На правах рукописи

ОКОЛЬНИШНИКОВА Елизавета Антоновна

# МЕТОДЫ ПОЛУЧЕНИЯ НИЖНИХ ОЦЕНОК СЛОЖНОСТИ ВЕТВЯЩИХСЯ ПРОГРАММ, ВЫЧИСЛЯЮЩИХ БУЛЕВЫ ФУНКЦИИ

специальность 01.01.09 — дискретная математика и математическая кибернетика

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
доктора физико-математических наук

Новосибирск — 2007

Работа выполнена в Институте математики им. С. Л. Соболева СО РАН РФ

**Официальные оппоненты:**

доктор физико-математических наук, профессор
Аблаев Фарид Мансурович

доктор физико-математических наук, профессор
Мошков Михаил Юрьевич

доктор физико-математических наук, профессор
Шоломов Лев Абрамович

**Ведущая организация:**

механико-математический факультет Московского государственного университета им. М.В. Ломоносова

Защита состоится 24 октября 2007 г. в ____ час. ____ мин. на заседании диссертационного совета Д 003.015.01 при Институте математики им. С. Л. Соболева СО РАН : 630090, г. Новосибирск, пр. Академика Коптюга, 4, к. 417.

С диссертацией можно ознакомиться в библиотеке Института математики им. С. Л. Соболева СО РАН.

Автореферат разослан "_____" сентября 2007 г.

Ученый секретарь
диссертационного совета
д.ф.-м.н. Ю.В. Шамардин

# ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы.** Теория сложности вычислений является важным разделом математической кибернетики. Целью теории является оценивание величины ресурсов, необходимых для решения тех или иных вычислительных задач. Рассматриваются различные модели вычисления такие, например, как машины Тьюринга, автоматы, нормальные алгоритмы, схемы из функциональных элементов, формулы в различных базисах и т. д.[1)] В качестве оцениваемых ресурсов рассматриваются время вычисления, объем используемой памяти, длина программы и др. Под сложностью вычисления понимается величина этого ресурса. При этом сложность зависит как от модели вычислений, так и от выбранного оцениваемого ресурса. Основным объектом теории является получение верхних и нижних оценок сложности. При этом получение нижних оценок сложности в большинстве рассматриваемых моделях вычислений представляет наибольшую трудность. Это объясняется тем, что при установлении нижних оценок сложности надо в той или иной мере просмотреть все возможные способы вычисления рассматриваемого объекта и показать, что вычислить этот объект с меньшими затратами невозможно. При получении нижних оценок сложности возникают, решаются и используются важные и интересные задачи из различных областей дискретной математики.

Известно [2, 4, 5, 18, 19], что во многих моделях вычисления, таких как схемы из функциональных элементов, контактные схемы, формулы в конечных базисах, ветвящиеся программы, почти все булевы функции вычисляются очень сложно (экспонента от числа переменных функции), тем не менее, лишь для небольшого числа полностью определенных булевых функций доказано, что их нельзя вычислить с

[1)] Важным понятием в теории сложности является также сложность объектов по Колмогорову, введенная в [3] для алгоритмического определения понятия количества информации.

линейной сложностью (для схем из функциональных элементов удалось получить лишь линейные оценки) относительно числа переменных булевой функции. К этому направлению относятся работы А. А. Разборова [8] и А. Е. Андреева [1], в которых были получены сверхполиномиальные[2)] нижние оценки сложности для схем из функциональных элементов в монотонном базисе, реализующих известные функции.

Сложность вычисления булевой функции зависит от модели вычисления. Так, например, линейная булева функция вычисляется с линейной сложностью в классе схем из функциональных элементов, контактных схем, ветвящихся программ, но реализуется схемой не менее чем квадратичной сложности в классе формул в базисе $(\vee, \wedge, \neg)$, и дизъюнктивными нормальными формами не менее чем экспоненциальной сложности.

В связи с этим возникает проблема нахождения таких функций, для которых удается получить нетривиальные нижние оценки сложности в данной модели вычислений. Удобным объектом для изучения сложности являются характеристические функции двоичных кодов. Эти функции детально изучаются в дискретной математике, в частности, в теории кодов, исправляющих ошибки. Интерес к этим функциям вызван как их структурными свойствами (одним из таких свойств является «достаточно равномерная» распределенность множества единиц значений характеристических функций этих кодов по $n$-мерному булеву кубу), так и широким практическим применением.

В данной работе рассматриваются вопросы сложности ветвящихся программ, вычисляющих булевы функции, а также операции над булевыми функциями, которые позволяют из просто вычислимых функций получать функции большей сложности.

---

[2)] Функция $\phi(n)$ называется сверхполиномиальной, если ее можно представить в виде $\phi(n) = n^{\psi(n)}$, где $\psi(n) \to \infty$ при $n \to \infty$.

Ветвящиеся программы — математическая модель вычислений, хорошо моделирующая работу компьютерных программ, состоящих из условных операторов. Этот класс схем активно изучается в последнее время различными авторами. Первыми работами, в которых рассматривались ветвящиеся программы, были [2, 14, 15].

*Детерминированной ветвящейся программой* от переменных $x_1, \ldots, x_n$ называется ориентированный граф без циклов с одной входной вершиной и двумя выходными вершинами, одна из которых помечена нулем, другая — единицей. Из каждой вершины, за исключением выходных, выходит ровно две дуги, одна из которых помечена нулем, другая — единицей. Все невыходные вершины помечены переменными из множества $\{x_1, \ldots, x_n\}$.

Под сложностью детерминированной ветвящейся программы понимается число вершин программы, помеченных переменными.

Булева функция $f(x_1, \ldots, x_n)$ принимает значение 1 на наборе $(a_1, \ldots, a_n)$, если существует путь от входной вершины к выходной вершине, помеченной единицей, который из вершин, помеченных переменной $x_i$, проходит по дугам, помеченных $a_i$. Через $\mathrm{BP}(f)$ обозначим сложность минимальной детерминированной ветвящейся программы, вычисляющей функцию $f$. Любую булеву функции от $n$ переменных можно вычислить детерминированной ветвящейся программой, сложность которой асимптотически не превосходит $2^n/n$.

В недетерминированных программах некоторые вершины становятся непомеченными и из каждой такой вершины выходит ровно две непомеченные дуги.

Булева функция $f$ принимает значение 1 на наборе $(a_1, \ldots, a_n)$, если существует путь от входной вершины к выходной вершине, помеченной единицей, который из вершин, помеченных переменной $x_i$, проходит по дугам, помеченных $a_i$. Под сложностью недетерминированной программы понимается число вершин, помеченных переменными. Через

$\mathrm{NBP}(f)$ обозначим сложность минимальной недетерминированной ветвящейся программы, вычисляющей функцию $f$. Любую булеву функции от $n$ переменных можно вычислить недетерминированной ветвящейся программой, сложность которой не превосходит $C2^{n/2}$, где $C$ — некоторая постоянная (эта оценка следует из результата О. Б. Лупанова для контактно-вентильных схем [4]).

В дальнейшем под программами будут пониматься только ветвящиеся программы и поэтому слово «ветвящаяся» часто будет опускаться.

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 [16] с помощью метода Нечипорука. Этот метод основан на мощностных соображениях и применим только к функциям специального вида, вычислимых в тех моделях, для которых сложность определяется через число элементов, помеченных переменными (контактные схемы, формулы, ветвящиеся программы и т. д.). Из оценки А. А. Разборова для контактно-вентильных схем [9] следует нижняя оценка $\Omega(n \log\log\log^* n)$[3)] для сложности недетерминированных программ, вычисляющих симметрические булевы функции, включая функцию голосования. Е. А. Окольнишниковой [32, 34] 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 [11], а также характеристические функции кодов

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

Боуза–Чоудхури–Хоквингема [25]. Кроме того, из оценки для глубины детерминированной программы [10] следует нелинейная нижняя оценка сложности детерминированных программ, вычисляющих булеву функцию, выражающую некоторое свойство пар чисел.

Изучаются также ветвящиеся программы с ограничениями на структуру схем. Одно из таких ограничений — ограничение на число проверок переменных в цепи, когда в любой цепи, идущей от входной вершины к выходной, вершины, помеченные любой переменной, встречаются не более $k$ раз. Такие программы называются ветвящимися $k$-программами ($k$-программами). Через $\mathrm{BP}k(f)$ и $\mathrm{NBP}k(f)$ обозначим сложность минимальных детерминированной и недетерминированной ветвящейся $k$ программ, вычисляющих функцию $f$.

Получены сверхполиномиальные нижние оценки сложности вычисления булевых функций детерминированными $k$-программами при $k \leq \log n / \log\log n$ [25] и недетерминированными $k$-программами при $k \leq \log n$ [12].

Так как одну и ту же функцию можно вычислить $k$-программами с различными значениями $k$, возникает вопрос о соотношении сложностей $k_1$- и $k_2$-программ, вычисляющих одну и ту же булеву функцию при $k_1 \neq k_2$. В ряде работ показано, что сложности 1- и 2-программ, вычисляющих одну и ту же последовательность функций, могут отличаться в сверхполиномиальное число раз (по числу переменных булевой функции) [13, 24, 37]).

В [28] конструктивно показано, что для любого натурального $k$, $k \geq 2$, существует последовательность булевых функций такая, что сложность недетерминированных $k$-программ, вычисляющих функции из этой последовательности, в сверхполиномиальное число раз (по числу переменных функции) превосходит сложность недетерминированных $(k \ln k / \ln 2 + C)$-программ (где $C$ — константа, не зависящая от $k$), вычисляющих ту же функцию. Оценка

была получена с помощью модификации метода получения нижних оценок сложности ветвящихся $k$-программ из [25]. Позднее Дж. Тхатхачаром [20] были приведены примеры таких последовательностей булевых функций, что сложность недетерминированных $k$-программ, вычисляющих функции из этой последовательности, в сверхполиномиальное число раз (по числу переменных функции) превосходит сложность недетерминированных $(k+1)$-программ, вычисляющих ту же функцию (оценка была получена с помощью метода из [12]).

Автором диссертации [25, 32] предложен метод, позволяющий сводить получение нижних оценок сложности программ без ограничений на структуры, вычисляющих булевы функции, к получению нижних оценок сложности $k$-программ, вычисляющих подфункции рассматриваемой функции. Применение этого метода позволило получить нелинейные нижние оценки сложности недетерминированных программ, вычисляющих характеристические функции кодов Рида–Маллера. Схемы с ограничениями рассматривались в работах многих авторов. Сверхполиномиальные нижние оценки для схем из функциональных элементов в монотонном базисе были получены А. А. Разборовым [8] и А. А. Андреевым [1]. Кроме того, С. В. Кузнецов, Е. А. Окольнишникова, А. К. Пулатов, Г. А. Ткачев и др. получили сверхполиномиальные нижние оценки для схем с различными ограничениями на структуру. Тем не менее, метод, изложенный в диссертации, является, видимо, первым методом, с помощью которого удалось получить нетривиальные нижние оценки для схем без ограничений, существенно используя нижние оценки сложности схем с ограничениями.

С рассмотрением факторов, влияющих на сложность вычисления булевых функций, связано рассмотрение операций над булевыми функциями, которые позволяют из просто вычислимых функций получать сложно вычислимые, в том числе и в классе программ. В [6, 7] было показано, что операция геометрического проектирования множества единиц

булевой функции на подмножество переменных этой функции может приводить к существенному усложнению функции, и построены примеры последовательностей функций, сложность вычисления которых как контактными схемами, так и формулами в любом конечном базисе существенно меньше сложности вычисления геометрической проекции этих функций по некоторому подмножеству переменных такими же схемами. В диссертации построен аналогичный пример функции для ветвящихся программ.

В [30] была введена операция *монотонного расширения* булевой функции. Монотонное расширение булевой функции $f$ — это монотонная булева функция с минимальным числом единиц, являющаяся расширением функции $f$. В диссертации показано, что операция монотонного расширения булевых функций может приводить к существенному усложнению функции, и построены примеры последовательностей функций, сложность вычисления которых контактными схемами, формулами в любом конечном базисе, ветвящимися программы существенно меньше сложности вычисления монотонного расширения этих функций.

**Научная новизна.** Все основные результаты диссертации являются новыми. Укажем наиболее важные из них.

— В диссертации предложен метод получения сверхполиномиальных нижних оценок сложности $k$-программ. С его помощью получена сверхполиномиальная нижняя оценка сложности ветвящихся $k$-программ, вычисляющих характеристические функции кодов Боуза–Чоудхури–Хоквингема (БЧХ–коды)

— Предложена модификация метода получения сверхполиномиальных нижних оценок сложности ветвящихся $k$-программ, вычисляющих булевы функции, которая (модификация) позволяет получать сверхполиномиальные нижние оценки сложности для функций, заданных на переменных, соответствующих ребрам графов, гиперграфов и иных объектах, имеющих многомерную природу. Получена

сверхполиномиальная нижняя оценка сложности вычисления характеристической функции свойства гиперграфов не содержать изолированных вершин. Показано, что для любого натурального $k$, $k \geq 2$, существует последовательность булевых функций такая, что сложность недетерминированных $k$-программ в сверхполиномиальное (по числу переменных булевой функции) число раз превосходит сложность $\lceil k \ln k / \ln 2 + C \rceil$-программ ($C$ — константа, не зависящая от $k$), вычисляющих функции из этой последовательности.

— Предложен метод получения нелинейных нижних оценок сложности детерминированных и недетерминированных программ, вычисляющих булевы функции. С его помощью получена оценка $\Omega(n \log n / \log \log n)$ для сложности детерминированных и недетерминированных программ, вычисляющих характеристические функции кодов Рида–Маллера и БЧХ–кодов (при некоторых значениях параметров этих кодов).

— Введена операция монотонного расширения булевой функции. Показано, что операции геометрического проектирования и монотонного расширения булевой функции могут приводить к существенному росту сложности схем, вычисляющих булевы функции для некоторых моделей вычисления, в том числе, для программ и для $k$-программ. Указывается на связь между операцией геометрического проектирования и монотонного расширения булевых функций.

**Методика исследования.** В работе используются методы дискретной математики и математической кибернетики.

**Практическая и теоретическая ценность.** Работа носит теоретический характер. Ее результаты могут быть использованы при исследовании различных вопросов сложности булевых функций.

**Апробация.** Результаты работы докладывались на следующих научных конференциях и семинарах: конференции «Проблемы теоретической кибернетики» (Иркутск, 1986; Горький, 1988; Нижний Новгород, 1999; Казань, 2002; Пенза, 2005), III конференция по прикладной логике (Новосибирск,

1992), V Международная конференция «Дискретные модели в теории управляющих систем» (Ратмино, 2003), III Международном симпозиуме «Stochactic algorithms: foundations and applications» (SAGA 2005) (Москва, 2005), Российская конференция «Дискретный анализ и исследование операций» (Новосибирск, 2002, 2004), 11-ый Международный симпозиум ее приложения» (Москва, 1993, 2004), Всесоюзные и Международные школы-семинары «Синтез и сложность управляющих систем» (Львов, 1988; Нижний Новгород, 1998; Нижний Новгород, 2000; Пенза, 2001; Нижний Новгород, 2003; Новосибирск, 2004), школа-семинар «Сложность булевых функций» (Казань, 1999), V Сибирская научная школа-семинар «Компьютерная безопасность и криптография» SIBERCRYPT'06 (Шушенское, 2006), в Международном математическом центре им. С. Банаха (Варшава, 1991), на семинарах «Complexity of Boolean functions» (Dagstuhl, 1999, 2001), в МГУ на семинаре «Математические вопросы кибернетики» (руководитель О. Б. Лупанов), на семинаре «Дискретный анализ» Института математики им. С. Л. Соболева СО РАН (руководители А. А. Евдокимов и А. Д. Коршунов).

**Публикации.** По теме диссертации опубликовано 28 работ, список которых приведен в конце автореферата.

**Структура диссертации.** Диссертация состоит из введения, пяти глав, и списка литературы, содержащего 123 наименований. Полный объем диссертации — 185 страниц.

## СОДЕРЖАНИЕ РАБОТЫ

В главе 1 диссертации приводится обзор результатов по сложности ветвящихся программ, указывается на связь ветвящихся программ с другими моделями вычислений.

В главе 2 диссертации приводится метод получения нижних оценок сложности детерминированных и недетерминированных $k$-программ, вычисляющих булевы функции. Этот метод позволяет получать сверхполиномиальные нижние оценки

сложности вычисления булевых функций $k$-программами для значений $k$, не превышающих $O(\log n/\log\log n)$.

Идея метода состоит в следующем. Пусть $\mathcal{P}$ — программа, вычисляющая булеву функцию $f$ от $N$ переменных. Если $f(a_1,\ldots,a_N)=1$, то в $\mathcal{P}$ существует хотя бы один путь от входной вершины к выходной вершине, помеченной единицей, в котором каждая дуга, выходящая из вершины, помеченной переменной $x_i$, помечена символом $a_i$. Поставим в соответствие набору $(a_1,\ldots,a_N)$ один из таких путей. На этом пути выбирается некоторое подмножество вершин. Мощности выбранных подмножеств зависят только от заранее выбранных параметров и существенно меньше, чем длина пути. С каждым таким подмножеством вершин ассоциируется функция $f_i$, зависящая только от этого подмножества вершин программы $\mathcal{P}$. При этом $f=\vee f_i$. Если число единиц каждой функции $f_i$ не очень большое, а число единиц функции $f$ велико, то число различных подмножеств вершин, которые ставятся в соответствие единицам булевой функции, велико. Это позволяет оценить снизу мощность множества вершин программы. С помощью этого метода были получены сверхполиномиальные нижние оценки сложности $k$-программ, вычисляющих характеристические функции БЧХ–кодов.

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

$$f(Y)=\bigvee_{j=1}^{A} f_j^1(Y_j^1\cup Y_j^0)\wedge f_j^2(Y_j^2\cup Y_j^0),$$

где $Y_j^1$, $Y_j^2$ и $Y_j^0$ — непересекающиеся множества; $Y=Y_j^1\cup Y_j^2\cup Y_j^0$; $|Y|=n$, $|Y_j^1|\geq m_1$, $|Y_j^2|\geq m_2$, $|Y_j^0|=n-|Y_j^1|-|Y_j^2|$.

Минимальное число дизъюнктивных членов в этом представлении обозначается через $A(f;n,m_1,m_2)$. Это число зависит только от рассматриваемой функции и от выбранных значений параметров $m_1$ и $m_2$. Доказана теорема 2.2,

позволяющая оценить снизу сложность $k$-программ, вычисляющих булевы функции, используя величину $A(f; n, m_1, m_2)$. Частным случаем этой теоремы при конкретных значения $m_1$ и $m_2$ является оценка сложности $k$-программы, вычисляющей булеву функцию $f$, существенно зависящую от $n$ переменных:

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

где $m_1 = \left\lceil n \Big/ \left(2(ke)^k\right)\right\rceil$, $m_2 = \lceil n/(k+1)\rceil$ (следствие 2.1).

Можно предложить несколько способов получения нижней оценки для величины $A(f; n, m_1, m_2)$ [25, 26]. В диссертации используется следующая оценка. Среди всех $i$-мерных граней булева куба размерности $n$ выделяется грань, в которой содержится максимальное число единиц функции $f$. Число единиц в такой грани обозначим через $H_i(f)$. В лемме 2.5 показано, что величина $A(f; n, m_1, m_2)$ удовлетворяет неравенству

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

Это позволяет получать нижние оценки сложности $k$-программ, используя величину $H_i(f)$ (теорема 2.4). Частным случаем этой теоремы при конкретных значениях $m_1$ и $m_2$ является нижняя оценка сложности $k$-программ, вычисляющих булеву функцию $f$, существенно зависящую от $n$ переменных,

$$\mathrm{NBP}k(f) \geq \max\left\{n; \frac{1}{8\sqrt{k}} \cdot \left(\frac{|f^{-1}(1)|}{2^{n-m_1-m_2} H_{m_1}(f) H_{m_2}(f)}\right)^{1/(4k)}\right\},$$

где $m_1 = \left\lceil n \Big/ \left(2(ke)^k\right)\right\rceil$, $m_2 = \lceil n/(k+1)\rceil$ (следствие 2.3).

Используя эти результаты, были получены сверхполиномиальные нижние оценки сложности $k$-программ, вычисляющих характеристические функций БЧХ–кодов $B_{2r+1}$

при некоторых значениях параметров кодов. А именно, было показано (теорема 2.5), что при $k = \lfloor C \ln n / \ln\ln n \rfloor$, где $0 < C < 1$ — константа, существуют БЧХ-коды с параметрами $\left(n, \frac{2^n}{(n+1)^{r_n}}, 2r_n + 1\right)$, где $r_n = n^{(1-C)/2} \cdot \exp\left(\frac{C \ln n}{2 \ln\ln n} \cdot \ln\ln\ln n + O\left(\frac{\ln n}{\ln\ln n}\right)\right)$, которые можно вычислить только $k$-программами, сложность которых не меньше чем $\exp(n^{(1-C)/2})$. В то же время существуют детерминированные программы сложности не более $n^2$, которые вычисляют характеристические функции таких кодов (лемма 2.7).

Прямое применение метода главы 2 не всегда позволяет получать высокие нижние оценки сложности $k$-программ, вычисляющих булевы функции. В главе 3 предложена модификация метода, позволяющая получать сверхполиномиальные нижние оценки сложности $k$-программ, вычисляющих функции от переменных, соответствующих ребрам графов, гиперграфов и иных объектов, имеющих многомерную природу. Вводится булева функция $F_{n,s}$ от $N = \binom{n}{s}$ булевых переменных, соответствующих ребрам гиперграфа, получена высокая нижняя оценка сложности $k$-программ, вычисляющих функцию $F_{n,s}$ (теорема 3.2). А именно, показано, что при $k(n) < C_1 \ln n / \ln\ln n$, где $C_1 < 1/2$ — константа, сложность недетерминированной $k$-программы, вычисляющей функцию $F_{n,s}$, при некоторых значениях параметров не меньше чем $\exp\left(3n^{1-2C_1}\right)$ (следствие 3.3).

С помощью функции $F_{n,s}$ показывается, что для любого натурального $k$, $k \geq 2$, существует последовательность булевых функций такая, что сложность недетерминированных $k$-программ, вычисляющих каждую функцию из этой последовательности, в сверхполиномиальное число раз (по числу переменных булевой функции) превосходит сложность недетерминированных $\lceil k \ln k / \ln 2 + C \rceil$-программ (где $C$ — константа, не зависящая от $k$), вычисляющих ту же функцию (теорема 3.3).

В главе 4 диссертации предложен метод получения

нелинейных нижних оценок сложности для программ без ограничений. Этот метод сводит получение нижних оценок сложности программ без ограничений, вычисляющих булевы функции, к получению нижних оценок сложности программ с ограничениями на число проверок каждой из переменной в любой цепи ($k$-программ), вычисляющих подфункции рассматриваемой функции (теорема 4.1).

Идея этого метода состоит в следующем. Пусть $\mathcal{P}$ — произвольная программа, вычисляющая булеву функцию $f(x_1, x_2, \ldots, x_n)$. Если для какой-то переменной $x_i$ число проверок по этой переменной в некоторой цепи (пути) от входной вершины к выходной превышает $k(n)$, где $k(n) \to \infty$ при $n \to \infty$, и число таких переменных не очень мало, то сложность программы $\mathcal{P}$ не может быть малой. Если число таких переменных мало, то эти переменные можно «забить» константами, что позволит от первоначальной схемы $\mathcal{P}$ перейти к схеме $\mathcal{P}'$ с ограничениями на число проверок каждой переменной в цепи, т. е. рассмотреть вычисление некоторой подфункции функции $f$ ветвящейся $k(n)$-программой. При этом для получения нижних оценок сложности $k$-программ, вычисляющих подфункции булевой функции, можно использовать как подход, предложенный в главах 2, 3 диссертации, так и подход А. Бородина, А. Разборова и Р. Смоленского [12, 20].

Совместное применение теоремы 4.1 и теоремы 2.2 позволяет получать нелинейные нижние оценки сложности ветвящихся программ, вычисляющих булевы функции, исходя из сложности покрытий множества единиц булевой функции функциями определенного вида (теоремы 4.2, 4.3 и 4.4) или исходя из числа единиц булевой функции в гранях определенной размерности (теоремы 4.5, 4.6 и 4.7). В частности, в теореме 4.6 утверждается, что сложность $\mathrm{NBP}(g_n)$ любой недетерминированной программы (без ограничений),

вычисляющей функцию $g_n(X_n)$, удовлетворяет неравенству

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

где $k(n)$ — растущая функция, $C$ — константа, $m_1 = \lceil \lceil (1-C)n \rceil / \left(2(ke)^k\right) \rceil$, $m_2 = \lceil \lceil (1-C)n \rceil / (k+1) \rceil$. Таким образом, для того чтобы использовать эту теорему для получения нетривиальных нижних оценок сложности, нужно иметь как «хорошую» нижнюю оценку числа единиц функции, так и «хорошую» верхнюю оценку числа единиц в подкубах размерности $m_1$ и $m_2$.

Применение теорем 4.5, 4.6 и 4.7 позволило получить нижние оценки сложности недетерминированных программ, вычисляющих характеристические функции кодов Рида–Маллера $\mathcal{R}(u, m)$ для широкого спектра параметров этих кодов (теоремы 4.10, 4.12). Для получения верхней оценки числа единиц кода Рида–Маллера в подкубах размерности $i$ используются результаты по обобщенным весам Хемминга из [23]. Приведена верхняя оценка сложности недетерминированных программ, вычисляющих характеристические функции кодов Рида–Маллера (теорема 4.13). Показано, что для сложности $\mathrm{NBP}(\mathcal{R}(u_m, m))$ вычисления характеристической функции кода $\mathcal{R}(u_{m-C_0}, m)$, где $C_0 \geq 3$ — константа, имеет место оценка

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

где $n$ — число переменных функции $\mathcal{R}(u_{m-C_0}, m)$

Показано, что существуют булевы функции, для которых применение теоремы 4.1 диссертации и подхода из [25, 32] для получения нижних оценок сложности $k$-программ дает лучшие оценки сложности программ без ограничений, вычисляющих эти функции, чем применение теоремы 4.1 и подхода А. Бородина, А А. Разборова, Р. Смоленского [12, 20].

И наоборот, известны примеры булевых функций, для которых имеет место обратное соотношение, а именно применение теоремы 4.1 и подхода А. Бородина, А А. Разборова, Р. Смоленского [12, 20] дает лучшие нижние оценки сложности программ без ограничений, вычисляющих эти функции, чем совместное использование теоремы 4.1 и подхода из [25, 32] (следствие 4.2).

Получены нижние оценки сложности программ, вычисляющих характеристические функции кодов с большим числом вершин (включая коды Боуза–Чоудхури–Хоквингема) (теорема 4.14 и следствие 4.5). При этом полученные нижние оценки $\Omega(n \ln n / \ln \ln n))$ при некоторых значениях параметров кодов оказываются близки к верхним оценкам (следствие 4.4).

В главе 5 рассматриваются понятия геометрической проекции и монотонного расширения булевых функций.

Введем понятие *геометрической проекции*. Проекцию булевой функции $f(x_1, ..., x_n)$ по переменным $x_{i_1}, ..., x_{i_k}$ будем обозначать через $Pf_{x_{i_1},...,x_{i_k}}(x_{j_1}, ..., x_{j_{n-k}})$, где $\{j_1, ..., j_{n-k}\} = \{1, 2, ..., n\} \setminus \{i_1, ..., i_k\}$. Без ограничения общности можно считать, что $i_l = l$ для $l = 1, ..., k$. По определению положим

$$\mathrm{P}f_{x_1,...,x_k}(x_{k+1}, ..., x_n) = \bigvee_{\sigma_1,...,\sigma_k} f(\sigma_1, ..., \sigma_k, x_{k+1}, ..., x_n),$$

где $\sigma_i \in \{0, 1\}$ при $i = 1, ..., k$.

Легко проверить, что для почти всех булевых функций от $n$ переменных сложность проекции меньше сложности функции для основных моделей вычисления. Тем не менее существуют последовательности булевых функций, проекции которых вычисляются существенно сложнее самих функций. В главе 5 строится пример последовательности булевых функций, проекция каждой из которых вычисляется существенно сложнее самой функции в классе формул в конечном базисе, в классе контактных схем, в классе детерминированных и недетерминированных программ, а также детерминированных

и недетерминированных $k$-программ при $k \geq 2$ (теорема 5.1). Достаточно высокие нижние оценки сложности для схем, вычисляющих проекции рассматриваемых функций, получены методом Нечипорука. Вместе с тем сама исходная функция вычисляется достаточно просто. В классе недетерминированных 1-программ сложность вычисления проекции булевой функции не превышает сложности вычисления самой функции (теорема 5.2).

Кроме того, показано, что если для некоторой булевой функции $f$ существует «большой» разрыв (более чем квадратичный относительно сложности $\mathrm{NBP}(f)$) между сложностью детерминированных и недетерминированных программ, вычисляющих эту функцию, то можно построить пример такой функции, что существует «большой» разрыв между сложностью детерминированных программ, вычисляющих эту функцию, и сложностью программ, вычисляющих ее проекцию (теорема 5.3).

Будем говорить, что булева функция $g(x_1, \ldots, x_k)$ является *монотонным расширением* функции $f(x_1, \ldots, x_k)$, если $g(\beta_1, \ldots, \beta_k) = 1$ тогда и только тогда, когда существует такой набор $(\alpha_1, \ldots, \alpha_k)$, что $(\alpha_1, \ldots, \alpha_k) \preceq (\beta_1, \ldots, \beta_k)$ и $f(\alpha_1, \ldots, \alpha_k) = 1$. (Здесь, как обычно, $(\alpha_1, \ldots, \alpha_k) \preceq (\beta_1, \ldots, \beta_k)$ означает, что $\alpha_1 \leq \beta_1, \ldots, \alpha_k \leq \beta_k$.) Таким образом, монотонное расширение булевой функции $f$ — это монотонная булева функция с минимальным числом единиц, среди которых содержатся единицы функции $f$.

Для почти всех булевых функций сложность вычисления монотонного расширения булевой функции не может быть существенно сложнее самой функции для большинства классов схем (схемы из функциональных элементов, контактные схемы, формулы в конечных базисах и др.). Поэтому представляют интерес примеры функций, для которых доказано, что сложность схем того или иного типа, вычисляющих эти функции, существенно меньше сложности схем из того же класса, вычисляющих монотонное расширение

этой функции. В главе 5 строится пример последовательности таких булевых функций, что монотонное расширение каждой функции вычисляется существенно сложнее самой функции в классе формул над конечным базисом, в классе контактных схем, в классе детерминированных и недетерминированных программ, а также детерминированных и недетерминированных $k$-программ при $k \geq 2$ (теорема 5.4). Достаточно высокие нижние оценки сложности для схем, вычисляющих монотонное расширение рассматриваемых функций, получены методом Нечипорука. Вместе с тем сами исходные функции вычисляются достаточно просто.

В теореме 5.6 указывается некоторая связь между операцией геометрического проектирования и операцией монотонного расширения. А именно, предложен алгоритм, позволяющий по произвольной булевой функции $f(X)$ от $n$ переменных построить функцию $g(X,Y)$ от $2n$ переменных такую, что
1) сложность ее вычисления незначительно отличается от сложности вычисления $f(X)$ в основных моделях вычислений;
2) проекция $g(X,Y)$ по переменным из $Y$ совпадает с монотонным расширением функции $f(X)$.

В заключение автор выражает глубокую признательность зав. лабораторией дискретного анализа А. А. Евдокимову, д.ф.-м.н. А. Д. Коршунову и к.ф.-м.н. Ю. Л. Васильеву за ряд ценных советов и замечаний при написании данной диссертации.

## ЛИТЕРАТУРА

[1] **Андреев А. Е.** Об одном методе получения нижних оценок сложности индивидуальных монотонных функций // Докл. АН СССР. — 1985. — Т. 282, № 5. — С. 1033–1037.

[2] **Кузьмин В. А.** Оценка сложности реализации функций алгебры логики простейшими видами бинарных программ

// Методы дискретного анализа в теории кодов и схем. Сб. научн. тр. — Вып. 29. — Новосибирск: Ин-т математики СО АН СССР, 1976. — С. 11–39.

[3] **Колмогоров А. Н.** Три подхода к определению понятия "количество информации"// Проблемы передачи информации. — 1965. — Т. I, вып.1. — С. 3–11.

[4] **Лупанов О. Б.** О вентильных и контактно-вентильных схемах // Докл. АН СССР. — 1956. — Т. 111, № 6. — С. 1171–1174.

[5] **Лупанов О. Б.** О синтезе некоторых классов управляющих систем // Проблемы кибернетики. Вып. 10. — М.: Физматгиз, 1963. — С. 63–97.

[6] **Окольнишникова Е. А.** О сравнении сложностей реализации булевых функций и их проекций // Методы дискретного анализа в теории управляющих систем: Сб. науч. тр. — Вып. 31.— Новосибирск: Ин-т математики СО АН СССР, 1977. — С. 76–80.

[7] **Пулатов А. К.** О влиянии нулевых цепей на сложность реализации булевых функций контактными схемами // Методы дискретного анализа в решении комбинаторных задач. Сб. науч. тр. — Вып. 30. — Новосибирск: Ин-т математики СО АН СССР. — 1977. — С. 30–37.

[8] **Разборов А. А.** Нижние оценки сложности монотонной сложности некоторых булевых функций // Докл. АН СССР. — 1985. — Т. 281, № 4. — С. 798–801.

[9] **Разборов А. А.** Нижние оценки сложности реализации симметрических булевых функций контактно–вентильными схемами // Мат. заметки. — 1990. — Т. 48, вып. 6. — С. 79–90.

[10] **Ajtai M.** A non-linear time lower bound for boolean branching programs // Proc. of the 40th Annual Symposium on Foundations of Computer Science, FOCS '99 (New York, October 17–19, 1999). — Los Alamitos: IEEE Computer Society, 1999. — P. 60–70.

[11] **Babai L., Pudlák P., Rödl V., and Szemerédi M.** Lower bounds to the complexity of symmetric Boolean functions // Theoret. Comput. Sci. — 1990. — V. 74, N 3. — P. 313–324.

[12] **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.

[13] **Dunne P. E.** Lower bounds on the complexity of 1-time only branching programs (preliminary version) // Fundamentals of Computation Theory, FCT'85 (Gorrbus, September 9–13, 1985). — Berlin: Springer-Verl. 1985. — P. 90–99. (Lecture Notes in Comput. Sci. — V. 199.)

[14] **Lee C. Y.** Representation of switching circuits by binary-decision programs. // Bell Syst. Techn. J. — 1959. — V. 38. — P. 985–999. (Имеется перевод: **Ли К.** Представление переключательных схем с помощью программ двоичного решения // Вопросы теории математических машин. — М.: Машиностроение, 1964. — С. 219–232.)

[15] **Mazek W.** A fast algorithm for the syring editing problem and decision graph complexity lower bound on complexity of branching programs // Master's thesis. Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology. — Massachusetts, 1976.

[16] **Pudlák P.** The hierarchy of Boolean circuits // Computers and Artificial Intelligence. — 1987. — V. 6, N 5. — P. 449–468.

[17] **Razborov A. A.** Lower bounds for deterministic and nondeterministic branching programs // Fundamentals of Computation Theory, 8th International symposium, FCT'91 (Gosen, September 9–13, 1991). — Berlin: Springer-Verlag, 1991. — P. 47–60. (Lecture Notes in Comput. Sci. — V. 529.)

[18] **Riordan J., Shannon C. E.** The number on two-terminal series parallel nerworks // J. Math. Phys. — 1942. — V. 21, N 2. — P. 83–93. (Русский перевод: **Шеннон К.Э.** Работы по теории информации и кибернетике. — М.: ИЛ, 1963. — С. 46–58.)

[19] **Shannon C. E.** The synthesis of two-terminal switching circuits // Bell Syst. Techn. J. — V. 28, N 1. — 1949. — P. 59–98. (Русский перевод: **Шеннон. К.Э.** Работы по теории информации и кибернетике. — М.: ИЛ, 1963. — С. 59–101.)

[20] **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.

[21] **Wegener I.** On the complexity of branching programs and decision trees for clique functions // Journal of the ACM. — 1988. — V. 35, N 2. — P. 461–471.

[22] **Wegener I.** Branching programs and binary decision diagrams. Theory and applications. — Philadelphia, PA: SIAM, 2000. — 408 pp.

[23] **Wei V. K.** Generalized Hamming weights for linear codes // IEEE Trans. on Inform. Theory. — 1991. — V. 37, N 5. — P. 1412–1418.

[24] **Žak S.** An exponential lower bound for one-time-only branching programs // Proc. of the 11th Int. Symp. on

Mathematical Foundations of Computer Science, MFCS'84 (Praha, September 3–7, 1984). — Berlin: Springer–Verlag, 1984. — P. 562–566. ( Lecture Notes in Comput. Sci. — V. 176.)

СТАТЬИ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

[25] **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.

[26] **Okol'nishnikova E. A.** Lower bounds on branching programs // Siberian Adv. Math. — 1993. — V. 3, N 1. — P. 152–166.

[27] **Окольнишникова Е. А.** О сравнении сложностей бинарных $k$-программ // Дискрет. анализ и исслед. операций. — 1995. — Т. 2, № 4. — С. 54-73. (Перевод статьи: **Okol'nishnikova E. A.** On Comparison between the sizes of read-$k$-times branching programs // Operation Research and Discrete Analysis (ed. A.D.Korshunov) (Series: Mathematics and Its Applications). — Dordrecht: Kluwer Academic Publishers, 1997. — P. 205–225.)

[28] **Okol'nishnikova E. A.** On the hierarchy of nondeterministic branching $k$-programs // Fundamentals of computation theory. 11th International symposium, FCT 97 (Krakóv, September 1–3, 1997). — Berlin: Springer, 1997. — P. 376–387. (Lecture Notes in Comput. Sci. — V. 1279.)

[29] **Окольнишникова Е. А.** О сравнении сложностей недетерминированных ветвящихся $k$-программ // Дискрет. анализ и исслед. операций. Серия 1. — 1999. — Т. 6, № 1. — С. 65–85. (Перевод статьи: **Okol'nishnikova E. A.**

Comparing the sizes of nondeterministic branching read-$k$-times programs // Discrete Applied Mathematics. — 2004. — V. 135. — P. 205–222.)

[30] **Окольнишникова Е. А.** О двух операциях над булевыми функциями // Дискрет. анализ и исслед. операций. Сер. 1. — 2000. — Т. 7, № 1. — С. 79–93.

[31] **Окольнишникова Е. А.** О сложности ветвящихся программ // Дискретная математика и ее приложения. Сб. лекций молодежных научных школ по дискретной математике и ее приложениям, II. — М.: Изд-во центра приклад. исслед. при мех.-мат. фак-те МГУ, 2001. — С. 41–58.

[32] **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.

[33] **Окольнишникова Е. А.** Сложность ветвящихся программ // Математические вопросы кибернетики. Вып. 10. — М.: Физматлит, 2001. — С. 69–82.

[34] **Окольнишникова Е. А.** О сложности недетерминированных ветвящихся программ, реализующих характеристические функции кодов Рида–Маллера // Дискрет. анализ и исслед. операций. Сер. 1. — 2003. Т. 10, № 3. С. 67–81.

[35] **Okol'nishnikova E. A.** On some bounds on the size of branching programs (a survey) // Stochastic Algorithms, Foundations and Application. 3rd International symposium, SAGA 2005 (Moscow, October 20–22, 2005). — Berlin: Springer, 2005. — P. 107–115. (Lecture Notes in Comput. Sci. — V. 3777. )

[36] **Окольнишникова Е. А.** Нижние оценки сложности ветвящихся программ // Вестник Томского гос. университета. Приложение. — 2006. — № 17. — С. 42–46.

## РАБОТЫ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ, ОПУБЛИКОВАННЫЕ В МАТЕРИАЛАХ СЕМИНАРОВ И ТЕЗИСАХ КОНФЕРЕНЦИЙ

[37] **Окольнишникова Е. А.** Об одном соотношении сложностей булевых функций // Проблемы теоретической кибернетики. VIII Всесоюз. науч. конф. (Горький, июль 1988 г.). Тез. докл. — Горький: Горьковский гос. пед. институт, 1988. — С. 63.

[38] **Окольнишникова Е. А.** Нижние оценки сложности реализации булевых функций бинарными программами // Логика и семантическое программирование (Вычислительные системы). Сб. научн. тр. — Вып. 146. — Новосибирск: Ин-т математики СО АН СССР, 1992. — С. 177–180.

[39] **Окольнишникова Е. А.** О нижних оценках сложности для бинарных программ // Сб. трудов IV Межгос. семинара по дискретной математике и ее приложениям (Москва, 2–4 февраля 1993 г.). — М.: Изд-во мех.–мат. фак-та МГУ, 1993. — С. 79.

[40] **Окольнишникова Е. А.** Об одном соотношении сложностей бинарных $k$-программ // Дискрет. анализ и исслед. операций (Тез. докл. VI Межгос. школа-семинар "Синтез и сложность управляющих систем". Нижний Новгород, 21–24 ноября 1994 г.). — 1995. — Т. 2, № 1. — С. 77–78.

[41] **Окольнишникова Е. А.** Об одном соотношении сложностей бинарных $k$-программ // Проблемы теоретической кибернетики. XI Междунар. конф. (Ульяновск, 10–14 июня 1996 г.). Тез. докл. — Москва: Изд. центр РГГУ, 1996. — С. 153–154.

[42] **Окольнишникова Е. А.** Об иерархии бинарных $k$-программ // II Сибирский Конгресс по Прикладной и Индустриальной Математике, ИНПРИМ-96. (Новосибирск, 27–31 мая 1996). Тез. докл. — Новосибирск: Изд-во Института математики СО РАН, 1996. — С. 122.

[43] **Окольнишникова Е. А.** О сложности ветвящихся программ // Материалы IX Межгосударственной школы-семинара "Синтез и сложность управляющих систем"(Нижний Новгород, 16–19 декабря 1998). — М.: Изд-во мех-мат. фак-та МГУ, 1999. — С. 63–70.

[44] **Окольнишникова Е. А.** О сложности реализации проекций булевых функций ветвящимися программами // Проблемы теоретической кибернетики. XII Междунар. конф. (Нижний Новгород, 17–22 мая 1999). Тез. докл. — М.: Изд-во Изд-во мех-мат. фак-та МГУ, 1999. — Часть 2. — С. 178.

[45] **Окольнишникова Е. А.** О двух операциях над булевыми функциями // Материалы XI Международной школы-семинара "Синтез и сложность управляющих систем"(Нижний Новгород, 20–25 ноября 2000 г.). — М.: Изд-во центра прикл. исслед. при мех.-мат. фак-те МГУ, 2001. — Часть II. — С. 126–134.

[46] **Окольнишникова Е. А.** Нижние оценки сложности ветвящихся программ // Материалы XII Межгосударственной школы-семинара "Синтез и сложность управляющих систем"(Пенза, 19-21 октября 2001 г.). — М.: Изд-во центра приклад. исслед. при мех.-мат. фак-те МГУ, 2001. — Часть II. — С. 160–164.

[47] **Окольнишникова Е. А.** Оценки сложности вычисления булевых функций ветвящимися программами // Российская конф. "Дискретный анализ и исследование

операций"(Новосибирск, 24–28 июня 2002 г.). Материалы конференции. — Новосибирск: Изд-во Ин-та математики, 2002. — С. 88–93.

[48] **Окольнишникова Е. А.** О сравнении двух методов получения нижних оценок сложности ветвящихся $k$-программ // Проблемы теоретической кибернетики. Тезисы докладов XIII Международной конф. (Казань, 27–31 мая 2002 г.). — М.: Изд-во центра прикл. исслед. при мех.-мат. фак-те МГУ, 2002. — Часть II. — С. 135.

[49] **Окольнишникова Е. А.** О сложности характеристических функций кодов Рида–Маллера // Материалы XIV Международной школы–семинара "Синтез и сложность управляющих систем"(Нижний Новгород, 27 октября – 1 ноября 2003 г.). — Нижний Новгород: Изд-во Нижегородского гос. пед. университета, 2003. — С. 60–64.

[50] **Окольнишникова Е. А.** О сложности ветвящихся программ // Материалы VIII Международного семинара "Дискретная математика и ее приложения"(Москва, 2–6 февраля 2004 г.). — М.: Изд-во мех.-мат. фак-та МГУ, 2004. — С. 85–86.

[51] **Окольнишникова Е. А.** О некоторых комбинаторных задачах, возникающих в теории сложности // Материалы XV Международной школы–семинара "Синтез и сложность управляющих систем"(Новосибирск, 18 – 23 октября 2004 г.). — Новосибирск: Изд-во ИМ СО РАН, 2004. — С. 57–61.

[52] **Okol'nishnikova E. A.** On some operations over Boolean functions // Proc. of the seminar "The complexity of Boolean functions"(Dagstuhl, 31 октября – 5 ноября 1999 г.) — Germany, Dagstuhl, 1999. — P. 10.