ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль—сентябрь 2003. Серия 1. Том 10, № 3, 67–81

УДК 519.714.4+ 519.725

О СЛОЖНОСТИ НЕДЕТЕРМИНИРОВАННЫХ ВЕТВЯЩИХСЯ ПРОГРАММ, РЕАЛИЗУЮЩИХ ХАРАКТЕРИСТИЧЕСКИЕ ФУНКЦИИ КОДОВ РИДА-МАЛЛЕРА*)

Е. А. Окольнишникова

Улучшены нижние оценки сложности недетерминированных ветвящихся программ, реализующих характеристические функции некоторых кодов Рида–Маллера.

Введение

Получение нижних оценок сложности дискретных устройств, реализующих последовательности булевых функций — важное направление в теоретической кибернетике и дискретной математике. В последнее десятилетие интенсивно изучаются ветвящиеся программы. Настоящая статья является развитием работ [2, 4]. В ней рассматривается получение нижних оценок сложности недетерминированных ветвящихся программ, реализующих характеристические функции кодов Рида–Маллера. Как и в [2, 4] нижние оценки сложности схем без ограничений получены с помощью нижних оценок для сложности схем с ограничениями, называемых ветвящимися k-программами. В статье используются два метода получения нижних оценок сложности ветвящихся k-программ (в [4] использовался только один метод). Это позволяет повысить нижние оценки сложности таких программ, реализующих характеристические функции кодов Рида–Маллера, и сравнить возможности применения этих двух методов для получения оценок сложности.

*)Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 03-01-00634) и программы поддержки ведущих научных школ (грант НШ–313.2003.1).

В [4] было рассмотрена реализация булевых функций с помощью недетерминированных ветвящихся программ. Проблема получения нелинейных нижних оценок сложности реализации булевых функций в классе схем без ограничений была сведена к проблеме получения нижних оценок сложности реализации булевых функций определенного типа [4], теорема 4) в классе схем с ограничениями, называемых ветвящимися k-программами. Применение этого подхода позволило получить нелинейные нижние оценки сложности недетерминированных ветвящихся программ, реализующих характеристические функции кодов Рида–Маллера.

Обзор результатов по нижним оценкам сложности ветвящихся программ имеется в [4].

В настоящее время известны два метода [2, 5] получения нижних оценок сложности ветвящихся k-программ, реализующих булевы функции. В [2] предложен метод получения экспоненциальных нижних оценок сложности детерминированных ветвящихся k-программ, реализующих булевы функции от n переменных, $k(n) = O(\log n/\log\log n)$. Впоследствии этот метод был использован при исследовании сложности недетерминированных ветвящихся программ [6]. Использование нижних оценок, полученных с применением этого метода, для получения нижних оценок сложности ветвящихся программ без ограничений позволило получить нижние оценки вида $\Omega(n\log n/\log\log n)$ для сложности реализации характеристических функций БЧХ–кодов. В [5] были получены экспоненциальные нижние оценки сложности недетерминированных ветвящихся k-программ, реализующих булевы функции от n переменных, $k(n) = O(\log n)$. Заметим, что методы получения высоких нижних оценок сложности ветвящихся k-программ, реализующих булевы функции, в [2, 6] и [5, 8] похожи.

Пусть $\mathcal{P}$ — ветвящаяся k-программа, реализующая булеву функцию f от n переменных. Каждой единице булевой функции f (т. е. набору, на котором функция f равна 1) поставим в соответствие путь в $\mathcal{P}$. Этот путь делится на «равные» части. Разделяющим множеством для этих частей является или подмножество вершин [2, 6], или подмножество ребер [5, 8] ветвящейся программы. Мощность этого множества зависит только от заранее выбранных параметров и значительно меньше длины пути. Каждому такому выбранному подмножеству вершин или ребер программы $\mathcal{P}$ ставится в соответствие функция f_i. Эта функция зависит только от этого подмножества вершин или ребер и не зависит от пути, которому эти подмножества принадлежат. Таким образом,

$$f = \vee f_i, \tag{1}$$

т. е. множества единиц функций f_i покрывают множество единиц функции f. Если число единиц каждой функции f_i невелико, а число единиц функции f большое, то число различных подмножеств, которые соответствуют единицам булевой функции, велико. Это позволяет получить нижнюю оценку числа вершин (или ребер) ветвящейся программы.

В [2] единицам функции ставились в соответствие подмножества вершин ветвящейся программы. В этом случае возникала необходимость преобразовывать ветвящуюся программу к специальному виду. Это преобразование незначительно увеличивает размер программы и делает возможным рассматривать обобщенные участки пути. При этом появляется возможность ставить в соответствие единице булевой функции не все вершины, которые выбирались в качестве разделяющего множества для пути, соответствующего этой вершине, а только некоторые.

В [5] единицам булевой функции ставились в соответствии подмножества ребер ветвящейся программы. С одной стороны, в этом случае не нужно преобразовывать программу к специальному виду, но, с другой стороны, этот метод не позволяет объединять участки пути, т. е. необходимо приписать пути все ребра, которые являются разделителями частей пути. При использовании этого метода для получения нижних оценок нужно извлекать корень большей, чем в [2], степени из мощности покрытия (1) множества единиц функции.

В [4] был использован метод из [2] для получения нижних оценок сложности ветвящихся k-программ, реализующих подфункции рассматриваемой функции. В ней показано, что применяя этот метод для оценки сложности ветвящихся программ без ограничений, реализующих характеристические функции кодов Рида–Маллера, удается получить нижние оценки вида $\Omega(n \log n / \log\log n)$, где n — число переменных реализуемой функции. Эта нижняя оценка является наилучшей среди тех, которые получаются прямым применением этого метода. В данной статье показано, что метод из [5, 8] для получения нижних оценок сложности ветвящихся k-программ, реализующих подфункции рассматриваемой функции, позволяет улучшить нижние оценки сложности ветвящихся программ, реализующих характеристические функции кодов Рида–Маллера для некоторых значений параметров этих кодов. Таким образом, установлено, что существуют такие функции, для которых совместное использование метода из [5, 8] и теоремы 4 из [4] для получения нижних оценок сложности программ без ограничений дает лучший результат, чем применение метода из [2, 4], и наоборот.

При получении этого результата, как и при получении результата в

[4], существенно используются результаты по обобщенным весам Хемминга для линейных кодов [9]. Кроме того, при получении этого результата использовались также некоторые результаты из [4]. Они будут приведены без доказательств.

Статья организована так же как и работа [4]. В § 1 приводится теорема 1, которая позволяет сводить получение нижних оценок сложности ветвящихся программ без ограничений, реализующих булевы функции, к получению нижних оценок сложности ветвящихся k-программ, реализующих подфункции рассматриваемой функции. В § 2 рассматриваются методы получения нижних оценок сложности ветвящихся k-программ. Теоремы, которые позволяют получать нижние оценки сложности реализации функций программами без ограничений, приведены в § 3. В § 4 результаты по обобщенным весам Хэмминга из [9] используются для подсчета числа единиц в подкубах размерности i для характеристических функций кодов Рида–Маллера. Эти результаты позволяют получить в § 5 нелинейные нижние оценки сложности недетерминированных ветвящихся программ, реализующих характеристические функции кодов Рида–Маллера. Здесь же приведена верхняя оценка сложности ветвящихся программ, реализующих характеристические функции таких кодов.

§ 1. Сведение нижних оценок сложности для программ без ограничений к оценкам сложности для k-программ

Определение недетерминированной ветвящейся программы и ветвящейся k-программы можно найти, например, в [7, 3, 4]. Под сложностью недетерминированной ветвящейся программы (недетерминированной ветвящейся k-программы) понимается число вершин программы, помеченных переменными. Сложность такой программы обозначается через $\mathrm{NBP}(\mathcal{P})$ ($\mathrm{NBP}k(\mathcal{P})$). Через $\mathrm{NBP}(f)$ и $\mathrm{NBP}k(f)$ обозначим соответственно сложности минимальных недетерминированных ветвящихся программ и минимальных недетерминированных ветвящихся k-программ, реализующих булеву функции f.

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

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

Следующая теорема показывает, что нижние оценки сложности ветвящихся программ без ограничений, реализующих булевы функции, можно получать используя ветвящиеся k-программы.

Теорема 1 ([4], 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 α в X_0, что сложность недетерминированных ветвящихся $k(n)$-программ, реализующих функцию $g\big|_{X_0=\alpha}(X \setminus X_0)$, не менее чем $n\psi(n)$, где $\psi(n)$ — растущая функция. Тогда сложность недетерминированных ветвящихся программ без ограничений, реализующих функцию g, не меньше* $\min\{Cnk(n), n\psi(n)\}$.

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

§ 2. Нижние оценки сложности k-программ

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

$$f(Y) = \bigvee_j f_1^j(Y_1^j \cup Y_0^j) \wedge f_2^j(Y_2^j \cup Y_0^j), \tag{2}$$

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

Через $A(f; n, m_1, m_2)$ обозначим минимальное число дизъюнктивных членов в представлении (2).*)

I. *Подход Е.А. Окольнишниковой.* Идея получения нижних оценок для сложности недетерминированных ветвящихся k-программ в [4] та же, что и в [2, 6]. В данной работе теорема 3 из [4] сформулирована для частного случая, когда $p = k$ и $t = k^2 + k$ (см. [4], лемма 3.1). Для этого случая имеем $A\left(f; n, \dfrac{n}{2(ke)^k}, \dfrac{n}{k+1}\right) = R\left(f; n, k, k, k^2 + k\right)$. Так как для любого натурального k выполняется неравенство

$$\frac{1}{4}\sqrt{\frac{2k}{e(k^2+k)}} \geqslant \frac{1}{8\sqrt{k}},$$

*) Это обозначение отличается от аналогичного обозначения в [4]. Изменение обозначений вызвано желанием сформулировать теоремы 2 и 3 в аналогичных терминах.

то теорема 3 из [4] о нижних оценках сложности ветвящихся k-программ может быть сформулирована в следующем виде.

Теорема 2 ([4], теорема 3). *Пусть f — булева функция, существенно зависящая от n переменных, $n \geqslant 16$. Тогда*

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

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

II. *Подход А. Бородина, А. Разборова и Р. Смоленского.*

В аналогичных терминах результаты из [5, 8] могут быть сформулированы следующим образом.

Теорема 3. *Пусть f — булева функция, существенно зависящая от n переменных. Тогда*

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

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

§ 3. Нижние оценки сложно сти ветвящихся программ без ограничений

Из теорем 1, 2 и 3 можно получить следующие утверждения.

Теорема 4. *Пусть заданы последовательность булевых функций $g_n(X_n)$, $|X_n| = n$, растущая функция $k(n)$ и константа C, $0 < C < 1$, и пусть $\Lambda(X_0)$ обозначает множество всевозможных наборов констант $0, 1$, определенных на множестве переменных из X_0. Тогда сложность $\mathrm{NBP}(g_n)$ любой недетерминированной ветвящейся программы, реализующей функцию $g_n(X)$, удовлетворяет неравенству*

$$\mathrm{NBP}(g_n) \geqslant \min_{\substack{X_0, X_0 \subseteq X_n, \\ |X_0| = \lfloor Cn \rfloor}} \max_{\lambda \in \Lambda(X_0)} \min\left\{Ck(n)n, \frac{1}{8\sqrt{k}} \cdot \Big(A(g_n\,|_{X_0=\lambda}; |X_n \setminus X_0|, \left\lceil |X_n \setminus X_0| \Big/ \left(2(ke)^k\right)\right\rceil, \lceil |X_n \setminus X_0| \,/\, (k+1)\rceil)\Big)^{1/(4k)}\right\}.$$

Теорема 5. *Пусть заданы последовательность булевых функций $g_n(X_n)$, $|X_n| = n$, растущая функция $k(n)$ и константа C, $0 < C < 1$,*

и пусть $\Lambda(X_0)$ *обозначает множество всевозможных наборов констант* $0, 1$, *определенных на множестве переменных из* X_0. *Тогда сложность* $\mathrm{NBP}(g_n)$ *любой недетерминированной ветвящейся программы, реализующей функцию* $g_n(X)$, *удовлетворяет неравенству*

$$\mathrm{NBP}(g_n) \geqslant \min_{\substack{X_0 : X_0 \subseteq X_n, \\ |X_0| = \lfloor Cn \rfloor}} \max_{\lambda \in \Lambda(X_0)} \min \Big\{ Ck(n)n, \tfrac{1}{2} \cdot \Big(A(g_n \,|_{X_0 = \lambda}; |X_n \setminus X_0|, \\ \left\lceil 2|X_n \setminus X_0| / \left(3 \cdot 2^k\right) \right\rceil, \left\lceil 2|X_n \setminus X_0| / \left(3 \cdot 2^k\right) \right\rceil \Big) \Big)^{1/(144k^2 \cdot 2^k)} \Big\}.$$

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 [4].

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 $H_i(f)$.

Легко доказать следующее утверждение.

Лемма 1 ([4], лемма 5). *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 лемму 1 и теоремы 4 и 5, можно доказать следующие теоремы.

Теорема 6. *Пусть заданы последовательность булевых функций* $g_n(X_n)$, $|X_n| = n$, *растущая функция* $k(n)$ *и константа* C, $0 < C < 1$. *Тогда*

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

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

Теорема 7. *Пусть заданы последовательность булевых функций* $g_n(X_n)$, $|X_n| = n$, *растущая функция* $k(n)$ *и константа* C, $0 < C < 1$. *Тогда*

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

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

§ 4. Подсчет числа единиц в гранях куба для кодов Рида-Маллера

В данном параграфе приведены результаты параграфа 5 из [4]. При доказательстве этих результатов существенно используются результаты по обобщенным весам Хемминга линейных кодов из [9].

Для кодов Рида–Маллера будем использовать обозначения из [1, 9]. Код Рида–Маллера $\mathcal{R}(u,m)$ рассматривается как линейное пространство, задаваемое булевыми полиномами степени не выше u от m переменных $v_1, v_2, \ldots, v_m$. Известно, что число кодовых вершин в коде $\mathcal{R}(u,m)$ равно

$$2^{1+\binom{m}{1}+\binom{m}{2}+\ldots+\binom{m}{u}}; \tag{3}$$

длина кодовых слов

$$n = 2^m; \tag{4}$$

минимальное расстояние $d = 2^{m-u}$.

Теорема 8 ([4], теорема 7). *Пусть натуральное число s не превосходит u. Тогда в любой $2^m/2^s$-мерной грани булева куба содержится не более $2^{\binom{m-s}{0}+\binom{m-s}{1}+\ldots+\binom{m-s}{u-s}}$ вершин кода $\mathcal{R}(u,m)$.*

§ 5. Нижние оценки сложности ветвящихся программ, реализующих характеристические функции кодов Рида-Маллера

Теоремы 6, 7 и 8 будут использованы для получения нижних оценок сложности произвольных ветвящихся программ, реализующих характеристические функций кодов Рида–Маллера.

Следующая теорема была доказана в [4] с использованием подхода автора.

Теорема 9 ([4], теорема 8). *Пусть $\frac{m}{m-u_m} \to \infty$ при $m \to \infty$ и $m-u \geqslant 3$. Тогда*

$$\mathrm{NBP}(\mathcal{R}(u_m,m)) \geqslant \left(2^m \frac{m}{8(m-u_m)} \Big/ \log_2 \frac{m}{m-u_m}\right).$$

Следствие 1. *Пусть $u_m = m - C^0$, где $C^0 \geqslant 3$ — константа. Тогда*

$$\mathrm{NBP}(\mathcal{R}(u_m,m)) = \Omega(n \log n / \log\log n),$$

где n — число переменных характеристической функции кода Рида–Маллера $\mathcal{R}(u_m, m)$.

Справедливость следующей теоремы доказывается с привлечением теоремы 7, доказанной с использованием подхода А. Бородина, А. Разборова, Р. Смоленского.

Теорема 10. *Пусть $\frac{m}{m-u_m} \to \infty$ при $m \to \infty$ и $m - u \geqslant 3$. Тогда*

$$\mathrm{NBP}(\mathcal{R}(u_m, m)) \geqslant 2^{m-1} \min\left\{\frac{m}{8(m-u_m)}, \frac{m-u_m}{4}\log_2\frac{m}{m-u_m}\right\}.$$

Доказательство. При $C = 1/2$ получим нижнюю оценку для величины

$$R = \frac{\left|(\mathcal{R}(u,m))^{-1}(1)\right|}{2^{n-m_1-m_2}H_{m_1}(\mathcal{R}(u,m))H_{m_2}(\mathcal{R}(u,m))},$$

где $m_1 = m_2 = \left\lceil (1/3)2^m/2^k \right\rceil$. Сначала покажем, что если $k \leqslant \frac{m}{8(m-u)}$, то выполняется неравенство

$$R \geqslant 2^{0{,}14\binom{m}{m-u-1}}.$$

Так как $\frac{m}{m-u_m} \to \infty$ при $m \to \infty$, то можно предположить, что

$$\frac{m}{m-u_m} \geqslant 2^{16}. \tag{5}$$

Пусть

$$k \leqslant \frac{m}{8(m-u)}. \tag{6}$$

В этом случае имеем

$$m_1 = m_2 = \left\lceil (1/3)2^m/2^k \right\rceil \geq 2^m/2^{s_0}, \tag{7}$$

где

$$s_0 = \left\lfloor \frac{m}{4(m-u)} \right\rfloor. \tag{8}$$

Так как при $n' \leqslant n''$ справедливо неравенство

$$H_{n''}(f) \leqslant 2^{n''-n'}H_{n'}(f),$$

то при уменьшении величин m_1, m_2 оценка из теоремы 7 остается справедливой. Поэтому можно считать, что $m_1 = m_2 = \frac{2^m}{2^{s_0}}$. Из этого факта и теоремы 8 следует, что

$$H_{m_1}(\mathcal{R}(u_m, m)) = H_{m_2}(\mathcal{R}(u_m, m)) \leqslant 2^{\binom{m-s_0}{0}+\binom{m-s_0}{1}+\ldots+\binom{m-s_0}{u-s_0}}. \tag{9}$$

Используя (3), (9), получаем

$$\begin{aligned} R &\geqslant \frac{2^{1+\binom{m}{1}+\binom{m}{2}+\ldots+\binom{m}{u}}}{2^{2^m-2^{m-s_0}-2^{m-s_0}}\cdot 2^{\binom{m-s_0}{0}+\binom{m-s_0}{1}+\ldots+\binom{m-s_0}{u-s_0}}\cdot 2^{\binom{m-s_0}{0}+\binom{m-s_0}{1}+\ldots+\binom{m-s_0}{u-s_0}}} \\ &= \frac{2^{2\cdot\sum\limits_{j=u-s_0+1}^{m-s_0}\binom{m-s_0}{j}}}{2^{\sum\limits_{j=u+1}^{m}\binom{m}{j}}} = \frac{2^{2\cdot\sum\limits_{j=0}^{m-u-1}\binom{m-s_0}{j}}}{2^{\sum\limits_{j=0}^{m-u-1}\binom{m}{j}}} \\ &= 2^{\sum\limits_{j=0}^{m-u-1}\left(2\binom{m-s_0}{j}-\binom{m}{j}\right)}. \end{aligned} \tag{10}$$

Поэтому при получении нижней оценки для R надо оценить снизу значение величины $\binom{m-s}{j}/\binom{m}{j}$ при $j \leqslant m-u-1$. Для этой цели воспользуемся (8), условиями теоремы и предположением (5). Имеем

$$m \geqslant 3\cdot 2^{16}; \quad 3 \leqslant m-u \leqslant m/2^{16}.$$

В [4] было показано, что если $j \leqslant m-u-1$ и $s \leq \frac{m}{4(m-u)}$, то при данных предположениях справедливо соотношение

$$\binom{m-s}{j}\Big/\binom{m}{j} \geq -\frac{2sj}{m} - 0,048.$$

Отсюда, а также из (8) и (5) получаем

$$\begin{aligned} \binom{m-s_0}{j}\Big/\binom{m}{j} &\geqslant \exp\left\{-\frac{2s_0j}{m} - 0,048\right\} \\ &\geqslant \exp\left\{-\tfrac{2m}{4(m-u)}(m-u-1)/m - 0,048\right\} \\ &\geqslant \exp\{-0,5-0,048\} \geqslant 0,57. \end{aligned} \tag{11}$$

Из (11) и (10) следует, что

$$\begin{aligned} R &\geqslant 2^{2\cdot\sum\limits_{j=0}^{m-u-1}\left(\binom{m-s_0}{j}+\binom{m-s_0}{j}-\binom{m}{j}\right)} \geqslant 2^{\sum\limits_{j=0}^{m-u-1}(1,14-1)\binom{m}{j}} \\ &\geqslant 2^{0,14\sum\limits_{j+0}^{m-u+1}\binom{m}{j}} \geqslant 2^{0,14\binom{m}{m-u-1}}. \end{aligned} \tag{12}$$

Пусть

$$k \leqslant \min\left\{\frac{m}{8(m-u)}; \frac{(m-u)}{4}\log_2\frac{m}{m-u}\right\}. \tag{13}$$

По теореме 7 для получения требуемой в формулировке теоремы оценки достаточно доказать, что $(1/2)R^{1/(144k^2 2^k)} \geqslant nk/2$. Так как $k \leqslant \frac{m}{8(m-u)}$, то справедливо неравенство (6), и, следовательно, выполняется соотношение (12).

Легко проверить, что при $m - u \leqslant m/4$ справедливо неравенство

$$\begin{aligned}\binom{m}{m-u-1} &= \frac{(m-u)\cdot m\cdot(m-1)\cdot\ldots\cdot(u+2)}{(m-u)\cdot(m-u-1)!}\\ &\geqslant (m-u)\left(\tfrac{m}{m-u}\right)^{m-u-1}.\end{aligned} \tag{14}$$

Из теоремы 7 и неравенств (13), (5), (12), (14) и (4) следует, что

$$\begin{aligned}&\mathrm{NBP}(\mathcal{R}(u,m)) \geqslant \min\left\{\tfrac{nk}{2}; \tfrac{1}{2}\cdot R^{1/(144k^2 2^k)}\right\}\\ &\geqslant \min\left\{\tfrac{nk}{2}; \tfrac{1}{2}\cdot 2^{0{,}14\cdot\frac{(m-u)^2}{m}\cdot(\frac{m}{m-u})^{m-u}\Big/\left(144\left(\frac{m-u}{4}\right)^2\log_2^2\frac{m}{m-u}\cdot 2^{\frac{m-u}{4}\log_2\frac{m}{m-u}}\right)}\right\}\\ &\geqslant \min\left\{\frac{nk}{2}; \frac{1}{2}\cdot 2^{0{,}005\cdot 2^{3/4(m-u)\log_2\frac{m}{m-u}}\Big/\left(m\log_2^2\frac{m}{m-u}\right)}\right\}.\end{aligned} \tag{15}$$

При $m - u \geqslant (1/4)\log_2 m$ и предположениях (5) имеем

$$\frac{0{,}005\cdot 2^{3/4(m-u)\log_2\frac{m}{m-u}}}{m\log_2^2\frac{m}{m-u}} - 1 \geqslant \frac{0{,}005\cdot m^3}{m\log_2^2\frac{m}{m-u}} - 1 \geqslant 9/8m. \tag{16}$$

При $m - u \leqslant (1/4)\log_2 m$, предположениях теоремы и (5) имеем

$$\begin{aligned}&\frac{0{,}005\cdot 2^{3/4(m-u)\log_2\frac{m}{m-u}}}{m\log_2^2\frac{m}{m-u}} - 1 \geqslant \frac{0{,}005\cdot 2^{9/4(\log_2 m-\log_2\log_2 m)}}{m\log_2^2\frac{m}{m-u}} - 1\\ &\geqslant \frac{0{,}005\cdot m^{9/4}}{m\,\log_2^2\frac{m}{m-u}\,(\log_2 m)^{9/4}} - 1 \geqslant 9/8m.\end{aligned} \tag{17}$$

Из (15)–(17) следует, что

$$\begin{aligned}&\mathrm{NBP}(\mathcal{R}(u,m)) \geqslant \min\left\{\tfrac{2^m}{2}\cdot\min\left\{\left\lfloor\tfrac{m}{4(m-u)}\right\rfloor - 2; \left\lfloor\tfrac{(m-u)}{4}\log_2\tfrac{m}{m-u}\right\rfloor\right\};\right.\\ &\left.2^{(9/8)m}\right\} \geqslant \tfrac{2^m}{2}\cdot\min\left\{\tfrac{m}{8(m-u)}; \tfrac{(m-u)}{4}\log_2\tfrac{m}{m-u}\right\}.\end{aligned}$$

Теорема 10 доказана.

Из теорем 9 и 10 получаем следующее утверждение.

Теорема 11. *Пусть* $\frac{m}{m-u_m} \to \infty$ *при* $m \to \infty$ *и* $m - u_m \geqslant 3$. *Тогда*

$$\mathrm{NBP}(\mathcal{R}(u_m, m)) \geqslant \frac{2^m}{2} \max\left\{ \frac{m}{4(m-u_m)} \Big/ \log_2 \frac{m}{m-u_m}, \min\left\{ \frac{m}{8(m-u_m)}, \frac{m-u_m}{4} \log_2 \frac{m}{m-u_m} \right\} \right\}.$$

Следствие 2. *Пусть* $\frac{m}{m-u_m} \to \infty$ *при* $m \to \infty$ *и* $m - u_m \geqslant 3$. *Тогда*

$$\mathrm{NBP}(\mathcal{R}(u_m, m)) \succcurlyeq \begin{cases} \frac{2^m m}{(m-u_m)} \Big/ \log_2 \frac{m}{m-u_m}, & \text{если } m - u_m \leqslant h; \\ 2^m \sqrt{m}, & \text{если } h \leqslant m - u_m \leqslant \frac{\sqrt{m}}{\log_2 \sqrt{m}}; \quad (18) \\ \frac{2^m (m-u_m)}{8} \log_2 \frac{m}{m-u_m}, & \text{если } \frac{\sqrt{m}}{\log_2 \sqrt{m}} \leqslant m - u_m \leqslant h_1; \\ 2^m \sqrt{m \log_2 m}, & \text{если } h_1 \leqslant m - u \leqslant \frac{\sqrt{m}}{\sqrt{\log_2(m)}}; \quad (19) \\ \frac{2^m m}{16(m-u_m)}, & \text{если } \frac{\sqrt{m}}{\sqrt{\log_2 m}} \leqslant m - u_m, \end{cases}$$

где $h = 2\sqrt{m}\left(1 - \frac{4 \log_2 \log_2 \sqrt{m}}{\log_2 m}\right) / \log_2 m$,

$h_1 = \sqrt{m / \log_2 m}\left(1 - \frac{2 \log_2 \log_2 m}{\log_2 m}\right)$.

Доказательство. Положим

$$\begin{aligned} X &= 2^{m-1} \frac{m}{4(m-u_m)} \Big/ \log_2 \frac{m}{m-u_m}; \\ Y &= 2^{m-1} \frac{m}{8(m-u_m)}; \\ Z &= 2^{m-1} \frac{m-u_m}{4} \log_2 \frac{m}{m-u_m}. \end{aligned}$$

По теореме 11 имеем

$$\mathrm{NBP}(\mathcal{R}(u_m, m)) \geqslant \max\{X, \min\{Y, Z\}\}. \quad (20)$$

Для простоты обозначений опустим индексы при u_m. Возможны 6 случаев упорядочения чисел X, Y, Z. Поскольку $X < Y$ при $m \to \infty$, то нужно рассмотреть только три случая:

1. Пусть $X \leqslant Y \leqslant Z$.

2. Пусть $X \leqslant Z \leqslant Y$.

3. Пусть $Z \leqslant X \leqslant Y$.

Ниже приведено доказательство только случая 2. Случаи 1 и 3 рассматриваются аналогично.

Случай 2. Пусть $m - u_m$ удовлетворяет неравенствам

$$m - u_m \geqslant \frac{\sqrt{m}}{\log_2 \sqrt{m}}, \tag{21}$$

$$m - u_m \leqslant \frac{\sqrt{m}\left(1 - \frac{2\log_2\log_2 m}{\log_2 m}\right)}{\sqrt{\log_2(m)}}. \tag{22}$$

Докажем, что в этом случае $X \leqslant Z \leqslant Y$. Тогда из теоремы 11 (см. также (20)) будет следовать, что

$$\mathrm{NBP}(\mathcal{R}(u_m, m)) \geqslant Z = 2^{m-1}\frac{m-u_m}{4}\log_2\frac{m}{m-u_m}.$$

Случай 2.1. Нужно проверить, что при $(m-u) \geqslant \frac{\sqrt{m}}{\log_2\sqrt{m}}$ выполняется неравенство

$$\frac{m}{m-u}\Big/\log_2\frac{m}{m-u} \leqslant (m-u)\log_2\frac{m}{m-u}. \tag{23}$$

Из $(m-u) \geqslant \frac{\sqrt{m}}{\log_2\sqrt{m}}$ следует, что $\frac{m}{m-u} \leqslant \sqrt{m}\log_2\sqrt{m}$. Функция $\left(\frac{m}{m-u}\right)^2 \Big/ \log_2^2\left(\frac{m}{m-u}\right)$ монотонна по $\left(\frac{m}{m-u}\right)^2$. Следовательно, выполняется неравенство

$$\left(\frac{m}{m-u}\right)^2 \Big/ \log_2^2\left(\frac{m}{m-u}\right) \leqslant \frac{m\log_2^2\sqrt{m}}{(\log_2\sqrt{m} + \log_2\log_2\sqrt{m})^2} \leqslant m.$$

Отсюда следует справедливость неравенства (23). В этом случае следствие доказано.

Случай 2.2. Нужно проверить, что если

$$m - u \leqslant \frac{\sqrt{m}}{\sqrt{\log_2 m}}\left(1 - \frac{2\log_2\log_2 m}{\log_2 m}\right),$$

то выполняется неравенство

$$\frac{m}{2(m-u)} \geqslant (m-u)\log_2\frac{m}{m-u}. \tag{24}$$

Из неравенства (22) следует, что

$$\frac{m}{m-u} \geqslant \frac{\sqrt{m\log_2 m}}{\left(1 - \frac{2\log_2\log_2 m}{\log_2 m}\right)}$$

и

$$\frac{m^2}{(m-u)^2} \geqslant \frac{m\log_2 m}{\left(1-\frac{2\log_2\log_2 m}{\log_2 m}\right)^2}.$$

Пусть $\varepsilon = \frac{\log_2\log_2 m}{\log_2 m}$. Функция $\left(\frac{m}{m-u}\right)^2 \Big/ \log_2\left(\frac{m}{m-u}\right)^2$ является монотонной по $\left(\frac{m}{m-u}\right)^2$ при $\frac{m}{m-u} \geqslant l$. Поэтому при $m \to \infty$ имеем

$$\begin{aligned}\frac{\left(\frac{m}{m-u}\right)^2}{\log_2\left(\frac{m}{m-u}\right)^2} &\geqslant \frac{m\log_2 m}{(1-q)^2\left(\log_2 m + \log_2\log_2 m - 2\log_2(1-q)\right)} \\ &\geqslant \frac{m\log_2 m}{(1-2\varepsilon)^2\log_2 m\left(1+\varepsilon-\frac{2\log_2(1-2\varepsilon)}{\log_2 m}\right)} \\ &= \frac{m}{1-3\varepsilon+4\varepsilon^3-o(\varepsilon)} \geqslant m,\end{aligned}$$

где $q = \dfrac{2\log_2\log_2 m}{\log_2 m} = 2\varepsilon$.

Отсюда следует выполнение неравенства (24). В этом случае следствие доказано.

Несложно проверить, что неравенства (18) и (19) также выполняются. Следствие 2 доказано.

Теорема 12. *Для кодов Рида–Маллера $\mathcal{R}(u,m)$ справедлива оценка*

$$\mathrm{NBP}(\mathcal{R}(u_m,m)) \leqslant 2^{m+1+1+\binom{m}{1}+\binom{m}{2}+\ldots+\binom{m}{m-u-1}}.$$

Доказательство. Код Рида–Маллера $\mathcal{R}(u,m)$ — линейный код и число проверочных символов в нем равно (см. [1]) $2^{1+\binom{m}{1}+\binom{m}{2}+\ldots+\binom{m}{m-u-1}}$.

Сложность минимальной ветвящейся программы, реализующей линейную функцию, не превышает $2n$. Поэтому сложность такой программы, реализующей характеристическую функцию кода Рида–Маллера $\mathcal{R}(u,m)$, не превышает $2\cdot 2^m\cdot 2^{1+\binom{m}{1}+\binom{m}{2}+\ldots+\binom{m}{m-u-1}}$. Теорема доказана.

Из теоремы (12) и следствия 1 вытекает

Следствие 3. *Пусть $u_m = m - C^0$, где C^0 — константа, не меньшая* 3.

Тогда

$$n \log n / \log\log n \preccurlyeq \mathrm{NBP}(\mathcal{R}(u_m, m)) \preccurlyeq n \log^{C_0 - 1} n,$$

где n — число переменных характеристической функции кода Рида–Маллера $\mathcal{R}(u_m, m)$.

Литература

1. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. **Окольнишникова 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.
3. **Окольнишникова Е. А.** Сложность ветвящихся программ// Математические вопросы кибернетики. Вып. 10. М.: Физматлит. 2001. С. 69–82.
4. **Окольнишникова 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.
5. **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.
6. **Okol'nishnikova E. A.** On the hierarchy of nondeterministic branching k-programs// Fundamentals of computation theory. 11th International symposium, FCT 97. Berlin: Springer, 1997. P. 376–387. (Lecture Notes in Comput. Sci.; V. 1279).
7. **Razborov A. A.** Lower bounds for deterministic and nondeterministic branching program// Fundamentals of computation theory. 8th International symposium, FCT 91 (Gosen, Germany, September 9-13, 1991). Proc. Berlin: Springer, 1991. P. 47–61. (Lecture Notes in Comput. Sci.; V. 529).
8. **Thathachar J. S.** On separating the read-k-times program hierarchy// Proc. of the 30th annual ACM Symposium on theory of comptuting (Dallas, 1998). New York: ACM Press, 1998. P. 652–662.
9. **Wei V.K.** Generalized Hamming weights for linear codes// IEEE Trans. on Inform. Theory. 1991. V. 37, N 5. P. 1412–1418.

Адрес автора:

Институт математики
им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090 Новосибирск,
Россия

Статья поступила
19 мая 2003 г.