ПРИБЛИЖЕННЫЕ ВЫЧИСЛЕНИЯ БУЛЕВЫХ ОПЕРАТОРОВ

А. В. Чашкин (Москва)

Неветвящейся программой с условной остановкой P с множеством независимых булевых переменных $X = \{x_1, \dots, x_n\}$, множеством внутренних переменных $Y = \{y_1, \dots, y_t, \dots\}$ и множеством выходных переменных $Z = \{z_1, \dots, z_m\}$ назовем список $p_1, \dots, p_L$ последовательно выполняемых команд двух видов — вычислительных команд и команд остановки. Если p_i — вычислительная команда, то она присваивает первой свободной внутренней переменной y_r или некоторой внутренней переменной z_l значение $f_i(a_1, a_2)$, где f_i — двухместная булева функция и $a_1, a_2 \in X \bigcup Z \bigcup \{y_1, \dots, y_{i-1}\}$. Если p_i — команда остановки $\mathtt{Stop}(a)$, где $a \in X \bigcup Z \bigcup \{y_1, \dots, y_{i-1}\}$, то эта команда останавливает вычисления если $a = 1$ и объявляет результатом работы $P(x)$ программы P на x значения выходных переменных из Z. Если $a = 0$, то выполняется следующая команда программы. Если ни одна команда остановки не остановила программу, то ее значением $P(x)$ объявляются последние значения выходных переменных. Число команд называется сложностью программы. Величина

$$T(P) = 2^{-n} \sum_{x \in \{0,1\}^n} T_P(x),$$

где $T_P(x)$ — число команд, выполненных программой на наборе x до ее остановки, называется средним временем работы программы P. Если для булева оператора f и любого двоичного набора x справедливо равенство $f(x) = P(x)$, то будем говорить, что программа P вычисляет оператор f. Величину

$$T(f) = \min T(P),$$

где минимум берется по всем программам, вычисляющим f, назовем средней сложностью оператора f.

Пусть $d(x, y)$ — расстояние Хемминга. Будем говорить, что булев (n,m)-оператор $f_\delta : \{0,1\}^n \to \{0,1\}^m$ является δ-приближением булева (n,m)-оператора $f : \{0,1\}^n \to \{0,1\}^m$, если $d(f(x), f_\delta(x)) \le \delta m$ для любого x.

Средней сложностью $T_\delta(f)$ δ-приближения булева оператора f назовем минимальную среднюю сложность его δ-приближений.

Теорема. *Пусть $n, m \to \infty$, $m \le n$, δ — положительная постоянная для которой $H(\delta) < 2/3$, где H — функция двоичной энтропии. Тогда*:
(1) *для любого (n, m)-оператора f*

$$T_\delta(f) \lesssim \frac{2^n m(1 - H(\delta))}{n};$$

(2) *для почти каждого (n, m)-оператора f*

$$T_\delta(f) \gtrsim \frac{2^n m(1 - H(\delta))}{33n}.$$

Верхняя оценка теоремы является прямым следствием верхней оценки основной теоремы из [1].

Докажем нижнюю оценку. С каждой программой P, вычисляющей булев оператор, свяжем линейный порядок на множестве двоичных наборов длины n. Каждому двоичному набору x длины n поставим в соответствие его номер $N_P(x)$ такой, что $N_P(x) \in \{1, 2, \ldots, 2^n\}$,

$$N_P(x) < N_P(y), \text{ если } T_P(x) < T_P(y);$$
$$N_P(x) < N_P(y), \text{ если } T_P(x) = T_P(y) \text{ и } |x| < |y|.$$

Пусть P минимальная программа оператора некоторого f. Рассмотрим набор x_0 такой, что $N_P(x_0) = 3 \cdot 2^{n-2}$. Тогда

$$T(f) = T(P) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} T_P(x) > \frac{1}{2^n} \sum_{x | N_P(x) > N_P(x_0)} T_P(x) \ge$$
$$\ge \frac{1}{2^n} \sum_{x | N_P(x) > N_P(x_0)} T_P(x_0) = \frac{1}{4} T_P(x_0).$$

Следовательно,
$$T_P(x_0) \le 4T(f).$$

Оценим число операторов, средняя сложность которых не превосходит величины
$$T = \frac{2^n m(1 - H(\delta))}{33n}.$$

Каждый такой оператор однозначно определяется первыми $T_P(x_0)$ командами своей минимальной программы и набором не более чем из 2^{n-2} двоичных векторов длины m — значениями на тех аргументах, время работы на которых больше времени работы на x_0. Нетрудно показать, что число программ с n независимыми и m выходными переменными, и состоящими не более чем из k команд, не превосходит $(cmk)^{2k}$, где c — константа. Поэтому, для числа N, равного числу различных программ, сложность которых не превосходит $T_P(x_0)$, справедливо неравенство

$$N \le (cmT_P(x_0))^{2T_P(x_0)} \le (4cmT)^{8T} \le$$
$$\le \left(\frac{2^{n+2}cm^2(1-H(\delta))}{33n}\right)^{2^{n+3}m(1-H(\delta))/33n} \le 2^{2^n m(1-H(\delta))/4}.$$

Следовательно, число рассматриваемых операторов не превосходит произведения

$$2^{2^n m(1-H(\delta))/4} \cdot 2^{m2^{n-2}} = 2^{m2^n/2 - m2^n H(\delta)/4}.$$

Каждый (n,m)-оператор является δ-приближением для $B(\delta m)^{2^n}$ различных (n,m)-операторов, где $B(\delta m)$ — число наборов в шаре радиуса δm в $\{0,1\}^m$. Известно, что

$$B(\delta m) \le 2^{mH(\delta)}.$$

Поэтому число операторов, у которых средняя сложность δ-приближения не превосходит определенной выше величины T не больше, чем

$$2^{m2^n/2 - 2^n mH(\delta)/4 + m2^n H(\delta)} = 2^{m2^n/2 + 3m2^n H(\delta)/4} =$$
$$= 2^{m2^n(1/2 + 3H(\delta)/4)} = o\left(2^{m2^n}\right).$$

Следовательно, средняя сложность δ-приближения почти всех рассматриваемых операторов не меньше T. Нижняя оценка доказана.

Статья опубликована при финансовой поддержке Минобрнауки России в рамках реализации программы Московского центра фундаментальной и прикладной математики по соглашению № 075–15–2022–284.

Список литературы

1. Чашкин А. В. О средней сложности недоопределенных функций // Дискретная математика. — 2017. — Т. 29, вып. 2. — С. 133–159.

DOI: 10.20948/dms-2022-28