О СХЕМАХ ГЛУБИНЫ 2 В БАЗИСЕ P_2

Д. Ю. Черухин (Москва)

Рассматривается класс схем из функциональных элементов глубины 2 в базисе P_2, состоящем из всех булевых функций. Сложностью схемы будем считать число рёбер. Сложность оператора F в данном классе обозначим через $L_2(F)$.

Пусть $F = (f_1, \dots, f_m)$ и каждая из функций f_j, $1 \leqslant j \leqslant m$, зависит от двух наборов переменных: $\tilde{x} = (x_1, \dots, x_n)$ и $\tilde{y} = (y_1, \dots, y_k)$. Разложим f_j в полином Жегалкина по переменным $\tilde{x}$:

$$f_j = f_j^0 \oplus f_j^1 x_1 \oplus \dots \oplus f_j^n x_n \oplus f_j',$$

где функция f_j^i, $0 \leqslant i \leqslant n$, зависит от $\tilde{y}$, f_j' — нелинейная по $\tilde{x}$ часть.

Рассмотрим матрицу $M = (f_j^i)$, $i = 1, \dots, n$, $j = 1, \dots, m$. Пусть i-му столбцу [j-й строке] матрицы M приписано множество функций M^i [M_j] от переменных $\tilde{y}$ таким образом, что каждая функция f_j^i вычислима через функции из множества $M^i \cup M_j$, т. е. представима в виде $h(g_1, \dots, g_s)$, где $g_1, \dots, g_s$ — функции из $M^i \cup M_j$, $h \in P_2$. Тогда набор $(M;\ M^1, \dots, M^n;\ M_1, \dots, M_m)$ назовём *M-функциональной таблицей*. Обозначим

$$\mathcal{L}(M) = \min\Big(\sum_i |M^i| + \sum_j |M_j|\Big),$$

где минимум берётся по всем M-функциональным таблицам.

ТЕОРЕМА. $L_2(F) \geqslant \mathcal{L}(M)$.

С помощью теоремы можно получить нижние оценки сложности вида $\Omega(N^{3/2})$ (где $N = n + k + m$) для операторов циклической свёртки, произведения многочленов, произведения матриц. Наибольшие известные нижние оценки в данном классе схем имеют вид $\Omega(N \log^2 N / \log\log N)$ и основаны на теоретико-графовой технике [1].

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

Список литературы

1. 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.