На правах рукописи

**Кафтан Дарья Владимировна**

# ОЦЕНКИ ДЛИНЫ ТЕСТОВ И СЕРТИФИКАТОВ ДЛЯ БЕСПОВТОРНЫХ ФУНКЦИЙ

Специальность 01.01.09 –
«Дискретная математика и математическая кибернетика»

Автореферат
диссертации на соискание учёной степени
кандидата физико-математических наук

Москва — 2021

Работа выполнена в кафедре математической кибернетики факультета вычислительной математики и кибернетики МГУ имени М. В. Ломоносова.

Научный руководитель: **Вороненко Андрей Анатольевич**
доктор физико-математических наук, профессор.

Официальные оппоненты: **Кочергин Вадим Васильевич,**
доктор физико-математических наук,
профессор кафедры дискретной математики механико-математического факультета МГУ имени М.В. Ломоносова

**Абросимов Михаил Борисович,**
доктор физико-математических наук, доцент,
заведующий кафедрой теоретических основ компьютерной безопасности и криптографии Саратовского государственного университета имени Н.Г. Чернышевского

**Часовских Анатолий Александрович,**
кандидат физико-математических наук, доцент,
доцент кафедры математической теории интеллектуальных систем механико-математического факультета МГУ имени М.В. Ломоносова

Защита состоится 29 декабря 2021 года в 16:45 на заседании диссертационного совета МГУ.05.01 при Московского государственного университета имени М. В. Ломоносова по адресу: Москва, Ленинские горы, д. 1, Главное здание МГУ, ауд. 14-08. E-mail: vasenin@msu.ru.

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ имени М.В. Ломоносова (Москва, Ломоносовский просп., д. 27) и на сайте ИАС «Истина»: https://istina.msu.ru/dissertations/411567347/.

Автореферат разослан 29 ноября 2021 года.

Ученый секретарь
диссертационного совета
МГУ.05.01,
к.ф.-м.н., с.н.с М. Кривчиков Кривчиков М.А.

## Общая характеристика работы

**Актуальность темы и степень ее разработанности.** Теория дискретных функций относится к наиболее важным направлениям исследований в дискретной математике. Развитие исследований в данном направлении обусловлено интенсивным развитием области информационных технологий. Аппарат дискретных функций широко используется при проектировании дискретных устройств, в задачах синтеза и диагностики схем, кодировании информации, математическом моделировании. Теория булевых функций является одной из главных областей теории дискретных функций. К перечню основных проблем теории булевых функций относится проблема выразимости заданной функции или множества функций с помощью суперпозиции функций из некоторой системы.

В 1921 г. Э. Постом были определены все порожденные с помощью суперпозиции замкнутые классы булевых функций. Впервые бесповторные булевы функции изучались в 40–50-х гг. двадцатого века. Применение разложимости в бесповторную декомпозицию было показано К. Шенноном. А. В. Кузнецов показал единственность бесповторного представления булевых функций над множеством неразделимых функций. Различные классы бесповторных функций используются в таких задачах дискретной математики и вычислительной техники, как синтез схем, позиционные игры, машинное обучение и построение вероятностных баз данных. Схемы, построенные на основе бесповторных функций, легко верифицируются.

Повторная в базисе $B$ функция называется слабоповторной, если все ее собственные подфункции бесповторны в $B$. Свойство слабоповторности лежит в основе многоярусной структуры классов базисов, эквивалентных по сложности формульного представления (задача поставлена О. Б. Лупановым, корректность сведения данной задачи к поиску слабоповторных функций обоснована Д. Ю. Черухиным). Базисы, эквивалентные элементарному по сложности, называют базисами нулевого яруса. Базисом $k$-го яруса ($k > 0$) называется базис, расширяющий какой-то из базисов $(k-1)$-го уровня и имеющий меньшую сложность формульного представления булевых функций в данном базисе. В.А. Стеценко были описаны базисы первого яруса и все семейства слабоповторных в $B_0$ функций. Базисы первого яруса также называются предэлементарными. Функции, слабоповторные в предэлементарных базисах, описаны в работах Н. А. Перязева, К. Д. Кириченко, И. К. Шаранхаева.

В работах С. В. Яблонского и И. А. Чегис был описан сформированный в середине 50-х годов тестовый подход к теории контроля управляющих систем, обобщающий задачи проверки и диагностики. Различные задачи схемного тестирования исследовались такими учеными, как С. Д. Вейс, В. Н. Носков, Г. Р. Погосян, С. М. Редди, Н. П. Редькин, Д. С. Романов, К. А. Попков, Е. В. Дуброва, Дж. К. Мьюзио, Н. А Соловьев, В. Б. Кудрявцев, Э. Э. Гасанов, О. А. Долотова.

А. А. Вороненко была поставлена невыроженная задача проверяющего тестирования – задача тестирования бесповторных функций, существенно зависящих от всех своих переменных. Данная задача называется задачей тестирования относительно *бесповторной альтернативы*. Д. В. Чистиковым установлено, что в элементарном базисе функция Шеннона длины теста относительно бесповторной альтернативы не превышает $2n + 1$. Таким образом, в базисах нулевого яруса тестирование относительно бесповторной альтернативы имеет линейную сложность. В диссертации Д. В. Чистикова исследуются задачи проверяющего и диагностического тестирования в различных базисах.

В теории бесповторных функций важной задачей является получение критериев бесповторности или повторности функций. Разными авторами были получены критерии бесповторности булевых функций в элементарном базисе (Б. А. Субботовская, А. П.Гурвич, А. А. Вороненко). В качестве функционала сложности часто рассматривается функция Шеннона для длины сертификата повторности – функция максимума длины минимального сертификата повторности функции. В англоязычной литературе для задач распознавания свойств булевых функций используется термин *exact learning* (*“точное обучение”*). Различными задачам расшифровки и распознавания эквивалетности классов булевых функций занимались такие ученые, как Ж. Ансель, Д. Англуин, Л. Хеллерштайн, М. Карпински, Н. Бшути, Т. Хэнкок, Н. Литтлстоун, Р. Уехара, К. Цучида, И. Вегенер, В.В. Осокин, А. Блюм.

Задача поиска сертификата, показывающего, что функция не принадлежит к некоторому классу, изучается больше двух десятков лет. Л. Хеллерштейн ввел так называемые *“полиномиальные сертификаты”* для оценки обучаемости в стандартной модели точного обучения. М. Эриас, Р. Хардон и Р.А. Серведио исследовали длины полиномиальных сертификатов для таких классов булевых функций, как монотонные КНФ, КНФ Хорна и поляризуемых КНФ. Е. В. Морозовым фактически получено, что функция Шеннона для длины сертификата существенности асимптотически равна $2n$.

Задачей поиска сертификата повторности называется задача поиска множества $n$-мерных булевых наборов значений переменных повторной в базисе $B$ функции $f(x_1, \ldots, x_n)$, такого, что для любой бесповторной в $B$ функции $h(x_1, \ldots, x_n)$ в этом множестве существует набор, на котором $f$ отличается от $h$. А.А. Вороненко, В.С. Федоровой и Д.С. Чистиковым установлено, что длина минимального сертификата повторности в базисах нулевого яруса ограничена сверху константой 6, а также доказано, что функция Шеннона для длины сертификата повторности в базисе, полученном расширением элементарного слабоповторной функцией семейства $f_t^s$ есть величина $\Omega(n^{s-1})$, и для базиса всех функций двух переменных справедлива верхняя оценка $3n + 1$. Для предэлементарного базиса, полученного из $B_0$ добавлением *дискриминирующей функции* – слабоповторной функции Стеценко семейства $f_d^s$, А. А. Вороненко получена верхняя оценка $n + 2$ функции Шеннона для длины сертификата повторности, а также с помощью метода разнозначных матриц получена нижняя оценка $\frac{n}{s}+1$. Далее при рассмотрении задачи поиска минимального сертификата повторности под *сложностью доказательства повторности* функции будем понимать порядок длины минимального сертификата повторности.

**Цели и задачи.** Целями данной работы являются:

1. Исследование сложности доказательства повторности булевых функций в предэлементарных базисах.
2. Исследование сложности тестирования булевых функций в элементарном базисе, расширенном монотонными слабопоторными функциями.

Задачами данной работы являются:

1. Получение новых оценок функций Шеннона для длины сертификата повторности в предэлементарных базисах.
2. Получение новых оценок функций Шеннона для длины теста относительно бесповторной альтернативы в элементарном базисе, расширенном монотонными слабопоторными функциями.

**Научная новизна.** Основные результаты являются новыми и состоят в следующем:

1. Улучшена нижняя линейная оценка функции Шеннона для длины сертификата повторности в элементарном базисе, расширенном слабоповторной функцией $f_d^s$.
2. Получены нетривиальные нижние растущие оценки функции Шеннона для длины сертификата повторности в элементарном базисе, расширенном монотонными слабоповторными функциями.
3. Получена новая верхняя полиномиальная оценка функции Шеннона для длины сертификата повторности в базисе всех функций $l$ переменных.
4. Доказана линейность с константой 3 функции Шеннона для длины теста относительно бесповторной альтернативы в элементарном базисе, расширенном всеми монотонными слабоповторными функциями.

**Практическая значимость.** Диссертация носит теоретический характер. Полученные результаты могут применяться в дальнейших исследованиях теории бесповторных функций и теории надежности (тестирования). Доказанные в диссертации утверждения могут включаться в спецкурсы, читаемые студентам и аспирантам математических специальностей.

**Методология и методы исследования.** В диссертации применяются методы дискретной математики и математической кибернетики. В работе используется аппарат алгебры логики, комбинаторики и теории графов.

**Основные положения, выносимые на защиту.** На защиту выносятся следующие основные результаты:

1. Нижняя оценка функции Шеннона для длины сертификата повторности в элементарном базисе, расширенном слабоповторной функцией $f_d^s$.

2. Нижние оценки функции Шеннона для длины сертификата повторности в элементарном базисе, расширенном монотонными слабоповторными функциями.
3. Верхняя полиномиальная оценка функции Шеннона для длины сертификата повторности в базисе всех функций $l$ переменных.
4. Верхние оценки функции Шеннона для длины теста относительно бесповторной альтернативы в элементарном базисе, расширенном монотонными слабоповторными функциями.

**Достоверность.** Достоверность полученных результатов базируется на применении математических методов дискретной математики и математической кибернетики и обеспечивается строгим применением используемого математического аппарата.

**Апробация работы.** Результаты работы докладывались на XIII Международном семинаре “Дискретная математика и ее приложения”имени академика О.Б. Лупанова (Москва, 2019), на 13-м Межвузовском научно-практическом семинаре “Комбинаторные конфигурации и их приложения”(Кировоград, Украина, 2012), на конференции “Проблемы теоретической кибернетики”, а также на научном семинаре кафедры математической кибернетики факультета вычислительной математики и кибернетики МГУ им. М.В. Ломоносова.

**Публикации и личный вклад автора.** Результаты диссертации опубликованы в 10 печатных изданиях, 3 – опубликованы в изданиях, входящих в международную научную базу цитирования Scopus, 1 – в журналах из научной базы РИНЦ, 3 в журналах, рекомендованных ВАК, 3 – в тезисах докладов. Из них 5 работ [1—5] – в научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 01.01.09 – дискретная математика и математическая кибернетика. В совместных работах [1; 5] основные результаты получены лично соискателем, научному руководителю А.А. Вороненко принадлежат постановка задачи в работе [1] и идея упрощения доказательства в работе [5].

**Структура и объем диссертации.** Диссертация состоит из введения, трех глав, заключения, двух приложений и списка литературы. Полный объем диссертации составляет 102 страницы, список литературы содержит 84 наименования.

## Содержание работы

Во **введении** обосновывается актуальность данной работы, представлен обзор литературы по теме исследования, указаны цели и задачи работы, научная новизна диссертации, теоретическая и практическая значимость работы, методы диссертационного исследования, основные результаты и структура работы. Также представлены степень достоверности, апробация результатов работ и публикации по теме диссертации.

**В первой главе** определяются базовые понятия и обозначения, а также некоторые вспомогательные утверждения, используемые далее в работе. Все логарифмы, используемые далее, будем считать двоичными.

Назовем (0,1)-матрицу *разнозначной*, если все ее строки различны, и она не имеет ни нулевых, ни единичных строк. Будем говорить, что функция $f(x_1,\ldots,x_n)$ моделирует разнозначную матрицу $M$ размерности $k \times n$, если $f(0,\ldots,0) = f(1,\ldots,1) = 1$ и $f(\alpha_1,\ldots,\alpha_n) = 0$ для любой строки $\{\alpha_1,\ldots,\alpha_n\}$ матрицы $M$.

Повторная в базисе $B$ функция называется *слабоповторной*, если любая ее собственная подфункция бесповторна в этом базисе. В.А.Стеценко получил все слабоповторные функции в элементарном базисе $B_0 = \{\&, \vee, \neg\}$. С точностью до преобразований обобщенной однотипности они образуют следующие пять семейств:

$$
\begin{aligned}
f_d^s &= x_1(\bar{x}_2 \vee x_3x_4\ldots x_s) \vee \bar{x}_2\bar{x}_3\ldots\bar{x}_s, && s \geqslant 3,\\
f_t^s &= x_1x_2\ldots x_s \vee \bar{x}_1\bar{x}_2\ldots\bar{x}_s, && s \geqslant 2,\\
f_m^s &= x_1(x_2 \vee \cdots \vee x_s) \vee x_2x_3\ldots x_s, && s \geqslant 3,\\
f_4 &= x_1(x_2 \vee x_3) \vee x_3x_4,\\
f_5 &= x_1(x_2 \vee x_3x_4) \vee x_5(x_2x_3 \vee x_4).
\end{aligned}
$$

Будем называть *специальными* функции $f_4, f_5$ и $f_m^s$. Обозначим используемые в работе базисы $B_4 = \{\vee,\&,\neg, f_4\}$, $B_5 = \{\vee,\&,\neg, f_5\}$, $B_m^s = \{\vee,\&,\neg, f_m^s\}$, где $s \geqslant 3$, $B_d^s = \{\&,\vee,\neg, f_d^s\}$, где $s \geqslant 3$, $B_t^s = \{\&,\vee,\neg, f_t^s\}$, где $s \geqslant 3$, $B_{unate} = \{\vee,\&,\neg\} \cup \{f_4, f_5\} \cup \bigcup\limits_{s=3}^{\infty}\{f_m^s\}$, а $B_{unate}^+$ – базис $B_{unate}$ без отрицания, $B^l$ – базис, состоящий из всех функций $l$ переменных.

Множество $n$-мерных булевых наборов $T$ назовем *проверяющим тестом* функции $f(x_1,\ldots,x_n)$ в базисе $B$, если для любой отличной от $f$ бесповторной в базисе $B$ функции $h(x_1,\ldots,x_n)$ существует набор $(\alpha_1,\ldots,\alpha_n) \in T$, такой, что $f(\alpha_1,\ldots,\alpha_n) \neq h(\alpha_1,\ldots,\alpha_n)$. Пусть функция $f(x_1,\ldots,x_n)$ существенно зависит от всех своих переменных. Тогда проверяющий тест на множестве всех бесповторных в $B$ функций, зависящих от переменных $\{x_1,\ldots,x_n\}$ произвольным образом, называется *тестом относительно бесповторной альтернативы*. Функцией Шеннона длины теста относительно бесповторной альтернативы в базисе $B$ называется функция максимума длин тестов минимальной длины среди всех бесповторных функций, зависящих от $n$ переменных.

Обозначим $T_{unate}(n)$ функцию Шеннона для длины теста относительно бесповторной альтернативы в базисе $B_{unate}$, и $T_{unate}^+(n)$ – функцию Шеннона для длины проверяющего теста в базисе $B_{unate}^+$.

Множество $n$-мерных булевых наборов $S$ назовем *сертификатом повторности* функции $f(x_1,\ldots,x_n)$ в базисе $B$, если для любой бесповторной в базисе $B$ функции $h(x_1,\ldots,x_n)$ существует набор $(\alpha_1,\ldots,\alpha_n) \in S$, такой, что $f(\alpha_1,\ldots,\alpha_n) \neq h(\alpha_1,\ldots,\alpha_n)$. Функцией Шеннона длины сертификата повторности функций в базисе $B$ называется функция максимума длин сертификатов повторности минимальной длины среди повторных в $B$ функций $n$ переменных.

Функции Шеннона для длины сертификата повторности для рассматриваемых базисов будем обозначать: $S_4(n)$ – в базисе $B_4$, $S_5(n)$ – в базисе $B_5$, $S^s_m(n)$ – в базисе $B^s_m$, $S^s_d(n)$ – в базисе $B^s_d$, $S^s_t(n)$ – в базисе $B^s_m$, $S^l(n)$ – в базисе $B^l$.

**Во второй главе** исследуется сложность доказательства повторности булевых функций для предэлементарных базисов, полученных расширением элементарного базиса слабоповторными функциями из следующих семейств Стеценко – $f_4, f_5, f^s_m$ и $f^s_d$, а также для базиса, содержащего все функции $l$ переменных.

В § 2.1 сложность доказательства повторности исследуется для элементарного базиса с дискриминирующей функции. Целью параграфа является получение нетривиальной нижней оценки функции Шеннона для длины сертификата повторности в данном базисе. В § 2.1 излагаются результаты, опубликованные в работе [5] и основанные на предложенном А.А. Вороненко методе разнозначных матриц.

**Лемма 2.1.** *Для любой разнозначной матрицы $M$ с $n > 2s-4$ столбцами и $k < \frac{n}{2}-s+1$ строками всегда найдется бесповторная в $B^s_d$ функция, моделирующая эту матрицу и равная единице на нулевом и единичном наборах.*

**Лемма 2.2.** *Пусть $n > 2s-4$ и $k < \frac{n}{2}-s+3$. Тогда для произвольных $k$ наборов значений переменных функции $f^n_t(x_1, \ldots, x_n)$ существует бесповторная в $B^s_d$ функция $g(x_1, \ldots, x_n)$, совпадающая с $f^n_t$ на этих наборах.*

**Теорема 2.1.** *При $n > 2s - 4$ верно:*

$$S^s_d(n) \geqslant \frac{n}{2} - s + 3.$$

В § 2.2 настоящей работы сложность доказательства повторности исследуется для предэлементарных базисов, состоящих из конъюнкции, дизъюнкции, отрицания и монотонной функции Стеценко – функции, принадлежащей одному из семейств $f_4, f_5$ или $f^s_m$. Целью параграфа является получение нетривиальных растущих нижних оценок функции Шеннона для длины сертификата повторности в данных базисах. Эти оценки получаются из оценок длины сертификата повторности для функции $f^n_m$ в данных базисах. Установлено, что при $n \to \infty$ длина сертификата повторности для функции $f^n_m$ не ограничена константой и не превосходит $2n$.

**Теорема 2.2.** *При $n \geqslant 4$ выполняется условие $S_4(n) \geqslant \log(n-1)$, при $n \geqslant 5$ выполняется $S_5(n) \geqslant \log(n-1) - \log 3 + 1$, а также при $n > s$ выполняется $S^s_m(n) \geqslant \log(n-1) + 1$.*

**Теорема 2.3.** *Базис $B_0$ является единственным базисом, содержащим как нелинейные, так и немонотонные функции, в котором длина сертификата повторности ограничена сверху константой.*

**Теорема 2.4.** *Пусть $S(n)$ – функция Шеннона для длины сертификата повторности в некотором базисе, содержащем вдобавок к $B_0$ произвольную слабоповторную функцию. Тогда, начиная с некоторого $n$, справедливо неравенство*:

$$S(n) \geqslant \log(n-1).$$

В § 2.3 сложность доказательства повторности исследуется для базиса всех функций $l$ переменных и излагаются результаты работы [1].

**Утверждение 1.** *Функция Шеннона длины сертификата повторности функции $n$ переменных в базисе $B^l$ есть величина $\Omega(n^{l-1})$.*

**Лемма 2.9.** *Пусть функция $g(y_1,\ldots,y_m,x)$ бесповторна в $B^l$. Пусть $g(y_1,\ldots,y_m,\sigma) = y_1 \vee \ldots \vee y_m$, где $\sigma$ – некоторая константа. Пусть функция $g$ имеет вид $\phi_0 \vee f(\phi_1,\ldots,\phi_k,x)$, где $\phi_i$ – дизъюнкции различных переменных $y_1,\ldots,y_m$, и $f$ – некоторая бесповторная в $B^l$ функция. Тогда функция $g$ однозначно восстанавливается по значениям на $C_m^k \cdot 2^k$ наборах.*

**Лемма 2.10.** *Пусть функция $g(y_1,\ldots,y_m,x)$ бесповторна в $B^l$. Пусть $g(y_1,\ldots,y_m,\sigma) = y_1\&\ldots\&y_m$, где $\sigma$ – некоторая константа. Пусть $g$ имеет вид $\phi_0\&f(\phi_1,\ldots,\phi_k,x)$, где $\phi_i$ – конъюнкции различных переменных $y_1,\ldots,y_m$. Тогда $g$ однозначно восстанавливается по значениям на $C_m^k \cdot 2^k$ наборах.*

**Лемма 2.11.** *Пусть функция $g(y_1,\ldots,y_m,x)$ бесповторна в $B^l$. Пусть $g(y_1,\ldots,y_m,\sigma) = y_1 \oplus \ldots \oplus y_m$, где $\sigma$ – некоторая константа. Пусть $g$ имеет вид $\phi_0 \oplus f(\phi_1,\ldots,\phi_k,x)$, где $\phi_i$ – суммы по модулю два различных переменных $y_1,\ldots,y_m$. Тогда $g$ однозначно восстанавливается по значениям на $C_m^k \cdot 2^k$ наборах.*

**Теорема 2.5.**

$$S^l(n) = O(n^l).$$

**В третьей главе** рассматривается задача проверяющего тестирования в элементарном базисе, расширенном монотонными функциями Стеценко – базисами, содержащими вдобавок к элементарному только одну монотонную функцию Стеценко семейства $f_4, f_5$ или $f_m^s$ или все такие функции сразу.

В § 3.1 приведено представление бесповторных функций деревьями. Установлен вид канонических деревьев, единственных для функций, бесповторных в рассматриваемых в главе базисах.

В § 3.2 показано, что функция $n$ переменных, бесповторная в рассматриваемых в главе базисах, восстанавливается из подфункции, существенно зависящей от $n-1$ переменных, за константное число наборов.

**Лемма 3.1.** *Пусть бесповторная в базисе* $B^+_{unate}$ *функция* $h(z_1, z_2, z_{k+2}, \dots, z_n)$ *существенно зависит от* $n - k + 1 \geqslant 2$ *переменных* ($k \geqslant 2$), *и лист, который помечен переменной* $z_1$, *смежен с вершиной* $u$, *помеченной конъюнкцией или специальной функцией, а лист, помеченный* $z_2$, *лежит в каком-то другом поддереве над* $u$. *Пусть* $f(x_1, \dots, x_n) = h(x_1 \vee \dots \vee x_k, x_{k+1}, \dots, x_n)$. *Пусть* $h(z_1, z_2, \beta_{k+2}, \dots, \beta_n) = z_1 \& z_2$. *Пусть* $f'(x_1, \dots, x_n)$ – *бесповторная в* $B^+_{unate}$ *функция, такая, что* $f'_{x_k=0} = f|_{x_k=0}$. *Тогда, если выполнено равенство*:

$$f'(x_1, \dots, x_{k+1}, \beta_{k+2}, \dots, \beta_n) = (x_1 \vee \dots \vee x_k) \& x_{k+1},$$

*то* $f' = f$.

**Лемма 3.2.** *Пусть бесповторная в* $B^+_{unate}$ *функция* $h(z_1, z_{s+1}, \dots, z_n)$ *существенно зависит от* $n - s + 1 \geqslant 2$ *переменных, где* $s \geqslant 3$, *и лист, который помечен переменной* $z_1$, *входит в вершину* $u$, *помеченную дизъюнкцией или специальной функцией. Пусть* $f(x_1, \dots, x_n) = h(g(x_1, \dots, x_s), x_{s+1}, \dots, x_n)$, *где* $g$ – *специальная функция* $s$ *переменных. Пусть* $h(z_1, \beta_{s+1}, \dots, \beta_n) = z_1$. *Пусть* $f'(x_1, \dots, x_n)$ – *бесповторная в B функция, такая, что* $f'_{x_1=0} = f|_{x_1=0}$. *Тогда, если выполнено равенство*:

$$f'(x_1, \dots, x_s, \beta_{s+1}, \dots, \beta_n) = g(x_1, \dots, x_s),$$

*то* $f' = f$.

В § 3.3 исследуются функции Шеннона для длины теста относительно бесповторной альтернативы в элементарном базисе, расширенном монотонными слабоповторными функциями, и устанавливается связь тестов относительно бесповторной альтернативы в таких базисах с проверяющими тестами в соответствующих базисах без отрицания. Также показано, что добавление в элементарный базис любого множества монотонных функций Стеценко оставляет функцию Шеннона линейной с мультипликативной константой 3.

**Лемма 3.3.** *Справедливо неравенство*

$$T_{unate}(n) \leqslant T^+_{unate}(n) + 2n.$$

**Теорема 3.1.** *Справедливо неравенство*

$$T^+_{unate}(n) \leqslant 3n - 4 \text{ при } n \geqslant 2.$$

**Теорема 3.2.** *Справедливо неравенство*

$$T_{unate}(n) \leqslant 3n - 2 \text{ при } n \geqslant 2.$$

В приложении А приводятся используемые при доказательствах таблицы. В приложении Б описываются процедуры разбиения разнозначных матриц, используемые в § 2.1.

В **заключении** приведены основные результаты работы, которые заключаются в следующем:

1. Получены новые оценки функции Шеннона для длины сертификата повторности для предэлементарных базисов, полученных расширением элементарного базиса слабоповторными функциями $f_4, f_5, f_m^s$ и $f_d^s$, а также для базиса, содержащего все функции $l$ переменных. Показано, что добавление в элементарный базис любой слабоповторной функции приводит к существенному увеличению длины сертификата повторности.
2. Улучшена нижняя оценка функции Шеннона для длины сертификата повторности в элементарном базисе, расширенном дискриминирующей функцией. Получены нижние растущие оценки и верхние линейные оценки Шеннона для длины сертификата повторности в элементарном базисе, расширенном монотонными функциями Стеценко.
3. Получены верхняя и нижняя полиномиальные оценки функции Шеннона для длины сертификата повторности в базисе всех функций $l$ переменных.
4. Установлено, что добавление в элементарный базис всех монотонных функций Стеценко оставляет линейной верхнюю оценку функции Шеннона для длины теста относительно бесповторной альтернативы с мультипликативной константой 3. Установлено отсутствие существенной связи между арностью функции в базисе и длиной теста.

Представляет интерес дальнейшее исследование вопроса об изменении сложности доказательства повторности при расширении базиса повторными в нем функциями. При наличии нижних логарифмических и верхних линейных оценок остается открытым вопрос о наличии нижних линейных или верхних логарифмических оценок функции Шеннона в предэлементарных базисах, содержащих вдобавок к элементарному некоторую слабоповторную функцию. Применив теорему Хегедуса к результатам главы 2, можно получить новые оценки сложности в классической модели обучения – обучения с помощью запросов принадлежности и эквивалентности. Остается не решенным вопрос о длине минимального теста относительно бесповторной альтернативы при расширении элементарного базиса дискриминирующей функцией. Кроме этого, интересен вопрос о возможности нелинейного роста длины теста относительно бесповторной альтернативы при добавлении иных монотонных функций.

## Публикации автора по теме диссертации

### В изданиях, входящих в международную базу цитирования Scopus


1. *Вороненко А. А.*, *Кафтан Д. В.* О длине сертификата повторности в базисе всех функций $l$ переменных // Прикладная математика и информатика. Вып. 44. — 2013. — 95—102. Пер. на англ. яз.: Voronenko A.A., Kaftan D.V. The length of a read-many certificate in the basis of all functions of $l$ variables

// Computational Mathematics and Modeling. — 2014. — **25**. — N 4. — P. 576—582. (Импакт-фактор Scopus: 0.226).

2. *Кафтан Д. В.* О длине сертификата повторности в некоторых расширенных элементарных базисах // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. — 2015. — № 2. — 40–46. (Импакт-фактор РИНЦ: 0.385) Пер. на англ. яз.: Kaftan D.V. On the length of a read-many certificate in certain extended elementary bases // Moscow University. Comput. Math. and Cybern. — 2015. — **39**. — N 2. — P. 88—95. (Импакт-фактор Scopus: 0.151).
3. *Кафтан Д. В.* Тестирование бесповторных функций в расширенном медианой элементарном базисе // Прикладная математика и информатика. Вып. 66. — 2021. — 104–110. Пер. на англ. яз.: Kaftan D.V. Testing read-once functions in a median-augmented element basis // Computational Mathematics and Modeling. — 2021. — **39**. — N 32. — P. 253—257. (Импакт-фактор Scopus: 0.226).

**В изданиях, входящих в научную базу РИНЦ**

4. *Кафтан Д. В.* Тестирование бесповторных функций в некоторых расширенных элементарных базисах // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. — 2021. — № 3. — 13–19. (Импакт-фактор РИНЦ: 0.340) Пер. на англ. яз.: Kaftan D.V. Testing on read-once functions in extended elementary bases // Moscow University. Comput. Math. and Cybern. — 2021. — **45**. — N 3. — P. 96—102.

**В изданиях из списка ВАК РФ**

5. *Кафтан Д. В.* О нижней оценке функции Шеннона для длины сертификата повторности булевых функций в одном семействе базисов // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2015. — № 1. — С. 69—78.
6. *Вороненко А. А.*, *Кафтан Д. В.* Тестирование бесповторных функций в элементарном базисе, расширенном всеми поляризуемыми слабоповторными функциями // Интеллектуальные системы. Теория и приложения. — 2021. — Т. 25, № 3. — С. 75—82.
7. *Кафтан Д. В.* Древесное представление бесповторных функций в расширенных элементарных базисах // Известия высших учебных заведений. Поволжский регион. Физико-математические наук. — 2017. — Т. 3, № 43. — С. 37—49.

**В сборниках трудов конференций**

8. *Вороненко А. А.*, *Кафтан Д. В.* О длине доказательства повторности в некоторых базисах // Дискретная математика и ее использование в экономико-математическом моделировании и информационных технологиях. Сборник тезисов. — Запорожье, Украина: Изд–во КНТУ, 2012. — С. 18—19.

9. *Вороненко А. А.*, *Кафтан Д. В.* Тестирование поляризуемых функций // Материалы XIII Международного семинара “Дискретная математика и ее приложения”имени академика О.Б. ЛУПАНОВА. Т. 1. — М.: Изд-во механико-математического факультета МГУ, 2019. — С. 119—121.
10. *Вороненко А. А.*, *Кафтан Д. В.* Тестирование бесповторных функций в поляризуемых предэлементарных базисах // Материалы семинара конференции “Проблемы теоретической кибернетики”. — Казань: Отечество, 2021. — С. 29—31.