САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

На правах рукописи

Деменков Евгений Александрович

# ВЕРХНИЕ И НИЖНИЕ ОЦЕНКИ НА СХЕМНУЮ СЛОЖНОСТЬ ЯВНО ЗАДАННЫХ БУЛЕВЫХ ФУНКЦИЙ

01.01.06 — Математическая логика, алгебра и теория чисел

А В Т О Р Е Ф Е Р А Т

диссертации на соискание учёной степени
кандидата физико-математических наук

Санкт-Петербург — 2013

Работа выполнена на кафедре математических и информационных технологий Санкт-Петербургского академического университета — Научно-образовательного центра нанотехнологий РАН

Научный руководитель: кандидат физико-математических наук, доцент
Куликов Александр Сергеевич

Официальные оппоненты: доктор физико-математических наук, проф., зав.кафедрой, вед.н.с. отдела алгебры и математической логики
НИИММ им. Н.Г.Чеботарева КГУ
Аблаев Фарид Мансурович
(Казанский федеральный университет)
кандидат физико-математических наук, научный сотрудник
Подольский Владимир Владимирович
(Математический институт им. В.А. Стеклова Российской академии наук)

Ведущая организация: Уральский федеральный университет имени первого Президента России Б.Н. Ельцина

Защита состоится “04” декабря 2013 г. в 16 часов на заседании диссертационного совета Д212.232.29 при Санкт-Петербургском государственном университете по адресу: 198504, Санкт-Петербург, В.О. 10 линия 33-35, ауд. 74.

С диссертацией можно ознакомиться в Научной библиотеке им. М. Горького Санкт-Петербургского государственного университета по адресу: 199034, Санкт-Петербург, Университетская наб., д. 7/9.

Автореферат разослан “ ” 2013 г.

Ученый секретарь диссертационного совета Нежинский В. М.

## Общая характеристика работы

**Актуальность темы.**

Теория сложности вычислений изучает зависимость потраченных ресурсов на вычисление некой функции от размера входных данных. В разных моделях вычислений рассматриваются разные виды ресурсов. К примеру, при изучении алгоритмов в качестве модели принято рассматривать машину Тьюринга, а в качестве ресурсов рассматривают обычно время или память, необходимые для вычисления функции. В коммуникационной сложности в качестве ресурса, как правило, выступает суммарный размер переданных сообщений.

Теория сложности интересна как с практической, так и с теоретической точек зрения. Практическая часть включает в себя построение явных конструкций (алгоритмов, протоколов, методов). Теоретическая часть изучает вопрос размера этих конструкций и включает в себя, в частности, доказательство нижних оценок на сложность конструкций.

Одним из крупных разделов теории сложности вычислений является схемная сложность. В качестве модели вычисления используется булева схема, представляющая из себя ориентированный ациклический граф, вершины которого помечены функциями из некоторого базиса $\Omega$. Роль ресурса играют вершины. Схемы представляют из себя неоднородную модель вычислений. Для входов различного размера допускаются разные схемы. В данной модели размеры минимальных схем для полных конечных базисов отличаются не более чем в константу раз. И эта константа зависит только от самих базисов.

Доказательство верхних и нижних оценок на схемную сложность явно заданных булевых функций — один из основных и самых сложных вопросов современной теоретической информатики. Изучение булевых схем можно найти в работах Шеннона. Они активно изучались советскими математиками с 1950-х годах. Обозначим через $C(n)$ функцию Шеннона для схем — максимальный размер минимальной схемы, вычисляющей функцию от $n$

переменных. Поскольку любую булеву функцию можно вычислить с помощью конъюнктивной нормальный формулы, то $C(n)$ можно оценить сверху через $O(n2^n)$. Шеннон в 1949 году показал, что для любого $\epsilon$ и достаточно большого $n$ верно неравенство $C(n) > (1-\epsilon)2^n/n$. В 1956 году Миллер доказал для любого конечного базиса верхнюю оценку $C(n) = \Theta(2^n/n)$. В 1959 году Лупанов показал, что $C(n) < (1+\alpha_n)2^n/n$, где $\alpha_n = O(\log n/n)$. Таким образом, мы знаем, что большинство функций от $n$ переменных имеют схемную сложность $\Omega(2^n/n)$.

Тем не менее, задача построения явно заданной булевой функции высокой схемной сложности оказалась очень трудной. Булеву функцию принято называть явно заданной, если прообраз единицы этой функции лежит в классе NP. Более формально, в данной работе под булевой функцией $f$ мы понимаем бесконечное семейство функций $\{f_i \colon i \in \mathbb{N}\}$, где $f_i \colon \{0,1\}^i \to \{0,1\}$. Такая функция называется явно заданной, если $\cup_{i\in\mathbb{N}} f_i^{-1}(1) \in \mathrm{NP}$.

Только в 1965 году Клосс и Малышев доказали первую нетривиальную нижнюю оценку $2n - O(1)$. Рекордная же нижняя оценка в полном базисе $3n - o(n)$ доказана Блюмом в 1984. Она довольно нетривиальна и требует разбора большого количества случаев.

Помимо полного бинарного базиса часто рассматриваю базис из бинарных функций, которые можно вычислить с помощью одной дизъюнкции и нескольких отрицаний. Первый нетривиальный результат в этом базисе $3(n-1)$ получен Шнором в 1974 году. Он доказал, что функция чётности имеет сложность $3(n-1)$. Рекордный же результат $5n - o(n)$ получили 2002 году Ивама и Морицуми. В 2012 году Куликов, Меланич и Михайлин получили значительно более простое доказательство такой же оценки для одновременного вычисления нескольких линейных функций.

**Цели работы.**

1. Усилить верхнюю оценку $5n + o(n)$ Лупанова на схемную сложность (над базисом $B_2$) всех симметрических функций.

2. Получить нетривиальные верхние оценки на схемную сложность од-

новременного вычисления всех MOD-функций.

3. Упростить доказательство нижней оценки $3n-o(n)$ на схемную сложность явно заданной функции(аффинного дисперсера).

4. Усилить нижнюю оценку на схемную сложность функции с $n$ выходами.

**Общая методика работы.** В работе используются как стандартные методы доказательства новых оценок, так и новые идеи и подходы. Так, для улучшения верхних оценок используется стандартный метод предкодирования. Для симметрических функций используется нестандартная кодировка суммы входных битов для построения более эффективного двойного сумматора. Для вычисления всех MOD-функций одновременно используется метод предподсчётаст остатков по простым модулям.

Для доказательства нижней оценки используется стандартный метод элиминации элементов, однако в нём впервые используются произвольные линейные подстановки. Для доказательства нижней оценки для функции с $n$ выходами усиливается метод Ламаньи и Сэведжа.

**Основные результаты.**

1. Получена верхняя оценка $4.5n+o(n)$ на схемную сложность всех симметрических функций (в базисе $B_2$).

2. Построена схема почти линейного размера, одновременно вычисляющая все MOD-функций.

3. Получена новая рекордная нижняя оценка $7n-o(n)$ на схемную сложность в базисе $U_2$ функции из $B_{n,n}$.

4. Получено более простое доказательство рекордной нижней оценки $3n - o(n)$ на схемную сложность явной заданной булевой функции в базисе $B_2$.

**Научная новизна.** Все полученные оценки являются новыми, ранее не известными и самыми сильными из известных на сегодняшний день.

Оценка $3n - o(n)$, доказанная в диссертация, также была получена в 1984 году Блюмом, но для другой функции. Приводящееся в диссертации доказательство значительно проще и, в частности, почти не содержит разбора случаев.

**Практическая и теоретическая ценность.** Разработанные идеи и методы доказательства нижних оценок могут быть использованы при дальнейшем изучении сложности булевых функций и имеют, скорее, теоретическую ценность. Построенные в работе схемы могут быть использованы при проектировании микросхем.

**Апробация работы.** Основные результаты обсуждались на следующих конференциях: международный симпозиум 36th International Symposium On Mathematical Foundations Of Computer Science (MFCS 2011), Польша, 2011; международный симпозиум 7th International Computer Science Symposium in Russia (CSR 2012), Россия, 2012. Результаты, лежащие в основе диссертации, также были доложены на семинаре в Московском государственном университете. Публикация в трудах конференции 7th International Computer Science Symposium in Russia получила приз как лучшая студенческая работа.

**Публикации.** Основные результаты диссертации опубликованы в четырёх работах [1], [2], [3], [4].

Работа [1] написана самостоятельно диссертантом. В работе [4] диссертантом доказана верхняя оценка 4.5n на схемную сложность вычисления суммы входных битов, изложенная в разделе 2. В работе [3] диссертанту принадлежит доказательство ключевой леммы 6, из которой выводится основной результат статьи. Теорема 1 доказана А. Куликовым и Х. Морицуми, теорема 2 доказана авторами работы совместно. В работе [2] диссертанту принадлежит идея использования переменных исходящей степени 1, с помощью которой доказывается теорема 1, содержащая основной результат статьи. А. Куликову принадлежит идея использования аффинного дисперсера и доказательство леммы 1. Работы [2], [3], [1] опубликованы в изданиях, входящих в список рекомендованных Высшей аттестационной

комиссией на момент публикации.

**Структура и объем диссертации.** Диссертация объёмом 60 страниц состоит из введения и трёх основных глав, разбитых на разделы и подразделы. Список цитируемой литературы состоит из 46 наименований.

## Содержание работы

**Основные определения.** Перед изложением содержания работы приведём необходимые определения.

Через $B_{n,m}$ обозначим множество всех булевых функций $f\colon \{0,1\}^n \to \{0,1\}^m$. $B_{n,1}$ обозначается через $B_n$. Функция $f \in B_n$ называется *симметрической*, если её значение зависит только от суммы входных битов. Другими словами, должен существовать вектор $v \in \{0,1\}^{n+1}$ (называемый *вектором значений* $f$) такой, что $f(x_1,\ldots,x_n) = v_s$, где $s = \sum_{1\le i\le n} x_i$. Фундаментальные симметрические функции EX, TH и MOD определяются следующим образом:

$$\begin{aligned}
\mathrm{EX}^n_k(x_1,\ldots,x_n) &= 1 \Leftrightarrow \sum_{1\le i\le n} x_i = k\,,\\
\mathrm{TH}^n_k(x_1,\ldots,x_n) &= 1 \Leftrightarrow \sum_{1\le i\le n} x_i \ge k\,,\\
\mathrm{MOD}^n_{m,r}(x_1,\ldots,x_n) &= 1 \Leftrightarrow \sum_{1\le i\le n} x_i \equiv r \pmod m\,.
\end{aligned}$$

Схемой называется ациклический ориентированный граф, все вершины которого имеют входящую степень 0 или 2. Вершины входящей степени 0 помечены переменными из множества $\{x_1,\ldots,x_n\}$ и называются входами. Вершины входящей степени 2 помечены функциями из $B_2$ и называются элементами. Также есть $m$ специально выделенных выходных элементов. Таким образом, схема вычисляет функцию из $B_{n,m}$. Пример схемы приведён на рисунке 1 . Размер схемы — это количество элементов в ней. Через $C(f)$ мы обозначаем минимальный размер схемы, вычисляющей $f$.

Всего существуют 16 различных бинарных функций:

- 2 константных функции — значение которых не зависят от входных значений.

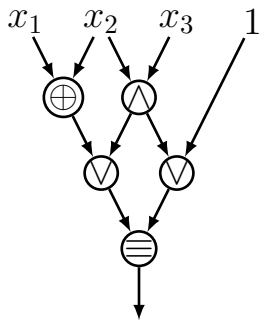


Рис. 1: Пример схемы.

- 4 вырожденных функции — значение которых определяется значением только одной из переменных.
- 2 функции типа $\oplus$ — они вычисляют функции вида $x \oplus y \oplus a$, где $a \in \{0, 1\}$.
- 8 функции типа $\wedge$ — они вычисляют функции вида $(x \oplus a) \wedge (y \oplus b) \oplus c$, где $a, b, c \in \{0, 1\}$.

Два наиболее часто рассматриваемых базиса — это полный бинарный базис $B_2$ и базис $U_2 = B_2 \setminus \{\oplus, \equiv\}$.

**Описание глав.** Во **введении** обсуждаются рассматриваемые в диссертации задачи, состояние исследований в этой области, формулируются основные результаты, описывается структура диссертации.

В **первой главе** определяются основные понятия и вводятся обозначения, используемые на протяжении всей диссертации.

**Вторая глава** диссертация посвящена новым верхним оценкам. В ней доказывается верхняя оценка $4.5n + o(n)$ на схемную сложность всех симметрических функций (в базисе $B_2$). Данная оценка улучшает классическую оценку $5n + o(n)$, доказанную Лупановым в 1965 году.

Следующим результатом второй главы является почти линейная верхняя оценка на схемную сложность одновременного вычисления всех MOD-функций. Несложно показать, что для почти всех наборов из $n$ симметрических функций схемная сложность почти квадратична — $\Theta(n^2/\log n)$. Ни одного такого явного набора, однако, неизвестно. В то

же время известно, что для одновременного вычисления всех функций EX и TH достаточно схем линейного размера. Мы усиливаем данный результат, доказывая, что и все MOD-функции можно вычислить схемами почти линейного, а для некоторых случаев линейного размера.

В **третьей главе** доказываются новые нижние оценки. Первым результатом является рекордная известная оценка $3n-o(n)$ на схемную сложность явной заданной булевой функции в базисе $B_2$. Данная оценка повторяет оценку, доказанную Блюмом в 1984 году, но доказывается значительно проще. В частности, доказательство почти не содержит разбора случаев. В то же время для доказательства понадобилась более сложная булева функция — так называемый аффинный дисперсер, явная конструкция которого была представлена только в 2009 года Бен-Сассоном и Коппарти. Отдельный интерес представляет то, что в данном доказательстве, в отличие от предыдущих доказательств, основанных на методе элиминации элементов, используются подстановки линейных функций.

Заключительным результатом диссертации является нижняя оценка $7n-o(n)$ на схемную сложность в базисе $U_2$ функции из $B_{n,n}$. Это улучшает предыдущую известную оценку $6n-o(n)$, получающуюся применением метода Ламаньи и Сэвэджа к оценке $5n-o(n)$, доказанной Ивамой и Морицуми. В отличие от метода элиминации элементов, использующемся в доказательстве предыдущей оценки, здесь анализируется часть схемы у выходов, а не входов.

## Публикации автора по теме диссертации

[1] Demenkov Evgeny. A Lower Bound on Circuit Complexity of Vector Function in $U_2$ // 7th International Computer Science Symposium in Russia (CSR 2012) / под ред. Edward Hirsch, Juhani Karhumaki, Arto Lepisto [и др.]. Т. 7353 из *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2012. С. 81–88.

[2] Demenkov Evgeny, Kulikov Alexander S. An elementary proof of a 3n- o (n) lower bound on the circuit complexity of affine dispersers // Mathematical Foundations of Computer Science 2011. Springer, 2011. С. 256–265.

[3] Computing All MOD-Functions Simultaneously / Evgeny Demenkov, Alexander S. Kulikov, Ivan Mihajlin [и др.] // Computer Science–Theory and Applications. Springer, 2012. С. 81–88.

[4] New upper bounds on the Boolean circuit complexity of symmetric functions / Evgeny Demenkov, Arist. Kojevnikov, Alexander S. Kulikov [и др.] // Information Processing Letters. 2010. Т. 110, № 7. С. 264–267.