

Московский государственный университет имени М. В. Ломоносова
Факультет вычислительной математики и кибернетики

На правах рукописи

УДК 519.718.7

Кафтан Дарья Владимировна

Оценки длины тестов и сертификатов для бесповторных функций

01.01.09 – дискретная математика и математическая кибернетика

ДИССЕРТАЦИЯ

на соискание ученой степени

кандидата физико-математических наук

Научный руководитель

проф., д. ф.-м. н.

Вороненко Андрей Анатольевич

Москва – 2021

Оглавление

Введение	4
Глава 1. Терминология и обозначения	18
§ 1.1. Булевы функции и их свойства	18
§ 1.2. Тесты и сертификаты	22
Глава 2. Оценки длины сертификатов повторности . .	25
§ 2.1. Сертификаты повторности в базисе с дискриминирующей функцией	25
§ 2.2. Сертификаты повторности в базисах с монотонными функциями Стеценко	33
§ 2.3. Сертификаты повторности в базисе всех функций l переменных	51
Глава 3. Проверяющие тесты для функций, неповторных в элементарном базисе, расширенном монотонными функциями Стеценко	60
§ 3.1. Представление неповторных функций в виде корневых деревьев	62
§ 3.2. Леммы о восстановлении неповторных функций . . .	64
§ 3.3. Верхние оценки длины тестов	76
Заключение	80

Приложение А. Таблицы	82
Приложение Б. Процедуры	84
Список литературы	90

Введение

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 [77]. Первые неповторные булевы функции изучались в 40–50-х гг. двадцатого века. Применение разложимости в неповторную декомпозицию было показано К. Шенноном [81]. А. В. Кузнецов [29] показал единственность неповторного представления булевых функций над множеством неразделимых функций. Различные классы неповторных функций используются в таких задачах дискретной математики и вычислительной техники, как синтез схем [52], позиционные игры [73,

20], машинное обучение [64, 68, 83] и построение вероятностных баз данных [79]. Схемы, построенные на основе бесповторных функций, легко верифицируются [9].

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 в работе [52], корректность сведения данной задачи к поиску слабоповторных функций обоснована Д. Ю. Черухиным [55]). 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 [50, 51]. Базисы первого яруса также называются предэлементарными. Функции, слабоповторные в предэлементарных базисах, описаны в работах [38, 27, 59, 60, 61].

В работах С. В. Яблонского и И. А. Чегис [53, 54] был описан сформированный в середине 50-х гг. тестовый подход к теории контроля управляющих систем, обобщающий задачи проверки и диагностики. В работе С. Д. Вейса [84] был установлен линейный порядок роста функции Шеннона для длины полного проверяющего те-

ста при константных неисправностях на входах схем. В работе В. Н. Носкова [37] была получена точная оценка данной функции. Г. Р. Погосян в работе [39] распространил этот результат на k -значный случай. Работа [78] С. М. Редди посвящена моделированию произвольных булевых функций схемой с одним дополнительным выходом в базисе Жегалкина, допускающей не зависящий от заданной функции единичный проверяющий тест длины не более $n+4$ относительно константных неисправностей на входах и выходах элементов. Н. П. Редькин в работе [45] доказал верхнюю оценку 3 функции Шеннона длины единичного проверяющего теста относительно инверсных неисправностей на выходах элементов в произвольном полном базисе. Д. С. Романовым в работе [47] доказаны константные нижняя и верхняя оценка функции Шеннона длины полного проверяющего теста относительно произвольных константных неисправностей на выходах элементов в специальном конечном полном базисе. Д. С. Романовым в работе [48] доказана константная верхняя оценка функции Шеннона длины единичного проверяющего теста относительно произвольных константных неисправностей на входах и выходах элементов в базисе Жегалкина. Работа К. А. Попкова [41] посвящена построению легкотестируемых схем при произвольных константных неисправностях на входах и выходах элементов. Работа [71] Е. В. Дубровой и Дж. К. Мьюзио посвящена задаче построения тестов для k -значных схем из функциональных элементов для простых $k > 2$ с

помощью моделирования полиномов. Попков К. А. в работе [40] рассматривает задачу поиска полных диагностических тестов для схем при инверсных неисправностях функциональных элементов, а в работе [42] получены оценки функции Шеннона длины теста относительно неисправности замыкания для контактных схем. Обзоры различных задач тестирования можно найти в монографиях [44, 49, 62, 28], диссертации Д. С. Романова [46] и К. А. Попкова [43].

В работе [2] А. А. Вороненко была поставлена невырожденная задача проверяющего тестирования — задача тестирования неповторных функций, существенно зависящих от всех своих переменных. Данная задача называется задачей тестирования относительно *бесповторной альтернативы*. Д. В. Чистиковым [57] 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 [56] исследуются задачи проверяющего и диагностического тестирования в различных базисах.

В теории неповторных функций важной задачей является получение критериев неповторности или повторности функций. Разными авторами были получены критерии неповторности (Б. А. Субботовская [52], А. П. Гурвич [18, 19], А. А. Вороненко [15, 4]) булевых функций в элементарном базисе. С обзором результатов по ис-

следованию критериев неповторности можно ознакомиться в монографии [21]. В качестве функционала сложности часто рассматривается функция Шеннона [80] 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”) [63]. В работе [72] предложена мера сложности обучения, совпадающая с функцией Шеннона для длины проверяющего теста. Ж. Анселем [74], в частности, было получено точное значение сложности расшифровки монотонных булевых функций. В работах Д. Англуин, Л. Хеллерштайн и М. Карпински [64], Н. Бшути, Т. Хэнкока и Л. Хеллерштайн [68] исследуются задачи расшифровки и распознавания эквивалентности булевых функций в различных базисах. Уехара Р., Цучида К., И. Вегенер [82] и Осокин В.В. [35, 36] занимались исследованием расшифровки и распознавания эквивалентности других классов булевых функций. В работах Морозова Е.В. [32, 33] исследуются тесты относительно слияний переменных в булевых функциях. А. Блюм, Л. Хеллерштайн и Н. Литтлстоун в работе [66] провели сравнение различных моделей расшифровки функций. В работе Н. Бшути [67] приведен обзор современного состояния тематики точного обучения.

Задача поиска сертификата, показывающего, что функция не принадлежит к некоторому классу, изучается больше двух десятков

лет. Л. Хеллерштейн в работе [76] ввел так называемые “*полиномиальные сертификаты*” для оценки обучаемости в стандартной модели точного обучения [63]. М. Эриас, Р. Хардон и Р.А. Серведио в работе [65] исследовали длины полиномиальных сертификатов для таких классов булевых функций, как монотонные КНФ, КНФ Хорна и поляризуемых КНФ. В работе [34] 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 $f(x_1, \dots, x_n)$, такого, что для любой бесповторной в B функции $h(x_1, \dots, x_n)$ в этом множестве существует набор, на котором f отличается от h . В работе [70], в частности, было показано, что длина минимального сертификата повторности в базисах нулевого яруса ограничена сверху константой. Для предэлементарного базиса, полученного из B_0 добавлением *дискриминирующей функции* — слабоповторной функции Стеценко семейства f_d^s , А. А. Вороненко в работе [4] получена верхняя оценка $n + 2$ функции Шеннона для длины сертификата повторности, а также с помощью метода разнозначных матриц [5] получена нижняя оценка $\frac{n}{s} + 1$. В работе [70] рассматривается предэлементарный базис, полученный расширением элементарного слабоповторной функцией семейства f_t^s , и установлено, что функция Шеннона для длины сертификата повтор-

ности в данном базисе есть величина $\Omega(n^{s-1})$, и для базиса всех функций двух переменных справедлива верхняя оценка $3n + 1$. Далее при рассмотрении задачи поиска минимального сертификата повторности под *сложностью доказательства повторности* функции будем понимать порядок длины минимального сертификата повторности.

Цели и задачи диссертации. 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.

В данной работе решаются следующие задачи:

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.

Теоретическая и 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 диссертационного исследования. В диссертации применяются методы дискретной математики и ма-

тематической кибернетики. В работе используется аппарат алгебры логики, комбинаторики и теории графов.

Основные положения, выносимые на защиту, и личный вклад соискателя. 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.

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

Объем и структура работы. Диссертация состоит из введения, трех глав, заключения, двух приложений и списка литературы, включающего 84 наименования. Общий объем диссертации составляет 102 страницы. Нумерация всех теорем и лемм ведется независимо, причем номер каждого такого утверждения состоит из двух частей — номера главы и номера раздела внутри главы. 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 главе 1 определяются базовые понятия и обозначения, а также некоторые вспомогательные утверждения, используемые далее в работе.

В главе 2 исследуется сложность доказательства повторности

булевых функций для предэлементарных базисов, полученных расширением элементарного базиса слабоповторными функциями из следующих семейств Стеценко [51] — f_4, f_5, f_m^s и f_d^s , 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 [24] и основанные на предложенном А. А. Вороненко методе разнозначных матриц [5].

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_m^s . Все указанные в работе логарифмы будем считать двоичными. 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_m^n в данных базисах. Установлено, что при $n \rightarrow \infty$ длина сертификата повторности для функции f_m^n не ограничена константой и не превосходит $2n$. Теорема 2.2 устанавливает нижнюю оценку $\log(n - 1)$ функции Шеннона в элементарном бази-

се, расширенном функцией f_4 , нижнюю оценку $\log(n-1) - \log 3 + 1$ функции Шеннона в элементарном базисе, расширенном функцией f_5 , а также нижнюю оценку $\log(n-1)+1$ функции Шеннона в элементарном базисе, расширенном функцией f_m^s . В теореме 2.3 настоящей работы устанавливается, что элементарный базис — единственный базис, содержащий как немонотонную, так и нелинейную функции, обладающий таким свойством. В теореме 2.4 доказывается, что для любого базиса, содержащего вдобавок к элементарному произвольную слабоповторную функцию, справедлива, начиная с некоторого n , нижняя оценка функции Шеннона для длины сертификата повторности, равная $\log(n-1)$. Также в § 2.2 показана верхняя линейная оценка функции Шеннона сертификата повторности в указанных базисах, равная $2n$.

В § 2.3 сложность доказательства повторности исследуется для базиса всех функций l переменных и излагаются результаты работы [11]. В утверждении 2.11 устанавливается, что минимальный сертификат повторности в базисе всех функций l переменных содержит не меньше $\Omega(n^{l-1})$ наборов. Основным результатом 2.3 является теорема 2.5, в которой показывается, что для доказательства повторности в базисе всех функций l переменных достаточно $O(n^l)$ наборов.

В главе 3 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 неповторных функций деревьями. Установлен вид канонических деревьев, единственных для функций, неповторных в рассматриваемых в главе базисах.

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

В § 3.3 исследуются функции Шеннона для длины теста относительно неповторной альтернативы в элементарном базисе, расширенном монотонными слабоповторными функциями, и устанавливается связь тестов относительно неповторной 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.

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

Публикации. Результаты диссертации опубликованы в 10 работах. Работы [11, 23, 25] опубликованы в изданиях, входящих в международную научную базу цитирования Scopus, работа [26] опубли-

кована в научной базе РИНЦ, работы [13, 22, 24] опубликованы в журналах, входящих в перечень ВАК, работы [10, 12, 14] – тезисы докладов. Из них 5 работ [11, 13, 23, 25, 26] – в научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 01.01.09 – дискретная математика и математическая кибернетика. В совместных работах [13, 11] основные результаты получены лично соискателем, научному руководителю А.А. Вороненко принадлежат постановка задачи в работе [11] и идея упрощения доказательства в работе [13].

Глава 1

Терминология и обозначения

В первой главе определяются некоторые понятия и обозначения, приводятся некоторые вспомогательные утверждения. Без определения используются базовые понятия дискретной математики, которые можно найти в учебниках (см., например, [1]).

§ 1.1. Булевы функции и их свойства

Булева функция $f(x_1, \dots, x_n)$, представляемая (не представляемая) формулой без повторения переменных — *бесповторной формулой* — в некотором базисе, называется *бесповторной (повторной)* в этом базисе.

Преобразованиями обобщенной однотипности называются замена переменной или самой функции на ее отрицание и перестановка переменных. Функции, получаемые друг из друга конечным числом преобразований обобщенной однотипности, называются *обобщенно однотипными*.

Константа α называется *забывающей константой* (не забывающей константой) переменной x_i функции $f(x_1, \dots, x_n)$, существенно зависящей от всех своих переменных, если подфункция $f|_{x_i=\alpha}$ имеет фиктивные переменные (не имеет фиктивных переменных).

Будем считать равными функции, отличающиеся только набором фиктивных переменных.

Верхним нулем монотонной функции называется набор, на котором она равна 0, такой, что на всех больших наборах функция равна 1. *Нижней единицей* монотонной функции называется набор, на котором она равна 1, такой, что на всех меньших наборах функция равна 0.

Функция $f(x_1, \dots, x_n)$ называется *поляризуемой*, если она монотонна или антимонотонна по каждой из переменных, и *неполяризуемой* в противном случае.

Вектором поляризации функции $f(x_1, \dots, x_n)$, существенно зависящей от всех своих переменных, называется набор $(\sigma_1, \dots, \sigma_n)$, где $\sigma_i = 0$, если f антимонотонна по x_i , и $\sigma_i = 1$, если монотонна.

Строку или столбец из одних единиц (нулей), будем называть *единичными* (*нулевыми*). Обозначим через e_i строку с одной единицей в i -й позиции.

Будем называть *наследственными* базисы, которые содержат все подфункции каждой лежащей в них функции. *Конечным* называется базис, содержащий конечное число функций.

Будем называть *формулой с поднятыми отрицаниями* формулу в базисе B , в которой отрицания или отсутствуют, или применяются только к булевым переменным.

Назовем $(0,1)$ -матрицу *разнозначной* [5], если все ее строки раз-

личны, и она не имеет ни нулевых, ни единичных строк.

Будем говорить, что функция $f(x_1, \dots, x_n)$ моделирует разнзначную матрицу M размерности $k \times n$, если $f(0, \dots, 0) = f(1, \dots, 1) = 1$ и $f(\alpha_1, \dots, \alpha_n) = 0$ для любой строки $\{\alpha_1, \dots, \alpha_n\}$ матрицы M .

Будем говорить, что строка имеет *0-преобладание*, если в ней количество нулей больше или равно количеству единиц, в противном случае будем говорить, что строка имеет *1-преобладание*. В строке с 0-преобладанием (1-преобладанием) значение 0 (соответственно 1) будем называть обычным, а значение 1 (соответственно 0) – особым.

Назовем $(0,1)$ -матрицу размерности $k \times n$ *матрицей нулей* (*матрицей единиц*) функции $f(x_1, \dots, x_n)$, если строки матрицы различны и $f(\alpha_1^i, \dots, \alpha_n^i) = 0$ ($f(\alpha_1^i, \dots, \alpha_n^i) = 1$) для всех строк α^i матрицы. Тогда будем говорить, что функция $f(x_1, \dots, x_n)$ *равна нулю* (*единице*) на этой матрице. Две матрицы с равным числом наборов назовем *двойственными*, если они состоят из попарно противоположных наборов. Будем говорить, что функция f *совпадает с двойственной функцией* на матрице M , если на M и двойственной ей матрице она равна противоположным значениям. Заметим, что такая функция не обязательно является самодвойственной.

Повторная в базисе B функция называется *слабоповторной*, если любая ее собственная подфункция бесповторна в этом базисе. В.А.Стеценко [51] получил все слабоповторные функции в элементарном базисе $B_0 = \{\&, \vee, \neg\}$. С точностью до преобразований обоб-

щенной однотипности они образуют следующие пять семейств:

$$f_d^s = x_1(\bar{x}_2 \vee x_3 x_4 \dots x_s) \vee \bar{x}_2 \bar{x}_3 \dots \bar{x}_s, \quad s \geq 3,$$

$$f_t^s = x_1 x_2 \dots x_s \vee \bar{x}_1 \bar{x}_2 \dots \bar{x}_s, \quad s \geq 2,$$

$$f_m^s = x_1(x_2 \vee \dots \vee x_s) \vee x_2 x_3 \dots x_s, \quad s \geq 3,$$

$$f_4 = x_1(x_2 \vee x_3) \vee x_3 x_4,$$

$$f_5 = x_1(x_2 \vee x_3 x_4) \vee x_5(x_2 x_3 \vee x_4).$$

Будем называть *специальными* функции f_4, f_5 и f_m^s . Будем называть функцию f_d^s *дискриминирующей функцией*.

Введем обозначения для следующих базисов:

- $B_4 = \{\vee, \&, \neg, f_4\}$;
- $B_5 = \{\vee, \&, \neg, f_5\}$;
- $B_m^s = \{\vee, \&, \neg, f_m^s\}$, где $s \geq 3$;
- $B_d^s = \{\&, \vee, \neg, f_d^s\}$, где $s \geq 3$;
- $B_t^s = \{\&, \vee, \neg, f_t^s\}$, где $s \geq 3$;
- $B_{unate} = \{\vee, \&, \neg\} \cup \{f_4, f_5\} \cup \bigcup_{s=3}^{\infty} \{f_m^s\}$, а B_{unate}^+ – базис B_{unate} без отрицания;
- B^l – базис, состоящий из всех функций l переменных.

Замечание 1.1. [23] *Функция f_4 совпадает с двойственной ей функцией на наборах*

$$(0000), (0001), (0100), (0101), (0010), (1000)$$

и равна нулю на них.

Функция f_5 совпадает с двойственной ей функцией на наборах

$$(00000), (00001), (00010), (00100), (00101), (00110),$$

$$(01000), (01001), (10100), (01100), (10010), (10000)$$

и равна нулю на них.

§ 1.2. Тесты и сертификаты

Множество n -мерных булевых наборов T назовем *проверяющим тестом* функции $f(x_1, \dots, x_n)$ в базисе B , если для любой отличной от f неповторной в базисе B функции $h(x_1, \dots, x_n)$ существует набор $(\alpha_1, \dots, \alpha_n) \in T$, такой, что $f(\alpha_1, \dots, \alpha_n) \neq h(\alpha_1, \dots, \alpha_n)$. Пусть функция $f(x_1, \dots, x_n)$ существенно зависит от всех своих переменных. Тогда проверяющий тест на множестве всех неповторных в B функций, зависящих от переменных $\{x_1, \dots, x_n\}$ произвольным образом, называется *тестом относительно неповторной альтернативы* [2]. *Длиной теста* назовем количество наборов в нем. Функцией Шеннона [80] длины теста относительно неповторной альтернативы в базисе B называется функция максимума длин тестов мини-

мальной длины среди всех неповторных функций, зависящих от n переменных.

Обозначим $T_{unate}(n)$ функцию Шеннона для длины теста относительно неповторной 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 $f(x_1, \dots, x_n)$ в базисе B , если для любой неповторной в базисе B функции $h(x_1, \dots, x_n)$ существует набор $(\alpha_1, \dots, \alpha_n) \in S$, такой, что $f(\alpha_1, \dots, \alpha_n) \neq h(\alpha_1, \dots, \alpha_n)$. *Длиной сертификата повторности* назовем количество наборов в нем. Функцией Шеннона [80] длины сертификата повторности функций в базисе B называется функция максимума длин сертификатов повторности минимальной длины среди повторных в B функций n переменных.

Введем обозначения функций Шеннона для длины сертификата повторности в некоторых базисах:

- $S_4(n)$ – в базисе B_4 ;
- $S_5(n)$ – в базисе B_5 ;
- $S_m^s(n)$ – в базисе B_m^s ;
- $S_d^s(n)$ – в базисе B_d^s ;
- $S_t^s(n)$ – в базисе B_m^s ;

- $S^l(n)$ – в базисе B^l .

Глава 2

Оценки длины сертификатов повторности

В главе 2 рассматривается задача поиска сертификата повторности в базисах, расширяющих элементарный. Исследуются функции Шеннона для длины сертификата повторности в базисах B_4, B_5, B_m^s и B_d^s , а также базисе, состоящем из всех функций l переменных.

§ 2.1. Сертификаты повторности в базисе с дискриминирующей функцией

В данном разделе будет показана нетривиальная нижняя оценка функции Шеннона для длины сертификата повторности $S_d^s(n) \geq \geq \frac{n}{2} - s + 3$ при $n > 2s - 4$ (см. [24]). Для этого с помощью метода разнозначных матриц покажем, что функцию f_t^n нельзя отличить от всех неповторных в B_d^s функций, равных единице на нулевом и единичном наборах, предъявив менее $\frac{n}{2} - s + 3$ наборов.

В приложении В описаны процедуры, используемые при доказательстве утверждений. При применении данных процедур из множества столбцов матрицы M получается три множества C_1, C_2, C_3 , а из множества всех строк матрицы M — два множества R_1, R_2 . Пусть $x_{i_1}, \dots, x_{i_l}$ — столбцы из C_1 , а $x_{i_{l+1}}, \dots, x_{i_m}$ — столбцы из C_2 .

Обозначим

$$\begin{aligned} g(x_{i_1}, \dots, x_{i_l}, x_{i_{l+1}}, \dots, x_{i_m}, x_1, \dots, x_{s-2}) = \\ = f_d^s(x_{i_1} \& \dots \& x_{i_l}, x_{i_{l+1}} \vee \dots \vee x_{i_m}, x_1, \dots, x_{s-2}). \end{aligned} \quad (2.1)$$

Утверждение 2.1. [24] *Либо множество R_1 совпадает с множеством всех строк матрицы M , либо содержит не менее $s - 2$ строк.*

Доказательство. В процедурах 2 и 3 на шаге 6 множество R_1 приравнивается множеству всех строк матрицы M . Множество всех строк, рассмотренных на шаге 2 процедуры 1, содержится в R_1 . Если на этом шаге закончились строки, то R_1 – множество всех строк матрицы M . Если этот шаг закончился при $|C_3| = s - 2$, то $|R_1| \geq s - 2$, так как за t рассмотренных на этом шаге строк мы добавили не более t столбцов.

Утверждение 2.2. [24] *Функция g , задаваемая равенством (2.1), равна нулю на множестве R_1 .*

Доказательство. Если матрица M содержит только строки с 0-преобладанием, то для любой строки s из R_1 возможны два варианта.

1. Строка s равна нулю на всех столбцах $x_1, \dots, x_{s-2}$. Случай соответствует шагу 3 процедуры 2: в C_2 оказался столбец, в котором строка s равна единице. Следовательно, функция g на этой строке равна нулю.

2. Строка s равна единице на каком-то из столбцов $x_1, \dots, x_{s-2}$.
Случай соответствует шагу 4 процедуры 2: в C_1 оказался столбец, в котором строка s равна нулю. Следовательно, функция g на этой строке равна нулю.

Если матрица M содержит только строки с 1-преобладанием, то для любой строки s из R_1 возможны два варианта.

1. Строка s равна единице на всех столбцах $x_1, \dots, x_{s-2}$. Случай соответствует шагу 3 процедуры 3: в C_1 оказался столбец, в котором строка s равна нулю. Следовательно, функция g равна нулю на этой строке.
2. Строка s равна нулю на каком-то из столбцов $x_1, \dots, x_{s-2}$. Случай соответствует шагу 4 процедуры 3: в C_2 оказался столбец, в котором строка s равна единице. Следовательно, функция g равна нулю на этой строке.

Если матрица M содержит строки обоих видов, то для любой строки s из R_1 возможны три варианта:

1. Строка s имеет 0-преобладание и равна нулю на каком-то столбце из C_1 . Случай соответствует пункту (b) шага 2 процедуры 1 и шагу 4: на одной из позиций $x_1, \dots, x_{s-2}$ есть единица. Следовательно, функция g равна нулю.
2. Строка s имеет 0-преобладание и на каждом столбце из C_1 строка равна единице. Случай соответствует пункту (c) шага

2 процедуры 1: строка s равна нулю на каком-то столбце из $x_1, \dots, x_{s-2}$. На шаге 8 процедуры 1 в C_2 был добавлен столбец с единицей в этой строке. Следовательно, функция g равна нулю на строке s .

3. Строка s имеет 1-преобладание. Случай соответствует шагу 7 процедуры 1: в C_2 был добавлен столбец, который равен единице в этой строке. Согласно случаю (а) на шаге 2 и шагу 4, в этой строке на одной из позиций $x_1, \dots, x_{s-2}$ есть ноль. Следовательно, g равна нулю на строке s .

Утверждение доказано.

Утверждение 2.3. [24] *Функция g , задаваемая равенством (2.1) равна нулю либо на всех строках матрицы M , либо на не менее чем $\frac{|C_1|+|C_2|+s-2}{2}$ строках матрицы M .*

Доказательство. По утверждению 2.1, R_1 либо является множеством всех строк матрицы M , либо $|R_1| \geq s - 2$. В первом случае, согласно утверждению 2.2, функция g равна нулю на всех строках матрицы M .

Пусть R_1 не является множеством всех строк матрицы M . Тогда $|C_1| + |C_2| \leq |R_1|$, так как на шагах 6–8 процедуры 1 для каждой строки из R_1 было взято не более одного столбца. Так как $|R_1| \leq s - 2$, то $|C_1| + |C_2| + s - 2 \leq |R_1| + s - 2 \leq 2|R_1|$. Следовательно, $|R_1| \geq \frac{|C_1|+|C_2|+s-2}{2}$.

Утверждение доказано.

Утверждение 2.4. [24] *Удаление столбцов из множества $C_1 \cup C_2 \cup \{x_1, \dots, x_{s-2}\}$ и строк, на которых функция g , задаваемая равенством (2.1), равна нулю, не приводит к образованию нулевых или единичных строк в матрице M .*

Доказательство. Функция g может быть не равна нулю только на каких-то строках из множества R_2 после применения процедуры 1, так как иначе по утверждению 2.3 множество R_1 – это множество всех строк матрицы M . Рассмотрим любую строку из R_2 . Возможны два варианта.

1. Все ее значения на столбцах $x_1, \dots, x_{s-2}$ – обычные. Тогда множества C_1 и C_2 не пересекаются с C_3 , так как каждый столбец перемещался только один раз из C в одно из этих множеств. На шаге 4 процедуры 1 в C_3 был добавлен столбец с особым значением в этой строке, поэтому строка имеет особое значение на каком-то столбце из C_3 , отличном от $x_1, \dots, x_{s-2}$.
2. Строка имеет особое значение на одном из столбцов $x_1, \dots, x_{s-2}$. Тогда строка так же, как в предыдущем случае, имеет особое значение на каком-то столбце из C_3 , отличном от $x_1, \dots, x_{s-2}$, иначе она оказалась бы в R_1 .

Таким образом, у строки есть столбец с особым значением, не лежащий в $C_1 \cup C_2 \cup \{x_1, \dots, x_{s-2}\}$. Всего удаляется не более по-

ловины столбцов: $n - (s - 2) - |C_1| - |C_2| \geq n - s + 2 - k > \frac{n}{2}$, поэтому существует хотя бы один столбец с обычным значением, не лежащий в $C_1 \cup C_2 \cup \{x_1, \dots, x_{s-2}\}$. Тогда при удалении столбцов $C_1 \cup C_2 \cup \{x_1, \dots, x_{s-2}\}$ в этой строке останется хотя бы одно особое значение и хотя бы одно обычное, т.е. строка будет разнозначной. Таким образом, удаление из матрицы M строк, на которых g равна нулю, не приводит к образованию нулевых или единичных строк. Утверждение доказано.

Из утверждения 2.3 следует

Утверждение 2.5. [24] *Если R_1 – множество всех строк матрицы M , то функция g , задаваемая равенством (2.1), ее моделирует.*

Лемма 2.1. [24] *Для любой разнозначной матрицы M с $n > 2s - 4$ столбцами и $k < \frac{n}{2} - s + 1$ строками всегда найдется неповторная в B_d^s функция, моделирующая эту матрицу и равная единице на нулевом и единичном наборах.*

Доказательство. Базис индукции. Пусть $2s - 4 < n \leq 4s - 8$. Рассмотрим преобладание строк в матрице M .

- Если матрица M имеет как строки с 0-преобладанием, так и строки с 1-преобладанием, то применим к матрице M процедуру 1.

- Если матрица M имеет только строки с 0-преобладанием, то применим к матрице M процедуру 2.
- Если матрица M имеет только строки с 1-преобладанием, то применим к матрице M процедуру 3.

В каждом из трех случаев на выходе процедуры получаем множества C_1, C_2, R_1 . Количество строк в матрице M меньше $s - 2$. Следовательно, R_1 – множество всех строк матрицы, и по утверждению 2.5 функция g , задаваемая равенством (2.1), ее моделирует. Следовательно, g будет искомой функцией. Заметим, что количество переменных функции g не превосходит $2s - 4$, так как $|C_1| + |C_2|$ не превосходит $|R_1|$.

Индуктивный переход. Пусть $n < 4s - 8$, и для всех $n' < n$ (где $n' > 2s - 4$) утверждение леммы выполнено. Применим к матрице M одну из процедур 1–3 в зависимости от преобладания строк. Получим множества C_1, C_2, R_1 и функцию g . Тогда возможны два варианта.

1. R_1 является множеством всех строк матрицы M . Тогда по утверждению 2.5 функция g моделирует матрицу M и является искомой функцией из утверждения леммы.
2. R_1 не является множеством всех строк матрицы M .

Получим матрицу M' из матрицы M удалением всех строк, на которых g равна нулю, столбцов из множеств C_1, C_2 и столб-

цов $x_1, \dots, x_{s-2}$. Уберем дублирующие строки, если таковые имеются. Покажем, что полученная матрица M' удовлетворяет условиям леммы. Действительно, M' имеет $k' = k - |R_1|$ строк и $n' = n - (|C_1| + |C_2| + s - 2)$ столбцов, для которых выполнено:

$$\begin{aligned} k' = k - |R_1| &\leq k - \frac{|C_1| + |C_2| + s - 2}{2} < \\ &< \frac{n}{2} - s + 1 - \frac{|C_1| + |C_2| + s - 2}{2} = \\ &= \frac{n - (|C_1| + |C_2| + s - 2)}{2} - s + 1 < \frac{n'}{2} - s + 1. \end{aligned}$$

Согласно утверждению 2.4, удаление этих столбцов и строк не приводит к образованию нулевых или единичных строк, поэтому полученная матрица разнзначная. Следовательно, по предположению индукции существует неповторная в B_d^s функция $g'(y_1, \dots, y_{n'})$, моделирующая матрицу M' . Тогда функция $g \& g'$ моделирует матрицу M . Действительно, на нулевом и единичном наборах обе функции равны единице, а на всех остальных наборах равна нулю либо g (по утверждению 2.2), либо g' (по предположению индукции). Таким образом, функция $g \& g'$ является искомой. Лемма доказана.

Лемма 2.2. [24] Пусть $n > 2s - 4$ и $k < \frac{n}{2} - s + 3$. Тогда для произвольных k наборов значений переменных функции $f_t^n(x_1, \dots, x_n)$ существует неповторная в B_d^s функция $g(x_1, \dots, x_n)$, совпадающая с f_t^n на этих наборах.

Доказательство. Пусть A – множество из k наборов значений переменных $\{x_1, \dots, x_n\}$. Если среди них нет нулевого или единичного набора, то f_t^n совпадает на A с одной из функций $x_1 \& \dots \& x_n$ или $\bar{x}_1 \& \dots \& \bar{x}_n$. Если A содержит и нулевой, и единичный наборы, то матрица M , составленная из остальных наборов A , является разностной матрицей размера $(k - 2) \times n$, где $k - 2 < \frac{n}{2} - s + 1$, и удовлетворяет условию леммы 2.1. Следовательно, существует неповторная в B_d^s функция $g(x_1, \dots, x_n)$, совпадающая с f_t^n на A . Лемма доказана.

Из леммы 2.2 следует утверждение следующей теоремы.

Теорема 2.1. [24] *При $n > 2s - 4$ верно:*

$$S_d^s(n) \geq \frac{n}{2} - s + 3.$$

§ 2.2. Сертификаты повторности в базисах с монотонными функциями Стеценко

Покажем, что функции Шеннона $S_m^s(n)$, $S_4(n)$ и $S_5(n)$ имеют нижние логарифмические оценки.

Утверждение 2.6. [23] *Если минимальная длина сертификата повторности для функций из семейства f_m^n при $n \rightarrow \infty$ не ограничена сверху константой в базисах B_4 , B_5 и ни в одном из B_m^s , то B_0 – единственный базис, содержащий как немонотонную, так и*

нелинейную функции, в котором минимальная длина сертификата повторности любой функции ограничена сверху константой.

Доказательство. Сертификатом повторности в базисах B_4 , B_5 и B_m^s для неполяризуемых слабоповторных функций являются любые 4 набора, на которых нарушается поляризуемость, так как все функции, неповторные в базисах B_4 , B_5 и B_m^s , поляризуемы. Количество поляризуемых слабоповторных в базисах B_4 , B_5 и B_m^s функций, отличных от функции f_m^n , конечно [59, 60, 61]. Поэтому сертификат повторности у них также ограничен константой. Остается невыясненным вопрос о наличии такой оценки для последовательности функций $\{f_m^n\}$ при $n \rightarrow \infty$. Если ее нет, то ее нет и у соответствующей функции Шеннона.

Любой базис, содержащий B_0 и повторные в B_0 функции, содержит хотя бы одну слабоповторную в B_0 функцию. Функции f_t^s, f_d^s и f_m^s повторны в любом базисе, содержащем функции менее s переменных, в силу их неразложимости. Минимальная длина сертификата повторности функции монотонна по расширению базиса. Таким образом, если одно из этих семейств не имеет константной оценки минимальной длины сертификата повторности при $n \rightarrow \infty$ в базисе, содержащем вдобавок к B_0 некоторую слабоповторную функцию, то минимальная длина сертификата повторности для этого семейства в любом базисе, содержащем эту функцию, также не будет ограничена сверху константой. В [3, 70] показано, что в базисах, содержащих

вдобавок к B_0 функцию вида f_t^s или f_d^s , минимальная длина сертификата повторности последовательности функций $\{f_m^n\}$ при $n \rightarrow \infty$ не будет ограничена сверху константой. Если минимальная длина сертификата повторности для последовательности функций $\{f_m^n\}$ при $n \rightarrow \infty$ не ограничена сверху константой в базисах, содержащих вдобавок к B_0 одну из монотонных слабоповторных в B_0 функций, то минимальная длина сертификата повторности не ограничена сверху константой ни в одном из базисов, содержащих B_0 и хотя бы одну повторную в нем функцию. Следовательно, B_0 – единственный базис, содержащий как немонотонную, так и нелинейную функции, в котором минимальная длина сертификата повторности ограничена сверху константой.

Утверждение 2.7. [23] *Если $\{\alpha_1, \dots, \alpha_k\}$ – сертификат повторности поляризуемой функции $f(x_1, \dots, x_n)$ в произвольном базисе B , то сертификатом повторности функции $\bar{f}(x_1, \dots, x_n)$ также будет множество $\{\alpha_1, \dots, \alpha_k\}$.*

Доказательство. Допустим, это не так и существует неповторная в B функция g , совпадающая с $\bar{f}$ на $\{\alpha_1, \dots, \alpha_k\}$. Тогда неповторная в B функция $\bar{g}$ совпадает с f на этих наборах, что противоречит тому, что $\{\alpha_1, \dots, \alpha_k\}$ – сертификат повторности функции f .

Утверждение 2.8. *У любой функции, неповторной в B_4, B_5*

или B_m^s , существует неповторная формула с поднятыми отрицаниями.

Доказательство. Легко заметить, что $\bar{f}_4(x_1, x_2, x_3, x_4) = f_4(\bar{x}_3, \bar{x}_2, \bar{x}_1, \bar{x}_4)$, $\bar{f}_5(x_1, x_2, x_3, x_4, x_5) = f_5(\bar{x}_1, \bar{x}_5, \bar{x}_3, \bar{x}_4, \bar{x}_2)$, а f_m^s – самодвойственная. Используя эти свойства и правила де Моргана, из любой неповторной в B_4 , B_5 или B_m^s формулы можно получить неповторную в соответствующем базисе формулу с поднятыми отрицаниями.

Утверждение 2.9. [23] Если $\{\alpha_1, \dots, \alpha_k\}$ – сертификат повторности монотонной функции $f(x_1, \dots, x_n)$ в монотонном базисе B , где B – один из базисов $\{\&, \vee, f_4\}$, $\{\&, \vee, f_5\}$ или $\{\&, \vee, f_m^s\}$, то сертификатом повторности функции вида $f(x_1^{\sigma_1}, \dots, x_n^{\sigma_n})$ в базисе B' , равном B_4, B_5 или B_m^s соответственно, будет любое множество наборов S , удовлетворяющее следующим условиям:

- 1) множество S содержит подмножество $\{\beta_1, \dots, \beta_k\}$, где β_i получается из α_i возведением j -й компоненты в степень σ_j ;
- 2) для каждой переменной x_i множество S содержит соседние по x_i наборы, на которых реализуется подфункция x_i или $\bar{x}_i$.

Доказательство. Рассмотрим множество S наборов значений переменных $\{x_1, \dots, x_n\}$, удовлетворяющее условиям 1 и 2 утверждения. Допустим, что множество S не является сертификатом повторности для функции $f(x_1^{\sigma_1}, \dots, x_n^{\sigma_n})$ в B' и существует неповторная

в базисе B' функция $g(x_1, \dots, x_n)$, совпадающая на множестве S с функцией $f(x_1^{\sigma_1}, \dots, x_n^{\sigma_n})$. Согласно условию 2, вектор поляризации функции f нам известен. Покомпонентным возведением наборов из множества S в соответствующую степень получим множество, содержащее $\{\alpha_1, \dots, \alpha_k\}$. Функция $g(x_1^{\sigma_1}, \dots, x_n^{\sigma_n})$ монотонна, что видно по наборам из условия 2, и неповторна в базисе B , так как в силу утверждения 2.8 из ее неповторной в базисе B' формулы можно получить формулу с поднятыми отрицаниями, которая, в силу монотонности функции, будет неповторной в базисе B формулой. Таким образом, получим, что неповторная в базисе B функция $g(x_1^{\sigma_1}, \dots, x_n^{\sigma_n})$ совпадает на наборе $\{\alpha_1, \dots, \alpha_k\}$ с функцией $f(x_1, \dots, x_n)$, что противоречит условию. Значит, S является сертификатом повторности для функции f в базисе B .

Утверждение 2.10. [23]

$$S_4(n) \leq 2n \text{ при } n > 4,$$

$$S_5(n) \leq 2n \text{ при } n > 5,$$

$$S_m^s(n) \leq 2n \text{ при } n > s.$$

Доказательство. Сертификатом повторности монотонной функции $f_m^n(x_1, \dots, x_n)$ в базисах B_m^s , B_4 и B_5 является множество наборов $S = \{e_1, e_1 \oplus e_2, \dots, e_1 \oplus e_n, 1 \oplus e_1, 1 \oplus e_1 \oplus e_2, \dots, 1 \oplus e_1 \oplus \dots \oplus e_n\}$, содержащее $2n$ наборов, так как по нему легко устанавливается монотонность функции по каждому аргументу и оно содержит

все верхние нули и нижние единицы монотонной функции. Произвольная функция семейства f_m^s , зависящая от n переменных, имеет вид $f_m^n(x_1^{\sigma_1}, \dots, x_n^{\sigma_n})$, так как f_m^s – самодвойственная. Для множества, полученного покомпонентным возведением наборов из множества S в степени $\sigma_1, \dots, \sigma_n$, получается множество, удовлетворяющее условиям 1 и 2 из утверждения 2.9. Действительно, условие 1 выполнено по построению, а условие 2 следует из того факта, что множество S для каждой переменной x_i содержит соседние наборы, на которых реализуются подфункции x_i или $\bar{x}_i$. Следовательно, для любой обобщенно-однотипной с f_m^n функцией существует сертификат повторности длины $2n$. Аналогичным свойством обладают множества верхних нулей и нижних единиц функций f_4 и f_5 , размер которых ограничен константой и не превышает 8 и 10 соответственно. Как было упомянуто выше в доказательстве утверждения 2.6, длина сертификата для немонотонных слабоповторных функций ограничена константой 4. Из этого следует линейная верхняя оценка $2n$ для $S_4(n)$, $S_5(n)$ и S_m^s при достаточно больших n .

Функция f_m^n слабоповторна в базисе B_0 и является неразложимой функцией в силу единственности бесповторного представления над множеством неразложимых функций [29], поэтому функция f_m^n является повторной в базисах B_m^s (при $n \neq s$), B_4 и B_5 . Докажем, что:

- 1) функцию f_m^n нельзя отличить от всех функций, представимых

бесповторными формулами над B_m^s , предъявив менее $\lceil \log(n-1) \rceil + 1$ наборов;

2) функцию f_m^n нельзя отличить от всех функций, представимых бесповторными формулами над B_4 , предъявив менее $\lceil \log(n-1) \rceil$ наборов;

3) функцию f_m^n нельзя отличить от всех функций, представимых бесповторными формулами над B_5 , предъявив менее $\lceil \log(n-1) - \log 3 \rceil + 1$ наборов.

Для этого используем метод разнозначных матриц [5].

Лемма 2.3. [23] Пусть $n \geq 4$ и $k < \log(n-1)$, а M – это $(0,1)$ -матрица размерности $(k-1) \times n$ с нулевым первым столбцом, не содержащая строку $(0, 1, \dots, 1)$. Тогда существует бесповторная в B_4 функция $g(x_1, \dots, x_n)$, равная нулю на матрице M и совпадающая на ней с двойственной функцией, такая, что $g(0, 1, \dots, 1) = 1$, $g(1, 0, \dots, 0) = 0$.

Доказательство. Базис индукции. Пусть $4 \leq n \leq 7$. Тогда $k \leq 2$ и матрица M содержит не более одной строки. Так как матрица не содержит строку $(0, 1, \dots, 1)$, то искомой функцией будет некоторая переменная.

Индуктивный переход. Пусть $n > 7$, и для всех $n' < n$ (где $n' > 3$) утверждение леммы выполнено. При $k < \log(n-1)$ среди $n-1$

последних столбцов $x_2, \dots, x_n$ матрицы M найдется три одинаковых столбца. Пусть это столбцы x_2, x_3, x_4 . Тогда возможны два случая.

1. Пусть столбцы x_2, x_3, x_4 состоят из одних единиц. Возьмем любую строку, содержащую хотя бы один ноль на столбцах из множества $\{x_2, \dots, x_n\}$. Такая обязательно найдется, так как матрица M не содержит строк $(0, 1, \dots, 1)$. Пусть x_2 будет столбцом, на котором эта строка равна нулю, и x_3, x_4 — два единичных столбца. Построим матрицу M' из M , удалив столбцы x_2, x_3, x_4 и строки, на которых $f_4(x_2, 0, 0, 0) = f_4(x_2, 0, 1, 0) = 0$, т. е. все строки, где $x_2 = 0$. Пусть n' — число столбцов матрицы M' , а k' — количество строк. При этом $n' = n - 3$ и $n' > 4$. Тогда при $n > 7$ выполняется

$$k' \leq k - 1 < \log(n - 1) - 1 \leq \log(n - 4) = \log(n' - 1).$$

Матрица M' не содержит строк $(0, 1, \dots, 1)$. Следовательно, по предположению индукции существует неповторная в B_4 функция $g'(y_1, \dots, y_{n'})$, такая, что $g'(0, 1, \dots, 1) = 1$, $g'(1, 0, \dots, 0) = 0$, а также равная нулю на матрице M' и совпадающая на ней с двойственной функцией. Рассмотрим функцию $g_1(x_1, \dots, x_n) = f_4(x_2, x_1, g'(\bar{x}_4, x_5, \dots, x_n), \bar{x}_3)$:

$$g_1(0, 1, \dots, 1) = f_4(1, 0, 1, 0) = 1,$$

$$g_1(1, 0, \dots, 0) = f_4(0, 1, 0, 1) = 0,$$

и на строках матрицы M , на которых $x_2 = 0$:

$$g_1(0, x_2, \dots, x_n) = f_4(x_2, 0, 0, 0) = f_4(x_2, 0, 1, 0) = 0.$$

Так как в матрицу M' по построению входят только те подстроки строк из матрицы M , в которых $x_2 = 1$, а g' равна нулю на любой строке из матрицы M' , то функция

$$g_1(0, 1, x_3, \dots, x_n) = g_1(0, 1, 1, 1, x_5, \dots, x_n) = f_4(1, 0, 0, 0) = 0$$

для любой строки из матрицы M , у которой $x_2 = 1$. Таким образом, функция $g_1(x_1, \dots, x_n) = 0$ на любой строке из матрицы M , и, согласно замечанию 1.1, функция g_1 совпадает на матрице M с двойственной функцией. Следовательно, функция g_1 является искомой функцией из условия леммы.

2. Пусть столбцы x_2, x_3, x_4 не являются единичными. Построим матрицу M' из матрицы M , удалив столбцы x_2, x_3, x_4 и строки, на которых $f_4(0, x_2, 0, x_3) = f_4(0, x_2, 1, x_3) = 0$. Если после удаления появились одинаковые строки, то оставляем в матрице M' только одну из них. Пусть n' – число столбцов матрицы M' , а k' – количество строк. При этом $n' = n - 3$ и $n' > 4$. Тогда при $n > 7$ выполняется

$$k' \leq k - 1 < \log(n - 1) - 1 \leq \log(n - 4) = \log(n' - 1).$$

Матрица M' не содержит строк $(0, 1, \dots, 1)$. Следовательно, по предположению индукции существует неповторная в B_4 функ-

ция $g'(y_1, \dots, y_{n'})$, такая, что $g'(0, 1, \dots, 1) = 1$, $g'(1, 0, \dots, 0) = 0$, а также равная нулю на матрице M' и совпадающая на ней с двойственной функцией. Рассмотрим функцию $g_2(x_1, \dots, x_n) = f_4(x_1, x_2, g'(\bar{x}_4, x_5, \dots, x_n), x_3)$:

$$g_2(0, 1, \dots, 1) = f_4(0, 1, 1, 1) = 1,$$

$$g_2(1, 0, \dots, 0) = f_4(1, 0, 0, 0) = 0,$$

и на строках матрицы M , на которых $x_2 = x_3 = 0$:

$$g_2(0, x_2, \dots, x_n) = f_4(0, x_2, 0, x_3) = f_4(0, x_2, 1, x_3) = 0.$$

Так как в матрицу M' по построению входят только те подстроки строк из матрицы M , у которых $x_2 = x_3 = 1$, а функция g' равна нулю на любой строке матрицы M' , то

$$g_2(0, 1, 1, 1, x_5, \dots, x_n) = f_4(0, 1, 0, 1) = 0$$

для любой строки из матрицы M , в которой $x_2 = x_3 = 1$. Таким образом, функция $g_2(x_1, \dots, x_n) = 0$ на любой строке из матрицы M , и, согласно замечанию 1.1, функция g_2 совпадает на матрице M с двойственной функцией. Следовательно, функция g_2 является искомой функцией из условия леммы.

Лемма доказана.

Лемма 2.4. [23] Пусть $n \geq 5$ и $k < \log(n-1) - \log 3 + 1$, а M – $(0,1)$ -матрица размерности $(k-1) \times n$ с нулевым первым столбцом, не содержащая строку $(0, 1, \dots, 1)$. Тогда существует бесспорная в базисе B_5 функция $g(x_1, \dots, x_n)$, равная нулю на матрице M и совпадающая на ней с двойственной функцией, такая, что $g(0, 1, \dots, 1) = 1$, $g(1, 0, \dots, 0) = 0$.

Доказательство. Базис индукции. Пусть $5 \leq n \leq 8$. Тогда $k \leq 2$ и матрица M содержит не более одной строки. Так как матрица не содержит строк $(0, 1, \dots, 1)$, то искомой функцией будет некоторая переменная.

Индуктивный переход. Пусть $n \geq 9$ и для всех $n' < n$ (где $n' > 4$) утверждение леммы выполнено.

При $k < \log(n-1) - \log 3 + 1$ среди последних $n-1$ столбцов M найдется четыре одинаковых столбца. Обозначим их через x_2, x_3, x_4, x_5 . Тогда возможны два случая.

1. Пусть эти столбцы состоят из одних единиц. Возьмем любой не единичный столбец. Обозначим его через x_6 . Построим матрицу M' , удалив из M столбцы x_2, x_3, x_4, x_5 и строки, на которых $f_5(0, x_6, x_3, \bar{x}_2, 0) = f_5(0, x_6, x_3, \bar{x}_2, 1) = 0$. Пусть n' – число столбцов матрицы M' , а k' – количество строк. При этом $n' = n - 4$ и $n' > 5$. Тогда при $n \geq 9$ выполняется

$$k' \leq k - 1 < \log(n-1) - \log 3 - 2 \leq$$

$$\leq \log(n-5) - \log 3 - 1 = \log(n'-1) - \log 3 - 1.$$

Матрица M' не содержит строку $(0, 1, \dots, 1)$. Следовательно, по предположению индукции существует неповторная в B_5 функция $g'(y_1, \dots, y_{n'})$, такая, что

$$g'(0, 1, \dots, 1) = 1, g'(1, 0, \dots, 0) = 0,$$

а также равная нулю на матрице M' и совпадающая на ней с двойственной функцией.

Любая строка из матрицы M в таком случае имеет вид

$$(1, 1, 1, 1, 0, \alpha_7, \dots, \alpha_n)$$

или

$$(1, 1, 1, 1, 1, \alpha_7, \dots, \alpha_n).$$

Тогда искомой функцией из условия леммы будет

$$g_3(x_1, \dots, x_n) = f_5(x_1, x_6, x_3, \bar{x}_2, g'(\bar{x}_4, x_5, x_7, \dots, x_n)).$$

Действительно, для функции g_3 верно:

$$g_3(0, 1, 1, 1, 1, 0, \alpha_7, \dots, \alpha_n) = f_5(0, 0, 1, 0, g'(0, 1, \alpha_7, \dots, \alpha_n)) = 0,$$

$$\begin{aligned} g_3(0, 1, 1, 1, 1, 1, \alpha_7, \dots, \alpha_n) &= f_5(0, 1, 1, 0, g'(0, 1, \alpha_7, \dots, \alpha_n)) = \\ &= f_5(0, 1, 1, 0, 0) = 0, \end{aligned}$$

$$g_3(0, 1, \dots, 1) = f_5(0, 1, 1, 0, g'(0, 1, 1, \dots, 1)) = f_5(0, 1, 1, 0, 1) = 1,$$

$$g_3(1, 0, \dots, 0) = f_5(1, 0, 0, 1, g'(1, 0, 0, \dots, 0)) = f_5(1, 0, 0, 1, 0) = 0,$$

и функция $g_3(x_1, \dots, x_n)$ совпадает на матрице M с двойственной функцией в силу замечания 1.1.

2. Пусть найденные столбцы не единичные. Построим матрицу M' , удалив из матрицы M столбцы x_2, x_3, x_4, x_5 и строки, на которых $f_5(x_2, 0, \bar{x}_3, x_4, 0) = f_5(x_2, 0, \bar{x}_3, x_4, 1) = 0$. Аналогично предыдущему случаю, существует неповторная в базисе B_5 функция $g'(y_1, \dots, y_{n'})$, такая, что

$$g'(0, 1, \dots, 1) = 1,$$

$$g'(1, 0, \dots, 0) = 0,$$

а также равная нулю на матрице M' и совпадающая на ней с двойственной функцией. Любая строка из матрицы M в таком случае имеет вид $(0, 0, 0, 0, \alpha_6, \dots, \alpha_n)$ или $(1, 1, 1, 1, \alpha_6, \dots, \alpha_n)$. Тогда искомой функцией из условия леммы является

$$g_4(x_1, \dots, x_n) = f_5(x_2, x_1, \bar{x}_3, x_4, g'(\bar{x}_5, x_6, \dots, x_n)).$$

Действительно, для функции g_4 верно:

$$g_4(0, 0, 0, 0, 0, \alpha_6, \dots, \alpha_n) = f_5(0, 0, 1, 0, g'(1, \alpha_6, \dots, \alpha_n)) = 0,$$

$$\begin{aligned} g_4(0, 1, 1, 1, 1, \alpha_6, \dots, \alpha_n) &= f_5(1, 0, 0, 1, g'(0, \alpha_6, \dots, \alpha_n)) = \\ &= f_5(1, 0, 0, 1, 0) = 0, \end{aligned}$$

$$g_4(0, 1, \dots, 1) = f_5(1, 0, 0, 1, g'(0, 1, \dots, 1)) = f_5(1, 0, 0, 1, 1) = 1,$$

$$g_4(1, 0, \dots, 0) = f_5(0, 1, 1, 0, g'(1, 0, \dots, 0)) = f_5(0, 1, 1, 0, 0) = 0,$$

и функция $g_4(x_1, \dots, x_n)$ совпадает на матрице M с двойственной функцией в силу замечания 1.1.

Лемма доказана.

Лемма 2.5. [23] Пусть $n > s$ и $k < \log(n - 1) + 1$, а M – $(0,1)$ -матрица размерности $(k-1) \times n$ с нулевым первым столбцом, не содержащая строку $(0, 1, \dots, 1)$. Тогда существует неповторная в базисе B_m^s самодвойственная функция $g(x_1, \dots, x_n)$, равная единице на наборе $(0, 1, \dots, 1)$ и нулю на матрице M .

Доказательство. Базис индукции. Пусть $k \leq n < 2s$. Так как $n < 2s$, и $k < \log(n - 1) + 1$, то $k \leq s$ при $s \geq 3$. Выберем для каждой строки по одному столбцу из $n - 1$ последних столбцов с нулем в этой строке. Это возможно, так как матрица M не содержит строку $(0, 1, \dots, 1)$. Обозначим выбранные столбцы через $x_{i_1}, \dots, x_{i_t}$. Очевидно неравенство $t < k \leq s$. Тогда функция

$$f_m^s(x_1, x_{i_1}, \dots, x_{i_t}, x_{j_1}, \dots, x_{j_{s-t}}),$$

где $x_{j_1}, \dots, x_{j_{s-t}}$ – любые оставшиеся столбцы, будет искомой функцией из условия леммы.

Индуктивный переход. Пусть $n \geq 2s$ и для всякого $n' < n$ (где $n' > s$) утверждение леммы выполнено.

Пусть в матрице M всего $t \leq s$ столбцов, содержащих нули. Если $t < s$, то добавим к ним произвольные $s - t$ столбцов. Не ограничивая общности, допустим, что выбранные t столбцов – первые. Так как все строки в матрице M различны и не равны $(0, 1, \dots, 1)$, то в любой строке найдется хотя бы два нуля в выбранных столбцах. Тогда $f_m^s(x_1, \dots, x_s)$ будет искомой функцией g из условия леммы.

Пусть в матрице M больше s столбцов, содержащих нули. Так как $k < \log(n - 1) + 1$ и количество разных столбцов длины $k - 1$ равно $2^{k-1} < n - 1$, то среди $n - 1$ последних столбцов матрицы найдется два одинаковых. Пусть это будут столбцы x_2 и x_3 . Тогда возможны два случая.

1. Если столбцы x_2 и x_3 состоят из одних единиц, то возьмем любой не нулевой и не единичный столбец. Так как строки различны, такой столбец существует. Пусть это будет столбец x_4 . Возьмем любые $s - 4$ столбца, отличных от уже выбранных столбцов. Пусть это будут столбцы $x_5, \dots, x_s$. Построим матрицу M' , удалив из M столбцы $\{x_2, \dots, x_s\}$ и строки, в которых хотя бы одна из переменных $\{x_4, \dots, x_s\}$ равна нулю. Так как столбец x_4 не единичный, то найдется хотя бы одна такая строка. Пусть n' – число столбцов матрицы M' , а k' – количество строк. При этом $n' = n - s + 1$ и $n' \geq s + 1$. Тогда при $n \geq 2s$ выполняется

$$k' \leq k - 1 < \log(n - 1) = \log(n' + s - 1) \leq \log(n' - 1) + 1.$$

Матрица M' не содержит единичных строк. Тогда по предположению индукции существует неповторная в базисе B_m^s самодвойственная функция $g'(y_1, \dots, y_{n'})$, такая, что $g'(0, 1, \dots, 1) = 1$ и $g'(y_1, \dots, y_{n'})$ равна нулю на матрице M' . Тогда искомой функцией является

$$g(x_1, \dots, x_n) = f_m^s(x_1, x_3, \dots, x_s, g'(\bar{x}_2, x_{s+1}, \dots, x_n)).$$

Действительно, в любой строке либо одна из переменных $\{x_3, \dots, x_s\}$ равна нулю, либо равна нулю функция g' , и тогда функция g равна нулю на всех строках матрицы M и является самодвойственной. Также верно, что

$$\begin{aligned} g(0, 1, \dots, 1) &= f_m^s(0, 1, \dots, 1, g'(0, 1, \dots, 1)) = \\ &= f_m^s(0, 1, \dots, 1, 1) = 1. \end{aligned}$$

2. Пусть столбцы x_2 и x_3 не являются единичными. Добавим к ним любые $s - 3$ столбца. Пусть это будут столбцы $x_4, \dots, x_s$. Построим матрицу M' , удалив из матрицы M столбцы $\{x_2, \dots, x_s\}$ и строки, на которых хотя бы одна из переменных $\{x_3, \dots, x_s\}$ равна нулю. Аналогично предыдущему случаю, существует неповторная в базисе B_m^s самодвойственная функция $g'(y_1, \dots, y_{n'})$, такая, что $g'(0, 1, \dots, 1) = 1$ и $g'(0, y_2, \dots, y_{n'})$ равна нулю на матрице M' и является самодвойственной. Тогда искомой функцией из условия леммы так же, как в предыдущем случае, является g .

Лемма доказана.

Лемма 2.6. [23] Пусть $n \geq 4$ и $k < \log(n - 1)$. Тогда для произвольных k наборов значений переменных функции $f_m^n(x_1, \dots, x_n)$ существует неповторная в базисе B_4 функция $g(x_1, \dots, x_n)$, совпадающая с f_m^n на этих наборах.

Доказательство. Пусть $A = \{\alpha_1, \dots, \alpha_k\}$ – множество наборов значений переменных $\{x_1, \dots, x_n\}$. Рассмотрим два случая.

1. Множество A не содержит хотя бы один из наборов $(0, 1, \dots, 1)$ или $(1, 0, \dots, 0)$. Тогда $f_m^n(x_1, \dots, x_n)$ на множестве A совпадает с одной из функций $x_1 \& (x_2 \vee \dots \vee x_n)$ или $x_1 \vee x_2 \& \dots \& x_n$.
2. Множество A содержит оба набора $(0, 1, \dots, 1)$ и $(1, 0, \dots, 0)$. Построим множество A' из наборов множества A с нулем в первой позиции, кроме набора $(0, 1, \dots, 1)$, и наборов, противоположных наборам с единицей в первой позиции, кроме набора $(1, 0, \dots, 0)$. Очевидно, что мощность множества A' не превосходит $k - 1$. Составим матрицу M из наборов множества A' . Тогда по лемме 2.3 существует неповторная в B_4 функция $g(x_1, \dots, x_n)$, равная нулю на наборе $(0, 1, \dots, 1)$, единице на наборе $(1, 0, \dots, 0)$, а также равная нулю на M и совпадающая на ней с двойственной функцией. Нетрудно заметить, что g равна нулю на всех наборах A , содержащих ноль в первой позиции, и единице на всех наборах, содержащих единицу в

первой позиции, кроме наборов $(0, 1, \dots, 1)$ или $(1, 0, \dots, 0)$ соответственно. Таким образом, функция $g(x_1, \dots, x_n)$ совпадает с $f_m^n(x_1, \dots, x_n)$ на наборах множества A .

Лемма доказана.

Лемма 2.7. [23] Пусть $n \geq 5$ и $k < \log(n-1) - \log 3 + 1$. Тогда для произвольных k наборов значений переменных функции $f_m^n(x_1, \dots, x_n)$ существует неповторная в B_5 функция $g(x_1, \dots, x_n)$, совпадающая с f_m^n на этих наборах.

Лемма 2.8. [23] Пусть $n > s$ и $k < \log(n-1) + 1$. Тогда для произвольных k наборов значений переменных функции $f_m^n(x_1, \dots, x_n)$ существует неповторная в B_m^s функция $g(x_1, \dots, x_n)$, совпадающая с f_m^n на этих наборах.

Доказательства лемм 2.7 и 2.8 проводятся аналогично доказательству леммы 2.6 с применением лемм 2.4 и 2.5 соответственно.

Из лемм 2.6, 2.7 и 2.8 следует

Теорема 2.2. [23] При $n \geq 4$ выполняется условие $S_4(n) \geq \log(n-1)$, при $n \geq 5$ выполняется $S_5(n) \geq \log(n-1) - \log 3 + 1$, а также при $n > s$ выполняется $S_m^s(n) \geq \log(n-1) + 1$.

Из теоремы 2.2 и утверждения 2.6 следуют теоремы 2.3 и 2.4.

Теорема 2.3. [23] *Базис B_0 является единственным базисом, содержащим как нелинейные, так и немонотонные функции, в котором длина сертификата повторности ограничена сверху константой.*

Теорема 2.4. [23] *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:*

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

§ 2.3. Сертификаты повторности в базисе всех функций l переменных

В этом параграфе будет показано, что функция Шеннона для длины сертификата повторности в базисе всех функций l переменных ограничена величиной $O(n^l)$.

В базисе B_t^s функция Шеннона для длины сертификата повторности $S_t^s(n) = \Omega(n^{s-1})$ [70]. Так как при добавлении функций в базис длина сертификата повторности монотонно не убывает, то из этого следует

Утверждение 2.11. [11] *Функция Шеннона длины сертификата повторности функции n переменных в базисе B^l есть величина $\Omega(n^{l-1})$.*

Лемма 2.9. [11] Пусть функция $g(y_1, \dots, y_m, x)$ неповторна в B^l . Пусть $g(y_1, \dots, y_m, \sigma) = y_1 \vee \dots \vee y_m$, где σ – некоторая константа. Пусть функция g имеет вид $\phi_0 \vee f(\phi_1, \dots, \phi_k, x)$, где ϕ_i – дизъюнкции различных переменных $y_1, \dots, y_m$, и f – некоторая неповторная в B^l функция. Тогда функция g однозначно восстанавливается по значениям на $C_m^k \cdot 2^k$ наборах.

Доказательство. Функция g при $x = \sigma$ имеет вид

$$g(y_1, \dots, y_m, \sigma) = y_1 \vee \dots \vee y_m.$$

Для восстановления g достаточно определить, в какую дизъюнкцию ϕ_i входит каждая переменная y_j . Зафиксируем первые k переменных $y_1, \dots, y_k$. Заменим на ноль все переменные, кроме $y_1 \vee \dots \vee y_k$ и x . Так как ноль является забывающей константой для любой переменной в дизъюнкции, то переменные $y_{k+1} \vee \dots \vee y_m$ останутся существенными. Возможны четыре случая.

- Переменные $y_1, \dots, y_k$ входят соответственно в $\phi_1, \dots, \phi_k$. Тогда неопределенной останется подфункция вида $f(y_1, \dots, y_k, x)$. Так как известна ее подфункция при $x = \sigma$, то функция $f(y_1, \dots, y_k, x)$ однозначно определяется по значениям на 2^k наборах на противоположном подкубе $x = \bar{\sigma}$.
- Среди переменных $y_1, \dots, y_k$ найдутся две переменные y_{j_1} и y_{j_2} , входящие в одну дизъюнкцию, например ϕ_1 , то получен-

ная функция будет иметь вид $h_1(y_{j_1} \vee y_{j_2}, y_{j_3}, \dots, y_{j_k}, x)$, где h_1 – некоторая булева функция k переменных.

- Хотя бы одна переменная y_i входит в функцию ϕ_0 . Тогда полученная функция будет иметь вид $y_i \vee h_2(y_{j_1}, \dots, y_{j_{k-1}}, x)$, где h_2 – некоторая булева функция k переменных.
- Переменные $y_1, \dots, y_k$ входят в разные дизъюнкции $\phi_1, \dots, \phi_k$, и полученная функция будет с точностью до перестановки переменных равна $f(y_1, \dots, y_k, x)$.

Рассмотрев все случаи, мы найдем функцию f и множество переменных $y_1, \dots, y_k$, входящих в разные дизъюнкции. Переберем все возможные множества из k переменных и проведем рассуждения аналогично рассмотренному выше множеству переменных $y_1, \dots, y_k$, что можно сделать C_m^k способами. При этом мы найдем все переменные, от которых зависят $\phi_1, \dots, \phi_k$ и не зависит ϕ_0 .

Покажем, какие из переменных $y_1, \dots, y_m$ входят в одну и ту же дизъюнкцию. Рассмотрим пару переменных y_1 и y_2 . Если они входят в разные дизъюнкции ϕ_i и ϕ_j , то встретилось хотя бы одно множество из k переменных, с помощью которых согласно вышеуказанной процедуре получается функция f . Таким образом, функции $f(\phi_1, \dots, \phi_k, x)$ и ϕ_0 определяются с точностью до перестановки переменных и функция g полностью восстанавливается по значениям на $C_m^k \cdot 2^k$ наборах. Лемма доказана.

Лемма 2.10. [11] Пусть функция $g(y_1, \dots, y_m, x)$ неповторна в B^l . Пусть $g(y_1, \dots, y_m, \sigma) = y_1 \& \dots \& y_m$, где σ – некоторая константа. Пусть g имеет вид $\phi_0 \& f(\phi_1, \dots, \phi_k, x)$, где ϕ_i – конъюнкции различных переменных $y_1, \dots, y_m$. Тогда g однозначно восстанавливается по значениям на $C_m^k \cdot 2^k$ наборах.

Доказательство проводится аналогично лемме 2.9, с заменой забивающей константы 0 на 1 в константных подстановках.

Лемма 2.11. [11] Пусть функция $g(y_1, \dots, y_m, x)$ неповторна в B^l . Пусть $g(y_1, \dots, y_m, \sigma) = y_1 \oplus \dots \oplus y_m$, где σ – некоторая константа. Пусть g имеет вид $\phi_0 \oplus f(\phi_1, \dots, \phi_k, x)$, где ϕ_i – суммы по модулю два различных переменных $y_1, \dots, y_m$. Тогда g однозначно восстанавливается по значениям на $C_m^k \cdot 2^k$ наборах.

Доказательство проводится полностью аналогично лемме 2.9.

Допустим, что количество переменных базисной функции f не известно заранее. Любое множество наборов для случая $k < l - 1$ входит в некоторое множество наборов для случая $k = l - 1$, так как каждый подкуб меньшей размерности k входит в подкуб большей размерности $l - 1$, а константные подстановки на места остальных переменных не зависят от функции f . По виду функций, полученных для каждого множества из l функций, k определяется как максимальное число переменных функции вида $h(y_{j_1}, \dots, y_{j_k}, x)$, где $y_{j_1}, \dots, y_{j_k}$ не входят в ϕ_0 и входят в разные ϕ_i . Таким образом, функ-

ция g , удовлетворяющая условиям леммы 2.9, 2.10 или 2.11 однозначно восстанавливается по $C_m^{l-1} \cdot 2^{l-1}$ наборам.

Утверждение 2.12. [11] *Пусть дано помеченное корневое ориентированное дерево D . Тогда число корневых поддеревьев с корнем в некоторой вершине v и не более чем p вершинами, такими, что любая внутренняя вершина входит в поддерево вместе со всеми смежными в дереве D вершинами, не превосходит 4^{p-1} .*

Данное утверждение доказывается в [11] аналогично классическому утверждению о числе упрямых корневых деревьев (см. [1]).

Утверждение 2.13. [57] *Проверяющий тест для неповторной в базисе B^l функции, существенно зависящей от n переменных, на множестве всех l -бесповторных функций содержит не более $C_n^l \cdot 2^l$ наборов.*

Теорема 2.5. [11]

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

Доказательство. Пусть функция $f(x_1, \dots, x_n)$ повторна в базисе B^l и существенно зависит от всех своих переменных. Тогда у нее существует некоторая слабоповторная подфункция g . Без ограничения общности, пусть g зависит от первых m переменных $x_1, \dots, x_m$. Известно (см. [30]), что у любой булевой функции есть переменная,

для которой существует незабывающая константа. Тогда у g найдутся переменная x_i и константа σ , такие, что подфункция g' , полученная подстановкой σ на место x_i , существенно зависит от всех остальных переменных. Полученная подфункция будет неповторна в B^l . По утверждению 2.13, она однозначно задается на $C_{m-1}^l \cdot 2^l$ наборах. Рассмотрим дерево D , реализующее произвольную неповторную функцию от переменных $x_1, \dots, x_m$, совпадающую с $g(x_1, \dots, x_m)$ при $x_i = \sigma$. При подстановке $x_i = \sigma$ из этого дерева получается поддерево D' , реализующее неповторную в B^l функцию g' . Это могло произойти следующим образом.

- Некоторое поддерево D'' дерева D' соответствует функции, полученной подстановкой $x_i = \sigma$ в функцию f' из B^l , которой помечена некоторая вершина в дереве D . Выделим такое поддерево. Пусть это поддерево имеет корень в вершине v . В нем не более чем $l - 1$ листьев, соответствующих входам вершины, помеченной f' в дереве D . Подставим константы на места переменных так, чтобы каждая функция, соответствующая входу функции f' , равнялась какой-либо переменной, а функция, которую реализует дерево D , равнялась функции f' . Получим подкуб размерности l , половина которого при $x_i = \sigma$ нам уже известна. Таким образом, на 2^{l-1} наборах целиком определяется функция f' , и, следовательно, восстанавливается функция, которую реализует дерево D . Функция g либо отличается на

каком-то из этих наборов от функции, которую реализует дерево D для любой такой функции f' , либо совпадает с ней на этих наборах, но отличается на каком-то еще наборе. Таким образом, достаточно предъявить $2^{l-1} + 1$ набор, чтобы отличить g от любой неповторной функции с подфункцией f' , чья подфункция при $x_i = \sigma$ представляет собой поддерево D'' . Посчитаем количество поддеревьев, которые можно выделить таким образом. С помощью индукции легко доказывается, что число вершин степени не меньше двух в дереве меньше количества листьев. Поэтому в D' не более $2l - 2$ вершин. Поддерево D' удовлетворяет условию утверждения 2.12, и количество таких поддеревьев не превосходит 4^{2l-3} . Таким образом, чтобы отличить g , соответствующие таким деревьям, достаточно не более $m \cdot (2^{l-1} + 1) \cdot 4^{2l-3}$ наборов.

- Переменная x_i в дереве D смежна с вершиной, помеченной функцией от двух переменных, которая отождествляется со второй переменной или ее отрицанием при подстановке $x_i = \sigma$. Функций, соответствующих дереву D в этом случае, не более 3 на каждое ребро. Так как все вершины, кроме листовых и смежных с ними, имеют степень не меньше двух, то общее число вершин в дереве не больше $3m$. Таким образом, чтобы отличить все функции, устроенные таким образом, достаточно не более $3 \cdot 3m$ наборов.

- Переменная x_i в дереве D входит в вершину v_1 , помеченную неразложимой функцией из B^l , которая при подстановке $x_i = \sigma$ превращается в функцию из множества $\{\vee, \&, \oplus\}$ и входит в вершину v_2 , помеченную той же функцией. Подставим константы на места переменных таким образом, чтобы на каждом входе этих двух вершин была одна переменная. Полученная функция удовлетворяет условию лемм 2.9, 2.10 или 2.11. Рассмотрим наборы, полученные в соответствующей лемме. Если функция, реализуемая деревом D , совпадает с g на всех $C_{m-1}^{k-1} \cdot 2^{k-1}$ наборах, то у нее существует хотя бы один другой набор, в котором она отличается от g . Если не совпадает, то повторность доказывается предъявлением всех использованных наборов. Для разных неповторных функций, полученных из этой вершины, предъявленные наборы будут одинаковы, так как одинаковы функции на входах функций в вершинах v_1 и v_2 . Таким образом, согласно следствию из вспомогательных лемм, повторность g в этом случае доказывается за не более чем $C_{m-1}^{l-1} \cdot 2^{l-1} + 1$ набор для каждой такой вершины и в целом не более $m \cdot (C_{m-1}^{l-1}) \cdot 2^{l-1} + m = O(m^l)$ для всей функции.

Всего суммарно получается $3 \cdot 3m + m \cdot (2^{l-1} + 1) \cdot 4^{2l-3} + m \cdot (C_{m-1}^{l-1}) \cdot 2^{l-1} + m = O(m^l)$ наборов, которых достаточно, чтобы отличить функцию $g(x_1, \dots, x_m)$ от всех неповторных, совпадающих с ней при $x_i = \sigma$. Так как $m \leq n$, то для доказательства повторности функции

f достаточно предъявить $O(n^l) + C_{n-1}^{l-1} \cdot 2^l = O(n^l)$ наборов значений переменных. Теорема доказана.

Замечание. *Применив теорему Хегедуса из работы [75] к верхним оценкам теоремы 2.5 и леммы 2.10, можно получить новые оценки сложности в классической модели обучения с помощью запросов принадлежности и эквивалентности.*

Глава 3

Проверяющие тесты для функций, бесповторных в элементарном базисе, расширенном монотонными функциями Стеценко

В данной главе рассматривается задача проверяющего тестирования в элементарном базисе, расширенном всеми специальными функциями – в базисе B_{unate} . Исследуется функция Шеннона для длины теста относительно бесповторной альтернативы в данном базисе и устанавливается связь теста относительно бесповторной альтернативы в данных в базисе B_{unate} с проверяющим тестом в соответствующем базисе без отрицания B_{unate}^+ .

Задача тестирования относительно бесповторной альтернативы была поставлена А. А. Вороненко в работе [2]. Там же было показано, что при добавлении в элементарный базис всех оставшихся функций двух переменных функция Шеннона длины теста относительно бесповторной альтернативы становится квадратичной. Из свойств функции $x_1 \dots x_n \vee \bar{x}_1 \dots \bar{x}_n$ следует, что тест относительно бесповторной альтернативы в базисе всех функций l переменных содержит не меньше $\Omega(n^l)$ наборов ([8], с. 64–66). Д.В. Чистиковым [57] была

доказана верхняя линейная оценка $2n + 1$ функции Шеннона длины теста относительно бесповторной альтернативы в элементарном базисе. Далее будет показано, что добавление в элементарный базис специальных функций оставляет функцию Шеннона линейной. В работе [25] устанавливается линейность функции Шеннона для длины теста относительно бесповторной альтернативы в элементарном базисе, расширенном медианой. В работе [26] устанавливается линейность функции Шеннона для длины теста относительно бесповторной альтернативы в элементарном базисе, расширенном любой специальной функцией. Далее в работе [13] рассматривается элементарный базис, расширенный всеми специальными функциями, и устанавливается верхняя линейная оценка функции Шеннона для длины теста относительно бесповторной альтернативы, равная $3n - 2$. Из вышеизложенного получаем, что функция Шеннона для длины теста относительно бесповторной альтернативы в элементарном базисе, расширенном любыми специальными функциями, также не превышает $3n - 2$. Из этого следует наличие такой же верхней линейной оценки функции Шеннона для длины теста относительно бесповторной альтернативы в предэлементарных базисах B_4, B_5, B_m^s .

§ 3.1. Представление неповторных функций в виде корневых деревьев

Древесное представление булевых функций широко используется в задаче построения схем из функциональных элементов в различных базисах и в теории контактных схем с независимыми контактами [29]. В работе [2] приведено представление неповторных функций в базисе, состоящем из всех функций, зависящих не более чем от двух аргументов, в виде так называемого *канонического дерева*, а в работе [3] приведен его частный случай в элементарном базисе. Введем понятие канонического дерева для функций, неповторных в элементарном базисе, расширенном специальными функциями.

Каноническим деревом функции $f(x_1, \dots, x_n)$, неповторной в базисе, состоящем из конъюнкции, дизъюнкции и специальных функций, назовем [26] помеченное корневое дерево, построенное согласно следующим правилам.

1. Листья дерева помечены переменными $x_1, \dots, x_n$. Разные листья помечены разными переменными.
2. Внутренние вершины дерева соответствуют подформулам неповторной формулы и помечены функциями из множества $\{\vee, \&\}$ или специальной функцией.
3. Если специальная функция – f_4 , то над вершиной находятся

четыре инцидентных ребра, пронумерованных $(1, 2, 3, 4)$. Канонические деревья, получаемые с помощью перестановки ребер $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ над вершинами, помеченными f_4 , считаются эквивалентными.

4. Если специальная функция – f_5 , то над вершиной находятся пять инцидентных ребер, пронумерованных $(1, 2, 3, 4, 5)$. Канонические деревья, полученные с помощью группы перестановок, порождаемых перестановками ребер $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$ над вершинами, помеченными f_5 , считаются эквивалентными.
5. Если специальная функция – f_m^s , то над вершиной находятся s инцидентных ребер с выделенным при $s \geq 4$ первым ребром.
6. Над вершиной, помеченной $\vee$ или $\&$, расположено не менее двух смежных вершин.
7. Вершины, помеченные функцией $\vee (\&)$, не смежны с вершинами, помеченными функцией $\vee (\&)$.

Каноническое дерево D реализует функцию f по неповторной формуле от листьев к корню, как и в работах [2, 7]. При этом арность $\&$ и $\vee$ в формуле совпадает с числом ребер над помеченной ими вершиной.

Перестановка $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ является единственной нетривиальной эквивалентной перестановкой для f_4 . Перестановки $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$

образуют полную систему эквивалентных преобразований на множестве переменных функции f_5 . Перестановка переменных является эквивалентной для функции f_m^s при $s \geq 4$ тогда и только тогда, когда она сохраняет первую переменную. Для функции f_m^3 являются эквивалентными любые перестановки переменных. В силу вышеизложенного канонические деревья для неповторных функций в базисе B_{unate}^+ являются единственными с точностью до эквивалентности [26, 22].

§ 3.2. Леммы о восстановлении неповторных функций

В данном разделе будет показано, что функция n переменных, неповторная в элементарном базисе, расширенном специальными функциями, восстанавливается из подфункции, существенно зависящей от $n - 1$ переменных, за константное число наборов.

Лемма 3.1. [26, 25, 13] *Пусть неповторная в базисе B_{unate}^+ функция $h(z_1, z_2, z_{k+2}, \dots, z_n)$ существенно зависит от $n - k + 1 \geq 2$ переменных ($k \geq 2$), 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 $f'(x_1, \dots, x_n)$ – неповторная*

в B_{unate}^+ функция, такая, что $f'_{x_k=0} = f|_{x_k=0}$. Тогда, если выполнено равенство:

$$f'(x_1, \dots, x_{k+1}, \beta_{k+2}, \dots, \beta_n) = (x_1 \vee \dots \vee x_k) \& x_{k+1}, \quad (3.1)$$

то $f' = f$.

Доказательство. Обозначим D' каноническое дерево функции f' . Возьмем в качестве v из таблицы А.1 корень поддерева функции $x_1 \vee \dots \vee x_k$ в дереве D . Функция $f|_{x_k=0}$ существенно зависит от $n - 1$ переменной – случай 1 из таблицы А.1. Обозначим D_0 дерево функции $f|_{x_k=0}$. Обозначим $\tilde{\beta} = (\beta_{k+2}, \dots, \beta_n)$.

Обозначим u' первую общую на пути к корню вершину для листьев x_1 и x_{k+1} в дереве D' .

Из равенства (3.1) и наличия у функции f' подфункции $x_1 \& x_{k+1}$ следует, что u' не может быть помечена $\vee$. Тогда в силу наличия у функции f' подфункции $(x_1 \vee x_k) \& x_{k+1}$ переменная x_k не может лежать вне дерева, корнем которого является u' .

Таким образом, u' помечена $\&$ или медианой и x_k лежит выше u' . Обозначим D_u (D'_u) поддерево с листом x_k и с корнем, смежным u (u'). Тогда v будет корнем D_u . Далее покажем, что D'_u совпадает с D_u и D' совпадает с D .

Так как $x_k = 0$ – забывающая подстановка, то D совпадает с D_0 всюду, кроме D_u (см. табл. А.1). Аналогичным образом D' совпадает с D_0 всюду, кроме D'_u . Так как u – первая на пути к корню

вершина у листьев x_1 и x_{k+1} и она не входит в D_u , а вершина u' – не входит в D'_u , то эти вершины совпадают. При этом деревья D и D' совпадают всюду, кроме, быть может, дерева D_u выше u и дерева D'_u выше u' – притом множества остальных деревьев выше u и u' совпадают. Следовательно, f' так же, как и f , имеет вид

$$f'(x_1, \dots, x_n) = h(\phi(x_1, \dots, x_k), x_{k+1}, \dots, x_n),$$

где ϕ существенно зависит k переменных. Тогда по условию леммы:

$$\begin{aligned} f'(x_1, \dots, x_{k+1}, \beta_{k+2}, \dots, \beta_n) &= h(\phi(x_1, \dots, x_k), x_{k+1}, \beta_{k+2}, \dots, \beta_n) = \\ &= \phi(x_1, \dots, x_k) \& x_{k+1} = (x_1 \vee \dots \vee x_k) \& x_{k+1}. \end{aligned}$$

Следовательно, D'_u совпадает с D_u , а $D' = D$ и $f' = f$. Лемма доказана.

Лемма 3.2. [26, 25, 13] Пусть неповторная в базисе B_{unate}^+ функция $h(z_1, z_2, z_{k+2}, \dots, z_n)$ существенно зависит от $n - k + 1 \geq 2$ переменных ($k \geq 2$), и лист ее канонического дерева, который помечен переменной z_1 , смежен с вершиной u , помеченной конъюнкцией (дизъюнкцией) или специальной функцией, а лист, помеченный z_2 , лежит в каком-то другом поддереве над u . Пусть $f(x_1, \dots, x_n) = h(x_1 \vee \dots \vee x_k, x_{k+1}, \dots, x_n)$ ($h(x_1 \& \dots \& x_k, x_{k+1}, \dots, x_n)$). Пусть $h(z_1, z_2, \beta_{k+2}, \dots, \beta_n) = z_1 \& z_2$ ($z_1 \vee z_2$). Тогда тест T' , содержащий наборы теста T функции $f|_{x_k=0}$ ($f|_{x_k=1}$) с добавленными компонентами $x_k = 0$ ($x_k = 1$) и наборами из строки 1 (строки 2) таблицы

А.2 является проверяющим тестом для функции f на множестве всех неповторных в B_{unate}^+ функций, существенно зависящих от n переменных.

Доказательство. Функция f отличается от всех неповторных в B_{unate}^+ функций, не совпадающих с ней на подкубе $x_k = 0$, при помощи теста для функции $f|_{x_k=0}$, а от совпадающих – на константной подстановке $\tilde{\beta}$ из леммы 3.1.

Верхними нулями и нижними единицами функции $(x_1 \vee \dots \vee x_k) \& x_{k+1}$ являются следующие наборы: верхние нули: $(0, \dots, 0, 1)$, $(1, \dots, 1, 0)$, нижние единицы: $(1, 0, \dots, 0, 1)$, $(0, 1, \dots, 0, 1)$, $\dots$, $(0, \dots, 0, 1, 1)$. При этом $x_k = 1$ только на двух из этих наборов. Для функции f эти наборы имеют вид $(1, \dots, 1, 0, \beta_{k+2}, \dots, \beta_n)$ и $(0, \dots, 0, 1, 1, \beta_{k+2}, \dots, \beta_n)$. В силу однозначного задания монотонной функции множеством верхних нулей и нижних единиц по лемме 3.1 указанных двух наборов достаточно, чтобы отличить f от функций, совпадающих с ней на подкубе $x_k = 0$. Таким образом, тест, состоящий из двух этих наборов и теста для функции $f|_{x_k=0}$ с добавленными компонентами $x_k = 0$, является тестом для f . Лемма доказана.

Замечание 3.1. [26] Пусть даны монотонные функции $g(x_1, \dots, x_n)$ и $g'(x_1, \dots, x_n)$. Пусть они совпадают на множестве верхних нулей и множестве нижних единиц функции $g(x_1, \dots, x_n)$. Тогда функции $g(x_1, \dots, x_n)$ и $g'(x_1, \dots, x_n)$ равны.

Утверждение 3.1. [26, 25, 13] Пусть функция $f(x_1, \dots, x_n)$, существенно зависящая от своих переменных и неповторная в базисе B , состоящем из $\&, \vee$ и специальной функции g , содержит подфункцию $g(x_1, \dots, x_s)$, где $s \geq 3$. Тогда дерево этой функции содержит вершину, помеченную g , а переменные $x_1, \dots, x_s$ лежат в разных поддеревьях над ней либо в прямом порядке от 1 до s , либо в любом эквивалентном порядке, задаваемом определением содержащего g канонического дерева.

Доказательство. От противного. Возможны три случая.

- Дерево функции f не содержит вершины, помеченной g , выше которой находятся листья, помеченные переменными $x_1, \dots, x_s$. Тогда применение константной подстановки, на которой f обращается в g , к дереву функции f , дает неповторное в $\{\&, \vee\}$ дерево функции g , что противоречит повторности g .
- Дерево функции f содержит вершину, помеченную g , выше которой находятся поддеревья, содержащие листья, помеченные переменными $x_1, \dots, x_s$, некоторые из которых находятся в одних и тех же поддеревьях. Тогда одно из поддеревьев над этой вершиной не содержит ни одной из данных переменных. На константной подстановке, на которой f обращается в $g(x_1, \dots, x_s)$, это дерево обратится в константу, что также означает существование неповторного в $\{\&, \vee\}$ дерева функции g .

- Дерево функции f содержит вершину, помеченную g , выше которой в разных поддеревьях находятся листья, помеченные переменными $x_1, \dots, x_s$, в порядке, не эквивалентном прямому. Тогда при любой константной подстановке на места остальных переменных получится функция $g(x_{i_1}, \dots, x_{i_s})$, не равная $g(x_1, \dots, x_s)$.

Следовательно, дерево функции f содержит вершину, помеченную g , а переменные $x_1, \dots, x_s$ лежат в разных поддеревьях над ней либо в прямом порядке от 1 до s , либо в любом эквивалентном порядке.

Лемма 3.3. [26, 25, 13] Пусть бесповторная в B_{unate}^+ функция $h(z_1, z_{s+1}, \dots, z_n)$ существенно зависит от $n - s + 1 \geq 2$ переменных, где $s \geq 3$, 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:

$$f'(x_1, \dots, x_s, \beta_{s+1}, \dots, \beta_n) = g(x_1, \dots, x_s), \quad (3.2)$$

то $f' = f$.

Доказательство. Пусть D – каноническое дерево функции f . Обозначим через v вершину, помеченную $g(x_1, \dots, x_s)$. По условиям

леммы выше нее только листья и она смежна с внутренней вершиной u , помеченной дизъюнкцией или специальной функцией. Корень дерева функции $g|_{x_1=0}$ (см. таблицу А.2) помечен конъюнкцией, что не совпадает с пометкой вершины u . Поэтому дерево, полученное из D заменой поддерева в вершине v на каноническое дерево функции $g|_{x_1=0}$, является каноническим по определению.

Так как $x_1 = 0$ – незабывающая подстановка для функции g (см. таблицу А.2), то $f|_{x_1=0}$ существенно зависит от $n - 1$ переменных по лемме о неповторной суперпозиции [31, с. 32]. Обозначим через D_0 дерево этой функции.

Обозначим через D' каноническое дерево функции f' . Так как выполнено равенство (3.2), то по утверждению 3.1 дерево D' содержит вершину v' помеченную функцией g и листьями $x_1, \dots, x_s$, лежащими в разных поддеревьях над ней. Следовательно, v' – первая общая на пути к корню вершина у листьев $x_1, \dots, x_s$ в дереве D' .

Соответственно, после подстановки $x_1 = 0$ дерево D' превращается в дерево D_0 и содержит дерево подфункции $g|_{x_1=0}$, а первой общей на пути к корню вершиной у листьев $x_2, \dots, x_s$ остается v' . Но в D_0 у листьев $x_2, \dots, x_s$ первая общая на пути к корню вершина – это v . Следовательно, v совпадает с v' , с вершиной v' смежны листья $x_2, \dots, x_s$, и все части деревьев D и D' , кроме, быть может, поддеревьев в вершинах v и v' , совпадают. Поскольку $f = f'$ на подстановке $x_{s+1} = \beta_{s+1}, \dots, x_n = \beta_n$ в силу равенства (3.2), поддеревья в вер-

шинах v и v' соответствуют одной и той же функции $g(x_1, \dots, x_s)$. Таким образом, канонические деревья D и D' эквивалентны и $f = f'$. Лемма доказана.

Лемма 3.4. [26, 13] *Пусть неповторная в базисе B_{unate}^+ функция $h(z_1, z_5, \dots, z_n)$ существенно зависит от $n - 4$ переменных, где $n > 4$, и лист, который помечен переменной z_1 , входит в вершину u , помеченную дизъюнкцией или специальной функцией. Пусть функция f зависит от переменных $x_1, \dots, x_n$, и для f и h выполнены следующие равенства:*

$$f(x_1, \dots, x_n) = h(f_4(x_1, x_2, x_3, x_4), x_5, \dots, x_n), \quad (3.3)$$

$$h(z_1, \beta_5, \dots, \beta_n) = z_1. \quad (3.4)$$

Тогда тест T' , содержащий наборы теста T функции $f|_{x_1=0}$ с добавлением компоненты $x_1 = 0$ и наборы $(1, 1, 0, 0, \beta_5, \dots, \beta_n)$, $(1, 0, 1, 0, \beta_5, \dots, \beta_n)$, $(1, 0, 0, 1, \beta_5, \dots, \beta_n)$, является проверяющим тестом для функции f на множестве всех неповторных в B_{unate}^+ функций, существенно зависящих от n переменных.

Доказательство. Рассмотрим неповторную в B_{unate}^+ функцию $f'(x_1, \dots, x_n)$, совпадающую с f на T' . Тогда в силу совпадения на наборах теста T верно $f'|_{x_1=0} = f|_{x_1=0}$.

Из условий (3.3), (3.4) следует равенство

$$f(x_1, x_2, x_3, x_4, \beta_5, \dots, \beta_n) = f_4(x_1, x_2, x_3, x_4).$$

Рассмотрим функцию $g(x_1, x_2, x_3, x_4) = f'(x_1, x_2, x_3, x_4, \beta_5, \dots, \beta_n)$. Так как f' совпадает с f на подкубе $x_1 = 0$, то $g(0, x_2, x_3, x_4) = f_4(0, x_2, x_3, x_4)$. По построению теста T' :

$$g(1, 1, 0, 0) = f'(1, 1, 0, 0, \beta_5, \dots, \beta_n) = f(1, 1, 0, 0, \beta_5, \dots, \beta_n) = f_4(1, 1, 0, 0) = 1,$$

$$g(1, 0, 1, 0) = f'(1, 0, 1, 0, \beta_5, \dots, \beta_n) = f(1, 0, 1, 0, \beta_5, \dots, \beta_n) = f_4(1, 0, 1, 0) = 0,$$

$$g(1, 0, 0, 1) = f'(1, 0, 0, 1, \beta_5, \dots, \beta_n) = f(1, 0, 0, 1, \beta_5, \dots, \beta_n) = f_4(1, 0, 0, 1) = 0,$$

$$g(1, 0, 1, 1) > g(0, 0, 1, 1) = f_4(0, 0, 1, 1) = 1 \Rightarrow g(1, 0, 1, 1) = 1.$$

Так как множество наборов $(1, 1, 0, 0)$, $(1, 0, 1, 0)$, $(1, 0, 0, 1)$, $(1, 0, 1, 1)$ является множеством верхних нулей и нижних единиц $f_4(1, x_2, x_3, x_4)$, то по замечанию 3.1 выполнено равенство $g(x_1, x_2, x_3, x_4) = f_4(x_1, x_2, x_3, x_4)$. Тогда для f' выполнено равенство (3.2) и по лемме 3.3 функция f' равна f .

Лемма 3.5. [26, 13] Пусть неповторная в базисе B_{unate}^+ функция $h(z_1, z_6, \dots, z_n)$ существенно зависит от $n - 5$ переменных, где $n > 5$, и лист, который помечен переменной z_1 , входит в вершину u , помеченную дизъюнкцией или специальной функцией. Пусть функция f зависит от переменных $x_1, \dots, x_n$, и для f и h выполне-

ны следующие равенства:

$$f(x_1, \dots, x_n) = h(f_5(x_1, x_2, x_3, x_4, x_5), x_6, \dots, x_n), \quad (3.5)$$

$$h(z_1, \beta_6, \dots, \beta_n) = z_1. \quad (3.6)$$

Тогда тест T' , содержащий наборы теста T функции $f|_{x_1=0}$ с добавлением компоненты $x_1 = 0$ и наборы $(1, 1, 0, 0, 0, \beta_6, \dots, \beta_n)$, $(1, 0, 0, 1, 0, \beta_6, \dots, \beta_n)$, $(1, 0, 1, 0, 1, \beta_6, \dots, \beta_n)$ и $(1, 0, 1, 1, 0, \beta_6, \dots, \beta_n)$ является проверяющим тестом для функции f на множестве всех неповторных в B_{unate}^+ функций, существенно зависящих от n переменных.

Доказательство. Рассмотрим неповторную в B_{unate}^+ функцию $f'(x_1, \dots, x_n)$, совпадающую с f на T' . Тогда в силу совпадения на наборах теста T верно $f'|_{x_1=0} = f|_{x_1=0}$.

Из условий (3.5), (3.6) следует равенство

$$f(x_1, x_2, x_3, x_4, x_5, \beta_6, \dots, \beta_n) = f_4(x_1, x_2, x_3, x_4, x_5).$$

Рассмотрим функцию

$$g(x_1, x_2, x_3, x_4, x_5) = f'(x_1, x_2, x_3, x_4, x_5, \beta_6, \dots, \beta_n).$$

Так как f' совпадает с f на подкубе $x_1 = 0$, то $g(0, x_2, x_3, x_4, x_5) = f_5(0, x_2, x_3, x_4, x_5)$. По построению теста T' :

$$\begin{aligned} g(1, 1, 0, 0, 0) &= f'(1, 1, 0, 0, 0, \beta_6, \dots, \beta_n) = \\ &= f(1, 1, 0, 0, 0, \beta_6, \dots, \beta_n) = f_5(1, 1, 0, 0, 0) = 1, \end{aligned}$$

$$\begin{aligned}
g(1, 0, 0, 1, 0) &= f'(1, 0, 0, 1, 0, \beta_6, \dots, \beta_n) = \\
&= f(1, 0, 0, 1, 0, \beta_6, \dots, \beta_n) = f_5(1, 0, 0, 1, 0) = 0, \\
g(1, 0, 1, 0, 1) &= f'(1, 0, 1, 0, 1, \beta_6, \dots, \beta_n) = \\
&= f(1, 0, 1, 0, 1, \beta_6, \dots, \beta_n) = f_5(1, 0, 1, 0, 1) = 0, \\
g(1, 0, 1, 1, 0) &= f'(1, 0, 1, 1, 0, \beta_6, \dots, \beta_n) = \\
&= f(1, 0, 1, 1, 0, \beta_6, \dots, \beta_n) = f_5(1, 0, 1, 1, 0) = 1, \\
g(1, 0, 0, 1, 1) &\geq g(0, 0, 0, 1, 1) = f_5(0, 0, 0, 1, 1) = 1 => \\
&=> g(1, 0, 0, 1, 1) = 1.
\end{aligned}$$

Так как множество наборов $(1, 1, 0, 0, 0)$, $(1, 0, 0, 1, 0)$, $(1, 0, 1, 0, 1)$, $(1, 0, 0, 1, 1)$ и $(1, 0, 1, 1, 0)$ является множеством верхних нулей и нижних единиц $f_5(1, x_2, x_3, x_4, x_5)$, то по замечанию 3.1 выполнено равенство $g(x_1, x_2, x_3, x_4, x_5) = f_5(x_1, x_2, x_3, x_4, x_5)$. Тогда для f' выполнено равенство (3.2) и по лемме 3.3 функция f' равна f .

Лемма 3.6. [26, 25, 13] *Пусть неповторная в базисе B_{unate}^+ функция $h(z_1, z_{s+1}, \dots, z_n)$ существенно зависит от $n - s + 1$ переменных, где $n > s \geq 3$, и лист, который помечен переменной z_1 , входит в вершину u , помеченную дизъюнкцией или специальной функцией.*

Пусть функция f зависит от переменных $x_1, \dots, x_n$, и для f и h выполнены следующие равенства:

$$f(x_1, \dots, x_n) = h(f_m^s(x_1, \dots, x_s), x_{s+1}, \dots, x_n), \quad (3.7)$$

$$h(z_1, \beta_{s+1}, \dots, \beta_n) = z_1. \quad (3.8)$$

Тогда тест T' , содержащий наборы теста T функции $f|_{x_1=0}$ с добавлением компоненты $x_1 = 0$, и наборов $(1, 0, \dots, 0, \beta_{s+1}, \dots, \beta_n)$, $(1, 1, 0, \dots, 0, \beta_{s+1}, \dots, \beta_n)$, $(1, 0, 1, \dots, 0, \beta_{s+1}, \dots, \beta_n)$, $\dots$, $(1, 0, \dots, 0, 1, \beta_{s+1}, \dots, \beta_n)$, является проверяющим тестом для функции f на множестве всех неповторных в B_{unate}^+ функций, существенно зависящих от n переменных.

Доказательство. Рассмотрим неповторную в B_{unate}^+ функцию $f'(x_1, \dots, x_n)$, совпадающую с f на T' . Тогда в силу совпадения на наборах теста T верно $f'|_{x_1=0} = f|_{x_1=0}$.

Из условий (3.7), (3.8) следует равенство

$$f(x_1, \dots, x_s, \beta_{s+1}, \dots, \beta_n) = f_m^s(x_1, \dots, x_s).$$

Рассмотрим функцию $g(x_1, \dots, x_s) = f'(x_1, \dots, x_s, \beta_{s+1}, \dots, \beta_n)$. Так как f' совпадает с f на подкубе $x_1 = 0$, то $g(0, x_2, \dots, x_s) = f_m^s(0, x_2, \dots, x_s)$.

По построению теста T' :

$$g(1, 0, \dots, 0) = f'(1, 0, \dots, 0, \beta_{s+1}, \dots, \beta_n) =$$

$$\begin{aligned}
&= f(1, 0, \dots, 0, \beta_{s+1}, \dots, \beta_n) = f_m^s(1, 0, \dots, 0) = 0, \\
&g(1, 1, 0, \dots, 0) = f'(1, 1, 0, \dots, 0, \beta_{s+1}, \dots, \beta_n) = \\
&= f(1, 1, 0, \dots, 0, \beta_{s+1}, \dots, \beta_n) = f_m^s(1, 1, 0, \dots, 0) = 1, \\
&g(1, 0, 1, \dots, 0) = f'(1, 0, 1, \dots, 0, \beta_{s+1}, \dots, \beta_n) = \\
&= f(1, 0, 1, \dots, 0, \beta_{s+1}, \dots, \beta_n) = f_m^s(1, 0, 1, \dots, 0) = 1, \\
&\dots \\
&g(1, 0, \dots, 0, 1) = f'(1, 0, \dots, 0, 1, \beta_{s+1}, \dots, \beta_n) = \\
&= f(1, 0, \dots, 0, 1, \beta_{s+1}, \dots, \beta_n) = f_m^s(1, 0, \dots, 0, 1) = 1.
\end{aligned}$$

Так как множество наборов $(1, 0, \dots, 0)$, $(1, 1, 0, \dots, 0)$, $(1, 0, 1, \dots, 0)$, $\dots$, $(1, 0, \dots, 0, 1)$ является множеством верхних нулей и нижних единиц $f_m^s(1, x_2, \dots, x_s)$, то по замечанию 3.1 выполнено равенство $g(x_1, \dots, x_s) = f_m^s(x_1, \dots, x_s)$. Тогда для f' выполнено равенство (3.2) и по лемме 3.3 функция f' равна f .

§ 3.3. Верхние оценки длины тестов

В данном разделе будет установлена связь тестов относительно неповторной альтернативы в элементарном базисе, расширенном специальными функциями, с проверяющими тестами в соответствующих базисах без отрицания и показано, что добавление в элементарный базис всех специальных функций оставляет функцию Шеннона линейной с мультипликативной константой 3.

Лемма 3.7. [13, 12] *Справедливо неравенство*

$$T_{unate}(n) \leq T_{unate}^+(n) + 2n.$$

Доказательство. Задача тестирования относительно бесповторной альтернативы функции $f(x_1, \dots, x_n)$ в базисе B_{unate} сводится к проверяющему тестированию в базисе B_{unate}^+ функции, получаемой из f заменой антимонотонных переменных на их отрицания. При этом требуется для каждой переменной добавить пару соседних по ней наборов, на которых функция принимает различные значения.

Лемма доказана.

Теорема 3.1. [13] *Справедливо неравенство*

$$T_{unate}^+(n) \leq 3n - 4 \text{ при } n \geq 2.$$

Доказательство. Построим тест для функции $f(x_1, \dots, x_n)$, применяя последовательно леммы 3.2 и 3.4–3.6. Построенный тест будем обозначать T_A . Длина теста T_A не уменьшится, если все пометки f_4 заменить на f_m^4 , а пометки f_5 заменить на f_m^5 в дереве функции f . Поэтому $|T_A(f(x_1, \dots, x_n))| \leq F_A(u_1, \dots, u_l)$, где $u_1, \dots, u_l$ – набор натуральных чисел, определяемый степенями захода вершин дерева. Каждой вершине, помеченной дизъюнкцией или конъюнкцией, соответствует набор из $t - 1$ единиц, где t – степень захода вершины, а каждой вершине, помеченной специальной функцией – число $t - 1$. При этом получается, что $u_1 + \dots + u_l = n - 1$.

Функционал F_A обладает следующими свойствами.

1. $F_A(1, u_2, \dots, u_l) = F_A(u_2, u_3, \dots, u_l) + 2$; при этом $F_A(1) = 2$.
2. $F_A(u_1, u_2, \dots, u_l) = F_A(\underbrace{1, \dots, 1}_{u_1-1}, u_2, \dots, u_l) + u_1 + 1$.

Из этих свойств следует:

$$F_A(u_1 + u_2, \dots, u_l) = F_A(u_1, u_2, \dots, u_l) + 1.$$

Поэтому

$$\max_{u_1 + \dots + u_l = n-1} F_A(u_1, \dots, u_l) = F_A(n-1),$$

$$F_A(n-1) = n + F_A(\underbrace{1, \dots, 1}_{n-2}) \leq n + 2(n-2) = 3n-4.$$

Таким образом, длина теста T_A не превосходит $3n-4$. Так как $T_{unate}^+(n) \leq T_A$, то $T_{unate}^+(n) \leq 3n-4$. Теорема доказана.

Теорема 3.2. [13] *Справедливо неравенство*

$$T_{unate}(n) \leq 3n-2 \text{ при } n \geq 2.$$

Доказательство. По теореме 3.1 и лемме 3.7 при $n \geq 2$ справедливо неравенство $T_{unate}(n) \leq 5n-4$.

Не ограничивая общности рассуждений, можем считать тестируемую функцию $f(x_1, \dots, x_n)$ монотонной. При этом обозначим $M_n, \dots, M_2$ множества наборов, добавляемые на каждом шаге алгоритма теоремы 3.1 в тест функции f , а через M_1 — полный тест для функции последней переменной. Заметим, что $M_n \cup \dots \cup M_2 = T_A$.

Докажем от противного, что множество $M_n \cup \dots \cup M_1$ – тест относительно неповторной альтернативы для функции f . Предположим, что $f(x_1, \dots, x_n)$ – функция с минимальным числом аргументов, для которой это не так. Тогда $M_{n-1} \cup \dots \cup M_1$ – тест для $f_{x_1=\alpha}$.

Таблица А.1 показывает существенность переменной x_1 во всех возможных случаях. Множество наборов $M_n \cup \dots \cup M_1$ содержит по построению T_A – проверяющий тест для функции в базисе B_{unate}^+ . Так как $x_1 = \alpha$ – забывающая подстановка для f , то $M_{n-1} \cup \dots \cup M_1$ показывает существенность оставшихся переменных. То есть $M_n \cup \dots \cup M_1$ является тестом для функции f . Противоречие. При этом

$$|M_n \cup \dots \cup M_1| \leq |T_A| + |M_1| \leq 3n - 2.$$

Теорема доказана.

Заключение

В главе 2 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. 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. Показано, что добавление в элементарный базис любой слабоповторной функции приводит к существенному увеличению длины сертификата повторности. Получены верхняя и нижняя полиномиальные оценки функции Шеннона для длины сертификата повторности в базисе всех функций l переменных. Также с применением полученных верхних оценок длин сертификатов можно получить новые оценки сложности в классической модели обучения с помощью запросов принадлежности и эквивалентности. В главе 3 установлено, что добавление в элементарный базис всех монотонных функций Стеценко оставляет линейной верхней оценкой функции Шеннона для длины теста относительно неповторной альтернативы с мультипликативной константой 3. Тем самым установлено от-

существование существенной связи между сложностью 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 добавок к элементарному некоторую слабоповторную функцию. Остается нерешенным вопрос о длине минимального теста относительно неповторной альтернативы при расширении элементарного базиса дискриминирующей функцией. Кроме этого, интересен вопрос о возможности нелинейного роста длины теста относительно неповторной альтернативы при добавлении иных монотонных функций.

Приложение А

Таблицы

Таблица А.1

Наборы, на которых показывается существенность x_1

№	Значение подфункции $f_{x_1=\alpha}$	Значение из M_n
1	$f(0, 0, \dots, 0, 1, \beta_{k+2}, \dots, \beta_n) = (0 \vee \dots \vee \vee 0) \& 1 = 0$	$f(1, 0, \dots, 0, 1, \beta_{k+2}, \dots, \beta_n) = 1$
2	$f(1, 1, \dots, 1, 0, \beta_{k+2}, \dots, \beta_n) = (1 \& \dots \& 1) \vee \vee 0 = 1$	$f(0, 1, \dots, 1, 0, \beta_{k+2}, \dots, \beta_n) = 0$
3	$f(0, 1, 0, 0, \beta_5, \dots, \beta_n) = f_4(0, 1, 0, 0) = 0$	$f(1, 1, 0, 0, \beta_5, \dots, \beta_n) = 1$
4	$f(1, 0, 1, 1, \beta_5, \dots, \beta_n) = f_4(1, 0, 1, 1) = 1$	$f(0, 0, 1, 1, \beta_5, \dots, \beta_n) = 0$
5	$f(0, 1, 0, 0, 0, \beta_6, \dots, \beta_n) = f_5(0, 1, 0, 0, 0) = 0$	$f(1, 1, 0, 0, 0, \beta_6, \dots, \beta_n) = 1$
6	$f(1, 1, 0, 0, 1, \beta_6, \dots, \beta_n) = f_5(1, 1, 0, 0, 1) = 1$	$f(0, 1, 0, 0, 1, \beta_6, \dots, \beta_n) = 0$
7	$f(0, 1, 0, \dots, 0, \beta_{s+2}, \dots, \beta_n) = f_m^s(0, 1, 0, \dots, 0) = 0$	$f(1, 1, 0, \dots, 0, \beta_{s+1}, \dots, \beta_n) = 1$
8	$f(1, 0, 1, \dots, 1, \beta_{s+2}, \dots, \beta_n) = f_m^s(1, 0, 1, \dots, 1) = 1$	$f(0, 0, 1, \dots, 1, \beta_{s+1}, \dots, \beta_n) = 0$

Подстановка $f|_{x_1=\alpha}$ для вершины v

№	Пометка v	α	Изменение дерева	Наборы для теста
1	$x_1 \vee \dots \vee x_k$	0	В D удаляется лист x_1 и при $k = 2$ вершина v заменяется на лист x_2	$f(1, 1, \dots, 1, 0, \beta_{k+2}, \dots, \beta_n) = 0$ $f(1, 0, \dots, 0, 1, \beta_{k+2}, \dots, \beta_n) = 1$
2	$x_1 \& \dots \& x_k$	1	В D удаляется лист x_1 и при $k = 2$ вершина v заменяется на лист x_2	$f(0, 0, \dots, 0, 1, \beta_{k+2}, \dots, \beta_n) = 1$ $f(0, 1, \dots, 1, 0, \beta_{k+2}, \dots, \beta_n) = 0$
3	f_4	0	Поддерево в вершине v заменяется на дерево функции $x_3(x_2 \vee x_4)$	$f(1, 1, 0, 0, \beta_5, \dots, \beta_n) = 1,$ $f(1, 0, 1, 0, \beta_5, \dots, \beta_n) = 0,$ $f(1, 0, 0, 1, \beta_5, \dots, \beta_n) = 0$
4	f_4	1	Поддерево в вершине v заменяется на дерево функции $x_2 \vee x_3 x_4$	$f(0, 0, 1, 1, \beta_5, \dots, \beta_n) = 1,$ $f(0, 1, 0, 1, \beta_5, \dots, \beta_n) = 0,$ $f(0, 1, 1, 0, \beta_5, \dots, \beta_n) = 1$
5	f_5	0	Поддерево в вершине v заменяется на дерево функции $x_5(x_2 \vee x_3 x_4)$	$f(1, 1, 0, 0, 0, \beta_6, \dots, \beta_n) = 1,$ $f(1, 0, 0, 1, 0, \beta_6, \dots, \beta_n) = 0,$ $f(1, 0, 1, 0, 1, \beta_6, \dots, \beta_n) = 0,$ $f(1, 0, 1, 1, 0, \beta_6, \dots, \beta_n) = 1$
6	f_5	1	Поддерево в вершине v заменяется на дерево функции $x_2 \vee x_4(x_3 \vee x_5)$	$f(0, 1, 1, 1, 0, \beta_6, \dots, \beta_n) = 0,$ $f(0, 1, 1, 0, 1, \beta_6, \dots, \beta_n) = 1,$ $f(0, 1, 0, 0, 1, \beta_6, \dots, \beta_n) = 0,$ $f(0, 0, 0, 1, 1, \beta_6, \dots, \beta_n) = 1$
7	f_m^s	0	Поддерево в вершине v заменяется на дерево функции $x_2 \& \dots \& x_s$	$f(1, 0, 0, \dots, 0, \beta_{s+1}, \dots, \beta_n) = 0,$ $f(1, 1, 0, \dots, 0, \beta_{s+1}, \dots, \beta_n) = 1,$ $f(1, 0, 1, \dots, 0, \beta_{s+1}, \dots, \beta_n) = 1$... $f(1, 0, \dots, 0, 1, \beta_{s+1}, \dots, \beta_n) = 1$
8	f_m^s	1	Поддерево в вершине v заменяется на дерево функции $x_2 \vee \dots \vee x_s$	$f(0, 1, 1, \dots, 1, \beta_{s+1}, \dots, \beta_n) = 1,$ $f(0, 0, 1, \dots, 1, \beta_{s+1}, \dots, \beta_n) = 0,$ $f(0, 1, 0, \dots, 1, \beta_{s+1}, \dots, \beta_n) = 0,$... $f(0, 1, \dots, 1, 0, \beta_{s+1}, \dots, \beta_n) = 0$

Приложение Б

Процедуры

Процедура 1 [24]

Дано: разнозначная $(0,1)$ -матрица M с $n > 2s - 4$ столбцами и $k < \frac{n}{2} - s + 1$ строками, имеющая и строки с 0-преобладанием, и строки с 1-преобладанием. Пусть первая строка матрицы имеет 0-преобладание, а вторая – 1-преобладание. Пусть C – множество всех столбцов матрицы. Получим из него три множества C_1, C_2, C_3 столбцов, а множество всех строк матрицы разобьем на два множества строк R_1, R_2 следующим образом.

1. Положим $C_1 = C_2 = C_3 = R_1 = R_2 = \emptyset$.
2. До тех пор, пока в C_3 меньше $s - 2$ столбца и пока не кончились строки, последовательно рассмотрим каждую строку, начиная с первой. Добавим рассматриваемую строку в R_1 . Возможны четыре случая.
 - (а) Строка имеет 1-преобладание и не имеет нулей на столбцах из C_3 . Тогда у нее есть ноль на каком-то столбце из C . Переместим этот столбец из C в C_3 .
 - (б) Строка имеет 0-преобладание, у нее нет единиц ни на одном столбце из C_3 или C_3 пусто. Тогда в C есть столбец, на котором она равна единице. Переместим его из C в C_3 .

- (с) C_3 непусто, строка имеет 0-преобладание и у нее есть единица на каком-то столбце из C_3 . Тогда в C есть столбец, на котором она равна нулю, так как $s - 2$ столбца – это меньше половины всех столбцов, а на строке с 0-преобладанием не менее половины столбцов равны нулю. Переместим его из C в C_3 .
- (d) Если не выполняются условия пунктов (а)–(с), то операции не производятся.

По результатам рассмотрения t строк добавлено не более t столбцов.

3. Если закончились строки и $|C_3| < s - 2$, то переместим еще несколько произвольных столбцов из C в C_3 , чтобы в C_3 стало $s - 2$ столбца.
4. Обозначим $x_1, \dots, x_{s-2}$ столбцы из C_3 . Если остались нерассмотренные строки, то для каждой из них сделаем следующее: если у строки есть особенное значение на каком-то столбце из C , то переместим его из C в C_3 . Если особые значения у строки есть только на столбцах $x_1, \dots, x_{s-2}$, то добавим эту строку в R_1 . При этом $|C_3| \leq k$.
5. Добавим в R_2 все строки матрицы, не вошедшие в R_1 .
6. Первая рассмотренная в пункте 2 строка имеет 0-преобладание.

Тогда она равна единице на каком-то из столбцов $x_1, \dots, x_{s-2}$, согласно случаю b) шага 2. Строка содержит больше половины нулей, а на предыдущих шагах из C было удалено меньше половины столбцов: $n - |C_3| \geq n - k > \frac{n}{2}$, поэтому существует хотя бы один столбец в C , на котором она равна нулю. Переместим его из C в C_1 .

7. Рассмотрим последовательно строки из R_1 , имеющие 1-преобладание. Строка содержит больше половины единиц, а на предыдущих шагах из C было удалено меньше половины столбцов: $n - |C_3| - 1 \geq n - k - 1 > \frac{n}{2}$, поэтому остался хотя бы один столбец с единицей либо в C_2 , либо в C . Если таких столбцов нет в C_2 , то таковой найдется в C . Переместим его из C в C_2 .
8. Рассмотрим последовательно все остальные строки из R_1 , не рассмотренные на шагах 6–7. Они имеют 0-преобладание. Если у рассматриваемой строки нет нулей ни на каком столбце из C_1 , то либо в C существует хотя бы один столбец с нулем в этой строке, либо в C остались только столбцы с единицами в этой строке. Если первое, то переместим столбец с нулем в этой строке из C в C_1 , если второе – то переместим любой столбец из C в C_2 .

Множества C_1 и C_2 непусты, так как на шаге 6 для первой строки матрицы один столбец добавлен в C_1 , а для второй строки на

шаге 7 один столбец добавлен в C_2 . Так как каждой строки из R_1 было взято не более одного столбца, то $|C_1| + |C_2| \leq |R_1|$. Процедура окончена.

П р о ц е д у р а 2 [24]

Дано: разнозначная матрица M с $n > 2s-4$ столбцами и $k < \frac{n}{2} - s + 1$ строками, имеющими 0-преобладание. Пусть C – множество всех столбцов матрицы. Получим из него два множества C_1, C_2 столбцов и множество строк R_1 следующим образом.

1. Положим $C_1 = C_2 = \emptyset$.
2. Обозначим первые $s - 2$ столбца матрицы $x_1, \dots, x_{s-2}$.
3. Последовательно для каждой строки, равной нулю на всех этих столбцах, сделаем следующее: так как матрица разнозначная и C_1 пусто, то либо в C_2 , либо в C есть столбец с единицей в этой строке. Если такого столбца нет в C_2 , то переместим один такой столбец из C в C_2 .
4. Последовательно для каждой строки, у которой есть единица на каком-то из столбцов $x_1, \dots, x_{s-2}$, сделаем следующее: так как количество строк с нулями во всех этих столбцах не превосходит общего количества строк, то количество выбранных на предыдущем шаге столбцов меньше половины всех столбцов матрицы. Поэтому либо в C , либо в C_1 у рассматриваемой строки существует столбец, на котором она равна нулю. Если

такого столбца нет в C_1 , то переместим один такой столбец из C в C_1 .

5. Если C_1 или C_2 пусто, то добавим туда любой столбец из C . Это возможно, так как количество выбранных столбцов не превосходит k , а значит меньше n .
6. Отметим, что в пунктах (3),(4) мы рассмотрели все строки. Положим R_1 равным множеству всех строк.

Процедура окончена.

П р о ц е д у р а 3 [24]

Дано: разнозначная матрица M с $n > 2s-4$ столбцами и $k < \frac{n}{2} - s + 1$ строками, имеющими 1-преобладание. Пусть C – множество всех столбцов матрицы, а C_1, C_2 – два множества столбцов.

- 1 Положим $C_1 = C_2 = \emptyset$.
- 2 Обозначим первые $s-2$ столбца матрицы $x_1, \dots, x_{s-2}$.
- 3 Последовательно для каждой строки, равной единице на всех этих столбцах, сделаем следующее. Так как матрица разнозначная и C_2 пусто, то либо в C_1 , либо в C , есть столбец с нулем в этой строке. Если такого столбца нет в C_1 , то переместим один такой столбец из C в C_1 .
- 4 Последовательно для каждой строки, у которой есть ноль на каком-то из столбцов $x_1, \dots, x_{s-2}$, сделаем следующее: так как

количество строк с единицами во всех этих столбцах не превосходит общего количества строк, то количество выбранных на предыдущем шаге столбцов меньше половины всех столбцов матрицы. Поэтому либо в C , либо в C_2 у рассматриваемой строки существует столбец, на котором она равна единице. Если такого столбца нет в C_2 , то переместим один такой столбец из C в C_2 .

5 Если C_1 или C_2 пусто, то добавим туда любой столбец из C . Это возможно, так как количество выбранных столбцов не превосходит k , а значит меньше n .

6 Отметим, что в пунктах (3),(4) мы рассмотрели все строки. Положим R_1 равным множеству всех строк.

Процедура окончена.

Список литературы

1. АЛЕКСЕЕВ В. Б. Лекции по дискретной математике. — М.: Изд. отдел ф-та ВМК МГУ им. М. В. Ломоносова, 2017. — 90 с.
2. ВОРОНЕНКО А. А. О проверяющих тестах для неповторных функций // *Математические вопросы кибернетики*. — 2002. — Вып. 11. — С. 165–176.
3. ВОРОНЕНКО А. А. О длине проверяющего теста для неповторных функций в базисе $\{0, 1, \&, \vee, \neg\}$ // *Дискретная математика*. — 2005. — **17**. — № 2. — С. 139–143.
4. ВОРОНЕНКО А. А. О функции Шеннона для длины сертификата повторности булевых функций в одном семействе базисов // *Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн.* — 2013. — № 4. — С. 45–47.
5. ВОРОНЕНКО А. А. О сложности доказательства повторности булевых функций в бинарном базисе // *Прикладная дискретная математика*. — 2011. — № 3(13). — С. 12–16.
6. ВОРОНЕНКО А. А. Распознавание неповторности в произвольном базисе. // *Прикладная математика и информатика. Вып. 23*. — М.: МАКС Пресс, 2006. — С. 67–84.
7. ВОРОНЕНКО А. А. О тестировании неповторных функций // *Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн.* — 2006. — № 2. — С. 45–48.

8. ВОРОНЕНКО А. А. Методы представления дискретных функций в задачах подсчета, тестирования и распознавания свойств: Дис. ... д.ф.-м.н. : 01.01.09 — М., 2007. — 154 с.
9. ВОРОНЕНКО А. А. Использование неповторных представлений // *Синтаксис и семантика логических систем: Материалы российской школы-семинара.* — Дальнаука ДВО РАН г. Владивосток, 2008. — С. 35–36.
10. 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.
11. ВОРОНЕНКО А. А., КАФТАН Д. В. О длине сертификата повторности в базисе всех функций l переменных // *Прикладная математика и информатика. Вып. 44.* — М.: МАКС Пресс, 2013. — С. 95–102.
(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.)
12. ВОРОНЕНКО А. А., КАФТАН Д. В. Тестирование поляризуемых функций // *Материалы XIII Международного семинара “Дискретная математика и ее приложения” имени академика О.Б. ЛУПАНОВА.* — М.: Изд-во механико-математическо-

- го факультета МГУ, Т.1, 2019. — С. 119–121.
13. ВОРОНЕНКО А. А., КАФТАН Д. В. Тестирование неповторных функций в элементарном базисе, расширенном всеми поляризуемыми слабоповторными функциями // *Интеллектуальные системы. Теория и приложения*. — 2021. — **25**. — № 3. — С. 75–82.
 14. ВОРОНЕНКО А. А., КАФТАН Д. В. Тестирование неповторных функций в поляризуемых предэлементарных базисах // *Материалы семинара конференции “Проблемы теоретической кибернетики”*. — Казань: Отечество, 2021. — С. 29–31.
 15. ВОРОНЕНКО А. А., ФЕДОРОВА В. С., ЧИСТИКОВ Д. В. Повторность булевых функций в элементарном базисе // *Известия ВУЗов. Математика*. — 2011. — № 11. — С. 72–77.
 16. ВОРОНЕНКО А. А., ЧИСТИКОВ Д. В. Индивидуальное тестирование неповторных функций // *Учен. записки Казан. гос. ун-та. Сер. Физ.-матем. науки*. — 2009. — **151**. — № 2. — С. 36–44.
 17. ВОРОНЕНКО А. А., ЧИСТИКОВ Д. В. Расшифровка неповторных функций оракулом – счетчиком четности // *Прикладная математика и информатика*. — М.: МАКС Пресс, Вып. 34. 2010. — С. 93–106.
 18. ГУРВИЧ В. А. О неповторных булевых функциях // *Успехи математических наук*. — 1977. — **32**. — № 1. — С. 183–184.
 19. ГУРВИЧ В. А. Критерии неповторности функций алгебры логи-

- ки // *ДАН СССР*. — 1991. — **318**. — № 3. — С. 532–537.
20. ГУРВИЧ В. А. О нормальной форме позиционных игр // *ДАН СССР*. — 1982. — **264**. — № 1. — С. 30–33.
21. Избранные вопросы теории булевых функций. — М.: *Физматлит*, 2001. — 192 с.
22. КАФТАН Д. В. Древесное представление неповторных функций в расширенных элементарных базисах // *Известия высших учебных заведений. Поволжский регион. Физико-математические науки*. — 2017. — **3**. — № 43. — С. 37–49.
23. КАФТАН Д. В. О длине сертификата повторности в некоторых расширенных элементарных базисах // *Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн.* — 2015. — № 2. — С. 40–46.
(КАФТАН 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.)
24. 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.
25. КАФТАН Д. В. Тестирование неповторных функций в расширенном медианой элементарном базисе // *Прикладная математика и информатика. Вып. 66*. — М.: *МАКС Пресс*, 2021. — С. 104–110.

- KAFTAN D. V. Testing read-once functions in a median-augmented element basis // *Computational Mathematics and Modeling*. — 2021. — **32**. — N 2. — P.253–257.
26. КАФТАН Д. В. Тестирование неповторных функций в некоторых расширенных элементарных базисах // *Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн.* — 2021. — № 3. — С.13–19.
(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.)
27. КИРИЧЕНКО К. Д. Слабоповторные булевы функции в некоторых предэлементарных базисах // *Дискретная математика и информатика. Вып. 13.* — Иркутск: Изд-во Иркутского ун-та, 2000. — С.1–60.
28. КУДРЯВЦЕВ В. Б., ГАСАНОВ Э. Э., ДОЛОТОВА О. А., ПОГОСЯН Г. Р. Теория тестирования логических устройств. — М.: *Физматлит*, 2006. — 159 с.
29. КУЗНЕЦОВ А. В. О неповторных контактных схемах и неповторных суперпозициях функций алгебры логики // *Труды математического института АН СССР*. — 1958. — **51**. — С. 186–225.
30. ЛУПАНОВ О. Б. О сложности реализации функций алгебры логики формулами // *Проблемы кибернетики*. — 1960. — Вып. 3. — С. 61–80.

31. ЛУПАНОВ О. Б. Конспект лекций по курсу “Введение в математическую логику”. — М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2007.
32. МОРОЗОВ Е. В. О тестах относительно множественных линейных слипаний переменных в булевых функциях // *Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн.* — 2014. — №. 1. — С. 22–25.
33. МОРОЗОВ Е. В. О тестах относительно множественных монотонных симметрических слипаний переменных в булевых функциях // *Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн.* — 2014. — №. 4. — С. 20–27.
34. МОРОЗОВ Е. В. О полных тестах относительно вытесняющих неисправностей входов схем // *Вестн. Моск. ун-та. Сер. 1. Мат. Мех.* — 2015. — №. 1. — С. 55–59.
35. ОСОКИН В. В. О расшифровке монотонных булевых функций с несущественными переменными // *Дискретная математика.* — 2010. — **22**. — № 4. — С. 84–97.
36. ОСОКИН В. В. О параллельной параметро-эффективной расшифровке псевдо-булевых функций // *Интеллектуальные системы.* — 2010. — **14**. — № 1–4. — С. 429–458.
37. НОСКОВ В. Н. О сложности тестов, контролирующих работу входов логических схем // *Дискретный анализ. Вып. 27.* — Новосибирск: ИМ СО АН СССР, 1975. — С. 23–51.

38. ПЕРЯЗЕВ Н. А. Слабоповторные булевы функции в бинарном базисе // *Дискретная математика и информатика. Вып. 4.* — Иркутск: Изд-во Иркутского ун-та, 1998. — С. 1–12.
39. ПОГОСЯН Г. Р. О проверяющих тестах для логических схем. — М.: ВЦ АН СССР, 1982. — 57 с.
40. ПОПКОВ К. А. Полные диагностические тесты длины 2 для схем при инверсных неисправностях функциональных элементов// *Труды МИАН.* — 2018. — **301**. — С.219–224.
(ПОПКОВ К. А. Complete diagnostic length 2 tests for logic networks under inverse faults of logic gates. // *Discrete Mathematics and Applications.* — 2019. — **29**. — N 5. — P. 321–333.)
41. ПОПКОВ К. А. Синтез легкотестируемых схем при произвольных константных неисправностях на входах и выходах элементов // *Прикладная дискретная математика.* — 2019. — № 43. — С. 78–100.
42. ПОПКОВ К. А. Оценки функций Шеннона длин тестов замыкания для контактных схем // *Дискретная математика.* — 2020. — **32**. — Вып. 3. — С. 49–67.
43. ПОПКОВ К. А. О возможностях построения легкотестируемых контактных схем и схем из функциональных элементов: Дис. ... д.ф.-м.н. : 01.01.09 — М., 2021. — 377 с.
44. РЕДЬКИН Н. П. Надежность и диагностика схем. — М.: Изд-во МГУ, 1992. — 192 с.

45. РЕДЬКИН Н. П. Единичные проверяющие тесты для схем при инверсных неисправностях элементов // *Математические вопросы кибернетики. Вып. 12.* — М.: Физматлит, 2003. — С. 217–230.
46. РОМАНОВ Д. С. Об оценках длин минимальных тестов для логических схем: Дис. ... д.ф.-м.н. : 01.01.09 — М., 2019. — 350 с.
47. РОМАНОВ Д. С. О синтезе схем, допускающих полные проверяющие тесты константной длины относительно произвольных константных неисправностей на выходах элементов // *Дискретная математика.* — 2013. — **25**. — № 2. — С.104–120.
 ROMANOV D. S. On the synthesis of circuits admitting complete fault detection test sets of constant length under arbitrary constant faults at the outputs of the gates. // *Discrete Mathematics and Applications.* — 2013. — **23**. — N 3–4. — P. 343–362.)
48. РОМАНОВ Д. С., РОМАНОВА Е. Ю. Метод синтеза неизбыточных схем, допускающих единичные проверяющие тесты константной длины // *Дискретная математика.* — 2017. — **29**. — № 4. — С.87–105.
 (ROMANOV D. S., ROMANOVA E. YU. A method of synthesis of irredundant circuits admitting single fault detection tests of constant length. // *Discrete Mathematics and Applications.* — 2019. — **29**. — № 1. — P. 35–48.)
49. СОЛОВЬЕВ Н. А. Тесты (теория, построение, применение). — Новосибирск: Наука (Сибирское отделение), 1978. — 186 с.

50. СТЕЦЕНКО В. А. Об одном необходимом максимальном признаке для предмаксимальных базисов в P_2 // *ДАН СССР*. — 1990. — **315**. — № 6. — С. 1304–1307.
51. СТЕЦЕНКО В. А. О предплохих базисах в P_2 // *Математические вопросы кибернетики. Вып. 4*. — М.: Физматлит, 1992. — С. 139–177.
52. СУВБОТОВСКАЯ Б. А. О сравнении базисов при реализации функций алгебры логики формулами // *ДАН СССР*. — 1963. — **149**(4). — С. 784–787.
53. ЧЕГИС И. А., ЯБЛОНСКИЙ С. В. О тестах для электрических схем // *Успехи мат. наук*. — 1955. — **10**. — Вып. 4(66). — С. 182–184.
54. ЧЕГИС И. А., ЯБЛОНСКИЙ С. В. Логические способы контроля электрических схем // *Тр. матем. ин-та им. В. А. Стеклова*. — 1958. — **51**. — С. 270–360.
55. ЧЕРУХИН Д. Ю. Алгоритмический критерий сравнения булевых базисов // *Математические вопросы кибернетики. Вып. 8*. — М.: Физматлит, 1999. — С. 118–160.
56. ЧИСТИКОВ Д. В. Сложность тестирования неповторных функций: Дис. ... к.ф.-м.н. : 01.01.09 — М., 2011. — 135 с.
57. ЧИСТИКОВ Д. В. Тестирование неповторных функций в элементарном базисе // *Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн.* — 2011. — № 4. — С. 37–40

58. ЧИСТИКОВ Д. В. О связи задач диагностического и проверяющего тестирования неповторных функций // *Дискретная математика*. — 2011. — **23**. — № 1. — С. 46–50.
59. ШАРАНХАЕВ И. К. О неповторных булевых функциях в предэлементарных монотонных базисах // *Дискретная математика*. — 2009. — **21**. — № 2. — С. 88–93.
60. ШАРАНХАЕВ И. К. О булевых базисах второго яруса // *Известия ВУЗов. Математика*. — 2004. — № 3. — С. 81–82.
61. ШАРАНХАЕВ И. К. О слабоповторных булевых функциях в одном предэлементарном базисе // *Дискретный анализ и исследование операций. Сер. 1*. — 2003. — **10**. — № 2. — С. 79–101.
62. ЯБЛОНСКИЙ С. В. Некоторые вопросы надежности и контроля управляющих систем // *Математические вопросы кибернетики. Вып. 1*. — М.: Наука; Физматлит, 1988. — С. 5–25.
63. ANGLUIN D. Queries and concept learning // *Machine Learning*. — 1988. — N 2. — P. 319–342.
64. ANGLUIN D., HELLERSTEIN L., KARPINSKI M. Learning read-once formulas with queries // *Journal of the ACM*. — 1993. — **40**. — N 1. — P. 185–210.
65. ARIAS M., KHARDON R., SERVEDIO R. A. Polynomial certificates for propositional classes // *Information and Computation*. — 2006. — **204**. — N 5. — P. 816–834.
66. BLUM A., HELLERSTEIN L., LITTESTONE N. Learning in the

- presence of finitely in infinitely many irrelevant attributes // *Journal of Computer and System Sciences*. — 1995. — **50**. — N 1. — P. 32–40.
67. BSHOUTY N. H. Exact learning from an honest teacher that answers membership queries // *Theoretical Computer Science*. — 2018. — **733**. — P. 4–43.
68. BSHOUTY N. H., HANCOCK T., HELLERSTEING L. Learning arithmetic read-once formulas // *Proc. 24th ACM Symposium on Theory of Computing*. — New York: ACM, 1992. — P. 185–210.
69. CHIMEV K. Structural properties of the functions // *7-th International Conference on Discrete Mathematics and Applications*. — Bansko, Bulgaria, 2004. — P. 3–4.
70. CHISTIKOV D., FEDOROVA V., VORONENKO A. Certificates of non-membership for classes of read-once functions // *Fundamenta Informaticae*. — 2014. — **132**. — N 1. — P. 63–77.
71. DUBROVA E. V., MUZIO J. C. Testability of generalized multiple-valued Reed-Muller circuits // *Proceedings of 26th International Symposium on Multiple-Valued Logic*. — IEEE, 1996. — P. 56–61.
72. GOLDMAN S. A., KWEK S. S., SCOTT S. D. Learning from examples with unspecified attribute values // *Information and Computation*. — 2003. — **180**. — N 1. — P. 82–100.
73. GOLUMBIC M. C., GURVICH V. A. Read-once functions (book chapter). In: Y. Crama, P. L. Hammer, *Boolean Functions: Theory, Algorithms and Applications*. *Encyclopedia of Mathematics and Its*

Applications. — 2011. — **142**.

74. HANSEL G. Sur le nombre des fonctions booleenes monotones des n variables // *Comptes Rendus de l'Academie des Sciences Paris. Serie A-B.* — Paris, 1966. — **2**. — P. 1088–1090.
(АНСЕЛЬ Ж. О числе монотонных булевых функций n переменных // *Киберн. сб. Новая серия.* — М.: Мир, 1968. — Вып. 5. — С. 53–57.)
75. HEGEDŰS T. Generalized teaching dimensions and the query complexity of learning// *Proceedings of COLT.* — 1995. — P. 108–117.
76. HELLERSTEIN L., PILLAIPAKKAMNATT K., RAGHAVAN V., WILKINS D. How many queries are needed to learn?// *Journal of the ACM.* — 1996. — **43**. — N 5. — P. 840–862.
77. POST E. L. Introduction to a general theory of elementary proposition // *Amer. J. Math.* — 1921. — **43**. — N 4. — P. 163–185.
78. REDDY S. M. Easily testable realization for logic functions // *IEEE Trans. Comput.* — 1972. — **21**. — N 1. — P. 124–141.
79. SEN P., DESHPANDE A., GETOOR L. Read-once functions and query evaluation in probabilistic databases // *Proceedings of the VLDB Endowment* — 2010. — **3**:(1–2). — P. 1068–1079.
80. SHANNON C. E A symbolic analysis of relay and switching circuits // *Trans. AIEE.* — 1938. — **57**. — P. 713–723.
81. SHANNON C. E The synthesis of two-terminal switching circuits //

Bell System Technical Journal. — 1949. — **28**. — N 1. — P. 59–98.

(ШЕННОН К. Е Синтез двух полюсных переключательных схем
// *Работы по теории информации и кибернетике.* — М.: Изд-во
иностранной литературы, 1963. — С. 59–105.)

82. UEHARA R., TSUCHIDA K., WEGENER I. Optimal attribute-efficient learning of disjunction, parity, and threshold functions
// *Computational Learning Theory (Third European Conference, EuroCOLT'97 Jerusalem. Proceedings). Lecture Notes in Computer Science. Vol. 1208.* — Berlin; Heidelberg: Springer-Verlag, 1997. — P. 171–184.
83. VALIANT L. G. A theory of the learnable // *Communications of the ACM.* — 1984. — **27**. — P. 1134–1142.
84. WEISS C. D. Bounds on the length of terminal stuck-fault tests // *IEEE Trans. Comput.* — 1972. — **C-21**. — N 4. — P. 305–309.