схемы (для удобства отождествляем вершину с вычисляемой в ней функцией от переменных $\tilde{x}$). Пусть G_l — подсхема схемы S, выходом которой является g_l; F_j — подсхема с выходом f_j, входами которой являются элементы $g_1, \ldots, g_q$. Подсхемы $G_1, \ldots, G_q$, $F_1, \ldots, F_m$ являются формулами и не пересекаются за исключением своих входов и выходов.

Обозначим через X_l множество таких индексов i, что хотя бы одна переменная из набора $\tilde{x}^i$ существенна для функции g_l. Положим $X'_i = \{l \mid i \in X_l\}$. Через Y_i обозначим множество тех индексов l, для которых элемент g_l используется при вычислении хотя бы одной функции из набора $\tilde{f}^i$. Наконец, пусть Y'_j — множество таких l, что g_l используется при вычислении функции f_j. Схема G_l является формулой, поэтому из (1) следует

$$L^1_B(G_l) \geqslant L^1_B(g_l) \geqslant c_B \sum_{i\colon i\in X_l} I(g_l, \tilde{x}^i). \tag{2}$$

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 $(g_l)_{l\in Y_i}$, мы получим набор их подфункций $(g'_l)_{l\in Y_i}$, $g'_l \in \mathcal{D}(g_l, \tilde{x}^i)$. Указанное соответствие $\tilde{f}' \mapsto (g'_l)_{l\in Y_i}$ инъективно: из двух равных наборов подфункций, производя одни и те же вычисления, мы получим равные подоператоры оператора $\tilde{f}$. Таким образом,

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

Следовательно,

$$I(\tilde{f}^i, \tilde{x}^i) \leqslant \sum_{l\in Y_i} I(g_l, \tilde{x}^i). \tag{3}$$

Заметим, что если $l \notin X'_i$, т. е. $i \notin X_l$, 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,

$$\sum_{l\in Y_i\setminus X'_i} I(g_l, \tilde{x}^i) \leqslant |Y_i \setminus X'_i| \leqslant |Y_i|. \tag{4}$$

Поскольку формуле F_j соответствует дерево с множеством листьев Y'_j, в котором степени вершин ограничены сверху, то для некоторой константы c''_B выполнено

$$|Y'_j| \leqslant c''_B L^1_B(F_j). \tag{5}$$

Из (2)–(5) для некоторой константы c'_B получим

$$\sum_{i=1}^{p} I(\tilde{f}^i, \tilde{x}^i) \leqslant \sum_{i,l\colon l\in Y_i} I(g_l, \tilde{x}^i) = \sum_{i,l\colon l\in Y_i\cap X'_i} I(g_l, \tilde{x}^i) + \sum_{i,l\colon l\in Y_i\setminus X'_i} I(g_l, \tilde{x}^i) \leqslant$$

$$\leqslant \sum_{i,l\colon l\in X'_i} I(g_l, \tilde{x}^i) + \sum_{i=1}^{p} |Y_i| \leqslant \sum_{l,i\colon i\in X_l} I(g_l, \tilde{x}^i) + \sum_{j=1}^{m} |Y'_j| \leqslant$$

$$\leqslant \frac{1}{c_B} \sum_{l=1}^{q} L^1_B(G_l) + c''_B \sum_{j=1}^{m} L^1_B(F_j) \leqslant \frac{1}{c'_B} L^2_B(S) = \frac{1}{c'_B} L^2_B(\tilde{f})$$

Теорема доказана. Для получения оценки $n^{2-o(1)}$ достаточно применить теорему к оператору, состоящему из n экземпляров функции Нечипорука [4].

Литература

1. Лупанов О. Б. *Асимптотические оценки сложности управляющих систем.* М.: МГУ, 1984.

2. Черухин Д. Ю. *О схемах из функциональных элементов с ограниченной глубиной ветвления* // Докл. РАН. 2005. Т. 405. №4. С. 467–470.

3. Черухин Д. Ю. *О схемах из функциональных элементов конечной глубины ветвления* // Дискретная математика. 2006. Т. 18. вып. 4. С. 73–83.

4. Нечипорук Э. И. *Об одной булевской функции* // ДАН СССР. 1966. Т. 169. №4. С. 765–766.

5. Radhakrishnan J., Ta-Shma A. *Bounds for dispersers, extractors and depth-two superconcentrators* // SIAM J. of Discrete Mathematics. 2000. V. 13 (1). P. 2–24.