



МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
имени М.В. Ломоносова  
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи

*Калачев*

Калачев Глеб Вячеславович

**О МОЩНОСТНОЙ СЛОЖНОСТИ  
ПЛОСКИХ СХЕМ**

Специальность 01.01.09 — дискретная математика и  
математическая кибернетика

АВТОРЕФЕРАТ  
диссертации на соискание учёной степени  
кандидата физико-математических наук

10.04.2013



**008713932**

Москва — 2017

Работа выполнена на кафедре математической теории интеллектуальных систем  
механико-математического факультета МГУ имени М.В. Ломоносова

**Научный руководитель:** Гасанов Эльяр Эльдарович,  
доктор физико-математических наук, профессор

**Официальные оппоненты:** Ложкин Сергей Андреевич,  
доктор физико-математических наук, профессор кафедры математической кибернетики факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова.

Чашкин Александр Викторович,  
доктор физико-математических наук, профессор кафедры дискретной математики механико-математического факультета МГУ имени М.В. Ломоносова.

Алексиадис Никос Филиппович,  
Кандидат физико-математических наук, доцент кафедры математического моделирования ФГБОУ ВО «Национальный исследовательский университет «МЭИ»

Заплита диссертации состоится «9» февраля 2018 г. в 11 часов 30 минут на заседании диссертационного совета МГУ.01.16 Московского государственного университета имени М.В. Ломоносова по адресу: 119991, Москва, Ленинские горы, вл.1, Главное здание, механико-математический факультет, ауд. 14-08.

E-mail: ilgova@cs.msu.su

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ (Ломоносовских проспект, д. 27), а также на сайте ИАС «ИСТИНА»: <http://istina.msu.ru/dissertations/87055540>

Автореферат разослан 20 декабря 2017 г.

Учёный секретарь  
диссертационного совета,  
доктор физико-математических наук,  
профессор

Гасанов Эльяр Эльдарович

## Общая характеристика работы

Одним из разделов математической кибернетики является теория управляющих систем. Основы этой теории были заложены в середине XX века в связи с практическими нуждами разработки логических схем для электронно-вычислительных устройств. При проектировании электронного устройства паряду с разработкой логики схемы нетривиальной задачей также является размещение логических элементов на плоскости при наличии физических и технологических ограничений.

Помимо размеров, важными физическими характеристиками реальных электронных схем являются энергопотребление (тепловыделение) и скорость выполнения операций. С одной стороны, имеются инженерные методы и программное обеспечение, позволяющие проектировать логику схемы и хорошую с практической точки зрения укладку элементов. С другой стороны, с помощью математических методов можно исследовать принципиальные ограничения снизу на электрическую мощность вычислительных устройств. Известны строгие математические модели, учитывающие как логику устройства, так и размещение элементов. В таких моделях вводятся меры сложности, отражающие указанные физические характеристики устройства.

В абстрактной постановке в рамках некоторой строгой модели задачу проектирования вычислительного устройства можно свести к задаче построения схемы, вычисляющей заданную булеву функцию (много входов и один выход) или булев оператор (много входов и много выходов). В рамках введённой модели требуется оптимизировать некоторые меры сложности схемы. Укажем основные направления исследований в этой области. Одним из направлений является построение оптимальных схем, реализующих конкретные операторы, такие как сумматоры, умножители, арифметические операции в конечных полях и т.п. Другим направлением является получение нижних оценок на сложность схем, реализующих конкретные функции или операторы, чаще всего — при некоторых дополнительных ограничениях на схемы. Третьим направлением является разработка универсальных и оптимальных в некотором смысле методов синтеза схем для заданного класса булевых функций или операторов. Фундаментальные асимптотические нижние оценки сложности схем, получаемые при доказательстве оптимальности таких методов, представляют всё больший интерес с ростом сложности вычислительных устройств. Результаты, полученные в настоящей работе, относятся к последнему упомянутому направлению.

## Актуальность темы и степень ее разработанности

Исторически первой моделью устройств, вычисляющих булевые функции, была модель контактных схем (далее — КС), введённых К. Шенноном<sup>1</sup> в 1938 году еще до появления электронно-вычислительных устройств (определения терминов, используемых во введении, можно найти, например, в учебнике А. В. Чапкина<sup>2</sup> и обзоре А. Д. Коршунова<sup>3</sup>).

В 1950-х годах популярность приобрела модель схем из функциональных элементов (далее — СФЭ). Д. Мюллер в работе<sup>4</sup> 1956 года определил сложность СФЭ, как количество её элементов, и показал, что сложность функций от  $n$  переменных имеет порядок  $2^n/n$  в худ-

<sup>1</sup> C. E. Shannon. "A symbolic analysis of relay and switching circuits". в: *Transactions of the American Institute of Electrical Engineers* 57.12 (1938), с. 713–723

<sup>2</sup> А. В. Чапкин. *Дискретная математика*. Академия Москва, 2012, с. 352

<sup>3</sup> А. Д. Коршунов. "Сложность вычислений булевых функций". в: *Успехи математических наук* 67.1 (2012), с. 97–108

<sup>4</sup> D. E. Muller. "Complexity in Electronic Switching Circuits". в: *IRE Transactions on Electronic Computers* EC-5.1 (1956), с. 15–19

шем случае. Под сложностью булевой функции понимается минимальная сложность среди СФЭ, реализующих эту функцию. Позднее О. Б. Лупанов доказал<sup>5</sup>, что в стандартном базисе  $\{\{V, \&, \neg\}\}$  сложность почти всех булевых функций асимптотически равна  $2^n/n$ . Более того, он исследовал взвешенную сложность СФЭ и нашёл её асимптотику для почти всех функций в произвольном конечном базисе с заданными положительными весами всех элементов базиса. Л. А. Шоломов предложил<sup>6</sup> асимптотически оптимальный метод синтеза СФЭ для класса частичных операторов, разбивающих область определения на части заданного размера, однако в теореме накладываются существенные ограничения на размеры этих частей и область определения. В одной из последующих работ<sup>7</sup> Шоломов нашёл асимптотику функции Шенюона сложности СФЭ, реализующих частичные булевые функции в произвольном конечном базисе. В частности, при некоторых ограничениях Шоломов доказал, что для почти всех частичных булевых функций сложность в стандартном базисе асимптотически равна  $d/\log_2 d$ , где  $d$  — число наборов, на которых значение функции определено. А. Е. Андреев усилил<sup>8</sup> результат Шоломова, найдя асимптотику функции Шенюона уже без ограничений на размер области определения.

А. Е. Андреев и И. А. Вихлянцев рассмотрели<sup>9</sup> другую меру сложности СФЭ, а именно, длину кода схемы, которая кроме числа элементов отражает и топологию их соединения. Каждой СФЭ ставится в соответствие двоичный код программы, которая позволяет последовательно вычислить функцию в соответствии с данной СФЭ. Фактически, кодирование СФЭ можно рассматривать, как топологическую сортировку её графа с последующей укладкой его вершин на целочисленные точки прямой так, чтобы все ребра были направлены вправо. При такой интерпретации длина кода СФЭ в основном определяется суммой логарифмов длины рёбер графа при заданной укладке. В этой же работе был предложен метод, позволяющий по произвольной СФЭ строить асимптотически оптимальный код, а также показано, что функция Шенюона длины кода СФЭ для функций от  $n$  переменных асимптотически равна  $2^n$ . Кроме того, было доказано, что для сумматора двух двоичных чисел длина кода СФЭ растёт линейно с увеличением числа переменных, а для умножителя — нелинейно.

М. И. Вайнцвайг ввёл<sup>10</sup> ещё одну меру сложности — мощность СФЭ. Согласно определению Вайнцвайга, мощность (активность) СФЭ равна максимальному количеству элементов схемы, выдающих на выходе единицу, где максимум берётся по всем возможным входным наборам. Мощность СФЭ отражает электрическую мощность устройства, вычисляющего булеву функцию. При таком определении мощности СФЭ предполагается, что функциональный элемент потребляет энергию только тогда, когда значение на его выходе равно 1. Вайнцвайг рассматривал мощность СФЭ в различных базисах и показал, что её порядок может быть как линейным (например, в базисе  $\{V, \&, \neg\}$ ), так и экспоненциальным (например, в базисе  $\{\bar{x} \vee \bar{y}\}$ ). Более детально зависимость мощности СФЭ от базиса исследовал О. М. Касим-Заде. Он предложил<sup>11</sup> метод синтеза СФЭ в базисе  $\{V, \&, \neg\}$ , позволяющий строить схемы

<sup>5</sup>О. Б. Лупанов. "Об одном подходе к синтезу управляющих систем — принципе локального кодирования". в: *Проблемы кибернетики. Вып 14*. Наука, М., 1965, с. 31 - 110

<sup>6</sup>Л. А. Шоломов. "О функционалах сложности систем недоопределённых функций". в: *Проблемы кибернетики. Вып 19*. Наука, М., 1967, с. 123 - 139

<sup>7</sup>Л. А. Шоломов. "О реализации недоопределённых булевых функций схемами из функциональных элементов", в: *Проблемы кибернетики. Вып 21*. Наука, М., 1969, с. 215 - 226

<sup>8</sup>А. Е. Андреев. "О сложности реализации частичных булевых функций схемами из функциональных элементов". в: *Дискретная математика 1.4* (1989), с. 36 - 45

<sup>9</sup>А. Е. Андреев и И. А. Вихлянцев. "Оценки длины кода для схем из функциональных элементов". в: *Дискретная математика 6.4* (1994), с. 10 - 20

<sup>10</sup>М. И. Вайнцвайг. "О мощности схем из функциональных элементов", в: *Докл. АН СССР 139.2* (1961), с. 320 - 323

<sup>11</sup>О. М. Касим-Заде. "Об одновременной минимизации сложности и мощности схем из функциональных

с линейной мощностью и асимптотически оптимальные по сложности. В другой работе<sup>12</sup> Касим-Заде установил порядок функции Шеннона мощности СФЭ для произвольного полного конечного базиса, а также привёл пример базиса, в котором для почти всех функций не существует схем с асимптотически оптимальной сложностью и оптимальной по порядку мощностью.

Касим-Заде также была введена<sup>13</sup> ещё одна мера мощности СФЭ —  $P$ -активность, которая рассчитывается следующим образом. Элемент схемы называется активным на заданном входном наборе, если при подаче этого набора на вход схемы либо один из входов этого элемента, либо его выход равен 1.  $P$ -активность схемы равна максимальному количеству активных элементов, при этом максимум берётся по всевозможным входным наборам. Фактически,  $P$ -активность, в отличие от обычной активности, учитывает степень ветвления на выходах элементов СФЭ. Как и для обычной активности, для  $P$ -активности Касим-Заде исследовалась зависимость от базиса и, в частности, показал, что в базисе  $\{\vee, \&, \neg\}$  любую функцию от  $n$  переменных можно реализовать при помощи СФЭ с  $P$ -активностью  $O(n^2)$ .

С. А. Ложкин и М. С. Шуплецов ввели<sup>14</sup> понятие динамической активности СФЭ, определив её, как максимальное количество выходов элементов, изменяющих своё значение при изменении входных наборов схемы. Введение данной меры сложности обусловлено тем, что большая часть энергии микросхемы выделяется именно при изменении значений на её входах и, соответственно, в узлах схемы. В той же работе было показано, что в любом полном базисе можно реализовать булеву функцию от  $n$  переменных с линейной динамической активностью. Также был предложен метод синтеза СФЭ в базисе  $\{\vee, \&, \neg\}$  для функций от  $n$  переменных с асимптотической сложностью  $2^n/n$  и линейной динамической активностью. Важно отметить, что, в отличие от обычной (статической) активности, порядок динамической активности не зависит от базиса.

Ещё одной важной мерой сложности СФЭ является её глубина. Если сложность моделирует размер устройства, а мощность — энергопотребление, то глубина определяет задержку между подачей на устройство входного набора и получением вычисленного значения на выходе. С. Б. Гапков показал<sup>15</sup>, что функция Шеннона глубины СФЭ для функций от  $n$  переменных равна  $n - \log_2 \log_2 n$  с точностью до аддитивной константы. Затем С. А. Ложкин показал<sup>16</sup>, что в базисе  $\{\vee, \&, \neg\}$  функция Шеннона глубины СФЭ равна  $[n - \log_2 \log_2 n + o(1)]$  при  $n \rightarrow \infty$ . В более поздней работе<sup>17</sup> Ложкин наилёг функцию Шеннона глубины СФЭ в произвольном полном конечном базисе с точностью до аддитивной константы.

СФЭ является далеко не единственной моделью, позволяющей определять меры сложности булевых функций. Другой такой моделью являются контактные схемы (далее КС). Сложность КС определяется, как количество её контактов. Лупанов показал<sup>18</sup>, что слож-

ности КС определяется, как количество её контактов. Лупанов показал<sup>18</sup>, что слож-

ности КС определяется, как количество её контактов. Лупанов показал<sup>18</sup>, что слож-

ности КС определяется, как количество её контактов. Лупанов показал<sup>18</sup>, что слож-

ности КС определяется, как количество её контактов. Лупанов показал<sup>18</sup>, что слож-

ности КС определяется, как количество её контактов. Лупанов показал<sup>18</sup>, что слож-

ности КС определяется, как количество её контактов. Лупанов показал<sup>18</sup>, что слож-

ности КС определяется, как количество её контактов. Лупанов показал<sup>18</sup>, что слож-

ности КС определяется, как количество её контактов. Лупанов показал<sup>18</sup>, что слож-

ности КС определяется, как количество её контактов. Лупанов показал<sup>18</sup>, что слож-

ность КС, реализующих булевые функции от  $n$  переменных, асимптотически равна  $2^n/n$ , как и сложность СФЭ. Ю. С. Шуткин ввёл<sup>19</sup> понятие временной сложности моделирования КС, которая является в определённом смысле аналогом мощности СФЭ. Он показал, что функция Шеннона сложности моделирования КС растёт линейно с ростом числа переменных.

А. В. Чашкин ввёл<sup>20</sup> ещё одну модель вычисления булевых функций — неветвящиеся программы с условной остановкой. СФЭ можно представить в виде неветвящейся программы следующим образом. Всем входам, выходам и рёбрам сопоставляются различные переменные, затем последовательность вычислений значений этих переменных записывается в виде программы, в которой каждая строчка имеет вид  $x_i = f_i(x_{j_{i,1}}, \dots, x_{j_{i,n}})$ , где  $f_i$  — функция, вычисляемая  $i$ -м функциональным элементом,  $x_{j_{i,1}}, \dots, x_{j_{i,n}}$  — переменные, приписанные входам этого элемента,  $x_i$  — переменная, приписанная его выходу. При таком сопоставлении сложность СФЭ равна количеству команд в программе, то есть её длине. В неветвящейся программе с условной остановкой левые части команд могут повторяться, и кроме обычных команд могут также использоваться команды вида  $stop(x_i)$ . Если  $x_i = 1$ , то выполнение программы на этом шаге завершается. Таким образом, среднее время выполнения программы с условной остановкой может быть существенно меньше, чем длина программы. Среднее время выполнения оптимальной программы с условной остановкой называется средней сложностью булевой функции. В работе Чашкина<sup>20</sup> были получены порядки роста функций Шеннона средней сложности для классов веяюю определённых булевых функций, частичных булевых функций и функций с малым числом единиц. В частности, было показано, что для почти всех булевых функций средняя сложность по порядку совпадает со сложностью СФЭ, а для класса функций от  $n$  переменных с малым числом единиц средняя сложность по порядку в  $n$  раз меньше сложности СФЭ.

Из перечисленных моделей наиболее подходящей для моделирования микросхем, реализующих булевые функции, является модель СФЭ. Недостаток данной модели заключается в том, что в ней не учитывается разводка проводов на плоскости, хотя при проектировании чипа размещение проводов является не менее важной задачей, чем построение самой логической схемы. С. С. Кравцов предложил<sup>21</sup> модель плоских (клеточных) схем, которая отражает как логическую часть микросхемы (СФЭ), так и размещение её элементов на плоскости. Фактически, плоская схема является укладкой СФЭ на целочисленную решётку на плоскости таким образом, что соединёнными могут быть лишь элементы, находящиеся с соседних точках решётки; при этом длины провода моделируются цепью элементов, реализующих тождественные функции. Кравцов доказал, что порядок функции Шеннона площасти плоских схем, реализующих функции от  $n$  переменных, равен  $2^n$ . А. Альбрехт показал<sup>22</sup>, что асимптотика функции Шеннона имеет вид  $\sigma 2^n$ . Однако его доказательство неконструктивно, и конкретное значение константы  $\sigma$  до сих пор неизвестно. Кроме того, эта константа может зависеть от базиса. Тем не менее, С. В. Грибок привёл<sup>23</sup> пример базиса, для которого константа  $\sigma$  вычисляется явно. В настоящей работе вводится определение плоской схемы, отличающейся от определения Кравцова, которое как правило используется в других работах. Однако с точки зрения оценок площасти и других мер сложности это отличие непринципиальный.

<sup>19</sup>Ю. С. Шуткин. "Об одновременной минимизации объёмной и временной сложности контактных и вентильных схем". в: *Интеллектуальные системы. Теория и приложения* 14.1-4 (2010), с. 595–615

<sup>20</sup>А. В. Чашкин. "О среднем времени вычисления значений булевых функций". в: *Дискретный анализ и исследование операций* 4.1 (1997), с. 60–78

<sup>21</sup>С. С. Кравцов. "О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов". в: *Проблемы кибернетики. Вып 19*. М.: Наука, 1967, с. 285–293

<sup>22</sup>А. Альбрехт. "О схемах из клеточных элементов". в: *Проблемы кибернетики. Вып 39*. М.: Наука, 1977, с. 209–214

<sup>23</sup>С. В. Грибок. "Об одном базисе для схем из клеточных элементов". в: *Вестник Московского Университета, сер. 15. Вычислительная математика и кибернетика* 4 (1999), с. 36–39

ально (когда речь не идёт о нахождении асимптотики). Перечисляемые ниже результаты, как и результаты Кравцова и Альбрехта верны вне зависимости от конкретного определения с точностью до мультипликативной константы. То же самое можно сказать и о результатах, полученных в данной диссертации. Определение плоской схемы, используемое в диссертации позволяет строить схемы без изолирующих элементов, что позволяет чуть компактнее изображать громоздкие схемы.

Н.А. Шкаликова исследовала<sup>24</sup> площадь плоских схем для некоторых конкретных семейств булевых операторов, а также для класса симметрических булевых функций. Кроме того, в этой работе была установлена связь между площадью плоских схем и объёмом трёхмерных схем, реализующих булевые операторы. Шкаликова показала, что если оператор реализуется трёхмерной схемой с объёмом  $V$ , то его можно реализовать плоской схемой с площадью  $O(V^{3/2})$ , причём порядок этой оценки нельзя понизить. А. А. Тиунчик нашёл<sup>25</sup> порядок роста функции Шеинона площади плоских схем константной ширины, в которых допускаются кратные входы. А. Ю. Яблонская усилила<sup>26</sup> этот результат и нашла асимптотику площади плоских схем константной ширины с кратными входами для некоторых классов булевых функций. Д. А. Жуков<sup>27,28,29</sup> для различных семейств булевых операторов и функций предложил методы синтеза плоских схем, позволяющие оптимизировать одновременно площадь и глубину. В частности, Жуков показал<sup>29</sup>, что произвольную частичную булеву функцию можно реализовать плоской схемой с площадью  $O(d)$  и глубиной  $O(\log d)$ , где  $d$  — размер области определения.

В данной диссертации вводятся меры мощности (активности) плоских схем, отражающие энергопотребление микросхемы, которую моделирует плоская схема. Одна из рассматриваемых мер мощности — *потенциал* (активность) — является аналогом мощности (статической активности) СФЭ. Эту меру мощности впервые ввёл О.В. Черемисин<sup>30</sup>, он показал что невозможно реализовать дешифратор плоской схемой с одновременно оптимальными по порядку площадью и потенциалом.

Также в данной работе рассматривается и другая мера мощности — *переключательная мощность*, которая является аналогом динамической активности СФЭ. Эта мера сложности лучше отражает энергопотребление микросхем, поскольку основная энергия тратится на переходные процессы, которые происходят при переключении элементов схемы.

Одним из основных направлений исследований диссертации является разработка универсальных методов синтеза плоских схем, позволяющих для большинства функций из заданного класса получать схемы с оптимальными по порядку мощностью и площадью. Вторым направлением является доказательство нижних оценок мощности плоских схем с целью обоснования оптимальности предложенных методов синтеза. Кроме того, в работе получено несколько универсальных оценок, связывающих меры сложности плоских схем. В частности,

<sup>24</sup> Н. А. Шкаликова. "О реализации булевых функций схемами из клеточных элементов". в: *Математические вопросы кибернетики. Вып. 2*. М.: Наука, 1989, с. 177–197

<sup>25</sup> А. А. Тиунчик. "О реализации функций алгебры логики клеточными схемами ограниченной ширины". в: *Методы дискретного анализа в решении экстремальных задач. Новосибирск: Институт математики СО АН СССР* 50 (1990), с. 73–83

<sup>26</sup> А. Ю. Яблонская. "О сложности реализации булевых функций из инвариантных классов схем ограниченной высоты с кратными входами". в: *Вестник НИГУ* 4.1 (2012), с. 225–231

<sup>27</sup> Д. А. Жуков. "О времени параллельного сложения нескольких чисел". в: *Вестник Московского университета. Серия 1, Математика. Механика* 6 (2001), с. 52–54

<sup>28</sup> Д. А. Жуков. "Быстрые клеточные схемы для умножения". в: *Дискретный анализ и исследование операций. Серия 1* 9.3 (2002), с. 40–47

<sup>29</sup> Д. А. Жуков. "О вычислении частичных булевых функций клеточными схемами". в: *Дискретный анализ и исследование операций. Серия 1* 11.2 (2004), с. 32–40

<sup>30</sup> О. В. Черемисин. "Об активности схем из клеточных элементов, реализующих систему всех конъюнкций". в: *Дискретная математика* 15.2 (2003), с. 113–122

в работе показано, что переключательная мощность и потенциал совпадают по порядку. В связи с этим далее вместо терминов «переключательная мощность» или «потенциал» часто употребляется слово «мощность», подчёркивающее, что утверждение относится к обеим мерам мощности.

Заметим, что в отличие от схем из функциональных элементов, для площасти плоских схем известен лишь порядок функции Шеннона, а асимптотика неизвестна. Поэтому в данной работе исследуется именно порядок, а не асимптотика функции Шеннона. Кроме того, для моделей схем, аналогичных модели плоских схем (например, для модели многослойных схемы с фиксированным числом слоёв) порядок роста всех рассматриваемых в диссертации мер сложности такой же, как и в модели плоских схем, поэтому все полученные результаты верны и во всех аналогичных моделях схем<sup>31</sup>.

Одним из основных результатов работы является нахождение порядка функции Шеннона мощности частичных булевых операторов. Отметим, что для схем из функциональных элементов важным фактором также является и глубина схемы, которая отражает скорость работы этой схемы. В одной из теорем показано, что для большого класса частичных операторов существуют схемы, одновременно оптимальные по мощности, площасти и глубине. Другим важным результатом является нахождение порядка функции Шеннона для булевых функций с малым числом единиц. Такие функции могут использоваться при построении схем для других классов булевых функций с целью понижения средней мощности путём фильтрации наборов, на которых значение функции вычисляется относительно просто. Также были найдены порядки функций Шеннона для всех замкнутых классов булевых функций.

## Цель работы

Цель работы состоит в исследовании функции Шеннона мощности плоских схем, реализующих булевые функции и операторы из различных классов. Также целью является выявление зависимости функции Шеннона от ограничений, наложенных на расположение входов и выходов схемы.

## Методы исследования

В работе используются методы дискретной математики, теории управляющих систем, теории вероятностей и математического анализа.

## Научная новизна

В работе получены оценки функции Шеннона мощности плоских схем, реализующих функции и операторы из различных классов. А именно, получен порядок роста функции Шеннона средней и максимальной мощности для класса частичных булевых операторов. Также получены более высокие нижние оценки мощности частичных булевых операторов при наличии ограничений на расположение выходов схемы. Показано, что если число выходов оператора по порядку больше, чем число входов, то существует оптимальное расстояние, на котором эти выходы должны быть расположены друг от друга, при таком расположении порядок роста мощности не более, чем линейно зависит от количества выходов схемы. При некоторых ограничениях на расположение выходов порядок роста мощности от количества выходов становится выше линейного. Во всех перечисленных результатах для класса частичных операторов оценки средней и максимальной мощности совпадают по порядку.

<sup>31</sup> От модели лишь требуется, чтобы в ней произвольный элемент, занимающий единицу площасти, реализовал булев оператор с числом входов и выходов, ограниченным некоторой константой.

Также получен порядок роста функции Шеннона максимальной мощности для класса функций с ограниченным числом единиц с учётом ограничений на расположение входов схемы. Как и в случае частичных операторов, показано, что наименьшая мощность достигается при определённом расстоянии между входами схемы.

В работе также исследован класс монотонных функций. Для этого класса получен порядок функции Шеннона средней и максимальной мощности. В частности, показано, что в классе монотонных функций порядки роста средней и максимальной мощности различаются. Как следствие получены порядки функции Шеннона для всех замкнутых классов булевых функций.

Кроме оценок функции Шеннона для конкретных классов функций, в работе есть несколько результатов о связи различных мер сложности плоских схем. Также доказана универсальная нижняя оценка функции Шеннона мощности для произвольного класса булевых функций.

## Теоретическая и практическая ценность работы

Диссертация носит теоретический характер. Результаты работы могут применяться при проектировании СВИС для уменьшения энергопотребления различных электронных устройств. Переключательная мощность плоских схем, исследованная в работе намного лучше отражает энергопотребление микросхемы, чем статическая мощность, которая обычно рассматривается при исследовании мощности схем из функциональных элементов. Однако в работе показано, что при определённых условиях переключательная и обычная мощности совпадают по порядку, откуда следует, что многие результаты для статической меры мощности могут быть обобщены и на переключательную мощность. Но даже переключательная мощность схем из функциональных элементов недостаточно точно отражает энергопотребление микросхемы, поскольку при современных технологиях проводники, соединяющие функциональные элементы, потребляют мощность, сравнимую с мощностью самих элементов. Поэтому, чтобы оптимизировать микросхему, необходимо учитывать энергию, выделяемую проводами, и модель, изучаемая в данной работе, позволяет это сделать. С практической точки зрения интересны не только методы синтеза, предложенные в работе, но и общие идеи оптимизации мощности, которые могут быть применены к конкретным схемам.

Разработанные методы получения нижних оценок могут применяться для получения нижних оценок для других классов булевых функций.

## Апробация работы и публикации автора

Основные результаты данной работы докладывались и публиковались в тезисах следующих конференций:

- Международная конференция студентов, аспирантов и молодых учёных «Ломоносов» (2013, 2014, Москва)
- Ломоносовские чтения (2013, 2014)
- XII Международный семинар «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (2016, Москва).
- XI Международная конференция «Интеллектуальные системы и компьютерные науки» (2016, Москва)

Результаты докладывались на семинарах механико-математического факультета МГУ имени М. В. Ломоносова:

- Семинаре «Теория автоматов» под руководством академика, проф., д.ф.-м.н. В. Б. Кудрявцева (2013 г., 2016 г., 2017 г.).
- Семинаре «Вопросы сложности алгоритмов поиска» под руководством проф., д.ф.-м.н. Э. Э. Гасанова (2013 – 2016 гг.).
- Спецсеминар для преподавателей, научных сотрудников, аспирантов и студентов «Дискретная математика и математическая кибернетика» (2016 г.).

Основные результаты диссертации опубликованы в статьях [1–6] в рецензируемых научных изданиях, определённых положением о присуждении учёных степеней в МГУ имени М. В. Ломоносова, а также в тезисах конференций [7–9].

## Структура и объем работы

Диссертация состоит из введения и трёх глав. Объем диссертации 164 страницы. Список литературы содержит 35 наименований.

## Благодарности

Автор выражает искреннюю благодарность заведующему кафедрой д.ф.-м.н., профессору, академику В.Б. Кудрявцеву и всему коллективу кафедры за опыт и знания, полученные во время обучения. Особую признательность хочется высказать научному руководителю д.ф.-м.н., профессору Э.Э. Гасанову за постановку задачи и научное руководство.

## Краткое содержание работы

### Плоские схемы

*Клеточным элементом* будем называть булев оператор, у которого в сумме не более четырёх входов и выходов, причём каждому его входу и каждому выходу сопоставлена некоторая метка из множества  $\{l, r, t, b\}$ , причём метки не повторяются.

Метки будем также называть сторонами элемента:

- $l$  — левая сторона;
- $r$  — правая сторона;
- $t$  — верхняя сторона;
- $b$  — нижняя сторона.

Клеточный элемент будем изображать в виде единичного квадрата на плоскости. При этом входам и выходам элемента сопоставляются стороны квадрата в соответствии с присвоенными им метками.

Метки, присвоенные входам (выходам) оператора будем называть *входами* (*выходами*) элемента. Метки, не присвоенные ни входам, ни выходам, будем называть изоляторами. Множество входов (выходов) элемента  $e$  будем обозначать  $in(e)$  ( $out(e)$ ).

Входы и выходы элемента будем называть его *контактами*.

Заметим, что это определение немного отличается от обычного тем, что допускается, чтобы на разных выходах реализовывались разные тождественные функции.

Если на всех выходах элемента реализуются тождественные функции, то будем называть элемент *коммутационным*, иначе — *логическим*.

Коммутационный элемент соответствует либо проводнику в микросхеме, либо пересечению проводов, либо тождественной функции, служащей для усиления сигнала.

Клеточный элемент можно описать уравнениями, которые задают его оператор, заменяя все переменные в них на сопоставленные им метки ( $l, r, t$  или  $b$ ). Тогда в левой части каждого уравнения будет стоять выходная метка, а в правую будут входить только входные метки.

Для удобства используется также пустой клеточный элемент — изолирующий.

Всюду далее значок  $:=$  будет обозначать «по определению равно».

Через  $E$  обозначим множество всех клеточных элементов,  $N_E := |E|$ .

*Сетью из клеточных элементов* на множестве  $M \subset \mathbb{Z}^2$  над базисом  $E' \subseteq E$  будем называть отображение  $K : M \rightarrow E'$ .

Элемент  $K(x, y)$  будем называть *элементом схемы*  $K$  с координатами  $(x, y)$ . Элемент с приписанными ему координатами будем называть *элементом схемы*.

*Левой, правой, верхней и нижней* сторонами элемента  $e$  с координатами  $(x, y)$  будем называть точки с координатами  $(x - \frac{1}{2}, y)$ ,  $(x + \frac{1}{2}, y)$ ,  $(x, y - \frac{1}{2})$  и  $(x, y + \frac{1}{2})$  соответственно (на рисунках ось  $y$  будет направлена вниз).

Будем говорить, что сеть  $K$  из клеточных элементов корректна, если для любых двух элементов  $x$  и  $y$  схемы  $K$  верно, что если сторона  $a$  элемента  $x$  совпадает со стороной  $b$  элемента  $y$ , то выполнено одно из условий:

- один из элементов  $x, y$  — изолирующий,
- стороны  $a$  и  $b$  являются изоляторами,
- Среди сторон  $a$  и  $b$  одна является выходом, другая — выходом, например,  $a$  — выход, а  $b$  — вход, в таком случае будем говорить, что выход  $a$  подключен к входу  $b$ ;

Множество  $M$  будем называть *носителем* сети  $K$ .

Введём понятие *графа корректной сети из клеточных элементов*  $K$  (будем обозначать  $G_K$ ).  $G_K$  — ориентированный граф, вершинами которого являются входы и выходы элементов схемы. Если выход одного элемента подключен ко входу другого, то им будет соответствовать одна и та же вершина графа (будем говорить, что эта вершина является выходом первого элемента и входом второго). Из вершины  $a$  в вершину  $b$  ведёт ребро в том и только том случае, когда существует элемент  $e$  такой, что  $a$  является его выходом,  $b$  — выходом, причём функция, реализуемая на выходе  $b$ , существенно зависит от входа  $a$ .

*Плоской схемой* или *схемой из клеточных элементов* на множестве  $M \subset \mathbb{Z}^2$  над базисом  $E' \subseteq E$  будем называть корректную сеть из клеточных элементов, в графе которой нет ориентированных циклов. Множество  $M$  будем называть *носителем* схемы  $K$ .

Далее везде используется базис  $E$ , то есть считается, что можно использовать любые клеточные элементы.

Если вход (выход) элемента не подключен к выходу (входу) другого элемента, будем его называть *входом* (выходом) схемы.

*Контактами* схемы будем называть ее входы и выходы. Множество входов (выходов) схемы  $K$  будем обозначать  $In(K)$  ( $Out(K)$ ).

Узлами схемы  $K$  будем называть вершины графа  $G_K$ .

Если  $M$  — носитель схемы  $K$ , то величину  $|M|$  будем называть *площадью* схемы  $K$  и обозначать  $|K|$ .

Расстоянием между узлами схемы будем называть число ребер в минимальной ориентированной цепи, соединяющей соответствующие вершины в  $G_K$ . Расстояние от узла  $a$  до узла  $b$  на схеме  $K$  будем обозначать  $\rho_K(a, b)$ .

Подсхемой схемы  $K$  с носителем  $M_0 \subseteq M$  будем называть схему  $K|_{M_0}$ . Если схема  $K$  фиксирована, то иногда будем говорить просто подсхема  $M_0$ .

Каждой плоской схеме  $K$  можно естественным образом сопоставить схему из функциональных элементов  $Circ(K)$ :

1. каждой функции  $f_{s,i}$ , которую реализует  $i$ -й выход элемента  $s$  клеточной схемы, сопоставим функциональный элемент  $e_{s,i}$ , реализующий  $f_{s,i}$ ; если  $i$ -й и  $j$ -й выходы являются выходами одной и той же функции, то им будет соответствовать один и тот же функциональный элемент.
2. если  $i$ -й выход  $s_1$  подключён к  $j$ -му входу  $s_2$  соединим выход элемента  $e_{s_1,i}$  с  $j$ -ми входами элементов  $e_{s_2,k}$  для всех  $k$ , для которых  $f_{s_2,k}$  зависит от  $j$ -го аргумента.
3. Удалим из схемы все тождественные функции, подсоединив их вход ко всем их выходам.

Будем говорить, что схема  $K$  реализует булев оператор  $f_K$ , если схема из функциональных элементов  $Circ(K)$  реализует  $f_K$ . Здесь следует отметить, что оператор  $f_K$  определяется схемой  $K$  с точностью до перестановки аргументов и компонент оператора.

Множество плоских схем, реализующих булев оператор  $f$  (возможно, частично определённый) будем обозначать  $Impl(f)$ .

Обозначим через  $S(f)$  минимальную площадь плоской схемы, реализующей оператор  $f$ .

### Меры мощности схем.

Для каждой схемы  $K$  зафиксируем некоторую нумерацию ее узлов. На  $i$ -м узле реализуется некоторая функция  $g_i$  от входных переменных схемы  $K$  (на входах считаем, что реализуются тождественные функции).

Везде далее будем считать, что схема  $K$  имеет  $n$  входов,  $l$  узлов и  $g_i$  — функция, реализуемая в  $i$ -м узле схемы  $K$ .

Состоянием схемы  $K$  на входном наборе  $x$  назовём вектор

$$s_K(x) := (g_1(x), \dots, g_l(x)).$$

Если  $v = (v_1, \dots, v_q) \in \{0, 1\}^q$ , обозначим  $|v| := v_1 + v_2 + \dots + v_q$ .

Введём операцию  $\oplus : \{0, 1\}^q \times \{0, 1\}^q \rightarrow \{0, 1\}^q$  — покомпонентное сложение по модулю 2, то есть  $(v_1, \dots, v_q) \oplus (u_1, \dots, u_q) = (v_1 \oplus u_1, \dots, v_q \oplus u_q)$ .

Заметим, что выполнено неравенство треугольника:

$$|v \oplus u| = \sum_{i=1}^l v_i \oplus u_i \leq \sum_{i=1}^l (v_i + u_i) = \sum_{i=1}^l v_i + \sum_{i=1}^l u_i = |v| + |u|. \quad (1)$$

Величина  $|v \oplus u|$  — количество компонент, по которым вектора  $u$  и  $v$  различаются.

Пусть схема  $K$  имеет  $n$  входов. Тогда

Потенциалом схемы  $K$  на входном наборе  $x \in \{0, 1\}^n$  назовём величину  $u_K(x) := |s_K(x)|$ . Фактически, потенциал схемы  $K$  на наборе  $x$  — это число узлов схемы  $K$ , принимающих значение 1, когда на вход схемы подан набор  $x$ .

Максимальным потенциалом схемы  $K$  с  $n$  входами на множестве входных наборов  $\mathcal{D} \subseteq \{0, 1\}^n$  назовём  $\hat{U}_{\mathcal{D}}(K) := \max_{x \in \mathcal{D}} u_K(x)$ .

Величину  $w_K(x, y) := |s_K(x) \oplus s_K(y)|$  назовём затратой энергии на переключение входа  $x$  на  $y$ .

Максимальной переключательной мощностью схемы  $K$  на множестве входных наборов  $\mathcal{D} \subseteq \{0, 1\}^n$  назовём величину

$$\widehat{W}_{\mathcal{D}}(K) := \max_{x, y \in \mathcal{D}} w_K(x, y).$$

В случае  $\mathcal{D} = \{0, 1\}^n$  индекс  $\mathcal{D}$  будем опускать, то есть  $\widehat{W}(K) = W_{\{0, 1\}^n}(K)$ .  $\widehat{W}(K)$  будем называть максимальной мощностью схемы  $K$ .

**Замечание.** Из 1 и свойства  $v \oplus u \oplus u \oplus w = v \oplus w$  следует неравенство треугольника для  $w_K$ :

$$w_K(x, y) + w_K(y, z) = |s_K(x) \oplus s_K(y)| + |s_K(y) \oplus s_K(z)| \geq |s_K(x) \oplus s_K(z)| = w_K(x, z), \quad (2)$$

то есть  $w_K$  является метрикой на множестве  $\{0, 1\}^n$ .

Средним потенциалом схемы  $K$  на множестве входных наборов  $\mathcal{D} \subseteq \{0, 1\}^n$  назовём величину

$$U_{\mathcal{D}}(K) := \frac{1}{|\mathcal{D}|} \sum_{x \in \mathcal{D}} w_K(x).$$

Средней переключательной мощностью схемы  $K$  на множестве входных наборов  $\mathcal{D} \subseteq \{0, 1\}^n$  назовём величину

$$W_{\mathcal{D}}(K) := \frac{1}{|\mathcal{D}|^2} \sum_{x, y \in \mathcal{D}} w_K(x, y).$$

Если  $\mathcal{D} = \{0, 1\}^n$ , то нижний индекс  $\mathcal{D}$  у меры мощности будем опускать.

Введём мощность и потенциал булевых операторов при заданном множестве  $Q$  допустимых плоских схем. Если  $H(K)$  — некоторая мера мощности ( $U_{\mathcal{D}}$ ,  $\widehat{U}_{\mathcal{D}}$ ,  $W_{\mathcal{D}}$  или  $\widehat{W}_{\mathcal{D}}$ ),  $F : \mathcal{D} \rightarrow \{0, 1\}^m$  — булев оператор (возможно, частичный),  $Q$  — множество допустимых плоских схем, то

$$H_Q(F) := \min_{K \in Impl(f) \cap Q} H(K).$$

Введём соответствующие функции Шеннона меры мощности  $H$  для класса функций  $\mathcal{F}$ :

$$H_Q(\mathcal{F}) := \max_{f \in \mathcal{F}} H_Q(f).$$

Обозначим  $P_2(\mathcal{D}', m)$  — множество частичных булевых операторов  $f : \mathcal{D}' \rightarrow \{0, 1\}^m$  с  $m$  выходами, определённых на множестве  $\mathcal{D}'$ . Отметим, что область определения оператора  $\mathcal{D}'$  может отличаться от множества  $\mathcal{D}$ , на котором измеряется мощность. Это связано с тем, рассматриваемая схема может быть подсхемой другой схемы, реализующей оператор с другой областью определения. При доказательстве нижних оценок также бывает полезно взять  $\mathcal{D} \subset \mathcal{D}'$ .

Обозначим  $P_2(n, m) := P_2(\{0, 1\}^n, m)$  — множество всюду определённых булевых операторов с  $n$  входами и  $m$  выходами.

Также введём функцию Шеннона мер мощности для булевых операторов. Если  $H$  — мера мощности функции ( $U_{\mathcal{D}, Q}$ ,  $\widehat{U}_{\mathcal{D}, Q}$ ,  $W_{\mathcal{D}, Q}$  или  $\widehat{W}_{\mathcal{D}, Q}$ ), то

$$\begin{aligned} H(\mathcal{D}') &:= H(P_2(\mathcal{D}', 1)), & H(n) &:= H(P_2(n, 1)); \\ H(\mathcal{D}', m) &:= H(P_2(\mathcal{D}', m)), & H(n, m) &:= H(P_2(n, m)). \end{aligned}$$

Во всех введённых обозначениях если множество допустимых схем  $Q$  совпадает со множеством всех схем, то индекс  $Q$  в мере мощности будем опускать.

## Общие обозначения

Введём несколько общих обозначений и определений, которые будут использоваться в формулировках теорем. В частности, в связи с большим числом параметров, от которых будут зависеть оценки (в том числе, неявно), уточним, как будут пониматься в работе такие стандартные обозначения, как  $o(\cdot)$ ,  $\omega(\cdot)$ ,  $O(\cdot)$  и  $\Omega(\cdot)$  в случае наличия неявных параметров. Часто нам понадобится писать асимптотические оценки различных величин, явно или неявно зависящих от набора параметров  $x = (x_1, \dots, x_k)$ , один из которых как правило стремится к бесконечности, а на остальные наложены асимптотические ограничения. Формально, есть некоторое множество допустимых наборов параметров  $X$ , и на нём задана база подмножеств<sup>32</sup>  $\mathfrak{B}$ . Могут быть и другие параметры, допустимые значения которых образуют множество  $Y$  и которые в данном контексте считаются фиксированными. Пусть величины  $f$  и  $g$  явно или неявно зависят от параметров  $x \in X$  и  $y \in Y$ . Введём несколько обозначений.

1. Будем писать  $f(x, y) = o(g(x, y))$  или  $g(x, y) = \omega(f(x, y))$  при базе  $\mathfrak{B}$ , если

$$\forall y \in Y \ (\exists B \in \mathfrak{B} \ \forall x \in B \ g(x, y) \neq 0) \text{ и } \lim_{\mathfrak{B}} \frac{f(x, y)}{g(x, y)} = 0,$$

то есть отношение  $f$  к  $g$  может стремиться к нулю неравномерно по  $y \in Y$ .

2.  $f(x, y) = O(g(x, y))$  или  $f(x, y) \preccurlyeq g(x, y)$  при базе  $\mathfrak{B}$ , если

$$\exists C > 0 \ \forall y \in Y \ \exists B \in \mathfrak{B} \ \forall x \in B \ f(x, y) \leq Cg(x, y),$$

то есть существует абсолютная константа  $C$  и подмножество  $B \subseteq X$ ,  $B \in \mathfrak{B}$  такие, что  $f(x, y) \leq Cg(x, y)$  для любых  $x \in B$ ,  $y \in Y$ .

3.  $f(x, y) \asymp g(x, y)$  при базе  $\mathfrak{B}$ , если  $f(x, y) \preccurlyeq g(x, y)$  и  $g(x, y) \preccurlyeq f(x, y)$  при базе  $\mathfrak{B}$ , то есть

$$\exists C_1 > 0, C_2 > 0 \ \forall y \in Y \ \exists B \in \mathfrak{B} \ \forall x \in B \ C_1g(x, y) \leq f(x, y) \leq C_2g(x, y).$$

Если каждый набор параметров  $x \in X$  задаёт некоторое множество объектов  $\mathcal{F}(x)$ , то будем говорить, что для почти всех элементов  $f \in \mathcal{F}(x)$  при базе  $\mathfrak{B}$  верно утверждение  $P(x, f)$ , если доля  $f \in \mathcal{F}(x)$ , для которых утверждение  $P(x, f)$  истинно, стремится к 1 по базе  $\mathfrak{B}$ , то есть

$$|\{f \in \mathcal{F}(x) : P(x, f)\}| = |\mathcal{F}(x)|(1 + o(1)) \text{ при } \mathfrak{B}.$$

Обычно множество  $\mathcal{F}(x)$  — множество булевых функций или операторов, а набор параметров  $x$  включает в себя число аргументов  $n$ , может также включать в себя область определения  $\mathcal{D}$ , число выходов оператора  $m$ , а также ограничения на геометрию схемы. База  $\mathfrak{B}$  как правило задаётся несколькими асимптотическими ограничениями на параметры при  $n \rightarrow \infty$ .

Для неасимптотических неравенств с точностью до константы будем использовать обозначение  $a \preceq b$ , если  $a \leq Cb$ , где  $C$  — некоторая абсолютная константа.

## Результаты

В первой главе доказаны общие результаты, связывающие различные меры сложности иллюстрирующих схем.

Будем говорить, что схемы  $K_1$  и  $K_2$  имеют однаковые укладки, если существует изоморфизм графов  $G_{K_1}$  и  $G_{K_2}$ , при котором соответствующие узлы схем  $K_1$  и  $K_2$  имеют однаковые координаты.

<sup>32</sup>Непустая система  $\mathfrak{B}$  подмножества множества  $X$  называется базой множества  $X$ , если  $\emptyset \notin \mathfrak{B}$  и для любых  $B_1, B_2 \in \mathfrak{B}$  существует  $B \in \mathfrak{B}$  такое, что  $B \subseteq B_1 \cap B_2$  (В. А. Зорич. *Математический анализ. Часть I*. МЦНМО Москва, 2017, с. 576).

**Теорема 1.1.** Если схема  $K$  имеет  $n$  входов и  $m$  выходов, то для любого множества  $\mathcal{D} \subseteq \{0, 1\}^n$  выполнены следующие утверждения.

1. Переключательная мощность по порядку не превосходит потенциал, а именно

$$\widehat{W}_{\mathcal{D}}(K) \leq 2\widehat{U}_{\mathcal{D}}(K), \quad W_{\mathcal{D}}(K) \leq 2U_{\mathcal{D}}(K).$$

2. Существует плоская схема  $K'$  с той же укладкой, что и схема  $K$  такая, что

$$F_K = F_{K'} \quad \text{и} \quad \widehat{U}_{\mathcal{D}}(K') \leq \widehat{W}_{\mathcal{D}}(K) + m + \min_{x \in \mathcal{D}} |x|.$$

3. Существует плоская схема  $K'$  с той же укладкой, что и схема  $K$  такая, что

$$F_K = F_{K'} \quad \text{и} \quad U_{\mathcal{D}}(K') \leq W_{\mathcal{D}}(K) + m + n.$$

**Следствие 1.** Для любого множества  $\mathcal{D} \subseteq \{0, 1\}^n$  и любого оператора  $F \in P_2(\mathcal{D}, m)$  выполнено

$$\widehat{U}_{\mathcal{D}}(F) - m \leq \widehat{W}_{\mathcal{D}}(F) \leq 2\widehat{U}_{\mathcal{D}}(F);$$

$$U_{\mathcal{D}}(F) - m - n \leq W_{\mathcal{D}}(F) \leq 2U_{\mathcal{D}}(F).$$

Отсюда, переходя к максимуму по  $F \in P_2(\mathcal{D}, m)$ , сразу получаем

**Следствие 2.** Для любого множества  $\mathcal{D} \subseteq \{0, 1\}^n$  выполнены неравенства

$$\widehat{U}(\mathcal{D}, m) - m \leq \widehat{W}(\mathcal{D}, m) \leq 2\widehat{U}(\mathcal{D}, m);$$

$$U(\mathcal{D}, m) - m - n \leq W(\mathcal{D}, m) \leq 2U(\mathcal{D}, m).$$

Таким образом, для функций максимальный потенциал и максимальная мощность — величины одного порядка, если нет ограничений на базис. Поэтому далее рассматривается только потенциал.

**Теорема 1.2.** Для любой булевой функции  $f$ , отличной от константы, выполнена оценка

$$\widehat{U}(f) \geq \frac{\sqrt{S(f)}}{4\sqrt{2}}.$$

Учитывая простую мощностную нижнюю оценку функции Шеннона для площади плоских схем, получим

**Следствие 1.** Пусть  $\mathcal{F}$  — некоторый класс булевых функций,  $\mathcal{F}(n) = \mathcal{F} \cap P_2(n)$ . Тогда для почти всех функций  $f \in \mathcal{F}(n)$  при  $n \rightarrow \infty$  выполнена оценка

$$\widehat{U}(f) \geq \sqrt{\log |\mathcal{F}(n)| - n \log n}.$$

Теперь сформулируем универсальную нижнюю оценку для среднего потенциала.

Для булевых функций от  $n$  переменных определим

- $|f| := |\{x : f(x) = 1\}|$  — вес булевой функции,
- $\text{dist}(f, g) := |f \oplus g|$  — метрика на множество булевых функций.

Пусть  $\mathcal{F}$  — класс булевых функций. Обозначим через  $\varphi_n(\mathcal{F}, t)$  максимальное количество функций из  $\mathcal{F}(n)$ , попадающих в шар радиуса  $2^n t$ ,

$$\varphi_n(\mathcal{F}, t) = \max_{f_0 \in P_2(n)} |\{f \in \mathcal{F}(n) : \text{dist}(f, f_0) \leq 2^n t\}|.$$

**Теорема 1.3.** Пусть задан класс функций  $\mathcal{F}$  такой, что  $n \log n = o(\log |\mathcal{F}(n)|)$  при  $n \rightarrow \infty$ . Тогда для любой невозрастающей последовательности  $\{t_n\}_{n=1}^{\infty}$ ,  $t_n \in (0, 1]$  для почти всех функций  $f \in \mathcal{F}_n$  при  $n \rightarrow \infty$  верна оценка

$$U(f) \geq t_n \sqrt{\log_2 \frac{|\mathcal{F}_n|}{\varphi_n(\mathcal{F}, t_n)}}.$$

Во второй главе исследуется мощность плоских схем, реализующих частичные булевы операторы. Нижние оценки доказаны как для случая схем без ограничений, так и с ограничением на расположение выходов. Для случая, когда на геометрию схемы не наложены никакие ограничения, имеет место следующая теорема.

**Теорема 2.4.** Пусть  $\mathcal{D} \subseteq \{0, 1\}^n$ . Тогда для почти всех частичных булевых операторов  $f : \mathcal{D} \rightarrow \{0, 1\}^m$  при  $n \rightarrow \infty$ ,  $|\mathcal{D}| = \omega(n \log n)$ ,  $m = 2^{o(|\mathcal{D}|)}$  выполнена оценка

$$U(f) \geq \sqrt{m|\mathcal{D}|} + m \frac{\sqrt{|\mathcal{D}|}}{\sqrt{\log_2 |\mathcal{D}|}}.$$

Если  $\log |\mathcal{D}| = o(m)$ , то при некоторых ограничениях на расположение выходов можно получить более высокую нижнюю оценку.

Поэтому сформулируем обобщение нижней оценки для случая с ограничением на расположение выходов. Рассмотрим множество  $P$  контактов схемы  $K$ . Для этого построим полный граф с вершинами в центрах клеток, контактами которых являются точки множества  $P$ . Сумму длин рёбер минимального остовного дерева этого графа обозначим через  $T_P$ .

Введём множество схем

$$Q_{out}[l, h] = \{K : l \leq T_{Out(K)} \leq h\}.$$

В частности, если  $l = 0$ , то это означает, что мы не ограничиваем  $T_{Out(K)}$  сверху, поскольку  $T_{Out(K)} \geq 0$  для любой схемы  $K$ .

**Теорема 2.5.** Если  $\mathcal{D} \subseteq \{0, 1\}^n$ , то для почти всех частичных булевых операторов  $f : \mathcal{D} \rightarrow \{0, 1\}^m$  при  $n \log n = o(|\mathcal{D}|)$  и  $m = 2^{o(|\mathcal{D}|)}$  выполнена оценка

$$U_{Q_{out}[0, h]}(f) \geq \frac{m^2 d}{(h + \sqrt{md}) \log_2 d}. \quad (3)$$

Для всюду определённых операторов эту оценку можно усилить, если на  $T_{Out(K)}$  наложить ограничение не только сверху, но и снизу. Пусть  $l, h \in \mathbb{N}$  такие, что  $l \leq h$ .

**Теорема 2.6.** Для почти всех операторов  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$  при  $n \rightarrow \infty$ ,  $\log m = o(2^n)$  и  $l \leq h$  выполнена оценка

$$U_{Q_{out}[l, h]}(f) \geq \begin{cases} \frac{m\sqrt{m}2^{n/2}}{n}, & h < \sqrt{m}2^{n/2}; \\ \frac{m^2 2^n}{nh}, & \sqrt{m}2^{n/2} \leq h < \frac{m2^{n/2}}{\sqrt{n}}; \\ \frac{m2^{n/2}}{\sqrt{n}}, & l \leq \frac{m2^{n/2}}{\sqrt{n}} \leq h; \\ l, & l > \frac{m2^{n/2}}{\sqrt{n}}. \end{cases}$$

При доказательстве верхней оценки мощности мы будем следить также за площадью и глубиной схемы. Введём ещё несколько определений.

*Цепью* в плоской схеме будем называть последовательность клеточных элементов, в которой выход каждого элемента, кроме последнего, подключён ко входу следующего элемента.

Элемент цепи назовём *существенным*, если он является логическим или он является разветвлением провода, то есть хотя бы на двух его выходах реализуется тождественная функция от одного и того же входа.

Всём цепи будем называть количество существенных элементов этой цепи.

Цепь максимального веса будем называть *максимальной* цепью.

Всё максимальной цепи схемы  $K$  будем называть *глубиной* и обозначать  $\delta(K)$ .

**Теорема 2.7.** *Если  $\mathcal{D} \subseteq \{0, 1\}^n$ , причём  $n^2 \leq |\mathcal{D}|$ , то для любого частичного оператора  $f : \mathcal{D} \rightarrow \{0, 1\}^m$  существует прямоугольная схема  $K$ , реализующая оператор  $f$  такая, что*

$$S(K) \preceq m|\mathcal{D}|, \quad \delta(K) \preceq \log_2 |\mathcal{D}| + \frac{m}{\log_2 |\mathcal{D}|},$$

$$\hat{U}(K) \preceq n \log_2^2 n + \frac{m \sqrt{|\mathcal{D}|}}{\sqrt{\min(m, \log_2 |\mathcal{D}|)}}.$$

Здесь следует отметить, что, хотя схема  $K$  реализует частичный оператор  $f$ , рассматривается максимальный потенциал по всем наборам, не только из области  $\mathcal{D}$ . Из этой теоремы, а также теоремы 2.4 следует основной результат второй главы — порядок функции Шеннона потенциала для частичных булевых операторов.

**Следствие 1.** *Если  $\mathcal{D} \subseteq \{0, 1\}^n$ , причём  $n^2 \log_2^4 n \leq |\mathcal{D}|$ , то*

$$\hat{U}(\mathcal{D}, m) \asymp U(\mathcal{D}, m) \asymp \frac{m \sqrt{|\mathcal{D}|}}{\sqrt{\min(m, \log_2 |\mathcal{D}|)}} \quad \text{при } n \rightarrow \infty, \quad m = 2^{o(|\mathcal{D}|)}.$$

Таким образом для почти всех частичных булевых операторов существуют прямоугольные схемы с оптимальной по порядку мощностью и площадью. Причём, при  $m \leq \log_2^2 |\mathcal{D}|$ , глубина схемы также будет оптимальна.

Если рассматривать не только прямоугольные схемы, то глубину можно сделать оптимальной по порядку для произвольного  $m$ .

**Теорема 2.8.** *Если  $\mathcal{D} \subseteq \{0, 1\}^n$ , причём  $|\mathcal{D}| \geq n^2 \log_2^4 n$ , то для любого частичного оператора  $f : \mathcal{D} \rightarrow \{0, 1\}^m$  существует схема  $K$ , реализующая оператор  $f$  такая, что*

$$S(K) \preceq m|\mathcal{D}|, \quad \hat{U}(K) \preceq \frac{m \sqrt{|\mathcal{D}|}}{\sqrt{\min(m, \log_2 |\mathcal{D}|)}}, \quad \delta(K) \preceq \log_2 m|\mathcal{D}|.$$

Вторую главу завершает доказательство следующего несложного утверждения, из которого следует, что полученные оценки площади и глубины являются оптимальными по порядку.

**Утверждение 2.1.** *Если  $\mathcal{D} \subseteq \{0, 1\}^n$ , причём  $|\mathcal{D}| \geq n^2 \log_2^4 n$ , то площадь  $O(m|\mathcal{D}|)$  и глубина  $O(\log_2 m|\mathcal{D}|)$  оптимальны по порядку для почти всех частичных операторов  $f : \mathcal{D} \rightarrow \{0, 1\}^m$  при  $n \rightarrow \infty, m = 2^{o(|\mathcal{D}|)}$ .*

В третьей главе рассматриваются разные классы булевых функций. Большая часть этой главы посвящена максимальному потенциалу булевых функций с ограниченным числом единиц. Такие функции являются характеристическими функциями подмножеств  $\{0, 1\}^n$  и могут использоваться в сочетании с частичными функциями и операторами, определенными на этих подмножествах. Поскольку схемы, реализующие эти функции, в основном могут использоваться в качестве вспомогательных блоков для реализации других функций, то распределение на их входах может не быть равномерным. Поэтому для этого класса функций наибольший интерес представляет именно максимальный потенциал, он не зависит от распределения вероятностей.

Для функций с малым числом единиц, как и для частичных операторов, исследуется зависимость потенциала от ограничений на схему, но на этот раз ограничения накладываются не на выходы, а на входы схемы. Поэтому для формулировки результатов нам потребуется множество схем  $Q_{in}[l, h] = \{K : l \leq T_{in(K)} \leq h\}$ .

Если  $\mathcal{D} \subseteq \{0, 1\}^n$ , то за  $\mathcal{F}_N^{\mathcal{D}}$  обозначим класс функций  $f : \mathcal{D} \rightarrow \{0, 1\}$ , принимающих значение 1 не более, чем на  $N$  наборах.

Оценки потенциала будут использовать функцию  $u_0(h, N, d)$ , которая определяется следующим образом.

$$u_0(h, N, d) := \frac{R \log_2 d}{\max(h, \sqrt{R}) \log_2 \frac{\max(2 \log_2 d, h, N)}{\log_2 d}}, \quad (4)$$

где  $R = N \log_2 \frac{d}{N}$ .

**Теорема 3.9.** Пусть  $\mathcal{D}$  – произвольное подмножество  $\{0, 1\}^n$  мощности  $d$ ,  $f_0$  – частичная функция из  $\mathcal{D}$  в  $\{0, 1\}$ ,  $h$  и  $N$  – некоторые параметры. Тогда если выполнены неравенства

$$N \leq \frac{d}{2} \quad \text{и} \quad N \log_2 \frac{d}{N} \geq C_0 h \log_2 h,$$

то для функций  $f \in \mathcal{F}_N^{\mathcal{D}}$ , для которых справедлива нижняя оценка максимального потенциала

$$\hat{U}_{Q_{in}[0, h]}(f_0 \oplus f) \geq C_1 u_0(h, N, d),$$

составляет не менее  $1 - \alpha(N, d)$ , где  $\alpha(N, d) = O(2^{-R/2})$  при  $N, d \rightarrow \infty$ . Здесь  $C_0, C_1$  – некоторые абсолютные константы.

Определим функции

$$h_1(N, n) = \sqrt{\frac{Nn(n - \log_2 N)}{\log_2 N}}$$

и

$$u_1(l, h, N, n) = \begin{cases} u_0(h, N, 2^n), & \text{если } h < h_1(N, n); \\ h_1(N, n), & \text{если } l \leq h_1(N, n) \leq h; \\ l, & \text{если } l > h_1(N, n). \end{cases}$$

**Теорема 3.10.** Для любых натуральных чисел  $n$  и  $N$ , а также параметров  $l$  и  $h \geq l$ , удовлетворяющих неравенствам

$$\log^2 n \leq N \leq 2^{n-1} \quad \text{и} \quad n \leq h$$

для функций  $f \in \mathcal{F}_N^n$ , для которых справедлива оценка (по порядку) максимального потенциала

$$\hat{U}_{Q_{in}[l, h]}(f) \asymp u_1(l, h, N, 2^n) \asymp \min_{t \in [l, h]} \max(t, u_0(t, N, 2^n)), \quad \text{при } n \rightarrow \infty,$$

составляет не менее  $1 - \alpha(n)$ , где  $\alpha(n) = O(2^{-C_1 N})$  при  $n \rightarrow \infty$ . Здесь  $C_1 > 0$  – некоторая абсолютная константа.

Введём обозначение  $Q_{\asymp h} := Q_{in}[h/2, h]$ .

Из теоремы 3.10 следует, что при  $N < 2^{n/2}$  для получения оптимального потенциала с ограничением  $Q_{\asymp h(n)}$ , нужно взять  $h(n) = h_1(N, n)$ . Отсюда вытекает оценка максимального потенциала без ограничений на расположение входов схемы.

**Следствие 1.** *Если параметр  $N$  удовлетворяет неравенству*

$$\log_2 n \leq N \leq 2^{n-1}.$$

*то для почти всех функций  $f \in F_N^n$  справедлива оценка (по порядку) максимального потенциала*

$$\widehat{U}(f) \asymp h_1(N, n), \text{ при } n \rightarrow \infty.$$

Хотя для класса  $F_N^n$  максимальный потенциал представляет больший интерес, чем средний потенциал сам по себе, сформулируем верхнюю оценку среднего потенциала, чтобы показать, что при определённом соотношении  $N$  и  $n$  он существенно меньше, чем максимальный потенциал.

**Теорема 3.11.** *Для произвольных  $n$ ,  $N \leq 2^n$  выполнена оценка*

$$U(F_N^n) = O\left(n + \sqrt{\frac{N \log_2 N}{n}}\right).$$

Разница между максимальным и средним потенциалом особенно существенная при  $N = n^3$ . В этом случае  $U(F_N^n) = O(n\sqrt{\log_2 n})$  по теореме 3.11, а  $\widehat{U}(F_N^n) \asymp \frac{n^2\sqrt{n}}{\sqrt{\log_2 n}}$  по следствию 1.

Ещё один результат третьей главы — оценки для класса монотонных функций.

За  $M_n$  будем обозначать класс монотонных функций от  $n$  переменных.

**Теорема 3.12.**

$$\widehat{U}(M_n) \asymp \frac{2^{n/2}}{\sqrt[3]{n}}, \quad U(M_n) \asymp \frac{2^{n/2}}{n^{3/4}} \text{ при } n \rightarrow \infty.$$

Из результатов для класса монотонных функций и для  $P_2$  можно получить порядок мощности для всех замкнутых классов. Чтобы сформулировать этот результат, разобьём все замкнутые классы<sup>33</sup> на 4 множества (рисунок 1).

$$R = \{P_2, T_0, T_1, T_{01}, S, S_{01}, I^\mu, I_1^\mu, I^\infty, I_1^\infty, O^\mu, O_0^\mu, O^\infty, O_0^\infty\};$$

$$R_M = \{M, M_0, M_1, M_{01}, SM, MI^\mu, MI_1^\mu, MI^\infty, MI_1^\infty, MO^\mu, MO_0^\mu, MO^\infty, MO_0^\infty\};$$

$$R_L = \{K, K_0, K_1, K_{01}, L, L_0, L_1, L_{01}, SL, D, D_0, D_1, D_{01}\};$$

$$R_C = \{U, SU, MU, U_0, U_1, U_{01}, C, C_0, C_1\}.$$

**Теорема 3.13.** *Если  $F$  — замкнутый класс, то имеют место следующие оценки.*

1. *Если  $F \in R$ , то  $\widehat{U}_F(n) \asymp U_F(n) \asymp 2^{n/2}$  при  $n \rightarrow \infty$ .*
2. *Если  $F \in R_M$ , то  $\widehat{U}_F(n) \asymp \frac{2^{n/2}}{\sqrt[3]{n}}$ ,  $U_F(n) \asymp \frac{2^{n/2}}{n^{3/4}}$  при  $n \rightarrow \infty$ .*
3. *Если  $F \in R_L$ , то  $\widehat{U}_F(n) \asymp U_F(n) \asymp n$  при  $n \rightarrow \infty$ .*
4. *Если  $F \in R_C$ , то  $\widehat{U}_F(n) \asymp U_F(n) = O(1)$ .*

Таким образом, все замкнутые классы делятся на 4 группы. Порядок мощности в любом замкнутом классе либо такой же, как в  $P_2$ , либо как в классе монотонных функций, либо линейный, либо константный.

<sup>33</sup>Обозначения замкнутых классов взяты из книги: А.Б. Угольников. *Классы Поста. Учебное пособие*. М.: Изд-во ЦПИ при механико-математическом факультете МГУ имени М.В. Ломоносова, 2008, с. 64

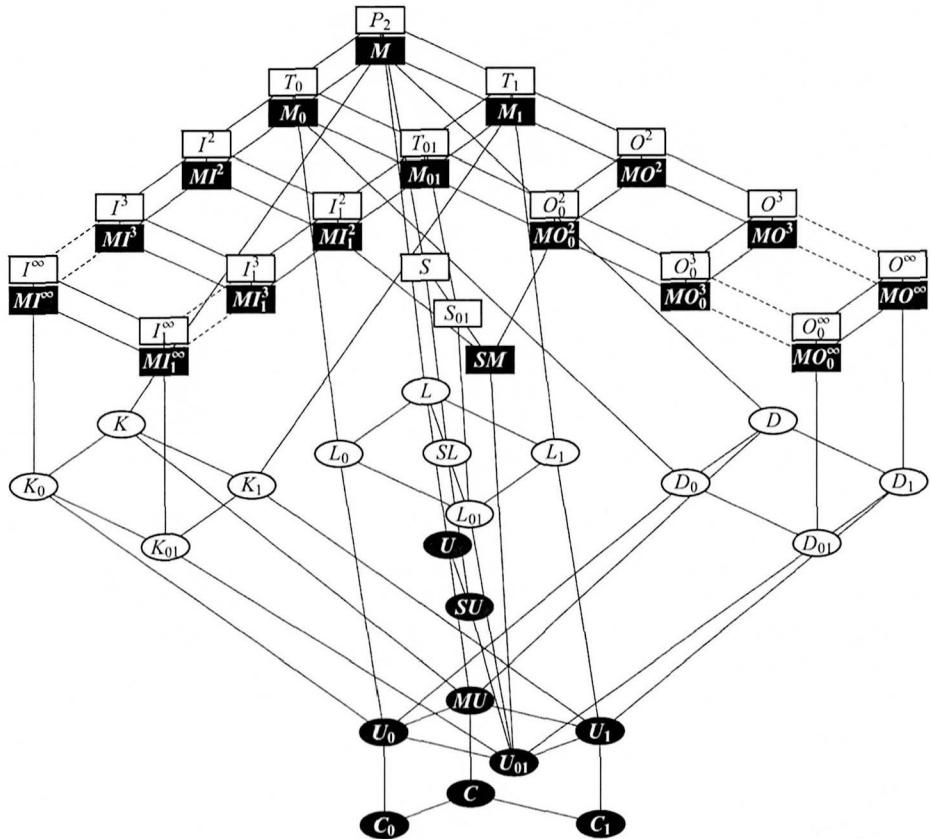


Рис. 1: Разбиение множества замкнутых классов на группы:  $R$  (белые прямоугольники),  $R_M$  (чёрные прямоугольники),  $R_L$  (белые эллипсы),  $R_C$  (чёрные эллипсы).

В следующей таблице собраны порядки функции Шеннона потенциала и площади плоских схем без ограничений для рассмотренных в работе классов всюду определённых булевых функций и операторов.

Класс $\mathcal{F}$	$S(\mathcal{F})$	$\hat{U}(\mathcal{F})$	$U(\mathcal{F})$
$P_2(n); F(n)$ при $F \in R$	$2^n$	$2^{n/2}$	$2^{n/2}$
$M(n); F(n)$ при $F \in R_M$	$2^n$	$2^{n/2}$	$2^{n/2}$
$F_N^n$ при $\log_2 n \leq N \leq 2^{n-1}$	$\sqrt{n}$	$\sqrt[4]{n}$	$\frac{n^{3/4}}{n}$
$P_2(n, m)$ при $\log m = o(2^n)$	$m2^n$	$\frac{m2^{n/2}}{\sqrt{\min(m, n)}}$	$\frac{m2^{n/2}}{\sqrt{\min(m, n)}}$

## Заключение

Основные результаты диссертации состоят в следующем.

- Введены понятия средней и максимальной переключательной мощности плоских схем, и показано, что переключательная мощность для любого булева оператора совпадает по порядку с потенциалом (который также называется активностью) плоских схем при условии, что в базисе имеются произвольные клеточные элементы.
- Получена нижняя оценка максимального потенциала для произвольной булевой функции через площадь минимальной схемы, реализующей данную функцию. Как следствие, получена универсальная нижняя оценка функции Шеннона максимального потенциала для произвольного класса булевых функций. Также получена универсальная нижняя оценка функции Шеннона среднего потенциала для произвольного класса булевых функций.
- Получен порядок функции Шеннона среднего и максимального потенциала плоских схем, реализующих частичные булевые операторы. При этом нижняя оценка доказана в большей общности и учитывает ограничения, которые могут быть наложены на расположение выходов. В частности, показано, что если число выходов существенно больше, чем входов, и все выходы схемы расположены рядом, то нижняя оценка потенциала существенно выше, чем потенциал оптимальной схемы без ограничений на расположение выходов. При доказательстве верхней оценки построена схема, имеющая оптимальные по порядку потенциал, площадь и глубину.
- Для класса функций с ограниченным числом единиц получена функция Шеннона максимального потенциала в зависимости от ограничений на расположение входов схемы. С использованием доказанной теоремы выводится порядок роста функции Шеннона для схем без ограничений. Из полученных результатов также следует, что для функций с малым числом единиц невозможно построить схему с расположенным рядом входами и потенциалом, оптимальным по порядку.
- Получен порядок функции Шеннона среднего и максимального потенциала для класса монотонных функций. С помощью этого результата и оценок для частичных булевых операторов получены порядки роста функции Шеннона среднего и максимального потенциала для всех замкнутых классов булевых функций.

Одно из направлений дальнейшей разработки темы диссертации может быть связано с исследованием функции Шеннона потенциала и переключательной мощности для других классов булевых функций и операторов. Другим направлением дальнейшего развития темы является исследование среднего потенциала и переключательной мощности плоских схем при неравномерном распределении вероятностей на входах. Для развития данного направления можно использовать результаты 3-й главы диссертации об оценках для функций с ограниченным числом единиц. Также вполне естественным является исследование мощности для плоских схем, реализующих автоматы (при этом в базис добавляется элемент задержки).

Кроме этого, интересным обобщением является исследование различных мер сложности в модели многослойных схем с растущим числом слоёв, на которых могут располагаться провода, а также в модели объёмных схем.

## Публикации автора по теме диссертации

- [1] Г. В. Калачев. "Порядок мощности плоских схем, реализующих булевы функции". в: *Дискретная математика* 26.1 (2014). (перевод: Kalachev G. V. Order of power of planar circuits implementing Boolean functions // *Discrete Mathematics and Applications*. – 2014. – Vol. 24, no. 4. – P. 185–205.), с. 49–74.
- [2] Г. В. Калачев. "Нижние оценки мощности плоских схем, реализующих частичные булевы операторы". в: *Интеллектуальные системы. Теория и приложения* (ранее: *Интеллектуальные системы по 2014, № 2, ISSN 2075-9460*) 18.2 (2014), с. 279–322.
- [3] Г. В. Калачев. "Об одновременной минимизации площади, мощности и глубины плоских схем, реализующих частичные булевы операторы". в: *Интеллектуальные системы. Теория и приложения* (ранее: *Интеллектуальные системы по 2014, № 2, ISSN 2075-9460*) 20.2 (2016), с. 203–266.
- [4] Г. В. Калачев. "Об оценках мощности плоских схем для замкнутых классов булевых функций". в: *Интеллектуальные системы. Теория и приложения* (ранее: *Интеллектуальные системы по 2014, № 2, ISSN 2075-9460*) 20.3 (2016), с. 52–57.
- [5] Г. В. Калачев. "Оценки мощности плоских схем, реализующих функции с ограниченным числом единиц". в: *Интеллектуальные системы. Теория и приложения* (ранее: *Интеллектуальные системы по 2014, № 2, ISSN 2075-9460*) 21.1 (2017), с. 28–96.
- [6] Г. В. Калачев. "Оценки мощности плоских схем, реализующих монотонные функции". в: *Интеллектуальные системы. Теория и приложения* (ранее: *Интеллектуальные системы по 2014, № 2, ISSN 2075-9460*) 21.2 (2017), с. 163–192.
- [7] Г. В. Калачев. "Порядок мощности плоских схем, реализующих булевы функции". в: *Тезисы докладов XX Международной научной конференции студентов, аспирантов и молодых учёных «Ломоносов-2013» / Секция «Математика и механика» / 2013г. / тезисы*. Москва, 2013.
- [8] Г. В. Калачев. "Оценки мощности плоских схем, реализующих булевы операторы". в: *Тезисы докладов XX Международной научной конференции студентов, аспирантов и молодых учёных «Ломоносов-2014». Секция «Математика и механика»*. 2014.
- [9] Г. В. Калачев. "О порядке роста мощности плоских схем для замкнутых классов булевых функций". в: *Материалы XII Международного семинара «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (Москва, МГУ, 20–25 июня 2016 г.)* Изд-во механико-математического факультета МГУ Москва, 2016, с. 132–133.

Подписано в печать 15.12.2017 г.

Формат А5

Бумага офсетная. Печать цифровая.

Тираж 100 Экз. Заказ № 125686-12-17

Типография ООО “МДМпринт”

(Печатный салон МДМ)

119146, г. Москва, Комсомольский пр-кт, д.28

Тел. 8-495-256-10-00

