

УДК 519.714.4 + 519.725

## НИЖНЯЯ ОЦЕНКА СЛОЖНОСТИ ВЫЧИСЛЕНИЯ ХАРАКТЕРИСТИЧЕСКИХ ФУНКЦИЙ БЧХ-КОДОВ ВЕТВЯЩИМИСЯ ПРОГРАММАМИ \*)

Е. А. Окольниковишникова

**Аннотация.** Получена нижняя оценка  $\Omega(n \log n)$  сложности вычисления недетерминированными ветвящимися программами характеристических функций кодов Боуза — Чоудхури — Хоквингема (БЧХ-кодов) при некоторых значениях параметров этих кодов.

**Ключевые слова:** сложность, нижняя оценка, ветвящаяся программа, коды.

### Введение

Получение нижних оценок сложности дискретных устройств, вычисляющих последовательности булевых функций, — важное направление в теоретической кибернетике и дискретной математике. В последние двадцать лет интенсивно изучаются ветвящиеся программы. Настоящая работа является развитием работ [1–3]. В ней рассматривается получение нижних оценок сложности реализации характеристических функций кодов (БЧХ-кодов) недетерминированными ветвящимися программами. Как и в [1–3], нижние оценки сложности для схем без ограничений получены с помощью нижних оценок сложности для схем с ограничениями, называемых *ветвящимися  $k$ -программами*. Определение недетерминированной ветвящейся программы и ветвящейся  $k$ -программы можно найти, например, в [2, 7].

Наилучшими известными нижними оценками сложности для детерминированных и недетерминированных программ, вычисляющих последовательности полностью определенных функций, являются оценки  $\Omega(n^2/\log^2 n)$  и  $\Omega(n^{3/2}/\log n)$  соответственно. Эти оценки получены в [8] с помощью метода Нечипорука. Этот метод основан на мощностных соображениях и применим только к функциям специального вида, вычисляемых в тех моделях, для которых сложность определяется через число

---

\*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 09–01–00528а).

элементов, помеченных переменными (контактные схемы, формулы, ветвящиеся программы и т. д.). Из оценки А. А. Разборова для контактно-вентильных схем [4] следует нижняя оценка  $\Omega(n \log \log \log^* n)^*$  для сложности недетерминированных программ, вычисляющих симметрические булевы функции, включая функцию голосования. Е. А. Окольнішніковой [2, 3] получены нижние оценки вида  $\Omega(n \log n / \log \log n)$  сложности недетерминированных программ, вычисляющих характеристические функции кодов Рида — Маллера. Такая же оценка справедлива для сложности детерминированных программ, вычисляющих некоторые симметрические булевы функции, включая функцию голосования [6], а также для сложности характеристических функций кодов Боуза — Чоудхури — Хоквингема [1]. Кроме того, из оценки для глубины детерминированной программы [5] следует нелинейная нижняя оценка сложности детерминированных программ, вычисляющих булеву функцию, выражающую некоторое свойство пар чисел. В данной работе получена нижняя оценка  $\Omega(n \log n)$  для сложности как детерминированных, так и недетерминированных ветвящихся программ, вычисляющих характеристические функции БЧХ-кодов при некоторых значениях параметров этих кодов.

В настоящее время известны два метода [1, 7] получения нижних оценок сложности ветвящихся  $k$ -программ, вычисляющих булевы функции. В [1] предложен метод получения сверхполиномиальных оценок сложности детерминированных ветвящихся  $k$ -программ, вычисляющих булевы функции от  $n$  переменных для  $k(n) = O(\log n / \log \log n)$ . Использование нижних оценок, полученных с применением этого метода, для получения нижних оценок сложности для ветвящихся программ без ограничений позволило получить нижние оценки вида  $\Omega(n \log n / \log \log n)$  для сложности вычисления характеристических функций БЧХ-кодов детерминированными ветвящимися программами [1]. В [7] получены сверхполиномиальные нижние оценки сложности недетерминированных ветвящихся  $k$ -программ, вычисляющих булевы функции от  $n$  переменных для  $k(n) = O(\log n)$ . В данной работе используется метод из [7, 9] для получения нижних оценок сложности вычисления характеристических функций БЧХ-кодов ветвящимися  $k$ -программами. Это позволяет получить оценки  $\Omega(n \log n)$  для сложности недетерминированных ветвящихся программ без ограничений, вычисляющих характеристические функции БЧХ-кодов.

---

\*Пусть функция  $t(x)$  от натурального аргумента  $x$  определяется следующей рекурсией:  $t(0) = 1$ ,  $t(x + 1) = 2^{t(x)}$ . Положим  $\log^* n = \max\{x \mid t(x) \leq n\}$ .

В [2] показано, что применяя метод из [1] для оценки сложности ветвящихся  $k$ -программ и теорему о сведении сложности вычисления булевых функций ветвящихся программ без ограничений к вычислению оценок сложности  $k$ -программ [1, 2] для характеристических функций кодов Рида — Маллера, удаётся получить нижние оценки вида

$$\Omega(n \log n / \log \log n),$$

где  $n$  — число переменных реализуемой функции. Это нижняя оценка является наилучшей среди тех, которые получаются прямым применением этого метода. Наилучшая оценка, которая получается применением метода из [7, 9] и теоремы о сведении для характеристических функций кодов Рида — Маллера равна  $\Omega(n \sqrt{\log n \log \log n})$ . В данной работе получены оценки порядка  $n \log n$  для сложности вычисления характеристических функций БЧХ-кодов. Эта оценка является наилучшей из тех, которые могут быть получены применением метода из [7, 9] и теоремы о сведении [1, 2].

### 1. Нижние оценки сложности ветвящихся программ

Через  $\text{NBP}(\mathcal{P})$  и  $\text{NBP}k(\mathcal{P})$  обозначим сложность недетерминированной ветвящейся программы  $\mathcal{P}$  (недетерминированной ветвящейся  $k$ -программы  $\mathcal{P}$ ). Через  $\text{NBP}(f)$  и  $\text{NBP}k(f)$  обозначим соответственно сложности недетерминированных ветвящихся программ и недетерминированных ветвящихся  $k$ -программ, вычисляющих булеву функцию  $f$ .

Идея метода получения нелинейных нижних оценок сложности ветвящихся программ та же, что и в [1, 2].

Пусть  $f(x_1, x_2, \dots, x_n)$  — булева функция,  $X' = \{x_{i_1}, \dots, x_{i_m}\}$  — подмножество множества переменных функции  $f$ , а  $\alpha = \{\alpha_{i_1}, \dots, \alpha_{i_m}\}$  — множество констант. Через  $f|_{X'=\alpha}$  обозначим функцию, которая получается из  $f$  подстановкой констант из  $\alpha$  вместо переменных из  $X'$ , а именно, заменой переменной  $x_{i_j}$  на константу  $\alpha_{i_j}$ ,  $1 \leq j \leq m$ .

**Теорема 1** [2, теорема 1]. Пусть  $g(X)$  — булева функция и  $C$  — константа,  $0 < C < 1$ . Пусть для любого подмножества переменных  $X_0$ ,  $X_0 \subseteq X$  и  $|X_0| = \lfloor Cn \rfloor$ , существует такая подстановка констант из  $\alpha$  в  $X_0$ , что сложность недетерминированных ветвящихся  $k(n)$ -программ, реализующих функции  $g|_{X_0=\alpha}(X \setminus X_0)$ , не менее чем  $n\psi(n)$ , где  $\psi(n)$  — возрастающая функция. Тогда сложность недетерминированных ветвящихся программ без ограничений, реализующих функции  $g$ , не меньше

$$\min\{Cnk(n), n\psi(n)\}.$$

Таким образом, для получения нижних оценок сложности программ без ограничений, реализующих функции  $g$ , надо научиться получать нижние оценки сложности ветвящихся  $k$ -программ, реализующих подфункции функции  $g$ .

Рассмотрим всевозможные представления функции  $f(Y)$ ,  $|Y| = n$ , в виде

$$f(Y) = \bigvee_j f_1^j(Y_1^j \cup Y_0^j) \wedge f_2^j(Y_2^j \cup Y_0^j), \quad (1)$$

где  $Y_1^j$ ,  $Y_2^j$  и  $Y_0^j$  — непересекающиеся множества,  $Y = Y_1^j \cup Y_2^j \cup Y_0^j$ ,  $|Y_1^j| \geq m_1$ ,  $|Y_2^j| \geq m_2$ .

Через  $A(f; n, m_1, m_2)$  обозначим минимальное число дизъюнктивных членов в представлении (1).

I. Подход Е. Окольнішніковой. Идея получения нижних оценок для сложности недетерминированных ветвящихся  $k$ -программ в [2] та же, что и в [1]. Сформулируем теорему 3 из [2] для частного случая.

**Теорема 2** [2, теорема 3]. Пусть  $f$  — булева функция, существенно зависящая от  $n$  переменных,  $n \geq 16$ . Сложность  $\text{NBP}k(f)$  недетерминированных ветвящихся  $k$ -программ, реализующих булеву функцию  $f$ , удовлетворяет неравенству

$$\text{NBP}k(f) \geq \max \left\{ n; \frac{1}{8\sqrt{k}} \cdot (A(f; n, m_1, m_2))^{1/(4k)} \right\},$$

где  $m_1 = \lceil n/(2(ke)^k) \rceil$ ,  $m_2 = \lceil n/(k+1) \rceil$ .

II. Подход А. Бородина, А. Разборова и Р. Смоленского. В этих терминах результаты из [7, 9] могут быть сформулированы следующим образом.

**Теорема 3** [3, теорема 3]. Пусть  $f$  — булева функция, существенно зависящая от  $n$  переменных. Сложность  $\text{NBP}k(f)$  недетерминированных ветвящихся  $k$ -программ, реализующих булеву функции  $f$ , удовлетворяет неравенству

$$\text{NBP}k(f) \geq \max \left\{ n; \frac{1}{2} (A(f; n, m_1, m_2))^{1/(144k^2 \cdot 2^k)} \right\},$$

где  $m_1 = \lceil (2/3)n/2^k \rceil$ ,  $m_2 = \lceil (2/3)n/2^k \rceil$ .

Можно предложить несколько способов для получения нижних оценок величины  $A(f; n, m_1, m_2)$ . В данной работе будет использован тот же способ, что и в [2].

Среди всех  $i$ -мерных граней булева куба размерности  $n$  выделим грань, в которой содержится максимальное число единиц функции  $f$ . Число единиц в этой грани обозначим через  $H_i(f)$ .

Имеет место

**Лемма 1.** Величина  $A(f; n, m_1, m_2)$  удовлетворяет неравенству

$$A(f; n, m_1, m_2) \geq \frac{|f^{-1}(1)|}{2^{n-m_1-m_2} H_{m_1}(f) H_{m_2}(f)}.$$

Используя эту лемму и теоремы 1, 2 и 3, можно доказать следующие теоремы.

**Теорема 4** [3, теорема 6]. Пусть заданы последовательность булевых функций  $g_n(X_n)$ ,  $|X_n| = n$ , возрастающая функция  $k(n)$  и константа  $C$ ,  $0 < C < 1$ . Тогда сложность  $\text{NBP}(g_n)$  любой недетерминированной ветвящейся программы (без ограничений), реализующей функцию  $g_n(X_n)$ , удовлетворяет неравенству

$$\text{NBP}(g_n) \geq \min \left\{ Cnk(n), \frac{1}{8\sqrt{k}} \left( \frac{|g_n^{-1}(1)|}{2^{n-m_1-m_2} H_{m_1}(g_n) H_{m_2}(g_n)} \right)^{1/(4k)} \right\},$$

где  $m_1 = \lceil [(1-C)n] / (2(ke)^k) \rceil$ ,  $m_2 = \lceil [(1-C)n] / (k+1) \rceil$ .

**Теорема 5** [3, теорема 7]. Пусть заданы последовательность булевых функций  $g_n(X_n)$ ,  $|X_n| = n$ , возрастающая функция  $k(n)$  и константа  $C$ ,  $0 < C < 1$ . Тогда сложность  $\text{NBP}(g_n)$  любой недетерминированной ветвящейся программы (без ограничений), реализующей функцию  $g_n(X_n)$ , удовлетворяет неравенству

$$\text{NBP}(g_n) \geq \min \left\{ Cnk(n), \frac{1}{2} \left( \frac{|g_n^{-1}(1)|}{2^{n-m_1-m_2} H_{m_1}(g_n) H_{m_2}(g_n)} \right)^{1/(144k^2 \cdot 2^k)} \right\},$$

где  $m_1 = m_2 = \lceil (2/3) \lceil (1-C)n \rceil 2^{-k} \rceil$ .

Пусть  $B_{2r+1}$  — последовательность характеристических функций БЧХ-кодов с параметрами  $(n, M_n, d_n)$ , где  $d \geq 2r + 1$ ,  $M \geq 2^n / (n + 1)^r$ ,  $n$  — число переменных,  $M$  — число кодовых вершин,  $d_n$  — минимальное расстояние между двумя кодовыми вершинами. Вычислим значение функции  $H_m(B_{2r+1})$ .

Так как все единицы кодовой функции  $B_{2r+1}$  лежат на расстоянии не меньше  $(2r+1)$  друг от друга, то

$$H_m \leq \frac{2^m}{\binom{m}{0} + \binom{m}{1} + \dots + \binom{m}{r}} \leq \frac{2^m}{\binom{m}{r}}. \quad (2)$$

Из формул Стирлинга при  $1 \leq r \leq m/2$  получаем

$$\frac{1}{\pi\sqrt{r}e^{3r^2/4m}} \cdot \left(\frac{me}{r}\right)^r \leq \binom{m}{r} \leq \frac{1}{2} \left(\frac{me}{r}\right)^r. \quad (3)$$

Используя теорему 5, докажем следующее утверждение.

**Теорема 6.** Пусть  $\alpha$ ,  $0 < \alpha < 1/2$ , — константа. Тогда

$$n \log n \preceq \text{NBP}(B_{2n^\alpha+1}) \preceq n^{1+\alpha} \log n.$$

ДОКАЗАТЕЛЬСТВО. Пусть  $C = 1/2$  и

$$r(n) = n^\alpha, \quad k(n) = \beta \log_2 n, \quad (4)$$

где  $\alpha > 0$  и  $\beta > 0$  — константы, причём  $\alpha > \beta$ ,  $\alpha + \beta < 1/2$ . По теореме 5 имеем

$$\text{NBP}(B_{2r(n)+1}) \geq \frac{1}{2} \min \left\{ nk(n), \left( \frac{|B_{2r(n)+1}^{-1}(1)|}{2^{n-m_1-m_2} H_{m_1}(B_{2r(n)+1}) H_{m_2}(B_{2r(n)+1})} \right)^{1/(144k^2 \cdot 2^k)} \right\}, \quad (5)$$

где  $m_1 = m_2 = \lceil (2/3) \lceil n/2 \rceil / n^\beta \rceil$ .\* Подставив оценку (2) в формулу (5), получим

$$\begin{aligned} \text{NBP}(B_{2r(n)+1}) &\geq \frac{1}{2} \min \left\{ nk(n), \left( \frac{2^{n-l_n}}{2^{n-m_1-m_2} \cdot \frac{2^{m_1}}{\binom{m_1}{r}} \cdot \frac{2^{m_2}}{\binom{m_2}{r}}} \right)^{1/(144k^2 \cdot 2^k)} \right\} \\ &\geq \frac{1}{2} \min \left\{ nk(n), \left( \binom{m_1}{r} \cdot \binom{m_2}{r} \cdot \frac{1}{(n+1)^r} \right)^{1/(144k^2 \cdot 2^k)} \right\}. \quad (6) \end{aligned}$$

---

\* Далее в доказательстве этой теоремы вместо обозначения  $r(n)$  будем использовать обозначение  $r$ .

Проверим, что

$$\frac{1}{2} \left( \binom{m_1}{r} \cdot \binom{m_2}{r} \cdot \frac{1}{(n+1)^r} \right)^{1/(144k^2 \cdot 2^k)} \geq \frac{1}{2} k(n) \cdot n. \quad (7)$$

Тогда из (6) следует, что

$$\text{NBP}(B_{2r(n)+1}) \geq \frac{1}{2} k(n) \cdot n.$$

Чтобы иметь возможность воспользоваться формулой (3), а также для оценки величины  $r/m_1$  проверим, что  $m_1/2 \geq r$ .

Поскольку  $m_1 = m_2 = \lceil (2/3) \lceil n/2 \rceil \cdot 2^{-k} \rceil$ ,  $\alpha + \beta < 1/2$ , при достаточно больших  $n$  имеем

$$m_1 \geq (1/3) n^{1-\beta} \geq n^\alpha = r.$$

Используя (3), покажем, что при достаточно больших  $n$  верно неравенство

$$\log_2 \left( \binom{m_1}{r} \cdot \binom{m_2}{r} \cdot \frac{1}{(n+1)^r} \right) \geq r \log_2 n (1 - 2\alpha - 2\beta + o(1)). \quad (8)$$

В самом деле,

$$\begin{aligned} \log_2 \left( \binom{m_1}{r} \cdot \binom{m_2}{r} \cdot \frac{1}{(n+1)^r} \right) &\geq \log_2 \left( \left( \frac{m_1 \cdot m_2 \cdot e^2}{r^2 \cdot (n+1)} \right)^r \cdot \frac{1}{\pi^2 r \cdot e^{3r^2/4m_1 + 3r^2/4m_2}} \right) \\ &\geq r \left( \log_2 m_1 + \log_2 m_2 + 2 \log_2 e - 2 \log_2 r - \log_2(n+1) \right. \\ &\quad \left. - \frac{\log_2 \pi^2 r}{r} - \frac{6r \log_2 e}{4m_1} \right) \geq r ((1 - 2\beta - 2\alpha) \log_2 n - O(1)). \end{aligned}$$

Перейдём к доказательству неравенства (7).

Прологарифмировав левую часть (7) и используя (8), а также соотношение  $\alpha > \beta$ , при достаточно больших  $n$  имеем

$$\begin{aligned} \log_2 \left( \binom{m_1}{r} \cdot \binom{m_2}{r} \cdot \frac{1}{(n+1)^r} \right)^{1/(144k^2 \cdot 2^k)} &\geq \frac{r}{144k^2 2^k} \log_2 n (1 - 2\alpha - 2\beta + o(1)) \\ &= \frac{n^\alpha}{144(\beta \log_2 n)^2 n^\beta} \log_2 n (1 - 2\alpha - 2\beta + o(1)) \\ &\gtrsim 2 \log_2 n \gtrsim \log_2 n + \log_2 \beta + \log_2 \log_2 n. \end{aligned}$$

Неравенство (7) доказано. Из этого неравенства следует нижняя оценка утверждения теоремы.

Поскольку БЧХ — линейные коды, то их можно вычислить как конъюнкцию не более чем  $l$  линейных функций, причём  $l < r \log_2(n + 1)$ . Известно, что сложность вычисления линейной функции от  $n$  переменных детерминированными программами не больше  $2n$ . Из этих фактов следует верхняя оценка утверждения теоремы. Теорема 6 доказана.

### ЛИТЕРАТУРА

1. Окольнішнікова Е. А. Нижние оценки сложности реализации характеристических функций двоичных кодов бинарными программами // Методы дискретного анализа в синтезе реализаций булевых функций: Сб. науч. тр. — Вып. 51. — Новосибирск: Ин-т математики СО АН СССР, 1991. — С. 61–83.
2. Окольнішнікова Е. А. Об одном методе получения нижних оценок сложности реализации булевых функций недетерминированными ветвящимися программами // Дискрет. анализ и исслед. операций. Сер. 1. — 2001. — Т. 8, № 4. — С. 76–112.
3. Окольнішнікова Е. А. О сложности недетерминированных ветвящихся программ, реализующих характеристические функции кодов Риды — Маллера // Дискрет. анализ и исслед. операций. Сер. 1. — 2003. — Т. 10, № 3. С. 67–81.
4. Разборов А. А. Нижние оценки сложности реализации симметрических булевых функций контактно-вентильными схемами // Мат. заметки. — 1990. — Т. 48, вып. 6. — С. 79–90.
5. Ajtai M. A non-linear time lower bound for boolean branching programs // Proc. of the 40th annual Symp. on foundations of Comp. Sci., FOCS '99 (New York, October 17–19, 1999). — Los Alamitos: IEEE Comp. Soc., 1999. — P. 60–70.
6. Babai L., Pudlák P., Rödl V., Szemerédi M. Lower bounds to the complexity of symmetric Boolean functions // Theoret. Comput. Sci. — 1990. — V. 74, N3. — P. 313–324.
7. Borodin A., Razborov A., Smolensky R. On lower bounds for read- $k$ -times branching programs // Computational Complexity. — 1993. — V. 3, N 1. — P. 1–18.
8. Pudlák P. The hierarchy of Boolean circuits // Computers and Artificial Intelligence. — 1987. — V. 6, N 5. — P. 449–468.



- 9. Thathachar J. S.** On separating the read- $k$ -times program hierarchy // Proc. of the 30th Ann. ACM Symp. on Theory of Computing, STOC'98 (Dallas, May 23–26, 1998). — New York: ACM, 1999. — P. 653–662.

*Окольнишникова Елизавета Антоновна,*  
e-mail: okoln@math.nsc.ru

Статья поступила  
10 августа 2009 г.