ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль—сентябрь 2004. Серия 1. Том 11, № 3, 3–15

УДК 519.7

О СРЕДНЕЙ СЛОЖНОСТИ БУЛЕВЫХ ФУНКЦИЙ, ЗАДАННЫХ ПОЛИНОМАМИ ЖЕГАЛКИНА

Р. Н. Забалуев

Рассматривается сложность реализации булевых функций, заданных полиномами Жегалкина степени не более k, неветвящимися программами с условной остановкой. Показано, что средняя сложность почти каждого полинома от n переменных, степень которого не превосходит k, не меньше $\frac{3}{8}\frac{S}{\log_2 S}(1+o(1))$, где $S=\sum\limits_{i=0}^{k}\binom{n}{i}$ и $n\to\infty$. Доказано, что для более половины значений k средняя сложность каждого полинома от n переменных степени k не превосходит величины $(1/2)\,\dfrac{S}{\log_2 S}(1+o(1))$, $n\to\infty$.

В настоящей статье рассматривается сложность реализации булевых функций, заданных полиномами Жегалкина степени не более k, неветвящимися программами с условной остановкой, которые введены А. В. Чашкиным в [2]. Рассматриваемые программы обобщают понятие схем из функциональных элементов и являются естественной моделью неветвящихся вычислений, т. е. вычислений, в которых нет условных переходов и косвенной адресации, но есть возможность досрочного прекращения работы при выполнении определенного условия.

Неветвящаяся программа с условной остановкой является последовательностью операторов двух типов. Каждый оператор первого типа вычисляет значения некоторой булевой функции, зависящей не более чем от двух переменных. Аргументами этой функции могут быть либо величины, вычисленные предыдущими операторами, либо значения входных переменных. Операторы второго типа могут прекращать выполнение программы. Результат работы оператора второго типа определяется значениями, вычисленными на некоторых двух предыдущих шагах. Для каждого конкретного оператора номера этих шагов фиксированы и могут быть различными для различных опрераторов.

Если на первый вход выполняемого оператора второго типа поступает единица, то выполнение программы прекращается и значение переменной, которая поступает на второй вход оператора, объявляется значением булевой функции на вычисляемом наборе переменных. В противном случае выполняется следующий оператор. Если последний оператор какой-либо программы является оператором первого типа и выполнение этой программы на предыдущих шагах не было прервано, то результатом работы программы считается величина, вычисленная последним оператором.

В отличие от обычных неветвящихся программ, затрачивающих одинаковое число шагов для вычисления функции на различных значениях переменных, время работы рассматриваемых программ может быть различным для различных значений переменных. Поэтому естественной мерой сложности таких программ является среднее время работы, взятое по всем наборам значений переменных.

Сложностью $L(P)$ программы P назовем число операторов этой программы. *Временем работы* $T_P(\tilde{\sigma})$ программы P на наборе $\tilde{\sigma} = (\sigma_1, ..., \sigma_n)$ назовем число операторов, выполненных до остановки программы. Величину $T(P) = 2^{-n} \sum T_P(\tilde{\sigma})$, где суммирование производится по всем двоичным наборам длины n, назовем *средним временем работы* программы P. Если для некоторой булевой функции f и любого двоичного набора $\tilde{\sigma}$ справедливо равенство $f(\tilde{\sigma}) = P(\tilde{\sigma})$, то будем говорить, что программа P *вычисляет* функцию f. Величину $T(f) = \min T(P)$, где минимум берется по всем программам, вычисляющим f, назовем *средней сложностью* функции f.

Пусть булева функция $f(x_1, ..., x_n)$ задана полиномом вида

$$f(x_1, ..., x_n) = \bigoplus_{\substack{1 \leqslant i_1 < i_2 < ... < i_j \leqslant n \\ 0 \leqslant j \leqslant n}} c_{i_1 i_2 ... i_j} x_{i_1} x_{i_2} ... x_{i_j},$$

где $c_{i_1 i_2 ... i_j} \in \{0, 1\}$ (при $j = 0$ положим $x_{i_1} x_{i_2} ... x_{i_j} \equiv 1$ и $c_{i_1 i_2 ... i_j} = c_0 \in \{0, 1\}$).

Такое задание функции назыывается *полиномом Жегалкина.* Выражение «полином f» всюду означает «полином Жегалкина, задающий функцию f».

Если коэффициент $c_{i_1 i_2 ... i_j}$ не равен нулю, то $x_{i_1} ... x_{i_j}$ называется *мономом* полинома f, число j — *степенью* этого монома. *Степень* полинома f, $f \neq 0$, опеределяется как наибольшая из степеней его мономов; если $f \equiv 0$, то степень полинома f равна нулю. Через $P_2^k[n]$ обозначим

класс полиномов от n переменных, степень каждого из которых не превосходит k.

Пусть $Q(n)$ — некоторый класс полиномов от n переменных. Будем говорить, что некоторое свойство выполнено для почти каждого полинома из класса $Q(n)$, если для подкласса $V(n)$ полиномов, не обладающих этим свойством $\lim\limits_{n\to\infty} |V(n)|/|Q(n)| = 0$. Заметим, что неветвящаяся программа без операторов остановки, вычисляющая функцию, отличную от входной переменной, является обычной схемой из функциональных элементов. Поэтому $T(f) \leqslant L(f)$ для любой булевой функции f, существенно зависящей не менее чем от двух переменных.

Из работы [2] следует, что обычная сложность $L(f)$ любого полинома $f \in P_2^k[n]$ $(2 \leqslant k \leqslant n)$ не превосходит величины $\dfrac{S_{n,k}}{\log S_{n,k}}(1 + o(1))$, где $S_{n,k} = \sum\limits_{i=0}^{k} \binom{n}{i}$ и $n \to \infty$ (здесь и далее $\log x$ означает $\log_2 x$). Значит, для каждого полинома $f \in P_2^k[n]$ справедливо соотношение

$$T(f) \leqslant \frac{S_{n,k}}{\log S_{n,k}}(1 + o(1)).$$

В данной статье показано, что для более половины значений k верхнюю оценку средней сложности для полиномов из класса $P_2^k[n]$ можно уменьшить в два раза. Также доказано, что средняя сложность почти каждого полинома $f(x_1, ..., x_n)$ степени k $(2 \leqslant k \leqslant n)$ не меньше величины $\dfrac{3}{8}\dfrac{S_{n,k}}{\log S_{n,k}}(1 + o(1))$.

Введем некоторые понятия и приведем ряд вспомогательных утверждений, которые понадобятся при доказательстве основных результатов. Число элементов в множестве H обозначим через $|H|$. Пусть $S_r(\tilde{\alpha})$ — шар радиусом r с центром в точке $\tilde{\alpha} \in E_n$ (E_n — множество наборов из нулей и единиц длины n) и H — какое-либо множество наборов из E_n. Через $wt(S_r(\tilde{\alpha}), H)$ обозначим величину $|S_r(\tilde{\alpha}) \cap H|$. Величину $P_r(H) = 2^{-n} \sum\limits_{\tilde{\alpha}\in E_n} wt(S_r(\tilde{\alpha}), H)$ будем называть *средним весом* шара радиусом r для множества H.

Лемма 1. (a) *Среди шаров радиусом r найдется такой шар $S'_r(\tilde{\alpha})$, в котором число наборов из H не меньше $P_r(H)$, т. е.*

$$wt(S'_r(\tilde{\alpha}), H) \geqslant P_r(H);$$

(*b*) *справедливо равенство*

$$P_r(H) = 2^{-n}|H| \sum_{i=0}^{r} \binom{n}{i}.$$

Доказательство. (*a*) Предположим что для любого набора $\tilde{\alpha} \in E_n$ верно неравенство $wt(S_r(\tilde{\alpha}), H) < P_r(H)$. Тогда

$$\sum_{\tilde{\alpha} \in E_n} wt(S_r(\tilde{\alpha}), H) < P_r(H)2^n = \sum_{\tilde{\alpha} \in E_n} wt(S_r(\tilde{\alpha}), H).$$

Противоречие. Следовательно утверждение (*a*) справедливо.

(*b*) Утверждение (*b*) следует из того, что каждый набор из H пересекается ровно с $\sum\limits_{i=0}^{r} \binom{n}{i}$ шарами радиусом r. Лемма 1 доказана.

Нетрудно видеть, что полином f степени k однозначно определяется по своим значениям на наборах шара радиусом k с центром в нулевом наборе. Оказывается, что полином f однозначно определяется по своим значениям на наборах любого шара радиусом k.

Лемма 2. *Пусть полином f принадлежит классу $P_2^k[n]$. Если известны значения f на каждом наборе шара $S_k(\tilde{\alpha})$ радиусом k с центром в произвольном наборе $\tilde{\alpha}$, то по этим значениям полином f определяется однозначно.*

Доказательство. Пусть $\tilde{\alpha} = (\alpha_1, ..., \alpha_n)$ — произвольный набор и $\tilde{\sigma} = (\sigma_1, ..., \sigma_n)$ — двоичный набор, в котором число единиц не больше k. Тогда набор $\tilde{\eta} = \tilde{\alpha} \oplus \tilde{\sigma} = (\alpha_1 \oplus \sigma_1, ..., \alpha_n \oplus \sigma_n)$ принадлежит шару $S_k(\tilde{\alpha})$ и известно значение полинома $f(\tilde{\eta})$. Докажем, что

$$c_{12...k} = \bigoplus f(\tilde{\alpha} \oplus \tilde{\sigma}'), \tag{1}$$

где суммирование ведется по таким наборам $\tilde{\sigma}' = (\sigma_1, ..., \sigma_n)$, что $\sigma_{k+1} = ... = \sigma_n = 0$. Так как $f \in P_2^k[n]$, то

$$f(x_1, ..., x_n) = \bigoplus_{\substack{1 \leqslant i_1 < i_2 < ... < i_j \leqslant n \\ 0 \leqslant j \leqslant k}} c_{i_1 i_2 ... i_j} x_{i_1} x_{i_2} ... x_{i_j}.$$

Каждый набор $\tilde{\eta}' = \tilde{\alpha} \oplus \tilde{\sigma}'$, где $\tilde{\sigma}' = (\sigma_1, ..., \sigma_k, 0, ..., 0)$, принадлежит шару $S_k(\tilde{\alpha})$ и

$$f(\tilde{\eta}') = f(\tilde{\alpha} \oplus \tilde{\sigma}') = \bigoplus_{\substack{1 \leqslant i_1 < i_2 < ... < i_j \leqslant n \\ 0 \leqslant j \leqslant k}} c_{i_1 i_2 ... i_j} (\alpha_{i_1} \oplus \sigma_{i_1})(\alpha_{i_2} \oplus \sigma_{i_2}) ... (\alpha_{i_j} \oplus \sigma_{i_j}).$$

Запишем правую часть из (1), подставив в нее выражение для $f(\tilde{\eta}')$:

$$\bigoplus_{\tilde{\sigma}'=(\sigma_1,\ldots,\sigma_k,0,\ldots,0)} f(\tilde{\alpha}\oplus\tilde{\sigma}')$$

$$= \bigoplus_{\tilde{\sigma}'=(\sigma_1,\ldots,\sigma_k,0,\ldots,0)} \bigoplus_{\substack{1\leqslant i_1<i_2<\ldots<i_j\leqslant n\\ 0\leqslant j\leqslant k}} c_{i_1i_2\ldots i_j}(\alpha_{i_1}\oplus\sigma_{i_1})(\alpha_{i_2}\oplus\sigma_{i_2})\ldots(\alpha_{i_j}\oplus\sigma_{i_j})$$

$$= \bigoplus_{\substack{1\leqslant i_1<i_2<\ldots<i_j\leqslant n\\ 0\leqslant j\leqslant k}} c_{i_1i_2\ldots i_j}\Big(\bigoplus_{\tilde{\sigma}'=(\sigma_1,\ldots,\sigma_k,0,\ldots,0)} (\alpha_{i_1}\oplus\sigma_{i_1})(\alpha_{i_2}\oplus\sigma_{i_2})\ldots(\alpha_{i_j}\oplus\sigma_{i_j})\Big). \quad (2)$$

Нетрудно видеть, что сумма

$$\bigoplus_{\tilde{\sigma}'=(\sigma_1,\ldots,\sigma_k,0,\ldots,0)} (\alpha_{i_1}\oplus\sigma_{i_1})(\alpha_{i_2}\oplus\sigma_{i_2})\ldots(\alpha_{i_j}\oplus\sigma_{i_j})$$

равна нулю, если набор индексов $\{i_1, i_2, ..., i_j\}$ отличен от набора $\{1, 2, \ldots, k\}$. Поэтому выполнено соотношение

$$\bigoplus_{\tilde{\sigma}'=(\sigma_1,\ldots,\sigma_k,0,\ldots,0)} f(\tilde{\alpha}\oplus\tilde{\sigma}')$$

$$= c_{12\ldots k}\Big(\bigoplus_{\tilde{\sigma}'=(\sigma_1,\ldots,\sigma_k,0,\ldots,0)} (\alpha_1\oplus\sigma_1)(\alpha_2\oplus\sigma_2)\ldots(\alpha_k\oplus\sigma_k)\Big). \quad (3)$$

Также справедлива следующая цепочка равенств

$$\bigoplus_{\tilde{\sigma}'=(\sigma_1,\ldots,\sigma_k,0,\ldots,0)} (\alpha_1\oplus\sigma_1)(\alpha_2\oplus\sigma_2)\ldots(\alpha_k\oplus\sigma_k)$$

$$= (\alpha_1\oplus 0)\Big(\bigoplus_{(\sigma_2,\ldots,\sigma_k)} (\alpha_2\oplus\sigma_2)\ldots(\alpha_k\oplus\sigma_k)\Big)\oplus(\alpha_1\oplus 1)\Big(\bigoplus_{(\sigma_2,\ldots,\sigma_k)} (\alpha_2\oplus\sigma_2)\ldots(\alpha_k\oplus\sigma_k)\Big)$$

$$= \bigoplus_{(\sigma_2,\ldots,\sigma_k)} (\alpha_2\oplus\sigma_2)(\alpha_3\oplus\sigma_3)\ldots(\alpha_k\oplus\sigma_k) = \ldots$$

$$= \bigoplus_{(\sigma_{k-1},\sigma_k)} (\alpha_{k-1}\oplus\sigma_{k-1})(\alpha_k\oplus\sigma_k) = \alpha_k\oplus(\alpha_k\oplus 1) = 1.$$

Отсюда с учетом (3) получаем (1). Аналогично доказывается равенство

$$c_{i_1i_2\ldots i_k} = \bigoplus_{\tilde{\sigma}'=(0,..,\sigma_{i_1},\ldots,\sigma_{i_k},\ldots,0)} f(\tilde{\alpha}\oplus\tilde{\sigma}'). \quad (4)$$

Итак, каждый коэффициент $c_{i_1 i_2 \ldots i_k}$ $(1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n)$ есть сумма некоторых известных значений полинома f на наборах из шара $S_k(\tilde{\alpha})$.

Теперь покажем, как выразить коэффициенты $c_{i_1 i_2 \ldots i_{k-1}}$ через значения полинома f на наборах из шара $S_{k-1}(\tilde{\alpha})$ радиусом $k-1$ и центром в наборе $\tilde{\alpha}$ и через уже определенные коэффициенты $c_{i_1 i_2 \ldots i_k}$. Пусть

$$g(x_1, \ldots, x_n) = \bigoplus_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} c_{i_1 i_2 \ldots i_k} x_{i_1} x_{i_2} \ldots x_{i_k}.$$

Тогда на наборах из шара $S_k(\tilde{\alpha})$ значения полинома g известны. Рассмотрим полином

$$z(\tilde{x}) = f(\tilde{x}) \oplus g(\tilde{x}) = \bigoplus_{\substack{1 \leqslant i_1 < i_2 < \ldots < i_j \leqslant n \\ 0 \leqslant j \leqslant k-1}} c_{i_1 i_2 \ldots i_j} x_{i_1} x_{i_2} \ldots x_{i_j}.$$

Очевидно, что значения полинома $z \in P_2^{k-1}[n]$ на наборах из шара $S_{k-1}(\tilde{\alpha})$ известны. Поэтому для того чтобы выразить коэффициенты $c_{i_1 i_2 \ldots i_{k-1}}$ полинома z, в формуле (4) символ f необходимо заменить на z и число k — на $k-1$:

$$c_{i_1 i_2 \ldots i_{k-1}} = \bigoplus_{\tilde{\sigma}' = (0, .., \sigma_{i_1}, \ldots, \sigma_{i_{k-1}}, \ldots, 0)} z(\tilde{\alpha} \oplus \tilde{\sigma}').$$

Значит, коэффициенты $c_{i_1 i_2 \ldots i_{k-1}}$ $(1 \leqslant i_1 < i_2 < \ldots < i_{k-1} \leqslant n)$ выражаются через значения полинома f на наборах из шара $S_k(\tilde{\alpha})$. Далее аналогичным образом можно выразить коэффициенты $c_{i_1 i_2 \ldots i_j}$ $(1 \leqslant i_1 < i_2 < \ldots < i_j \leqslant n, 0 \leqslant j \leqslant k-2)$ полинома f через значения полинома f на наборах из шара $S_k(\tilde{\alpha})$, и, значит, определить сам полином f. Лемма 2 доказана.

Теорема 1. *Для почти каждого полинома $f \in P_2^k[n]$, $2 \leqslant k \leqslant n$, при $n \to \infty$ справедливо неравенство*

$$T(f) \geqslant \frac{3}{8} \cdot \frac{\sum\limits_{i=0}^{k} \binom{n}{i}}{\log \sum\limits_{i=0}^{k} \binom{n}{i}} (1 + o(1)).$$

Доказательство. Обозначим через $N(L, n)$ число различных программ, в каждой из которых содержится не более L операторов. В [3] доказано, что

$$N(L, n) \leqslant (c_1(L+n))^{\frac{4}{3}L+n}. \tag{5}$$

Пусть $f(x_1, ..., x_n)$ — булева функция, заданная полиномом степени k, и P — минимальная программа, вычисляющая f. Каждому двоичному набору $\tilde{\sigma}$ длины n поставим в соответствие такой номер $N_P(\tilde{\sigma})$, что:

1) $1 \leqslant N_P(\tilde{\sigma}) \leqslant 2^n$;

2) $N_P(\tilde{\sigma}) < N_P(\tilde{\gamma})$ для любого набора $\tilde{\gamma}$ такого, что $T_P(\tilde{\sigma}) < T_P(\tilde{\gamma})$;

3) $N_P(\tilde{\sigma}) < N_P(\tilde{\gamma})$ для любого $\tilde{\gamma}$ такого, что $T_P(\tilde{\sigma}) = T_P(\tilde{\gamma})$ и $\tilde{\sigma} \prec \tilde{\gamma}$ (запись $\tilde{\sigma} \prec \tilde{\gamma}$ означает, что набор $\tilde{\sigma}$ предшествует набору $\tilde{\gamma}$).

Положим $S_{n,k} = \sum\limits_{j=0}^{k} \binom{n}{j}$. Пусть $\tilde{\sigma}_i$ — такой двоичный набор, что $N_P(\tilde{\sigma}_i) = i2^n/q$, где $q = 2^{q_0}$, q_0 — целое, $q \asymp \log S_{n,k}$ и $i = 1, 2, ..., q$.

Оценим сверху число полиномов из $P_2^k[n]$, что для минимальной программы, реализующих любой такой полином, найдется набор $\tilde{\sigma}_i$ такой, что

$$T_P(\tilde{\sigma}_i) \leqslant \frac{3i}{4q} \frac{S_{n,k}}{\log S_{n,k}}. \tag{6}$$

Пусть M_i — множество, состоящее из наборов $\tilde{\sigma}$ таких, что $N_P(\tilde{\sigma}) \leqslant N_P(\tilde{\sigma}_i)$. Из неравенства (5) следует, что число N_i различных программ, сложность каждой из которых не больше $T_P(\tilde{\sigma}_i)$, удовлетворяет неравенству

$$N_i \leqslant \left(c_1 \left(\frac{3i}{4q} \frac{S_{n,k}}{\log S_{n,k}} + n \right) \right)^{\frac{4}{3} \frac{3i}{4q} \frac{S_{n,k}}{\log S_{n,k}} + n}.$$

Отсюда после несложных преобразований получаем неравенство

$$N_i \leqslant 2^{\frac{i}{q} S_{n,k} - c_2 \frac{i}{q} S_{n,k} \frac{\log\log S_{n,k}}{\log S_{n,k}}}. \tag{7}$$

Из леммы 1 следует, что найдется шар $S'_n(\tilde{\alpha}_i)$ радиусом k, в котором имеется не менее $2^{-n}|M_i| \sum\limits_{j=0}^{k} \binom{n}{j} = \frac{i}{q} S_{n,k}$ наборов из M_i. Отсюда и из леммы 2 следует, что полином f однозначно определяется первыми $T_P(\tilde{\sigma}_i)$ операторами и булевым набором длины не более $(1 - \frac{i}{q})S_{n,k}$, состоящим из значений f на тех наборах шара $S'_n(\tilde{\alpha}_i)$, которые не принадлежат M_i.

Пользуясь этим фактом и (7), получаем, что число M полиномов, удовлетворяющих соотношению (6), не превосходит величины $\sum\limits_{i=1}^{q} 2^D$, где

$$D = \frac{i}{q} S_{n,k} - c_2 \frac{i}{q} S_{n,k} \frac{\log\log S_{n,k}}{\log S_{n,k}} + (1 - \frac{i}{q}) S_{n,k}.$$

Оценим D. Так как $i \leqslant q \asymp \log S_{n,k}$, то

$$D \leqslant \frac{i}{q} S_{n,k} - c_2 \frac{i}{q} S_{n,k} \frac{\log\log S_{n,k}}{\log S_{n,k}} + (1 - \frac{i}{q}) S_{n,k}$$
$$\leqslant S_{n,k} - c_3 S_{n,k} \frac{\log\log S_{n,k}}{\log^2 S_{n,k}}.$$

Поэтому

$$M \leqslant q \cdot 2^{S_{n,k} - c_3 S_{n,k} \frac{\log\log S_{n,k}}{\log^2 S_{n,k}}} \leqslant 2^{S_{n,k} - c_4 S_{n,k} \frac{\log\log S_{n,k}}{\log^2 S_{n,k}}}.$$

Заметим, что число полиномов в $P_2^k[n]$ равно $2^{S_{n,k}}$. Сравнивая это число с оценкой для M, получаем, что минимальная программа P, реализующая почти каждый полином из $P_2^k[n]$, удовлетворяет условию:

если $\tilde{\sigma}_i$ такое, что $N_P(\tilde{\sigma}_i) = \dfrac{i2^n}{q}$, где $q = 2^{q_0}$, q_0 — целое,

$$q \asymp \log S_{n,k},\ i = 1, 2, ..., q,\ \text{то } T_P(\tilde{\sigma}_i) > \frac{iS_{n,k}}{q \log S_{n,k}}.$$

Пусть $W_i = \{\tilde{\sigma} | N_P(\tilde{\sigma}_i) < N_P(\tilde{\sigma}) \leqslant N_P(\tilde{\sigma}_{i+1})\}$. Тогда среднее время $T(P)$ работы каждой такой программы удовлетворяет соотношению

$$T(P) = 2^{-n} \sum_{\sigma \in \{0,1\}^n} T_P(\tilde{\sigma}) \geqslant 2^{-n} \sum_{i=1}^{q-1} T_P(\tilde{\sigma}_i) |W_i|$$
$$= 2^{-n} \sum_{i=1}^{q-1} T_P(\tilde{\sigma}_i) \frac{2^n}{q} > \frac{1}{q} \sum_{i=1}^{q-1} \frac{3iS_{n,k}}{4q \log S_{n,k}}$$
$$= \frac{q(q-1)}{2q^2} \frac{3S_{n,k}}{4 \log S_{n,k}} = \frac{3 \sum\limits_{j=0}^{k} \binom{n}{j}}{8 \log \sum\limits_{j=0}^{k} \binom{n}{j}} \left(1 + O\left(\log^{-1}\left(\sum_{j=0}^{k} \binom{n}{j}\right)\right)\right).$$

Теорема 1 доказана.

Теорема 2. *Для каждого полинома $f \in P_2^k[n]$, $2 \leqslant k \leqslant n$, при $n \to \infty$ выполнено неравенство*

$$T(f) \leqslant \frac{\sum\limits_{i=0}^{k} \binom{n}{i}}{\log \sum\limits_{i=0}^{k} \binom{n}{i}} (1 + o(1)).$$

Доказательство. Из результатов [1] следует, что для полинома $f(x_1, ..., x_n)$ степени k $(2 \leqslant k \leqslant n)$ при $n \to \infty$ выполнено неравенство

$$L(f) \leqslant \frac{\sum\limits_{i=0}^{k} \binom{n}{i}}{\log \sum\limits_{i=0}^{k} \binom{n}{i}}(1 + o(1)). \tag{8}$$

Отсюда и из неравенства $T(f) \leqslant L(f)$ следует справедливость теоремы 2.

Каждому двоичному набору $(\sigma_1, ..., \sigma_n)$ поставим в соответствие его номер $N(\sigma_1, ..., \sigma_n) = 1 + \sum\limits_{i=1}^{n} \sigma_i 2^{i-1}$.

Теорема 3. *Для каждого полинома $f \in P_2^k[n]$, где $\lceil n/2 \rceil - a\sqrt{n} \leqslant k \leqslant n$ и $a > 0$, при $n \to \infty$ выполнено неравенство*

$$T(f) \leqslant \frac{1}{2} \cdot \frac{\sum\limits_{i=0}^{k} \binom{n}{i}}{\log \sum\limits_{i=0}^{k} \binom{n}{i}}(1 + o(1)).$$

Доказательство. Положим $d = \lfloor \log n \rfloor$. Представим полином $f \in P_2^k[n]$ в следующем виде

$$f(x_1, ..., x_n) = \bigvee_{(\sigma_1, ..., \sigma_d)} f(\sigma_1, ..., \sigma_d, x_{d+1}, ..., x_n) x_1^{\sigma_1} ... x_d^{\sigma_d}.$$

Программу, вычисляющую полином f, запишем в виде

$$P = P_0 P_1 ... P_j ... P_{2^d},$$

где P_0 — программа, вычисляющая всевозможные конъюнкции вида $x_1^{\sigma_1} \dots x_d^{\sigma_d}$, $j = N(\sigma_1, ..., \sigma_d)$, P_j — программа, вычисляющая полином

$$f_j(x_{d+1}, ..., x_n) = f(\sigma_1, ..., \sigma_d, x_{d+1}, ..., x_n)$$

и прекращающая работу программы P, если $x_1^{\sigma_1} ... x_d^{\sigma_d} = 1$. Поэтому для любых двух различных наборов $(x_{d+1}, ..., x_n)$ и $(x'_{d+1}, ..., x'_n)$ имеем

$$T_P(\sigma_1, ..., \sigma_d, x_{d+1}, ..., x_n) = T_P(\sigma_1, ..., \sigma_d, x'_{d+1}, ..., x'_n). \tag{9}$$

Следовательно, справедливы соотношения

$$T(P) \sim 2^{-n} \sum_{p=1}^{2^d} \left(2^{n-d} \sum_{j=0}^{p} L(P_j) \right) = 2^{-d} \sum_{p=1}^{2^d} \sum_{j=0}^{p} L(P_j). \tag{10}$$

Рассмотрим два случая:

$$\lceil n/2 \rceil - a\sqrt{n} \leqslant k \leqslant n - d \tag{11}$$

и

$$n - d < k \leqslant n. \tag{12}$$

Пусть k удовлетворяет (11). При подстановке констант $\sigma_1, ..., \sigma_d$ в полином $f(x_1, ..., x_n)$ получается полином $f_j(x_{d+1}, ..., x_n)$ степени не более k. Из (8) вытекает оценка для $L(P_j)$:

$$L(P_j) \leqslant \frac{\sum\limits_{i=0}^{k} \binom{n-d}{i}}{\log \sum\limits_{i=0}^{k} \binom{n-d}{i}}(1 + o(1)). \tag{13}$$

Отсюда и из (10) следует, что

$$T(P) \lesssim 2^{-d} \frac{\sum\limits_{i=0}^{k} \binom{n-d}{i}}{\log \sum\limits_{i=0}^{k} \binom{n-d}{i}} \sum_{j=1}^{2^d} j \sim 2^{d-1} \frac{\sum\limits_{i=0}^{k} \binom{n-d}{i}}{\log \sum\limits_{i=0}^{k} \binom{n-d}{i}}. \tag{14}$$

Покажем, что при $n \to \infty$ выполнены асиптотические равенства:

$$2^d \sum_{i=0}^{k} \binom{n-d}{i} \sim \sum_{i=0}^{k} \binom{n}{i}; \quad \log\left(\sum_{i=0}^{k} \binom{n-d}{i}\right) \sim \log\left(\sum_{i=0}^{k} \binom{n}{i}\right). \tag{15}$$

Отсюда с использованием (4) получаем требуемую оценку:

$$T(P) \leqslant \frac{1}{2} \cdot \frac{\sum\limits_{i=0}^{k} \binom{n}{i}}{\log \sum\limits_{i=0}^{k} \binom{n}{i}}(1 + o(1)).$$

Убедимся в справедливости первого асимптотического равенства в (15). Вначале покажем справедливость следующего соотношения

$$2^d \sum_{i=0}^{k} \binom{n-d}{i} - \sum_{i=1}^{d} 2^{i-1} \binom{n-i}{k} = \sum_{i=0}^{k} \binom{n}{i}. \tag{16}$$

Действительно,

$$\sum_{i=0}^{k}\binom{n}{i}=\sum_{i=0}^{k}\left(\binom{n-1}{i}+\binom{n-1}{i-1}\right)=\sum_{i=0}^{k}\binom{n-1}{i}+\sum_{i=0}^{k-1}\binom{n-1}{i}$$

$$=2\sum_{i=0}^{k}\binom{n-1}{i-1}-\binom{n-1}{k}=2\sum_{i=0}^{k}\left(\binom{n-2}{i}+\binom{n-2}{i-1}\right)-\binom{n-1}{k}$$

$$=2^2\sum_{i=0}^{k}\binom{n-1}{i-1}-\sum_{i=1}^{2}2^{i-1}\binom{n-i}{k}.$$

После нескольких таких преобразовний получим выражение (16). Далее покажем, что при выбранном d выполняется равенство

$$\sum_{i=1}^{d}2^{i-1}\binom{n-i}{k}=o\left(2^d\sum_{i=0}^{k}\binom{n-d}{i}\right). \tag{17}$$

Для оценки суммы из левой части (17) воспользуемся следующим утверждением (см., например, [4]): *если* $|r|\leqslant t(n)\sqrt{n}$, *где* $t(n)=o(n^{1/6})$, *то при* $n\to\infty$ *справедливо соотношение*

$$\binom{n}{\lceil n/2\rceil-r}\sim\frac{2^n}{\sqrt{\pi n/2}}e^{-2r^2/n}. \tag{18}$$

Поэтому имеем

$$\sum_{i=1}^{d}2^i\binom{n-i}{k}\leqslant\sum_{i=1}^{d}2^i\binom{n-i}{\lceil n/2-i/2\rceil}\sim\sum_{i=1}^{d}\frac{2^i2^{n-i}}{\sqrt{\pi(n-i)/2}}$$

$$\leqslant\sum_{i=1}^{d}\frac{2^n}{\sqrt{\pi(n-d)/2}}\leqslant\frac{2^n\log n}{\sqrt{\pi(n-\log n)/2}}(1+o(1)). \tag{19}$$

Теперь оценим выражение из правой части равенства (17). Известно (см., например, [4]), что при $q<p$

$$\frac{1}{2^n}\sum_{\lceil n/2\rceil+\frac{q\sqrt{n}}{2}\leqslant i\leqslant\lceil n/2\rceil+\frac{p\sqrt{n}}{2}}\binom{n}{i}\sim\frac{1}{\sqrt{2\pi}}\int_q^p e^{-x^2/2}dx.$$

Отсюда получаем

$$\frac{2^d\sum\limits_{i=0}^{k}\binom{n-d}{i}}{2^n}>0.$$

Но из (19) следует, что

$$\frac{1}{2^n}\sum_{i=0}^{d} 2^i \binom{n-i}{k} \leqslant \frac{\log n}{\sqrt{\pi(n-\log n)/2}}(1+o(1)),$$

поэтому выполнено (17).

Теперь докажем второе равенство из (15). Учитывая (18), замечаем, что

$$\log \sum_{i=0}^{k} \binom{n-d}{i} \sim n-d \sim n \sim \log \sum_{i=0}^{k} \binom{n}{i}.$$

Итак, условия (15) выполнены, а значит, в случае (11) теорема 3 доказана.

Рассмотрим случай, когда k удовлетворяет (12). Степень полинома $f_j(x_{d+1},...,x_n)$ не превосходит $n-d$. Поэтому из (8) получаем

$$L(P_j) \leqslant \frac{\sum\limits_{i=0}^{n-d}\binom{n-d}{i}}{\log \sum\limits_{i=0}^{n-d}\binom{n-d}{i}}(1+o(1)) = \frac{2^{n-d}}{n-d}(1+o(1)). \tag{20}$$

Очевидно, что в этом случае

$$\frac{\sum\limits_{i=0}^{k}\binom{n}{i}}{\log \sum\limits_{i=0}^{k}\binom{n}{i}} \sim \frac{2^n}{n}.$$

Отсюда, а также из (10) и (20) получаем

$$T(P) \lesssim 2^{-d}\frac{2^{n-d}}{n-d}\sum_{j=1}^{2^d} j \leqslant 2^{d-1}\frac{2^{n-d}}{n-d}(1+o(1)) = \frac{1}{2}\frac{\sum\limits_{i=0}^{k}\binom{n}{i}}{\log \sum\limits_{i=0}^{k}\binom{n}{i}}(1+o(1)).$$

Теорема 3 доказана.

ЛИТЕРАТУРА

1. **Забалуев Р. Н.** О сложности реализации полиномов Жегалкина // Дискретная математика. 2004. Т. 16, вып. 1. С. 79–94.

2. Чашкин А. В. О среднем времени вычисления значений булевых функций // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 1. С. 60–78.

3. Чашкин А. В. Об одном методе вычисления частичных булевых функций // Мат. вопросы кибернетики. Вып. 12. М.: Наука, 2004. С. 231–246.

4. Яблонский С. В. Введение в дискретную математику. М.: Наука, 1986.

Адрес автора:
МГУ,
Мех.–мат. факультет,
Воробьевы горы,
119992 Москва,
Россия.

Статья поступила
15 апреля 2004 г.