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

На правах рукописи

Селезнева Светлана Николаевна

Полиномиальные представления дискретных функций

Специальность 01.01.09 – дискретная математика и математическая кибернетика

Диссертация на соискание ученой степени доктора физико-математических наук

Москва – 2015 г.

Оглавление

Введение	3
Основные определения	40
Часть 1. Сложность полиномиальных представлений функций k -значной логики	49
1. Полиномиальные формы функций	49
2. Приближение функций полиномами	96
Часть 2. Алгоритмические вопросы полиномиальных представлений функций k -значной логики	115
3. Распознавание свойств функций, заданных полиномами	115
4. Нахождение полиномиальных представлений функций	152
5. Мультипликативная сложность функций алгебры логики	195
Заключение	219
Список литературы	223
Публикации автора по теме работы	247

Введение

Начало развития вычислительной техники подтолкнуло исследования функций k -значных логик. Функция k -значной логики – это такая функция, каждая переменная и значение которой принадлежат конечному множеству $E_k = \{0, 1, \dots, k - 1\}$, где $k \geq 2$ – натуральное число. Функции двузначной логики называются также функциями алгебры логики, логическими, переключательными или булевыми функциями. При $k \geq 3$ функции k -значных логик называют функциями многозначных логик. Функции k -значных логик подходят для построения моделей при решении широкого класса задач. Кроме того, при $k = 2$ они допускают достаточно простую физическую реализацию, чем вызвано их повсеместное применение в схемотехнике [217, 220]. Следует также отметить, что вплоть до настоящего времени не прекращаются исследования, относящиеся к созданию и проектированию устройств на основе функций многозначных логик [14, 15, 23, 29–31, 47, 55, 87, 129, 131–133, 209, 211]. В работах [55, 87] приведены описания существующих промышленных цифровых устройств на многозначной основе.

Первые исследования функций k -значной логики касались вопросов полноты и выразимости одних функций при помощи других [83, 181, 182]. Эти исследования стали теоретической основой применения функций k -значных логик при разработке интегральных схем [139, 215]. Особую роль играет выразимость функций k -значных логик при помощи операций сложения и умножения по модулю k [116]. При помощи эквивалентных преобразований такие выражения можно привести к полиномиальным формам, то есть к виду суммы произведений некоторых базисных выражений. Если базисные выражения – это степени переменных, то полиномиальная форма – это обычный полином по модулю k .

То, что каждую логическую функцию можно задать полиномом по модулю два, было доказано И.И. Жегалкиным еще в 1927 г. [58, 59]. Ответ на вопрос о выразимости каждой функции k -значной логики полиномом был получен А.В. Кузнецовым в 1958 г. ([139], раздел 18). Оказывается, что выразимость каждой функции k -значной логики полиномом по модулю k зависит от вида числа k , а именно, каждая функция k -значной логики задается полиномом по модулю k тогда и только тогда, когда k – простое число. Функции k -значной логики, которые представимы полиномами по модулю k , были названы полиномиальными.

Необходимо сказать, что в алгебраических исследованиях рассматривались вопросы о полиномиально полных алгебраических структурах, т.е. изучалось, в каких случаях полиномами над конечным кольцом R можно выразить произвольную одноместную функцию над этим кольцом. Было доказано, что это возможно тогда и только тогда, когда кольцо R является полем [165, 166, 183], [212] (стр. 474). В работах [178, 197] найдены канонические виды полиномов по модулю k , представляющие одноместные полиномиальные функции.

Отметим некоторые работы, касающиеся отыскания критериев полиномиальности функций k -значной логики при составных k . В работе L. Carlitz [152] в 1964 г. указаны критерии полиномиальности одноместных и двуместных функций при $k = p^m$, где p – простое число, $m \geq 1$. В 1975 г. в работе I.G. Rosenberg [188] эти критерии полиномиальности обобщены на случай функций, зависящих от произвольного числа переменных. В работе Н.Н. Айзенберга, И.В. Семейона в 1971 г. сформулировано изящное необходимое условие полиномиальности функций, а также доказано, что если число k является произведением попарно различных простых чисел, то это необходимое условие является и достаточным [5]. Впоследствии независимо А.Н. Черепов [137]

и Д.Г. Мещанинов [103] доказали, что это необходимое условие является достаточным тогда и только тогда, когда число k является произведением попарно различных простых чисел.

Полное решение задачи выразимости одних функций при помощи других состоит в построении решетки замкнутых классов по включению. В двузначном случае эта решетка оказалась счетной [181, 182]. При $k \geq 3$ эта решетка уже континуумальна [140]. Кроме того, А.В. Кузнецов в 1958 г. ([139], раздел 18) доказал, что при каждом составном k все полиномиальные функции k -значной логики образуют замкнутый класс, не являющийся предполным классом. Поэтому рядом исследователей описывались и описываются важные фрагменты этой решетки, в частности, решетки замкнутых классов, содержащих все полиномиальные функции k -значной логики, и решетки полиномиальных функций k -значной логики, содержащих все линейные функции [44, 45, 82, 103–108, 120, 127, 136–138]. При этих исследованиях получен ряд критериев полиномиальности функций k -значной логики при составных k , например в работах [108, 120, 137]. Отметим, что эти критерии полиномиальности разрабатывались при исследовании замкнутых классов функций k -значных логик, и они наиболее подходят для применения в этой области. Д.Г. Мещанинов в 1995 г. оценил алгоритмическую сложность проверки своего критерия полиномиальности функций k -значной логики при $k = p^m$, где p – простое число, $m \geq 2$ [108].

Таким образом, одно из направлений исследований полиномиальных представлений функций k -значной логики проистекает из задач полноты и выразимости. Оно появилось первым и тесно связано с логикой и алгеброй.

Другое направление исследований функций k -значной логики относится к синтезу и сложности управляющих систем (СФЭ, контактных схем и др.) [94, 139]. В этом случае речь идет не о функциональной выразимости функции,

как в первом случае, а о представимости функции определенным образом. При этом появляется вопрос о сложности представления. Надо отметить, что это направление тесно соприкасается и с прикладными исследованиями в связи с широким распространением вычислительной техники и необходимостью развития и изучения моделей представления и преобразования сигналов в ней. Среди других моделей рассматриваются различные виды полиномиальных форм и полиномиальных выражений. В работах [1–3, 18, 77, 86, 95–97, 173, 177] рассматриваются представления функций алгебры логики различными полиномиальными формами с точки зрения их применения при проектировании цифровых устройств. В работах [33–36, 64, 111, 113] исследуются вопросы о полиномиальной декомпозиции функций алгебры логики и функций k -значной логики при $k \geq 3$. Эти задачи важны как теоретически, так и в технических приложениях, т.к. в них исследуются возможности представления функции при помощи функций меньшей размерности, в этом случае, суммами более простых функций. В работе [114] изучаются различные представления, в том числе, полиномиальные для недоопределенных частичных функций алгебры логики. В работах [32, 37, 63, 112] исследуются операторные полиномиальные представления функций алгебры логики и функций k -значной логики при $k \geq 3$. В монографии [208] глава посвящена операторным полиномиальным представлениям функций алгебры логики.

Изучаются также представления логических функций и их систем в программируемых логических матрицах (ПЛМ) [217]. ПЛМ – это такой вид интегральных схем, что потребитель может с небольшими затратами настроить эту интегральную схему для своих целей. ПЛМ содержит два блока, называемых матрицами: матрицу умножений и матрицу сложений. Матрица умножений определяется элементами конъюнкции, а матрица сложений может быть устроена либо на основе элементов дизъюнкции, либо на осно-

ве элементов сложения по модулю два. С логической точки зрения в первом случае в ПЛМ представляется некоторая дизъюнктивная нормальная форма (ДНФ), а во втором случае – некоторая полиномиальная нормальная форма (ПНФ). ПНФ – это сумма по модулю два произведений переменных или их отрицаний. Представления функций в ПЛМ тем эффективнее, чем меньше слагаемых соответственно в ДНФ или ПНФ этих функций. Поэтому актуальны исследования сложности представления логических функций полиномиальными формами различных видов. В связи с чем появляются работы с описанием алгоритмов упрощения полиномиальных форм и с оценками сложности функций алгебры логики в некоторых классах полиномиальных форм [38, 68, 69, 76, 115, 130, 163, 168, 191, 192]. Отметим работы [115, 130, 191] о длине функций алгебры логики при представлении их поляризованными полиномиальными формами (ППФ). ППФ – это сумма по модулю два произведений переменных или их отрицаний, но каждая переменная может входить в ППФ или только с отрицанием, или только без него. Такие полиномиальные формы были введены в работах I.S. Reed [185] и D.E. Muller [176] в 1954 г. при построении кодов, которые впоследствии были названы их именами. Приведем работу К.Д. Кириченко 2005 г. [76]. В ней доказана верхняя оценка длины представления функций алгебры логики ПНФ. Если сравнивать длину ДНФ [48, 80, 125] и длину ПНФ для функций алгебры логики, то оказывается, что при помощи ПНФ функции задаются более короткими представлениями (для самых сложных функций). Экспериментальные результаты показывают, что и для функций, зависящих от четырех переменных, ситуация аналогична: средняя длина ДНФ равна 4, 13, а средняя длина ПНФ равна 3, 66 [192, 220]. В работах [38, 168] исследуется длина ПНФ для функций алгебры логики, зависящих от небольшого числа переменных. В работе [163] изучаются псевдополиномиальные формы для функций алгебры логики и их

применение при проектировании интегральных схем. В работах [61, 62] изучаются алгоритмы построения полиномов для частичных функций алгебры логики. Отметим также недавние работы, в которых исследуется сложность полиномиальных представлений функций k -значных логик при $k \geq 3$ [21, 63].

С развитием вычислительной техники все большую актуальность приобретали вопросы построения быстрых алгоритмов для решения важных задач. Отметим работы, в которых рассматривались задачи построения алгоритмов, относящихся к функциям k -значных логик. В работах [7–10, 39–41, 56] разработаны методы построения алгоритмов для распознавания свойств функций k -значной логики, заданных вектором своих значений, и построены быстрые распознающие алгоритмы для соответствующих задач. Заметим, что в этих работах рассматриваются свойства, связанные с полнотой и выразимостью, а также некоторые другие свойства функций. В работах [56, 57] доказывается NP-трудность распознавания выразимости и α -выразимости функций k -значной логики при помощи других функций при $k \geq 3$. В работах [6, 71–75, 78, 79, 161] изучалась алгоритмическая сложность расшифровки и отыскания максимального верхнего нуля для некоторых монотонных функций k -значных логик в некоторых моделях алгоритмов. Построение полинома по модулю k для функции k -значной логики также является одной из важных задач. В книге [205] (1-е изд. 1977 г., стр. 35; 3-е изд. 2004 г., стр. 53) описан алгоритм построения полинома Жегалкина для функции алгебры логики с временной сложностью $O(N \log N)$ (в алгоритмической модели СФЭ), где $N = 2^n$ и n – число переменных функции алгебры логики, подаваемой на вход алгоритма в виде вектора своих значений. Этот алгоритм напрямую обобщается на случай функций k -значной логики для произвольного простого числа k . При составных k задача построения полинома по модулю k для функций k -значной логики разбивается на две части: выяснения поли-

номиальности функции k -значной логики и в случае положительного ответа построения какого-то ее полинома по модулю k . Как уже отмечалось, в 1995 г. Д.Г. Мещанинов [108] описал алгоритм, который по вектору значений функции k -значной логики при $k = p^m$, где p – простое число, $m \geq 2$, выясняет, является ли эта функция полиномиальной, и в случае положительного ответа строит какой-то ее полином по модулю k . Временная сложность этого алгоритма $O(N \log^m N)$ (в алгоритмической модели равнодоступных адресных машин, РАМ), где $N = k^n$ и n – число переменных функции k -значной логики, подаваемой на вход алгоритма в виде вектора своих значений.

Изучается также алгоритмическая сложность распознавания свойств функций алгебры логики и функций k -значной логики при $k \geq 3$, заданных полиномами. Полином по модулю k (при простых k) в тех случаях, когда он содержит относительно небольшое число слагаемых, может рассматриваться как сокращенное представление функции k -значной логики или вектора из k^n ее значений. В связи с известным результатом об NP-полноте задачи выполнимости конъюнктивных нормальных форм (КНФ) [154] представляет интерес построение полиномиальных алгоритмов распознавания свойств функций k -значных логик в том случае, когда функция подается на вход алгоритма полиномом. Этот интерес вызван тем, что задачи распознавания свойств функций, заданных своими сокращенными представлениями, часто оказываются NP-трудными. Например, если функция алгебры логики подается на вход алгоритма в виде ДНФ, то NP-полны задачи распознавания ее нелинейности, немонотонности, несамодвойственности, немультиаффинности, небиюнктивности и некоторых других свойств [51]. Если на вход алгоритма n -местная функция алгебры логики подается в виде полинома Жегалкина, то NP-трудна задача распознавания равенства ее веса числу 2^{n-1} [159]. NP-полной является задача выполнимости каждой функции из системы функций

алгебры логики, подаваемых на вход алгоритма в виде полиномов Жегалкина [206] (стр. 321). Отметим работу С.П. Горшкова [51], в которой было доказано, что по полиному Жегалкина с полиномиальной временной сложностью можно распознать мультиаффинность, биюнктивность, слабую положительность и слабую отрицательность функции алгебры логики. Напомним, что эти свойства функций алгебры логики рассматривались в [196] в связи с изучением сложности распознавания выполнимости конъюнктивных форм. В работе [52] доказано, что задача построения по полиному Жегалкина сокращенной КНФ монотонной функции не является полиномиальной. В работе [43] исследуется алгоритмическая сложность основных задач комбинаторики слов в том случае, когда слово из нулей и единиц длины 2^n – это вектор значений n -местной функции алгебры логики, которая подается на вход алгоритма в виде полинома Жегалкина. В недавних работах [26–28, 150] построены полиномиальные временные алгоритмы для распознавания некоторых свойств функций алгебры логики и функций k -значных логик при простых $k \geq 3$ в том случае, когда функции задаются полиномами. В частности, для свойств 1-инвариантности функций алгебры логики и сохранения некоторых множеств для функций k -значных логик. Отметим также работы [42, 88–90], в которых изучаются комбинаторные свойства полиномов Жегалкина и рассматриваются их применения.

Таким образом, еще одно направление исследований полиномиальных представлений функций k -значных логик можно определить как алгоритмическое.

Полиномы по модулю k и их обобщения служат не только предметом изучения, но и являются подходящим средством при решении других важных задач. Например, в работах [117, 118, 179] полиномы по модулю два применялись в методах доказательства экспоненциальных нижних оценок сложности

СФЭ ограниченной глубины в базисах, содержащих сложение по модулю два, для некоторых функций алгебры логики. В [198] при доказательстве экспоненциальных нижних оценок сложности применялись полиномы по модулю степени простого числа. Полиномиальные представления функций алгебры логики над конечными кольцами изучаются в связи с применением их в теории сложности [145, 153, 200], в задачах квантовых вычислений [141]. Полиномы над конечными полями и кольцами применяются при построении генераторов псевдослучайных последовательностей потоковых шифров [85, 144]. Полиномиальные формы находят применение при разработке самопроверяемых цифровых устройств [49, 50], при проектировании интегральных схем, т.к. построенные при помощи них схемы допускают достаточно простое тестирование [156–158, 184, 189, 190, 193, 201]. В ряде недавних работ [22, 121–123] при помощи поляризованных полиномиальных форм (ППФ) разработаны методы построения управляющих систем (СФЭ, контактных схем), допускающих тесты линейной и конечной длин.

В нулевые годы полиномы Жегалкина и в общем полиномы над конечными полями или кольцами нашли широкое применение при решении задач криптографии. Полиномы Жегалкина, или алгебраические нормальные формы (АНФ) и полиномиальные выражения оказались очень подходящими для исследования и описания криптографических свойств функций алгебры логики. Отметим книгу [213], а также некоторые недавние работы, например, [13, 19, 20, 24, 25, 92, 93, 102, 134]. Изучается также близость функций алгебры логики к различным классам полиномов. Например, важным криптографическим параметром функций алгебры логики является ее нелинейность. Нелинейность функции выражает расстояние от этой функции до множества всех линейных функций. Среди всех функций наиболее подходящими для криптографических целей считаются максимально нелинейные

функции, т.е. функции, которые имеют наибольшую нелинейность. Рассматриваются также обобщения понятия нелинейности, при которых определяется расстояние от функции не до множества линейных функций, а до другого множества функций, например, до множества всех полиномов определенной степени [213] (глава 6), [11, 84, 124].

Исследуются не только полиномиальные формы, но и представления в полиномиальных базисах, т.е. такие представления, которые построены при помощи умножения и сложения по модулю k , а также констант. В работе [60] найдена сложность реализации полиномов определенной степени СФЭ в полиномиальном базисе (базисе Жегалкина).

Важный класс задач появляется, если рассматривать представления с применением только операции сложения по модулю два, т.е. рассматривать только линейные функции алгебры логики или системы таких функций. В ряде работ изучается сложность реализации систем линейных функций алгебры логики СФЭ в базисе из одного элемента сложения по модулю два (например, см. обзор [164]). Отметим одну особенность, касающуюся сравнения операций дизъюнкции и сложения по модулю два. Заметим, что операции дизъюнкции и сложения по модулю два уже сравнивались между собой в связи с представлениями функций алгебры логики ДНФ и ПНФ. Для систем элементарных дизъюнкций, которые определяют так называемую матрицу без прямоугольников, еще в 1969 г. Э.А. Нечипорук доказал [110], что сложность их реализации СФЭ в базисе из одного элемента дизъюнкции тривиальна, т.е. равна сумме сложностей реализации СФЭ в этом же базисе составляющих их функций. К настоящему времени получены нелинейные нижние оценки сложности реализации явно заданных систем дизъюнкций СФЭ в базисе из одного элемента дизъюнкции [17, 46, 53, 170, 171, 174]. При исследовании сложности реализации СФЭ в базисе из одного элемента сложения по модулю два ситуация

оказалась другой. В 1996 г. К.А. Зыков [66] построил последовательность таких систем линейных функций, образующих матрицы без прямоугольников, что сложность реализации каждой системы этой последовательности СФЭ в базисе из одного элемента сложения по модулю два асимптотически в два раза меньше, чем тривиальная реализация этой системы. В работах [46, 53] этот результат существенно усилен. К настоящему времени для явно заданных систем линейных функций известны только линейные нижние оценки сложности СФЭ в базисе из одного элемента сложения по модулю два, например, [135, 143, 162], нелинейные нижние оценки сложности явно заданных систем получены в СФЭ с ограничениями (например, см. обзор [164]).

Рассматриваются также задачи, связанные с изучением наименьшего числа умножений, необходимого для вычисления функции или системы функций в полиномиальном базисе. Например, при получении лучших из существующих на сегодняшний день оценок сложности умножения матриц, важной прикладной задачи, оказался подходящим класс билинейных алгоритмов, в которых оценивается число умножений [12, 70, 142, 199]. В двузначном случае оценки наименьшего числа умножений для вычисления функции алгебры логики в полиномиальном базисе (базисе Жегалкина) находят применение в криптографии [146]. В работах [81, 109, 147, 148, 175, 195] изучается мультипликативная сложность функций алгебры логики, т.е. наименьшее число конъюнкций, которые необходимы, чтобы вычислить эту функцию в базисе из элементов сложения по модулю два, конъюнкции и константы единица. В работе [169] показано соотношение между мультипликативной сложностью функций алгебры логики и нижней оценкой сложности реализации этих же функций СФЭ в базисе из всех двухвходовых функций.

Исследуются также полиномиальные представления над кольцом целых чисел [98, 99]. Полиномиальные представления функций алгебры логики над

кольцом целых чисел находят применения при проектировании и тестировании интегральных схем [3, 18, 77, 95–97, 173, 177], в криптографии [151].

Таким образом, целью работы является решение следующих задач при исследовании полиномиальных представлений функций k -значной логики: нахождение оценок сложности представлений функций k -значной логики полиномиальными формами различных видов и разработка методов, обеспечивающих эти оценки; нахождение оценок сложности полиномов, приближающих функции k -значной логики с заданной точностью; отыскание полиномиальных алгоритмов для распознавания важных свойств функций k -значной логики, заданных в виде полиномов; получение оценок алгоритмической сложности построения полиномов по модулю k для функций k -значной логики; нахождение оценок некоторых видов сложности вычисления функций k -значной логики в полиномиальных базисах и разработка методов, обеспечивающих эти оценки.

Основное содержание работы разделено на две части, которые разбиты на разделы. Каждый раздел представляет собой изложение результатов автора по определенной подтеме работы. При этом сначала описываются результаты, предшествующие результатам автора, а после указываются новые результаты других авторов в этой области.

В части 1 исследуется сложность представления функций k -значной логики полиномиальными формами различных видов, а также сложность полиномиальных приближений функций k -значной логики (при простых k).

Раздел 1 посвящен исследованию сложности функций k -значной логики в различных классах полиномиальных форм. В 90-е годы 20-го столетия опубликованы работы, в которых изучались полиномиальные декомпозиции функций алгебры логики и функций k -значной логики при $k \geq 3$ [33–37, 111, 112]. В то же время появились работы об оценках длины функций алгебры

логики в классе поляризованных полиномиальных форм (ППФ) [115, 130, 191] и важности этого параметра при проектировании ПЛМ. Отметим, что в работе [115] получено точное значение функции Шеннона длины функций алгебры логики в классе ППФ. Автором диссертации рассмотрено обобщение понятия ППФ на случай функций k -значной логики при $k \geq 3$ и получены оценки длины функций k -значной логики в классе ППФ [235, 239], однако точное значение функции Шеннона получено только для функций k -значной логики, зависящих от одной переменной (при $k \geq 3$). В работе [63] рассматривались полиномиальные операторные представления функций k -значной логики и получены некоторые оценки их длины. Впоследствии автором диссертации рассмотрены другие обобщения ППФ на случай функций k -значной логики при $k \geq 3$ (обобщенно поляризованные полиномиальные формы, ОППФ) и получены оценки длины функций в этом классе [249]. В 2005 г. в работе [76] найдена оценка функции Шеннона длины функций алгебры логики в классе полиномиальных нормальных форм (ПНФ). В работах автора диссертации [245, 268] рассмотрено обобщение ПНФ на случай функций k -значной логики при $k \geq 3$ и получены оценки длины функций k -значной логики в классе ПНФ. В 2012 г. в работе [100] улучшена известная оценка функции Шеннона длины функций трехзначной логики в классе ППФ. В 2015 г. автором диссертации рассмотрена сложность систем функций k -значной логики при $k \geq 2$ в классе ППФ и найдено точное значение функции Шеннона сложности в этом классе для систем функций алгебры логики и трехзначной логики, содержащих не менее двух функций [273]. В 2004 г. в работе [163] рассматривались псевдополиномиальные формы (ПСПФ) для функций алгебры логики и их применение при синтезе интегральных схем. В работе [267] автором найдены оценки функции Шеннона длины функций алгебры логики в классе ПСПФ. В 2014 г. в работе [21] рассмотрено еще одно обобщение ППФ

на случай функций k -значной логики при $k \geq 3$ и найдена верхняя оценка функции Шеннона длины функций в этом классе.

В разделе 1 сначала рассматриваются поляризованные полиномиальные формы (ППФ) и доказывается теорема об однозначной представимости каждой функции k -значной логики ППФ по каждому вектору поляризации (при простых k).

Теорема 1.1. [235] *Если k – простое число, то для каждого вектора поляризации $\delta \in E_k^n$ каждую функцию k -значной логики $f(x_1, \dots, x_n)$ можно задать единственной ППФ по этому вектору δ .*

Вводятся длина $l^{\text{ППФ}}(f)$ функции k -значной логики $f(x_1, \dots, x_n)$ в классе ППФ как наименьшая длина среди всех ППФ, представляющих эту функцию, и длина (функция Шеннона длины) $L_k^{\text{ППФ}}(n)$ функций k -значной логики в классе ППФ как наибольшая длина в классе ППФ среди всех функций, зависящих от n переменных. Для величины $L_k^{\text{ППФ}}(n)$ доказываются следующие оценки.

Теорема 1.2. [239] *Если $k \geq 3$ – простое число, то $L_k^{\text{ППФ}}(1) = k - 1$.*

Теорема 1.3. [235] *Если k – простое число, то $L_k^{\text{ППФ}}(n) < \frac{k(k-1)}{k(k-1)+1} \cdot k^n$.*

Теорема 1.4. [237] *Если k – простое число, то $L_k^{\text{ППФ}}(n) \geq \frac{k-1}{k} \cdot (1 - \varepsilon(n)) \cdot k^n$ для некоторой такой функции $\varepsilon(n)$, что $\varepsilon(n) \rightarrow 0$ при $n \rightarrow \infty$.*

В трехзначной логике строится последовательность симметрических периодических функций, длина которых в классе ППФ растет как $\lfloor \frac{3}{4} \cdot 3^n \rfloor$ при $n \rightarrow \infty$.

Теорема 1.5. [273] *При $n \geq 1$ для периодических функций трехзначной*

логики $f_n = f_{(1122)}^n$ и $g_n = f_{(1221)}^n$ верны следующие равенства:

$$\begin{aligned} l^{\text{ППФ}}(f_n) = l^{\text{ППФ}}(g_n) &= (3^{n+1} - 1)/4, \text{ если } n - \text{нечетное число,} \\ l^{\text{ППФ}}(f_n) = l^{\text{ППФ}}(g_n) &= (3^{n+1} - 3)/4 + 1, \text{ если } n - \text{четное число.} \end{aligned}$$

Затем исследуется вопрос о сложности систем функций k -значной логики в классе ППФ. Сложностью системы ППФ, имеющих один и тот же вектор поляризации, называется число попарно различных слагаемых, встречающихся во всех этих ППФ. Сложностью $L_k^{\text{ППФ}}(F)$ системы F функций k -значной логики в классе ППФ называется наименьшая сложность среди всех таких систем ППФ, что все ППФ каждой системы имеют один и тот же вектор поляризации, и для каждой функции $f \in F$ найдется ППФ, реализующая функцию F , в этой системе ППФ. При простых k для произвольной системы F функций k -значной логики, зависящих от переменных $x_1, \dots, x_n$, верно $L_k^{\text{ППФ}}(F) \leq k^n$.

Вводятся функции Шеннона $L_k^{\text{ППФ}}(m, n)$ и $L_{S_k}^{\text{ППФ}}(m, n)$ сложности систем функций k -значной логики и, соответственно, систем симметрических функций k -значной логики в классе ППФ как наибольшая сложность среди всех систем с m функциями и, соответственно, с m симметрическими функциями, зависящими от одних и тех же n переменных. Доказываются точные значения величин $L_k^{\text{ППФ}}(m, n)$ и $L_{S_k}^{\text{ППФ}}(m, n)$ при $k = 2$ и $k = 3$, если $m \geq 2$.

Теорема 1.6. [273] *Для всех $m \geq 2$, $n = 1, 2, \dots$ найдется такая система функций алгебры логики $F_{m,n} = \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\}$, что*

$$L_2^{\text{ППФ}}(F_{m,n}) = 2^n.$$

Более того, можно требовать, чтобы каждая из систем $F_{n,m}$ содержала только симметрические функции.

Следствие 1.3. [273] Для всех $m \geq 2$, $n = 1, 2, \dots$ верны равенства

$$L_2^{\text{ППФ}}(m, n) = L_{S_2}^{\text{ППФ}}(m, n) = 2^n.$$

Теорема 1.7. [273] Для всех $m \geq 2$, $n = 1, 2, \dots$ найдется такая система функций трехзначной логики $F_{m,n} = \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\}$, что

$$L_3^{\text{ППФ}}(F_{m,n}) = 3^n.$$

Более того, можно требовать, чтобы каждая из систем $F_{m,n}$ содержала только симметрические функции.

Следствие 1.4. [273] Для всех $m \geq 2$, $n = 1, 2, \dots$ верны равенства

$$L_3^{\text{ППФ}}(m, n) = L_{S_3}^{\text{ППФ}}(m, n) = 3^n.$$

Затем рассматриваются обобщенно поляризованные полиномиальные формы (ОППФ). ОППФ является расширением ППФ, но при этом, как и в случае ППФ, каждая функция k -значной логики представима однозначной ОППФ по каждому вектору поляризации (при простых k).

Теорема 1.8. [249] Если k – простое число, то для каждого обобщенного вектора поляризации δ каждую функцию k -значной логики $f(x_1, \dots, x_n)$ можно задать единственной ОППФ по этому вектору δ .

Вводятся длина функции k -значной логики в классе ОППФ как наименьшая длина среди всех ОППФ, представляющих эту функцию, и длина (функция Шеннона длины) $L_k^{\text{ОППФ}}(n)$ функций k -значной логики в классе ОППФ как наибольшая длина в классе ОППФ среди всех функций, зависящих от n переменных. Для величины $L_k^{\text{ОППФ}}(n)$ доказываются следующие оценки.

Теорема 1.9. [249] Если k – простое число, то $L_k^{\text{ОППФ}}(n) \leq \frac{k}{k+1} \cdot k^n$.

Теорема 1.10. [249] Если k – простое число, то $L_k^{\text{ОППФ}}(n) \geq \frac{k-1}{k} \cdot (1 - \varepsilon(n)) \cdot k^n$ для некоторой такой функции $\varepsilon(n)$, что $\varepsilon(n) \rightarrow 0$ при $n \rightarrow \infty$.

Далее рассматриваются полиномиальные нормальные формы (ПНФ). Вводятся длина $l^{\text{ПНФ}}(f)$ функции k -значной логики $f(x_1, \dots, x_n)$ в классе ПНФ как наименьшая длина среди всех ПНФ, представляющих эту функцию, и длина (функция Шеннона длины) $L_k^{\text{ПНФ}}(n)$ функций k -значной логики в классе ПНФ как наибольшая длина в классе ПНФ среди всех функций, зависящих от n переменных. Доказывается, что для произвольной функции k -значной логики $f(x_1, \dots, x_n)$ величину $l^{\text{ПНФ}}(f)$ можно сверху оценить мощностью затеняющего множества куба E_k^n , увеличенной на единицу, или удвоенной мощностью покрытия полушарами куба E_k^n (при простых k). Как следствия получаются верхние оценки длины $L_k^{\text{ПНФ}}(n)$. Затем доказывается нижняя оценка длины $L_k^{\text{ПНФ}}(n)$.

Теорема 1.11. [245] Пусть k – простое число. Если $T, T \subseteq E_k^n$, – затеняющее множество куба E_k^n , то для каждой функции k -значной логики $f(x_1, \dots, x_n)$ можно построить такую ПНФ, представляющую функцию f , что длина этой ПНФ не превосходит $(|T| + 1)$.

Теорема 1.12. [268] Пусть k – простое число. Если $T, T \subseteq E_k^n$, – покрытие полушарами куба E_k^n , то для каждой функции k -значной логики $f(x_1, \dots, x_n)$ можно построить такую ПНФ, представляющую функцию f , что длина этой ПНФ не превосходит $2 \cdot |T|$.

Теорема 1.13. [245] Если k – простое число, то $L_k^{\text{ПНФ}}(n) \geq (1 - \varepsilon(n)) \cdot \frac{k^n}{n \cdot \log_k(k(k-1)+1)}$ для некоторой такой функции $\varepsilon(n)$, что $\varepsilon(n) \rightarrow 0$ при $n \rightarrow \infty$.

Следствие 1.5. [268] Если k – простое число, то $L_k^{\text{ПНФ}}(n) = \Theta\left(\frac{k^n}{n}\right)$.

Затем рассматриваются псевдополиномиальные формы (ПСПФ). Вводятся длина $l^{\text{ПСПФ}}(f)$ функции алгебры логики $f(x_1, \dots, x_n)$ в классе ПСПФ как наименьшая длина среди всех ПСПФ, представляющих эту функцию, и длина (функция Шеннона длины) $L_2^{\text{ПСПФ}}(n)$ функций алгебры логики в классе ПСПФ как наибольшая длина в классе ПСПФ среди всех функций, зависящих от n переменных. Сначала доказывается нижняя оценка длины $L_2^{\text{ПСПФ}}(n)$. Затем доказывается, что для произвольной функции алгебры логики $f(x_1, \dots, x_n)$ величину $l^{\text{ПСПФ}}(f)$ можно сверху оценить удвоенной мощностью покрытия шарами радиуса 1 куба E_2^n . Как следствие получается верхняя оценка длины $L_2^{\text{ПСПФ}}(n)$.

Теорема 1.14. [267] *Справедливо неравенство $L_2^{\text{ПСПФ}}(n) \geq (1 - \varepsilon(n)) \frac{2^{n+1}}{n^2}$ для некоторой такой функции $\varepsilon(n)$, что $\varepsilon(n) \rightarrow 0$ при $n \rightarrow \infty$.*

Теорема 1.15. [267] *Если $T, T \subseteq E_2^n$, – покрытие шарами радиуса 1 куба E_2^n , то для каждой функции алгебры логики $f(x_1, \dots, x_n)$ можно построить такую ПСПФ, представляющую функцию f , что длина этой ПСПФ не превосходит $2 \cdot |T|$.*

Следствие 1.6. [267] *Справедливо неравенство $L_2(n) \leq (1 + \varepsilon(n)) \frac{2^{n+1}}{n}$ для некоторой такой функции $\varepsilon(n)$, что $\varepsilon(n) \rightarrow 0$ при $n \rightarrow \infty$.*

В разделе 2 рассматриваются приближения с заданной точностью функций k -значной логики полиномами (при простых k). В 1982 г. опубликована работа [54], в которой получены оценки степени и длины полиномов, приближающих функции алгебры логики с заданной точностью. В работе автора [244] получены оценки степени и длины полиномов по модулю k , приближающих функции k -значной логики с заданной точностью. При этом автором диссертации рассматривается более широкий класс видов точности приближений. Отметим, что вопросы приближенной реализации функций алгебры

логики изучались в задачах синтеза управляющих систем [16, 126, 180]. Надо также отметить, что приближения функций полиномами (в других постановках) рассматриваются в задачах криптографии, например, [213] (глава 6), [11, 65, 84, 128].

Вводятся величины $r_k^{\delta_n}(n)$ и $l_k^{\delta_n}(n)$ соответственно как наименьший ранг полиномов и наименьшая длина полиномов, такие, что полиномами по модулю k этого ранга и соответственно этой длины можно приблизить каждую функцию k -значной логики, зависящую от n переменных, с точностью δ_n .

Теорема 2.1. [244] Пусть k – простое число, δ , $0 \leq \delta \leq 1$, – действительное число, δ_n , $0 \leq \delta_n \leq 1$ – последовательность действительных чисел, $\delta_n \rightarrow 0$ при $n \rightarrow \infty$, q , $q \geq 1$, – натуральное число. Тогда

- 1) $r_k^{\delta}(n) = 0$ при $\delta \geq \frac{k-1}{k}$;
- 2) $r_k^{\delta}(n) \sim \frac{k-1}{k} \cdot n$ при $0 < \delta < \frac{k-1}{k}$ и $n \rightarrow \infty$;
- 3) $r_k^{\delta_n}(n) \sim \frac{k-1}{k} \cdot n$ при $\frac{1}{k^n} = o(\delta_n)$ и $n \rightarrow \infty$;
- 4) $r_k^{(q)}(n) = n$ для всех n , начиная с некоторого значения n_0 , при $k \geq 3$;
- 5) $n - 2 \leq r_2^{(q)}(n) \leq n - 1$ для всех n , начиная с некоторого значения n_0 при $q \geq 2$, $r_2^{(1)}(n) = n - 1$;
- 6) $r_k^{\delta}(n) = n$ при $\delta = 0$.

Теорема 2.2. [244] Пусть k – простое число, $k \geq 2$, δ , $0 \leq \delta \leq 1$, – действительное число, δ_n , $0 < \delta_n \leq 1$ – последовательность действительных чисел, $\delta_n \rightarrow 0$ при $n \rightarrow \infty$, q , $q \geq 1$ – натуральное число. Тогда

- 1) $l_k^{\delta}(n) = 1$ при $\delta \geq \frac{k-1}{k}$;
- 2) $l_k^{\delta}(n) \leq \frac{k-1}{k} \cdot (1 - \delta) \cdot k^n + C \cdot (k - 1)^n$ при $0 < \delta < \frac{k-1}{k}$ для некоторого действительного числа C , $C > 0$;
- 3) $l_k^{\delta_n}(n) \sim \frac{k-1}{k} \cdot k^n$ при $\delta_n \geq (\frac{k-1}{k})^n$ и $n \rightarrow \infty$.
- 4) $l_2^{(q)}(n) \sim \frac{1}{2} \cdot 2^n$ при $n \rightarrow \infty$.

$$5) l_k^\delta(n) = k^n \text{ при } \delta = 0.$$

Часть 2 посвящена алгоритмическим вопросам, связанным с полиномиальными представлениями функций k -значной логики. В ней исследуются алгоритмическая сложность распознавания свойств функций k -значной логики, заданных полиномами по модулю k при простых k , алгоритмическая сложность распознавания полиномиальности функций k -значной логики при составных k , алгоритмическая сложность нахождения полиномиальных представлений функций k -значной логики, а также рассматриваются вопросы о числе умножений при вычислении функций и систем функций алгебры логики в полиномиальном базисе.

В разделе исследуется алгоритмическая сложность распознавания принадлежности функций k -значной логики, заданных полиномами по модулю k , к предполным классам. В 90-е годы 20-го столетия опубликованы работы, в которых доказана полиномиальность распознавания некоторых свойств функций k -значных логик, заданных полиномами. Среди них работа [51] о полиномиальности распознавания свойств мультиаффинности, биюнктивности, слабой положительности и слабой отрицательности, работы автора [223, 225] о полиномиальности распознавания полноты конечных систем функций алгебры логики и распознавания принадлежности функции k -значной логики к предполным классам самодвойственных функций. Далее можно привести работы автора [231–233]. В перечисленных работах автора диссертации доказана полиномиальность распознавания принадлежности функции k -значной логики, заданной полиномом, к предполным классам из пяти семейств предполных классов (при простых k). Кроме того, в работах автора диссертации предложены два подхода к построению распознающих полиномиальных алгоритмов. Первый подход состоит в следующем. Сначала доказывается, что если функция обладает некоторым свойством P , то ее полиномиальное представле-

ние обладает некоторым свойством Q . Затем для распознавания свойства P применяется в общем случае экспоненциальный алгоритм, но проверка доказанного свойства Q обеспечивает полиномиальность алгоритма. Этот подход был применен для распознавания четности и самодвойственности функций k -значной логики. В этом случае было доказано, что если функция является четной (инвариантной), то ее полиномиальное представление содержит достаточно много слагаемых относительно своего ранга. Впоследствии в работах [28, 150] при помощи этого подхода была доказана полиномиальность распознавания 1-инвариантности и периодичности относительно данного периода функции алгебры логики, заданной полиномом. В совместной работе [270] этот подход описан и показано, для распознавания каких свойств функций алгебры логики его можно применить. Вторым подходом применялся для доказательства полиномиальности распознавания сохранения функцией вполне рефлексивного и вполне транзитивного отношения, и, как следствие, была получена полиномиальность распознавания принадлежности функции к некоторым предполным классам. В 2004 г. появилась работа [43] о полиномиальности распознавания некоторых свойств комбинаторики слов. Затем в работе автора [241] доказана полиномиальность нахождения остатка веса функции алгебры логики от деления на 2^m , где m – заранее известное натуральное число. Отметим, что задача распознавания по полиному n -местной функции алгебры логики того, что ее вес равен числу 2^{n-1} , является NP-трудной [159]. В работах [26, 27], в частности, доказана полиномиальность распознавания принадлежности функции k -значной логики, заданной полиномом, к некоторым предполным классам из шестого семейства предполных классов (при простых k).

При исследовании алгоритмической сложности распознавания свойств функций k -значной логики, заданных полиномами, под алгоритмической мо-

делью подразумевается равнодоступная адресная машина (РАМ), на вход которой подается полином $P(f)$ функции k -значной логики $f(x_1, \dots, x_n)$ в виде слова $\alpha(P(f)) \in A^*$, где $A = E_k \cup \{+\} = \{0, 1, \dots, k-1, +\}$. А именно, если

$$P(f) = \sum_{\alpha=(a_1, \dots, a_n) \in E_k^n} c_f(\alpha) X_\alpha,$$

где $c_f(\alpha) \in E_k$, $X_\alpha = x_1^{a_1} \cdot \dots \cdot x_n^{a_n}$ – мономы, то

$$\alpha(P(f)) = \sum_{c_f(\alpha) \neq 0} c_f(\alpha) a_1 a_2 \dots a_n.$$

При этом длина $|\alpha(P(f))|$ слова $\alpha(P(f))$ равна $l(P(f)) \cdot (n+2) - 1$.

В разделе 3 доказываются следующие теоремы.

Теорема 3.1. [232] Пусть $k = p^h$, где p – простое число, $h \geq 1$, $F_k = (E_k; +, \cdot)$ и $F = (E_k; \oplus, \otimes)$ – поля над множеством E_k . Существует детерминированный алгоритм, который для каждого слова $\alpha(P_{F_k}(f))$ в алфавите $A = E_k \cup \{+\}$ с полиномиальной временной сложностью определяет, является функция $f(x_1, \dots, x_n)$ линейной по отношению к группе $G = (E_k; \oplus)$ или нет.

Следующая теорема является основой для построения полиномиального распознающего алгоритма для предполных классов самодвойственных функций.

Теорема 3.3. [233] Пусть $k = p^h$, где p – простое число, $h \geq 1$, $F_k = (E_k; +, \cdot)$ – поле. Если функция $f(x_1, \dots, x_n) \in P_k$, не равна нулю и инвариантна относительно набора связанных преобразований $s_1(x), \dots, s_n(x)$ ранга q , то для ранга $r = r(P_{F_k}(f))$ и веса $w = w(P_{F_k}(f))$ полинома $P_{F_k}(f)$ функции f верно неравенство $w^q \geq 2^r$.

Следующая теорема устанавливает соотношение между свойствами самодвойственности и инвариантности функций k -значной логики.

Теорема 3.4. [223, 225] Пусть k – простое число, $s(x) \in P_k^1$ – перестановка, образующая цикл длины k . Функция k -значной логики $f(x_1, \dots, x_n)$ самодвойственна относительно перестановки $s(x)$ тогда и только тогда, когда функция k -значной логики

$$g(x_1, \dots, x_n) = q(f(x_1, \dots, x_n)) + (k - 1) \cdot q(x_1),$$

где $q(x) \in P_k^1$ – такая перестановка, что $s(x) = q^{-1}(q(x) + 1)$, инвариантна относительно преобразования $s(x)$ по каждой переменной.

Теорема 3.5. [223, 225] Пусть k – простое число, $s(x) \in P_k^1$ – перестановка, образующая цикл длины k . Существует детерминированный алгоритм, который для каждого слова $\alpha(P(f))$ в алфавите $A = E_k \cup \{+\}$ с полиномиальной временной сложностью определяет, является функция k -значной логики $f(x_1, \dots, x_n) \in P_k$ самодвойственной относительно перестановки $s(x)$ или нет.

Следующая теорема описывает необходимое и достаточное условие сохранения функцией k -значной логики вполне рефлексивного и вполне транзитивного отношения.

Теорема 3.6. [231] Пусть $k \geq 2$, $R \subseteq E_k^h$ – вполне рефлексивное и вполне транзитивное отношение, $h \geq 2$, $\chi_R(z_1, \dots, z_h) \in P_k$ – его характеристическая функция, т.е. $\chi_R(a_1, \dots, a_h) = 1$, где $a_1, \dots, a_h \in E_k$, если и только если $R(a_1, \dots, a_h)$. Функция k -значной логики $f(x_1, \dots, x_n)$ сохраняет отношение R тогда и только тогда, когда для каждого i , $1 \leq i \leq n$, для каждой h таких элементов $a_1, \dots, a_h \in E_k$, что $R(a_1, \dots, a_h)$, и для каждой пары индексов j_1, j_2 ($1 \leq j_1 < j_2 \leq h$) и для всех возможных значений переменных $x_{j_1}, \dots, x_{j_{i-1}}, x_{j_{i+1}}, \dots, x_{j_n}$ при $j = 1, \dots, h$, $j \neq j_1$, $j \neq j_2$, $y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_n$ верно тождество

$$\chi_R(z_1, \dots, z_h) = 1,$$

где $z_j = f(x_{j,1}, \dots, x_{j,i-1}, a_1, x_{j,i+1}, \dots, x_{j,n})$ при $j = 1, \dots, h$, $j \neq j_1$, $j \neq j_2$,
 $z_{j_1} = f(y_1, \dots, y_{i-1}, a_{j_1}, y_{i+1}, \dots, y_n)$, $z_{j_2} = f(y_1, \dots, y_{i-1}, a_{j_2}, y_{i+1}, \dots, y_n)$.

Теорема 3.7. [231] Пусть k – простое число, и $R^{(h)} \subseteq E_k^h$ – вполне рефлексивное и вполне транзитивное отношение. Существует детерминированный алгоритм, который для каждого слова $\alpha(P(f))$ в алфавите $A = E_k \cup \{+\}$ с полиномиальной временной сложностью определяет, сохраняет функция k -значной логики $f(x_1, \dots, x_n)$ отношение R или нет.

Предполные классы монотонных функций, функций, сохраняющих разбиение, и предполные классы типа В описываются вполне рефлексивными и вполне транзитивными отношениями. Поэтому как следствия получаем следующие утверждения.

Следствие 3.1. [231] Пусть k – простое число, и $\leq_k$ – отношение частичного порядка на множестве E_k . Существует детерминированный алгоритм, который для каждого слова $\alpha(P(f))$ в алфавите $A = E_k \cup \{+\}$ с полиномиальной временной сложностью определяет, является функция k -значной логики $f(x_1, \dots, x_n)$ монотонной относительно частичного порядка $\leq_k$ или нет.

Следствие 3.2. [231] Пусть k – простое число, и D – разбиение множества E_k . Существует детерминированный алгоритм, который для каждого слова $\alpha(P(f))$ в алфавите $A = E_k \cup \{+\}$ с полиномиальной временной сложностью определяет, сохраняет функция k -значной логики $f(x_1, \dots, x_n)$ разбиение D или нет.

Следствие 3.3. [231] Пусть k – простое число, и $R \subseteq E_k^h$ – отношение типа В, $h \geq 3$. Существует детерминированный алгоритм, который для каждого слова $\alpha(P(f))$ в алфавите $A = E_k \cup \{+\}$ с полиномиальной временной сложностью определяет, сохраняет функция k -значной логики

$f(x_1, \dots, x_n)$ отношение R или нет.

В завершение раздела рассматривается задача нахождения остатка от деления веса функции алгебры логики на степень двойки.

Теорема 3.8 [241] *Пусть $m, m \geq 1$, – заданное натуральное число. Существует детерминированный алгоритм, который для каждого слова $\alpha(P(f))$ в алфавите $A = E_2 \cup \{\oplus\}$ с полиномиальной временной сложностью находит остаток от деления веса функции алгебры логики $f(x_1, \dots, x_n)$ на 2^m .*

В разделе 4 исследуется алгоритмическая сложность распознавания полиномиальности функций k -значной логики при составных k и в случае положительного ответа построения какого-то полинома этой функции, а также некоторые вопросы, связанные с алгоритмической сложностью построения полиномов для функций k -значной логики при простых k .

В 1971 г. в работе [5] найден критерий полиномиальности функций k -значной логики при составных k вида $k = p_1 \cdot \dots \cdot p_s$, где $p_1, \dots, p_s$ – попарно различные простые числа, $s \geq 2$, который можно проверить со сложностью $O(N)$ (в алгоритмической модели СФЭ), где $N = k^n$ и n – число переменных функции k -значной логики, подаваемой на вход алгоритма в виде вектора своих значений. Затем при исследовании фрагментов решетки замкнутых классов, связанных с классом полиномиальных функций, в получены критерии полиномиальности функций k -значной логики при составных k [108, 120, 137]. В работе [108] доказано, что распознать полиномиальность функции k -значной логики при $k = p^m$, где p – простое число, $m \geq 2$, и в случае положительного ответа построить какой-то ее полином можно со сложностью $O(N \log^m N)$ (в алгоритмической модели РАМ), где $N = k^n$ и n – число переменных функции k -значной логики, подаваемой на вход алгоритма в виде

вектора своих значений. В работах [7–10, 39–41, 56] разработаны методы и построены быстрые алгоритмы для распознавания некоторых свойств функций k -значной логики, заданных вектором из своих $N = k^n$ значений (в алгоритмической модели СФЭ). В работах автора [252, 257] для случая $k = p^m$, где p – простое число, $m \geq 2$, и в работах автора [258, 261] для произвольного составного k доказано, что распознать полиномиальность функции k -значной логики и в случае положительного ответа построить какой-то ее полином можно со сложностью $O(N)$ (в алгоритмической модели СФЭ), где $N = k^n$ и n – число переменных функции k -значной логики, подаваемой на вход алгоритма в виде вектора своих значений. При этом автором в работе [252] предложен канонический вид полиномиальных функций k -значной логики при $k = p^m$, где p – простое число, $m \geq 2$, который обобщает канонический вид одноместных полиномиальных функций из [4, 178, 197] на случай функций многих переменных. На основе этого канонического вида автором диссертации получены распознающие алгоритмы полиномиальности. В книге [205] (стр. 35) описан алгоритм построения полинома Жегалкина для произвольной функции алгебры. Сложность этого алгоритма в алгоритмической модели СФЭ в базисе из одного элемента сложения по модулю два равна $\frac{1}{2}N \log_2 N$, где $N = 2^n$ и n – число переменных функции алгебры логики, подаваемой на вход алгоритма в виде вектора своих значений. В работах [149, 167, 256] доказана оптимальность этого алгоритма в СФЭ с некоторыми ограничениями их структуры. В книге [213] (стр. 71) и в работе [1] указана формула вычисления коэффициентов полинома Жегалкина функции алгебры логики через значения этой функции. В совместной работе автора диссертации [248] указана формула вычисления коэффициентов полинома по модулю k для функции k -значной логики через значения этой функции для произвольного простого k .

Множество всех полиномиальных функций k -значной логики обозначается

как Pol_k . Сначала рассматривается случай, когда $k = p^m$, p – простое число, $m \geq 1$. Вводится составная характеристика $cd(X_\alpha)$ (по отношению к простому числу p и числу m) для монома X_α и определяется линейный порядок $\preceq$ на множестве мономов $\{X_\alpha \mid \alpha \in E_k^n\}$. Доказывается теорема о каноническом виде полиномов полиномиальных функций p^m -значной логики.

Теорема 4.1. [252] Пусть p – простое число, $m \geq 1$. Каждая функция $f(x_1, \dots, x_n) \in Pol_{p^m}$ представима однозначным полиномом по модулю p^m вида

$$f(x_1, \dots, x_n) = \sum_{i=1}^l a_i \cdot X_i,$$

где $cd(X_i) < m$ и $a_i < p^{m-cd(X_i)}$, $i = 1, \dots, l$.

Однозначный полином по модулю p^m для функции $f \in Pol_{p^m}$ из теоремы 9.1 обозначается как $P(f)$. Затем доказывается критерий полиномиальности функций p^m -значной логики. Функции $f_1(x), f_2(x) \in P_{p^m}$ называются p^t -эквивалентными, где $1 \leq t \leq m$, если $f_1(x) = f_2(x) \pmod{p^t}$.

Теорема 4.2. [252] Пусть $k = p^m$, где p – простое число, $m \geq 1$.

Пусть $f(y, x_1, \dots, x_n) \in P_k$, для каждого $j \in E_k$ функции $f_j(x_1, \dots, x_n) = f(j, x_1, \dots, x_n) \in Pol_k$ и их канонические полиномы $P(f_j)$ имеют вид

$$P(f_j) = \sum_{i=1}^l a_i^{(j)} X_i,$$

где X_l – наибольший (относительно линейного порядка $\preceq$) моном среди слагаемых всех полиномов $P(f_j)$, $j \in E_k$.

Тогда функция $f(y, x_1, \dots, x_n) \in Pol_k$ тогда и только тогда, когда для функции $\psi_l(y)$, где $\psi_l(j) = a_l^{(j)}$, $j \in E_k$, найдется $p^{m-cd(X_l)}$ -эквивалентная ей функция $\xi_l(y) \in Pol_k^1$ и

$$f(y, x_1, \dots, x_n) - X_l \cdot \xi_l(y) \in Pol_k.$$

Затем доказываются теоремы об алгоритмической сложности распознавания полиномиальности функций k -значной логики и в случае положительного ответа построения какого-то ее полинома по модулю k при составных k .

Теорема 4.3. [252, 257] Пусть $k = p^m$, где p – простое число, $m \geq 2$, $B \subseteq P_k$ – полная система множества P_k .

Существует последовательность СФЭ S_n , $n = 1, 2, \dots$, в базе B с k^n входами $u(\alpha)$, $\alpha \in E_k^n$, и $k^n + 1$ выходами $v(\alpha)$, $\alpha \in E_k^n$, и z , такая, что если на входы $u(\alpha)$ подаются значения $f(\alpha)$, $\alpha \in E_k^n$, произвольной функции k -значной логики $f(x_1, \dots, x_n)$, то на выходе z появляется 1, если $f \in Pol_k$, на выходе z появляется 0, если $f \notin Pol_k$, в случае $z = 1$ на выходах $v(\alpha)$ появляются значения коэффициентов $c_\alpha(f)$, $\alpha \in E_k^n$, канонического полинома $P(f)$ функции f , и $L(S_n) = O(N)$, где $N = k^n$ – длина вектора значений функции f .

Теорема 4.4. [261] Пусть k – составное число, $B \subseteq P_k$ – полная система множества P_k .

Существует последовательность СФЭ S_n , $n = 1, 2, \dots$, в базе B с k^n входами $u(\alpha)$, $\alpha \in E_k^n$, и $k^n + 1$ выходами $v(\alpha)$, $\alpha \in E_k^n$, и z , такая, что если на входы $u(\alpha)$ СФЭ S_n поступают значения $f(\alpha)$ произвольной функции k -значной логики, то на выходе z появляется 1, если $f \in Pol_k$, на выходе z появляется 0, если $f \notin Pol_k$, в случае $z = 1$ на выходах $v(\alpha)$, $\alpha \in E_k^n$, появляются значения коэффициентов $c(\alpha)$ при мономах X_α в каком-то полиноме по модулю k , задающего функцию f , и $L(S_n) = O(N)$, где $N = k^n$ – длина вектора значений функции f .

Далее исследуется сложность построения полинома Жегалкина функции алгебры логики в алгоритмической модели СФЭ с некоторыми ограничени-

ями их структуры, а именно в классе СФЭ с разделенными переменными (СФЭРП). Пусть Π_n обозначает систему из 2^n линейных функций алгебры логики, выражающих коэффициенты полинома Жегалкина произвольной n -местной функции алгебры логики через значения этой функции на всех наборах переменных. Обозначим как $L_B^{СФЭРП}(\Pi_n)$ наименьшую сложность среди всех СФЭРП в базисе B , $B \subseteq P_2$, реализующих систему Π_n .

Теорема 4.5. [256] *В базисе $B_{L_0} = \{x \oplus y\}$ верно $L_{B_{L_0}}^{СФЭРП}(\Pi_n) \geq n \cdot 2^{n-1}$.*

Следствие 4.3. [256] *В базисе $B_{L_0} = \{x \oplus y\}$ верно $L_{B_{L_0}}^{СФЭРП}(\Pi_n) = n \cdot 2^{n-1}$.*

Теорема 4.6. [256] *В базисе $B_0 = \{x \& y, x \vee y, \bar{x}\}$ верно*

$$3n \cdot 2^{n-1} \leq L_{B_0}^{СФЭРП}(\Pi_n) \leq 4n \cdot 2^{n-1}.$$

В завершение этого раздела доказана формула, при простых k выражающая значения коэффициентов полинома по модулю k функции k -значной логики через значения этой функции на всех наборах переменных.

Теорема 4.7. [248] *Пусть k – простое число, $f(x_1, \dots, x_n) \in P_k^n$. Тогда для каждого набора $\alpha = (a_1, \dots, a_n) \in E_k^n$ верно*

$$c_f(\alpha) = (-1)^{r(\alpha)} \sum_{\beta: t(\beta) \subseteq t(\alpha)} f(\beta) \prod_{a_i \neq 0} b_i^{k-1-a_i},$$

где $\beta = (b_1, \dots, b_n) \in E_k^n$ (полагаем, что произведение по пустому множеству индексов равно 1 и $0^0 = 1$).

В разделе 5 изучается мультипликативная сложность функций алгебры логики. Мультипликативной сложностью $\mu(f)$ функции алгебры логики f (соответственно $\mu(F)$ системы функций алгебры логики F) называется наименьшее число конъюнкций, которое требуется для вычисления этой функ-

ции (соответственно, всех функций из этой системы) СФЭ в базисе из конъюнкции, сложения по модулю два и константы единица. Еще в 1962 г. в работе [109] получена асимптотика функции Шеннона мультипликативной сложности функций алгебры логики. В работах 90-х–нулевых годов [81, 147, 148, 175, 195] изучается мультипликативная сложность функций алгебры логики. В работах [147, 175] исследована мультипликативная сложность квадратичных функций алгебры логики. В работах автора [269, 272, 274] получены дальнейшие результаты о мультипликативной сложности квазиквадратичных функций алгебры логики. В работе [195] изучена мультипликативная сложность мультиаффинных функций алгебры логики. В работах автора [269, 274] исследована мультипликативная сложность функций алгебры логики, представимых суммой двух мультиаффинных функций. В работе [169] показано соотношение между мультипликативной сложностью функций алгебры логики и нижней оценкой сложности реализации этих же функций СФЭ в базисе из всех двухвходовых функций.

В разделе 5 доказываются следующие теоремы.

Теорема 5.1. [269] 1. Если $n \geq 3$, и функция алгебры логики $f(x_1, \dots, x_n)$ может быть представлена в виде $x_1 \cdot \dots \cdot x_n \oplus q(x_1, \dots, x_n)$, где $\deg(q) = 2$, то $\mu(f) = n - 1$.

2. Если $F = \{x_1 \cdot \dots \cdot x_n, q(x_1, \dots, x_n)\}$, где $\deg(q) = 2$, то $\mu(F) = n - 1$ ($n \geq 2$).

Теорема 5.2. [269] 1. Если функция алгебры логики $f(x_1, \dots, x_n)$ может быть представлена в виде $f_1(x_1, \dots, x_n) \oplus f_2(x_1, \dots, x_n)$, где f_1, f_2 – мультиаффинные функции, и $\deg(f) = n$, то $\mu(f) = n - 1$ ($n \geq 2$).

2. Если $F = \{x_1 \cdot \dots \cdot x_n, f(x_1, \dots, x_n)\}$, где f – мультиаффинная функция алгебры логики, $\deg(f) < n$, то $\mu(F) = n - 1$ ($n \geq 1$).

Теорема 5.3. [269] 1. Если функция алгебры логики $f(x_1, \dots, x_n)$ может быть представлена в виде $f_1(x_1, \dots, x_n) \oplus f_2(x_1, \dots, x_n)$, где f_1, f_2 – мультиаффинные функции, $f_1 \neq f_2$, и $\deg(f_1) = \deg(f_2) = n$, то $\mu(f) = n - 2$ ($n \geq 2$).

2. Если $F = \{x_1 \cdot \dots \cdot x_n, f(x_1, \dots, x_n)\}$, где f – мультиаффинная функция алгебры логики, $\deg(f) = n$, то $\mu(F) = n - 1$ ($n \geq 1$).

Теорема 5.4. [269] 1. Если функция алгебры логики $f(x_1, \dots, x_n)$ может быть представлена в виде $f_1(x_1, \dots, x_n) \oplus f_2(x_1, \dots, x_n)$, где f_1, f_2 – мультиаффинные функции, и $\deg(f_1) < n$, $\deg(f_2) < n$, то $\mu(f) \leq n - 1$ ($n \geq 2$).

2. Если $F = \{f_1(x_1, \dots, x_n), f_2(x_1, \dots, x_n)\}$, где f_1, f_2 – мультиаффинные функции алгебры логики, то $\mu(F) \leq n - 1$, ($n \geq 1$).

Теорема 5.5. [272] Если функция алгебры логики $f(x_1, \dots, x_n)$ может быть представлена в виде $x_1 x_2 x_3 \oplus q(x_1, \dots, x_n)$, где $\deg(q) = 2$, $n \geq 3$, то $\mu(f) \leq t + 1$ при $n = 2t$ или $n = 2t + 1$.

Теорема 5.6. [272] Если $f_n(x_1, \dots, x_n) = x_1 x_2 x_3 \oplus x_4 x_5 \oplus x_6 x_7 \oplus \dots \oplus x_{n-1} x_n$, где $n = 2t + 1$, $n \geq 3$, то $\mu(f_n) = t + 1$.

Теорема 5.7. [272] Если $f_n(x_1, \dots, x_n) = x_1 x_2 x_3 \oplus x_1 x_4 \oplus x_2 x_5 \oplus x_3(x_4 \oplus x_5) \oplus x_6 x_7 \oplus x_8 x_9 \oplus \dots \oplus x_{n-1} x_n$, где $n = 2t + 1$, $n \geq 5$, то $\mu(f_n) = t + 1$.

Теорема 5.8. [272] Если $f_n(x_1, \dots, x_n) = x_1 x_2 x_3 \oplus x_1 x_4 \oplus x_2 x_5 \oplus x_3 x_6 \oplus x_7 x_8 \oplus x_9 x_{10} \oplus \dots \oplus x_{n-1} x_n$, где $n = 2t$, $n \geq 6$, то $\mu(f_n) = t + 1$.

Пусть Q – это множество всех квазиквадратичных функций алгебры логики, имеющих вид $\varphi(x_1, x_2, x_3) \oplus q(x_1, \dots, x_n)$, где $\deg(\varphi) = 3$, а q – квадратичная функция, и $\mu_Q(n) = \max_{f(x_1, \dots, x_n) \in Q} \mu(f)$.

Следствие 5.1. [272] При $n \geq 5$ справедливо равенство $\mu_Q(n) = \lceil (n + 1)/2 \rceil$.

Все результаты диссертации являются новыми и получены автором самостоятельно. Результаты диссертации докладывались на научных и научно-исследовательских семинарах в Институте системного программирования РАН, в Казанском (Поволжском) федеральном университете, “Математические вопросы кибернетики” механико-математического факультета МГУ имени М.В. Ломоносова, “Дискретная математика и математическая кибернетика” факультета ВМК МГУ имени М.В. Ломоносова, а также на следующих конференциях:

- IV Международный семинар “Дискретная математика и ее приложения” (Москва, 29 января – 2 февраля 2001 г.)
- 31th International Symposium of Multiple-Valued Logic (Poland, Warsaw, May 22-24, 2001 y.)
- Международная школа-семинар “Дискретная математика и математическая кибернетика” (Ратмино, 31 мая–3 июня 2001 г.)
- V Международная конференция “Дискретные модели в теории управляющих систем” (Ратмино, 26–29 мая 2003 г.)
- VI Международная конференция “Дискретные модели в теории управляющих систем” (Москва, 7–11 декабря 2004 г.)
- IX Международный семинар “Дискретная математика и ее приложения”, посвященный 75-летию со дня рождения академика О.Б. Лупанова (Москва, 18–23 июня 2007 г.)
- Третья международная конференция по проблемам безопасности и противодействия терроризму. Секция: Математические вопросы безопасности информационных технологий, МАБИТ-2007 (Москва, МГУ имени М.В. Ломоносова, 25–27 октября 2007 г.)

- Четвертая международная научная конференция по проблемам безопасности и противодействия терроризму. Секция: Математические вопросы безопасности информационных технологий, МАБИТ-2008 (Москва, МГУ имени М.В. Ломоносова, 30–31 октября 2008 г.)
- VIII Международная конференция “Дискретные модели в теории управляющих систем” (Москва, 6–9 апреля 2009 г.)
- XV Международная конференция “Проблемы теоретической кибернетики” (Казань, 2009 г.)
- X Международный семинар “Дискретная математика и ее приложения” (Москва, 1–6 февраля 2010 г.)
- Десятая общероссийская научная конференция “Математика и безопасность информационных технологий”. Секция: Математические проблемы информационной безопасности (Москва, МГУ имени М.В. Ломоносова, 2011 г.)
- XI Международный семинар “Дискретная математика и ее приложения”, посвященный 80-летию со дня рождения академика О.Б. Лупанова (Москва, МГУ, 18–23 июня 2012 г.)
- 7th International Computer Science Symposium in Russia, CSR 2012 (Nizhny Novgorod, July, 3–7, 2012 y.)
- Тихоновские чтения (Москва, МГУ имени М.В. Ломоносова, 28 октября–1 ноября 2013 г.)
- Ломоносовские чтения (Москва, МГУ имени М. В. Ломоносова, 14–23 апреля 2014 г.)
- XVII международная конференция “Проблемы теоретической кибернетики” (Казань, 16–20 июня 2014 г.)

- Third Russian Finnish Symposium on Discrete Mathematics (Petrozavodsk, September 16–18, 2014 y.)
- Тихоновские чтения (Москва, МГУ имени М.В. Ломоносова, 2014 г.)
- IX Международная конференция “Дискретные модели в теории управляющих систем” (Москва и Подмосковье, 20–22 мая 2015 г.)

Результаты диссертации опубликованы в работах [221]– [275], из которых работы [223, 225, 231–233, 235, 239, 241, 244, 245, 248, 249, 252, 257, 258, 261, 267–270, 272–274], а также перевод работы [256] в журналах из списка рецензируемых изданий, рекомендованного ВАК. В совместной работе [245] автору диссертации принадлежат постановка задачи и теоремы 1.11 и 1.13 диссертации, в совместной работе [248] автору диссертации принадлежат постановка задачи и теорема 4.7 диссертации, в совместной работе [268] автору диссертации принадлежат постановка задачи и теорема 1.12 диссертации. Совместная работа [270] обзорна, в ней описан подход, разработанный автором диссертации при доказательстве полиномиальности распознавания самодвойственности функции k -значной логики по ее полиному, а также рассматриваются свойства функций алгебры логики, для распознавания которых можно применить этот подход.

Диссертация носит теоретический характер. При получении верхних оценок длины функций k -значных логик в различных классах полиномиальных форм описаны методы построения этих полиномиальных форм для произвольных функций. Эти методы могут применяться при проектировании цифровых устройств. Полученные в работе быстрые алгоритмы решения рассматриваемых задач могут применяться при решении этих задач на практике.

Основные результаты работы

1. Сформулированы задачи о длине функций k -значной логики в классах поляризованных полиномиальных форм (ППФ), обобщенно поляризованных полиномиальных форм (ОППФ) и полиномиальных нормальных форм (ПНФ) при простых $k \geq 3$. Найдены верхние и нижние оценки наибольшей длины функций k -значной логики в классах ППФ, ОППФ, ПНФ при простых $k \geq 3$ и в классе псевдополиномиальных форм (ПСПФ) при $k = 2$. Предложены методы построения соответствующих полиномиальных форм, обеспечивающие верхние оценки. При каждом простом k , $k \geq 3$, найдено точное значение наибольшей длины функций k -значной логики, зависящих от одной переменной, в классе ППФ.
2. Сформулирована задача о сложности систем функций алгебры логики и функций k -значной логики при простых $k \geq 3$ в классе ППФ. Найдены точные значения сложности самых сложных систем функций k -значной логики, содержащих хотя бы две функции, в классе ППФ при $k = 2$ и $k = 3$.
3. Сформулированы задачи о сложности полиномов, приближающих функции k -значной логики с заданной точностью при простых $k \geq 3$. Найдены оценки, в том числе асимптотически точные для длины и ранга полиномов по модулю k , приближающих с заданной точностью функции k -значной логики при простых k .
4. Найдены функциональные свойства функций k -значной логики, инвариантных относительно связных преобразований, и структурные свойства их полиномов относительно операций конечного поля из k элементов. При помощи этих свойств доказана полиномиальность задачи распознавания принадлежности функции k -значной логики, заданной полиномом

по модулю k , к предполным классам самодвойственных функций (при простых k). На основе полученного доказательства сформулирован подход к построению полиномиальных распознающих алгоритмов.

5. Доказана полиномиальность задачи распознавания сохранения функцией k -значной логики, заданной полиномом по модулю k , вполне рефлексивного и вполне транзитивного отношения (при простых k). Как следствие получена полиномиальность задач распознавания принадлежности функции k -значной логики, заданной полиномом по модулю k , к предполным классам монотонных функций, функций, сохраняющих разбиение, и к предполным классам типа В (при простых k). Доказана полиномиальность задачи распознавания принадлежности функции k -значной логики, заданной полиномом относительно операций конечного поля из k элементов, к предполным классам линейных функций.
6. Предложен канонический вид полиномиальных функций по составному модулю k . При каждом составном k доказана линейная оценка алгоритмической сложности (в алгоритмической модели схем из функциональных элементов, СФЭ) задачи распознавания полиномиальности функции k -значной логики, заданной вектором своих значений, и в случае положительного ответа построения вектора коэффициентов ее канонического полинома по модулю k .
7. Предложена алгоритмическая модель СФЭ с некоторым ограничением структуры – СФЭ с разделенными переменными (СФЭРП). В модели СФЭРП доказаны нелинейные нижние оценки, в том числе достижимые для алгоритмической сложности задачи построения вектора коэффициентов полинома Жегалкина функции алгебры логики, заданной вектором своих значений.

8. Найдены точные значения мультипликативной сложности функций алгебры логики, представимых как сумма по модулю два или произведения всех переменных и квадратичной функции, или двух мультиаффинных функций, а также найдено точное значения наибольшей мультипликативной сложности функций в одном классе квазиквадратичных функций. Разработаны методы построения СФЭ в базисе Жегалкина, обеспечивающие верхние оценки мультипликативной сложности для соответствующих функций.

Основные определения

Пусть $k \geq 2$ – натуральное число, $E_k = \{0, 1, \dots, k-1\}$. Определим на наборах из множества E_k^n частичный порядок: если $\alpha = (a_1, \dots, a_n) \in E_k^n$ и $\beta = (b_1, \dots, b_n) \in E_k^n$, то $\alpha \leq \beta$ при $a_i \leq b_i$ для всех $i = 1, \dots, n$. Множество E_k^n с этим частичным порядком $\leq$ будем называть n -мерным k -значным кубом. *Типом* набора $\alpha = (a_1, \dots, a_n) \in E_k^n$ назовем множество $t(\alpha) = \bigcup_{a_i \neq 0} \{i\} \subseteq \{1, \dots, n\}$. Если $E \subseteq E_k^n$, то $T(E) = \{t(\alpha) \mid \alpha \in E\}$ – семейство (множество) типов элементов из множества E . *Рангом* набора $\alpha = (a_1, \dots, a_n) \in E_k^n$ назовем число $r(\alpha) = |t(\alpha)|$. *Весом* набора $\alpha = (a_1, \dots, a_n) \in E_k^n$ назовем число $|\alpha| = \sum_{i=1}^n a_i$ (здесь рассматривается сумма целых чисел). *Слоем s* куба E_k^n назовем множество $\{\alpha \in E_k^n \mid |\alpha| = s\}$, $0 \leq s \leq (k-1) \cdot n$. Если $\alpha, \beta \in E_k^n$, то $\alpha + \beta, \alpha - \beta \in E_k^n$ – это наборы, полученные соответственно покординатной суммой и разностью по модулю k наборов α и β .

Для набора $\alpha \in E_k^n$ введем его тень “вверх” $\hat{S}(\alpha)$ и его тень “вниз” $\check{S}(\alpha)$:

$$\begin{aligned}\hat{S}(\alpha) &= \{\beta \in E_k^n \mid |\beta| = |\alpha| + 1, \alpha \leq \beta\}, \\ \check{S}(\alpha) &= \{\beta \in E_k^n \mid |\beta| = |\alpha| - 1, \beta \leq \alpha\}.\end{aligned}$$

Заметим, что если $\beta \in \check{S}(\alpha)$, то $|\alpha - \beta| = 1$.

Если $T \subseteq E_k^n$, то $\check{S}(T) = \bigcup_{\alpha \in T} \check{S}(\alpha)$. Множество $T, T \subseteq E_k^n$, назовем *затемняющим* множеством куба E_k^n , если $\check{S}(T) = E_k^n \setminus \widetilde{(k-1)}$, где $\widetilde{(k-1)} = (k-1, \dots, k-1)$ – наибольший набор из множества E_k^n . Множество $T, T \subseteq E_k^n$, назовем *покрытием полушарами* куба E_k^n , если $T \cup \check{S}(T) = E_k^n$. *Шаром* радиуса 1 с центром в точке $\alpha \in E_k^n$ называется множество $S_1(\alpha) = \{\alpha\} \cup \check{S}(\alpha) \cup \hat{S}(\alpha)$. Множество $T, T \subseteq E_k^n$, называется *покрытием шарами радиуса 1* куба E_k^n , если $\bigcup_{\alpha \in T} S_1(\alpha) = E_k^n$.

Функцией k -значной логики называется отображение $f(x_1, \dots, x_n) : E_k^n \rightarrow$

E_k , $n = 0, 1, \dots$. Множество всех функций k -значной логики обозначим как P_k , множество всех функций k -значной логики, зависящих от переменных $x_1, \dots, x_n$, обозначим как P_k^n . Функции двузначной логики (при $k = 2$) называются также функциями алгебры логики, или булевыми функциями. Переменная x_i называется *существенной* для функции k -значной логики $f(x_1, \dots, x_n)$, если найдутся такие элементы $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n \in E_k$, что функция k -значной логики $\varphi(x_i) = f(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n)$ принимает по меньшей мере два различных значения. *Вектором значений* функции k -значной логики $f(x_1, \dots, x_n)$ назовем вектор с координатами $f(\alpha)$, где все наборы $\alpha \in E_k^n$ перечислены в каком-то определенном, например, в лексико-графическом порядке. *Весом* $|f|$ функции k -значной логики $f(x_1, \dots, x_n)$ назовем число ненулевых координат в ее векторе значений.

Пусть $j_i(x)$, где $i \in E_k$, обозначает такую функцию k -значной логики, что $j_i(i) = 1$, и $j_i(x) = 0$ при $x \neq i$. Если $s(x) \in P_k^1$ и $m \geq 1$ – целое число, то $(s(x))^m$ обозначает *степень* функции $s(x)$, т.е.

$$(s(x))^m = \underbrace{s(x) \cdot s(x) \cdot \dots \cdot s(x)}_m, \quad m \geq 1, \quad (s(x))^0 = 1.$$

Если $s(x) = x$, то в выражении $(s(x))^m$ внешние скобки будем опускать и писать x^m .

Функция k -значной логики $f(x_1, \dots, x_n)$ называется симметрической, если для всех возможных значений переменных $x_1, \dots, x_n$ верно

$$f(\pi(x_1), \dots, \pi(x_n)) = f(x_1, \dots, x_n)$$

для произвольной перестановки π на множестве переменных $\{x_1, \dots, x_n\}$. Множество всех симметрических функций k -значной логики обозначим как S_k . Симметрическая функция $f(x_1, \dots, x_n)$ называется *периодической с периодом* $\tau = (\tau_0 \tau_1 \dots \tau_{T-1}) \in E_k^T$, если $f(\alpha) = \tau_j$ при $|\alpha| = j \pmod{T}$ для каждо-

го набора $\alpha \in E_k^n$. При этом число T называется длиной периода. Периодическую функцию k -значной логики $f(x_1, \dots, x_n)$ с периодом $\tau = (\tau_0 \tau_1 \dots \tau_{T-1}) \in E_k^T$ будем обозначать как $f_{(\tau_0 \tau_1 \dots \tau_{T-1})}^{(n)}$.

Функция k -значной логики задается (или представляется) полиномом по модулю k , если эту функцию можно записать в виде

$$\sum_{j=1}^l c_j X_j, \quad (1)$$

где $c_j \in E_k$ – коэффициенты, X_j – произведения переменных в некоторых степенях, и сложение и умножение рассматриваются по модулю k , $j = 1, \dots, l$. Мы будем полагать, что в представлениях вида (1) приведены подобные слагаемые и опущены слагаемые с нулевыми коэффициентами. Если $c_j = 0$ при всех $j = 1, \dots, l$, то мы говорим, что это пустой полином 0 с нулевым числом слагаемых, который представляет константу 0. Будем говорить, что моном X_j входит в полином вида (1) (или является слагаемым этого полинома), если коэффициент при нем не равен нулю, т.е. если $c_j \neq 0$. Множество всех функций k -значной логики, представимых полиномами по модулю k , обозначим как Pol_k , множество функций из Pol_k , зависящих от переменных $x_1, \dots, x_n$, обозначается как Pol_k^n . Каждая функция из множества Pol_k называется *полиномиальной*. Известно ([218], стр. 69), что $Pol_k = P_k$ тогда и только тогда, когда k – простое число.

Моном (одночлен) $X_\alpha = \prod_{i=1}^n x_i^{a_i}$, где $x_i^{a_i}$ – степени, назовем *соответствующим* набору $\alpha = (a_1, \dots, a_n) \in E_k^n$. *Типом* монома X_α , $\alpha \in E_k^n$, назовем множество $t(X_\alpha) = t(\alpha) \subseteq \{1, \dots, n\}$. *Рангом* монома X_α , $\alpha \in E_k^n$, назовем число $r(X_\alpha) = |t(\alpha)|$. *Степенью* монома X_α , $\alpha \in E_k^n$, назовем число $\deg(X_\alpha) = |\alpha|$.

Если k – простое число, то каждая функция k -значной логики $f(x_1, \dots, x_n)$

может быть однозначно задана полиномом вида

$$f(x_1, \dots, x_n) = \sum_{\alpha \in E_k^n: c_f(\alpha) \neq 0} c_f(\alpha) X_\alpha, \quad (2)$$

где $c_f(\alpha) \in E_k$ – коэффициенты, $\alpha \in E_k^n$, и операции сложения и умножения рассматриваются по модулю k [218] (стр. 69-71), [219] (стр. 38-39) (если $c_f(\alpha) = 0$ при всех $\alpha \in E_k^n$, то это пустой полином 0). Это представление функции k -значной логики назовем ее *полиномом по модулю k* . В двузначном случае полином по модулю 2 вида (2) называется полиномом Жегалкина. При простом k однозначно определенный полином по модулю k вида (2) для функции k -значной логики f будем обозначать как $P(f)$. При простом k вектором коэффициентов полинома $P(f)$ функции k -значной логики $f(x_1, \dots, x_n)$ называется вектор значений функции $c_f(x_1, \dots, x_n)$.

Везде в дальнейшем, если не оговорено другое, будем считать, что k – простое число, и под операциями сложения и умножения в формулах для функций k -значной логики понимается сложение и умножение по модулю k . При этом, если не оговорено другое, знак $\oplus$ обозначает операцию сложения по модулю два.

Рангом $r(f)$ (соответственно, *степенью* $\deg(f)$) функции k -значной логики $f(x_1, \dots, x_n)$ назовем наибольший ранг (соответственно, степень) среди слагаемых с ненулевыми коэффициентами в ее полиноме $P(f)$, $r(0) = \deg(0) = 0$ по определению. *Длиной* $l(f)$ функции k -значной логики $f(x_1, \dots, x_n)$ назовем число попарно различных слагаемых с ненулевыми коэффициентами в ее полиноме $P(f)$. Множеством (семейством) типов слагаемых полинома функции $f(x_1, \dots, x_n)$ назовем семейство $T(P(f))$ типов слагаемых с ненулевыми коэффициентами в полиноме $P(f)$. *Весом* $w(P(f))$ полинома функции k -значной логики $f(x_1, \dots, x_n)$ назовем число $|T(P(f))|$.

Функция k -значной логики $f(x_1, \dots, x_n)$ называется *аффинной*, если ее сте-

пень не больше единицы, т.е. если $\deg(f) \leq 1$. Аффинная функция k -значной логики $f(x_1, \dots, x_n)$ называется *линейной*, если $c_f(0, \dots, 0) = 0$. Функция k -значной логики $f(x_1, \dots, x_n)$ называется *мультиаффинной*, если эта функция может быть представлена в виде произведения некоторых аффинных функций. Функция k -значной логики $f(x_1, \dots, x_n)$ называется *квадратичной*, если ее степень равна двум, т.е. если $\deg(f) = 2$.

Мы будем рассматривать полиномиальные формы для функций k -значной логики. В общем виде, полиномиальной формой (ПФ) для функций k -значной логики будем называть формулу вида

$$\sum_{j=1}^l c_j X_j, \quad (3)$$

где $c_j \in E_k$, а X_j – это произведения функций k -значной логики определенного вида. Эти функции определенного вида будем называть базисными функциями. Мы будем считать, что в ПФ приведены подобные слагаемые, при этом мы будем полагать, что слагаемые X_j различны, если в них перемножаются разные совокупности базисных функций. Также будем считать, что в ПФ слагаемые с нулевыми коэффициентами ($c_j = 0$) опущены. Если $c_j = 0$ при всех $j = 1, \dots, l$, то мы говорим, что это пустая ПФ 0 с нулевым числом слагаемых, которая представляет константу 0. Мы будем говорить, что выражение X_j входит в некоторую ПФ (является слагаемым этой ПФ), если в этой ПФ коэффициент c_j при нем не равен нулю. Обычный полином по модулю k также является ПФ. Длиной $l(Q)$ ПФ Q назовем число ее попарно различных слагаемых с ненулевыми коэффициентами. Пусть K – какой-то класс полиномиальных форм, которыми представима каждая функция k -значной логики. Тогда *длиной* $l_k^K(f)$ функции $f \in P_k$ в классе ПФ K называется наименьшая из длин среди всех ПФ из класса K , которые задают функцию f . *Длиной* $L_k^K(n)$ функций k -значной логики в классе ПФ K

называется наибольшая из длин функций из множества P_k^n в классе ПФ K .

Различные полиномиальные формы отличаются видом их базисных функций. Мы будем рассматривать следующие полиномиальные формы: поляризованные полиномиальные формы (ППФ), обобщенно поляризованные полиномиальные формы (ОППФ), полиномиальные нормальные формы (ПНФ) и псевдополиномиальные формы (ПСПФ). Каждый следующий вид полиномиальной формы в этом перечислении является расширением предыдущего. Каждый из перечисленных видов полиномиальных форм будет строго определен в соответствующем разделе.

Пусть $A_k \subseteq P_k$ – свойство на множестве функций k -значной логики P_k . Тогда под задачей распознавания свойства A_k для функций k -значной логики, заданных полиномами по модулю k , мы понимаем следующую задачу.

Вход: функция k -значной логики $f(x_1, \dots, x_n)$, заданная в виде полинома $P(f)$.

Вопрос: верно ли, что $f \in A_k$.

При исследовании алгоритмической сложности распознавания свойств функций k -значной логики, заданных полиномами, мы будем подразумевать некоторую алгоритмически полную алгоритмическую модель, например, равнодоступную адресную машину (РАМ) [203] (стр. 15), на вход которой подается полином $P(f)$ функции k -значной логики $f(x_1, \dots, x_n)$ в виде слова $\alpha(P(f)) \in A^*$, где $A = E_k \cup \{+\} = \{0, 1, \dots, k-1, +\}$. А именно, если

$$P(f) = \sum_{\alpha=(a_1, \dots, a_n) \in E_k^n} c_f(\alpha) X_\alpha,$$

то

$$\alpha(P(f)) = \sum_{c_f(\alpha) \neq 0} c_f(\alpha) a_1 a_2 \dots a_n.$$

Отметим, что при этом длина $|\alpha(P(f))|$ слова $\alpha(P(f))$ равна $l(P(f)) \cdot (n + 2) - 1$.

При исследовании алгоритмической сложности построения полиномов по модулю k для функций k -значной логики и при исследовании мультипликативной сложности функций алгебры логики мы применяем алгоритмическую модель схем из функциональных элементов (СФЭ) [202] (стр. 25). *Схемой из функциональных элементов (СФЭ) S* в базисе (из функциональных элементов) $B \subseteq P_k$ называется ориентированный граф без ориентированных циклов $G = (V, E)$, в котором каждой вершине $v \in V$ с полустепеннью захода $d(v)$ приписаны пометки по правилам:

1) если $d(v) = 0$, то вершина v называется *входной* и ей приписывается или переменная x_i , или константа из множества E_k ;

2) если $d(v) \geq 1$, то вершина v называется *внутренней* и ей приписывается какая-то функция (функциональный элемент) $f \in B$, зависящая от $d(v)$ переменных, причем дуги, входящие в вершину v , по какому-то правилу согласуются с переменными функции f , при этом вершина v вместе с приписанной ей функцией f называется (функциональным) элементом в СФЭ;

3) какие-то из вершин (как входные, так и внутренние) называют *выходными* и им приписывают попарно различные выходные переменные y_j .

Если в СФЭ S входным вершинам приписаны переменные $x_1, \dots, x_n$ и выходным вершинам приписаны переменные $y_1, \dots, y_m$, говорят, что СФЭ S – это СФЭ с *входами* $x_1, \dots, x_n$ и *выходами* $y_1, \dots, y_m$ и обозначают ее как $S(x_1, \dots, x_n; y_1, \dots, y_m)$. *Сложностью* $L(S)$ СФЭ S назовем число ее внутренних вершин, т.е. число функциональных элементов в ней.

В каждой вершине v СФЭ $S(x_1, \dots, x_n; y_1, \dots, y_m)$ реализуется некоторая функция k -значной логики. Если вершина v – входная, тогда если ей приписана переменная x_i , то в вершине v реализуется функция $f_v = x_i$, а если ей приписана константа $a \in E_k$, то в вершине v реализуется функция $f_v = a$. Если вершина v – внутренняя, ей приписана функция $f \in B$, и в вершинах, из

которых ведут дуги в эту вершину v , реализуются (согласованно с переменными функции f) функции $f_1, \dots, f_{d(v)}$, то в вершине v реализуется функция $f_v = f(f_1, \dots, f_{d(v)})$. Будем полагать, что СФЭ $S(x_1, \dots, x_n; y_1, \dots, y_m)$ реализует систему $F_S = \{f_{y_1}, \dots, f_{y_m}\}$ функций, реализующихся в выходных ее вершинах $y_1, \dots, y_m$.

При исследовании мультипликативной сложности функций алгебры логики мы будем рассматривать СФЭ в базисе $B_P = \{x \& y, x \oplus y, 1\}$. *Мультипликативной* (или *конъюнктивной*) *сложностью* $\mu(S)$ СФЭ S в базисе $B_P = \{x \& y, x \oplus y, 1\}$ называется число вершин в этой СФЭ, которым приписаны функциональные элементы конъюнкции $\&$. *Мультипликативной* (или *конъюнктивной*) *сложностью* $\mu(F)$ системы функций F называется наименьшая мультипликативная сложность среди всех СФЭ в базисе $B_P = \{x \& y, x \oplus y, 1\}$, реализующих систему F . *Мультипликативной* (или *конъюнктивной*) *сложностью* $\mu(f)$ функции $f(x_1, \dots, x_n)$ называется наименьшая мультипликативная сложность среди всех СФЭ в базисе $B_P = \{x \& y, x \oplus y, 1\}$, реализующих функцию f .

Если $(X; \leq)$ – частично упорядоченное множество, и $E \subseteq X$, то под *наибольшим* (соответственно, *наименьшим*) элементом из E будем понимать такой элемент $a \in E$, что для любого элемента $x \in E$ верно $x \leq a$ (соответственно, верно $a \leq x$), а под *максимальным* (соответственно, *минимальным*) элементом из E будем понимать такой элемент $a \in E$, что для любого элемента $x \in E$ из того, что $a \leq x$ (соответственно, $x \leq a$) следует, что $x = a$. Если $x, y \in E$ и $x \leq y$, $x \neq y$, то будем обозначать это как $x < y$.

Биномиальные коэффициенты будем обозначать как C_n^r . Нам понадобятся следующие свойства биномиальных коэффициентов:

- 1) для всех $n \geq 1$ и $r \leq n$ верно $C_n^r \leq \frac{n^n}{r^r \cdot (n-r)^{n-r}}$ (полагаем, что $0^0 = 1$);
- 2) если $r = \lambda n$ для некоторого числа λ , $0 < \lambda < 1$, то $C_n^r \leq (\lambda)^{-\lambda n} \cdot (1 -$

$\lambda)^{-(1-\lambda)n}$.

Доказательство свойства 1 можно провести индукцией по значению n . Свойство 2 следует из свойства 1.

При доказательствах утверждений нам понадобится функция k -значной энтропии

$$H_k(x) = x \log_k \frac{1}{x} + (1-x) \log_k \frac{1}{1-x} + x \log_k(k-1)$$

на интервале $(0; 1)$ и ее свойства, которые несложно проверить:

- 1) функция $H_k(x)$ непрерывна на своей области определения;
- 2) $x = \frac{k-1}{k}$ – точка максимума, при $x \in (0; \frac{k-1}{k}]$ функция $H_k(x)$ строго возрастает, принимая значения из полуинтервала $(0; 1]$, а при $x \in [\frac{k-1}{k}; 1)$ функция $H_k(x)$ строго убывает, принимая значения из полуинтервала $[1; \log_k(k-1))$.

Если a – действительное число, то $[a]$ обозначает наибольшее целое число, не превосходящее число a , $\lceil a \rceil$ обозначает наименьшее целое число, не меньшее числа a .

Часть 1. Сложность полиномиальных представлений функций k -значной логики

1 Полиномиальные формы функций

В этом разделе исследуются представления функций k -значных логик полиномиальными формами различных видов. Все результаты этого раздела опубликованы в работах [230, 234–237, 239, 240, 245, 247, 249–251, 259, 263, 266–268, 273, 275].

В алгебре логики рассматривается представление функций поляризованными полиномиальными формами [115, 130, 191]. Пусть $\delta = (d_1, \dots, d_n) \in E_2^n$. Поляризованной полиномиальной формой (ППФ) по вектору поляризации δ называется сумма модулю 2 произведений выражений вида $(x_i \oplus d_i)$. Т.е. в ППФ каждая переменная x_i встречается или только без отрицания, или только с отрицанием, $i = 1, \dots, n$. Длиной $l(P)$ ППФ P называется число ее попарно различных слагаемых. Для каждой функции $f \in P_2^n$ ее представление по каждому вектору $\delta \in E_2^n$ однозначно. Обозначим это представление как $P^\delta(f)$. Для исследования сложности представления функций алгебры логики поляризованными полиномиальными формами вводится функция Шеннона $L_2^{\text{ППФ}}(n) = \max_{f \in P_2^n} \min_{\delta \in E_2^n} l(P^\delta(f))$ длины функций алгебры логики в классе ППФ. Т. Sasao [191], В.П. Супруном [130] получены оценки функции Шеннона $L_2^{\text{ППФ}}(n)$. Н.А. Перязевым в [115] найдено точное значение функции Шеннона: $L_2^{\text{ППФ}}(n) = \lfloor \frac{2}{3} \cdot 2^n \rfloor$.

На случай многозначных логик понятие поляризованной полиномиальной формы можно обобщать различными способами. Мы рассмотрим два вида обобщений, которые называем *поляризованные полиномиальные формы* и *обобщенно поляризованные полиномиальные формы*.

Пусть $k \geq 2$ – натуральное число. Назовем *вектором поляризации* δ произвольный набор $(d_1, \dots, d_n) \in E_k^n$. *Поляризованным мономом* по вектору поляризации $\delta = (d_1, \dots, d_n) \in E_k^n$ назовем произведение по модулю k выражений $(x_i + d_i)$ в некоторых степенях. *Поляризованной полиномиальной формой* (ППФ), или *поляризованным полиномом* по вектору поляризации $\delta \in E_k^n$ назовем сумму по модулю k поляризованных мономов по этому же вектору поляризации с некоторыми коэффициентами из E_k . Т.е. поляризованный полином – это сумма по модулю k произведений переменных, смещенных на некоторую величину, причем в поляризованном полиноме каждая переменная x_i смещена на величину $d_i \in E_k$, и эта величина d_i для переменной x_i не меняется от слагаемого к слагаемому. Длиной $l(P)$ ППФ P назовем число ее попарно различных слагаемых с ненулевыми коэффициентами. Длиной $l^{\text{ППФ}}(f)$ функции $f \in P_k$ в классе ППФ назовем наименьшую длину среди всех ППФ, задающих функцию f . Длиной (или функцией Шеннона длины) $L_k^{\text{ППФ}}(n)$ функций k -значной логики в классе ППФ назовем наибольшую длину в классе ППФ среди всех функций k -значной логики, зависящих от n переменных.

Если k – простое число, то в ППФ степень каждой переменной ограничим числом $(k - 1)$. Для доказательств удобно ввести соответствие между поляризованными мономами и наборами из E_k^n . Будем говорить, что набор $\alpha = (a_1, \dots, a_n) \in E_k^n$ и поляризованный по вектору $\delta = (d_1, \dots, d_n) \in E_k^n$ моном $X_\alpha^\delta = \prod_{i=1}^n (x_i + d_i)^{a_i}$, где $(x + d)^a$ – степени, *соответствуют* друг другу. Получаем, что ППФ по вектору поляризации $\delta \in E_k^n$ – это выражение вида

$$\sum_{\alpha \in E_k^n} c(\alpha) X_\alpha^\delta,$$

где $c(\alpha) \in E_k$ – коэффициенты. Мы будем полагать, что в ППФ всегда приведены все подобные слагаемые и опущены слагаемые с нулевыми коэффициентами.

ентами, при этом сумма по пустому множеству индексов – это пустая ППФ 0.

Теорема 1.1. [235] *Если k – простое число, то для каждого вектора поляризации $\delta \in E_k^n$ каждую функцию k -значной логики $f(x_1, \dots, x_n)$ можно задать единственной ППФ по этому вектору δ .*

Доказательство. Пусть $\delta = (d_1, \dots, d_n) \in E_k^n$, и $f(x_1, \dots, x_n) \in P_k$.

Рассмотрим функцию $g(x_1, \dots, x_n) = f(x_1 - d_1, \dots, x_n - d_n) \in P_k$. Функция $g \in P_k$ представима полиномом по модулю k [218] (стр. 69), т.к. k – простое число. Пусть $g(x_1, \dots, x_n) = \sum_{\alpha \in E_k^n} c_g(\alpha) X_\alpha$ для некоторых $c_g(\alpha) \in E_k$.

Тогда $f(x_1, \dots, x_n) = g(x_1 + d_1, \dots, x_n + d_n) = \sum_{\alpha \in E_k^n} c_g(\alpha) X_\alpha^\delta$. Существование ППФ по вектору δ для функции f доказано.

Докажем единственность. Пусть найдутся две различные ППФ Q_1 и Q_2 по вектору δ для функции $f(x_1, \dots, x_n)$. Тогда по этим ППФ Q_1 и Q_2 получаются два различных полинома по модулю k для функции k -значной логики $g(x_1, \dots, x_n)$, где

$$g(x_1, \dots, x_n) = f(x_1 - d_1, \dots, x_n - d_n).$$

А это противоречит тому, что при простых k каждая функция k -значной логики задается единственным полиномом по модулю k вида (2) [218] (стр. 69-71), [219] (стр. 38-39). Значит, ППФ по вектору δ для функции f однозначна.

Теорема 1.1 доказана. □

Однозначную ППФ по вектору поляризации $\delta \in E_k^n$ для функции $f \in P_k^n$ будем обозначать как $P^\delta(f)$.

Сначала мы установим (теорема 1.2) точное значение длины функций k -значной логики, зависящих от одной переменной, в классе ППФ (при простых k).

Теорема 1.2. [239] *Если $k \geq 3$ – простое число, то $L_k^{\text{ППФ}}(1) = k - 1$.*

Доказательство. 1. Верхняя оценка. Рассмотрим произвольную функцию $f(x) \in P_k$. Пусть ее полином по модулю k имеет вид

$$P(f) = c_{k-1} \cdot x^{k-1} + \dots + c_1 \cdot x + c_0,$$

где $c_{k-1}, \dots, c_1, c_0 \in E_k$. Если $c_{k-1} = 0$, то в качестве ППФ функции $f(x)$ оставим ее полином по модулю k . Его длина не больше $(k-1)$. В противном случае выполним следующие преобразования:

1) вынесем за скобки множитель c_{k-1} :

$$f(x) = c_{k-1} \cdot \left(x^{k-1} + \frac{c_{k-2}}{c_{k-1}} \cdot x^{k-2} + \dots + \frac{c_1}{c_{k-1}} \cdot x + \frac{c_0}{c_{k-1}} \right);$$

2) в выражении, оставшемся в скобках, выделим слагаемые, образующие разложение в полином степени $(x+d)^{k-1}$, где элемент d выбирается так, чтобы поглотить слагаемое $c_{k-2} \cdot x^{k-2}$:

$$\begin{aligned} f(x) &= c_{k-1} \cdot (x^{k-1} + (k-1) \cdot \frac{c_{k-2}}{c_{k-1} \cdot (k-1)} \cdot x^{k-2} + \dots) = \\ &= c_{k-1} \cdot (x+d)^{k-1} + c'_{k-3} \cdot x^{k-3} + \dots + c'_1 \cdot x + c'_0, \end{aligned}$$

где $d = \frac{c_{k-2}}{c_{k-1} \cdot (k-1)}$, и $c'_{k-3}, \dots, c'_1, c'_0 \in E_k$.

Представим функцию $f(x)$ ППФ, поляризованной по вектору $\delta = (d) \in E_k^1$. Ее длина будет не больше $(k-1)$.

2. Нижняя оценка. Рассмотрим функцию $f(x) = a \cdot x^{k-1} + (x+1)^{k-1} \in P_k$, где $a \in E_k$, $a \neq 0$, $a \neq k-1$. Докажем, что коэффициент a можно так подобрать, что при любой поляризации переменной x получаемый поляризованный полином будет иметь не менее $(k-1)$ слагаемого.

Запишем полином функции $f(x)$, поляризованный по вектору $\delta = (-d) \in E_k^1$:

$$\begin{aligned} f(x+d) &= a \cdot (x+d)^{k-1} + (x+d+1)^{k-1} = \\ &= c_{k-1} \cdot x^{k-1} + c_{k-2} x^{k-2} + \dots + c_1 x + c_0, \end{aligned} \tag{4}$$

где $c_{k-1} = a + 1 \neq 0$, $c_{k-2}, \dots, c_1, c_0 \in E_k$.

Каждый коэффициент $c_{(k-1)-i}$ вычисляется как $C_{k-1}^{(k-1)-i} \cdot (a \cdot d^i + (d+1)^i)$, $i = 1, \dots, k-1$. Заметим, что если $d = 0$, то каждый из коэффициентов $c_{k-1}, c_{k-2}, \dots, c_1, c_0 \in E_k$ не равен нулю.

Для $d \neq 0$ проведем доказательство от противного. Предположим, что среди коэффициентов $c_{k-2}, \dots, c_1, c_0$ по меньшей мере два нулевых. Пусть их номера равны $(k-i)$ и $(k-j)$, где $i < j$. Тогда

$$C_{k-1}^{(k-1)-i} \cdot (a \cdot d^i + (d+1)^i) = 0,$$

$$C_{k-1}^{(k-1)-j} \cdot (a \cdot d^j + (d+1)^j) = 0.$$

Или, т.к. $C_{k-1}^{(k-1)-i} \neq 0$ и $C_{k-1}^{(k-1)-j} \neq 0$,

$$a \cdot d^i + (d+1)^i = 0, \tag{5}$$

$$a \cdot d^j + (d+1)^j = 0. \tag{6}$$

Выразим $(d+1)^i$ из равенства (5) и подставим в равенство (6). Получим

$$a \cdot d^j - a \cdot d^i \cdot (d+1)^{j-i} = 0.$$

Отсюда

$$a \cdot d^i \cdot (d^{j-i} - (d+1)^{j-i}) = 0.$$

Т.к. $a \cdot d^i \neq 0$, получаем

$$d^{j-i} = (d+1)^{j-i}. \tag{7}$$

Обозначим разность $(j-i)$ как m , $1 \leq m \leq k-2$. Тогда, поделив левую и правую части равенства 7 на d^m (заметим, что $d^m \neq 0$), мы получим

$$\left(1 + \frac{1}{d}\right)^m = 1,$$

или

$$(1+b)^m = 1, \tag{8}$$

где $b = \frac{1}{d}$. Пусть m_1 – наибольший общий делитель чисел m и $(k - 1)$, т.е. $m_1 \cdot m_2 = m$ и $m_1 \cdot s = k - 1$, где числа m_2 и s – взаимно просты, причем $s > 1$, т.к. $m \leq k - 2$.

Рассмотрим элемент $(1 + b)$ поля $(E_k; +, \cdot)$, где $+$ и $\cdot$ обозначают соответственно операции сложения и умножения по модулю k . Пусть e – примитивный элемент поля $(E_k; +, \cdot)$. Тогда

$$1 + b = e^t$$

для некоторого t , $1 \leq t \leq k - 1$. Рассмотрим элементы поля $(E_k; +, \cdot)$

$$(1 + b), (1 + b)^2, \dots, (1 + b)^{m-1}, (1 + b)^m.$$

Перепишем их в виде

$$e^t, e^{2t}, \dots, e^{(m-1)t}, e^{mt}. \quad (9)$$

По равенству (8) $e^{mt} = 1 = e^{k-1}$, откуда $m \cdot t = (k - 1) \cdot l_1$, где l_1 – некоторое натуральное число, или $m_1 \cdot m_2 \cdot t = m_1 \cdot s \cdot l_1$. Сократим левую и правую части на m_1 ($m_1 \neq 0$). Получим $m_2 \cdot t = s \cdot l_1$, причем число s , $s > 1$, – делитель числа $(k - 1)$. Заметим, что число t обязано делиться на число s .

Теперь докажем, что в ряду (9) не может встретиться примитивный элемент e . Предположим противное. Пусть $e = (1 + b)^r = e^{rt}$ для некоторого числа r , $1 \leq r < m$. Отсюда $r \cdot t = (k - 1) \cdot l_2 + 1$, где l_2 – некоторое натуральное число. Получаем противоречие, т.к. левая часть этого равенства делится на s , а правая часть при делении на s дает в остатке 1.

Следовательно, все степени элемента $(1 + b)$ не равны примитивному элементу e . Положим, что $a = -e$, $a \neq 0$, $a \neq k - 1$. Из равенства (5) получаем

$$a = - \left(1 + \frac{1}{d} \right)^i = -(1 + b)^i. \quad (10)$$

Но по доказанному равенство (10) при $a = -e$ не может выполняться, если

среди коэффициентов $c_{k-2}, \dots, c_1, c_0$ в выражении (4) по меньшей мере два нулевые.

Таким образом, доказано, что $l^{\text{ППФ}}(f) \geq k - 1$.

Сопоставляя верхнюю и нижнюю оценку получаем, что $L_k^{\text{ППФ}}(1) = k - 1$.

Теорема 1.2 доказана. $\square$

Следствие 1.1. [239] *Если $k \geq 3$ – простое число, то $L_k^{\text{ППФ}}(n) \geq (k - 1)^n$.*

Доказательство. Достаточно рассмотреть функцию

$$g(x_1, \dots, x_n) = f(x_1) \cdot f(x_2) \cdot \dots \cdot f(x_n),$$

где $f(x)$ – функция, построенная при доказательстве нижней оценки в теореме 1.2. $\square$

Теперь найдем верхнюю оценку длины функций k -значной логики в классе ППФ.

Теорема 1.3. [235] *Если k – простое число, то $L_k^{\text{ППФ}}(n) < \frac{k(k-1)}{k(k-1)+1} \cdot k^n$.*

Доказательство. Доказательство проведем индукцией по числу n .

Базис индукции: пусть $n = 1$. В теореме 1.2 доказано, что для произвольной функции $f(x) \in P_k$ можно подобрать такой вектор поляризации $\delta \in E_k^1$, что $l(P^\delta(f)) \leq k - 1$.

Проверим выполнение утверждения теоремы 1.3 при $n = 1$:

$$\begin{aligned} l(P^\delta(f)) \leq k - 1 &< \frac{k(k-1)}{k(k-1)+1} \cdot k^1 = \frac{(k(k-1)+1)-1}{k(k-1)+1} \cdot k^1 = \\ &= k - \frac{k}{k(k-1)+1}. \end{aligned}$$

Индуктивный переход. Предположим, что теорема 1.3 верна при некотором значении n . Докажем, что в таком случае теорема также верна и при значении $(n+1)$. Некоторые идеи индуктивного перехода почерпнуты из [115].

Рассмотрим произвольную функцию $f(x_1, \dots, x_n, x_{n+1}) \in P_k^{n+1}$. Представим ее полином $P(f)$ в виде

$$P(f) = \sum_{i=0}^{k-1} x_{n+1}^i \cdot f_i(x_1, \dots, x_n),$$

где $f_{k-1}, \dots, f_1, f_0 \in P_k^n$.

По предположению индукции существует ППФ функции $f_{k-1}(x_1, \dots, x_n)$, длина которой меньше $\frac{k(k-1)}{k(k-1)+1} \cdot k^n$. Пусть $\delta' = (d_1, \dots, d_n) \in E_k^n$ – вектор поляризации этой ППФ.

Запишем каждую из функций

$$f_{k-1}(x_1, \dots, x_n), f_{k-2}(x_1, \dots, x_n), \dots, f_1(x_1, \dots, x_n), f_0(x_1, \dots, x_n)$$

ППФ, поляризованными по вектору δ' . В результате получим ППФ функции $f(x_1, \dots, x_n, x_{n+1})$, поляризованную по вектору $(d_1, \dots, d_n, 0) \in E_k^{n+1}$.

Рассмотрим ППФ $P^{\delta'}(f_{k-1})$ и $P^{\delta'}(f_{k-2})$. Пусть каждый из поляризованных по вектору δ' мономов $X_\alpha^{\delta'}$, $\alpha \in E_k^n$, входит в ППФ $P^{\delta'}(f_{k-1})$ и $P^{\delta'}(f_{k-2})$ с коэффициентами $c'_\alpha \in E_k$ и $c''_\alpha \in E_k$ соответственно.

Рассмотрим следующие ППФ по вектору поляризации δ' :

$$Q_j(x_1, \dots, x_n) = \sum_{\alpha: c'_\alpha \neq 0, c''_\alpha = j} c'_\alpha X_\alpha^{\delta'},$$

где $j \in E_k$, и

$$Q_k(x_1, \dots, x_n) = \sum_{\alpha: c''_\alpha = 0} c''_\alpha X_\alpha^{\delta'}.$$

Заметим, что ППФ $Q_0, Q_1, \dots, Q_{k-1}, Q_k$ не содержат одинаковых слагаемых.

Следовательно,

$$\sum_{j=0}^k l(Q_j) \leq k^n.$$

Кроме того верно, что

$$P^{\delta'}(f_{k-1}) = \sum_{j=0}^{k-1} Q_j,$$

откуда, применяя предыдущее замечание и выбор вектора поляризации δ' , получаем

$$\sum_{j=0}^{k-1} l(Q_j) < \frac{k(k-1)}{k(k-1)+1} \cdot k^n.$$

Выберем такой номер d , $d \in E_k$, что

$$l(Q_d) \geq \frac{1}{k} \cdot l(P^{\delta'}(f_{k-1})).$$

Такой номер всегда можно выбрать.

Рассмотрим ППФ для функции $f(x_1, \dots, x_n, x_{n+1})$, поляризованную по вектору $\delta = (d_1, \dots, d_n, -d) \in E_k^{n+1}$. Эту ППФ можно записать в виде:

$$\begin{aligned} P^\delta(f) = & (x_{n+1} - d)^{k-1} \left(\sum_{j=0}^{k-1} Q_j \right) + (x_{n+1} - d)^{k-2} \left(Q_k + \sum_{j \in E_k, j \neq d} c_j \cdot Q_j \right) + \\ & + \sum_{i=0}^{k-3} (x_{n+1} - d)^i g_i(x_1, \dots, x_n), \end{aligned}$$

где $c_j \in E_k$ – некоторые коэффициенты, $j = 0, \dots, k-1$, $j \neq d$, а $g_{k-3}, \dots, g_1, g_0$ – некоторые функции. Тогда

$$l(P^\delta(f)) \leq \left(\sum_{j=0}^k l(Q_j) \right) + \left(\sum_{j \in E_k, j \neq d} l(Q_j) \right) + \left(\sum_{i=0}^{k-3} l(P^{\delta'}(g_i)) \right).$$

Верны следующие неравенства:

$$\begin{aligned} \sum_{j=0}^k l(Q_j) & \leq k^n, \\ \sum_{j \in E_k, j \neq d} l(Q_j) & < \frac{k-1}{k} \cdot \frac{k(k-1)}{k(k-1)+1} \cdot k^n, \\ l(P^{\delta'}(g_i)) & \leq k^n, i = 0, 1, \dots, k-3. \end{aligned}$$

Отсюда получаем

$$\begin{aligned} l(P^\delta(f)) &< (k-1) \cdot k^n + \frac{k-1}{k} \cdot \frac{k(k-1)}{k(k-1)+1} \cdot k^n = \\ &= (k-1) \cdot \left(1 + \frac{(k-1)}{k(k-1)+1}\right) \cdot k^n = \frac{k(k-1)}{k(k-1)+1} \cdot k^{n+1}. \end{aligned}$$

Теорема 1.3 доказана. □

Теперь найдем нижнюю оценку длины функций k -значной логики в классе ППФ. Доказательство следующей теоремы 1.4 практически дословно повторяет доказательство нижней оценки для длины функций k -значных логик в классе обобщенно поляризованных полиномов из [249].

Теорема 1.4. [237] *Если k – простое число, то $L_k^{\text{ППФ}}(n) \geq \frac{k-1}{k} \cdot (1 - \varepsilon(n)) \cdot k^n$ для некоторой такой функции $\varepsilon(n)$, что $\varepsilon(n) \rightarrow 0$ при $n \rightarrow \infty$.*

Доказательство. Для получения нижней оценки применим мощностные рассуждения. Пусть L , $L < \frac{k-1}{k} \cdot k^n$, – некоторое натуральное число. Найдем число ППФ с длиной, не большей L , которые задают функции k -значной логики, зависящие от переменных $x_1, \dots, x_n$.

Всего мономов над переменными $x_1, \dots, x_n$ есть k^n , полиномов длины, не большей L , из них можно составить $\sum_{i=0}^L C_{k^n}^i (k-1)^i$. Всего поляризаций есть k^n . Поэтому поляризованных полиномов от переменных $x_1, \dots, x_n$ длины, не большей L , не более

$$\sum_{i=0}^L C_{k^n}^i (k-1)^i k^n. \quad (11)$$

Для оценки полученного выражения воспользуемся свойствами биномиальных коэффициентов и функции k -значной энтропии $H_k(x)$. Оценим выражение (11):

$$k^n \cdot \sum_{i=0}^L C_{k^n}^i (k-1)^i \leq L C_{k^n}^L (k-1)^L k^n \leq$$

$$\leq L \frac{(k^n)^{k^n}}{L^L (k^n - L)^{k^n - L}} (k - 1)^L k^n \leq L k^{H_k(\frac{L}{k^n}) k^n} k^n. \quad (12)$$

Пусть $\varepsilon > 0$ – действительное число, и $L \leq (\frac{k-1}{k} - \varepsilon)k^n$. Тогда по свойствам функции k -значной энтропии $H_k(x)$ найдется такое действительное число ε_1 , $\varepsilon_1 > 0$, что

$$H_k\left(\frac{L}{k^n}\right) \leq H_k\left(\frac{k-1}{k} - \varepsilon\right) \leq 1 - \varepsilon_1.$$

Отсюда для выражения (11) находим

$$L k^{H_k(\frac{L}{k^n}) k^n} k^n \leq \left(\frac{k-1}{k} - \varepsilon\right) k^{2n} k^{(1-\varepsilon_1)k^n}.$$

Полученное выражение при $n \rightarrow \infty$ растет медленнее, чем k^{k^n} . Другими словами, для каждого действительного числа $\varepsilon > 0$ при $L \leq (\frac{k-1}{k} - \varepsilon)k^n$ ППФ длины, не большей L , не хватит, чтобы задать все функции от переменных $x_1, \dots, x_n$. Отсюда получаем утверждение теоремы 1.4.

Теорема 1.4 доказана. □

Таким образом, полученная нижняя мощностная оценка длины функций k -значной логики в классе ППФ асимптотически не совпадает с полученной нами верхней оценкой для этой же длины. В двузначном случае Н.А. Перязевым доказано, что нижняя мощностная оценка не является асимптотически точной в классе ППФ. Им была построена последовательность симметрических функций алгебры логики $f_n(x_1, \dots, x_n)$, для длины которых верно $l^{\text{ППФ}}(f_n) \geq \lfloor \frac{2}{3} \cdot 2^n \rfloor$ [115]. Н.К. Маркелов построил такую последовательность функций трехзначной логики $f_n(x_1, \dots, x_n)$, что $l^{\text{ППФ}}(f_n) \geq \lfloor \frac{3}{4} \cdot 3^n \rfloor$ [100]. Таким образом, в трехзначном случае длина функций в классе ППФ также растет быстрее, чем полученная нижняя мощностная оценка.

Мы строим последовательность симметрических функций трехзначной логики $f_n(x_1, \dots, x_n)$, длина которых в классе ППФ также растет как $\lfloor \frac{3}{4} \cdot 3^n \rfloor$ при

$n \rightarrow \infty$. Для построения этой последовательности симметрических функций трехзначной логики рассмотрим периодические функции трехзначной логики $f_{(1122)}^{(n)}$ и $f_{(1221)}^{(n)}$ с периодами длины 4. Для простоты обозначим их как f_n и g_n .

Лемма 1.1. [273] *При $n \geq 1$ для периодических функций трехзначной логики $f_n = f_{(1122)}^{(n)}$, $g_n = f_{(1221)}^{(n)}$ верны следующие равенства:*

$$\begin{aligned} f_{n+1} &= j_0(x_{n+1})f_n + j_1(x_{n+1})g_n + j_2(x_{n+1})2f_n = \\ &= x_{n+1}^2 2g_n + x_{n+1} 2(f_n + g_n) + f_n = \\ &= (x_{n+1} + 1)^2 2g_n + (x_{n+1} + 1)(2f_n + g_n) + 2f_n = \\ &= (x_{n+1} + 2)^2 2g_n + (x_{n+1} + 2)2f_n + g_n. \end{aligned}$$

Доказательство. Рассмотрим функцию $f_{(1122)}^{(n+1)}(x_1, \dots, x_n, x_{n+1})$. По определению функций $j_i(x) \in P_3$, $i \in E_3$, ее можно записать в виде

$$f_{(1122)}^{(n+1)} = j_0(x_{n+1})f_{(1122)}^{(n)} + j_1(x_{n+1})f_{(1221)}^{(n)} + j_2(x_{n+1})f_{(2211)}^{(n)},$$

или

$$f_{n+1} = j_0(x_{n+1})f_n + j_1(x_{n+1})g_n + j_2(x_{n+1})2f_n.$$

Проверим выполнение оставшихся трех равенств. Для этого подставим значения $x_{n+1} = 0, 1, 2$. Проверим равенство

$$f_{n+1} = j_0(x_{n+1})f_n + j_1(x_{n+1})g_n + j_2(x_{n+1})2f_n = x_{n+1}^2 2g_n + x_{n+1} 2(f_n + g_n) + f_n :$$

$$x_{n+1} = 0 : f_n = f_n,$$

$$x_{n+1} = 1 : 2g_n + 2(f_n + g_n) + f_n = g_n,$$

$$x_{n+1} = 2 : 2g_n + (f_n + g_n) + f_n = 2f_n.$$

Проверим равенство

$$\begin{aligned} f_{n+1} &= j_0(x_{n+1})f_n + j_1(x_{n+1})g_n + j_2(x_{n+1})2f_n = \\ &= (x_{n+1} + 1)^2 2g_n + (x_{n+1} + 1)(2f_n + g_n) + 2f_n : \end{aligned}$$

$$\begin{aligned}
x_{n+1} = 0 &: (0+1)^2 2g_n + (0+1)(2f_n + g_n) + 2f_n = f_n, \\
x_{n+1} = 1 &: (1+1)^2 2g_n + (1+1)(2f_n + g_n) + 2f_n = g_n, \\
x_{n+1} = 2 &: (2+1)^2 2g_n + (2+1)(2f_n + g_n) + 2f_n = 2f_n.
\end{aligned}$$

Проверим равенство

$$\begin{aligned}
f_{n+1} &= j_0(x_{n+1})f_n + j_1(x_{n+1})g_n + j_2(x_{n+1})2f_n = \\
&= (x_{n+1} + 2)^2 2g_n + (x_{n+1} + 2)2f_n + g_n :
\end{aligned}$$

$$\begin{aligned}
x_{n+1} = 0 &: (0+2)^2 2g_n + (0+2)2f_n + g_n = 2g_n + f_n + g_n = f_n, \\
x_{n+1} = 1 &: (1+2)^2 2g_n + (1+2)2f_n + g_n = g_n, \\
x_{n+1} = 2 &: (2+2)^2 2g_n + (2+2)2f_n + g_n = 2g_n + 2f_n + g_n = 2f_n.
\end{aligned}$$

Лемма 1.1 доказана. □

Следующие леммы 1.2–1.4 доказываются аналогично доказательству леммы 1.1.

Лемма 1.2. [273] *При $n \geq 1$ для периодических функций трехзначной логики $f_n = f_{(1122)}^{(n)}$, $g_n = f_{(1221)}^{(n)}$ верны следующие равенства:*

$$\begin{aligned}
g_{n+1} &= j_0(x_{n+1})g_n + j_1(x_{n+1})2f_n + j_2(x_{n+1})2g_n = \\
&= x_{n+1}^2 f_n + x_{n+1}(f_n + 2g_n) + g_n = \\
&= (x_{n+1} + 1)^2 f_n + (x_{n+1} + 1)2(f_n + g_n) + 2g_n = \\
&= (x_{n+1} + 2)^2 f_n + (x_{n+1} + 2)2g_n + 2f_n.
\end{aligned}$$

Лемма 1.3. [273] *При $n \geq 1$ для периодических функций трехзначной логики $f_n = f_{(1122)}^{(n)}$, $g_n = f_{(1221)}^{(n)}$ верны следующие равенства:*

$$\begin{aligned}
f_{n+1} + g_{n+1} &= j_0(x_{n+1})(f_n + g_n) + j_1(x_{n+1})(2f_n + g_n) + j_2(x_{n+1})2(f_n + g_n) = \\
&= x_{n+1}^2 (f_n + 2g_n) + x_{n+1}g_n + (f_n + g_n) = \\
&= (x_{n+1} + 1)^2 (f_n + 2g_n) + (x_{n+1} + 1)f_n + 2(f_n + g_n) = \\
&= (x_{n+1} + 2)^2 (f_n + 2g_n) + (x_{n+1} + 2)2(f_n + g_n) + 2f_n + g_n.
\end{aligned}$$

Лемма 1.4. [273] При $n \geq 1$ для периодических функций трехзначной логики $f_n = f_{(1122)}^{(n)}$, $g_n = f_{(1221)}^{(n)}$ верны следующие равенства:

$$\begin{aligned}
2f_{n+1} + g_{n+1} &= j_0(x_{n+1})(2f_n + g_n) + j_1(x_{n+1})2(f_n + g_n) + \\
&\quad + j_2(x_{n+1})(f_n + 2g_n) = \\
&= x_{n+1}^2(f_n + g_n) + x_{n+1}2f_n + 2f_n + g_n = \\
&= (x_{n+1} + 1)^2(f_n + g_n) + (x_{n+1} + 1)g_n + f_n + 2g_n = \\
&= (x_{n+1} + 2)^2(f_n + g_n) + (x_{n+1} + 2)(f_n + 2g_n) + 2(f_n + g_n).
\end{aligned}$$

Пусть h_n обозначает функцию $f_{(2010)}^{(n)}$, t_n обозначает функцию $f_{(0102)}^{(n)}$. Заметим, что

$$f_n + g_n = f_{(2010)}^{(n)} = h_n, \quad 2f_n + g_n = f_{(0102)}^{(n)} = t_n.$$

Пусть $\delta' = (d_1, \dots, d_n, d_{n+1}) \in E_3^{n+1}$ – вектор поляризации, обозначим вектор $(d_1, \dots, d_n) \in E_3^n$ как δ . Если имеет место равенство

$$P^{\delta'}(q_{n+1}) = a(x_{n+1} + d)^2 P^\delta(q'_n) + b(x_{n+1} + d)P^\delta(q''_n) + cP^\delta(q'''_n),$$

где $q, q', q'', q''' \in \{f, g, h, t\}$, $a, b, c \in \{1, 2\}$, то упорядоченную тройку символов $q'q''q'''$ назовем *типом* функции q_{n+1} при поляризации d_{n+1} по переменной x_{n+1} . Заметим, что при этом верно, что

$$l(P^{\delta'}(q_{n+1})) = l(P^\delta(q'_n)) + l(P^\delta(q''_n)) + l(P^\delta(q'''_n)).$$

Таблицу типов функций $f_{n+1}, g_{n+1}, h_{n+1}, t_{n+1}$ при каждой из поляризаций переменной x_{n+1} выпишем в следующей лемме 1.5. Лемма 1.5 является непосредственным следствием лемм 1.1–1.4.

Лемма 1.5. [273] При $n \geq 1$ периодические функции трехзначной логики $f_{n+1} = f_{(1122)}^{(n+1)}$, $g_{n+1} = f_{(1221)}^{(n+1)}$, $h_{n+1} = f_{n+1} + g_{n+1}$, $t_{n+1} = 2f_{n+1} + g_{n+1}$ имеют следующие типы при каждой из поляризаций переменной x_{n+1} (на пересечении строки q_{n+1} со столбцом d_{n+1} выписан тип функции q_{n+1} при поляризации

d_{n+1} переменной x_{n+1}):

$q_{n+1} \setminus d_{n+1}$	0	1	2
f_{n+1}	ghf	gtf	gfg
g_{n+1}	ftg	fhg	fgf
h_{n+1}	tgh	tfh	tht
t_{n+1}	hft	hgt	hth

Следующая лемма 1.6 описывает функции f_1, g_1, h_1, t_1 .

Лемма 1.6. [273] Для функций трехзначной логики $f_1 = f_{(1122)}^{(1)}$, $g_1 = f_{(1221)}^{(1)}$, $h_1 = f_1 + g_1$, $t_1 = 2f_1 + g_1$ имеют место следующие равенства:

$$\begin{aligned}
 f_1(x) &= 2x^2 + x + 1 = 2(x+1)^2 + 2 = 2(x+2)^2 + 2(x+2) + 1, \\
 g_1(x) &= x^2 + 1 = (x+1)^2 + (x+1) + 2 = (x+2)^2 + 2(x+2) + 2, \\
 h_1(x) &= x + 2 = (x+1) + 1 = (x+2), \\
 t_1(x) &= 2x^2 + 2x = 2(x+1)^2 + (x+1) = 2(x+2)^2 + 1.
 \end{aligned}$$

Доказательство. Выпишем таблицу значений функций f_1, g_1, h_1, t_1 :

x_1	f_1	g_1	h_1	t_1
0	1	1	2	0
1	1	2	0	1
2	2	2	1	0

По этой таблице получаем требуемые равенства.

Лемма 1.6 доказана. □

Следствие 1.2. [273] При каждой из поляризации (d), $d \in E_3$, переменной x_1 функции трехзначной логики $f_1 = f_{(1122)}^{(1)}$, $g_1 = f_{(1221)}^{(1)}$, $h_1 = f_1 + g_1$, $t_1 = 2f_1 + g_1$ имеют следующую длину (на пересечении строки q_1 со столбцом

(d) выписано значение $l(P^{(d)}(q_1))$:

$q_1 \setminus (d)$	(0)	(1)	(2)
f_1	3	2	3
g_1	2	3	3
h_1	2	2	1
t_1	2	2	2

Теперь найдем длину функций f_n, g_n в классе ППФ (теорема 1.5). Заметим, что каждая из этих функций является симметрической. Сначала докажем вспомогательную лемму 1.7.

Лемма 1.7. [273] *При $n \geq 1$ для периодических функций трехзначной логики $f_n = f_{(1122)}^{(n)}$, $g_n = f_{(1221)}^{(n)}$, $h_n = f_n + g_n$, $t_n = 2f_n + g_n$ верно следующее: если вектор поляризации $\delta = (d_1, \dots, d_n) \in E_3^n$ таков, что $d_i \in \{0, 1\}$ при всех $i = 1, \dots, n$, то четверка длин $l(\delta)$, где*

$$l(\delta) = (l(P^\delta(f_n)), l(P^\delta(g_n)), l(P^\delta(h_n)), l(P^\delta(t_n))),$$

имеет следующие свойства:

1) если n – нечетное число, то в этой четверке три числа $(3^{n+1} - 1)/4$ и одно число $(3^{n+1} - 1)/4 + 1$, причем $(3^{n+1} - 1)/4 + 1$ – это длина $l(P^\delta(f_n))$ или длина $l(P^\delta(g_n))$;

2) если n – четное число, то в этой четверке три числа $(3^{n+1} - 3)/4 + 1$ и одно число $(3^{n+1} - 3)/4$, причем $(3^{n+1} - 3)/4$ – это длина $l(P^\delta(h_n))$ или длина $l(P^\delta(t_n))$.

Доказательство. Докажем лемму 1.7 индукцией по значению n . *Базис индукции:* $n = 1$ и $n = 2$. Если $n = 1$, то справедливость леммы следует из следствия 1.2. Если $n = 2$, то по лемме 1.5 из четверки длин, в которой три числа 2 и одно число 3, причем 3 – это длина ППФ функции f_1 или функции

g_1 , получаем четверку длин, в которой три числа 7 и одно число 6, причем 6 – это длина ППФ функции h_2 или функции t_2 . Базис индукции обоснован.

Индуктивный переход: пусть для четверки длин $l(\delta)$, где $\delta = (d_1, \dots, d_n) \in E_3^n$, $d_i \in \{0, 1\}$, $i = 1, \dots, n$, утверждение леммы 1.7 верно. Рассмотрим четверку длин $l(\delta')$, где $\delta' = (d_1, \dots, d_n, d_{n+1})$, $d_{n+1} \in \{0, 1\}$. Рассмотрим все возможные случаи.

1) Если n – нечетное число, то в четверке длин $l(\delta)$ три числа $(3^{n+1} - 1)/4$ и одно число $(3^{n+1} - 1)/4 + 1$, причем $(3^{n+1} - 1)/4 + 1$ – это длина $l(P^\delta(f_n))$ или длина $l(P^\delta(g_n))$.

1а) Пусть $d_{n+1} = 0$. По лемме 1.5 четверка длин $l(\delta')$ получается сложением всеми возможными способами трех чисел из чисел четверки $l(\delta)$. Следовательно, в четверке $l(\delta')$ три числа равны

$$(3^{n+1} - 1)/4 + 1 + 2 \cdot ((3^{n+1} - 1)/4) = (3^{n+2} - 3)/4 + 1,$$

а четвертое число – на единицу меньше их, т.е. четвертое число равно $(3^{n+2} - 3)/4$. При этом это четвертое число равно длине $l(P^{\delta'}(h_{n+1}))$, если $l(P^\delta(f_n)) = (3^{n+1} - 1)/4 + 1$, и равно длине $l(P^{\delta'}(t_{n+1}))$, если $l(P^\delta(g_n)) = (3^{n+1} - 1)/4 + 1$.

1б) Случай $d_{n+1} = 1$ рассматривается аналогично.

2) Если n – четное число, то в четверке длин $l(\delta)$ три числа $(3^{n+1} - 3)/4 + 1$ и одно число $(3^{n+1} - 3)/4$, причем $(3^{n+1} - 3)/4$ – это длина $l(P^\delta(h_n))$ или длина $l(P^\delta(t_n))$.

2а) Пусть $d_{n+1} = 0$. По лемме 1.5 четверка длин $l(\delta')$ получается сложением всеми возможными способами трех чисел из чисел четверки $l(\delta)$. Следовательно, в четверке $l(\delta')$ три числа равны

$$(3^{n+1} - 3)/4 + 2 \cdot ((3^{n+1} - 3)/4 + 1) = (3^{n+2} - 1)/4,$$

а четвертое число – на единицу больше их, т.е. четвертое число равно $(3^{n+2} - 1)/4 + 1$. При этом это четвертое число равно длине $l(P^{\delta'}(f_{n+1}))$, если $l(P^\delta(t_n))$

$= (3^{n+1} - 3)/4$, и равно длине $l(P^{\delta'}(g_{n+1}))$, если $l(P^{\delta}(h_n)) = (3^{n+1} - 3)/4$.

2б) Случай $d_{n+1} = 1$ рассматривается аналогично.

Лемма 1.7 доказана. □

Теорема 1.5. [273] *При $n \geq 1$ для периодических функций трехзначной логики $f_n = f_{(1122)}^n$ и $g_n = f_{(1221)}^n$ верны следующие равенства:*

$$\begin{aligned} l^{\text{ППФ}}(f_n) &= l^{\text{ППФ}}(g_n) = (3^{n+1} - 1)/4, \text{ если } n - \text{нечетное число,} \\ l^{\text{ППФ}}(f_n) &= l^{\text{ППФ}}(g_n) = (3^{n+1} - 3)/4 + 1, \text{ если } n - \text{четное число.} \end{aligned}$$

Доказательство. Пусть $\delta = (d_1, \dots, d_n) \in E_3^n$ – произвольный вектор поляризации. Функции f_n и g_n являются симметрическими, поэтому, не ограничивая общности рассуждений, мы можем считать, что вектор δ имеет следующий вид: $d_1, \dots, d_s \in \{0, 1\}$, $d_{s+1} = \dots = d_n = 2$, $0 \leq s \leq n$.

1. Пусть $1 \leq s \leq (n - 1)$. Обозначим вектор $(d_1, \dots, d_s) \in E_3^s$ как δ_1 . По лемме 1.7 верно, что неупорядоченная пара длин $(l^{\delta_1}(f_s), l^{\delta_1}(g_s))$ имеет вид $((3^{s+1} - 1)/4 + 1, (3^{s+1} - 1)/4)$ при нечетных s , и $((3^{s+1} - 3)/4 + 1, (3^{s+1} - 3)/4 + 1)$ при четных s .

Докажем индукцией по значению $(n - s)$, что для пары чисел $l(P^{\delta}(f_n))$, $l(P^{\delta}(g_n))$ верно следующее: если n – нечетно, то каждое из этих чисел не меньше, чем $(3^{n+1} - 1)/4 + 1$; если n – четно, то каждое из этих чисел не меньше, чем $(3^{n+1} - 3)/4 + 1$.

Базис индукции: пусть $(n - s) = 1$.

1а) Если n – нечетное число, то по лемме 1.7 верно, что

$$l(P^{\delta_1}(f_s)) = l(P^{\delta_1}(g_s)) = (3^{s+1} - 3)/4 + 1.$$

По лемме 1.5 получаем, что

$$\begin{aligned} l(P^{\delta}(f_{s+1})) &= l(P^{\delta_1}(f_s)) + 2l(P^{\delta_1}(g_s)) = (3^{s+2} - 1)/4 + 1, \\ l(P^{\delta}(g_{s+1})) &= 2l(P^{\delta_1}(f_s)) + l(P^{\delta_1}(g_s)) = (3^{s+2} - 1)/4 + 1. \end{aligned}$$

1б) Если n – четное число, то по лемме 1.7 верно, что одно из чисел $l(P^{\delta_1}(f_s)), l(P^{\delta_1}(g_s))$ равно $((3^{s+1}-1)/4+1)$, а другое число равно $(3^{s+1}-1)/4$. По лемме 1.5 аналогично получаем, что одно из чисел $l(P^\delta(f_{s+1})), l(P^\delta(g_{s+1}))$ равно $(3^{s+2}-3)/4+2$, а другое число равно $(3^{s+2}-3)/4+1$.

Базис индукции обоснован.

Индуктивный переход. Обозначим вектор $(d_1, \dots, d_s, d_{s+1}, \dots, d_{n-1}) \in E_3^{n-1}$ как δ_2 . Пусть для пары чисел $l(P^{\delta_2}(f_{n-1})), l(P^{\delta_2}(g_{n-1}))$, $n-1 \geq s+1$, утверждение верно.

1в) Если n – нечетное число, то по индуктивному предположению верно, что каждое из чисел $l(P^{\delta_2}(f_{n-1})), l(P^{\delta_2}(g_{n-1}))$ не меньше, чем $(3^n-3)/4+1$. По лемме 1.5 получаем, что каждое из чисел $l(P^\delta(f_n)), l(P^\delta(g_n))$ не меньше, чем

$$3((3^n-3)/4+1) = (3^{n+1}-9)/4+3 = (3^{n+1}-1)/4+1.$$

1г) Если n – четное число, то по индуктивному предположению верно, что каждое из чисел $l(P^{\delta_2}(f_{n-1})), l(P^{\delta_2}(g_{n-1}))$ не меньше, чем $(3^n-1)/4+1$. По лемме 1.5 получаем, что каждое из чисел $l(P^\delta(f_n)), l(P^\delta(g_n))$ не меньше, чем

$$3((3^n-1)/4+1) = (3^{n+1}-3)/4+3.$$

2. Пусть $s = 0$. Тогда по лемме 1.5

$$l(P^\delta(f_n)) = l(P^\delta(g_n)) = 3^n.$$

3. Пусть $s = n$. Тогда по лемме 1.7 верно, что каждое из чисел $l(P^\delta(f_n)), l(P^\delta(g_n))$ не меньше, чем $(3^{n+1}-1)/4$, если n – нечетное число, и не меньше, чем $(3^{n+1}-3)/4+1$, если n – четное число. Кроме того, заметим, что из леммы 1.7 следует, что если n – нечетное число, то найдутся такие векторы поляризации $\delta' = (d'_1, \dots, d'_n) \in E_3^n$, $\delta'' = (d''_1, \dots, d''_n) \in E_3^n$, $d'_i, d''_i \in \{0, 1\}$, $i = 1, \dots, n$, что $l(P^{\delta'}(f_n)) = (3^{n+1}-1)/4$ и $l(P^{\delta''}(g_n)) = (3^{n+1}-1)/4$; а если n

– четное число, то найдется такой вектор поляризации $\delta = (d_1, \dots, d_n) \in E_3^n$, $d_i \in \{0, 1\}$, $i = 1, \dots, n$, что $l(P^\delta(f_n)) = l(P^\delta(g_n)) = (3^{n+1} - 3)/4 + 1$. Отсюда получаем утверждение теоремы 1.5.

Теорема 1.5 доказана. □

Таким образом, построена последовательность симметрических функций трехзначной логики, длина которых в классе ППФ растет быстрее, чем полученная нижняя мощностная оценка соответствующей функции Шеннона. Но, в отличие от двухзначного случая, длина функций в построенной нами последовательности не достигает и полученной нами верхней оценки функции Шеннона в классе ППФ (теорема 1.3). Поэтому вопрос об асимптотике длины функций k -значной логики в классе ППФ (при $n \rightarrow \infty$) при $k \geq 3$ остается открытым.

Можно рассматривать ППФ не для отдельных функций, а систем функций k -значной логики. В этом случае можно по-разному определять сложность (длину) таких представлений систем функций. Мы рассмотрим такое определение сложности систем функций k -значной логики в классе ППФ, которое уместно с точки зрения реализации систем функций программируемыми логическими матрицами (ПЛМ) [217].

Сложностью системы ППФ, имеющих один и тот же вектор поляризации, называется число попарно различных слагаемых, встречающихся во всех этих ППФ. При простых k сложностью $L_k^{\text{ППФ}}(F)$ системы функций k -значной логики $F = \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\}$ в классе ППФ называется наименьшая сложность среди всех таких систем ППФ $\{p_1, \dots, p_m\}$, что все ППФ $p_1, \dots, p_m$ имеют один и тот же вектор поляризации, и ППФ p_j реализует функцию f_j , $j = 1, \dots, m$. Для произвольной системы функций k -значной логики $F = \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\}$ верно $L_k^{\text{ППФ}}(F) \leq k^n$.

Пусть k – простое число, и $A_k \subseteq P_k$, а $A_k^n = A_k \cap P_k^n$. Введем функцию $L_{A_k}^{\text{ППФ}}(m, n)$ (функцию Шеннона) сложности систем функций k -значной логики, принадлежащих множеству A , в классе ППФ:

$$L_{A_k}^{\text{ППФ}}(m, n) = \max_{B \subseteq A_k^n, B = \{f_1, \dots, f_m\}} L_k^{\text{ППФ}}(B).$$

Если $A_k = P_k$, то функцию Шеннона будем обозначать как $L_k^{\text{ППФ}}(m, n)$.

Найдем точные значения сложности систем функций двухзначной и трехзначной логик в классе ППФ в том случае, если системы содержат не менее двух функций.

Рассмотрим периодические функции алгебры логики $f_{(110)}^{(n)}, f_{(101)}^{(n)}, f_{(011)}^{(n)}$ с периодами длины 3. Для простоты обозначим их как f_n, g_n, h_n соответственно. Эти функции рассматривал Н.А. Перязев в [115]. В [115] доказаны следующие свойства этих функций: при $n \geq 1$ для периодических функций алгебры логики $f_n = f_{(110)}^{(n)}, g_n = f_{(101)}^{(n)}, h_n = f_{(011)}^{(n)}$ имеют место равенства

$$\begin{aligned} f_{n+1} &= \bar{x}_{n+1}f_n \oplus x_{n+1}g_n = x_{n+1}h_n \oplus f_n = \bar{x}_{n+1}h_n \oplus g_n, \\ g_{n+1} &= \bar{x}_{n+1}g_n \oplus x_{n+1}h_n = x_{n+1}f_n \oplus g_n = \bar{x}_{n+1}f_n \oplus h_n, \\ h_{n+1} &= \bar{x}_{n+1}h_n \oplus x_{n+1}f_n = x_{n+1}g_n \oplus h_n = \bar{x}_{n+1}g_n \oplus f_n. \end{aligned}$$

Кроме того, верно, что $f_1 = 1, g_1 = \bar{x}_1, h_1 = x_1$.

Теперь мы можем доказать теорему 1.6 о сложности систем функций алгебры логики в классе ППФ.

Теорема 1.6. [273] *Для всех $m \geq 2, n = 1, 2, \dots$ найдется такая система функций алгебры логики $F_{m,n} = \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\}$, что*

$$L_2^{\text{ППФ}}(F_{m,n}) = 2^n.$$

Более того, можно требовать, чтобы каждая из систем $F_{n,m}$ содержала только симметрические функции.

Доказательство. 1. Сначала рассмотрим случай $m = 2$. Докажем, что для каждой из систем $F_1 = \{f_n, g_n\}$, $F_2 = \{f_n, h_n\}$, $F_3 = \{g_n, h_n\}$, где $f_n = f_{(110)}^{(n)}$, $g_n = f_{(101)}^{(n)}$, $h_n = f_{(011)}^{(n)}$ верно, что $L_2^{\text{ППФ}}(F_j) = 2^n$, $n \geq 1$, $j = 1, 2, 3$.

Доказательство проведем индукцией по n . *Базис индукции:* $n = 1$. Тогда при поляризации $\delta = (0)$ мы получаем следующие системы ППФ $\{1, x_1 \oplus 1\}$, $\{1, x_1\}$, $\{x_1 \oplus 1, x_1\}$. При поляризации $\delta = (1)$ мы получаем такие системы ППФ $\{1, \bar{x}_1\}$, $\{1, \bar{x}_1 \oplus 1\}$, $\{\bar{x}_1, \bar{x}_1 \oplus 1\}$. Мы видим, что при каждой из возможных поляризаций сложность каждой из рассматриваемых систем равна двум. Следовательно, базис индукции обоснован.

Индуктивный переход: предположим, что для некоторого n , $n \geq 1$, утверждение теоремы 1.6 верно. Рассмотрим вектор поляризации $\delta' = (d_1, \dots, d_n, d_{n+1}) \in E_k^{n+1}$. Обозначим вектор $(d_1, \dots, d_n) \in E_k^n$ как δ .

Сначала рассмотрим систему $F_1 = \{f_{n+1}, g_{n+1}\}$. Пусть $d_{n+1} = 0$. Тогда по перечисленным выше свойствам из [115] верно, что

$$\begin{aligned} P^{\delta'}(f_{n+1}) &= x_{n+1}P^\delta(h_n) \oplus P^\delta(f_n), \\ P^{\delta'}(g_{n+1}) &= x_{n+1}P^\delta(f_n) \oplus P^\delta(g_n). \end{aligned}$$

По индуктивному предположению при векторе поляризации δ ППФ $P^\delta(f_n)$ и $P^\delta(g_n)$ содержат 2^n попарно различных слагаемых. Аналогично по индуктивному предположению при векторе поляризации δ ППФ $P^\delta(h_n)$ и $P^\delta(f_n)$ содержат 2^n попарно различных слагаемых. А значит, и ППФ $x_{n+1}P^\delta(h_n)$ и $x_{n+1}P^\delta(f_n)$ содержат 2^n попарно различных слагаемых. Следовательно, при векторе поляризации $(d_1, \dots, d_n, 0) \in E_k^{n+1}$ сложность системы F_1 равна 2^{n+1} .

Пусть теперь $d_{n+1} = 1$. Тогда по перечисленным выше свойствам из [115] верно, что

$$\begin{aligned} P^{\delta'}(f_{n+1}) &= \bar{x}_{n+1}P^\delta(h_n) \oplus P^\delta(g_n), \\ P^{\delta'}(g_{n+1}) &= \bar{x}_{n+1}P^\delta(f_n) \oplus P^\delta(h_n). \end{aligned}$$

Аналогичными рассуждениями доказываем, что при векторе поляризации

$(d_1, \dots, d_n, 1) \in E_k^{n+1}$ сложность системы F_1 равна 2^{n+1} . Следовательно, для системы F_1 индуктивный переход обоснован.

Индуктивный переход для систем F_2 и F_3 обосновывается аналогично.

2. Теперь рассмотрим общий случай $m \geq 2$. Положим, что система $F_{m,n}$ такова, что $f_{(110)}^{(n)} \in F_{m,n}$, и $f_{(101)}^{(n)} \in F_{m,n}$. Тогда по доказанному в п. 1 верно $L_2^{\text{ППФ}}(F_{m,n}) = 2^n$.

Теорема 1.6 доказана. □

Следствие 1.3. [273] *Для всех $m \geq 2$, $n = 1, 2, \dots$ верны равенства*

$$L_2^{\text{ППФ}}(m, n) = L_{S_2}^{\text{ППФ}}(m, n) = 2^n.$$

Теперь мы докажем теорему 1.7 о сложности систем функций трехзначной логики в классе ППФ.

Теорема 1.7. [273] *Для всех $m \geq 2$, $n = 1, 2, \dots$ найдется такая система функций трехзначной логики $F_{m,n} = \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\}$, что*

$$L_3^{\text{ППФ}}(F_{m,n}) = 3^n.$$

Более того, можно требовать, чтобы каждая из систем $F_{m,n}$ содержала только симметрические функции.

Доказательство. 1. Сначала рассмотрим случай $m = 2$. Докажем, что для каждой из систем функций трехзначной логики $F_1 = \{f_n, g_n\}$, $F_2 = \{h_n, t_n\}$, где $f_n = f_{(1122)}^{(n)}$, $g_n = f_{(1221)}^{(n)}$, $h_n = f_n + g_n$, $t_n = 2f_n + g_n$, верно, что $L_3^{\text{ППФ}}(F_j) = 3^n$, $n \geq 1$, $j = 1, 2$.

Доказательство проведем индукцией по n . *Базис индукции:* $n = 1$. По лемме 1.6 мы видим, что при каждой из возможных поляризациих (d) , $d \in E_3$,

сложность каждой из рассматриваемых систем равна 3. Следовательно, базис индукции обоснован.

Индуктивный переход: предположим, что для некоторого n , $n \geq 1$, утверждение теоремы 1.7 верно. Рассмотрим вектор поляризации $\delta' = (d_1, \dots, d_n, d_{n+1}) \in E_k^{n+1}$. Обозначим вектор $(d_1, \dots, d_n) \in E_k^n$ как δ .

Сначала рассмотрим систему $F_1 = \{f_{n+1}, g_{n+1}\}$. Пусть $d_{n+1} = 0$. По лемме 1.5 мы получаем, что

$$\begin{aligned} P^{\delta'}(f_{n+1}) &= a_1 x_{n+1}^2 P^\delta(g_n) + b_1 x_{n+1} P^\delta(h_n) + c_1 P^\delta(f_n), \\ P^{\delta'}(g_{n+1}) &= a_2 x_{n+1}^2 P^\delta(f_n) + b_2 x_{n+1} P^\delta(t_n) + c_2 P^\delta(g_n), \end{aligned}$$

где $a_1, b_1, c_1, a_2, b_2, c_2 \in \{1, 2\}$. По индуктивному предположению при векторе поляризации δ ППФ $P^\delta(f_n)$ и $P^\delta(g_n)$ содержат 3^n попарно различных слагаемых. Значит, и ППФ $x_{n+1}^2 P^\delta(f_n)$ и $x_{n+1}^2 P^\delta(g_n)$ содержат 3^n попарно различных слагаемых. Аналогично по индуктивному предположению при векторе поляризации δ ППФ $P^\delta(h_n)$ и $P^\delta(t_n)$ содержат 3^n попарно различных слагаемых. А значит, и ППФ $x_{n+1} P^\delta(h_n)$ и $x_{n+1} P^\delta(t_n)$ содержат 3^n попарно различных слагаемых. Следовательно, при векторе поляризации $(d_1, \dots, d_n, 0) \in E_k^{n+1}$ сложность системы F_1 равна 3^{n+1} .

Аналогичными рассуждениями доказываем, что при векторах поляризации $(d_1, \dots, d_n, d_{n+1}) \in E_k^{n+1}$ при $d_{n+1} = 1$ и $d_{n+1} = 2$ сложность системы F_1 равна 3^{n+1} . Следовательно, для системы F_1 индуктивный переход обоснован.

Индуктивный переход для системы F_2 обосновывается аналогично.

2. Теперь рассмотрим общий случай $m \geq 2$. Положим, что система $F_{m,n}$ такова, что $f_{(1122)}^{(n)} \in F_{m,n}$, и $f_{(1221)}^{(n)} \in F_{m,n}$. Тогда по доказанному в п. 1 верно $L_3^{\text{ППФ}}(F_{m,n}) = 3^n$.

Теорема 1.7 доказана. □

Следствие 1.4. [273] *Для всех $m \geq 2$, $n = 1, 2, \dots$ верны равенства*

$$L_3^{\text{ППФ}}(m, n) = L_{S_3}^{\text{ППФ}}(m, n) = 3^n.$$

Таким образом, получено точное значение сложности систем функций алгебры логики и систем функций трехзначной логики, содержащих не менее двух функций, в соответствующих классах ППФ.

Мы получили оценки длины функций k -значной логики в классе ППФ. Теперь мы обобщим понятие поляризации и рассмотрим обобщенно поляризованные полиномиальные формы.

Обозначим множество всех одноместных функций k -значной логики, степень которых в точности равна m , как D_m , $m = 1, \dots, k - 1$. Пусть $D = D_{k-1} \times \dots \times D_1$. *Обобщенным вектором поляризации* назовем вектор $\delta = (\delta_1, \dots, \delta_n)$, в котором $\delta_i = (s_{i,k-1}(x_i), \dots, s_{i,1}(x_i)) \in D$, т.е. степень функции $s_{i,m}(x_i)$ равна m .

Обобщенно поляризованным мономом по вектору δ назовем произведение вида $\prod_{j=1}^r s_{i_j, m_j}(x_{i_j})$, в котором все переменные попарно различны. *Обобщенно поляризованной полиномиальной формой* (ОППФ), или *обобщенно поляризованным полиномом* по вектору δ назовем сумму попарно различных обобщенно поляризованных по тому же вектору мономов с коэффициентами из E_k . Число попарно различных слагаемых с ненулевыми коэффициентами обобщенно поляризованного полинома P назовем его длиной $l(P)$.

Теорема 1.8. [249] *Если k – простое число, то для каждого обобщенно-го вектора поляризации δ каждую функцию k -значной логики $f(x_1, \dots, x_n)$ можно задать единственной ОППФ по этому вектору δ .*

Доказательство. Вначале докажем существование для каждой функции задающей ее ОППФ по каждому вектору поляризации.

Проведем индукцию по значению n . *Базис индукции:* $n = 1$. Пусть

$$\delta = (s_{k-1}(x), \dots, s_1(x)),$$

где $\deg(s_i) = i$, $i = k-1, \dots, 1$, – обобщенный вектор поляризации.

Пусть функция $f(x) \in P_k^1$, и ее полиномом по модулю k имеет вид:

$$P(f) = c_{k-1}x^{k-1} + \dots + c_1x + c_0,$$

где $c_{k-1}, \dots, c_1, c_0 \in E_k$.

Запишем функцию $f(x)$ ОППФ по вектору δ . Применим деление полиномов с остатком. Это можно сделать, т.к. множество E_k с операциями сложения и умножения по модулю k образуют поле [212] (стр. 27). Получаем

$$\begin{aligned} f(x) &= c'_{k-1}s_{k-1}(x) + g_{k-2}(x), \quad \deg(g_{k-2}) \leq k-2, \\ g_{k-2}(x) &= c'_{k-2}s_{k-2}(x) + g_{k-3}(x), \quad \deg(g_{k-3}) \leq k-3, \\ &\dots, \\ g_1(x) &= c'_1s_1(x) + c'_0, \quad c'_0 \in E_k. \end{aligned}$$

Тогда

$$f(x) = c'_{k-1}s_{k-1}(x) + \dots + c'_1s_1(x) + c'_0,$$

т.е. получена ОППФ по вектору δ для функции $f(x)$.

Индуктивный переход. Пусть для каждой функции k -значной логики, зависящей от n переменных, найдется ОППФ по каждому обобщенному вектору поляризации.

Рассмотрим функцию $f(y, x_1, \dots, x_n) \in P_k^{n+1}$. Представим ее полиномом $P(f)$, который запишем в виде:

$$P(f) = y^{k-1}f_{k-1}(x_1, \dots, x_n) + \dots + yf_1(x_1, \dots, x_n) + f_0(x_1, \dots, x_n).$$

Пусть $\delta = (\delta_0, \delta_1, \dots, \delta_n)$ – обобщенный вектор поляризации. Обозначим как δ' вектор $(\delta_1, \dots, \delta_n)$. Учитывая предположение индукции, запишем каж-

дую из функций

$$f_{k-1}(x_1, \dots, x_n), \dots, f_1(x_1, \dots, x_n), f_0(x_1, \dots, x_n)$$

ОППФ по вектору δ' .

Затем, аналогично базису индукции проводя деление полиномов с остатком, поляризуем переменную y по вектору δ_0 . При этом операции сложения и умножения на число с функциями от переменных $x_1, \dots, x_n$ проводим формально над ОППФ по вектору δ' . Получим ОППФ по вектору δ для функции $f(y, x_1, \dots, x_n)$.

Теперь докажем, что для каждой функции k -значной логики можно построить не более одной ОППФ по каждому обобщенному вектору поляризации.

Пусть $\delta = (\delta_1, \dots, \delta_n)$ – обобщенный вектор поляризации. Подсчитаем число ОППФ по вектору δ , зависящих от переменных $x_1, \dots, x_n$.

Обобщенно поляризованных мономов с переменными $x_1, \dots, x_n$ по вектору δ можно составить k^n (каждая переменная x_i может либо не входить в моном, либо содержаться в нем в виде $s_{i,m}(x_i)$, $m = k - 1, \dots, 1$). Из этих мономов можно построить k^{k^n} ОППФ по вектору δ . Т.е. число ОППФ по вектору δ , зависящих от переменных $x_1, \dots, x_n$, совпадает с числом функций k -значной логики, зависящих от этих же переменных.

Значит, каждая функция k -значной логики задается ОППФ по каждому обобщенному вектору поляризации однозначно.

Теорема 1.8 доказана. □

Однозначную ОППФ по обобщенному вектору поляризации δ функции $f \in P_k$ обозначим как $P^\delta(f)$. Заметим, что ОППФ функции $f(x_1, \dots, x_n) \in P_k$ по обобщенному вектору поляризации

$$\delta = ((x_1^{k-1}, \dots, x_1), \dots, (x_n^{k-1}, \dots, x_n))$$

является обычным полиномом по модулю k . ППФ функции $f(x_1, \dots, x_n) \in P_k$ по вектору поляризации $(d_1, \dots, d_n) \in E_k^n$ является частным случаем ОППФ по обобщенному вектору поляризации

$$\delta = (((x_1 + d_1)^{k-1}, \dots, x_1 + d_1), \dots, ((x_n + d_n)^{k-1}, \dots, x_n + d_n)).$$

Длиной $l^{\text{ОППФ}}(f)$ функции $f \in P_k$ в классе ОППФ назовем наименьшую длину среди всех ОППФ, задающих функцию f . Длиной (или функцией Шеннона длины) $L_k^{\text{ОППФ}}(n)$ функций k -значной логики в классе ОППФ назовем наибольшую длину в классе ОППФ среди всех функций k -значной логики, зависящих от n переменных.

Сначала докажем верхнюю оценку длины функций k -значной логики в классе ОППФ.

Теорема 1.9. [249] *Если k – простое число, то $L_k^{\text{ОППФ}}(n) \leq \frac{k}{k+1} \cdot k^n$.*

Доказательство. Рассмотрим произвольную функцию $f(x_1, \dots, x_n) \in P_k$. Докажем, что для нее всегда можно подобрать такой обобщенный вектор поляризации δ , что $l(P^\delta(f)) \leq \frac{k}{k+1} \cdot k^n$.

Доказательство проведем индукцией по числу переменных функции.

Базис индукции: $n = 1$. Рассмотрим $f(x) \in P_k^1$. Если $\deg(f) = 0$, то $l(P^\delta(f)) \leq 1$. Пусть $\deg(f) = m$, $m \geq 1$.

Тогда длина ОППФ функции $f(x)$ по обобщенному вектору поляризации

$$\delta = (x^{k-1}, \dots, x^{m+1}, f(x), x^{m-1}, \dots, x)$$

равна 1.

Индуктивный переход. Пусть

$$f(y, x_1, \dots, x_n) = y^{k-1} f_{k-1}(x_1, \dots, x_n) + \dots + y f_1(x_1, \dots, x_n) + f_0(x_1, \dots, x_n),$$

где $f_{k-1}, \dots, f_1, f_0 \in P_k$. По предположению индукции функцию f_{k-1} можно так задать ОППФ по некоторому обобщенному вектору $\delta' = (\delta_1, \dots, \delta_n)$,

что $l(P^{\delta'}(f_{k-1})) \leq \frac{k}{k+1} \cdot k^n$. Будем полагать, что все рассматриваемые дальше в доказательстве функции, зависящие от переменных $x_1, \dots, x_n$, записаны ОППФ по вектору поляризации δ' .

Найдем такой обобщенный вектор поляризации $\delta = (\delta_0, \delta_1, \dots, \delta_n)$, в котором $(\delta_1, \dots, \delta_n) = \delta'$, что длина ОППФ по нему для функции $f(y, x_1, \dots, x_n)$ не больше $\frac{k}{k+1} \cdot k^{n+1}$.

В векторе δ неизвестна компонента δ_0 . Вектор δ_0 построим последовательным уточнением. Для уточнения вектора δ_0 проведем последовательно шаги $1, 2, \dots, k-1$.

Шаг i , $1 \leq i \leq k-1$.

Пусть на предыдущем шаге $(i-1)$ был получен вектор

$$\delta_0^{(i-1)} = (s_{k-1}^{(i-1)}(y), \dots, s_{(k-1)-(i-1)}^{(i-1)}(y), y^{(k-1)-i}, \dots, y) \in D,$$

обобщенный вектор поляризации

$$\delta^{(i-1)} = (\delta_0^{(i-1)}, \delta_1, \dots, \delta_n)$$

и функция k -значной логики

$$F_{i-1}(y, x_1, \dots, x_n) = s_{k-1}^{(i-1)}(y) f_{k-1}^{(i-1)}(x_1, \dots, x_n) + \dots + s_{(k-1)-(i-1)}^{(i-1)}(y) f_{(k-1)-(i-1)}^{(i-1)}(x_1, \dots, x_n),$$

для длины L_{i-1} ОППФ по вектору $\delta^{(i-1)}$ которой верно

$$L_{i-1} = \sum_{j=0}^{i-1} l(P^{\delta'}(f_{(k-1)-j}^{(i-1)})) \leq \beta_{i-1} k^n,$$

где β_{i-1} – некоторая константа.

Если $i = 1$, то положим $\delta_0^{(0)} = (y^{k-1}, \dots, y)$, $\delta^{(0)} = (\delta_0^{(0)}, \delta_1, \dots, \delta_n)$ и $F_0(y, x_1, \dots, x_n) = y^{k-1} f_{k-1}(x_1, \dots, x_n)$. Заметим, что $L_0 = l(P^{\delta'}(f_{k-1})) \leq \frac{k}{k+1} k^n$ по предположению индукции. Поэтому определим $\beta_0 = \frac{k}{k+1}$.

Опишем шаг i , $1 \leq i \leq k-1$.

Выберем индекс a , $0 \leq a \leq i - 1$, так, что

$$l_i = l(P^{\delta'}(f_{(k-1)-a}^{(i-1)})) \geq \frac{1}{i}L_{i-1}.$$

Такой индекс a всегда возможно выбрать.

Пусть X – произвольный обобщенно поляризованный по вектору δ' моном над переменными $x_1, \dots, x_n$. Пусть c' и c'' – коэффициенты, с которыми он входит в ОППФ $P^{\delta'}(f_{(k-1)-a}^{(i-1)})$ и $P^{\delta'}(f_{(k-1)-i})$ соответственно. Тогда, если $c' \neq 0$, то

$$c' s_{(k-1)-a}^{(i-1)}(y)X + c'' y^{(k-1)-i} X = c' \left(s_{(k-1)-a}^{(i-1)}(y) + \frac{c''}{c'} y^{(k-1)-i} \right) X.$$

Пусть ОППФ $Q_j(x_1, \dots, x_n)$ составлены из всех таких слагаемых $c'X$, для которых $\frac{c''}{c'} = j$, $j \in E_k$, а ОППФ $Q_k(x_1, \dots, x_n)$ содержит все слагаемые ОППФ $P^{\delta'}(f_{(k-1)-i})$, которых нет в ОППФ $P^{\delta'}(f_{(k-1)-a}^{(i-1)})$, со своими коэффициентами.

Тогда выражение

$$s_{(k-1)-a}^{(i-1)}(y) f_{(k-1)-a}^{i-1}(x_1, \dots, x_n) + y^{(k-1)-i} f_{(k-1)-i}(x_1, \dots, x_n)$$

можно переписать в виде

$$\sum_{j \in E_k} (s_{(k-1)-a}^{(i-1)}(y) + j y^{(k-1)-i}) Q_j(x_1, \dots, x_n) + y^{(k-1)-i} Q_k(x_1, \dots, x_n).$$

Заметим, что по построению в ОППФ

$$Q_j(x_1, \dots, x_n), \quad j \in E_k, \quad \text{и} \quad Q_k(x_1, \dots, x_n)$$

нет совпадающих слагаемых с, может быть, различными коэффициентами.

Кроме того, по построению $\sum_{j \in E_k} Q_j(x_1, \dots, x_n) = P^{\delta'}(f_{(k-1)-a}^{(i-1)})$.

Выберем индекс $b \in E_k$ так, что

$$l_i^b = l(Q_b) \geq \frac{1}{k} l_i.$$

Такой индекс b всегда можно выбрать.

Вектор поляризации $\delta_0^{(i)}$ получим из вектора поляризации $\delta_0^{(i-1)}$ заменой функции

$$s_{(k-1)-a}^{(i-1)}(y)$$

на функцию

$$s_{(k-1)-a}^{(i-1)}(y) + by^{(k-1)-i}.$$

Переобозначим компоненты вектора $\delta_0^{(i)}$. Пусть

$$\delta_0^{(i)} = (s_{k-1}^{(i)}(y), \dots, s_{(k-1)-i}^{(i)}(y), y^{(k-1)-(i+1)}, \dots, y).$$

Пусть $\delta^{(i)} = (\delta_0^{(i)}, \delta_1, \dots, \delta_n)$ и

$$F_i(y, x_1, \dots, x_n) = F_{i-1}(y, x_1, \dots, x_n) + y^{(k-1)-i} f_{(k-1)-i}(x_1, \dots, x_n).$$

Запишем функцию $F_i(y, x_1, \dots, x_n)$ ОППФ по вектору поляризации $\delta^{(i)}$.

По рассмотренному выше получаем

$$\begin{aligned} F_i(y, x_1, \dots, x_n) &= F_{i-1}(y, x_1, \dots, x_n) + y^{(k-1)-i} f_{(k-1)-i}(x_1, \dots, x_n) = \\ &= \sum_{j \in \{0, \dots, i-1\}} s_{(k-1)-j}^{(i-1)}(y) f_{(k-1)-j}^{(i-1)}(x_1, \dots, x_n) + y^{(k-1)-i} f_{(k-1)-i}(x_1, \dots, x_n) = \\ &= \sum_{j \in \{0, \dots, i-1\} \setminus \{a\}} s_{(k-1)-j}^{(i-1)}(y) f_{(k-1)-j}^{(i-1)}(x_1, \dots, x_n) + \\ &+ \left(s_{(k-1)-a}^{(i-1)}(y) f_{(k-1)-a}^{(i-1)}(x_1, \dots, x_n) + y^{(k-1)-i} f_{(k-1)-i}(x_1, \dots, x_n) \right) = \\ &= \sum_{j \in \{0, \dots, i-1\} \setminus \{a\}} s_{(k-1)-j}^{(i-1)}(y) f_{(k-1)-j}^{(i-1)}(x_1, \dots, x_n) + \\ &+ (s_{(k-1)-a}^{(i-1)}(y) + by^{(k-1)-i}) f_{(k-1)-a}^{(i-1)}(x_1, \dots, x_n) + \\ &+ y^{(k-1)-i} (f_{(k-1)-i}(x_1, \dots, x_n) - b f_{(k-1)-a}^{(i-1)}(x_1, \dots, x_n)). \end{aligned}$$

Отсюда

$$f_{(k-1)-j}^{(i)}(x_1, \dots, x_n) = f_{(k-1)-j}^{(i-1)}(x_1, \dots, x_n), \quad j = 0, 1, \dots, i-1;$$

$$f_{(k-1)-i}^{(i)}(x_1, \dots, x_n) = f_{(k-1)-i}(x_1, \dots, x_n) - b f_{(k-1)-a}^{(i-1)}(x_1, \dots, x_n).$$

Для того, чтобы найти длину ОППФ $P^{\delta^{(i)}}(F_i)$, перепишем функцию F_i в виде

$$\begin{aligned} F_i(y, x_1, \dots, x_n) &= \sum_{j \in \{0, \dots, i-1\} \setminus \{a\}} s_{(k-1)-j}^{(i)}(y) f_{(k-1)-j}^{(i-1)}(x_1, \dots, x_n) + \\ &\quad + s_{(k-1)-a}^{(i)}(y) f_{(k-1)-a}^{(i-1)}(x_1, \dots, x_n) + \\ &\quad + s_{(k-1)-i}^{(i)}(y) (f_{(k-1)-i}(x_1, \dots, x_n) - b f_{(k-1)-a}^{(i-1)}(x_1, \dots, x_n)) = \\ &= \sum_{j \in \{0, \dots, i-1\} \setminus \{a\}} s_{(k-1)-j}^{(i)}(y) f_{(k-1)-j}^{(i-1)}(x_1, \dots, x_n) + \\ &\quad + s_{(k-1)-a}^{(i)}(y) \left(\sum_{j \in E_k} Q_j \right) + \\ &\quad + s_{(k-1)-i}^{(i)}(y) \left(Q_k + \sum_{j \in E_k \setminus \{b\}} (j-b) Q_j \right). \end{aligned}$$

ОППФ по вектору поляризации δ'

$$Q_b, (j-b)Q_j \text{ при } j \in E_k \setminus \{b\} \text{ и } Q_k \quad (3)$$

не имеют общих слагаемых.

По построению верны следующие оценки:

$$\begin{aligned} \sum_{j \in \{0, \dots, i-1\} \setminus \{a\}} l(P^{\delta'}(f_{(k-1)-j}^{(i-1)})) &\leq L_{i-1} - l_i, \\ \sum_{j \in E_k} l(Q_j) &\leq k^n, \\ \sum_{j \in E_k \setminus \{b\}} l(Q_j) &\leq \frac{k-1}{k} l_i, \end{aligned}$$

Тогда

$$l(P^{\delta^{(i)}}(F_i)) \leq (\beta_{i-1} k^n - l_i) + k^n + \frac{k-1}{k} l_i \leq \beta_{i-1} k^n + k^n - \frac{1}{k} l_i \leq$$

$$\leq \beta_{i-1}k^n + k^n - \frac{1}{ki}\beta_{i-1}k^n \leq \left(1 + \left(1 - \frac{1}{ki}\right)\beta_{i-1}\right)k^n.$$

Положим $\beta_i = 1 + \left(1 - \frac{1}{ki}\right)\beta_{i-1}$.

Заметим, что

$$F_{k-1}(y, x_1, \dots, x_n) = f(y, x_1, \dots, x_n).$$

Положим $\delta_0 = \delta_0^{(k-1)}$ и $\delta = (\delta_0, \delta_1, \dots, \delta_n)$.

Тогда ОППФ по вектору δ для функции $f(y, x_1, \dots, x_n)$ имеет длину, не большую $\beta_{k-1}k^n$, которую можно подсчитать по следующим равенствам при $\beta_0 = \frac{k}{k+1}$:

$$\beta_1 = 1 + \left(1 - \frac{1}{k}\right)\beta_0,$$

$$\beta_2 = 1 + \left(1 - \frac{1}{2k}\right)\beta_1,$$

$\dots,$

$$\beta_{k-1} = 1 + \left(1 - \frac{1}{(k-1)k}\right)\beta_{k-2}.$$

В результате непосредственного подсчета получаем $\beta_{k-1} = \frac{k^2}{k+1}$, или что $l(P^\delta(f)) \leq \frac{k}{k+1}k^{n+1}$. Индуктивный переход обоснован.

Теорема 1.9 доказана. □

Теперь докажем нижнюю оценку длины функций k -значной логики в классе ОППФ.

Теорема 1.10. [249] *Если k – простое число, то $L_k^{\text{ОППФ}}(n) \geq \frac{k-1}{k} \cdot (1 - \varepsilon(n)) \cdot k^n$ для некоторой такой функции $\varepsilon(n)$, что $\varepsilon(n) \rightarrow 0$ при $n \rightarrow \infty$.*

Доказательство. Пусть $L, L \leq \frac{k-1}{k} \cdot k^n$, – некоторое натуральное число. Найдем число ОППФ длины не большей L , задающих функции, зависящих от переменных $x_1, \dots, x_n$.

Всего мономов над переменными $x_1, \dots, x_n$ есть k^n , полиномов длины, не большей L , из них можно составить $\sum_{i=0}^L C_{k^n}^i (k-1)^i$. Каждую переменную мож-

но обобщенно поляризовать не более, чем $(k^k)^{(k-1)}$ способами (не более k^k вариантов обобщенной поляризации для каждой степени переменной и $(k-1)$ степеней переменной).

Следовательно, всего ОППФ, зависящих от переменных $x_1, \dots, x_n$, длины, не большей L , не более

$$\sum_{i=0}^L C_{k^n}^i (k-1)^i (k^k)^{(k-1)n} \quad (13)$$

Для оценки полученного выражения воспользуемся оценкой биномиального коэффициента и свойствами функции k -значной энтропии $H_k(x)$. Оценим выражение (13)

$$\begin{aligned} \sum_{i=0}^L C_{k^n}^i (k-1)^i (k^k)^{(k-1)n} &\leq LC_{k^n}^L (k-1)^L k^{k(k-1)n} \leq \\ &\leq L \frac{(k^n)^{k^n}}{L^L (k^n - L)^{k^n - L}} (k-1)^L k^{k(k-1)n} \leq L k^{H_k(\frac{L}{k^n})k^n} k^{k(k-1)n} \end{aligned} \quad (14)$$

Пусть $\varepsilon > 0$ – действительное число и $L \leq (\frac{k-1}{k} - \varepsilon)k^n$. Тогда по свойствам функции k -значной энтропии найдется такое действительное число ε_1 , $\varepsilon_1 > 0$, что

$$H_k\left(\frac{L}{k^n}\right) \leq H_k\left(\frac{k-1}{k} - \varepsilon\right) \leq 1 - \varepsilon_1.$$

Отсюда для выражения (14) находим

$$L k^{H_k(\frac{L}{k^n})k^n} k^{k(k-1)n} \leq \left(\frac{k-1}{k} - \varepsilon\right) k^n k^{(1-\varepsilon_1)k^n} k^{k(k-1)n}.$$

Полученное выражение при $n \rightarrow \infty$ растет медленнее, чем k^{k^n} . Другими словами, для каждого действительного числа $\varepsilon > 0$ при $L \leq (\frac{k-1}{k} - \varepsilon)k^n$ ОППФ длины, не большей L , не хватит, чтобы задать все функции k -значной логики, зависящие от переменных $x_1, \dots, x_n$. Отсюда получаем утверждение теоремы 1.10.

Теорема 1.10 доказана. □

В [21] предложено обобщение ОППФ и получена верхняя оценка длины функций k -значной логики в этом классе полиномиальных форм при $k \geq 3$.

Теперь мы отказываемся от каноничности полиномиальных форм, т.е. от требования, чтобы каждая функция задавалась однозначной полиномиальной формой по заданному вектору поляризации.

Полиномиальные нормальные формы (ПНФ) для функций алгебры логики – это сумма по модулю два элементарных конъюнкций. Это представление функций алгебры логики аналогично дизъюнктивным нормальным формам (ДНФ), только вместо операции дизъюнкции применяется операция сложения по модулю два. Экспериментальные результаты показывают, что представление функций от небольшого числа переменных (не более четырех) в виде ПНФ имеет в среднем меньшую длину (меньшее число слагаемых), чем представление этих же функций в виде ДНФ [192, 220]. Для исследования сложности представления функций алгебры логики вводится функция Шеннона $L_2^{\text{ПНФ}}(n)$ длины функций алгебры логики в классе ПНФ как длина самой длинной функции, зависящей от n переменных. К.Д. Кириченко [76] была получена верхняя оценка функции Шеннона $L_2^{\text{ПНФ}}(n) \leq 2 \cdot \frac{2^n}{n}(\log_2 n + 1)$. Эта оценка показывает, что представление функций алгебры логики в виде ПНФ имеет меньшую длину, чем их представление в виде ДНФ, и для самых длинных функций при росте числа переменных функций.

Полиномиальные нормальные формы по модулю k для функций k -значной логики обобщают понятие ПНФ для функций алгебры логики. Определим полиномиальные нормальные формы по модулю k . Под *поляризованной переменной* x_i будем понимать, как и раньше, выражение вида $(x_i + d)$, где $d \in E_k$. Произведение попарно различных поляризованных переменных назовем *мономом с поляризованными переменными*. Обычный моном является частным случаем монома с поляризованными переменными.

Сумму по модулю k мономов с поляризованными переменными с некоторыми коэффициентами из E_k назовем *полиномиальной нормальной формой по модулю k* (ПНФ). Длиной ПНФ называется число ее попарно различных слагаемых с ненулевыми коэффициентами. Мы будем полагать константу 0 ПНФ с длиной, равной 0.

Каждую функцию k -значной логики (при простых k) можно представить различными ПНФ по модулю k . Назовем длиной функции f в классе ПНФ величину $l^{\text{ПНФ}}(f)$, равную наименьшей длине среди всех ПНФ, представляющих функцию f . Длиной (функцией Шеннона длины) $L_k^{\text{ПНФ}}(n)$ функций k -значной логики в классе ПНФ называется наибольшая длина в классе для функций k -значной логики, зависящих от n переменных.

В [160] найдена нижняя мощностная оценка длины функций алгебры логики в классе ПНФ. К.Д. Кириченко [76] получена верхняя оценка $L_2^{\text{ПНФ}}(n) \leq 2 \cdot \frac{2^n}{n} (\log_2 n + 1)$. Эта оценка была получена методом построения ПНФ на основе затеняющего множества куба E_2^n . Мощность затеняющего множества на E_2^n была оценена при помощи разбиения куба E_2^n на сферы. Но с учетом результата из [155] можно получить более точную оценку мощности затеняющего множества на E_2^n и, как следствие, оценку $L_2^{\text{ПНФ}}(n) = \Theta\left(\frac{2^n}{n}\right)$.

Мы обобщаем метод из [76] на случай функций k -значной логики и получаем оценки длины функций k -значной логики в классе ПНФ. Мы доказываем теорему 1.11, в которой оцениваем длину ПНФ для произвольной функции k -значной логики через мощность затеняющего множества куба E_k^n , и теорему 1.12, в которой оцениваем длину ПНФ для произвольной функции k -значной логики через мощность покрытия полушарами куба E_k^n . Отметим также, что в теоремах 1.11 и 1.12 описаны методы построения для функции k -значной логики $f(x_1, \dots, x_n)$ ПНФ с соответствующими сложностями, и этими методами строятся разные ПНФ для функции f .

Теорема 1.11. [245] Пусть k – простое число. Если $T, T \subseteq E_k^n$, – затемняющее множество куба E_k^n , то для каждой функции k -значной логики $f(x_1, \dots, x_n)$ можно построить такую ПНФ, представляющую функцию f , что длина этой ПНФ не превосходит $(|T| + 1)$.

Доказательство. Пусть $T = \{\alpha_1, \dots, \alpha_{|T|}\}$ – затемняющее множество на E_k^n , причем для всех $i, j = 1, 2, \dots, |T|$ верно, что $|\alpha_i| \geq |\alpha_j|$ при $i < j$.

Положим $f_0(x_1, \dots, x_n) = f(x_1, \dots, x_n) - \sum_{j=1}^{|T|} X_{\alpha_j}$ и $Q_0 = P(f_0)$.

Для всех $j, j = 1, \dots, l$, повторим следующие рассуждения.

1) Рассматриваем набор $\alpha_j = (a_1, \dots, a_n) \in E_k^n$ и соответствующий ему моном X_{α_j} . Пусть для каждого $\beta \in \check{S}(\alpha_j)$ моном (без поляризованных переменных) X_β входит в ПНФ Q_{j-1} с коэффициентом c_β .

2) Для каждого набора $\beta \in \check{S}(\alpha_j)$ рассмотрим набор $\alpha_j - \beta \in E_k^n$. Этот набор имеет вид

$$\alpha_j - \beta = (0, \dots, 0, 1, 0, \dots, 0).$$

Пусть $i_\beta, 1 \leq i_\beta \leq n$, номер единственной координаты в наборе $\alpha_j - \beta$, в которой находится единица. Положим $Y_{\alpha_j} = \prod_{\beta \in \check{S}(\alpha_j)} (X_{\alpha_j - \beta} + \frac{c_\beta}{a_{i_\beta}})^{a_{i_\beta}}$.

Пусть $f_j(x_1, \dots, x_n) = Q_{j-1} + X_{\alpha_j} + Y_{\alpha_j} - P(Y_{\alpha_j})$, и Q_j есть ПНФ, полученная приведением подобных слагаемых в этом выражении для функции $f_j(x_1, \dots, x_n)$.

Обратим внимание, что выражения Y_{α_j} и $P(Y_{\alpha_j})$ равны как функции k -значной логики, поэтому

$$f_j(x_1, \dots, x_n) = f(x_1, \dots, x_n) - \sum_{i=j+1}^{|T|} X_{\alpha_i}.$$

3) Заметим, что полином $P(Y_{\alpha_j})$ содержит слагаемое X_{α_j} с коэффициентом 1 и все слагаемые $X_\beta, \beta \in \check{S}(\alpha_j)$, с коэффициентами c_β . По построению все

они сокращаются в ПНФ Q_j . Все другие слагаемые полинома $P(Y_{\alpha_j})$ имеют степени не больше $(|\alpha_j| - 2)$. Поэтому в ПНФ Q_j не могут входить мономы без поляризованных переменных, соответствующие наборам из $\check{S}(\alpha_j)$.

Рассмотрев все наборы из затеняющего множества T , получим ПНФ

$$Q_{|T|} = c \cdot x_1^{k-1} \cdot \dots \cdot x_n^{k-1} + \sum_{j=1}^{|T|} Y_{\alpha_j},$$

где $c \in E_k$. Она задает функцию $f(x_1, \dots, x_n)$ (см. п. 2 рассуждений), и ее длина не больше $(|T| + 1)$.

Теорема 1.11 доказана. □

Для того, чтобы найти оценку длины функций k -значной логики в классе ПНФ по теореме 1.11, требуется оценить мощность затеняющего множества куба E_k^n . В [245] градиентным алгоритмом (см. [216], стр. 53) была получена оценка: для каждого k , $k \geq 1$, можно построить такое затеняющее множество T куба E_k^n , что $|T| \leq (2 + \varepsilon(n)) \cdot \frac{k^n}{n} \cdot \ln n$ для некоторой функции $\varepsilon(n)$, такой, что $\varepsilon(n) \rightarrow 0$ при $n \rightarrow \infty$. Отсюда получается верхняя оценка длины функций k -значной логики в классе ПНФ (при простых k).

Теорема 1.12. [268] *Пусть k – простое число. Если T , $T \subseteq E_k^n$, – покрытие полушарами куба E_k^n , то для каждой функции k -значной логики $f(x_1, \dots, x_n)$ можно построить такую ПНФ, представляющую функцию f , что длина этой ПНФ не превосходит $2 \cdot |T|$.*

Доказательство. Пусть $T = \{\alpha_1, \dots, \alpha_{|T|}\}$ – покрытие полушарами куба E_k^n , причем для всех $i, j = 1, 2, \dots, |T|$ верно, что $|\alpha_i| \geq |\alpha_j|$ при $i < j$.

Мы опишем алгоритм, в котором последовательно выполним шаги $1, 2, \dots, |T|$. После шага j мы будем получать некоторый полином P_j и некоторую ПНФ Q_j , такие что $f(x_1, \dots, x_n) = Q_j + P_j$. Кроме того, для каждого слага-

евого X_β , $\beta \in E_k^n$, с ненулевым коэффициентом в полиноме P_j будет верно, что $\beta \notin \bigcup_{i=1}^j (\{\alpha_i\} \cup \check{S}(\alpha_i))$.

Перед началом работы алгоритма положим, что $Q_0 = 0$, $P_0 = P(f)$.

Шаг j .

1) Пусть $\alpha_j = (a_1, \dots, a_n) \in E_k^n$. Для каждого $\beta \in \{\alpha_j\} \cup \check{S}(\alpha_j)$ пусть моном X_β входит в полином P_{j-1} с коэффициентом c_β . Для каждого набора $\beta \in \check{S}(\alpha_j)$ рассмотрим набор $\alpha_j - \beta \in E_k^n$. Этот набор имеет вид

$$\alpha_j - \beta = (0, \dots, 0, 1, 0, \dots, 0).$$

Пусть i_β , $1 \leq i_\beta \leq n$, номер единственной координаты в наборе $\alpha_j - \beta$, в которой находится единица. Положим $\check{X}_{\alpha_j} = \prod_{\beta \in \check{S}(\alpha)} (X_{\alpha_j - \beta} + \frac{c_\beta}{a_{i_\beta}})^{a_{i_\beta}}$. Заметим, что $\check{X}_{\alpha_j}$ – это моном с поляризованными переменными.

2) Пусть P_j есть полином, полученный в результате приведения подобных слагаемых в полиномиальном выражении $P_{j-1} + (1 - c_{\alpha_j})X_{\alpha_j} - P(\check{X}_{\alpha_j})$. Положим, что Q_j – это ПНФ $Q_{j-1} + \check{X}_{\alpha_j} + (c_{\alpha_j} - 1)X_{\alpha_j}$.

Заметим, что полином $P(\check{X}_{\alpha_j})$ содержит слагаемое X_{α_j} с коэффициентом 1 и все слагаемые X_β , где $\beta \in \check{S}(\alpha_j)$, с коэффициентами c_β . По построению все они сокращаются в полиноме P_j . Все другие слагаемые полинома $P(\check{X}_{\alpha_j})$ имеют степени, не большие $(|\alpha_j| - 2)$. Поэтому в полиноме P_j не могут входить мономы, соответствующие наборам из $\check{S}(\alpha_j)$. Для полинома P_{j-1} верно, что если X_β , $\beta \in E_k^n$, является слагаемым с ненулевым коэффициентом в этом полиноме, то $\beta \notin \bigcup_{i=1}^{j-1} (\{\alpha_i\} \cup \check{S}(\alpha_i))$. Т.к. $|\alpha_i| \geq |\alpha_j|$ для всех $i = 1, \dots, j-1$, получаем, что если X_β , $\beta \in E_k^n$, является слагаемым с ненулевым коэффициентом в полиноме P_j , то $\beta \notin \bigcup_{i=1}^j (\{\alpha_i\} \cup \check{S}(\alpha_i))$.

Кроме того, верно

$$\begin{aligned} f(x_1, \dots, x_n) &= P_{j-1} + Q_{j-1} = P_{j-1} + Q_{j-1} + \\ &\quad + ((1 - c_{\alpha_j})X_{\alpha_j} - P(\check{X}_{\alpha_j})) + (\check{X}_{\alpha_j} + (c_{\alpha_j} - 1)X_{\alpha_j}) = \\ &= P_j + Q_j. \end{aligned}$$

3) Теперь если $j < |T|$, то переходим к шагу $(j + 1)$; если $j = |T|$, то алгоритм завершает работу.

Для полинома $P_{|T|}$ верно, что если моном X_β , $\beta \in E_k^n$, является слагаемым с ненулевым коэффициентом в этом полиноме, то $\beta \notin \bigcup_{i=1}^{|T|} (\{\alpha_i\} \cup \check{S}(\alpha_i))$. Но множество T является покрытием полушарами куба E_k^n . Значит, полином $P_{|T|}$ не содержит слагаемых с ненулевыми коэффициентами, т.е. $P_{|T|} = 0$. Поэтому

$$f(x_1, \dots, x_n) = P_{|T|} + Q_{|T|} = Q_{|T|} = \sum_{j=1}^{|T|} (c_j X_{\alpha_j} + d_j \check{X}_{\alpha_j}),$$

где $c_1, \dots, c_{|T|}, d_1, \dots, d_{|T|} \in E_k$ – некоторые коэффициенты.

Т.е. мы нашли ПНФ, представляющую функцию $f(x_1, \dots, x_n)$, и длина этой ПНФ не превосходит $2 \cdot |T|$.

Теорема 1.12 доказана. □

Для того, чтобы найти оценку длины функций k -значной логики в классе ПНФ по теореме 1.12, требуется оценить мощность покрытия полушарами куба E_k^n . В [268] вероятностным методом была получена оценка: при каждом натуральном $k \geq 2$ и при каждом натуральном $n \geq 1$ существует множество мощности $c \cdot \frac{k^n}{n}$, покрывающее полушарами куб E_k^n , где $c > 0$ – некоторая действительная константа, зависящая только от k . Отсюда получается более точная верхняя оценка длины функций k -значной логики в классе ПНФ (при простых k).

Докажем нижнюю оценку длины функций k -значной логики в классе ПНФ.

Теорема 1.13. [245] Если k – простое число, то $L_k^{\text{ПНФ}}(n) \geq (1 - \varepsilon(n)) \cdot \frac{k^n}{n \cdot \log_k(k(k-1)+1)}$ для некоторой такой функции $\varepsilon(n)$, что $\varepsilon(n) \rightarrow 0$ при $n \rightarrow \infty$.

Доказательство. Пусть L , $L \leq \frac{k-1}{k} \cdot k^n$, – некоторое натуральное число. Подсчитаем число ПНФ длины не большей L , задающих функции k -значной логики, зависящие от переменных $x_1, \dots, x_n$.

Различных мономов с поляризованными переменными $x_1, \dots, x_n$ можно построить $(k(k-1)+1)^n$, т.к. каждая переменная может находиться в одной из степеней $0, 1, \dots, k-1$ и, если ее степень не 0, может быть поляризована смещением на одну из констант $0, 1, \dots, k-1$. Следовательно, ПНФ длины, не большей L , из них можно составить $(k(k(k-1)+1)^n)^L$.

Если $(k(k(k-1)+1)^n)^L < k^{k^n}$, то ПНФ длины L не хватает для представления всех k^{k^n} функций k -значной логики, зависящих от переменных $x_1, \dots, x_n$. Отсюда получаем утверждение теоремы 1.13.

Теорема 1.13 доказана. □

Собирая верхнюю и нижнюю оценки, получаем

Следствие 1.5. [268] Если k – простое число, то $L_k^{\text{ПНФ}}(n) = \Theta\left(\frac{k^n}{n}\right)$.

В заключение раздела мы рассмотрим полиномиальную форму для функций алгебры логики, которую называем *полиномиальной формой с аффинными множителями в слагаемых*, или *псевдополиномиальной формой*.

В [163] рассматривались псевдополиномиальные формы для функций алгебры логики и их применение при проектировании интегральных схем. Псевдополиномиальная форма (ПСПФ) – это сумма по модулю произведений аффинных (линейных) функций алгебры логики. Т.е. ПСПФ – это выражение вида

$$\bigoplus_{i=1}^l \prod_{j=1}^{r_i} g_{i_j},$$

где $g_{i_1}, \dots, g_{i_{r_i}}$ – некоторые аффинные функции, $r_i \geq 1, i = 1, \dots, l$. Несложно заметить, что каждая функция алгебры логики задается какой-то ПСПФ, например, своим полиномом Жегалкина.

Длиной $l(P)$ ПСПФ P называется число попарно различных ее слагаемых с ненулевыми коэффициентами. Длиной $l^{\text{ПСПФ}}(f)$ функции алгебры логики f в классе ПСПФ назовем наименьшую длину среди всех ПСПФ, каждая из которых представляет функцию f . Длиной (функцией Шеннона длины) $L_2^{\text{ПСПФ}}(n)$ функций алгебры логики в классе ПСПФ называется наибольшая длина в классе ПСПФ среди всех функций алгебры логики, зависящих от n переменных.

Сначала найдем нижнюю оценку длины функций алгебры логики в классе ПСПФ. Напомним, что функция алгебры логики $f(x_1, \dots, x_n)$ называется *мультиаффинной*, если она представима в виде произведения аффинных функций.

Лемма 1.8. [267] *Число мультиаффинных функций, зависящих от переменных $x_1, \dots, x_n$, не превосходит величины $2^{\frac{n(n+3)}{2}}$*

Доказательство. Пусть $f(x_1, \dots, x_n)$ – мультиаффинная функция, и

$$f(x_1, \dots, x_n) = \prod_{i=1}^l g_i(x_1, \dots, x_n)$$

– ее представление в виде произведения аффинных функций $g_1, \dots, g_l, l \geq 1$.

Рассмотрим систему линейных уравнений

$$\begin{cases} g_1(x_1, \dots, x_n) = 1, \\ \dots \\ g_l(x_1, \dots, x_n) = 1. \end{cases}$$

Множество решений этой системы задает множество наборов куба E_2^n , на которых функция $f(x_1, \dots, x_n)$ принимает значение 1. Из линейной алгеб-

ры [210] известно, что такая система может быть преобразована к системе линейных уравнений с тем же множеством решений, которая имеет следующий вид:

$$\left\{ \begin{array}{l} h_1(x_1, x_2, \dots, x_{n-1}, x_n) = 0, \\ h_2(x_2, \dots, x_{n-1}, x_n) = 0, \\ \dots \\ h_{n-1}(x_{n-1}, x_n) = 0, \\ h_n(x_n) = 0, \end{array} \right.$$

где $h_1(x_1, \dots, x_n)$, $h_2(x_2, \dots, x_n)$, $\dots$, $h_{n-1}(x_{n-1}, x_n)$, $h_n(x_n)$ – некоторые аффинные функции.

Следовательно, каждая мультиаффинная функция, зависящая от переменных $x_1, \dots, x_n$, задается системой линейных уравнений указанного вида. А таких систем не больше, чем

$$2^{n+1} \cdot 2^n \cdot \dots \cdot 2^3 \cdot 2^2 = 2^{\frac{n(n+3)}{2}}.$$

Лемма 1.8 доказана. □

Теорема 1.14. [267] *Справедливо неравенство $L_2^{\text{ПСПФ}}(n) \geq (1 - \varepsilon(n)) \frac{2^{n+1}}{n^2}$ для некоторой такой функции $\varepsilon(n)$, что $\varepsilon(n) \rightarrow 0$ при $n \rightarrow \infty$.*

Доказательство. Для доказательства этой оценки применим мощностной метод. Подсчитаем число $\nu(n, L)$ ПСПФ, зависящих от переменных $x_1, \dots, x_n$ и имеющих длину, не превосходящую L . Каждое слагаемое такой формы – это некоторая мультиаффинная функция, зависящая от переменных $x_1, \dots, x_n$, число слагаемых не превосходит L . Поэтому

$$\nu(n, L) \leq \left(2^{\frac{n(n+3)}{2}} \right)^L \leq 2^{\frac{n^2 L + 3nL}{2}}.$$

Для $L = L_2^{\text{ПСПФ}}(n)$ должно выполняться неравенство: $\nu(n, L_2^{\text{ПСПФ}}(n)) \geq 2^{2n}$. Отсюда получаем утверждение теоремы 1.14.

Теорема 1.14 доказана. □

Теперь мы докажем верхнюю оценку длины функций алгебры логики в классе ПСПФ. Отметим, что мы применяем метод, который, в некотором смысле, развивает и усложняет метод для ПНФ из [76].

Метод состоит в применении к группам слагаемых полинома Жегалкина функции алгебры логики правил Π_1 и Π_2 и последовательного построения ПСПФ этой функции. Правило Π_1 имеет вид

$$\Pi_1 : \bigoplus_{\beta \in \{\alpha\} \cup \hat{S}(\alpha)} c_\beta X_\beta = X_\alpha \cdot \left(\bigoplus_{\beta \in \{\alpha\} \cup \hat{S}(\alpha)} c_\beta X_{\beta \oplus \alpha} \right),$$

где $\alpha \in E_2^n$, $c_\beta \in B$ – произвольные коэффициенты. Равенство Π_1 является тождеством. Рассмотрим выражение

$$\Pi_2 : X_\alpha \oplus \bigoplus_{\beta \in \check{S}(\alpha)} c_\beta X_\beta = \left(\prod_{\beta \in \check{S}(\alpha)} (X_{\alpha \oplus \beta} \oplus c_\beta) \right) \oplus \bigoplus_{\gamma \in E_2^n : |\gamma| \leq |\alpha| - 2} c_\gamma X_\gamma,$$

где $\alpha \in E_2^n$, $c_\beta, c_\gamma \in B$. Для произвольного набора $\alpha \in E_2^n$ и произвольных коэффициентов c_β , где $\beta \in \check{S}(\alpha)$, найдутся такие однозначные коэффициенты $c_\gamma \in B$, где $\gamma \in E_2^n$, $|\gamma| \leq |\alpha| - 2$, что равенство Π_2 является тождеством. Под правилом Π_2 будем понимать именно такое равенство Π_2 , являющееся тождеством.

Теорема 1.15. [267] *Если $T, T \subseteq E_2^n$, – покрытие шарами радиуса 1 куба E_2^n , то для каждой функции алгебры логики $f(x_1, \dots, x_n)$ можно построить такую ПСПФ, представляющую функцию f , что длина этой ПСПФ не превосходит $2 \cdot |T|$.*

Доказательство. Пусть $T = \{\alpha_1, \dots, \alpha_{|T|}\}$ – покрытие шарами радиуса 1 куба E_2^n , причем при всех $i < j$, $i, j = 1, \dots, |T|$, верно, что $|\alpha_i| \geq |\alpha_j|$.

Пусть нам задана функция алгебры логики $f(x_1, \dots, x_n)$.

Выполним последовательно шаги $1, 2, \dots, |T|$. После шага j получим такие ПСПФ Q_j и полином Жегалкина P_j , что $f(x_1, \dots, x_n) = Q_j \oplus P_j$. Кроме того, для каждого j окажется верным, что если моном X_β , $\beta \in E_2^n$, является слагаемым полинома P_j , то $\beta \notin \bigcup_{i=1}^j S_1(\alpha_i)$. Перед началом работы алгоритма положим, что $Q_0 = 0$, а P_0 – это полином Жегалкина функции $f(x_1, \dots, x_n)$.

Шаг j , $j = 1, 2, \dots, |T|$. Пусть $f(x_1, \dots, x_n) = Q_{j-1} \oplus P_{j-1}$, где Q_{j-1} – ПСПФ, а P_{j-1} – полином Жегалкина, для каждого слагаемого X_β которого верно, что $\beta \notin \bigcup_{i=1}^{j-1} S_1(\alpha_i)$.

Выделим в полиноме Жегалкина P_{j-1} группу слагаемых вида X_β , где $\beta \in S_1(\alpha_j)$. Пусть каждое из этих слагаемых встречается в полиноме Жегалкина P_{j-1} с коэффициентом $c_\beta \in B$. Положим, что $P_j(\alpha_j)$ – это полином Жегалкина $\bigoplus_{\beta \in S_1(\alpha_j)} c_\beta X_\beta$.

Возможны две ситуации: $c_{\alpha_j} = 1$ или $c_{\alpha_j} = 0$. В первом случае положим, что $\hat{P}_j(\alpha_j)$ – это полином Жегалкина $\bigoplus_{\beta \in \hat{S}(\alpha_j)} c_\beta X_\beta$, а $\check{P}_j(\alpha_j)$ – это полином

Жегалкина $\hat{P}_j(\alpha_j) \oplus P_j(\alpha_j)$. Во втором случае положим, что $\hat{P}_j(\alpha_j)$ – это полином Жегалкина $X_{\alpha_j} \oplus \bigoplus_{\beta \in \hat{S}(\alpha_j)} c_\beta X_\beta$, а $\check{P}_j(\alpha_j)$ – это полином Жегалкина

$\hat{P}_j(\alpha_j) \oplus P_j(\alpha_j)$. В обоих случаях $\hat{P}_j(\alpha_j) \oplus \check{P}_j(\alpha_j) = P_j(\alpha_j)$.

Применим к полиному Жегалкина $\hat{P}_j(\alpha_j)$ правило Π_1 , получим произведение аффинных множителей, которое обозначим как $\hat{Y}_j$. Применим к полиному Жегалкина $\check{P}_j(\alpha_j)$ правило Π_2 , получим сумму по модулю два двух слагаемых. Первое слагаемое – это произведение аффинных множителей, которое обозначим как $\check{Y}_j$. Второе слагаемое – это некоторая функция, ее полином Жегалкина обозначим как P'_j . Каждое слагаемое полинома Жегалкина P'_j имеет ранг, не больший $|\alpha_j| - 2$.

Правила Π_1 и Π_2 являются тождествами, поэтому $\hat{P}_j(\alpha_j) = \hat{Y}_j$ и $\check{P}_j(\alpha_j) =$

$\check{Y}_j \oplus P'_j$.

Обозначим ПСПФ $Q_{j-1} \oplus \check{Y}_j \oplus \hat{Y}_j$ как Q_j , а полином Жегалкина функции $P_{j-1} \oplus P_j(\alpha_j) \oplus P'_j$ как P_j . Напомним, что для каждого слагаемого X_β полинома Жегалкина P_{j-1} было верно, что $\beta \notin \bigcup_{i=1}^{j-1} S_1(\alpha_i)$. Полином Жегалкина P_j получается из полинома Жегалкина P_{j-1} удалением всех слагаемых X_β , для которых $\beta \in S_1(\alpha_j)$, а также, возможно, добавлением некоторых слагаемых X_β , для которых $|\beta| \leq |\alpha_j| - 2$. Кроме того, $|\alpha_j| \leq |\alpha_i|$ для всех $i = 1, 2, \dots, j-1$. Поэтому для каждого слагаемого X_β полинома Жегалкина P_j будет верно, что $\beta \notin \bigcup_{i=1}^j S_1(\alpha_i)$.

Заметим, что

$$\begin{aligned} f(x_1, \dots, x_n) &= Q_{j-1} \oplus P_{j-1} = Q_{j-1} \oplus (\hat{P}_j(\alpha) \oplus \check{P}_j(\alpha) \oplus P_j(\alpha)) \oplus P_{j-1} = \\ &= (Q_{j-1} \oplus \hat{Y}_j \oplus \check{Y}_j) \oplus (P'_j \oplus P_j(\alpha) \oplus P_{j-1}) = Q_j \oplus P_j. \end{aligned}$$

Теперь если $j < |T|$, то перейдем к шагу $(j + 1)$. Если $j = |T|$, то алгоритм завершает свою работу.

После шага $|T|$ мы получим, что для каждого слагаемого X_β полинома Жегалкина $P_{|T|}$ верно, что $\beta \notin \bigcup_{i=1}^{|T|} S_1(\alpha_i)$. Но так как множество T является покрытием шарами радиуса 1 куба E_2^n , в полиноме Жегалкина $P_{|T|}$ нет ни одного слагаемого, т.е. $P_{|T|} = 0$. Но $f(x_1, \dots, x_n) = Q_{|T|} \oplus P_{|T|}$. Отсюда получаем, что

$$f(x_1, \dots, x_n) = Q_{|T|} \oplus P_{|T|} = Q_{|T|} = \bigoplus_{j=1}^{|T|} (\hat{Y}_j \oplus \check{Y}_j).$$

Следовательно, найдена ПСПФ функции $f(x_1, \dots, x_n)$ с длиной, не превосходящей $2 \cdot |T|$.

Теорема 1.15 доказана. □

Для того, чтобы найти верхнюю оценку длины $L_2^{\text{ПСПФ}}(n)$ по теореме 1.15, нам надо найти оценку мощности покрытия шарами радиуса 1 куба E_2^n . Если воспользоваться кодом Хэмминга (см., например, [214]), то мы получим, что при каждом n куб E_2^n можно покрыть не более, чем $\frac{2^{n+1}}{n}$ шарами. Отсюда получается верхняя оценка $L_2^{\text{ПСПФ}}(n) \leq \frac{2^{n+2}}{n}$. Однако в [67] доказано более сильное утверждение, а именно, что существует покрытие куба $E_2^n (1+\varepsilon(n))\frac{2^n}{n}$ шарами радиуса 1, где $\varepsilon(n)$ – некоторая такая функция, что $\varepsilon(n) \rightarrow 0$ при $n \rightarrow \infty$. Поэтому получаем следующую теорему 1.6 о верхней оценке длины $L_2^{\text{ПСПФ}}(n)$ функций алгебры логики в классе ПСПФ.

Следствие 1.6. [267] *Справедливо неравенство $L_2(n) \leq (1 + \varepsilon(n))\frac{2^{n+1}}{n}$ для некоторой такой функции $\varepsilon(n)$, что $\varepsilon(n) \rightarrow 0$ при $n \rightarrow \infty$.*

Отметим, что в [175, 195] было найдено точное значение функции Шеннона $L_2^{\text{ПСПФ}}(n, 2)$ длины функций алгебры логики степени два в классе ПСПФ:
 $L_2^{\text{ПСПФ}}(n, 2) = \lfloor \frac{n}{2} \rfloor + 1$.

2 Приближение функций полиномами

В этом разделе мы рассматриваем приближение функций k -значных логик полиномами по модулю k и исследуем сложность таких приближений. Все результаты этого раздела опубликованы в [244].

Р.М. Джавадовым рассматривались приближенные представления функций алгебры логики полиномами Жегалкина, дизъюнктивными нормальными формами (ДНФ) и некоторыми их обобщениями и исследовались оценки сложности таких приближений [54]. Мы рассматриваем приближения с заданной точностью функций k -значных логик полиномами по модулю k . Под мерой приближения одной функции к другой понимается число наборов, в которых эти функции отличаются друг от друга.

Если $f, g \in P_k^n$, то назовем *расстоянием* между функциями f и g величину $d(f, g)$, равную числу наборов куба E_k^n , в которых эти функции различаются.

Пусть δ , $0 \leq \delta \leq 1$, – действительное число, q , $q \geq 1$, – натуральное число.

Для функции $f(x_1, \dots, x_n)$ функция $g(x_1, \dots, x_n)$ называется δ -*приближением*, если доля наборов из E_k^n , в которых функции f и g отличаются, не превосходит δ , т.е. если $\frac{d(f, g)}{k^n} \leq \delta$. Назовем *длиной* $l^\delta(f)$ (соответственно, *рангом* $r^\delta(f)$) функции $f \in P_k^n$ с точностью δ величину $\min l(g)$ (соответственно, $\min r(g)$), где минимум берется по всем функциям $g \in P_k^n$, являющимся δ -приближениями функции f .

Для функции $f(x_1, \dots, x_n)$ функция $g(x_1, \dots, x_n)$ является *приближением с точностью до q точек*, если число наборов куба E_k^n , в которых функции f и g различаются, не больше q , т.е. если $d(f, g) \leq q$. Аналогично вводим понятия длины и ранга функции $f \in P_k^n$ с точностью до q точек.

Будем говорить, что полином $P(g)$ является δ -*приближением* функции $f \in P_k^n$, если δ -приближением функции f является функция $g \in P_k^n$. Будем

исследовать числовые характеристики полиномов по модулю k , приближающих с заданной точностью все функции из P_k^n .

Пусть δ_n , $0 \leq \delta_n \leq 1$, $n = 0, 1, \dots$, – последовательность действительных чисел. Пусть при каждом n величина $r_k^{\delta_n}(n)$ (соответственно, $l_k^{\delta_n}(n)$) обозначает такое наименьшее число r (соответственно, наименьшее число l), что полиномами ранга, не большего r , (длины, не большей l), над переменными $x_1, \dots, x_n$ можно приблизить все функции из P_k^n с точностью δ_n . Другими словами, $r_k^{\delta_n}(n) = \max r^{\delta_n}(f)$ и $l_k^{\delta_n}(n) = \max l^{\delta_n}(f)$, где максимум берется по всем функциям $f \in P_k^n$.

В зависимости от вида последовательности δ_n введем некоторые обозначения. Если $\delta_n = \delta$, где $0 \leq \delta \leq 1$ – действительное число, то величины $r_k^{\delta_n}(n)$ и $l_k^{\delta_n}(n)$ будем обозначать как $r_k^\delta(n)$ и $l^\delta(n)$ соответственно.

Если $\delta_n = \frac{q}{k^n}$, где $q \geq 1$ – натуральное число, то величины $r_k^{\delta_n}(n)$ и $l_k^{\delta_n}(n)$ будем обозначать как $r_k^{(q)}(n)$ и $l^{(q)}(n)$ соответственно. Заметим, что в этом случае каждая функция $f \in P_k^n$ приближается с точностью до q точек.

Предложение 2.1. [244] Пусть k – простое число. Пусть δ , $0 < \delta \leq 1$, – действительное число, δ_n , $0 < \delta_n \leq 1$, $\delta_n \rightarrow 0$ при $n \rightarrow \infty$, $\frac{1}{k^n} = o(\delta_n)$, q – натуральное число, $q \geq 1$. Тогда для всех n , начиная с некоторого значения n_0 , верно

- 1) $0 \leq r_k^\delta(n) \leq r_k^{\delta_n}(n) \leq r_k^{(q)}(n) \leq \dots \leq r_k^{(1)}(n) \leq n$.
- 2) $0 \leq l_k^\delta(n) \leq l_k^{\delta_n}(n) \leq l_k^{(q)}(n) \leq \dots \leq l_k^{(1)}(n) \leq k^n$.

Р.М. Джавадовым были получены следующие оценки ранга и длины полиномов, приближающих функции алгебры логики с различными точностями [54]:

- 1) $r_2^\delta(n) = 0$ при $\delta \geq \frac{1}{2}$;
- 2) $r_2^\delta(n) \sim \frac{1}{2} \cdot n$ при $0 < \delta < \frac{1}{2}$ и $n \rightarrow \infty$;

- 3) $l_2^\delta(n) = 1$ при $\delta \geq \frac{1}{2}$;
 4) $l_2^\delta(n) \leq (\frac{1-\delta}{2} + o(1)) \cdot 2^n$ при $0 < \delta < \frac{1}{2}$ и $n \rightarrow \infty$.

Мы доказываем оценки ранга и длины полиномов, приближающих функции k -значной логики заданной точностью, а также рассматриваем некоторые другие виды точностей приближений для функций алгебры логики.

Сначала докажем некоторые вспомогательные утверждения, которые нам понадобятся в дальнейшем.

Лемма 2.1. [244] 1. Если $k \geq 2$ и $r < \frac{k-1}{k}n$, то

$$\sum_{i=0}^r C_n^i (k-1)^i \leq \frac{(k-1)(n-r)}{(k-1)n - kr} \cdot C_n^r \cdot (k-1)^r.$$

Если при этом $\frac{r}{n} = \lambda \leq \delta$ для некоторого действительного числа $\delta < \frac{k-1}{k}$, то $\sum_{i=0}^r C_n^i (k-1)^i \leq \frac{1}{1 - \frac{k}{k-1}\delta} \cdot k^{H_k(\delta)n}$, где $H_k(x)$ – функция k -значной энтропии.

2. Если $k \geq 2$ и $r > \frac{k-1}{k}n$, то

$$\sum_{i=r}^n C_n^i (k-1)^i \leq \frac{r}{kr - (k-1)n} \cdot C_n^r \cdot (k-1)^r.$$

Если при этом $\frac{r}{n} = (1 - \lambda) \geq (1 - \delta)$ для некоторого действительного числа $\delta < \frac{1}{k}$, то $\sum_{i=0}^r C_n^i (k-1)^i \leq \frac{1}{1 - k\delta} \cdot k^{H_k(\delta)n}$, где $H_k(x)$ – функция k -значной энтропии.

Доказательство. Докажем аналогично доказательству из [218] (стр. 213).

1. Пусть $r < \frac{k-1}{k} \cdot n$. Подсчитаем сумму $\sum_{i=0}^r C_n^i (k-1)^i$:

$$\begin{aligned} \sum_{i=0}^r C_n^i (k-1)^i &= C_n^0 (k-1)^0 + C_n^1 (k-1)^1 + \dots + C_n^r (k-1)^r = \\ &= C_n^r (k-1)^r + \dots + C_n^1 (k-1)^1 + C_n^0 (k-1)^0 \leq \\ &\leq C_n^r (k-1)^r \left(1 + \frac{r}{(n-r+1)(k-1)} + \frac{r^2}{(n-r+1)^2(k-1)^2} + \dots\right) \leq \\ &\leq C_n^r (k-1)^r \left(1 + \frac{r}{(n-r)(k-1)} + \frac{r^2}{(n-r)^2(k-1)^2} + \dots\right) \end{aligned}$$

При $r < \frac{k-1}{k} \cdot n$ верно $\frac{r}{(n-r)(k-1)} < 1$, т.е. в скобках стоит сумма бесконечно убывающей геометрической прогрессии. Эта сумма равна $\frac{1}{1 - \frac{r}{(n-r)(k-1)}} = \frac{(k-1)(n-r)}{(k-1)n - kr}$.

Пусть теперь $r = \lambda n \leq \delta n$, для некоторых действительных чисел $\lambda \leq \delta < \frac{k-1}{k}$. Тогда по оценке биномиального коэффициента и по свойствам функции $H_k(x)$ получаем, что

$$C_n^r (k-1)^r = C_n^{\lambda n} (k-1)^{\lambda n} \leq \lambda^{-\lambda n} \cdot (1-\lambda)^{-(1-\lambda)n} \cdot (k-1)^{\lambda n} = k^{H_k(\lambda)n} \leq k^{H_k(\delta)n}.$$

Следовательно,

$$\sum_{i=0}^r C_n^i (k-1)^i \leq \frac{(k-1)(n-r)}{(k-1)n - kr} C_n^r (k-1)^r = \frac{1-\lambda}{1 - \frac{k}{k-1}\lambda} C_n^r (k-1)^r \leq \frac{1}{1 - \frac{k}{k-1}\delta} k^{H_k(\delta)n}.$$

2. Пусть $r > \frac{k-1}{k} \cdot n$. Подсчитаем сумму $\sum_{i=r}^n C_n^i (k-1)^i$:

$$\begin{aligned} \sum_{i=r}^n C_n^i (k-1)^i &= C_n^r (k-1)^r + C_n^{r+1} (k-1)^{r+1} + \dots + C_n^n (k-1)^n \leq \\ &\leq C_n^r (k-1)^r \left(1 + (k-1) \cdot \frac{n-r}{r+1} + (k-1)^2 \cdot \frac{(n-r)^2}{(r+1)^2} + \dots \right) \leq \\ &\leq C_n^r (k-1)^r \left(1 + (k-1) \cdot \frac{n-r}{r} + (k-1)^2 \cdot \frac{(n-r)^2}{r^2} + \dots \right) \leq \\ &\leq C_n^r (k-1)^r \frac{1}{1 - \frac{(k-1)(n-r)}{r}} = \\ &= C_n^r (k-1)^r \frac{r}{kr - (k-1)n}. \end{aligned}$$

Здесь также было учтено, что при $r > \frac{k-1}{k} \cdot n$ верно $\frac{n-r}{r} < 1$, и в скобках сумма бесконечно убывающей геометрической прогрессии.

Пусть теперь $r = (1-\lambda)n \geq (1-\delta)n$, для некоторых действительных чисел $\lambda \leq \delta < \frac{1}{k}$. Тогда по оценке биномиального коэффициента и по свойствам функции $H_k(x)$ получаем, что

$$C_n^r (k-1)^r = C_n^{\lambda n} (k-1)^{\lambda n} \leq \lambda^{-\lambda n} \cdot (1-\lambda)^{-(1-\lambda)n} \cdot (k-1)^{\lambda n} = k^{H_k(1-\lambda)n} \leq k^{H_k(1-\delta)n}.$$

Следовательно,

$$\sum_{i=r}^n C_n^i (k-1)^i \leq \frac{r}{kr - (k-1)n} C_n^r (k-1)^r = \frac{1-\lambda}{1-k\lambda} C_n^r (k-1)^r \leq \frac{1}{1-k\delta} k^{H_k(1-\delta)n}.$$

Лемма 2.1 доказана. $\square$

Лемма 2.2. [244] Если $k \geq 2$ и $r(n)$ – последовательность натуральных чисел, $\lambda_n = \frac{r(n)}{n} \leq \delta < \frac{k-1}{k}$, где δ – действительное число, то найдется такое действительное число ε , $0 < \varepsilon < 1$, что $\sum_{i=0}^{r(n)} C_n^i (k-1)^i \leq k^{\varepsilon n}$ для всех n , начиная с некоторого значения n_0 .

Доказательство. Для каждого n рассмотрим сумму $\sum_{i=0}^{r(n)} C_n^i (k-1)^i$.

По лемме 2.1

$$\sum_{i=0}^{r(n)} C_n^i (k-1)^i = \sum_{i=0}^{\lambda_n n} C_n^i (k-1)^i \leq \frac{1}{1 - \frac{k}{k-1} \delta} k^{H_k(\delta)n}.$$

Отсюда, учитывая, что $H_k(\delta) < H_k(\frac{k-1}{k}) = 1$, получаем, что найдется такое действительное число ε , $0 < \varepsilon < 1$, что $\sum_{i=0}^{r(n)} C_n^i (k-1)^i \leq k^{\varepsilon n}$ для всех n , начиная с некоторого значения n_0 .

Лемма 2.2 доказана. □

Лемма 2.3. [244] Пусть $k \geq 2$ и $r(n)$ – последовательность натуральных чисел, $\lambda_n = \frac{r(n)}{n} \leq \delta_n$, где $\delta_n \rightarrow 0$ при $n \rightarrow \infty$.

Тогда для любого действительного числа $\varepsilon > 0$ найдется такое действительное число ε_1 , $0 < \varepsilon_1 < 1$, что для любой такой последовательности $l(n)$ положительных чисел, что $l(n) \leq (\frac{k-1}{k} - \varepsilon) \cdot n$, верно, что $\sum_{i=0}^{r(n)} C_n^i (k-1)^i \cdot \sum_{j=0}^{l(n)} C_n^j (k-1)^j \leq k^{(1-\varepsilon_1)n}$ для всех n , начиная с некоторого значения n_0 .

Доказательство. Рассмотрим произведение

$$\sum_{i=0}^{r(n)} C_n^i (k-1)^i \cdot \sum_{j=0}^{l(n)} C_n^j (k-1)^j.$$

По лемме 2.1 выписанное произведение не больше

$$\frac{1}{1 - \frac{k}{k-1} \delta_n} \cdot k^{H_k(\delta_n)n} \cdot \frac{1}{1 - \frac{k}{k-1} (\frac{k-1}{k} - \varepsilon)} \cdot k^{H_k(\frac{k-1}{k} - \varepsilon)n}.$$

Оценим значение выражения $H_k(\delta_n) + H_k\left(\frac{k-1}{k} - \varepsilon\right)$.

Для этого рассмотрим функцию

$$\hat{H}_k = H_k(x) + H_k\left(\frac{k-1}{k} - \varepsilon\right)$$

интервале $(0; \frac{k-1}{k})$.

Найдем ее свойства:

- 1) $\lim_{x \rightarrow 0} \hat{H}_k(x) = H_k\left(\frac{k-1}{k} - \varepsilon\right) < 1$;
- 2) функция $\hat{H}_k(x)$ непрерывна на промежутке $(0, \frac{k-1}{k} - \varepsilon)$.

Следовательно, найдется такая окрестность справа нуля I и такое действительное число ε_2 , $\varepsilon_2 > 0$, что для всех x , $x \in I$, верно $\hat{H}_k(x) \leq 1 - \varepsilon_2$.

Если δ_n – последовательность положительных чисел и $\delta_n \rightarrow 0$ при $n \rightarrow \infty$, то для всех n , начиная с некоторого значения n_0 , верно $\delta_n \in I$, и значит, $\hat{H}_k(\delta_n) \leq 1 - \varepsilon_2$.

Т.е. $\sum_{i=0}^{r(n)} C_n^i (k-1)^i \cdot \sum_{j=0}^{l(n)} C_n^j (k-1)^j \leq C \cdot k^{(1-\varepsilon_2)n} \leq k^{(1-\varepsilon_1)n}$ для некоторого действительного числа ε_1 , $0 < \varepsilon_1 < \varepsilon_2$, и всех n , начиная с некоторого значения n_0 .

Лемма 2.3 доказана. □

Теперь докажем теорему 2.1 о ранге полиномов, приближающих функции k -значной логики с заданной точностью.

Теорема 2.1. [244] Пусть k – простое число, δ , $0 \leq \delta \leq 1$, – действительное число, δ_n , $0 \leq \delta_n \leq 1$ – последовательность действительных чисел, $\delta_n \rightarrow 0$ при $n \rightarrow \infty$, q , $q \geq 1$, – натуральное число. Тогда

- 1) $r_k^\delta(n) = 0$ при $\delta \geq \frac{k-1}{k}$;
- 2) $r_k^\delta(n) \sim \frac{k-1}{k} \cdot n$ при $0 < \delta < \frac{k-1}{k}$ и $n \rightarrow \infty$;
- 3) $r_k^{\delta_n}(n) \sim \frac{k-1}{k} \cdot n$ при $\frac{1}{k^n} = o(\delta_n)$ и $n \rightarrow \infty$;
- 4) $r_k^{(q)}(n) = n$ для всех n , начиная с некоторого значения n_0 , при $k \geq 3$;

5) $n - 2 \leq r_2^{(q)}(n) \leq n - 1$ для всех n , начиная с некоторого значения n_0 , при $q \geq 2$, $r_2^{(1)}(n) = n - 1$;

6) $r_k^\delta(n) = n$ при $\delta = 0$.

Доказательство. Рассмотрим произвольную функцию $f(x_1, \dots, x_n) \in P_k^n$.

1. Если $\delta \geq \frac{k-1}{k}$, то полином с требуемым приближением для функции f можно построить следующим образом. Найдем такое значение $c \in E_k$, что число наборов куба E_k^n , в которых функция f принимает значение c , не меньше, чем $\frac{1}{k} \cdot k^n$. Такое значение c всегда существует. Рассмотрим функцию $g(x_1, \dots, x_n) = c \in P_k$. Приближим функцию f полиномом $P(g) = c$. По построению функция g является δ -приближением функции f . Ранг полинома $P(g)$ равен 0. Полиномов меньшего ранга нет (по определению $r(0) = 0$).

Следовательно, при $\delta \geq \frac{k-1}{k}$ верно $r_k^\delta(n) = 0$.

2. Пусть $0 < \delta < \frac{k-1}{k}$.

Верхняя оценка. Пусть $\varepsilon > 0$ – действительное число и $r(n)$ – такая последовательность целых чисел, что $r(n) \leq (\frac{k-1}{k} + \varepsilon) \cdot n$. Отсечем в полиноме $P(f)$ все слагаемые ранга, большего $r(n)$. Получим полином некоторой функции $g(x_1, \dots, x_n) \in P_k^n$.

Заметим, что функции f и g совпадают на всех наборах куба E_k^n , в которых не менее $(n - r(n))$ нулей. На оставшихся наборах эти функции могут отличаться. Наборов, в которых функции f и g могут отличаться, не больше $\sum_{i=r(n)}^n C_n^i (k-1)^i$. По лемме 2.1 $\sum_{i=r(n)+1}^n C_n^i (k-1)^i \leq \frac{1}{k\varepsilon} k^{H_k(\frac{k-1}{k}-\varepsilon)n}$.

Т.к. $H_k(\frac{k-1}{k} - \varepsilon) < 1$, найдется такое значение n_0 , что для всех $n \geq n_0$ выполняется $\frac{1}{k\varepsilon} k^{H_k(\frac{k-1}{k}-\varepsilon)n} \leq \delta k^n$. Т.е. функция g является δ -приближением функции f .

Нижняя оценка. Пусть $\varepsilon > 0$ – действительное число и $r(n)$ – такая последовательность целых чисел, что $r(n) \leq (\frac{k-1}{k} - \varepsilon) \cdot n$.

Подсчитаем, сколько функций k -значной логики, зависящих от переменных $x_1, \dots, x_n$, можно приблизить полиномами над переменными $x_1, \dots, x_n$ ранга, не большего $r(n)$.

Таких полиномов ранга, не превосходящего $r(n)$, не более $k^{\sum_{j=0}^{r(n)} C_n^j (k-1)^j}$. Каждый из них может являться δ -приближением не более $\sum_{i=0}^{\delta k^n} C_{k^n}^i (k-1)^i$ функций. Поэтому такими полиномами ранга, не большего $r(n)$, можно приблизить не более $k^{\sum_{j=0}^{r(n)} C_n^j (k-1)^j} \cdot \sum_{i=0}^{\delta k^n} C_{k^n}^i (k-1)^i$ функций.

По лемме 2.2 найдутся такие действительные числа ε_1 и ε_2 , $0 < \varepsilon_1, \varepsilon_2 < 1$, что $\sum_{j=0}^{r(n)} C_n^j (k-1)^j \leq k^{\varepsilon_1 n}$ и $\sum_{i=0}^{\delta k^n} C_{k^n}^i (k-1)^i \leq k^{\varepsilon_2 k^n}$ для всех n , начиная с некоторого значения n_0 .

Следовательно, для всех n , начиная со значения n_0 , полиномов над переменными $x_1, \dots, x_n$ ранга, не большего $r(n)$, не хватает для приближения всех k^{k^n} функций. Т.е. для любого $\varepsilon > 0$ для всех n , начиная с некоторого значения $n_0 = n_0(\varepsilon)$ верно $r_k^\delta(n) \geq (\frac{k-1}{k} - \varepsilon) \cdot n$.

Собирая вместе верхнюю и нижнюю оценки, получаем $r_k^\delta(n) \sim \frac{k-1}{k} \cdot n$ при $n \rightarrow \infty$.

3. Пусть δ_n , $0 < \delta_n \leq 1$, – последовательность действительных чисел, $\delta_n \rightarrow 0$ при $n \rightarrow \infty$ и $\frac{1}{k^n} = \bar{o}(\delta_n)$ при $n \rightarrow \infty$.

Верхняя оценка доказывается аналогично верхней оценке п. 2, т.к. оценка $\frac{1}{k^\varepsilon} k^{H_k(\frac{k-1}{k} - \varepsilon)n} \leq \delta_n k^n$ выполняется для всех n , начиная с некоторого значения n_0 , при указанных ограничениях на последовательность δ_n .

Нижняя оценка следует из предложения 2.1.

Поэтому $r_k^{\delta_n} \sim \frac{k-1}{k} \cdot n$ при $n \rightarrow \infty$.

4. *Верхняя оценка.* По предложению 2.1 верно $r_k^{(q)}(n) \leq n$.

Нижняя оценка. Подсчитаем, сколько функций k -значной логики, зави-

сящих от переменных $x_1, \dots, x_n$, можно приблизить полиномами над переменными $x_1, \dots, x_n$ ранга, не большего $(n - 1)$. Всего таких полиномов не более $k^{k^n - (k-1)^n}$. Каждый из них может приближать не более $\sum_{i=0}^q C_{k^n}^i \leq q \cdot k^{qn}$ функций. Следовательно, полиномами ранга, не большего $(n - 1)$, можно приблизить не более $k^{k^n - (k-1)^n} \cdot q \cdot k^{qn}$ функций. Полученное выражение меньше k^{k^n} при $k \geq 3$ для всех n , начиная с некоторого значения n_0 . Т.е. $r_k^{(q)}(n) \geq n$ для всех n , начиная с некоторого значения n_0 , при $k \geq 3$.

Получаем $r_k^{(q)}(n) = n$ для всех n , начиная с некоторого значения n_0 , при $k \geq 3$.

5. Рассмотрим функцию $f(x_1, \dots, x_n) \in P_2^n$. Вычеркнем в полиноме $P(f)$ моном ранга n (если он есть). Получим полином некоторой функции $g(x_1, \dots, x_n) \in P_2^n$. Значения функций f и g могут отличаться не более, чем на одном наборе куба E_2^n . Следовательно, $r_2^{(q)}(n) \leq r_2^{(1)}(n) \leq n - 1$.

Теперь подсчитаем, сколько функций алгебры логики, зависящих от переменных $x_1, \dots, x_n$, можно приблизить полиномами над переменными $x_1, \dots, x_n$ ранга, не большего $(n - 3)$. Всего таких полиномов не более $2^{2^n - C_n^2 - n - 1}$. Каждый из них может приближать не более $\sum_{i=0}^q C_{2^n}^i \leq q \cdot 2^{qn}$ функций. Следовательно, такими полиномами ранга, не большего $(n - 3)$, можно приблизить не более $2^{2^n - \frac{n(n-1)}{2} - n - 1} \cdot q \cdot 2^{qn}$ функций. Полученное выражение меньше 2^{2^n} для всех n , начиная с некоторого значения n_0 , если $q \geq 2$. Т.е. $r_2^{(q)}(n) \geq n - 2$ при $q \geq 2$.

Если $q = 1$, то подсчитаем, сколько функций алгебры логики, зависящих от переменных $x_1, \dots, x_n$, можно приблизить полиномами над переменными $x_1, \dots, x_n$ ранга $(n - 2)$. Получаем, что не более, чем $2^{2^n - n - 1} \cdot (2^n + 1)$ функций. Т.е. число таких функций меньше 2^{2^n} , откуда $r_2^{(1)}(n) \geq n - 1$.

Собирая вместе верхние и нижние оценки, получаем $n - 2 \leq r_2^{(q)}(n) \leq n - 1$ для всех n , начиная с некоторого значения n_0 при $q \geq 2$, и $r_2^{(1)}(n) = n - 1$.

6. Если $\delta = 0$, то требуется построить функцию k -значной логики, которая не отличается от функции f ни на одном наборе куба E_k^n . А значит, единственной подходящей функцией будет она сама. А т.к. при простых k каждая функция k -значной логики задается полиномом по модулю k вида (2) однозначно и наибольший ранг полинома функции, зависящей от переменных $x_1, \dots, x_n$, равен n , то $r_k^\delta(n) = n$.

Теорема 2.1 доказана. □

Замечание 2.1. Во время работы над диссертацией автору В.Б. Алексеевым было сообщено, что можно доказать, что $r_2^{(q)}(n) \leq n - 2$ при $q \geq 2$. В самом деле, пусть функция $f(x_1, \dots, x_n) \in P_2$ имеет вид

$$f(x_1, \dots, x_n) = h(x_1, \dots, x_n) \oplus cx_1 \dots x_n \oplus \bigoplus_{|\beta|=n-1} c_\beta X_\beta,$$

где $\deg(h) \leq n - 2$, $c, c_\beta \in E_2^n$. Тогда функция

$$g(x_1, \dots, x_n) = f(x_1, \dots, x_n) \oplus (c \oplus 1)x_1 \dots x_n \oplus \prod_{|\beta|=n-1} (X_{\beta \oplus (1, \dots, 1)} \oplus c_\beta)$$

является приближением функции f с точностью до двух точек, и $r(g) \leq n - 2$. Отсюда с учетом нижней оценки получаем, что $r_2^{(q)}(n) = n - 2$ при $q \geq 2$ для всех n , начиная с некоторого значения n_0 .

Для оценки длины приближений функций k -значной логики полиномами докажем еще несколько вспомогательных утверждений.

Лемма 2.4. [244] Пусть k – простое число. Если для некоторого типа t , $t \subseteq \{1, \dots, n\}$, функция $f(x_1, \dots, x_n) \in P_k^n$ равна нулю на всех таких наборах $\alpha \in E_k^n$, что $t(\alpha) \subseteq t$, то ее полином $P(f)$ не содержит таких слагаемых X , что $t(X) \subseteq t$.

Доказательство. Пусть $t = \{i_1, \dots, i_r\}$, $0 \leq r \leq n$. Предположим противное: пусть полином $P(f)$ содержит такое слагаемое X , что $t(X) \subseteq t$.

Для функции $f(x_1, \dots, x_n)$ положим $x_j = 0$ для всех $j \neq i_1, \dots, i_r$. Получим некоторую функцию $g(x_{i_1}, \dots, x_{i_r}) \in P_k$.

Заметим, что полином $P(g)$ не пустой полином, т.к. по меньшей мере он содержит слагаемое X . Т.к. при простом k каждая функция k -значной логики задается полиномом по модулю k вида (2) однозначно, и тождественно равную нулю функцию задает пустой полином [218] (стр. 69–71), функция $g(x_{i_1}, \dots, x_{i_r})$ принимает ненулевое значение хотя бы на одном наборе значений переменных.

Приходим к противоречию, т.к. по описанию функции $f(x_1, \dots, x_n)$ получающаяся из нее функция $g(x_{i_1}, \dots, x_{i_r})$ тождественно равна нулю.

Следовательно, предположение неверно, и полином $P(f)$ не содержит таких слагаемых X , что $t(X) \subseteq t$.

Лемма 2.4 доказана. □

Следствие 2.1. [244] *Если k – простое число, и функция $f(x_1, \dots, x_n) \in P_k^n$ равна нулю на всех наборах ранга, не большего r , $0 \leq r \leq n$, то полином $P(f)$ не содержит слагаемых ранга, меньшего либо равного r .*

Пусть $E \subseteq E_k^n$. Назовем множество E *стабильным*, если оно обладает следующим свойством: если оно содержит набор типа t , то оно содержит также все возможные наборы типа t .

Лемма 2.5. [244] *Пусть k – простое число. Если $E, E \subseteq E_k^n$, – стабильное множество, то для каждой функции $f(x_1, \dots, x_n) \in P_k^n$ найдется такая функция $g(x_1, \dots, x_n) \in P_k^n$, совпадающая с функцией $f(x_1, \dots, x_n)$ на множестве E , для которой $t(g) \subseteq t(E)$.*

Доказательство. Доказательство леммы 2.5 проведем индукцией по числу различных типов в множестве E .

Базис индукции. Пусть множество E содержит наборы только одного типа t . Пусть $t = \{i_1, \dots, i_r\}$, $0 \leq r \leq n$.

Рассмотрим функцию $f_0(x_1, \dots, x_n) \in P_k^n$:

$$f_0(x_1, \dots, x_n) = \begin{cases} f(x_1, \dots, x_n) & \text{на } E, \\ 0 & \text{на } E_k^n \setminus E. \end{cases}$$

Положим в функции $f_0(x_1, \dots, x_n)$ равными нулю все переменные x_j при $j \neq i_1, \dots, i_r$. Получим функцию $g_0(x_{i_1}, \dots, x_{i_r}) \in P_k$. По следствию 2.1 полином $P(g_0)$ может содержать только слагаемые ранга r . Следовательно, $t(g_0) \subseteq t(E)$.

По построению значения функции $g(x_1, \dots, x_n) = g_0(x_{i_1}, \dots, x_{i_r}) \in P_k^n$ совпадают со значениями функции $f(x_1, \dots, x_n)$ на множестве E и $t(g) \subseteq t(E)$. Т.е. функция $g(x_1, \dots, x_n)$ – искомая.

Индуктивный переход. Пусть для каждого стабильного подмножества E_k^n с числом различных типов τ , $\tau \geq 1$, утверждение леммы 2.5 верно.

Рассмотрим стабильное множество E , $E \subseteq E_k^n$, в котором $(\tau + 1)$ различных тип.

Выделим в множестве E некоторый тип t , $t = \{i_1, \dots, i_r\}$, максимальный (в частичном упорядочении множества всех подмножеств из $\{1, \dots, n\}$ по включению) среди всех типов множества E (если максимальных типов несколько, то можно взять любой из них).

Разобьем множество E на две части: стабильное подмножество E_1 , содержащее наборы всех типов, кроме типа t , и стабильное подмножество E_2 , $E_2 = E \setminus E_1$.

По предположению индукции найдется функция $g_1(x_1, \dots, x_n) \in P_k^n$, совпадающая с функцией $f(x_1, \dots, x_n)$ на множестве E_1 , для которой верно $t(g_1) \subseteq t(E_1)$.

Рассмотрим функцию $f_2(x_1, \dots, x_n) \in P_k^n$:

$$f_2(x_1, \dots, x_n) = \begin{cases} f(x_1, \dots, x_n) - g_1(x_1, \dots, x_n) & \text{на } E_2, \\ 0 & \text{на } E_k^n \setminus E_2. \end{cases}$$

По следствию 2.1 полином $P(f_2)$ не содержит слагаемые ранга, меньшего r . Пусть $g_2(x_1, \dots, x_n) \in P_k^n$ – такая функция, что $P(g_2)$ – это полином, получающийся из полинома $P(f_2)$, если в нем оставить только слагаемые типа t . Заметим, что функция $g_2(x_1, \dots, x_n)$ равна нулю на всех наборах ранга меньшего r и на наборах ранга, равного r , но тип которых не t .

Рассмотрим функцию $g(x_1, \dots, x_n) = g_1(x_1, \dots, x_n) + g_2(x_1, \dots, x_n) \in P_k^n$.

$$\begin{aligned} g(x_1, \dots, x_n) &= \begin{cases} g_1(x_1, \dots, x_n) & \text{на } E_1, \\ g_1(x_1, \dots, x_n) + g_2(x_1, \dots, x_n) & \text{на } E_2, \end{cases} \\ &= \begin{cases} g_1(x_1, \dots, x_n) & \text{на } E_1, \\ g_1(x_1, \dots, x_n) + f(x_1, \dots, x_n) - g_1(x_1, \dots, x_n) & \text{на } E_2, \end{cases} \\ &= \begin{cases} f(x_1, \dots, x_n) & \text{на } E_1, \\ f(x_1, \dots, x_n) & \text{на } E_2. \end{cases} \end{aligned}$$

По построению полином $P(g)$ состоит только из слагаемых типов элементов множества E .

Лемма 2.5 доказана. □

Следствие 2.2. [244] Пусть k – простое число. Если E , $E \subseteq E_k^n$, – стабильное множество, то для каждой функции $f(x_1, \dots, x_n) \in P_k^n$ найдется такая функция $g(x_1, \dots, x_n) \in P_k^n$, совпадающая с функцией $f(x_1, \dots, x_n)$ на множестве E , что длина полинома $P(g)$ не больше $|E|$.

Следствие 2.3. [244] Если k – простое число, то $l_k^\delta(n) \leq (1 - \delta) \cdot k^n + (k - 1)^n$ при $0 \leq \delta \leq 1$.

Доказательство. Выберем стабильное множество E , $E \subseteq E_k^n$, по следующим правилам:

1) если мы добавили некоторый набор $\alpha \in E_k^n$ к множеству E , то мы

добавим к нему все наборы типа $t(\alpha)$;

2) если в множестве E меньше $\lceil (1 - \delta) \cdot k^n \rceil$ наборов, то продолжаем добавлять к нему наборы.

Пусть таким образом мы построим стабильное множество $|E|$, содержащее l наборов. Заметим, что $\lceil (1 - \delta) \cdot k^n \rceil \leq l \leq \lceil (1 - \delta) \cdot k^n \rceil + (k - 1)^n - 1$.

По лемме 2.5 найдется функция $g(x_1, \dots, x_n) \in P_k^n$, совпадающая с функцией $f(x_1, \dots, x_n)$ на множестве E , для которой $t(g) \subseteq t(E)$. Т.е. функции f и g различаются не более, чем на

$$k^n - \lceil (1 - \delta) \cdot k^n \rceil \leq k^n - (1 - \delta) \cdot k^n \leq \delta \cdot k^n$$

наборах куба E_k^n . Другими словами, функция g является δ -приближением функции f .

По следствию 2.2 длина полинома $P(g)$ не больше l , т.е. не больше $\lceil (1 - \delta) \cdot k^n \rceil + (k - 1)^n - 1 \leq (1 - \delta) \cdot k^n + (k - 1)^n$.

Следствие 2.3 доказано. □

Теперь докажем теорему 2.2 о длине приближений функций k -значной логики полиномами по модулю k .

Теорема 2.2. [244] Пусть k – простое число, δ , $0 \leq \delta \leq 1$, – действительное число, δ_n , $0 < \delta_n \leq 1$ – последовательность действительных чисел, $\delta_n \rightarrow 0$ при $n \rightarrow \infty$, q , $q \geq 1$ – натуральное число. Тогда

1) $l_k^\delta(n) = 1$ при $\delta \geq \frac{k-1}{k}$;

2) $l_k^\delta(n) \leq \frac{k-1}{k} \cdot (1 - \delta) \cdot k^n + C \cdot (k - 1)^n$ при $0 < \delta < \frac{k-1}{k}$ для некоторого

действительного числа C , $C > 0$;

3) $l_k^{\delta_n}(n) \sim \frac{k-1}{k} \cdot k^n$ при $\delta_n \geq (\frac{k-1}{k})^n$ и $n \rightarrow \infty$.

4) $l_2^{(q)}(n) \sim \frac{1}{2} \cdot 2^n$ при $n \rightarrow \infty$.

5) $l_k^\delta(n) = k^n$ при $\delta = 0$.

Доказательство. Рассмотрим произвольную функцию $f(x_1, \dots, x_n) \in P_k^n$.

1. Если $\delta \geq \frac{k-1}{k}$, то полином с требуемым приближением можно построить аналогично доказательству п. 1 теоремы 2.1. Длина полинома будет равна 1. Полиномами меньшей длины не обойтись.

Следовательно, при $\delta \geq \frac{k-1}{k}$ верно $l_k^\delta(n) = 1$.

2. Пусть $0 < \delta < \frac{k-1}{k}$.

Верхняя оценка.

Определим стабильное множество E_0 , $E_0 \subseteq E_k^n$, по правилам:

1) нулевой набор; наборы, содержащие ровно $(n-1)$ ноль; наборы содержащие ровно $(n-2)$ нуля; и т. д.

2) каждый раз будем добавлять наборы одного типа, и только если наборы этого типа заканчиваются, будем переходить к другому типу;

3) так будем действовать до тех пор, пока не наберем ровно $\lceil (1-\delta) \cdot k^n \rceil + (k-1)^n$ наборов;

4) для выполнения условия леммы 2.5 может быть будет нужно добавить еще не более $(k-1)^n - 1$ наборов.

Пусть $|E_0| = l_0$. Заметим, что $\lceil (1-\delta) \cdot k^n \rceil + (k-1)^n \leq l_0 \leq \lceil (1-\delta) \cdot k^n \rceil + 2(k-1)^n - 1$.

Пусть $\hat{X} = \{X_\alpha \mid \alpha \in E_0\}$, т.е. X_0 – множество всех мономов, соответствующих наборам из множества E_0 .

По лемме 2.5 найдется такая функция $g_0(x_1, \dots, x_n) \in P_k^n$, в полиноме $P(g_0)$ которой не более l_0 слагаемых, что значения функции g_0 совпадают со значениями функции f на множестве E_0 .

Рассмотрим функцию $h(x) = x^{k-1} + x^{k-2} + \dots + x + 1$.

Т.к. $h(x) = \frac{x^k - 1}{x - 1}$ и при простых k верно $x^k = x \pmod{k}$, получаем $h(x) = 1$ при $x \neq 1$. Несложно проверить, что $h(1) = 0$.

Пусть $h_n(x_1, \dots, x_n) = h(x_1) \cdot \dots \cdot h(x_n)$. Функция $h_n(x_1, \dots, x_n)$ принимает

значение 1 на $(k-1)^n$ наборах куба E_k^n и значение 0 на $k^n - (k-1)^n$ наборах куба E_k^n . Ее полином $P(h_n)$ содержит k^n слагаемых, и все коэффициенты в полиноме $P(h_n)$ равны единице.

Оставим в полиноме $P(h_n)$ только слагаемые, являющиеся мономами из множества $\hat{X}$. Получим новую функцию $\hat{h}_n(x_1, \dots, x_n) \in P_k^n$, которая задается этим полиномом $P(\hat{h}_n)$ с l_0 слагаемыми.

Рассмотрим два случая.

1) Если в полиноме $P(g_0)$ не более, чем $\frac{k-1}{k} \cdot l_0$ слагаемых, то положим $g(x_1, \dots, x_n) = g_0(x_1, \dots, x_n)$. Различия между значениями функции g и функции f могут быть не более, чем на

$$k^n - \lceil (1 - \delta) \cdot k^n \rceil - (k - 1)^n \leq \delta \cdot k^n - (k - 1)^n \leq \delta \cdot k^n$$

наборах куба E_k^n .

2) Иначе, запишем полином $P(g_0)$ в виде

$$P(g_0) = Q_1 + 2Q_2 + \dots + (k-1)Q_{k-1},$$

где в полиномах Q_s , $s = 1, \dots, k-1$, все коэффициенты равны единице.

Выберем такое значение s , $0 \leq s \leq k-1$, что длина полинома Q_s не меньше $\frac{1}{k} \cdot l_0$. Такое s всегда существует.

Пусть $g(x_1, \dots, x_n) = g_0(x_1, \dots, x_n) - s \cdot \hat{h}_n(x_1, \dots, x_n)$. Значения функций g и g_0 на множестве E_0 различаются не более, чем на $(k-1)^n$ наборах куба E_k^n . Отсюда следует, что функции g и f могут различаться не более, чем на

$$k^n - \lceil (1 - \delta) \cdot k^n \rceil \leq \delta \cdot k^n$$

наборах куба E_k^n .

Длина полинома $P(g)$ не больше $\frac{k-1}{k} \cdot l_0$.

В обоих случаях функция g является δ -приближением функции f .

Длина полинома $P(g)$ не больше

$$\frac{k-1}{k} \cdot (\lceil (1-\delta) \cdot k^n \rceil + 2(k-1)^n - 1) \leq \frac{k-1}{k} \cdot ((1-\delta) \cdot k^n + 2(k-1)^n).$$

Т.е. $l_k^\delta(n) \leq \frac{k-1}{k} \cdot (1-\delta) \cdot k^n + C \cdot (k-1)^n$ для некоторого действительного числа C , $C > 0$.

3. *Верхняя оценка.* Рассмотрим функцию $h_n(x_1, \dots, x_n) \in P_k^n$, построенную в доказательстве п. 2 теоремы 2.2. Она принимает значение 1 на $(k-1)^n$ наборах куба E_k^n , и ее полином $P(h_n)$ содержит k^n слагаемых.

Если полином $P(f)$ содержит не более $\frac{k-1}{k} \cdot k^n$ слагаемых, то положим $g(x_1, \dots, x_n) = f(x_1, \dots, x_n)$.

Иначе, пусть полином $P(f)$ имеет вид

$$P(f) = Q_1 + 2Q_2 + \dots + (k-1)Q_{k-1},$$

где в каждом из полиномов Q_s , $s = 1, \dots, k-1$, все коэффициенты равны 1.

Выберем такое значение s , $1 \leq s \leq k-1$, что длина полинома Q_s не меньше $\frac{1}{k} \cdot k^n$. Такое значение s всегда существует.

Положим

$$g(x_1, \dots, x_n) = f(x_1, \dots, x_n) - s \cdot h_n(x_1, \dots, x_n).$$

В обоих случаях функция g отличается от функции f не более, чем на $(k-1)^n$ наборах куба E_k^n , что не больше $\delta_n \cdot k^n$. Полином $P(g)$ содержит не более $\frac{k-1}{k} \cdot k^n$ слагаемых. Отсюда $l_k^{\delta_n}(n) \leq \frac{k-1}{k} \cdot k^n$.

Нижняя оценка. Подсчитаем число функций k -значной логики, зависящих от переменных $x_1, \dots, x_n$, которые можно приблизить полиномами над переменными $x_1, \dots, x_n$ длины, не большей l .

Всего полиномов над переменными $x_1, \dots, x_n$ длины, не большей l , не более $\sum_{j=0}^l C_{k^n}^j (k-1)^j$. Для каждого n приближающие полиномы могут отличаться

от приближаемых функций не более, чем на $\delta_n \cdot k^n$ наборах куба E_k^n . Значит, каждый из полиномов может быть приближением не более

$$\sum_{i=0}^{\delta_n k^n} C_{k^n}^i (k-1)^i$$

функций.

Значит полиномами длины l можно приблизить не более

$$\sum_{i=0}^{\delta_n k^n} C_{k^n}^i (k-1)^i \cdot \sum_{j=0}^l C_{k^n}^j (k-1)^j$$

функций.

Пусть $\varepsilon > 0$ – действительное число. Положим $l(n) = (\frac{k-1}{k} - \varepsilon) \cdot k^n$. Тогда по лемме 2.2 для всех n , начиная с некоторого значения n_0 , выписанное произведение не больше $k^{(1-\varepsilon_1)k^n}$, где $\varepsilon_1 > 0$. Т.е. полиномов длины $l(n)$ не хватает для того, чтобы приблизить все k^{k^n} функций, зависящих от n переменных, при $n \geq n_0$.

Получаем, что $l_k^{\delta_n}(n) \geq (\frac{k-1}{k} - \varepsilon) \cdot k^n$ для любого $\varepsilon > 0$ при всех n , начиная с некоторого значения $n_0 = n_0(\varepsilon)$.

Следовательно, $l_k^{\delta_n}(n) \sim \frac{k-1}{k} \cdot k^n$ при $n \rightarrow \infty$.

4. Рассмотрим функцию $f(x_1, \dots, x_n)$ из P_2^n . Построим функцию $g(x_1, \dots, x_n) \in P_2^n$ как в п. 3 теоремы 2.2. Она может отличаться от функции f только на одном наборе $(0, \dots, 0)$. Ее полином $P(g)$ содержит не более $\frac{1}{2} \cdot 2^n$ слагаемых.

Значит, $l_2^{(g)}(n) \leq \frac{1}{2} \cdot 2^n$.

Из предложения 2.1 и п. 3 теоремы 2.2 получаем $l_2^{(g)}(n) \geq l_2^{\delta_n}(n) \geq (\frac{1}{2} - \varepsilon) \cdot 2^n$ для любого действительного числа $\varepsilon > 0$.

Следовательно, $l_2^{(g)}(n) \sim \frac{1}{2} \cdot 2^n$ при $n \rightarrow \infty$.

5. Если $\delta = 0$, то требуется построить функцию k -значной логики, которая не отличается от функции f ни на одном наборе куба E_k^n . А значит, един-

ственной подходящей функцией будет она сама. А т.к. при простых k каждая функция k -значной логики задается полиномом по модулю k вида (2) однозначно, и наибольшая длина полинома функции, зависящей от переменных $x_1, \dots, x_n$, равна k^n , то $l_k^\delta(n) = k^n$.

Теорема 2.2 доказана. □

Часть 2. Алгоритмические вопросы полиномиальных представлений функций k -значной логики

3 Распознавание свойств функций, заданных полиномами

В этом разделе мы докажем, что некоторые свойства функций k -значной логики распознаются с полиномиальной временной сложностью, если на вход алгоритма функции подаются в виде полиномов. Все результаты этого раздела опубликованы в работах [221–229, 231–233, 238, 241, 243, 246, 264, 270].

Мы будем исследовать алгоритмическую сложность распознавания свойств функций k -значной логики, связанных с задачей распознавания полноты систем функций. Пусть $M \subseteq P_k$. Множество M называется полной системой, если каждая функция k -значной логики может быть получена при помощи операции суперпозиции из функций множества M [218] (стр. 48). По критерию полноты [83] множество M – полная система тогда и только тогда, когда оно не содержится ни в одном из конечного числа *предполных классов*. Все предполные классы конструктивно описаны [101, 139, 172, 186, 187]. Их можно разделить на шесть семейств: предполные классы монотонных, самодвойственных, линейных функций, функций, сохраняющих разбиение, предполные классы типа В и типа С.

Алгоритмическая сложность распознавания свойств функций k -значной логики зависит от способа представления функций. Если функции заданы в виде формул в общем случае и даже в виде определенных форм (конъюнктивных или дизъюнктивных нормальных форм), то уже в двузначной логике часто задачи оказываются NP -трудными. Мы доказываем, что при представлении функций k -значных логик полиномами задачи распознавания принадлежности функции пяти семействам предполных классов, а именно

классам монотонных, самодвойственных, линейных функций, функций, сохраняющих разбиение, и классам функций типа В, имеют полиномиальное решение.

Мы рассматривали представление функций k -значной логики полиномами по модулю k . Но возможно полиномиальное представление каждой функций k -значной логики и при некоторых других значениях k . Каждую функцию k -значной логики можно представить полиномом, если и только если $k = p^h$, где p – простое число, $h \geq 1$ [218] (стр. 71). При таких значениях k на множестве E_k можно ввести двуместные операции $+$ и $\cdot$, относительно которых множество E_k образует поле $F_k = (E_k, +, \cdot)$. Полиномы, представляющие функции k -значной логики, являются полиномами относительно операций поля F_k . При этом каждая функция k -значной логики задается однозначно таким полиномом, в котором степень каждой переменной ограничена числом $(k - 1)$ [219] (стр. 39). Таким образом, при $k = p^h$, где p – простое число, $h \geq 1$ мы можем рассмотреть однозначное представление функции k -значной логики в виде

$$f(x_1, \dots, x_n) = \sum_{\alpha \in E_k^n} c_f(\alpha) X_\alpha,$$

где $c_f(\alpha) \in E_k$ – коэффициенты, и сложение и умножение – это соответствующие операции поля $F_k = (E_k, +, \cdot)$, сумма по пустому множеству индексов определяет пустой полином 0. Для функции $f \in P_k$ этот ее однозначный полином относительно операций поля F_k обозначим как $P_{F_k}(f)$. Перенесем все определения, касающиеся однозначных полиномов по модулю k для функций k -значной логики, на их однозначные полиномы относительно поля F_k . При этом в обозначениях добавим нижний индекс F_k .

Сначала мы докажем существование алгоритма с полиномиальной временной сложностью для распознавания принадлежности функции k -значной ло-

гики, представленной полиномом относительно операций поля $(E_k; +, \cdot)$, к предполным классам линейных функций. Отметим, что задачи распознавания нелинейности функций алгебры логики при их представлениях формулами, дизъюнктивными нормальными формами (ДНФ) или конъюнктивными нормальными формами (КНФ) является NP -трудными. Доказать NP -трудность задачи распознавания нелинейности функции двузначной логики, представленной КНФ, можно полиномиальным сведением к ней NP -полной задачи выполнимости конъюнктивных нормальных форм. Действительно, некоторая КНФ выполнима тогда и только тогда, когда нелинейна функция, полученная из нее умножением на выражение $t_1 \cdot t_2$, где t_1, t_2 – не присутствующие в записи этой КНФ переменные. Как следствие, NP -трудны задачи распознавания нелинейности функций, представленных ДНФ и формулами в общем случае.

Предполный класс линейных функций двузначной логики был определен Э. Постом [181, 182]. В k -значной логике часть предполных классов линейных функций была найдена С.В. Яблонским [139], окончательно все предполные классы линейных функций k -значной логики описал Ло Чжу-Кай [172].

Определим предполные классы линейных функций k -значной логики. Пусть на множестве E_k задана абелева группа $G = (E_k; \oplus_k)$ с нулем 0_k . Пусть $\ominus_k$ обозначает элемент группы G , обратный к элементу a ($a \in E_k$) (все алгебраические понятия и факты можно найти, например, в [204, 212]). Для простоты будем обозначать $\oplus_k$, $\ominus_k$ и 0_k как $\oplus$, $\ominus$ и 0 соответственно. Будем говорить, что функция k -значной логики $f(x_1, \dots, x_n)$ *линейна по отношению к группе G* , если верно тождество

$$f(x_1 \oplus y_1, \dots, x_n \oplus y_n) = f(x_1, \dots, x_n) \oplus f(y_1, \dots, y_n) \ominus f(0, \dots, 0).$$

Обозначим как $L_k(G)$ множество всех функций k -значной логики, линейных

по отношению к группе G .

Пусть теперь $k = p^h$, где p — простое число, $h \geq 1$, и в группе G каждый ненулевой элемент имеет порядок p . В этом случае к операции сложения $\oplus$ в группе G можно так добавить операцию умножения $\otimes$, что множество E_k относительно них образует поле $F = (E_k; \oplus, \otimes)$. Верны следующие утверждения [219] (стр. 36–42).

1. Множество $L_k(G)$ — предполный класс тогда и только тогда, когда $k = p^h$, где p — простое число, $h \geq 1$, и $G = (E_k; \oplus)$ — абелева группа над множеством E_k , каждый ненулевой элемент которой имеет порядок p .
2. Пусть $k = p^h$, где p — простое число, $h \geq 1$, $F = (E_k, \oplus_k, \otimes_k)$ — поле над множеством E_k . Функция k -значной логики $f(x_1, \dots, x_n)$ линейна по отношению к группе $G = (E_k; \oplus)$, если и только если она представима в виде

$$f(x_1, \dots, x_n) = a_0 \oplus \bigoplus_{i=1}^n \bigoplus_{j=0}^{h-1} a_{ij} \otimes x_i^{p^j}, \quad (15)$$

где $a_0, a_{ij} \in E_k$, $i = 1, \dots, n$, $j = 0, \dots, h - 1$.

В утверждении 1 определяются все возможные предполные классы линейных функций k -значной логики. В утверждении 2 описывается явный вид полиномов (относительно операций поля F $\oplus$ и $\otimes$) функций k -значной логики, принадлежащих определенному предполному классу линейных функций.

Обратим внимание на то, что и требование представления функции k -значной логики полиномом, и требование существования предполных классов линейных функций накладывают одно и то же ограничение на значность логики, а именно $k = p^h$, где p — простое число, $h \geq 1$. Поэтому везде в дальнейшем при исследовании алгоритмической сложности задачи распознавания принадлежности функции k -значной логики к предполным классам

линейных функций полагаем, что число k имеет только такие значения.

Задача состоит в следующем. Пусть $k = p^h$, где p – простое число, $h \geq 1$. Задана функция k -значной логики, представленная полиномом относительно операций поля $F_k = (E_k; +, \cdot)$. Требуется выяснить, с какой временной сложностью можно распознать, принадлежит ли она к предполному классу линейных функций, определенному заданной группой $G = (E_k; \oplus)$.

Заметим, что нами рассматриваются два различных поля над множеством E_k : первое поле $F = (E_k; \oplus, \otimes)$, через которое определяется предполный класс линейных функций, и второе поле $F_k = (E_k; +, \cdot)$, относительно операций которого записываются полиномами функции k -значной логики.

Но существует единственное с точностью до изоморфизма поле над множеством E_k из p^h элементов [212] (стр. 67), т.е. поля F и F_k изоморфны. Пусть $\varphi : E_k \rightarrow E_k$ – изоморфизм поля F на поле F_k , т.е. такое взаимно однозначное отображение, что для произвольных элементов a и b из E_k верно

$$\varphi(a \oplus b) = \varphi(a) + \varphi(b),$$

$$\varphi(a \otimes b) = \varphi(a) \cdot \varphi(b).$$

Пусть $f(x_1, \dots, x_n)$ – линейная по отношению к группе $G = (E_k; \oplus)$ функция. По выражению (15) она имеет вид

$$f(x_1, \dots, x_n) = a_0 \oplus \bigoplus_{i=1}^n \bigoplus_{j=0}^{h-1} a_{ij} \otimes x_i^{p^j}.$$

Рассмотрим функцию $\varphi(f(x_1, \dots, x_n))$:

$$\begin{aligned} \varphi(f(x_1, \dots, x_n)) &= \varphi(a_0 \oplus \bigoplus_{i=1}^n \bigoplus_{j=0}^{h-1} a_{ij} \otimes x_i^{p^j}) = \\ &= \varphi(a_0) + \sum_{i=1}^n \sum_{j=0}^{h-1} \varphi(a_{ij}) \cdot (\varphi(x_i))^{p^j}. \end{aligned} \quad (16)$$

Представление (15) описывает явный вид полинома относительно операций поля F функции, линейной по отношению к группе $G = (E_k; \oplus)$. Т.к. предполный класс линейных функций задан, т.е. известно поле F , а значит и отображение φ , известны также и полиномы относительно операций поля F_k , выражающие функции

$$\varphi(x), (\varphi(x))^p, \dots, (\varphi(x))^{p^{h-1}}.$$

Изложенные рассуждения позволяют сформулировать и доказать следующую теорему 3.1.

Теорема 3.1. [232] Пусть $k = p^h$, где p – простое число, $h \geq 1$, $F_k = (E_k; +, \cdot)$ и $F = (E_k; \oplus, \otimes)$ – поля над множеством E_k . Существует детерминированный алгоритм, который для каждого слова $\alpha(P_{F_k}(f))$ в алфавите $A = E_k \cup \{+\}$ с полиномиальной временной сложностью определяет, является функция $f(x_1, \dots, x_n)$ линейной по отношению к группе $G = (E_k; \oplus)$ или нет.

Доказательство. Опишем алгоритм, опираясь на который можно построить требуемую РАМ.

1. Пусть $g(x_1, \dots, x_n) = \varphi(f(x_1, \dots, x_n))$, где $\varphi : E_k \rightarrow E_k$ – изоморфизм поля F на поле F_k . Находим полином $P_{F_k}(g)$. Для нахождения полинома $P_{F_k}(g)$ требуется полиномиальная временная сложность относительно длины записи полинома $P_{F_k}(f)$.

2. Если полином $P_{F_k}(g)$ содержит хотя бы одно слагаемое с произведением различных переменных, то сразу ответ $f \notin L_G$ в соответствии с представлением (16). Выполнить эту проверку можно с полиномиальной временной сложностью относительно длины полинома $P_{F_k}(g)$.

3. Пусть теперь

$$g(x_1, \dots, x_n) = b_0 + \sum_{i=1}^n \sum_{j=1}^{p^h-1} b_{ij} \cdot x_i^j. \quad (17)$$

Если функция $f(x_1, \dots, x_n)$ линейна по отношению к группе G , то, ввиду однозначности представления функции k -значной логики полиномом (с ограничениями на степени переменных) относительно операций поля F_k , представления (16) и (17) совпадают. Приравняем соответствующие коэффициенты в представлениях (16) и (17). Получим систему линейных уравнений относительно неизвестных коэффициентов $\varphi(a_0), \varphi(a_{ij}), i = 1, \dots, n; j = 1, \dots, h-1$. Длина записи полученной системы уравнений полиномиальна относительно длины полинома $P_{F_k}(g)$.

Если решение полученной системы уравнений существует, то ответ $f \in L_G$. Более того, решив эту систему уравнений, мы получим представление функции $f(x_1, \dots, x_n)$ полиномом относительно операций поля F .

Если система несовместна, то ответ $f \notin L_G$ в соответствии с представлением (16).

Решить полученную систему линейных уравнений можно, например, методом Гаусса [210] (стр. 17) с полиномиальной временной сложностью относительно длины системы.

Теорема 3.1 доказана. □

Теперь обратимся к распознаванию принадлежности функции k -значной логики, представленной полиномом по модулю k , к предполным классам самодвойственных функций. Для построения полиномиальных алгоритмов распознавания принадлежности функций k -значной логики, заданных полиномами, к предполным классам самодвойственных функций мы применим следующий подход. Сначала с полиномиальной временной сложностью пре-

образуем полином функции k -значной логики таким образом, что исходная функция – самодвойственна в том и только в том случае, когда полученная функция инвариантна относительно некоторого набора преобразований. Мы доказываем, что если функция инвариантна, то длина ее полинома экспоненциальна относительно его ранга. Полиномиальный распознающий алгоритм строится, опираясь на это свойство полиномов инвариантных функций. Этот подход был применен для распознавания самодвойственности функций k -значных логик, заданных полиномами по модулю k , в работах [223, 225]. В работе [233] было рассмотрено более общее понятие инвариантности и рассматривалось представление функций k -значной логики полиномами относительно некоторого поля $F_k = (E_k; +, \cdot)$ при $k = p^h$, где p – простое число, $h \geq 1$. Сейчас мы рассмотрим этот общий случай.

Пусть $F_k = (E_k; +, \cdot)$ – поле из $k = p^h$ элементов, где p – простое число, $h \geq 1$, 0_{F_k} и 1_{F_k} соответственно его нулевой и единичный элементы. Как и ранее, для простоты эти элементы будем обозначать как 0 и 1.

Функции из P_k^1 будем называть *преобразованиями (множества E_k)*. Заметим, что в определении преобразования мы не требуем взаимной однозначности отображения, определяемого функцией из P_k^1 . Другими словами, рассматриваем в том числе и вырожденные преобразования множества E_k . Если же преобразование $s(x) \in P_k^1$ является взаимно однозначной функцией, то мы его также будем называть *перестановкой*.

Преобразование $s(x)$ назовем *связным*, если для произвольных элементов $a, b \in F$ найдутся такие числа $m_1 \geq 0$ и $m_2 \geq 0$, что $s^{m_1}(a) = s^{m_2}(b)$ (под записью $s^m(x)$ мы понимаем $\underbrace{s(\dots(s(x))\dots)}_m$, если $m \geq 1$, $s^0(x) = x$).

Функцию k -значной логики $f(x_1, \dots, x_n) \in P_k$ назовем *инвариантной относительно набора преобразований $s_1(x), \dots, s_n(x)$ из P_k^1* (или просто *инва-*

риантной, подразумевая при этом некоторый набор преобразований), если для всех возможных значений переменных $x_1, \dots, x_n$ верно равенство

$$f(s_1(x_1), \dots, s_n(x_n)) = f(x_1, \dots, x_n).$$

Каждому преобразованию $s(x)$ из P_k^1 поставим в соответствие ориентированный граф (в котором могут быть петли) $G(s)$ с множеством вершин E_k и множеством дуг $\{(a, s(a))\}$ для всех $a \in E_k$. Заметим, что граф $G(s)$ обладает тем свойством, что полустепень исхода каждой его вершины в точности равна единице (понятия, относящиеся к графам, можно найти, например, в [207]). Если преобразование $s(x)$ связно, то граф $G(s)$ связан. Из перечисленных двух свойств графа $G(s)$ можно доказать, что в нем содержится в точности один ориентированный цикл. Число вершин в этом единственном цикле графа связного преобразования $s(x)$ назовем *рангом* преобразования $s(x)$. Если ранг преобразования $s(x)$ равен k (т.е. все его элементы – циклические), то преобразование $s(x)$ называем *перестановкой, образующей цикл длины k* . *Рангом* набора связных преобразований $s_1(x), \dots, s_n(x)$ назовем наибольший ранг составляющих его преобразований.

Для доказательства основных теорем о свойствах полиномов инвариантных функций нам понадобятся вспомогательные леммы. Сначала докажем несколько лемм, в которых описываются свойства функций k -значной логики, инвариантных относительно связных преобразований.

Пусть $s(x)$ – связное преобразование. Назовем элементы a и b из F *эквивалентными* (относительно преобразования $s(x)$) и обозначим $a \sim_s b$, если найдется такое число $m \geq 0$, что $s^m(a) = s^m(b)$. Другими словами, если $a \sim_s b$, то в графе $G(s)$ найдутся пути одинаковой длины соответственно из вершин a и b к некоторой вершине. Введенное отношение является отношением эквивалентности на множестве E_k .

В самом деле, его рефлексивность и симметричность очевидны. Докажем его транзитивность. Пусть для элементов a, b и c из E_k верно, что $s^{m_1}(a) = s^{m_1}(b)$ и $s^{m_2}(b) = s^{m_2}(c)$, где m_1 и m_2 — некоторые числа. Тогда если m — большее из чисел m_1, m_2 , то верно равенство $s^m(a) = s^m(c)$. Таким образом, каждое связное преобразование $s(x)$ введенным отношением эквивалентности разбивает множество E_k на множество классов эквивалентности $E_k/\sim_s$.

Лемма 3.1. [233] Пусть $k \geq 2$. Если функция $f(x_1, \dots, x_n) \in P_k$ инвариантна относительно набора связных преобразований $s_1(x), \dots, s_n(x)$, и $a, b \in E_k$ такие элементы, что $a \sim_{s_i} b$, то

$$f_1(x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_n) = f_2(x_1, \dots, x_{i-1}, b, x_{i+1}, \dots, x_n).$$

Доказательство. Положим для определенности, что $i = 1$. Т.к. $a \sim_{s_1} b$, найдется такое число $m \geq 0$, что $s_1^m(a) = s_1^m(b) = c \in E_k$.

Функция $f(x_1, \dots, x_n) \in P_k$ инвариантна относительно набора преобразований $s_1(x), \dots, s_n(x)$, поэтому

$$f(s_1(x_1), \dots, s_n(x_n)) = f(x_1, \dots, x_n),$$

откуда

$$f(s_1^m(x_1), \dots, s_n^m(x_n)) = f(x_1, \dots, x_n).$$

Положим $x_1 = a$ и $x_1 = b$, получим:

$$f(c, s_2^m(x_2), \dots, s_n^m(x_n)) = f(a, x_2, \dots, x_n)$$

и

$$f(c, s_2^m(x_2), \dots, s_n^m(x_n)) = f(b, x_2, \dots, x_n).$$

Отсюда следует утверждение леммы 3.1. □

Преобразования $s_1(x)$ и $s_2(x)$ назовем *эквивалентными*, если для любых элементов a, b из E_k верны условия:

- 1) $a \sim_{s_1} b$ тогда и только тогда, когда $a \sim_{s_2} b$;
- 2) $s_1(a) \sim_{s_1} s_2(a)$ (а в силу условия 1 и $s_1(a) \sim_{s_2} s_2(a)$).

Заметим, что если преобразования $s_1(x)$ и $s_2(x)$ эквивалентны, то из того, что $a \sim_{s_1} b$ (а значит, и $a \sim_{s_2} b$) следует, что $s_1(a) \sim_{s_1} s_2(b)$ (и $s_1(a) \sim_{s_2} s_2(b)$). Действительно,

$$a \sim_{s_1} b \text{ и } a \sim_{s_2} b,$$

откуда

$$s_1(a) \sim_{s_1} s_1(b) \text{ и } s_2(a) \sim_{s_2} s_2(b).$$

По условию 1 определения эквивалентных преобразований верно

$$s_2(a) \sim_{s_1} s_2(b). \quad (18)$$

По условию 2 определения эквивалентных преобразований верно

$$s_1(a) \sim_{s_1} s_2(a). \quad (19)$$

По транзитивности отношения $\sim_{s_1}$ из свойств (19) и (18) следует, что $s_1(a) \sim_{s_1} s_2(b)$.

Лемма 3.2. [233] Пусть $k \geq 2$. Если функция $f(x_1, \dots, x_n) \in P_k$ инвариантна относительно набора связанных преобразований $s_1(x), \dots, s_n(x)$ и для некоторого i ($1 \leq i \leq n$) преобразования $s_i(x)$ и $s'_i(x)$ эквивалентны, то функция $f(x_1, \dots, x_n)$ инвариантна относительно набора преобразований $s_1(x), \dots, s_{i-1}, s'_i(x), s_{i+1}, \dots, s_n(x)$.

Доказательство. Положим для определенности, что $i = 1$.

Т.к. функция $f(x_1, \dots, x_n)$ инвариантна относительно набора преобразований $s_1(x), \dots, s_n(x)$, верно равенство

$$f(s_1(x_1), s_2(x_2), \dots, s_n(x_n)) = f(x_1, x_2, \dots, x_n). \quad (20)$$

Рассмотрим $f(s'_1(x_1), s_2(x_2), \dots, s_n(x_n))$.

Преобразования $s_1(x)$ и $s'_1(x)$ эквивалентны, поэтому по свойству 2 определения эквивалентных преобразований верно, что $s_1(x_1) \sim_{s_1} s'_1(x_1)$. Тогда по лемме 3.1 верно, что

$$f(s_1(x_1), s_2(x_2), \dots, s_n(x_n)) = f(s'_1(x_1), s_2(x_2), \dots, s_n(x_n)). \quad (21)$$

Из равенств (20) и (21) следует, что

$$f(s'_1(x_1), s_2(x_2), \dots, s_n(x_n)) = f(x_1, x_2, \dots, x_n).$$

Т. е. функция $f(x_1, \dots, x_n)$ инвариантна относительно набора преобразований $s'_1(x), s_2(x), \dots, s_n(x)$.

Лемма 3.2 доказана. □

Пусть $s(x)$ – связное преобразование. Каждый элемент единственного цикла графа $G(s)$ назовем *циклическим* элементом преобразования $s(x)$. Отметим некоторые свойства циклических элементов преобразований. Если $a \in E_k$ – циклический элемент связного преобразования $s(x) \in P_k^1$ ранга q , то

- 1) для произвольного элемента $b \in E_k$ найдется такое число $m \geq 0$, что $s^m(b) = a$;
- 2) $s^q(a) = a$;
- 3) для произвольного числа $m \geq 0$ элемент $s^m(a)$ также является циклическим.

Перечисленные свойства циклических элементов следуют из определения циклического элемента.

Зафиксируем некоторый циклический элемент $a \in E_k$ связного преобразования $s(x) \in P_k^1$. Тогда для произвольного числа $m > 0$ найдется такой единственный циклический элемент $b \in E_k$, что $s^m(b) = a$. Положим по определению, что $s^{-m}(a) = b$.

Лемма 3.3. [233] Пусть $k \geq 2$. Если функция $f(x_1, \dots, x_n) \in P_k$ инвариантна относительно набора связных преобразований $s_1(x), \dots, s_n(x)$, то для произвольного i ($1 \leq i \leq n$) найдется такое связное преобразование $s'_i(x)$ с нулевым циклическим элементом, эквивалентное преобразованию $s_i(x)$, что функция $f(x_1, \dots, x_n)$ инвариантна относительно набора преобразований $s_1(x), \dots, s_{i-1}(x), s'_i(x), s_{i+1}(x), \dots, s_n(x)$.

Доказательство. 1. Рассмотрим преобразование $s_i(x)$ ($1 \leq i \leq n$).

Возможны две ситуации: либо 0 является циклическим элементом $s_i(x)$, либо нет. Если верна первая из них, то пусть $s'_i(x) = s_i(x)$.

Иначе, пусть $a \in E_k$ – некоторый циклический элемент преобразования $s_i(x)$.

Т.к. $s_i(x)$ – связное преобразование, найдутся такие числа $m_{i_1} \geq 0$ и $m_{i_2} \geq 0$, что $s_i^{m_{i_1}}(0) = s_i^{m_{i_2}}(a)$.

Положим, что $m_{i_3} = m_{i_2} - m_{i_1}$. Тогда циклический элемент $s_i^{m_{i_3}}(a) \in E_k$ эквивалентен элементу 0. Таким образом, мы обнаружили циклический элемент (обозначим его как c), эквивалентный элементу 0.

Построим преобразование $s'_i(x)$ по следующим правилам:

а) $s'_i(0) = s_i(c)$;

б) $s'_i(c) = s_i(0)$;

в) если $s_i(x) = 0$, то $s'_i(x) = c$;

г) если $s_i(x) = c$, то $s'_i(x) = 0$;

д) во всех оставшихся возможных случаях преобразования $s'_i(x)$ и $s_i(x)$ совпадают.

2. Докажем, что преобразования $s'_i(x)$ и $s_i(x)$ эквивалентны. Другими словами, нам надо доказать верность двух условий определения эквивалентных преобразований. Содержательно их выполнение следует из того, что т.к. $0 \sim_{s_i} c$, классы эквивалентности, на которые разбивают множество E_k пре-

образования s_i и s'_i , совпадают и порядок следования их друг за другом при применении преобразований s_i и s'_i одинаков. Теперь более подробно.

1) Если $a \sim_{s_i} b$, то это верно тогда и только тогда, когда $a \sim_{s'_i} b$, т.к. $0 \sim_{s_i} c$.

2) Пусть $a \in E_k$. Тогда

2а) если $a = 0$, то $s'_i(0) = s_i(c)$, и $s_i(0) \sim_{s_i} s'_i(0)$ и $s_i(0) \sim_{s'_i} s'_i(0)$, т.к. $0 \sim_{s_i} c$; аналогично, если $a = c$;

2б) если $s_i(a) = 0$, то $s'_i(a) = c$, и $0 \sim_{s_i} c$ и $0 \sim_{s'_i} c$; аналогично, если $s_i(a) = c$;

2в) если $s_i(a) \neq 0$ и $s_i(a) \neq c$, то $s_i(a) = s'_i(a)$, и значит $s_i(a) \sim_{s_i} s'_i(a)$ и $s_i(a) \sim_{s'_i} s'_i(a)$.

Таким образом, преобразования $s_i(x)$ и $s'_i(x)$ эквивалентны, и один из циклических элементов преобразования $s'_i(x)$ есть 0.

3. По лемме 3.2 функция $f(x_1, \dots, x_n)$ инвариантна относительно набора преобразований $s_1(x), \dots, s_{i-1}(x), s'_i(x), s_{i+1}(x), \dots, s_n(x)$.

Лемма 3.3 доказана. □

Леммы 3.1, 3.2 и 3.3 описывают функциональные свойства функций k -значной логики, инвариантных относительно связных преобразований. В следующей лемме 3.4 представлено одно структурное свойство их полиномов относительно операций поля F_k .

Напомним, что семейство всех типов слагаемых полинома $P_{F_k}(f)$ обозначается как $T(P_{F_k}(f))$. Обозначим как $T^{(l)}(P_{F_k}(f))$ множество пересечений всех возможных l элементов (не обязательно различных) из семейства $T(P_{F_k}(f))$.

Лемма 3.4. [233] Пусть $k = p^h$, где p – простое число, $h \geq 1$, и $F_k = (E_k; +, \cdot)$ – поле. Если функция $f(x_1, \dots, x_n) \in P_k$, не равна нулю и инвариантна относительно набора связных преобразований $s_1(x), \dots, s_n(x)$ ранга q , то $\emptyset \in T^{(q)}(P_{F_k}(f))$.

Доказательство. По лемме 3.3 мы можем полагать, что элемент 0 является циклическим для каждого из преобразований $s_i(x)$.

1. Если функция f равна константе $a \in E_k$, $a \neq 0$, то $P_{F_k}(f) = a$, и $\emptyset \in T^{(q)}(P_{F_k}(f))$.

2. Пусть теперь функция f не равна константе. Заметим, что функция $f(x_1, \dots, x_n)$ инвариантна относительно некоторого набора преобразований тогда и только тогда, когда относительно этого же набора преобразований инвариантна функция $f(x_1, \dots, x_n) + a$ для произвольного $a \in E_k$. Поэтому, мы можем считать, что $f(0, \dots, 0) = 0$. Т.к. функция $f(x_1, \dots, x_n)$ не равна 0, найдется такой ненулевой набор $(a_1, \dots, a_n) \in E_k^n$, что $f(a_1, \dots, a_n) \neq 0$. Пусть $m_1, \dots, m_n \geq 0$ – такие числа, что $s_i^{m_i}(a_i) \in E_k$ являются циклическими элементами, $i = 1, \dots, n$. Пусть m – наибольшее из чисел $m_1, \dots, m_n$. Положим, что $b_i = s^m(a_i) \in E_k$. По замечанию к определению циклического элемента $b_1, \dots, b_n$ являются циклическими элементами.

3. Т.к. функция $f(x_1, \dots, x_n)$ инвариантна относительно преобразований $s_1(x), \dots, s_n(x)$, то

$$f(b_1, \dots, b_n) = f(a_1, \dots, a_n) \neq 0.$$

Построим множества индексов $I_j \subseteq \{1, \dots, n\}$ по следующему правилу: $i \in I_j$, если и только если $s_i^j(b_i) = 0$, $i = 1, \dots, n$. Т.к. ранг набора преобразований $s_1(x), \dots, s_n(x)$ равен q , число множеств I_j не больше q . Заметим также, что множества I_j попарно не пересекаются, а их объединение есть множество $\{1, \dots, n\}$.

4. Рассмотрим непустое множество I_j .

$$f(s_1^j(b_1), \dots, s_n^j(b_n)) = f(b_1, \dots, b_n) \neq 0.$$

Следовательно, в полиноме $P_{F_k}(f)$ найдется моном, не содержащий переменные с индексами из I_j . Обозначим его как $X^{(j)}$.

5. Пересечение типов всех мономов $X^{(j)}$, построенных таким образом, есть $\emptyset$. Т.к. их число не больше, чем q , верно, что $\emptyset \in T^{(q)}(P_{F_k}(f))$.

Лемма 3.4 доказана. □

Каждому связному преобразованию $s(x)$ с нулевым циклическим элементом сопоставим функцию $t_s(x)$, построенную по правилу: для каждого элемента $a \in E_k$ верно $t_s(a) = m$, если m – наименьшее из всех таких чисел, что $s^m(a) = 0$, $m \geq 0$. Назовем функцию $t_s(x)$ *функцией расстояний преобразования* $s(x)$. По определению функции расстояний $t_s(x)$ связного преобразования $s(x)$ с нулевым циклическим элементом верно, что $s^{t_s(x)}(x) = 0$ и $s^{t_s(0)}(x) = s^0(x) = x$. Имеет место также следующее равенство: если $s_1(x)$ – связное преобразование с нулевым циклическим элементом, $t_{s_1}(x)$ – его функция расстояний, и $s_2(x)$ – связное преобразование, то $s_2^{t_{s_1}(s_1(x))}(s_2(y)) = s_2^{t_{s_1}(x)}(y)$. Действительно, $s_2^{t_{s_1}(s_1(x))}(s_2(y)) = s_2^{t_{s_1}(s_1(x))+1}(y) = s_2^{t_{s_1}(x)}(y)$.

Лемма 3.5. [233] Пусть $k \geq 2$. Функция $f(x_1, \dots, x_n) \in P_k$ инвариантна относительно набора связных преобразований $s_1(x), \dots, s_n(x)$ с нулевыми циклическими элементами тогда и только тогда, когда

$$f(x_1, \dots, x_n) = h(s_1^{t_{s_i}(x_i)}(x_1), \dots, s_{i-1}^{t_{s_i}(x_i)}(x_{i-1}), s_{i+1}^{t_{s_i}(x_i)}(x_{i+1}), \dots, s_n^{t_{s_i}(x_i)}(x_n)),$$

где $h(y_1, \dots, y_{n-1})$ – некоторая функция из P_k , и $t_{s_i}(x)$ – функция расстояний преобразования $s_i(x)$, $1 \leq i \leq n$.

Доказательство. Положим для определенности, что $i = 1$.

1. Докажем необходимость. Пусть функция $f(x_1, \dots, x_n)$ инвариантна относительно набора связных преобразования $s_1(x), \dots, s_n(x)$ с нулевыми циклическими элементами. Пусть $t_1(x)$ – функция расстояний преобразования $s_1(x)$.

Определим функцию $h(y_1, \dots, y_{n-1})$ как $f(0, y_1, \dots, y_{n-1})$. Тогда верно

$$\begin{aligned} h(s_2^{t_1(x_1)}(x_2), \dots, s_n^{t_1(x_1)}(x_n)) &= f(0, s_2^{t_1(x_1)}(x_2), \dots, s_n^{t_1(x_1)}(x_n)) = \\ &= f(s_1^{t_1(x_1)}(x_1), s_2^{t_1(x_1)}(x_2), \dots, s_n^{t_1(x_1)}(x_n)) = f(x_1, \dots, x_n). \end{aligned}$$

2. Докажем достаточность.

Пусть для некоторой функции $h(y_1, \dots, y_{n-1})$ из P_k верно равенство

$$f(x_1, \dots, x_n) = h(s_2^{t_1(x_1)}(x_2), \dots, s_n^{t_1(x_1)}(x_n)).$$

Тогда можно заключить, что

$$\begin{aligned} f(s_1(x_1), s_2(x_2), \dots, s_n(x_n)) &= h(s_2^{t_1(s_1(x_1))}(s_2(x_2)), \dots, s_n^{t_1(s_1(x_1))}(s_n(x_n))) = \\ &= h(s_2^{t_1(x_1)}(x_2), \dots, s_n^{t_1(x_1)}(x_n)) = f(x_1, \dots, x_n). \end{aligned}$$

Т.е. функция $f(x_1, \dots, x_n)$ инвариантна относительно набора преобразований $s_1(x_1), \dots, s_n(x_n)$.

Лемма 3.5 доказана. □

Лемма 3.5 представляет собой критерий инвариантности функций k -значной логики относительно связных преобразований с нулевыми циклическими элементами.

При $k = p^h$, где p – простое число, $h \geq 1$, для функции k -значной логики $f(x_1, \dots, x_n)$, инвариантной относительно набора связных преобразований $s_1(x), \dots, s_n(x)$ с нулевыми циклическими элементами, введем функционал $f_{x_i}^{(x_j)}$, называемый *производной по переменной x_i через переменную x_j* , причем $i \neq j$.

Не ограничивая общности рассуждений, положим, что $i = n$ и $j = 1$.

По лемме 3.5 верно $f(x_1, \dots, x_n) = h(s_2^{t_{s_1}(x_1)}(x_2), \dots, s_n^{t_{s_1}(x_1)}(x_n))$, причем $h(x_2, \dots, x_n) = f(0, x_2, \dots, x_n)$.

Пусть $g(x_2, \dots, x_n) = h'_{x_n}(x_2, \dots, x_n)$, т.е. мы рассматриваем производную полинома (многочлена над полем F_k) $P_{F_k}(h)$ по переменной x_n , которую можно ввести без применения понятия непрерывности (см., например, [212], стр. 43).

Тогда $f_{x_n}^{(x_1)} = g(s_2^{t_{s_1}(x_1)}(x_2), \dots, s_n^{t_{s_1}(x_1)}(x_n))$.

Из последнего равенства сразу следует лемма 3.6 (по лемме 3.5).

Лемма 3.6. [233] Пусть $k = p^h$, где p – простое число, $h \geq 1$, $F_k = (E_k; +, \cdot)$ – поле. Если функция $f(x_1, \dots, x_n) \in P_k$ инвариантна относительно набора связных преобразований $s_1(x), \dots, s_n(x)$ с нулевыми циклическими элементами, то функция $f_{x_i}^{(x_j)}$ также инвариантна относительно набора преобразований $s_1(x), \dots, s_n(x)$, $1 \leq i, j \leq n$, $i \neq j$.

Лемма 3.7. [233] Пусть $k = p^h$, где p – простое число, $h \geq 1$, $F_k = (E_k; +, \cdot)$ – поле. Пусть функция $f(x_1, \dots, x_n) \in P_k$ инвариантна относительно набора связных преобразований $s_1(x), \dots, s_n(x)$ с нулевыми циклическими элементами, а X – некоторый моном, причем $j \notin t(X)$, и $i \neq j$, $1 \leq i, j \leq n$. Если моном X является слагаемым в полиноме $P_{F_k}(f_{x_i}^{(x_j)})$, то моном $x_i \cdot X$ является слагаемым полинома $P_{F_k}(f)$.

Доказательство. Положим для определенности, что $j = 1$.

Т.к. функция $f(x_1, \dots, x_n)$ инвариантна относительно набора связных преобразований $s_1(x), \dots, s_n(x)$ с нулевыми циклическими элементами, по лемме 3.5 верно, что

$$f(x_1, \dots, x_n) = h(s_2^{t_{s_1}(x_1)}(x_2), \dots, s_n^{t_{s_1}(x_1)}(x_n)).$$

Т.к.

$$s_2^{t_{s_1}(0)}(x_2) = x_2, \dots, s_n^{t_{s_1}(0)}(x_n) = x_n,$$

верно, что $h(x_2, \dots, x_n) = f(0, x_2, \dots, x_n)$. Т.е. можно записать, что

$$f(x_1, \dots, x_n) = x_1 \cdot g(x_1, \dots, x_n) + h(x_2, \dots, x_n),$$

где $g(x_1, \dots, x_n)$ – некоторая функция из P_k . Так же можно записать, что

$$f_{x_i}^{(x_1)} = x_1 \cdot g_1(x_1, \dots, x_n) + h'_{x_i}(x_2, \dots, x_n),$$

где $g_1(x_1, \dots, x_n)$ – тоже некоторая функция из P_k .

Т.к. переменная x_1 не входит в качестве сомножителя в моном X , полином $P_{F_k}(h'_{x_i})$ содержит моном X как слагаемое. Следовательно, по правилам производной полином $P_{F_k}(h)$ содержит моном $x_i \cdot X$ как слагаемое. Значит, моном $x_i \cdot X$ является слагаемым полинома $P_{F_k}(f)$.

Лемма 3.7 доказана. □

Теперь докажем теоремы 3.2 и 3.3 о свойствах полиномов инвариантных функций, которые будем применять при построении распознающих полиномиальных алгоритмов. Теорема 3.3 является следствием теоремы 3.2.

Теорема 3.2. [233] Пусть $k = p^h$, где p – простое число, $h \geq 1$, $F_k = (E_k; +, \cdot)$ – поле. Если функция $f(x_1, \dots, x_n) \in P_k$, не равна нулю и инвариантна относительно набора связных преобразований $s_1(x), \dots, s_n(x)$ ранга q , то каждый подтип произвольного типа из множества $T(P_{F_k}(f))$ содержится в множестве $T^{(q)}(P_{F_k}(f))$.

Доказательство. По лемме 3.3 мы можем полагать, что элемент 0 является циклическим для каждого из преобразований $s_i(x)$, $i = 1, \dots, n$.

Рассмотрим некоторое слагаемое X полинома $P_{F_k}(f)$. Пусть $|t(X)| = r$, где $1 \leq r \leq n$. Подтип $t = t(X)$ содержится в $T^{(q)}_{F_k}(f)$.

1. Пусть $r = n$. Докажем, что если в полиноме $P_{F_k}(f)$ содержится слагаемое X ранга n , то в полиноме $P_{F_k}(f)$ также содержатся слагаемые всех возможных типов мощности $(n - 1)$. По лемме 3.5

$$f(x_1, \dots, x_n) = h(s_2^{t_{s_1}(x_1)}(x_2), \dots, s_n^{t_{s_1}(x_1)}(x_n)),$$

где $h(x_2, \dots, x_n) = f(0, x_2, \dots, x_n)$. Отсюда

$$f(x_1, \dots, x_n) = x_1 \cdot g(x_1, \dots, x_n) + h(x_2, \dots, x_n)$$

для некоторой функции $g(x_1, \dots, x_n) \in P_k$. Если полином $P_{F_k}(h)$ не содержит слагаемое типа $\{2, \dots, n\}$, то полином $P_{F_k}(f)$ не может содержать слагаемое X . Это следует из того, что

$$f(x_1, \dots, x_n) = h(\varphi_2(x_1, x_2), \dots, \varphi_n(x_1, x_n)),$$

где $\varphi_i(x_1, x_i) = s_i^{t_{s_1}(x_1)}(x_i)$, $i = 2, \dots, n$. Аналогично, для всех типов $\{1, \dots, i-1, i+1, \dots, n\}$, $i = 2, \dots, n$.

2. Пусть $r \leq n - 1$. Рассмотрим подтип $t = \{i_1, \dots, i_{r_1}\}$, $t \subseteq t(X)$, где $1 \leq r_1 < r$. Т.к. $r < n$, найдется некоторый номер переменной, не входящий в тип $t(X)$. Не ограничивая общности рассуждений, обозначим его как $(r+1)$.

Рассмотрим функцию

$$g(x_1, \dots, x_n) = f_{x_{i_1} \dots x_{i_{r_1}}}^{(x_{r+1}) \dots (x_{r+1})}(x_1, \dots, x_n).$$

Функция $g(x_1, \dots, x_n)$ не равна нулю, и по лемме 3.6 инвариантна относительно набора связных преобразований $s_1(x), \dots, s_n(x)$.

По лемме 3.4 найдутся слагаемые $X^{(1)}, \dots, X^{(q)}$ в полиноме $P_{F_k}(g)$, пересечение типов которых есть $\emptyset$.

По лемме 3.7 слагаемые

$$x_{i_1} \cdot \dots \cdot x_{i_r} \cdot X^{(1)}, \dots, x_{i_1} \cdot \dots \cdot x_{i_r} \cdot X^{(q)}$$

содержатся в полиноме $P_{F_k}(f)$. Пересечение их типов есть тип t .

2. Подтип t , равный $\emptyset$, типа $t(X)$ содержится в множестве $T^{(q)}(P_{F_k}(f))$ согласно лемме 3.4.

Теорема 3.2 доказана. □

Мы доказываем теорему 3.3, обобщающую результаты из [223, 225].

Теорема 3.3. [233] Пусть $k = p^h$, где p – простое число, $h \geq 1$, $F_k = (E_k; +, \cdot)$ – поле. Если функция $f(x_1, \dots, x_n) \in P_k$, не равна нулю и инвариантна относительно набора связных преобразований $s_1(x), \dots, s_n(x)$ ранга

q , то для ранга $r = r(P_{F_k}(f))$ и веса $w = w(P_{F_k}(f))$ полинома $P_{F_k}(f)$ функции f верно неравенство $w^q \geq 2^r$.

Доказательство. Т.к. ранг полинома $P_{F_k}(f)$ равен r , в этом полиноме найдется слагаемое X вида $x_{i_1}^{m_1} \cdot \dots \cdot x_{i_r}^{m_r}$. Всего есть 2^r подтипов типа слагаемого X .

В теореме 3.2, в частности, утверждается, что каждый подтип типа слагаемого X содержится в множестве $T^{(q)}(P_{F_k}(f))$.

Мощность множества $T^{(q)}(P_{F_k}(f))$ не более w^q . Следовательно, $w^q \geq 2^r$.

Теорема 3.3 доказана. □

Полученные свойства полиномов инвариантных функций обеспечивают существование полиномиального алгоритма для распознавания инвариантности относительно набора связных преобразований для произвольной функции k -значной логики $f(x_1, \dots, x_n)$, заданной полиномом относительно операций поля $F_k = (E_k; +, \cdot)$. В самом деле, сначала нужно проверить выполнение неравенства из теоремы 3.3. В случае его невыполнения, сразу получаем, что функция f не инвариантна. В случае выполнения этого утверждения, проверяем инвариантность функции f по определению. А именно, подставляем в полином $P_{F_k}(f)$ вместо каждой переменной x_i полином $P_{F_k}(s_i(x_i))$, выполняем возведение в степени, перемножение скобок и приведение подобных слагаемых и сравниваем полученный полином с полиномом $P_{F_k}(f)$. Если имеет место совпадение полиномов, то функций f – инвариантна, если нет, то функция f – не инвариантна. Временная сложность этого алгоритма полиномиальна, т.к. в силу выполнения неравенства из теоремы 3.3 длина полинома $P_{F_k}(f)$ экспоненциальна относительно его ранга.

Опираясь на свойства полиномов инвариантных функций, мы доказываем, что если k – простое число, то задача распознавания принадлежности

функции k -значной логики, заданной полиномом по модулю k , к предполным классам самодвойственных функций является полиномиальной.

Отметим, что задачи распознавания несамодвойственности функций алгебры логики при их представлениях формулами, ДНФ или КНФ являются NP -трудными. Доказать NP -трудность задачи распознавания несамодвойственности функции двузначной логики, представленной КНФ, можно полиномиальным сведением к ней NP -полной задачи выполнимости конъюнктивных нормальных форм. Действительно, некоторая КНФ выполнима тогда и только тогда, когда несамодвойственна функция, полученная из нее добавлением в каждую скобку через дизъюнкцию не присутствующей в ее записи переменной t . Как следствие, NP -трудны задачи распознавания несамодвойственности функций, представленных ДНФ и формулами в общем случае.

Определим предполные классы самодвойственных функций. Предполный класс самодвойственных функций двузначной логики был определен Э. Постом [181, 182]. В k -значной логике при $k \geq 3$ предполные классы самодвойственных функций были найдены С.В. Яблонским [139].

Пусть функция $s(x) \in P_k^1$ является перестановкой множества элементов E_k . Функция k -значной логики $f(x_1, \dots, x_n)$ самодвойственна относительно перестановки $s(x)$, если верно тождество

$$f(s(x_1), \dots, s(x_n)) = s(f(x_1, \dots, x_n)).$$

Обозначим как $S_k(s)$ множество всех функций k -значной логики, самодвойственных относительно перестановки $s(x)$. Множество $S_k(s)$ – предполный класс тогда и только тогда, когда перестановка $s(x)$ раскладывается в произведение циклов одинаковой простой длины [139]. Мы рассмотрим случай простого k . В этом случае множество $S_k(s)$ – предполный класс тогда и только тогда, когда перестановка $s(x)$ образует цикл длины k .

Сначала докажем несколько вспомогательных утверждений.

Лемма 3.8. [223, 225] Пусть k – простое число, $s(x) \in P_k^1$. Функция $s(x)$ является перестановкой, образующей цикл длины k , тогда и только тогда, когда $s(x) = q^{-1}(q(x) + 1)$ для некоторой перестановки $q(x) \in P_k^1$, где $q^{-1}(x)$ – функция, обратная к функции $q(x)$.

Доказательство. 1. Докажем необходимость. Пусть перестановка $s(x) \in P_k^1$ образует цикл длины k . Определим $q(x) \in P_k^1$ следующим образом. Пусть $a \in E_k$. Положим, что $q(a) = 0$, $q(b) = t$, если $b = s^t(a)$, $b \in E_k$, $b \neq a$, $t = 1, \dots, k-1$. Т.к. перестановка $s(x)$ образует цикл длины k , получаем, что $q(x)$ – перестановка. Кроме того,

$$\begin{aligned} q^{-1}(q(a) + 1) &= q^{-1}(1) = s(a), \\ q^{-1}(q(b) + 1) &= q^{-1}(t + 1) = s(b). \end{aligned}$$

2. Докажем достаточность. Пусть $q(x) \in P_k^1$ – перестановка, и $s(x) = q^{-1}(q(x) + 1)$. Рассмотрим $a \in E_k$. Тогда

$$\begin{aligned} a &= q^{-1}(q(a)), \\ s(a) &= q^{-1}(q(a) + 1), \\ s^2(a) &= q^{-1}(q(q^{-1}(q(a) + 1)) + 1) = q^{-1}(q(a) + 2), \\ s^t(a) &= q^{-1}(q(a) + t), \quad t = 1, \dots, k-1, \\ s^k(a) &= q^{-1}(q(a) + k) = a. \end{aligned}$$

Функция $q(x)$ – перестановка, поэтому элементы $a, s(a), s^2(a), \dots, s^{k-1}(a)$ различны. Т.е. $s(x)$ – перестановка, образующая цикл длины k .

Лемма 3.8 доказана. □

Теорема 3.4. [223, 225] Пусть k – простое число, $s(x) \in P_k^1$ – перестановка, образующая цикл длины k . Функция k -значной логики $f(x_1, \dots, x_n)$ самодвойственна относительно перестановки $s(x)$ тогда и только тогда,

когда функция k -значной логики

$$g(x_1, \dots, x_n) = q(f(x_1, \dots, x_n)) + (k - 1) \cdot q(x_1)$$

инвариантна относительно преобразования $s(x)$ по каждой переменной, где $q(x) \in P_k^1$ такая перестановка, что $s(x) = q^{-1}(q(x) + 1)$.

Доказательство. 1. Докажем необходимость. Если $f(x_1, \dots, x_n) \in P_k$ самодвойственна относительно перестановки $s(x)$, то

$$\begin{aligned} g(s(x_1), \dots, s(x_n)) &= q(f(s(x_1), \dots, s(x_n))) + (k - 1) \cdot q(s(x_1)) = \\ &= q(s(f(x_1, \dots, x_n))) + (k - 1) \cdot q(s(x_1)) = \\ &= q(q^{-1}(q(f(x_1, \dots, x_n) + 1))) + (k - 1) \cdot q(s(x_1)) = \\ &= q(f(x_1, \dots, x_n) + 1 + (k - 1) \cdot q(q^{-1}(q(x_1) + 1))) = \\ &= q(f(x_1, \dots, x_n)) + 1 + (k - 1) \cdot (q(x_1) + 1) = \\ &= g(x_1, \dots, x_n). \end{aligned}$$

Следовательно, функция $g(x_1, \dots, x_n)$ инвариантна относительно преобразования $s(x)$ по каждой переменной.

2. Докажем достаточность. Если функция $g(x_1, \dots, x_n)$ инвариантна относительно преобразования $s(x)$ по каждой переменной, то

$$\begin{aligned} f(s(x_1), \dots, s(x_n)) &= q^{-1}(q(f(s(x_1), \dots, s(x_n))) + k \cdot q(s(x_1))) = \\ &= q^{-1}(g(s(x_1), \dots, s(x_n)) + q(s(x_1))) = \\ &= q^{-1}(g(x_1, \dots, x_n) + q(q^{-1}(q(x_1) + 1))) = \\ &= q^{-1}(g(x_1, \dots, x_n) + q(x_1) + 1) = \\ &= q^{-1}(q(f(x_1, \dots, x_n)) + (k - 1) \cdot q(x_1) + q(x_1) + 1) = \\ &= q^{-1}(q(f(x_1, \dots, x_n) + 1)) = s(f(x_1, \dots, x_n)). \end{aligned}$$

Следовательно, функция $f(x_1, \dots, x_n)$ самодвойственна относительно перестановки $s(x)$.

Теорема 3.4 доказана. □

Теперь докажем теорему 3.5 о существовании полиномиального алгоритма для распознавания принадлежности функции k -значной логики, заданной полиномом по модулю k , к предполному классу самодвойственных функций.

Теорема 3.5. [223, 225] Пусть k – простое число, $s(x) \in P_k^1$ – перестановка, образующая цикл длины k . Существует детерминированный алгоритм, который для каждого слова $\alpha(P(f))$ в алфавите $A = E_k \cup \{+\}$ с полиномиальной временной сложностью определяет, является функция k -значной логики $f(x_1, \dots, x_n) \in P_k$ самодвойственной относительно перестановки $s(x)$ или нет.

Доказательство. Опишем алгоритм, по которому можно построить требуемую РАМ. Пусть задана функция $f(x_1, \dots, x_n)$. Построим функцию

$$g(x_1, \dots, x_n) = q(f(x_1, \dots, x_n)) + (k - 1) \cdot q(x_1),$$

где $s(x) = q^{-1}(q(x) + 1)$ для некоторой перестановки $q(x) \in P_k^1$ (см. леммы 3.8 и 3.4). Полином $P(g)$ по полиному $P(f)$ можно построить с полиномиальной временной сложностью.

Теперь проверим выполнение неравенства $(l(g))^k \geq 2^{r(g)}$ (т.к. $l(g) \geq w(g)$). Если это неравенство не выполняется, то $f \notin S_k(s)$ по теореме 3.3 и лемме 3.4. Если же это неравенство выполняется, то проверим выполнение равенства

$$g(s(x_1), \dots, s(x_n)) = g(x_1, \dots, x_n).$$

Для этого в полином $P(g)$ подставим вместо каждой переменной x_i полином $P(s(x_i))$, выполним возведение в степени, перемножим скобки, приведем подобные слагаемые и сравним полученный полином с полиномом $P(g)$. Если равенство выполняется, то $f \in S_k(s)$, если равенство не выполняется, то $f \notin S_k(s)$ по определению инвариантной функции и лемме 3.4. При построении полинома функции $g(s(x_1), \dots, s(x_n))$ мы выполним полиномиальное число операций, т.к. самая трудоемкая часть здесь – это перемножение не

более $r(g)$ полиномов одной переменной не более $l(g)$ раз. Но с учетом выполненного неравенства мы затрачиваем здесь не более $l(g) \cdot k^{r(g)} = (l(g))^{k \log_2 k + 1}$ операций, т.е. полиномиальное число операций.

Правильность предложенного алгоритма следует из лемм 3.8, 3.4 и теоремы 3.3.

Теорема 3.5 доказана. □

Теперь обратимся к распознаванию принадлежности функции k -значной логики, представленной полиномом по модулю k , к предполным классам монотонных функций, функций, сохраняющих разбиение, и к предполным классам типа В. При построении полиномиальных распознающих алгоритмов мы применим следующий подход. Каждый из перечисленных предполных классов можно определить как класс функций, сохраняющих некоторое отношение. Мы покажем, что каждое из этих отношений является вполне рефлексивным и вполне транзитивным, и докажем, что существует полиномиальный алгоритм для распознавания принадлежности функции k -значной логики, заданной полиномом, к классу функций, сохраняющих вполне рефлексивное и вполне транзитивное отношение. Как следствие, получим полиномиальное распознавание принадлежности функции k -значной логики, заданной полиномом, к предполным классам монотонных функций, функций, сохраняющих разбиение, и к предполным классам типа В.

Пусть $R^{(h)} \subseteq E_k^h$ – некоторое h -местное отношение, $h \geq 2$. Будем говорить, что h наборов $\alpha^{(j)} = (a_1^{(j)}, \dots, a_n^{(j)}) \in E_k^n$, $j = 1, \dots, h$, находятся в отношении R , если верно $R(a_i^{(1)}, \dots, a_i^{(h)})$ для всех $i = 1, \dots, n$. Функция k -значной логики $f(x_1, \dots, x_n)$ сохраняет отношение R , если для любых h наборов $\alpha^{(j)} \in E_k^n$, $j = 1, \dots, h$, находящихся в отношении R , верно $R(f(\alpha^{(1)}), \dots, f(\alpha^{(h)}))$. Множество всех функций k -значной логики, сохраняя-

ющих отношение R , будем обозначать как $A_k(R)$.

Отношение $R^{(h)} \subseteq E_k^h$ называется *вполне рефлексивным*, если верно $R(a_1, \dots, a_h)$ для произвольных элементов $a_1, \dots, a_h \in E_k$, среди которых хотя бы два элемента равны. Отношение $R^{(h)} \subseteq E_k^h$ называется *вполне симметричным*, если из справедливости $R(a_1, \dots, a_h)$ следует справедливость $R(a_{j_1}, \dots, a_{j_h})$, где $j_1, \dots, j_h$ – произвольная перестановка индексов $1, \dots, h$. Отношение $R^{(h)} \subseteq E_k^h$ назовем *вполне транзитивным*, если для произвольных элементов $a_1, \dots, a_h, a_{h+1} \in E_k$ из справедливости $R(a_1, \dots, a_{j-1}, a_{h+1}, a_{j+1}, \dots, a_h)$ для всех $j = 1, \dots, h$ следует справедливость $R(a_1, \dots, a_{h-1}, a_h)$.

Наборы $\alpha = (a_1, \dots, a_n) \in E_k^n$ и $\beta = (b_1, \dots, b_n) \in E_k^n$ назовем *соседними*, если они отличаются только в одной координате. Следующая лемма 3.9 в некотором смысле является обобщением леммы о существовании для немонотонной функции алгебры логики пары соседних наборов, на которых нарушается ее монотонность [139].

Лемма 3.9. [231] Пусть $R^{(h)} \subseteq E_k^h$ – вполне рефлексивное и вполне транзитивное отношение, $h \geq 2$. Функция k -значной логики $f(x_1, \dots, x_n) \notin A_k(R)$ тогда и только тогда, когда найдутся такие h наборов $\alpha^{(j)} \in E_k^n$, $j = 1, \dots, h$, находящихся в отношении R , среди которых два соседние, что не верно $R(f(\alpha^{(1)}), \dots, f(\alpha^{(h)}))$.

Доказательство. 1. Докажем необходимость. Т.к. $f(x_1, \dots, x_n) \notin A_k(R)$, найдутся h таких наборов $\beta^{(j)} = (b_1^{(j)}, \dots, b_n^{(j)}) \in E_k^n$, $j = 1, \dots, h$, находящихся в отношении R , что не верно $R(f(\beta^{(1)}), \dots, f(\beta^{(h)}))$.

- 1) Если наборы $\beta^{(j)}$, $j = 1, \dots, h$, содержат два соседних, то они искомые.
- 2) Иначе, выберем из них какие-то два набора. Пусть мы выбрали наборы $\beta^{(1)}$ и $\beta^{(2)}$ и i_0 – координата с наименьшим номером, в которой они отлича-

ются. Рассмотрим набор

$$\gamma = (b_1^{(1)}, \dots, b_{i_0-1}^{(1)}, b_{i_0}^{(2)}, b_{i_0+1}^{(1)}, \dots, b_n^{(1)}) \in E_k^n.$$

Отношение R вполне рефлексивно, поэтому для каждого $j = 1, \dots, h$ наборы

$$\beta^{(1)}, \dots, \beta^{(j-1)}, \gamma, \beta^{(j+1)}, \dots, \beta^{(h)}$$

находятся в отношении R . Отношение R вполне транзитивно, поэтому хотя бы одно из отношений

$$R(f(\beta^{(1)}), \dots, f(\beta^{(j-1)}), f(\gamma), f(\beta^{(j+1)}), \dots, f(\beta^{(h)}))$$

не верно, т.к. в противном случае было бы верно $R(f(\beta^{(1)}), \dots, f(\beta^{(h)}))$, что не так.

Выберем такое j , $1 \leq j \leq h$, что значения функции f на наборах

$$\beta^{(1)}, \dots, \beta^{(j-1)}, \gamma, \beta^{(j+1)}, \dots, \beta^{(h)},$$

не находятся в отношении R . Если среди этих наборов наборы $\beta^{(1)}$ и γ , то среди них есть два соседних набора. Иначе, среди них есть наборы γ и $\beta^{(2)}$, в которых число различающихся координат на единицу меньше, чем в наборах $\beta^{(1)}$ и $\beta^{(2)}$. Повторим рассуждения для новых h наборов. Через конечное число шагов получим искомые наборы.

2. Достаточность непосредственно следует из определения непринадлежности функции $f(x_1, \dots, x_n)$ к классу $A_k(R)$.

Лемма 3.9 доказана. □

Лемма 3.9 утверждает, что для установления принадлежности функции k -значной логики классу функций, сохраняющих вполне рефлексивное и вполне транзитивное отношение, достаточно ограничиться проверкой ее принадлежности этому классу на части всех наборов, а именно, на наборах, среди которых есть пара соседних.

Теорема 3.6. [231] Пусть $k \geq 2$, $R \subseteq E_k^h$ – вполне рефлексивное и вполне транзитивное отношение, $h \geq 2$, $\chi_R(z_1, \dots, z_h) \in P_k$ – его характеристическая функция, т.е. $\chi_R(a_1, \dots, a_h) = 1$, где $a_1, \dots, a_h \in E_k$, если и только если $R(a_1, \dots, a_h)$. Функция k -значной логики $f(x_1, \dots, x_n)$ сохраняет отношение R тогда и только тогда, когда для каждого i , $1 \leq i \leq n$, для каждой h таких элементов $a_1, \dots, a_h \in E_k$, что $R(a_1, \dots, a_h)$, и для каждой пары индексов j_1, j_2 ($1 \leq j_1 < j_2 \leq h$) и для всех возможных значений переменных $x_{j,1}, \dots, x_{j,i-1}, x_{j,i+1}, \dots, x_{j,n}$ при $j = 1, \dots, h$, $j \neq j_1$, $j \neq j_2$, $y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_n$ верно тождество

$$\chi_R(z_1, \dots, z_h) = 1,$$

где $z_j = f(x_{j,1}, \dots, x_{j,i-1}, a_1, x_{j,i+1}, \dots, x_{j,n})$ при $j = 1, \dots, h$, $j \neq j_1$, $j \neq j_2$, $z_{j_1} = f(y_1, \dots, y_{i-1}, a_{j_1}, y_{i+1}, \dots, y_n)$, $z_{j_2} = f(y_1, \dots, y_{i-1}, a_{j_2}, y_{i+1}, \dots, y_n)$.

Доказательство. 1. Докажем необходимость от противного. Предположим, что $f(x_1, \dots, x_n) \in A_k(R)$, но найдется такой номер i и такие h элементов $a_1, \dots, a_h \in E_k$, что $R(a_1, \dots, a_h)$ и для некоторой пары индексов j_1, j_2 ($1 \leq j_1 < j_2 \leq h$) тождество из леммы 3.6 не верно. Но это означает, что найдутся такие h наборов из множества E_k^n , находящихся в отношении R и среди которых есть два соседних, что отношение R не выполняется на значениях функции f на этих наборах. Но этого не может быть, т.к. $f \in A_k(R)$. Следовательно, необходимость обоснована.

2. Достаточность следует из леммы 3.9.

Теорема 3.6 доказана. □

Теперь докажем теорему 3.7 о существовании полиномиального алгоритма для распознавания принадлежности функции k -значной логики, заданной полиномом, к классу функций, сохраняющих вполне рефлексивное и вполне транзитивное отношение.

Теорема 3.7. [231] Пусть k – простое число, и $R^{(h)} \subseteq E_k^h$ – вполне рефлексивное и вполне транзитивное отношение. Существует детерминированный алгоритм, который для каждого слова $\alpha(P(f))$ в алфавите $A = E_k \cup \{+\}$ с полиномиальной временной сложностью определяет, принадлежит функция k -значной логики $f(x_1, \dots, x_n)$ к классу $A_k(R)$ или нет.

Доказательство. Опишем алгоритм, по которому можно построить требуемую РАМ. Пусть $f(x_1, \dots, x_n) \in P_k$. Проверим тождество из теоремы 3.6. Для этого запишем функцию $\chi_R(z_1, \dots, z_h)$ полиномом по модулю k . Для каждого i , $1 \leq i \leq n$, для каждого h таких элементов $a_1, \dots, a_h \in E_k$, что $R(a_1, \dots, a_h)$, и для каждой пары индексов j_1, j_2 ($1 \leq j_1 < j_2 \leq h$) проверим тождество

$$P(\chi_R(P(z_1), \dots, P(z_h))) = 1,$$

где

$$P(z_j) = P(f(x_{j,1}, \dots, x_{j,i-1}, a_1, x_{j,i+1}, \dots, x_{j,n})), \quad j = 1, \dots, h, \quad j \neq j_1, \quad j \neq j_2,$$

$$P(z_{j_1}) = P(f(y_1, \dots, y_{i-1}, a_{j_1}, y_{i+1}, \dots, y_n)),$$

$$P(z_{j_2}) = P(f(y_1, \dots, y_{i-1}, a_{j_2}, y_{i+1}, \dots, y_n)).$$

При фиксированных $i, j_1, j_2, a_1, \dots, a_h$ проверку тождества выполняем следующим образом. В выражении $P(\chi_R(P(z_1), \dots, P(z_h)))$ перемножаем скобки, приводим подобные слагаемые и сравниваем полученный полином по модулю k с константой 1. Т.к. h – фиксированная величина, эти преобразования можно выполнить с полиномиальной временной сложностью.

Теперь подсчитаем, сколько раз надо выполнить проверку тождеств. Число выборок h элементов $a_1, \dots, a_h \in E_k$, для которых верно $R(a_1, \dots, a_h)$, не больше k^h , и число пар индексов j_1, j_2 ($1 \leq j_1 < j_2 \leq h$) не больше h^2 . Заметим, что $n \leq |\alpha(P(f))|$, величины k^h и h^2 фиксированы. Поэтому временная сложность предлагаемого алгоритма будет полиномиальной.

Правильность алгоритма следует из леммы 3.6.

Теорема 3.7 доказана. □

Теперь применим доказанную теорему 3.7 к распознаванию принадлежности функций k -значной логики, заданных полиномами, к предполным классам монотонных функций, функций, сохраняющих разбиение, и к предполным классам типа В.

Определим предполные классы монотонных функций. Предполный класс монотонных функций двузначной логики был определен Э. Постом [181, 182]. В k -значной логике при $k \geq 3$ часть предполных классов монотонных функций была получена С.В. Яблонским [139], все предполные классы монотонных функций описал В.В. Мартынюк [101].

Пусть $\leq_k$ – частичный порядок на множестве элементов E_k . Функция k -значной логики $f(x_1, \dots, x_n)$ монотонна относительно частичного порядка $\leq_k$, если для любых наборов $\alpha = (a_1, \dots, a_n) \in E_k^n$ и $\beta = (b_1, \dots, b_n) \in E_k^n$ из того, что $a_1 \leq_k b_1, \dots, a_n \leq_k b_n$ следует, что $f(\alpha) \leq_k f(\beta)$. Обозначим как $M_k(\leq_k)$ множество всех функций k -значной логики, монотонных относительно частичного порядка $\leq_k$. Множество $M_k(\leq_k)$ – предполный класс тогда и только тогда, когда частичный порядок $\leq_k$ содержит наименьший и наибольший элементы [101].

Отметим, что задачи распознавания немонотонности функций алгебры логики при их представлениях формулами, ДНФ или КНФ является NP -трудными. Доказать NP -трудность задачи распознавания немонотонности функции двузначной логики, представленной КНФ, можно полиномиальным сведением к ней NP -полной задачи выполнимости конъюнктивных нормальных форм. Действительно, некоторая КНФ выполнима тогда и только тогда, когда немонотонна функция, полученная из нее умножением на $\bar{t}$, где t – некото-

рая, не присутствующая в этой КНФ, переменная. Как следствие, NP -трудны задачи распознавания немонотонности функций, представленных ДНФ и формулами в общем случае.

Отметим, что $M_k(\leq_k) = A_k(\leq_k)$, а отношение $\leq_k$ является рефлексивным и транзитивным, т.к. это отношение частичного порядка. Поэтому как следствие теоремы 3.7 получаем

Следствие 3.1. [231] Пусть k – простое число, и $\leq_k$ – отношение частичного порядка на множестве E_k . Существует детерминированный алгоритм, который для каждого слова $\alpha(P(f))$ в алфавите $A = E_k \cup \{+\}$ с полиномиальной временной сложностью определяет, является функция k -значной логики $f(x_1, \dots, x_n)$ монотонной относительно частичного порядка $\leq_k$ или нет.

Определим предполные классы функций, сохраняющих разбиение. В двузначной логике предполных классов функций, сохраняющих разбиение нет. В k -значной логике при $k \geq 3$ предполные классы функций, сохраняющих разбиение, описаны С.В. Яблонским [139].

Пусть $D = \{D_1, \dots, D_s\}$ – разбиение множества элементов E_k , т.е. $D_i \subseteq E_k$, $D_i \neq \emptyset$ при $i = 1, \dots, s$, $D_i \cap D_j = \emptyset$ при $i \neq j$, и $\bigcup_{i=1}^s D_i = E_k$. Функция k -значной логики $f(x_1, \dots, x_n)$ сохраняет разбиение D , если для любых наборов $\alpha = (a_1, \dots, a_n) \in E_k^n$ и $\beta = (b_1, \dots, b_n) \in E_k^n$ из того, что $a_1, b_1 \in D_{i_1}, \dots, a_n, b_n \in D_{i_n}$ для некоторых $i_1, \dots, i_n$ следует, что $f(\alpha), f(\beta) \in D_i$ для некоторого i . Обозначим как $U_k(D)$ множество всех функций k -значной логики, сохраняющих разбиение D . Множество $U_k(D)$ – предполный класс тогда и только тогда, когда $1 < s < k$ [139].

Отметим, что $U_k(D) = A_k(R_D)$, где $R_D \subseteq E_k^2$ и $R_D(a, b)$ при $a, b \in D_i$ для некоторого i . Отношение R_D является рефлексивным и транзитивным, т.к.

это отношение эквивалентности. Поэтому как следствие теоремы 3.7 получаем

Следствие 3.2. [231] Пусть k – простое число, и D – разбиение множества E_k . Существует детерминированный алгоритм, который для каждого слова $\alpha(P(f))$ в алфавите $A = E_k \cup \{+\}$ с полиномиальной временной сложностью определяет, сохраняет функция k -значной логики $f(x_1, \dots, x_n)$ разбиение D или нет.

Определим предполные классы типа В. В двузначной логике нет предполных классов типа В. Класс Слупецкого, являющийся предполным классом типа В в k -значной логике при $k \geq 3$, получен С.В. Яблонским [139]. В k -значной логике при $k \geq 3$ все предполные классы типа В были найдены И. Розенбергом [186, 187]. Для описания предполных классов типа В введем вспомогательные понятия. Зафиксируем некоторые числа h ($h \geq 3$) и s . Произвольное число a , $0 \leq a \leq h^s - 1$, однозначно может быть записано в виде

$$a = a_0 + a_1 \cdot h + \dots + a_{s-1} \cdot h^{s-1}, \quad (22)$$

где $0 \leq a_0, a_1, \dots, a_{s-1} \leq h - 1$. Введем отношение $\zeta_s \subseteq E_{h^s}^h$. Элементы $a^{(1)}, \dots, a^{(h)} \in E_{h^s}^h$ находятся в отношении ζ_s , если при представлении каждого числа $a^{(j)}$ в виде (22) среди чисел $a_i^{(1)}, \dots, a_i^{(h)}$ есть хотя бы два равные для каждого $i = 0, 1, \dots, s - 1$.

Отношение $R^h \subseteq E_k^h$, $h \geq 3$, назовем отношением типа В, если найдется такое отображение φ из множества E_k на множество E_{h^s} при некотором s , $h^s \leq k$, что для произвольных элементов $a_1, \dots, a_h \in E_k$ верно $R(a_1, \dots, a_h)$ тогда и только тогда, когда верно $\zeta_s(\varphi(a_1), \dots, \varphi(a_h))$.

Если $R \subseteq E_k^h$ – отношение типа В, $h \geq 3$, то множество $A_k(R)$ – предполный класс P_k [186, 187]. Отметим, что отношение типа В является вполне рефлексивным. Докажем, что отношение типа В является вполне транзитив-

НЫМ.

Лемма 3.10. [231] Пусть $k \geq 3$, $R^{(h)} \subseteq E_k^h$ – отношение типа В, $h \geq 3$. Тогда R является вполне транзитивным отношением.

Доказательство. Пусть $R \subseteq E_k^h$ – отношение типа В, $h \geq 3$, и $\varphi : E_k \rightarrow E_{h^s}$ – требуемое его определением отображение ($h^s \leq k$). Отметим, что отношение типа В является вполне симметричным. Пусть $a_1, \dots, a_h, a_{h+1} \in E_k$, и пусть $b^{(j)} = \varphi(a_j) \in E_{h^s}$, $j = 1, \dots, h, h+1$.

Если верно $R(a_1, \dots, a_{j-1}, a_{h+1}, a_{j+1}, \dots, a_h)$ при всех $j = 1, \dots, h$, то верно также $\zeta_s(b^{(1)}, \dots, b^{(j-1)}, b^{(h+1)}, b^{(j+1)}, \dots, b^{(h)})$ при всех $j = 1, \dots, h$. Пусть

$$b^{(j)} = \sum_{i=0}^{s-1} b_i^{(j)} \cdot h^i$$

при $j = 1, \dots, h, h+1$. Тогда для каждого i , $i = 0, 1, \dots, s-1$, и каждого $j = 1, \dots, h$, среди h элементов

$$b_i^{(1)}, \dots, b_i^{(j-1)}, b_i^{(h+1)}, b_i^{(j+1)}, \dots, b_i^{(h)}$$

хотя бы два равны. Отсюда следует, что для каждого i , $i = 0, 1, \dots, s-1$, среди h элементов

$$b_i^{(1)}, \dots, b_i^{(h-1)}, b_i^{(h)}$$

также хотя бы два равны. Иначе, пусть для некоторого номера i , $0 \leq i \leq s-1$, элементы $b_i^{(1)}, \dots, b_i^{(h-1)}, b_i^{(h)}$ попарно различны. Среди элементов

$$b_i^{(h+1)}, b_i^{(2)}, \dots, b_i^{(h)}$$

хотя бы два равны, поэтому $b_i^{(h+1)} = b_i^{(j_0)}$ для некоторого j_0 , $2 \leq j_0 \leq h$. Тогда элементы $b_i^{(1)}, \dots, b_i^{(j_0-1)}, b_i^{(h+1)}, b_i^{(j_0+1)}, \dots, b_i^{(h)}$ попарно различны, чего не может быть.

Значит, верно $\zeta_s(b^{(1)}, \dots, b^{(h-1)}, b^{(h)})$, откуда верно $R(a_1, \dots, a_{h-1}, a_h)$.

Лемма 3.10 доказана. □

Теперь как следствие теоремы 3.7 и леммы 3.10 получаем

Следствие 3.3. [231] Пусть k – простое число, и $R \subseteq E_k^h$ – отношение типа B , $h \geq 3$. Существует детерминированный алгоритм, который для каждого слова $\alpha(P(f))$ в алфавите $A = E_k \cup \{+\}$ с полиномиальной временной сложностью определяет, сохраняет функция k -значной логики $f(x_1, \dots, x_n)$ отношение R или нет.

В завершение этого раздела рассмотрим задачу нахождения остатка от деления веса функции алгебры логики на степень двойки. В книге [213] (стр. 76) отмечено, что для произвольной функции алгебры логики $f(x_1, \dots, x_n)$ ее вес кратен двум тогда и только тогда, когда $\deg(f) < n$. Рассмотрим следующую задачу: с какой алгоритмической сложностью можно найти по полиному Жегалкина функции алгебры логики $f(x_1, \dots, x_n)$ остаток от деления ее веса на 2^m , где $m = 2, 3, \dots$. Отметим, что в [159] доказано, что задача определения по полиному Жегалкина n -местной функции алгебры логики равенства ее веса числу 2^{n-1} является NP-трудной.

Для решения нашей задачи рассмотрим представления функций алгебры логики полиномами над кольцом целых чисел. В [151] доказано, что каждая функция алгебры логики $f(x_1, \dots, x_n)$ представима однозначным полиномом $P_{\mathbb{Z}}(f)$ над кольцом целых чисел, в котором степень каждой переменной не выше единицы, а также получены следующие свойства:

1. Если $P(f) = \bigoplus_{j=1}^l X_j$, то $P_{\mathbb{Z}}(f) = \sum_{s=1}^l \sum_{1 \leq j_1 < \dots < j_s \leq l} (-1)^{s-1} \cdot 2^{s-1} \cdot X_{j_1} \cdot \dots \cdot X_{j_s}$.
2. Если $P_{\mathbb{Z}}(f) = \sum_{\alpha \in E_2^n} c_f^{\mathbb{Z}}(\alpha) X_{\alpha}$, где $c_f^{\mathbb{Z}}(\alpha) \in \mathbb{Z}$, то $|f| = \sum_{\alpha \in E_2^n} 2^{n-|\alpha|} \cdot c_f^{\mathbb{Z}}(\alpha)$.

В представлениях п.п. 1, 2 $+$ и $\cdot$ обозначают соответственно сложение и умножение целых чисел.

Теорема 3.8. [241] Пусть $m, m \geq 1$, – заданное натуральное число. Существует детерминированный алгоритм, который для каждого слова $\alpha(P(f))$ в алфавите $A = E_2 \cup \{\oplus\}$ с полиномиальной временной сложностью находит остаток от деления веса функции алгебры логики $f(x_1, \dots, x_n)$ на 2^m .

Доказательство. Опишем требуемый алгоритм.

В начале работы алгоритма текущая сумма (остаток от деления веса функции на 2^m) равна нулю. Последовательно повторяем шаги $1, 2, \dots, m$.

Шаг $j, 1 \leq j \leq m$. Рассматриваем все возможные произведения по j слагаемых полинома Жегалкина функции $f(x_1, \dots, x_n)$, проводя упрощения по правилу $x \cdot x = x$. Пусть X – очередной моном, полученный таким образом, и его ранг равен r . Если $r \geq n - m + j$, то к текущей сумме добавляем слагаемое $(-2)^{j-1} \cdot 2^{n-r}$.

При каждом изменении текущую сумму следует приводить по модулю 2^m . После завершения шага m в текущей сумме останется остаток от деления веса функции f на 2^m .

Сложность предложенного алгоритма полиномиальна.

Правильность этого алгоритма определяется описанными выше свойствами из [151], если заметить следующее:

1) достаточно построить все возможные произведения мономов полинома Жегалкина по s при $s \leq m$, т.к. коэффициенты при произведениях мономов полинома Жегалкина по s при $s > m$ будут иметь вид $a \cdot 2^m$, a – некоторое целое число. Т.е. эти коэффициенты равны нулю по модулю 2^m ;

2) получаемые при помощи произведений мономы можно рассматривать до ранга r , где $r \geq n - m + 1$, т.к. числовые множители при новых мономах ранга r , где $r < n - m + 1$, имеют вид $b \cdot 2^m$, b – некоторое целое число. Т.е. они также равны нулю по модулю 2^m .

Теорема 3.8 доказана. □

Таким образом, в этом разделе доказана полиномиальность задач распознавания принадлежности функций k -значной логики, заданных полиномами, к предполным классам из пяти семейств предполных классов (при простых k).

4 Нахождение полиномиальных представлений функций

В этом разделе мы исследуем алгоритмическую сложность построения полиномов по модулю k для функций k -значной логики. Все результаты этого раздела опубликованы в работах [242, 248, 252–257, 260, 261].

Сначала мы исследуем алгоритмическую сложность задачи распознавания полиномиальности функции k -значной логики при составном k и в случае положительного ответа построения какого-то ее полинома по модулю k .

Каждая функция k -значной логики может быть представлена полиномом по модулю k тогда и только тогда, когда k – простое число [139] (раздел 18). В [5] найден критерий полиномиальности функций k -значной логики при составных k вида $k = p_1 \cdot \dots \cdot p_s$, где $p_1, \dots, p_s$ – попарно различные простые числа, $s \geq 2$, который можно проверить со сложностью $O(N)$ (в алгоритмической модели СФЭ), где $N = k^n$ и n – число переменных функции k -значной логики, подаваемой на вход алгоритма в виде вектора своих значений. При исследовании фрагментов решетки замкнутых классов, связанных с классом полиномиальных функций, получены критерии полиномиальности функций k -значной логики при составных k [108, 120, 137]. В [108] доказано, что распознать полиномиальность функции k -значной логики при $k = p^m$, где p – простое число, $m \geq 2$, и в случае положительного ответа построить какой-то ее полином можно со сложностью $O(N \log^m N)$ (в алгоритмической модели РАМ), где $N = k^n$ и n – число переменных функции k -значной логики, подаваемой на вход алгоритма в виде вектора своих значений. В [7–10, 39–41, 56] разработаны методы и построены быстрые алгоритмы для распознавания некоторых свойств функций k -значной логики, заданных вектором из своих $N = k^n$ значений (в алгоритмической модели СФЭ).

При исследовании полиномиальности функций k -значных логик при со-

ставных k мы обобщаем и развиваем подход, примененный в работе [4] для подсчета числа функций из Pol_k^n при составных k . Мы предлагаем канонический вид полиномов, представляющих полиномиальные функции k -значной логики при составных k , который обобщает канонический вид одноместных полиномиальных функций из [4, 178, 197] на функции многих переменных. На основе предложенного канонического вида мы строим алгоритм, который по вектору значений функции k -значной логики $f(x_1, \dots, x_n)$, где k – составное число, определяет, является ли функция f полиномиальной и в случае положительного ответа находит ее канонический полином со сложностью $O(N)$ (в алгоритмической модели СФЭ), где $N = k^n$ – длина вектора значений функции.

Обозначим как $I(k, n)$ множество всех полиномов по модулю k , зависящих от n переменных и задающих функцию k -значной логики, тождественно равную нулю. Иногда один и тот же формальный полином мы будем рассматривать по разным модулям. Поэтому если для некоторого полинома $g(x_1, \dots, x_n)$ мы пишем, что $g \in I(k, n)$ (или $g \notin I(k, n)$), то это означает что под операциями сложения и умножения в полиноме g понимаются операции сложения и умножения по модулю k .

Пусть p – простое число, $m \geq 2$. По малой теореме Ферма верно, что полином $x^p - x$ равен нулю по модулю p , т.е. $x^p - x = 0(\text{mod } p)$. Отсюда следует, что

$$(x^p - x)^m = 0(\text{mod } p^m). \quad (23)$$

Если $g(x_1, \dots, x_n)$ – некоторый полином по модулю p^m , и в нем степень какой-то переменной x_i выше $mp - 1$, то мы можем формально поделить с остатком этот полином с остатком на полином $(x_i^p - x_i)^m$. Полученный при делении остаток также представляет ту же функцию p^m -значной логики, что

и полином g . Т.к. $mp \leq p^m$ при p – простым числе, $m \geq 2$, мы будем, как правило, рассматривать полиномы вида

$$\sum_{\alpha \in E_{p^m}^n} c(\alpha) X_\alpha,$$

где $c(\alpha) \in E_{p^m}$ – коэффициенты.

Следующая лемма 4.1 является обобщением леммы из работы [4] на случай полиномов, зависящих от n переменных, $n \geq 2$.

Лемма 4.1. [252] *Пусть p – простое число и $m \geq 1$. Если*

$$g(x_1, \dots, x_n) = \sum_{\alpha \in E_p^n} c_\alpha X_\alpha,$$

где $c_\alpha \in E_{p^m}$, причем не все коэффициенты c_α равны нулю, то $g(x_1, \dots, x_n) \notin I(p^m, n)$.

Доказательство. Доказательство проведем индукцией по значению m .

Базис индукции. Пусть $m = 1$. Тогда справедливость леммы 4.1 следует из теоремы об однозначности задания каждой k -значной функции полиномом по модулю k указанного вида при простом $k = p$ [218] (стр. 69–71), [219] (стр. 38–39).

Индуктивный переход. Пусть для всех m , $1 \leq m < m_0$, утверждение леммы 4.1 верно. Рассмотрим $m = m_0$. Докажем от противного.

Пусть существует такой непустой полином $g(x_1, \dots, x_n)$, что $g(x_1, \dots, x_n) \in I(p^{m_0}, n)$ и степень каждой переменной в каждом его слагаемом не выше $(p - 1)$. Пусть

$$g(x_1, \dots, x_n) = \sum_{i=1}^l a_i X_i,$$

где $a_1, \dots, a_l \in E_{p^{m_0}} \setminus \{0\}$, $l \geq 1$.

Пусть $b_i \in E_{p^{m_0-1}}$ и $b_i = a_i \pmod{p^{m_0-1}}$ при $i = 1, \dots, l$. Рассмотрим полином

$$g_1(x_1, \dots, x_n) = \sum_{i=1}^l b_i X_i.$$

Верно, что $g_1(x_1, \dots, x_n) \in I(p^{m_0-1}, n)$. Но для полинома $g_1(x_1, \dots, x_n)$ выполняются условия леммы 4.1. Поэтому по предположению индукции $b_i = 0$ для всех $i = 1, \dots, l$. Т.е. $a_i = p^{m_0-1} \cdot c_i$, где $c_i \in E_p \setminus \{0\}$, при $i = 1, \dots, l$. Тогда для полинома

$$g_2(x_1, \dots, x_n) = \sum_{i=1}^l c_i X_i$$

выполняются условия леммы 4.1 и верно, что $g_2(x_1, \dots, x_n) \in I(p, n)$. Это противоречит индуктивному предположению.

Лемма 4.1 доказана. □

Введем следующее определение.

Определение 4.1. Пусть p – простое число, $m \geq 1$ и X_α – моном, $\alpha \in E_{p^m}^n$. Определим *составную характеристику* $\text{cd}(X_\alpha)$ (по отношению к простому числу p и числу m) для монома X_α .

1. Если найдется полином

$$g(x_1, \dots, x_n) = X_\alpha + \sum_{\beta < \alpha} c_\beta X_\beta \in I(p^m, n),$$

где $c_\beta \in E_{p^m}$, то $\text{cd}(X_\alpha) = m$.

2. Иначе, составной характеристикой $\text{cd}(X_\alpha)$ назовем такое число m_0 , $0 \leq m_0 < m$, что

1) найдется полином

$$g(x_1, \dots, x_n) = X_\alpha + \sum_{\beta < \alpha} c_\beta X_\beta \in I(p^{m_0}, n),$$

где $c_\beta \in E_{p^m}$ (при этом полагаем по определению, что $g(x_1, \dots, x_n) = X_\alpha \in I(p^0, n)$);

2) для каждого полинома

$$g_1(x_1, \dots, x_n) = \sum_{\beta \leq \alpha} c_\beta X_\beta \in I(p^{m_0+1}, n)$$

где $c_\beta \in E_{p^m}$, верно, что c_α делится на p .

Другими словами, величина $\text{cd}(X_\alpha)$ (по отношению к простому числу p и числу m) обозначает такое наибольшее число m_0 из чисел $0, 1, \dots, m-1, m$, что найдется полином

$$g(x_1, \dots, x_n) = X_\alpha + \sum_{\beta < \alpha} c_\beta X_\beta \in I(p^{m_0}, n),$$

где $c_\beta \in E_{p^m}$.

Замечание 4.1. Заметим, что если найдется полином $g(x_1, \dots, x_n) \in I(p^m, n)$, в котором максимальный среди слагаемых с ненулевыми коэффициентами моном X_α встречается с коэффициентом $c_\alpha \in E_{p^m}$, $c_\alpha \neq 0$, то найдется также и полином

$$g_0(x_1, \dots, x_n) = \sum_{\beta \leq \alpha} c_\beta X_\beta \in I(p^m, n).$$

Достаточно в качестве полинома g_0 рассмотреть полином, получающийся подстановкой нулей в полином g вместо всех переменных с номерами из множества $\{1, \dots, n\} \setminus t(\alpha)$.

Лемма 4.2. [252] *Если p – простое число, $m \geq 1$, $\alpha = (a_1, \dots, a_n) \in E_{p^m}^n$, то $\text{cd}(X_\alpha) = 0$ тогда и только тогда, когда $\alpha \in E_p^n$.*

Доказательство. В одну сторону утверждение леммы 4.2 доказано в лемме 4.1. Докажем в другую сторону. По малой теореме Ферма $x^p = x \pmod{p}$.

Отсюда

$$x^p - x \in I(p, 1).$$

Предположим, что $\alpha = (a_1, \dots, a_n) \notin E_p^n$, т.е. $a_i \geq p$ для некоторого i , $1 \leq i \leq n$. Тогда $X_\alpha = X_\beta \cdot x_i^{a_i}$, где $\beta = (a_1, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n) \in E_p^n$. Получаем, что

$$g(x_1, \dots, x_n) = X_\beta \cdot x_i^{a_i-p} \cdot (x_i^p - x_i) = X_\alpha - X_\beta \cdot x_i^{a_i-p+1} \in I(p, n)$$

и $\text{cd}(X_\alpha) \geq 1$ (т.к. $p \geq 2$). □

Несложно проверить справедливость следующего предложения 4.1.

Предложение 4.1. *Если p – простое число, $t \geq 1$, $\alpha, \beta \in E_{p^t}^n$, и $\alpha \leq \beta$, то $\text{cd}(X_\alpha) \leq \text{cd}(X_\beta)$.*

Пусть p – простое число, $t \geq 1$. Введем *линейный порядок* $\preceq$ на множестве мономов $X^n = \{X_\alpha \mid \alpha \in E_{p^t}^n\}$ над переменными $x_1, \dots, x_n$ так, чтобы выполнялись свойства:

- 1) если $X_\alpha \prec X_\beta$, то $\text{cd}(X_\alpha) \leq \text{cd}(X_\beta)$;
- 2) если $\alpha < \beta$, то $X_\alpha \prec X_\beta$.

Такой линейный порядок существует. Например, можно вначале разбить все мономы из множества X^n над переменными $x_1, \dots, x_n$ на классы эквивалентности по значению составной характеристики и линейно упорядочить эти классы по значению составной характеристики. А затем внутри каждого класса эквивалентности линейно упорядочить мономы так, чтобы выполнялось условие 2.

Следующая лемма 4.3 является обобщением леммы из работы [4] на случай полиномов, зависящих от n , $n \geq 2$, переменных.

Лемма 4.3. [252] *Пусть p – простое число, $t \geq 1$.*

Если

$$g(x_1, \dots, x_n) = \sum_{i=1}^l a_i X_i \in I(p^m, n),$$

где $a_i \in E_{p^m}$, X_l – наибольший (относительно линейного порядка $\preceq$) моном среди слагаемых полинома g , $a_l \neq 0$, и

$$t = m - \text{cd}(X_l) \geq 0,$$

то все коэффициенты a_i делятся на p^t , $i = 1, \dots, l$.

Доказательство. Пусть $X_l = X_\alpha$ для некоторого набора $\alpha = (a_1, \dots, a_n) \in E_{p^m}^n$.

Если $t = 0$, то утверждение леммы 4.3 верно.

При $1 \leq t \leq m$ докажем лемму 4.3 индукцией относительно линейного порядка $\preceq$ на множестве мономов над переменными $x_1, \dots, x_n$.

Базис индукции: пусть в мономе X_l степени всех переменных не выше $(p-1)$. Тогда утверждение следует из леммы 4.1.

Индуктивный переход: пусть для произвольного полинома из множества $I(p^m, n)$ верно, что если наибольший моном X среди его слагаемых строго меньше X_l относительно линейного порядка $\preceq$, то все коэффициенты в этом полиноме делятся на $p^{m-\text{cd}(X)}$.

Т.к. $\text{cd}(X_l) < m$, по определению составной характеристики коэффициент a_l делится на p . Пусть $a_l = p^{m-r} \cdot b_l$, где число b_l не делится на p и $1 \leq r \leq m-1$. По определению составной характеристики найдется полином

$$h(x_1, \dots, x_n) = X_\alpha + \sum_{\beta < \alpha} c_\beta X_\beta \in I(p^{\text{cd}(X_l)}, n),$$

где $c_\beta \in E_{p^m}$. Среди слагаемых полинома h моном X_l является наибольшим относительно частичного порядка $\leq$, а значит, и относительно линейного порядка $\preceq$ мономом.

Рассмотрим два случая.

1. Пусть $r > \text{cd}(X_l)$. Тогда получаем, что полином

$$g_1(x_1, \dots, x_n) = g(x_1, \dots, x_n) - p^{m-r} \cdot b_l \cdot h(x_1, \dots, x_n) \in I(p^{m-r+\text{cd}(X_l)}, n).$$

Заметим, что все слагаемые полинома g_1 меньше (относительно линейного порядка $\preceq$) монома X_l .

Пусть X – наибольший моном относительно линейного порядка $\preceq$ среди слагаемых полинома g_1 . Тогда моном X входит с ненулевым коэффициентом или в полином g , или в полином h . В обоих случаях по свойствам линейного порядка $\preceq$ верно, что

$$\text{cd}(X) \leq \text{cd}(X_l).$$

Для полинома $g_1(x_1, \dots, x_n) \in I(p^{m-r+\text{cd}(X_l)}, n)$ верно предположение индукции. Поэтому все его коэффициенты делятся на $p^{m-r+\text{cd}(X_l)-\text{cd}(X)}$ и, соответственно, на p^{m-r} , т.к. $\text{cd}(X) \leq \text{cd}(X_l)$. А это означает, что все коэффициенты a_i , $i = 1, \dots, l$, исходного полинома g делятся на p^{m-r} .

Пусть $a_i = p^{m-r} \cdot b_i$, где $b_i \in E_{p^r}$, $i = 1, \dots, l$. Тогда полином

$$g_2(x_1, \dots, x_n) = \sum_{i=1}^l b_i X_i \in I(p^r, n),$$

причем коэффициент b_l не делится на p . А этого не может быть по определению составной характеристики. Поэтому этот случай невозможен.

2. Пусть теперь $r \leq \text{cd}(X_l)$. Тогда полином

$$p^{m-r} \cdot b_l \cdot h(x_1, \dots, x_n) \in I(p^{m-r+\text{cd}(X_l)}, n),$$

а значит, т.к. $r \leq \text{cd}(X_l)$, верно

$$p^{m-r} \cdot b_l \cdot h(x_1, \dots, x_n) \in I(p^m, n).$$

Получаем, что полином

$$g_1(x_1, \dots, x_n) = g(x_1, \dots, x_n) - p^{m-r} \cdot b_l \cdot h(x_1, \dots, x_n) \in I(p^m, n).$$

Заметим, что все слагаемые полинома g_1 меньше (относительно линейного порядка $\preceq$) монома X_l .

Пусть X – наибольший моном относительно линейного порядка $\preceq$ среди слагаемых полинома g_1 . Тогда моном X входит с ненулевым коэффициентом или в полином g , или в полином h . В обоих случаях по свойствам линейного порядка $\preceq$ верно, что

$$\text{cd}(X) \leq \text{cd}(X_l).$$

Для полинома $g_1(x_1, \dots, x_n) \in I(p^m, n)$ верно предположение индукции. Поэтому все его коэффициенты делятся на $p^{m-\text{cd}(X)}$, а также на $p^{m-\text{cd}(X_l)}$, т.к. $\text{cd}(X) \leq \text{cd}(X_l)$. А это означает, что все коэффициенты a_i , $i = 1, \dots, l$, исходного полинома g делятся на $p^{m-\text{cd}(X_l)}$.

Лемма 4.3 доказана. □

Следствие 4.1. [252] Пусть p – простое число, $m \geq 1$.

Если

$$g(x_1, \dots, x_n) = \sum_{i=1}^l a_i X_i,$$

где $a_i \in E_{p^m}$, $i = 1, \dots, l$, – полином по модулю p^m , X_l – наибольший (относительно линейного порядка $\preceq$) моном среди слагаемых полинома g и $0 < a_l < p^t$, где

$$t = m - \text{cd}(X_l) \geq 1,$$

то $g(x_1, \dots, x_n) \notin I(p^m, n)$.

Теперь мы можем доказать теорему о каноническом виде полиномов функций из Pol_p^m , где p – простое число, $m \geq 1$. Отметим, что для одноместных полиномиальных функций k -значной логики аналогичный однозначный вид полиномов найден в [4, 178, 197].

Теорема 4.1. [252] Пусть p – простое число, $m \geq 1$. Каждая функция $f(x_1, \dots, x_n) \in \text{Pol}_{p^m}^n$ задается однозначным полиномом по модулю p^m вида

$$f(x_1, \dots, x_n) = \sum_{i=1}^l a_i \cdot X_i,$$

где $\text{cd}(X_i) < m$ и $a_i < p^{m-\text{cd}(X_i)}$, $i = 1, \dots, l$.

Доказательство. Пусть $f(x_1, \dots, x_n) \in \text{Pol}_{p^m}^n$. Значит, найдется полином по модулю p^m , задающий функцию f .

1. Построим полином описанного в теореме 4.1 вида для функции f .

Шаг 1. Рассмотрим наибольшее (относительно линейного порядка $\preceq$) слагаемое X среди всех слагаемых полинома функции f , составная характеристика которых равна m .

Т.к. $\text{cd}(X) = m$, найдется полином $g(x_1, \dots, x_n) \in I(p^m, n)$ с наибольшим (относительно частичного порядка $\leq$, а значит, и относительно линейного порядка $\preceq$) слагаемым X , коэффициент при котором равен 1.

Вычтем из полинома функции f равный нулю полином g столько раз, чтобы занулить коэффициент при мономе X . Полученный полином также задает функцию f .

Повторим эти рассуждения для полученного полинома функции f , если в нем есть слагаемые с составной характеристикой, равной m .

Повторив эти рассуждения достаточное число раз, получим полином h для функции f , не содержащий слагаемых с составной характеристикой, равной m .

Шаг 2. Рассмотрим полином h .

Рассмотрим наибольшее (относительно линейного порядка $\preceq$) слагаемое X среди всех слагаемых полинома h . Отметим, что $\text{cd}(X) < m$.

По определению составной характеристики найдется полином

$$g_0(x_1, \dots, x_n) \in I(p^{\text{cd}(X)}, n)$$

с наибольшим (относительно частичного порядка $\leq$, а значит, и относительно линейного порядка $\preceq$) слагаемым X , коэффициент при котором равен 1, $i = 1, \dots, n$. Тогда полином

$$g(x_1, \dots, x_n) = p^{m-\text{cd}(X)} g_0(x_1, \dots, x_n) \in I(p^m, n).$$

Вычтем из полинома h равный тождественно нулю полином g столько раз, чтобы коэффициент при слагаемом X в получившемся полиноме оказался меньшим числа $p^{m-\text{cd}(X)}$. Так всегда можно сделать.

Повторим эти рассуждения для получившегося полинома функции f .

Повторив эти рассуждения достаточное число раз, получим полином функции f , который описан в утверждении теоремы 4.1.

2. Теперь докажем однозначность полинома такого вида для функции f .

Пусть для функции f найдутся два различных полинома f_1 и f_2 такого вида, ее задающие. Пусть X – наибольшее (относительно линейного порядка $\preceq$) слагаемое X , встречающееся в полиномах f_1 и f_2 с разными коэффициентами $c_1 \in E_{p^m}$ и $c_2 \in E_{p^m}$. Пусть, для определенности, $c_1 > c_2$.

Рассмотрим полином

$$g(x_1, \dots, x_n) = f_1(x_1, \dots, x_n) - f_2(x_1, \dots, x_n) \in I(p^m, n).$$

Полином $g(x_1, \dots, x_n)$ – не пустой. Рассмотрим в нем наибольшее (относительно линейного порядка $\preceq$) слагаемое X с ненулевым коэффициентом $c = c_1 - c_2$. Заметим, что $c < p^{m-\text{cd}(X)}$. Это противоречит следствию 4.1.

Теорема 4.1 доказана. □

Для функции $f(x_1, \dots, x_n) \in \text{Pol}_{p^m}$ ее однозначный полином из теоремы 4.1 назовем *каноническим полиномом* и будем обозначать его $P(f)$. Заметим,

что в работе [4] рассматривается другой канонический вид полиномиальных функций из Pol_{p^m} при числе их переменных $n \geq 2$.

Теперь докажем некоторые свойства составной характеристики.

Лемма 4.4. [252] Пусть p – простое число, $m \geq 1$, $\alpha = (a_1, \dots, a_n) \in E_{p^m}^n$. Тогда если $\text{cd}(X_\alpha) < m$, то

$$\text{cd}(X_\alpha) = \sum_{i=1}^n \text{cd}(x_i^{a_i}).$$

Доказательство. Пусть $\alpha = (a_1, \dots, a_n) \in E_{p^m}^n$, $\text{cd}(x_i^{a_i}) = m_i$ и $\sum_{i=1}^n m_i = m_0$.

По определению составной характеристики найдутся полиномы

$$g_i(x_i) \in I(p^{m_i}, 1),$$

в которых их наибольший моном $x_i^{m_i}$ встречается с коэффициентом 1.

Следовательно, полином

$$g(x_1, \dots, x_n) = \prod_{i=1}^n g_i(x_i) \in I(p^{m_0}, n),$$

и в полиноме g наибольший (относительно частичного порядка $\leq$) моном X_α встречается с коэффициентом 1.

Отсюда $m_0 < m$ и

$$\text{cd}(X_\alpha) \geq m_0 = \sum_{i=1}^n \text{cd}(x_i^{a_i}).$$

Докажем индукцией по значению r , $0 \leq r \leq n$, координат в наборе α , больших $(p-1)$, что

$$\text{cd}(X_\alpha) = \sum_{i=1}^n \text{cd}(x_i^{a_i}).$$

Базис индукции. Если $r = 0$, то утверждение верно (т.к. $\text{cd}(x^{a_i}) = 0$ при $0 \leq a_i \leq p-1$).

Индуктивный переход обоснуем от противного. Предположим, что найдется полином $h(x_1, \dots, x_n) \in I(p^{m_0+1}, n)$, наибольший (относительно частичного порядка $\leq$) моном X_α в котором встречается с коэффициентом 1.

Не ограничивая общности, пусть $a_1 > p - 1$. Вынесем в полиноме h моном $x_1^{a_1}$ за скобки. Получим выражение вида

$$h(x_1, \dots, x_n) = x_1^{a_1} \cdot h_1(x_2, \dots, x_n) + h_2(x_1, \dots, x_n).$$

Пусть $\alpha_1 = (a_2, \dots, a_n) \in E_{p^{m_0+1}}^{n-1}$. Заметим, что т.к. моном X_α является наибольшим (относительно частичного порядка $\leq$) среди мономов полинома h , моном X_{α_1} является наибольшим (относительно частичного порядка $\leq$) среди мономов полинома h_1 , а также, он входит в полином h_1 с коэффициентом 1. Кроме того, в полиноме h_2 нет слагаемых с множителем x_1^t при $t \geq a_1$.

Рассмотрим два случая.

1. Пусть найдется такой набор $\beta = (b_2, \dots, b_n) \in E_{p^{m_0+1}}^{n-1}$, что $h_1(\beta) = c$, где c не делится на $p^{(m_0+1)-m_1}$. Тогда

$$h_1(x_1) = h(x_1, b_2, \dots, b_n) = cx_1^{a_1} + c_{a_1-1}x_1^{a_1-1} + \dots + c_1x_1 \in I(p^{m_0+1}, 1)$$

для некоторых коэффициентов $c_{a_1-1}, \dots, c_1 \in E_{p^{m_0+1}}$. Но значение коэффициента c противоречит лемме 4.3.

2. Следовательно, $h_1(x_2, \dots, x_n) \in I(p^{(m_0+1)-m_1}, n-1)$. Отсюда $\text{cd}(X_{\alpha_1}) \geq (m_0+1) - m_1$. Но для полинома h_1 верно предположение индукции, т.е.

$$\text{cd}(X_{\alpha_1}) = \sum_{i=2}^n m_i = m_0 - m_1.$$

Получили противоречие.

Лемма 4.4 доказана. □

Лемма 4.4 показывает, что значение составной характеристики монома (если она меньше m) можно подсчитать как сумму составных характеристик его

сомножителей.

Лемма 4.5. [252] Пусть p – простое число, $m \geq 2$, $\alpha = (a_1, \dots, a_n) \in E_p^n$, $\text{cd}(x_i^{a_i}) = m_i$ при $i = 1, \dots, n$, и

$$\sum_{i=1}^n m_i = m_0 < m.$$

Тогда

1. $a_i \leq mp - 1$ для всех $i = 1, \dots, n$.
2. Можно построить такой полином $g(x_1, \dots, x_n) \in I(p^{m_0}, n)$,

$$g(x_1, \dots, x_n) = \sum_{\beta \leq \alpha} a_\beta X_\beta,$$

где $a_\alpha = 1$, $a_\beta \in E_{p^{m_0}}$, длина которого меньше $(mp)^m$.

Доказательство. 1. По малой теореме Ферма если p – простое число и $x \in E_p$, то $x^p = x \pmod{p}$. Поэтому для произвольного $s \geq 1$

$$u_s(x) = (x^p - x)^s \in I(p^s, 1), \quad \text{deg}(u_s) = sp.$$

Значит, при $m_i \geq 1$ верно $\text{cd}(x^{m_i p}) \geq m_i = \text{cd}(x^{a_i})$.

Отсюда при $m_i \geq 1$ получаем $a_i \leq m_i p$, и $a_i \leq mp - 1$.

При $m_i = 0$ по лемме 4.1 верно $a_i \leq p - 1$, и $a_i \leq mp - 1$.

2. Рассмотрим полином

$$g(x_1, \dots, x_n) = \prod_{i=1}^n g_i(x_i) \in I(p^{m_0}, n)$$

из доказательства леммы 4.4.

Т.к. $\text{deg}(g_i) = a_i$, то при $a_i > p - 1$ длина каждого из полиномов g_i не превышает a_i ($g_i(0) = 0$). И по п. 1 меньше mp .

Если $a_i \leq p - 1$, то пусть $g_i(x_i) = x_i^{a_i}$.

По условию леммы

$$\sum_{i=1}^n m_i = m_0 < m.$$

Отсюда, число координат a_i , больших $(p - 1)$, меньше m . Оценка длины полинома g получена. Следовательно, полином g – искомым.

Лемма 4.5 доказана. □

Следствие 4.2. [252] Пусть p – простое число, $m \geq 1$. Если функция $f(x_1, \dots, x_n) \in Pol_{p^m}$ и $c_\alpha \neq 0$ – коэффициент при мономе X_α , где $\alpha = (a_1, \dots, a_n) \in E_{p^m}^n$, в ее каноническом полиноме $P(f)$, то $\alpha \in E_{mp}$.

Пусть $k = p^m$, где p – простое число, $m \geq 2$ и $f(x_1, \dots, x_n) \in Pol_k$. Тогда найдутся такие коэффициенты $c_f(\alpha) \in E_k$, где $\alpha \in E_k^n$, что

$$P(f) = \sum_{\alpha \in E_k^n} c_f(\alpha) X_\alpha$$

ее канонический полином. Вектор значений функции $c_f(x_1, \dots, x_n) \in P_k^n$ назовем *вектором коэффициентов* канонического полинома функции $f(x_1, \dots, x_n)$. По следствию 4.2 это определение корректно.

Пусть $k = p^m$, где p – простое число, $m \geq 1$ и $1 \leq t \leq m$. Функции $f_1(x), f_2(x) \in P_k$ назовем p^t -эквивалентными, если $f_1(x) = f_2(x) \pmod{p^t}$.

Следующая теорема 4.2 является основной для построения алгоритма, распознающего полиномиальность функций k -значной логики.

Теорема 4.2. [252] Пусть $k = p^m$, где p – простое число, $m \geq 1$.

Пусть $f(y, x_1, \dots, x_n) \in P_k$, для каждого $j \in E_k$ функции $f_j(x_1, \dots, x_n) = f(j, x_1, \dots, x_n) \in Pol_k$ и их канонические полиномы $P(f_j)$ имеют вид

$$P(f_j) = \sum_{i=1}^l a_i^{(j)} X_i,$$

где X_l – наибольший (относительно линейного порядка $\preceq$) моном среди слагаемых всех полиномов $P(f_j)$, $j \in E_k$, $a_i^{(j)} \in E_k$, $i = 1, \dots, l$, $j \in E_k$.

Тогда функция $f(y, x_1, \dots, x_n) \in Pol_k$ тогда и только тогда, когда для функции $\psi_l(y)$, где $\psi_l(j) = a_l^{(j)}$, $j \in E_k$, найдется $p^{m-\text{cd}(X_l)}$ -эквивалентная ей функция $\xi_l(y) \in Pol_k^1$ и

$$f(y, x_1, \dots, x_n) - X_l \cdot \xi_l(y) \in Pol_k.$$

Доказательство. 1. Докажем необходимость. Пусть $f(y, x_1, \dots, x_n) \in Pol_k$. Рассмотрим ее канонический полином $P(f)$ (по теореме 4.1) и сгруппируем слагаемые так, чтобы получилось выражение вида

$$f(y, x_1, \dots, x_n) = \sum_{i=1}^l \varphi_i(y) \cdot X_i,$$

Пусть X_l – наибольший (относительно линейного порядка $\preceq$) моном среди всех мономов X_i в полученном выражении. Пусть

$$\varphi_l(y) = b_s y^s + \dots + b_1 y + b_0,$$

где $b_s, \dots, b_1, b_0 \in E_k$ – коэффициенты, $s \geq 0$.

Т.к. исходный полином функции $f(y, x_1, \dots, x_n)$ – канонический, получаем

$$b_i < p^{m-\text{cd}(y^i \cdot X_l)}$$

для всех $i = s, \dots, 1, 0$. А значит, в силу того, что $\text{cd}(y^i) \leq \text{cd}(y^i \cdot X_l)$, и

$$b_i < p^{m-\text{cd}(y^i)}.$$

Отсюда полином $\varphi_l(y)$ – канонический. Следовательно, он задает функцию, не равную тождественно нулю. Кроме того, полином

$$\varphi_l(y) = b_s y^s + \dots + b_1 y + b_0 \notin I(p^{m-\text{cd}(X_l)}, 1),$$

т.к. иначе полином функции $f(y, x_1, \dots, x_n)$ не являлся бы каноническим. В самом деле, если

$$\varphi_l(y) = b_s y^s + \dots + b_1 y + b_0 \in I(p^{m-\text{cd}(X_l)}, 1),$$

то рассмотрим полином $g(x_1, \dots, x_n) \in I(p^{\text{cd}(X_l)}, n)$, в котором среди всех его слагаемых моном X_l является наибольшим относительно частичного порядка $\leq$ и встречается с коэффициентом 1. Полином $g(x_1, \dots, x_n)$ существует по определению составной характеристики. Тогда полином

$$g_1(y, x_1, \dots, x_n) = \varphi_l(y) \cdot g(x_1, \dots, x_n) \in I(p^m, n+1),$$

наибольшим слагаемым (относительно линейного порядка $\preceq$) в нем является моном $y^s \cdot X_l$, и коэффициент при этом слагаемом равен b_s , причем $b_s < p^{m-\text{cd}(y^s \cdot X_l)}$. Но это противоречит следствию 4.1.

Поэтому моном X_l будет наибольшим (относительно линейного порядка $\preceq$) среди слагаемых всех канонических полиномов $f(j, x_1, \dots, x_n)$, $j \in E_k$.

Для каждого $j \in E_k$ канонический полином $f(j, x_1, \dots, x_n)$ может быть получен из полинома

$$f(j, x_1, \dots, x_n) = \sum_{i=1}^l \varphi_i(j) \cdot X_i$$

выполнением преобразований из доказательства теоремы 4.1. А именно, для слагаемого X_l из коэффициента при нем могут вычитаться числа, кратные $p^{m-\text{cd}(X_l)}$, до тех пор, пока он не станет меньше $p^{m-\text{cd}(X_l)}$. Поэтому

$$\psi_l(y) = \varphi_l(y) \pmod{p^{m-\text{cd}(X_l)}}.$$

Положим $\xi_l(y) = \varphi_l(y) \in \text{Pol}_k$. Тогда

$$f(y, x_1, \dots, x_n) - X_l \cdot \xi_l(y) \in \text{Pol}_k$$

как разность двух полиномиальных функций.

Необходимость обоснована.

2. Докажем достаточность. Пусть найдется такая функция $\xi_l(y) \in Pol_k^1$, что $\psi_l(y) = \xi_l(y) \pmod{p^{m-\text{cd}(X_l)}}$. Тогда

$$f(y, x_1, \dots, x_n) = (f(y, x_1, \dots, x_n) - X_l \cdot \xi_l(y)) + X_l \cdot \xi_l(y) \in Pol_k$$

как сумма двух полиномиальных функций.

Достаточность обоснована.

Теорема 4.2 доказана. □

Замечание 4.2. В условиях теоремы 4.2 условие каноничности полиномов для каждой подфункции $f_j(x_1, \dots, x_n) = f(j, x_1, \dots, x_n) \in Pol_k$ можно заменить требованием, чтобы они были представлены какими-то полиномами по модулю k , в которых для каждого слагаемого X верно $\text{cd}(X) < m$.

В самом деле, пусть подфункции $f_j(x_1, \dots, x_n)$, $j \in E_k$, представлены полиномами P_j ,

$$P_j = \sum_{i=1}^t c_i^{(j)} Y_i,$$

где Y_t – наибольший (относительно линейного порядка $\preceq$) моном среди слагаемых всех полиномов P_j , $j \in E_k$, $\text{cd}(Y_t) < m$, $c_i^{(j)} \in E_k$, $i = 1, \dots, t$, $j \in E_k$. Пусть $\psi'_t(j) = c_t^{(j)}$. Тогда $P_j - P(f_j) \in I(p^m, n)$.

1) Если $X_l \prec Y_t$, то по лемме 4.1 $c_t^{(j)} = 0 \pmod{p^{m-\text{cd}(Y_t)}}$. Значит, функция $\xi_t(y) = 0 \in Pol_k$ является $p^{m-\text{cd}(Y_t)}$ -эквивалентной полиномиальной функцией к функции $\psi'_t(y)$.

2) Если $X_l = Y_t$, то по лемме 4.1 $c_t^{(j)} = a_t^{(j)} \pmod{p^{m-\text{cd}(X_l)}}$. По теореме 4.2 найдется полиномиальная $p^{m-\text{cd}(X_l)}$ -эквивалентная функция $\xi_l(y) \in Pol_k$ к функции $\psi_l(y)$. Значит, $\xi_l(y) \in Pol_k$ является $p^{m-\text{cd}(X_l)}$ -эквивалентной функцией и к функции $\psi'_t(y)$.

Замечание 4.3. Пусть $k = p^m$, где p – простое число, $m \geq 1$. В условиях теоремы 4.2 если наибольший моном X_l таков, что $\text{cd}(X_l) = 0$, то условие существования $p^{m-\text{cd}(X_l)}$ -эквивалентной к $\psi_l(y)$ функции из Pol_k меняется на условие $\psi_l(y) \in Pol_k$.

Замечание 4.4. Теорема 4.2 предлагает идею построения алгоритма распознавания полиномиальности функций. Рассмотрим подробнее достаточность в этой теореме. В условиях теоремы $\xi_l(y) - \psi_l(y) = 0 \pmod{p^{m-\text{cd}(X_l)}}$. По определению составной характеристики $\text{cd}(X_l)$ найдется полином

$$g(x_1, \dots, x_n) = X_l + g_1(x_1, \dots, x_n) \in I(p^{\text{cd}(X_l)}, n),$$

причем в полиноме g_1 все мономы меньше (относительно частичного порядка $\leq$) монома X_l . Тогда

$$\begin{aligned} & (\xi_l(y) - \psi_l(y)) \cdot g(x_1, \dots, x_n) = \\ & = (\xi_l(y) - \psi_l(y)) \cdot (X_l + g_1(x_1, \dots, x_n)) = 0 \pmod{p^m}. \end{aligned}$$

Заметим, что

$$f(y, x_1, \dots, x_n) = \sum_{i=1}^l \psi_i(y) \cdot X_i,$$

где функции $\psi_i(y)$ не обязательно полиномиальны. Тогда

$$\begin{aligned} f(y, x_1, \dots, x_n) & = f(y, x_1, \dots, x_n) + (\xi_l(y) - \psi_l(y)) \cdot g(x_1, \dots, x_n) = \\ & = \sum_{i=1}^l \psi_i(y) \cdot X_i + (\xi_l(y) - \psi_l(y)) \cdot (X_l + g_1(x_1, \dots, x_n)) = \\ & = \xi_l(y) \cdot X_l + \sum_{i=1}^{l-1} \psi_i(y) \cdot X_i + (\xi_l(y) - \psi_l(y)) \cdot g_1(x_1, \dots, x_n). \end{aligned}$$

Отсюда следует, что канонические полиномы всех подфункций по переменной y функции

$$f(y, x_1, \dots, x_n) - X_l \cdot \xi_l(y)$$

содержат только мономы, меньшие (относительно линейного порядка $\preceq$) чем моном X_l . А значит, мы можем рекурсивно применить к ней эту же теорему 4.2.

В качестве алгоритмической модели рассмотрим схемы из функциональных элементов (СФЭ) в некотором полном в P_k базисе. Под сложностью алгоритма будем понимать число функциональных элементов в соответствующей СФЭ.

Теорема 4.3. [252] Пусть $k = p^m$, где p – простое число, $m \geq 2$, $B \subseteq P_k$ – полная система множества P_k .

Существует последовательность СФЭ S_n , $n = 1, 2, \dots$, в базисе B с k^n входами $u(\alpha)$, $\alpha \in E_k^n$, и $k^n + 1$ выходами $v(\alpha)$, $\alpha \in E_k^n$, и z , такая, что если на входы $u(\alpha)$ подаются значения $f(\alpha)$, $\alpha \in E_k^n$, произвольной функции k -значной логики $f(x_1, \dots, x_n)$, то на выходе z появляется 1, если $f \in Pol_k$, на выходе z появляется 0, если $f \notin Pol_k$, в случае $z = 1$ на выходах $v(\alpha)$ появляются значения коэффициентов $c_\alpha(f)$, $\alpha \in E_k^n$, канонического полинома $P(f)$ функции f , и $L(S_n) = O(N)$, где $N = k^n$ – длина вектора значений функции f .

Доказательство. Опишем алгоритм, который для произвольной функции $f \in P_k^n$ по вектору ее значений определяет, является ли она полиномиальной, и в случае положительного ответа, строит вектор коэффициентов ее канонического полинома. По этому алгоритму можно построить требуемую последовательность СФЭ S_n .

В описании знак “:=” означает “присваивание”, т.е. переменной, находящейся слева от этого знака, надо присвоить значение выражения, находящегося справа от знака. Кроме операций сложения, вычитания, умножения, деления (когда это возможно) по модулю k , будем применять следующие

операции: $\min(x, y)$ – нахождение минимального из двух элементов из множества E_k ; mod – взятия остатка левого операнда по модулю правого операнда, причем операнды из множества E_k . Заметим, что все эти операции можно реализовать СФЭ в базисе B с константной сложностью. Если $j \in E_k$, $\alpha = (a_1, \dots, a_n) \in E_k^n$, то

$$(j, \alpha) = (j, a_1, \dots, a_n) \in E_k^{n+1}.$$

Алгоритм опишем индуктивно.

Базис индукции: $n = 1$. В этом случае в СФЭ S_1 будет содержаться информация о всех функциях из множества Pol_k^1 и об их канонических полиномах. Если на входы поступают значения функции $f(x_1)$, то в СФЭ S_1 сравниваются эти значения со всеми полиномиальными функциями. Если находится совпадающая полиномиальная функция, то на выход z выдается 1, и на оставшиеся выходы выдаются коэффициенты канонического полинома $P(f)$. Если не находится совпадающая полиномиальная функция, то на все выходы СФЭ S_1 выдаются 0. Сложность СФЭ S_1 будет константной.

Индуктивный переход. Пусть СФЭ S_n уже построена. Опишем, как построить СФЭ S_{n+1} . На входы СФЭ S_{n+1} будут подаваться значения функции $f(y, x_1, \dots, x_n) \in P_k^{n+1}$. Пусть

$$f_j(x_1, \dots, x_n) = f(j, x_1, \dots, x_n),$$

где $j \in E_k$.

Построение СФЭ S_{n+1} опишем по шагам.

Шаг 1. Проверка полиномиальности всех подфункций функции f .

Возьмем k уже построенных СФЭ S_n , которые обозначим $S_{n,0}, S_{n,1}, \dots, S_{n,(k-1)}$. Их входы обозначим соответственно $u(j, \alpha)$, $\alpha \in E_k^n$, $j \in E_k$, эти входы являются входами СФЭ S_{n+1} . Выходы СФЭ $S_{n,0}, S_{n,1}, \dots, S_{n,(k-1)}$ обозначим соответственно $v_j(\alpha)$, $\alpha \in E_k^n$, и z_j , $j \in E_k$

Итак, $z_j = 1$, если $f_j \in Pol_k^n$, и $z_j = 0$, иначе, и

$$v_j(\alpha) = \begin{cases} c_{f_j}(\alpha), & z_j = 1, \\ 0, & z_j = 0, \end{cases}$$

для всех $j \in E_k$, $\alpha = (a_1, \dots, a_n) \in E_k^n$.

Введем переменные z , $v(j, \alpha)$, $j \in E_k$, $\alpha \in E_k^n$, и положим

$$z := \min_{0 \leq j \leq k-1} z_j,$$

и

$$v(j, \alpha) := v_j(\alpha)$$

для всех значений j , α .

Шаг 2. Построение полиномиальных функций по переменной y для функции f (по теореме 4.2 и замечанию 4.2).

Из шага 1 следует, что в переменных $v(j, \gamma)$, $\gamma \in E_k^n$ записаны коэффициенты канонический полиномов подфункций $f(j, x_1, \dots, x_n)$, $j \in E_k$, функции $f(y, x_1, \dots, x_n)$ (если какая-то из подфункций не является полиномиальной, то в соответствующих ей переменных записаны нули).

Для всех наборов $\alpha = (a_1, \dots, a_n) \in E_{mp}^n$ повторяем для всех мономов X_α , $cd(X_\alpha) < m$, начиная с наибольшего относительно линейного порядка $\preceq$ и по убыванию относительно этого порядка, следующие операции.

Пусть сейчас мы рассматриваем моном X_α , $\alpha = (a_1, \dots, a_n) \in E_{mp}^n$.

По значениям переменных $v(j, \alpha)$, $j \in E_k$, определим функцию

$$\psi(j) = v(j, \alpha), \quad j \in E_k.$$

Введем переменную z_α и положим $z_\alpha := 1$, если найдется $p^{m-cd(X_\alpha)}$ -эквивалентная функция из Pol_k к функции $\psi(y)$, и $z_\alpha := 0$, иначе. Для того, чтобы определить значение переменной z_α мы обратимся к списку всех полиномиальных функций Pol_k^1 и проверим наличие в нем соответствующей

$p^{m-\text{cd}(X_\alpha)}$ -эквивалентной функции для функции $\psi(y)$. Сложность СФЭ, находящей значение переменной z_α таким образом константна.

Положим

$$z := \min(z, z_\alpha),$$

и для всех $j \in E_k$

$$v(j, \alpha) := \begin{cases} c_\xi(j), & z_\alpha = 1, \\ 0, & z_\alpha = 0, \end{cases}$$

где $\xi(y)$ есть $p^{m-\text{cd}(X_\alpha)}$ -эквивалентная функция из Pol_k к функции $\psi(y)$.

По лемме 4.5 и найдется полином

$$g_\alpha(x_1, \dots, x_n) = X_\alpha + \sum_{i=1}^l b_i X_{\beta_i} \in I(p^{\text{cd}(X_\alpha)}, n),$$

где X_α – наибольший моном относительно частичного порядка $\leq$ среди всех его слагаемых и для длины l которого верно $l \leq (mp)^m$.

Положим

$$v(j, \beta_i) := v(j, \beta_i) + (\xi(j) - \psi(j)) \cdot b_i,$$

где $j \in E_k$, $i = 1, \dots, l$ (см. замечание 4.4). Сложность СФЭ, вычисляющей значения всех переменных $v(j, \beta_i)$, $j \in E_k$, $i = 1, \dots, l$, $l \leq (mp)^m$, константна.

Шаг 3. Приведение полученного полинома функции f к каноническому виду (по теореме 4.1).

Для всех значений $j \in E_k$ для всех наборов $\alpha = (a_1, \dots, a_n) \in E_{mp}^n$ повторяем для всех мономов X_γ , где

$$\gamma = (j, \alpha) \in E_k \times E_{mp}^n,$$

начиная с наибольшего относительно линейного порядка $\preceq$ и по убыванию относительно этого порядка, следующие операции.

Пусть X_γ – рассматриваемый моном.

1) Пусть $\text{cd}(X_\gamma) = m$, а $\text{cd}(X_\alpha) < m$. Тогда $\text{cd}(y^j) \geq m - \text{cd}(X_\alpha)$, т.к. если $\text{cd}(y^j) < m - \text{cd}(X_\alpha)$, то $\text{cd}(y^j) + \text{cd}(X_\alpha) < m$, и $\text{cd}(X_\gamma) < m$, что не так.

По лемме 4.5 найдется полином

$$g_\alpha(x_1, \dots, x_n) \in I(p^{\text{cd}(X_\alpha)}, n),$$

в котором моном X_α – наибольший относительно частичного порядка $\leq$ среди всех его слагаемых и длина полинома g не больше $(mp)^m$.

По определению составной характеристики найдется полином

$$g_j(y) \in I(p^{\text{cd}(y^j)}, 1), \text{ deg}(g_j) = j,$$

в котором коэффициент при мономе y^j равен 1.

Тогда полином

$$g_\gamma(y, x_1, \dots, x_n) = g_j(y) \cdot g_\alpha(x_1, \dots, x_n) \in I(p^m, n + 1)$$

и его длина не больше $j \cdot (mp)^m \leq p^m (mp)^m$.

Пусть

$$g_\gamma(y, x_1, \dots, x_n) = X_\gamma + \sum_{i=1}^l d_i X_{\gamma_i},$$

в котором моном X_γ – наибольший относительно частичного порядка $\leq$ среди всех его слагаемых.

Положим

$$v(\gamma_i) := v(\gamma_i) - v(\gamma) \cdot d_i,$$

где $i = 1, \dots, l$, и

$$v(\gamma) := 0$$

Сложность СФЭ, вычисляющей значения всех переменных $v(\gamma_i)$, $i = 1, \dots, l$, $l \leq p^m (mp)^m$, константна.

2) Пусть $\text{cd}(X_\gamma) < m$.

По лемме 4.5 найдется полином

$$g_\gamma(x_1, \dots, x_n) = X_\gamma + \sum_{i=1}^l d_i X_{\gamma_i} \in I(p^{\text{cd}(X_\gamma)}, n),$$

в котором моном X_γ – наибольший относительно частичного порядка $\leq$ среди всех его слагаемых и для длины l которого верно $l \leq (mp)^m$.

Положим

$$v(\gamma_i) := v(\gamma_i) - (v(\gamma) - (v(\gamma) \bmod p^{m-\text{cd}(X_\gamma)})) \cdot d_i,$$

где $i = 1, \dots, l$, и

$$v(\gamma) := v(\gamma) \bmod p^{m-\text{cd}(X_\gamma)}.$$

Сложность СФЭ, вычисляющей значения всех переменных $v(\gamma_i)$, $i = 1, \dots, l$, $l \leq (mp)^m$, константна.

Описание алгоритма закончено. Теперь $z = 1$, если $f \in Pol_k$, и $z = 0$, иначе. Кроме того, если $z = 1$, то $v(\gamma) = c_f(\gamma)$, где $\gamma \in E_k^{n+1}$. Правильность описанного алгоритма следует из теоремы 4.2 и замечания 4.4.

Оценим сложность предложенного алгоритма. Итак, СФЭ S_1 можно построить с константной сложностью $L(S_1)$. Пусть $S_n^{(1)}$, $S_n^{(2)}$, $S_n^{(3)}$ – СФЭ, реализующие соответственно шаги 1, 2, 3 алгоритма, описанного в индуктивном переходе. Тогда для их сложностей $L(S_n^{(i)})$, $i = 1, 2, 3$, верно:

$$L(S_n^{(1)}) \leq kL(S_n) + C_1,$$

где $C_1 > 0$ – некоторая константа, т.к. СФЭ $S_n^{(1)}$ содержит k схем $S_{n,j}$, $j \in E_k$, построенных по индуктивному предположению, и вычисление значения переменной z ,

$$L(S_n^{(2)}) \leq C_2(mp)^n,$$

где $C_2 > 0$ – некоторая константа, т.к. в СФЭ $S_n^{(2)}$ требуется не более, чем для $(mp)^n$ мономов X_α выполнить константное число операций,

$$L(S_n^{(3)}) \leq C_3 k(mp)^n,$$

где $C_3 > 0$ – некоторая константа, т.к. в СФЭ $S_n^{(3)}$ требуется не более, чем для $k(mp)^n$ мономов X_γ выполнить константное число операций.

Тогда для сложности $L(S_{n+1})$ СФЭ S_{n+1} , которая является последовательным соединением СФЭ $S_n^{(1)}$, $S_n^{(2)}$, $S_n^{(3)}$ с согласованием входов и выходов, верно

$$\begin{aligned} L(S_{n+1}) &\leq L(S_n^{(1)}) + L(S_n^{(2)}) + L(S_n^{(3)}) \leq kL(S_n) + C_4(mp)^n \leq \\ &\leq k(kL(S_{n-1}) + C_4(mp)^{n-1}) + C_4(mp)^n \leq \dots \leq \\ &\leq k^n L(S_1) + C_4(k^{n-1}(mp) + \dots + (mp)^n) \leq \\ &\leq Ck^n \left(\sum_{i=1}^n \left(\frac{mp}{p^m} \right)^i \right) \end{aligned}$$

где $C_4, C > 0$ – некоторые константы.

Если $k > 4$, то $mp < p^m$. И выражение, стоящее в скобках, можно ограничить суммой соответствующей бесконечно убывающей геометрической прогрессии. Отсюда $L(S_n) = O(N)$ при $k > 4$.

В случае, когда $mp = p^m$, т.е. при $k = 4$, проведем дополнительные исследования. Заметим, что

$$(x^2 + x)(y^2 + y) \in I(2^2, 2).$$

Поэтому, если в мономе X не менее двух переменных в степенях, больших единицы, то $\text{cd}(X) \geq 2$ (по отношению к простому числу $p = 2$ и $m \geq 2$).

Следовательно, на шагах 2 и 3 можно рассматривать только наборы

$$\alpha = (a_1, \dots, a_n) \in E_4^n,$$

в которых не более одной координаты, большей 1. Всего таких наборов

$$2^n + 2n2^{n-1} \leq C_6n2^n,$$

где $C_6 > 0$ – некоторая константа.

Тогда

$$\begin{aligned}
L(S_{n+1}) &\leq L(S_n^1) + L(S_n^2) + L(S_n^3) \leq 4L(S_n) + C_7 n 2^n \leq \\
&\leq 4(4L(S_{n-1}) + C_7(n-1)2^{n-1}) + C_7 n 2^n \leq \dots \leq \\
&\leq 4^n L(S_1) + C_7(4^{n-1}2 + \dots + n2^n) \leq \\
&\leq C4^n \left(\sum_{i=0}^n i \left(\frac{1}{2}\right)^i \right)
\end{aligned}$$

где $C_7, C > 0$ – некоторые константы.

Выражение, стоящее в скобках, можно ограничить суммой соответствующего бесконечного сходящегося ряда. Отсюда $L(S_n) = O(N)$ при $k = 4$.

Следовательно, $L(S_n) = O(N)$, если $k = p^m$, где p – простое число, $m \geq 2$.

Теорема 4.3 доказана. $\square$

Замечание 4.5. В [257] показано, что т.к. функция $2 \cdot j_0(x) \in Pol_4$, при $k = 4$ в теореме 4.2 условие существования $p^{m-\text{cd}(X_l)}$ -эквивалентной функции из Pol_4 для функции $\psi_l(y)$ можно заменить на условие $\psi_l(y) \in Pol_4$. Поэтому алгоритм из теоремы 4.3 при $k = 4$ становится несколько проще.

Пример 4.1. Рассмотрим функцию $f(x, y) \in P_4$ и применим к ней алгоритм из теоремы 4.3 с учетом замечания 4.5.

x	0 0 0 0	1 1 1 1	2 2 2 2	3 3 3 3
y	0 1 2 3	0 1 2 3	0 1 2 3	0 1 2 3
f	3 3 3 3	0 3 2 1	3 3 3 3	2 1 0 3

Тогда

$$f(3, y) = 3y + 2,$$

$$f(2, y) = 3,$$

$$f(1, y) = 3y,$$

$$f(0, y) = 3.$$

Получаем функции $\psi_i(x)$, $i = 3, 2, 1, 0$, для которых надо проверить условие $\psi_i(x) \in Pol_4$. Запишем функции $\psi_i(x)$, $i = 3, 2, 1, 0$, в таблицу:

x	ψ_3	ψ_2	ψ_1	ψ_0
0	0	0	0	3
1	0	0	3	0
2	0	0	0	3
3	0	0	3	2

Получаем, что все $\psi_i \in Pol_4$, причем $\psi_3(x) = \psi_2(x) = 0$, $\psi_1(x) = x^2 + 2x$, $\psi_0(x) = x^3 + 3$. Отсюда находим

x	0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3
y	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
c_f	3	0	0	1	0	2	1	0	0	0	0	0	0	0	0	0

и получаем полином по модулю 4 для функции $f(x, y)$:

$$f(x, y) = 3 + 2xy + x^2y + x^3.$$

Он уже записан в каноническом виде.

Пример 4.2. Рассмотрим другую функцию $f(x, y) \in P_4$ и применим к ней алгоритм из теоремы 4.3 с учетом замечания 4.5.

x	0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3
y	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
f	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Тогда

$$f(3, y) = 0,$$

$$f(2, y) = 0,$$

$$f(1, y) = 0,$$

$$f(0, y) = y^3 + y + 2.$$

Получаем функции $\psi_i(x)$, $i = 3, 2, 1, 0$, для которых надо проверить условие $\psi_i(x) \in Pol_4$. Запишем функции $\psi_i(x)$, $i = 3, 2, 1, 0$, в таблицу:

x	ψ_3	ψ_2	ψ_1	ψ_0
0	1	0	1	2
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0

Для функции $\psi_3(x)$ верно $\psi_3(x) \notin Pol_4$ (в таблице эта функция выделена жирным шрифтом). Отсюда получаем, что $f(x, y) \notin Pol_4$.

Теперь рассмотрим общий случай, т.е. когда k – произвольное составное число.

Теорема 4.4. [261] Пусть k – составное число, $B \subseteq P_k$ – полная система множества P_k .

Существует последовательность СФЭ S_n , $n = 1, 2, \dots$, в базисе B с k^n входами $u(\alpha)$, $\alpha \in E_k^n$, и $k^n + 1$ выходами $v(\alpha)$, $\alpha \in E_k^n$, и z , такая, что если на входы $u(\alpha)$ СФЭ S_n поступают значения $f(\alpha)$ произвольной функции k -значной логики, то на выходе z появляется 1, если $f \in Pol_k$, на выходе z появляется 0, если $f \notin Pol_k$, в случае $z = 1$ на выходах $v(\alpha)$, $\alpha \in E_k^n$, появляются значения коэффициентов $c(\alpha)$ при мономах X_α в каком-то полиноме по модулю k , задающего функцию f , и $L(S_n) = O(N)$, где $N = k^n$ – длина вектора значений функции f .

Доказательство. Опишем алгоритм, который для произвольной функции $f \in P_k^n$ по вектору ее $N = k^n$ значений определяет, является ли функция f полиномиальной, и в случае положительного ответа строит какой-то ее полином. По приведенному описанию несложно построить соответствующую СФЭ S_n .

Пусть k – составное число, $k = p_1^{m_1} \cdot \dots \cdot p_r^{m_r}$, где p_i – попарно различные простые числа, $m_i \geq 1$.

Если $r = 1$, т.е. $k = p^m$, где p – простое число, $m \geq 2$, то применим алгоритм из теоремы 4.3.

Пусть $r \geq 2$. Тогда кольцо $\mathbb{Z}_k$ вычетов по модулю k есть прямая сумма идеалов, изоморфных кольцам $\mathbb{Z}_{p_i^{m_i}}$ вычетов по модулю $p_i^{m_i}$, $i = 1, \dots, r$ [204]. Опишем алгоритм по шагам, опираясь на этот факт.

Шаг 1. Пусть $d_i = p_i^{m_i}$, $i = 1, \dots, r$.

Пусть $\alpha = (a_1, \dots, a_n) \in E_k^n$ и $\beta = (b_1, \dots, b_n) \in E_k^n$. Будем говорить, что наборы α и β сравнимы по модулю d_i и обозначать $\alpha = \beta \pmod{d_i}$, если

$$a_1 = b_1 \pmod{d_i}, \dots, a_n = b_n \pmod{d_i}.$$

По свойствам полиномов над кольцами вычетов по модулю k если функция $f(x_1, \dots, x_n)$ принадлежит множеству Pol_k , то для любых наборов α, β из E_k^n из $\alpha = \beta \pmod{d_i}$ следует $f(\alpha) = f(\beta) \pmod{d_i}$ [5, 108].

Выполним проверку этого необходимого условия полиномиальности для функции $f(x_1, \dots, x_n)$. Для этого для каждого i , $i = 1, \dots, r$, сравниваем значения функции f на наборах из множества E_k^n , сравнимых по модулю $p_i^{m_i}$. Т.к. сравнимость наборов по модулю $p_i^{m_i}$ задает отношение эквивалентности на множестве E_k^n , то проверку для каждого i можно выполнить со сложностью $O(N)$. Значит, сложность шага 1 будет также $O(N)$.

Если хотя бы однажды условие не выполняется, то $f \notin Pol_k$. Иначе, переходим к шагу 2.

Шаг 2. По китайской теореме об остатках сопоставим каждому элементу $a \in E_k$ однозначный набор $(a_1, \dots, a_r) \in E_{p_1^{m_1}} \times \dots \times E_{p_r^{m_r}}$, являющийся решением системы сравнений

$$a = a_1 \pmod{p_1^{m_1}}, \dots, a = a_r \pmod{p_r^{m_r}}.$$

В силу выполненного условия шага 1 функции $f(x_1, \dots, x_n) \in P_k^n$ сопоставим набор функций $(f_1, \dots, f_r) \in P_{p_1}^n \times \dots \times P_{p_r}^n$.

Теперь для каждого i , $i = 1, \dots, r$, проверим, задается ли функция $f_i(x_1, \dots, x_n) \in P_{p_i}^n$ полиномом по модулю $p_i^{m_i}$ и в случае положительного ответа найдем какой-то ее полином.

Применим известные алгоритмы. Если $m_i = 1$, то применим алгоритмы построения полиномов при простых p_i , а именно, если $p_i = 2$, то алгоритм из [205], если $p_i \neq 2$, то алгоритм, предложенный Ю.В. Таранниковым (устное сообщение) или алгоритм из [248]. Получим вектор коэффициентов c_{f_i} полинома функции f_i со сложностью $O(p_i^{m_i n})$. Если $m_i \geq 2$, то применим алгоритм распознавания полиномиальности и построения полиномов при составных $p_i^{m_i}$ (теорема 4.3). Если $f_i \notin \text{Pol}_{p_i^{m_i}}$, то $f \notin \text{Pol}_k$. Иначе, получим вектор коэффициентов c_{f_i} канонического полинома функции f_i со сложностью $O(p_i^{m_i n})$.

Сложность шага 2 равна $O(N)$.

Шаг 3. Если все функции f_i – полиномиальны (каждая по своему модулю), то по китайской теореме об остатках по набору коэффициентов $c_1 \in E_{p_1^{m_1}}, \dots, c_r \in E_{p_r^{m_r}}$ при мономе X в полиномах функций $f_1, \dots, f_r$ соответственно найдем коэффициент $c \in E_k$ при мономе X в полиноме функции f , являющийся решением системы сравнений:

$$c = c_1 \pmod{p_1^{m_1}}, \dots, c = c_r \pmod{p_r^{m_r}}.$$

Выполнить шаг 3 можно со сложностью $O(N)$.

По приведенному описанию алгоритма можно построить соответствующую СФЭ S_n , причем $L(S_n) = O(N)$, где $N = k^n$.

Теорема 4.4 доказана. □

Отметим, что при распознавании полиномиальности важны все значения

исходной функции $f(x_1, \dots, x_n)$, т.к. можно найти неполиномиальную функцию, отличающуюся от полиномиальной только на одном наборе значений переменных. Отсюда заключаем, что в алгоритмической модели СФЭ при каждом фиксированном составном k алгоритмическая сложность задачи распознавания полиномиальности функций k -значной логики по вектору их $N = k^n$ значений линейна.

Рассмотрим примеры применения алгоритма из теоремы 4.4.

Пример 4.3. Рассмотрим $f(x) \in P_{12}$:

x	0	1	2	3	4	5	6	7	8	9	10	11
f	0	10	9	3	4	6	9	7	0	6	1	3

Заметим, что $12 = 3 \cdot 2^2$.

Рассмотрим $d_1 = 3$. Для удобства в таблице наборы значений переменной x , сравнимые по модулю d_1 , и соответствующие им значения функции f выделим разными шрифтами. Тогда

x	0	1	2	3	4	5	6	7	8	9	10	11
f	0	10	9	3	4	6	9	7	0	6	1	3

и

x	0	1	2
f_1	0	1	0

При $d_2 = 4$ получаем:

x	0	1	2	3	4	5	6	7	8	9	10	11
f	0	10	9	3	4	6	9	7	0	6	1	3

и

x	0	1	2	3
f_2	0	2	1	3

Тогда $f_1(x) = 2x^2 + 2x$, $f_2(x) \notin \text{Pol}_4$. Отсюда $f(x) \notin \text{Pol}_{12}$.

Пример 4.4. Рассмотрим $g(x) \in P_{12}$:

x	0	1	2	3	4	5	6	7	8	9	10	11
g	0	7	6	9	4	3	6	1	0	3	10	9

Заметим, что $12 = 3 \cdot 2^2$.

При $d_1 = 3$ получаем:

x	0	1	2	3	4	5	6	7	8	9	10	11
f	0	7	6	9	4	3	6	1	0	3	10	9

и

x	0	1	2
f_1	0	1	0

При $d_2 = 4$ получаем:

x	0	1	2	3	4	5	6	7	8	9	10	11
f	0	7	6	9	4	3	6	1	0	3	10	9

и

x	0	1	2	3
f_2	0	2	1	3

Тогда $g_1(x) = 2x^2 + 2x$, $g_2(x) = 3x$, и $g(x) = 8x^2 + 11x$.

Теперь обратимся к случаю, когда k – простое число. Мы исследуем сложность построения полинома Жегалкина функции алгебры логики в алгоритмической модели СФЭ с некоторыми ограничениями их структуры. А именно, мы докажем достижимую нижнюю оценку этой сложности в классе СФЭ с разделенными переменными.

СФЭ S с входами $x_1, \dots, x_n$ и выходами $y_1, \dots, y_m$ называется *схемой с разделенными переменными* (СФЭРП), если для любых i и j ориентированный путь от входа x_i к выходу y_j существует только в том случае, когда реализующаяся на выходе y_j функция *существенно* зависит от переменной x_i . Отметим, что разделенность переменных – существенное свойство схем. К.А. Зыковым [66] найдено семейство множеств линейных функций, которые в классе схем с разделенными переменными имеют большую сложность, чем в классе схем без ограничений.

Пусть v – вершина в СФЭ $S(x_1, \dots, x_n; y_1, \dots, y_m)$. Рассмотрим все ориентированные пути из входов $x_1, \dots, x_n$ в вершину v . Пусть V' и E' – множества вершин и дуг, принадлежащих этим путям, $G' = (V', E')$ – соответствующий

граф, и $S'(x_{i_1}, \dots, x_{i_r}; v)$ – соответствующая СФЭ на графе G' с одним выходом v . Назовем эту СФЭ $S'(x_{i_1}, \dots, x_{i_r}; v)$ *кустом*, растущим из вершины v .

В [205] (1-е изд. 1977 г., стр. 35; 3-е изд. 2004 г., стр. 53) описан алгоритм построения по вектору значений функции алгебры логики ее полинома Жегалкина. Этот алгоритм реализуется СФЭРП в базисе $B_{L_0} = \{x \oplus y\}$ со сложностью $n \cdot 2^{n-1}$. Мы докажем, что этот алгоритм является оптимальным для задачи построения полинома Жегалкина в классе СФЭРП. Отметим, что в [149, 167] также доказана оптимальность этого алгоритма в моделях СФЭ с ограничениями. Отметим, что мы применяем другую технику доказательств.

Известно [213], что для каждой функции алгебры логики $f(x_1, \dots, x_n) \in P_2^n$ каждый коэффициент $c_f(\alpha)$, $\alpha \in E_2^n$, ее полинома Жегалкина может быть найден по формуле

$$c_f(\alpha) = \bigoplus_{\beta \leq \alpha} f(\beta).$$

Обозначим как Π_n систему из 2^n линейных функций алгебры логики $v(\alpha)$, $\alpha \in E_2^n$, зависящих от переменных $u(\alpha)$, $\alpha \in E_2^n$:

$$\Pi_n = \left\{ v(\alpha) = \bigoplus_{\beta \leq \alpha} u(\beta) \mid \alpha \in E_2^n \right\}.$$

Обозначим как $L_B^{\text{СФЭРП}}(\Pi_n)$ наименьшую сложность среди всех СФЭРП в базисе B , $B \subseteq P_2$, реализующих систему Π_n .

Для доказательств нам будет нужна вспомогательная лемма.

Лемма 4.6. [256] *Если $\alpha, \beta \in E_2^n$, $\alpha \neq \beta$, то*

$$|(\{\alpha\} \cup \check{S}(\alpha)) \cap (\{\beta\} \cup \check{S}(\beta))| \leq 1.$$

Доказательство. Действительно, если наборы α и β из разных слоев куба E_2^n , то в пересечении указанных множеств может быть не более одного элемента (если один из наборов лежит в тени другого). Если наборы α и β из

одного и того же слоя куба E_2^n , то в пересечении их теней также не более одного элемента. Это следует из того, что их тени из одного слоя, а наборы одного слоя различаются не менее, чем в двух координатах.

Лемма 4.6 доказана. □

Теперь докажем теорему 4.5.

Теорема 4.5. [256] *В базисе $B_{L_0} = \{x \oplus y\}$ верно $L_{B_{L_0}}^{C\Phi\mathcal{E}P\Pi}(\Pi_n) \geq n \cdot 2^{n-1}$.*

Доказательство. Пусть нам задана какая-то СФЭРП S_n в базисе B_{L_0} , реализующая систему Π_n .

Докажем, что в СФЭРП S_n каждому такому набору $\alpha \in E_2^n$, что $1 \leq |\alpha| \leq n$, можно сопоставить не менее $|\alpha|$ элементов сложения по модулю 2, причем так, что для разных наборов α и β соответствующие им множества элементов не пересекаются, и если v соответствует набору α , то из этого элемента s найдется ориентированный путь в выход $v(\alpha)$. Доказывать это утверждение будем индукцией по весу наборов t , $1 \leq t \leq n$.

Базис индукции: $t = 1$. Пусть $\alpha \in E_2^n$, и $|\alpha| = 1$. Рассмотрим в СФЭРП S_n куст, растущий из выхода $v(\alpha)$. На выходе $v(\alpha)$ реализуется функция $f(0, \dots, 0) \oplus f(\alpha)$, поэтому этот куст содержит хотя бы один элемент сложения по модулю два. Припишем выходному элементу этого куста пометку α . Ясно, что если $\alpha \neq \beta$, $|\alpha| = |\beta| = 1$, то пометки α и β будут приписаны разным элементам.

Индуктивный переход от $t - 1$ к t , $2 \leq t \leq n$. Пусть в СФЭРП S_n каждому такому набору $\beta \in E_2^n$, что $1 \leq |\beta| \leq t - 1$, сопоставлено не менее $|\beta|$ элементов сложения по модулю 2, причем множества элементов, сопоставленных разным наборам, не пересекаются, и если элемент s сопоставлен набору β , то из этого элемента s найдется ориентированный путь в выходную вершину $v(\beta)$.

Преобразуем СФЭРП S_n : подадим на все входы $u(\beta)$, $|\beta| \leq t-2$ значение 0. Рассмотрим в СФЭРП S_n произвольный элемент s , которому сопоставлен набор β , где $1 \leq |\beta| \leq t-2$. Из элемента s есть ориентированный путь в выход $v(\beta)$, поэтому в элемент s могут вести ориентированные пути только из входов, на которые поданы 0. Преобразуем СФЭРП S_n по правилам алгебры логики $0 \oplus x = x$, $0 \oplus 0 = 0$ до тех пор, пока это возможно. При этом мы удалим все входы $u(\beta)$, $|\beta| \leq t-2$, все вершины, хотя бы на один вход которых пришел 0, и все выходы $v(\beta)$, $|\beta| \leq t-2$ (на каждом из таких выходов реализуется функция, тождественно равная нулю). Отметим также, что при этом удалятся все элементы, которым были сопоставлены наборы β , где $1 \leq |\beta| \leq t-2$, т.к. в эти элементы вели ориентированные пути только от входов, которым мы приписали 0. Обозначим полученную СФЭРП с входами $u(\alpha)$, $|\alpha| \geq t-1$, и выходами $v(\alpha)$, $|\alpha| \geq t-1$, как $\hat{S}_n^{(t)}$.

Итак, в СФЭРП $\hat{S}_n^{(t)}$ нет элементов сложения по модулю 2, сопоставленных наборам β , где $1 \leq |\beta| \leq t-2$. Но в СФЭРП $\hat{S}_n^{(t)}$ могут быть элементы, сопоставленные каким-то наборам β , $|\beta| = t-1$. Рассмотрим такой элемент s . Пусть он сопоставлен набору β . Рассмотрим выход $v(\beta)$, $|\beta| = t-1$. На нем реализуется тождественная функция $u(\beta)$. Из элемента s есть ориентированный путь в выход $v(\beta)$. Поэтому, в силу разделенности переменных СФЭРП $\hat{S}_n^{(t)}$, в элемент s могут вести ориентированные пути только из входа $u(\beta)$. Поэтому элемент s можно удалить без ущерба для функционирования СФЭРП и не увеличивая ее сложность. Таким образом, мы удалим все элементы, сопоставленные наборам β , $|\beta| = t-1$.

Обозначим полученную СФЭРП с входами $u(\alpha)$, $|\alpha| \geq t-1$, и выходами $v(\alpha)$, $|\alpha| \geq t-1$, как $S_n^{(t)}$. Заметим, что по построению в СФЭРП $S_n^{(t)}$ нет элементов сложения по модулю 2, сопоставленных наборам β , $1 \leq |\beta| \leq t-1$.

Пусть $|\alpha| = t$. Рассмотрим в СФЭРП $S_n^{(t)}$ куст, растущий из выхода $v(\alpha)$.

На выходе $v(\alpha)$ реализуется функция $u(\alpha) \oplus \bigoplus_{\beta \in \check{S}(\alpha)} u(\beta)$, поэтому этот куст содержит не менее t элементов сложения по модулю два в силу существенности всех переменных этой функции алгебры логики. Припишем всем таким элементам пометку α .

Если $\alpha_1 \neq \alpha_2$, $|\alpha_1| = |\alpha_2| = t$, то пометки α_1 и α_2 будут приписаны разным элементам. В самом деле, пусть какой-то элемент s получил хотя бы две пометки, α_1 и α_2 , $\alpha_1 \neq \alpha_2$. Рассмотрим куст, растущий из элемента s . Если он содержит только один вход, то его без ущерба для СФЭРП (т.е. не меняя функционирование СФЭРП и не увеличивая сложность) можно удалить. Пусть он содержит хотя бы два входа $u(\beta_1)$ и $u(\beta_2)$, $\beta_1 \neq \beta_2$. Тогда, т.к.

$$|(\{\alpha_1\} \cup \check{S}(\alpha_1)) \cap (\{\alpha_2\} \cup \check{S}(\alpha_2))| \leq 1,$$

например, не верно, что $\beta_1 \leq \alpha_2$.

Тогда, с одной стороны, найдется ориентированный путь от входа $u(\beta_1)$ к элементу s . А с другой стороны, найдется ориентированный путь от элемента s к выходу $v(\alpha_2)$. Получаем противоречие с разделенностью переменных СФЭРП. Индуктивный переход обоснован.

$$\text{Следовательно, } L(S_n) \geq \sum_{t=1}^n \sum_{\alpha \in E_2^n, |\alpha|=t} t = \sum_{t=1}^n t \cdot C_n^t = n \cdot 2^{n-1}.$$

Теорема 4.5 доказана. □

Следствие 4.3. [256] В базисе $B_{L_0} = \{x \oplus y\}$ верно $L_{B_{L_0}}^{\text{СФЭРП}}(\Pi_n) = n \cdot 2^{n-1}$.

Доказательство. Верно, что $L_{B_{L_0}}^{\text{СФЭРП}}(\Pi_1) = 1$. Если построить СФЭРП S_n для системы Π_n при $n \geq 2$ по индукции как в [205] по свойству

$$f(x_1, x_2, \dots, x_n) = f(0, x_2, \dots, x_n) \oplus x_1(f(0, x_2, \dots, x_n) \oplus f(1, x_2, \dots, x_n))$$

выводим соотношение

$$L_{B_{L_0}}^{\text{СФЭРП}}(\Pi_n) \leq 2L_{B_{L_0}}^{\text{СФЭРП}}(\Pi_{n-1}) + 2^{n-1}.$$

Отсюда получаем СФЭРП для системы Π_n со сложностью $n \cdot 2^{n-1}$.

Нижняя оценка получена в теореме 4.5.

Следствие 4.3 доказано. □

Теперь оценим сложность СФЭРП Π_n в базисе $B_0 = \{x \& y, x \vee y, \bar{x}\}$ из элементов конъюнкции, дизъюнкции и отрицания.

Теорема 4.6. [256] *В базисе $B_0 = \{x \& y, x \vee y, \bar{x}\}$ верно*

$$3n \cdot 2^{n-1} \leq L_{B_0}^{\text{СФЭРП}}(\Pi_n) \leq 4n \cdot 2^{n-1}.$$

Доказательство. Нижняя оценка доказывается аналогично доказательству теоремы 4.5. Пусть задана какая-то СФЭРП S_n в базисе B_0 , реализующая систему Π_n .

Докажем, что в СФЭРП S_n каждому такому набору $\alpha \in E_2^n$, что $1 \leq |\alpha| \leq n$, можно сопоставить не менее $3 \cdot |\alpha|$ элементов конъюнкции или дизъюнкции, причем так, что для разных наборов α и β соответствующие им множества элементов не пересекаются, и если элемент s соответствует набору α , то из этого элемента s найдется ориентированный путь в выход $v(\alpha)$. Доказывать это утверждение будем индукцией по весу наборов t , $1 \leq t \leq n$.

Базис индукции: $t = 1$. Пусть $\alpha \in E_2^n$, и $|\alpha| = 1$. Рассмотрим в СФЭРП S_n куст, растущий из выхода $v(\alpha)$. На выходе $v(\alpha)$ реализуется функция $f(0, \dots, 0) \oplus f(\alpha)$, поэтому этот куст содержит хотя бы 3 элемента конъюнкции или дизъюнкции [194]. Припишем всем таким элементам пометку α . Если $\alpha_1 \neq \alpha_2$, $|\alpha_1| = |\alpha_2| = 1$, то пометки α_1 и α_2 будут приписаны разным элементам. В самом деле, пусть какой-то элемент s получил хотя бы две пометки, α_1 и α_2 , $\alpha_1 \neq \alpha_2$. Рассмотрим куст, растущий из элемента s . Если он содержит только один вход, то элемент s без ущерба для СФЭРП можно удалить. Пусть он содержит два входа, например, $u(0, \dots, 0)$ и $u(\alpha_1)$. Но тогда есть ориентированный путь из входа $u(\alpha_1)$ к элементу s , и есть ориентированный

путь из элемента s к выходу $v(\alpha_2)$. Противоречие, этого не может быть в силу разделенности переменных СФЭРП.

Индуктивный переход от $t - 1$ к t , $2 \leq t \leq n$. Пусть в СФЭРП S_n каждому такому набору $\beta \in E_2^n$, что $1 \leq |\beta| \leq t - 1$, сопоставлено не менее $3 \cdot |\beta|$ элементов конъюнкции или дизъюнкции, причем множества элементов, сопоставленных разным наборам, не пересекаются, и если элемент s сопоставлен набору β , то из этого элемента s найдется ориентированный путь в выходную вершину $v(\beta)$.

Преобразуем СФЭРП S_n : подадим на все входы $u(\beta)$, $|\beta| \leq t - 2$ значение 0. Рассмотрим в СФЭРП S_n произвольный элемент конъюнкции или дизъюнкции s , которому сопоставлен набор β , где $1 \leq |\beta| \leq t - 2$. Из элемента s есть ориентированный путь в выход $v(\beta)$, поэтому в элемент s могут вести ориентированные пути только из входов, на которые поданы 0. Преобразуем СФЭРП S_n по правилам алгебры логики $0 \& x = 0$, $0 \vee x = x$, $\bar{0} = 1$, $1 \& x = x$, $1 \vee x = 1$ и т.д. до тех пор, пока это возможно. При этом мы удалим все входы $u(\beta)$, $|\beta| \leq t - 2$, все элементы, хотя бы на один вход которых пришла константа 0 или константа 1, и все выходы $v(\beta)$, $|\beta| \leq t - 2$ (на каждом из таких выходов реализуется функция, тождественно равная нулю). Отметим также, что при этом удалятся все вершины, которым были сопоставлены наборы β , где $1 \leq |\beta| \leq t - 2$, т.к. в эти вершины вели ориентированные пути только от входов, которым мы приписали 0. Обозначим полученную СФЭРП с входами $u(\alpha)$, $|\alpha| \geq t - 1$, и выходами $v(\alpha)$, $|\alpha| \geq t - 1$, как $\hat{S}_n^{(t)}$.

Итак, в СФЭРП $\hat{S}_n^{(t)}$ нет элементов конъюнкции и дизъюнкции, сопоставленных наборам β , где $1 \leq |\beta| \leq t - 2$. Но в СФЭРП $\hat{S}_n^{(t)}$ могут быть элементы конъюнкции или дизъюнкции, сопоставленные каким-то наборам β , $|\beta| = t - 1$. Рассмотрим такой элемент s . Пусть он сопоставлен набору β . Рассмотрим выход $v(\beta)$, $|\beta| = t - 1$. На нем реализуется тождественная функция

$u(\beta)$. Из элемента s есть ориентированный путь в выход $v(\beta)$. Поэтому в силу разделенности переменных СФЭРП $\hat{S}_n^{(t)}$ в элемент s могут вести ориентированные пути только из входа $u(\beta)$. Поэтому элемент s можно удалить без ущерба для функционирования СФЭРП и не увеличивая ее сложность. Таким же образом удалим все элементы конъюнкции и дизъюнкции, сопоставленные наборам β , $|\beta| = t - 1$.

Обозначим полученную СФЭРП с входами $u(\alpha)$, $|\alpha| \geq t - 1$, и выходами $v(\alpha)$, $|\alpha| \geq t - 1$, как $S_n^{(t)}$. Заметим, что по построению в СФЭРП $S_n^{(t)}$ нет элементов конъюнкции и дизъюнкции, сопоставленных наборам β , $1 \leq |\beta| \leq t - 1$.

Пусть $|\alpha| = t$. Рассмотрим в СФЭРП $S_n^{(t)}$ куст, растущий из выхода $v(\alpha)$. На выходе $v(\alpha)$ реализуется функция $u(\alpha) \oplus \bigoplus_{\beta \in \check{S}(\alpha)} u(\beta)$, т.е. сумма по модулю 2 своих $(t + 1)$ входов. Для этого требуется не менее $3(t + 1) - 3 = 3t$ элементов конъюнкции и дизъюнкции [194]. Припишем всем таким элементам пометку α .

Если $\alpha_1 \neq \alpha_2$, $|\alpha_1| = |\alpha_2| = t$, то пометки α_1 и α_2 будут приписаны разным элементам. В самом деле, пусть какой-то элемент s получил хотя бы две пометки, α_1 и α_2 , $\alpha_1 \neq \alpha_2$. Рассмотрим куст, растущий из элемента s . Если он содержит только один вход, то его без ущерба для СФЭ можно удалить. Пусть он содержит хотя бы два входа $u(\beta_1)$ и $u(\beta_2)$, $\beta_1 \neq \beta_2$. Тогда, т.к.

$$|(\{\alpha_1\} \cup \check{S}(\alpha_1)) \cap (\{\alpha_2\} \cup \check{S}(\alpha_2))| \leq 1,$$

например, не верно, что $\beta_1 \leq \alpha_2$.

Тогда, с одной стороны, найдется ориентированный путь от входа $u(\beta_1)$ к элементу s . А с другой стороны, найдется ориентированный путь от элемента s к выходу $v(\alpha_2)$. Получаем противоречие с разделенностью переменных СФЭРП. Индуктивный переход обоснован.

Поэтому

$$L(S_n) \geq \sum_{t=1}^n \sum_{\alpha \in E_2^n, |\alpha|=t} 3t = \sum_{t=1}^n (3t) \cdot C_n^t = 3n \cdot 2^{n-1}.$$

Верхняя оценка получается применением алгоритма из [205] (как в следствии 4.3) и из того факта, что сложность реализации функции алгебры логики $x \oplus y$ в базисе B_0 равна 4 [119]. Т.е. из соотношения

$$L_{B_0}^{\text{СФЭРП}}(\Pi_n) \leq 2L_{B_0}^{\text{СФЭРП}}(\Pi_{n-1}) + 4 \cdot 2^{n-1},$$

откуда $L_{B_0}^{\text{СФЭРП}}(\Pi_n) \leq 4n \cdot 2^{n-1}$.

Теорема 4.6 доказана. □

Замечание 4.6. Аналогично доказательству теоремы 4.6, учитывая оценку из [194], можно доказать, что в базисе $U_2 = P_2^2 \setminus \{x \oplus y, x \sim y\}$, где $x \sim y = x \oplus y \oplus 1$, верно $L_{U_2}^{\text{СФЭРП}}(\Pi_n) = 3n \cdot 2^{n-1}$.

В заключение этого раздела докажем теорему 4.7, которая аналогично двузначному случаю [213] (стр.71) при простых k описывает формулу, выражающую коэффициенты полинома по модулю k для функции k -значной логики через значения этой функции.

Теорема 4.7. [248] Пусть k – простое число, $f(x_1, \dots, x_n) \in P_k^n$.

Тогда для каждого набора $\alpha = (a_1, \dots, a_n) \in E_k^n$ верно

$$c_f(\alpha) = (-1)^{r(\alpha)} \sum_{\beta: t(\beta) \leq t(\alpha)} f(\beta) \prod_{a_i \neq 0} b_i^{k-1-a_i},$$

где $\beta = (b_1, \dots, b_n) \in E_k^n$ (полагаем, что произведение по пустому множеству индексов равно 1 и $0^0 = 1$).

Доказательство. Докажем индукцией по числу переменных n .

Базис индукции: $n = 1$. Тогда для набора $\alpha = (a_1) \in E_k^1$ по доказанному в [248] получаем

1) если $a_1 = 0$, то

$$c_f(a_1) = f(0) = (-1)^{r(\alpha)} f(0);$$

2) если $a_1 = 1, \dots, k-1$, то

$$c_f(a_1) = - \sum_{i=0}^{k-1} i^{k-1-a_1} f(i) = (-1)^{r(\alpha)} \sum_{\beta: t(\beta) \subseteq t(\alpha)} b_1^{k-1-a_1} f(b_1).$$

Индуктивный переход. Пусть для всех функций k -значной логики, зависящих не более, чем от $(n-1)$, $n \geq 2$, переменной, утверждение теоремы 4.7 верно. Рассмотрим функцию $f(x_1, \dots, x_n) \in P_k^n$.

Пусть $\alpha = (a_1, \dots, a_n) \in E_k^n$ и $\alpha' = (a_2, \dots, a_n)$. Тогда с учетом индуктивного предположения получаем

1) если $a_1 = 0$, то

$$\begin{aligned} c_f(0, a_2, \dots, a_n) &= c_{f_0}(a_2, \dots, a_n) = \\ &= (-1)^{r(\alpha')} \sum_{\beta': t(\beta') \subseteq t(\alpha')} \left(\prod_{a_i \neq 0, i \geq 2} b_i^{k-1-a_i} \right) f_0(b_2, \dots, b_n) = \\ &= (-1)^{r(\alpha)} \sum_{\beta: t(\beta) \subseteq t(0, \alpha')} \left(\prod_{a_i \neq 0} b_i^{k-1-a_i} \right) f(0, b_2, \dots, b_n), \end{aligned}$$

где $\beta = (b_1, b_2, \dots, b_n) \in E_k^n$ и $\beta' = (b_2, \dots, b_n)$.

2) если $a_1 \neq 0$, то

$$\begin{aligned} c_f(a_1, a_2, \dots, a_n) &= - \sum_{b_1=0}^{k-1} b_1^{k-1-a_1} c_{f_{b_1}}(a_2, \dots, a_n) = \\ &= - \sum_{b_1=0}^{k-1} b_1^{k-1-a_1} \left((-1)^{r(\alpha')} \sum_{\beta': t(\beta') \subseteq t(\alpha')} \left(\prod_{a_i \neq 0, i \geq 2} b_i^{k-1-a_i} \right) f_{b_1}(b_2, \dots, b_n) \right) = \\ &= (-1)^{r(\alpha)} \sum_{\beta: t(\beta) \subseteq t(\alpha)} \left(\prod_{a_i \neq 0} b_i^{k-1-a_i} \right) f(b_1, b_2, \dots, b_n), \end{aligned}$$

где $\beta = (b_1, b_2, \dots, b_n) \in E_k^n$ и $\beta' = (b_2, \dots, b_n)$.

Теорема 4.7 доказана.

□

5 Мультипликативная сложность функций алгебры логики

В этом разделе мы исследуем мультипликативную сложность некоторых функций алгебры логики. Все результаты этого раздела опубликованы в работах [262, 265, 269, 271, 272, 274].

Мультипликативной (или конъюнктивной) сложностью функции алгебры логики $f(x_1, \dots, x_n)$ (системы функций алгебры логики $F = \{f_1, \dots, f_m\}$) называется наименьшее число элементов конъюнкции в СФЭ в базисе $B_P = \{x \& y, x \oplus y, 1\}$, каждая из которых реализует функцию f (все функции из системы F). Мультипликативную сложность функции f (системы функций F) будем обозначать как $\mu(f)$ (как $\mu(F)$). Т.е. теперь функции задаются не полиномиальными формами, а в полиномиальном базисе. В [175] показано, что для квадратичных функций алгебры логики СФЭ с наименьшим числом умножений (элементов конъюнкции) можно построить по ПСПФ этих функций.

Мы найдем значения мультипликативной сложности для функций алгебры логики, представимых суммой произведения всех переменных функции и квадратичной функции или суммой двух мультиаффинных функций, а также квазиквадратичных функций алгебры логики.

Сначала мы докажем леммы, которые будут применяться при доказательстве оценок мультипликативной сложности функций.

Обозначим множество всех аффинных функций алгебры логики, зависящих от переменных $x_1, \dots, x_n$, как A^n , множество всех линейных функций алгебры логики, зависящих от переменных $x_1, \dots, x_n$, как L^n . Линейные функции алгебры логики $g_1, \dots, g_m$ называются линейно независимыми, если из равенства

$$c_1 g_1 \oplus \dots \oplus c_m g_m = 0,$$

где $c_1, \dots, c_m \in E_2$, следует, что $c_1 = \dots = c_m = 0$. Иначе, линейные функции $g_1, \dots, g_m$ называются линейно зависимыми. Множество L^n является линейным пространством размерности n .

Лемма 5.1. [269] *Если $g_i \in L^n$, $i = 1, \dots, l$, $l \geq 2$, и функции $g_1, \dots, g_l$ являются линейно независимыми, то найдутся такие константы $a_1, \dots, a_n \in E_2$ и такие функции $h_{l+1}, \dots, h_n \in A^n$, что*

$$\left(\prod_{i=1}^l (g_i \oplus a_i) \right) \cdot \left(\prod_{i=l+1}^n h_i \right) = x_1 \cdot \dots \cdot x_n.$$

Доказательство. Добавим к линейным функциям $g_1, \dots, g_l$ такие линейные функции $g_{l+1}, \dots, g_n \in L^n$, что линейные функции $g_1, \dots, g_n$ являются линейно независимыми. Мы всегда можем это сделать, так как размерность линейного пространства L^n равна n .

Рассмотрим систему линейных уравнений

$$\begin{cases} g_1(x_1, \dots, x_n) = g_1(1, \dots, 1), \\ \dots, \\ g_n(x_1, \dots, x_n) = g_n(1, \dots, 1). \end{cases}$$

Заметим, что по построению единичный набор $(1, \dots, 1) \in B^n$ является решением этой системы. Линейные функции $g_1, \dots, g_n$ линейно независимы, поэтому (см., например, [210], стр. 81) эта система имеет единственное решение. Заметим, что множество решений этой системы является множеством наборов из E_2^n , на которых функция $\prod_{i=1}^n (g_i \oplus g_i(1, \dots, 1) \oplus 1)$ принимает значение 1. Так как единственное решение этой системы – это единичный набор $(1, \dots, 1) \in E_2^n$, получаем, что

$$\prod_{i=1}^n (g_i \oplus g_i(1, \dots, 1) \oplus 1) = x_1 \cdot \dots \cdot x_n.$$

Отсюда находим, что $a_i = g_i(1, \dots, 1) \oplus 1$ при $i = 1, \dots, l$, $h_i(x_1, \dots, x_n) = g_i(x_1, \dots, x_n) \oplus g_i(1, \dots, 1) \oplus 1$ при $i = l + 1, \dots, n$.

Лемма 5.1 доказана. □

Лемма 5.2. [269] Если $g_i \in L^n$, $a_i \in E_2$, $i = 1, \dots, l$, $l \geq 2$, функции $g_1, \dots, g_l$ являются линейно независимыми и s – такое число, что $n - s \leq l$, то найдутся такие функции $h_1, \dots, h_{n-s} \in A^n$ и $h_{n-s+1}, \dots, h_l \in A^s$, что

$$\prod_{i=1}^l (g_i \oplus a_i) = \prod_{i=1}^l h_i.$$

Доказательство. Рассмотрим систему линейных уравнений

$$\begin{cases} g_1(x_1, \dots, x_n) = a_1 \oplus 1, \\ \dots, \\ g_l(x_1, \dots, x_n) = a_l \oplus 1. \end{cases}$$

Так как функции $g_1, \dots, g_l$ – линейно независимы, мы можем (см., например, [210]) преобразовать эту систему к виду

$$\begin{cases} h_1(x_1, \dots, x_s, x_{s+1}, \dots, x_{n-1}, x_n) = 1, \\ h_2(x_1, \dots, x_s, x_{s+1}, \dots, x_{n-1}) = 1, \\ \dots, \\ h_{n-s}(x_1, \dots, x_s, x_{s+1}) = 1, \\ h_{n-s+1}(x_1, \dots, x_s) = 1, \\ \dots, \\ h_l(x_1, \dots, x_s) = 1, \end{cases}$$

где $h_1, \dots, h_{n-s} \in A^n$, $h_{n-s+1}, \dots, h_l \in A^s$, так, что множества решений этих систем совпадают. Следовательно,

$$\prod_{i=1}^l h_i = \prod_{i=1}^l (g_i \oplus a_i).$$

Лемма 5.2 доказана. □

Лемма 5.3. [269] 1. Если $f_n(x_1, \dots, x_n) = x_1 \cdot \dots \cdot x_n \oplus \bar{x}_1 \cdot \dots \cdot \bar{x}_n \in P_2$, где $n \geq 2$, то $\mu(f_n) = n - 2$.

2. Если $F_n = \{x_1 \cdot \dots \cdot x_n, \bar{x}_1 \cdot \dots \cdot \bar{x}_n\}$, $n \geq 1$, то $\mu(F_n) = n - 1$.

Доказательство. 1. *Верхняя оценка.* Заметим, что

$$f_n(x_1, \dots, x_n) = (x_1 \sim x_2)(x_2 \sim x_3) \dots (x_{n-2} \sim x_{n-1})(x_{n-1} \sim x_n),$$

где $x \sim y = x \oplus y \oplus 1$. Отсюда $\mu(f_n) \leq n - 2$.

Нижняя оценка. Заметим, что $\deg(f_n) = n - 1$. В [195] доказано, что для произвольной функции f верно, что $\mu(f) \geq \deg(f) - 1$. Поэтому $\mu(f_n) \geq n - 2$.

Получаем, что $\mu(f_n) = n - 2$.

2. *Верхняя оценка.* Заметим, что

$$\begin{aligned} x_1 \cdot \dots \cdot x_n &= x_1 \cdot f_n(x_1, \dots, x_n), \\ \bar{x}_1 \cdot \dots \cdot \bar{x}_n &= x_1 \cdot \dots \cdot x_n \oplus f_n(x_1, \dots, x_n), \end{aligned}$$

где

$$f_n(x_1, \dots, x_n) = x_1 \cdot \dots \cdot x_n \oplus \bar{x}_1 \cdot \dots \cdot \bar{x}_n.$$

По п.1 леммы 5.3 $\mu(f_n) \leq n - 2$. Поэтому $\mu(F_n) \leq n - 1$.

Нижняя оценка. Заметим, что степень каждой из функций системы F_n равна n . Поэтому $\mu(F_n) \geq n - 1$ [195].

Получаем, что $\mu(F_n) = n - 1$.

Лемма 5.3 доказана. □

Напомним, что функция алгебры логики f называется квадратичной, если $\deg(f) = 2$. В [175] доказано, что для произвольной квадратичной функции, зависящей от n переменных, верно, что $\mu(f) \leq \lfloor n/2 \rfloor$. Кроме того, в [175] описаны квадратичные функции, зависящие от n переменных, мультипликативная сложность которых равна $\lfloor n/2 \rfloor$. Мы доказываем (теорема 5.1), что мультипликативная сложность каждой функции алгебры логики, которую можно представить как сумму по модулю два произведения n переменных и какой-то квадратичной функции, зависящей от n переменных, равна $(n - 1)$.

Теорема 5.1. [269] 1. Если $n \geq 3$, и функция алгебры логики $f(x_1, \dots, x_n)$ может быть представлена в виде $x_1 \cdot \dots \cdot x_n \oplus q(x_1, \dots, x_n)$, где $\deg(q) = 2$, то $\mu(f) = n - 1$.

2. Если $F = \{x_1 \cdot \dots \cdot x_n, q(x_1, \dots, x_n)\}$, где $\deg(q) = 2$, то $\mu(F) = n - 1$ ($n \geq 2$).

Доказательство. 1. *Верхняя оценка.* В [175, 195] показано, что каждую функцию алгебры логики степени два можно представить в виде $g_0 \oplus \bigoplus_{i=1}^l g_{2i-1} g_{2i}$, где $g_i \in L^n$, $i = 1, \dots, 2l$, $g_0 \in A^n$, и линейные функции $g_1, \dots, g_{2l}$ линейно независимы. Представим функцию $q(x_1, \dots, x_n)$ в таком виде. Заметим, что $2l \leq n$, т.к. размерность линейного пространства L^n равна n .

По лемме 5.1 найдем такие константы $a_1, \dots, a_{2l} \in E_2$ и такие функции $h_{2l+1}, \dots, h_n \in A^n$, что

$$\left(\prod_{i=1}^l (g_{2i-1} \oplus a_{2i-1}) \cdot (g_{2i} \oplus a_{2i}) \right) \cdot \left(\prod_{i=2l+1}^n h_i \right) = x_1 \cdot \dots \cdot x_n.$$

Заметим, что

$$g_{2i-1} \cdot g_{2i} = (g_{2i-1} \oplus a_{2i-1}) \cdot (g_{2i} \oplus a_{2i}) \oplus h_i$$

для некоторых $h_i \in A^n$, $i = 1, \dots, l$. Отсюда получаем, что

$$q(x_1, \dots, x_n) = h_0 \oplus \bigoplus_{i=1}^l (g_{2i-1} \oplus a_{2i-1}) \cdot (g_{2i} \oplus a_{2i}),$$

где $h_0 = g_0 \oplus \bigoplus_{i=1}^l h_i \in A^n$. Следовательно,

$$\begin{aligned} f(x_1, \dots, x_n) &= \left(\prod_{i=1}^l (g_{2i-1} \oplus a_{2i-1}) \cdot (g_{2i} \oplus a_{2i}) \right) \cdot \left(\prod_{i=2l+1}^n h_i \right) \oplus \\ &\oplus h_0 \oplus \bigoplus_{i=1}^l (g_{2i-1} \oplus a_{2i-1}) \cdot (g_{2i} \oplus a_{2i}). \end{aligned} \quad (24)$$

СФЭ, реализующую функцию f , будем строить по полученной формуле (24). Сначала реализуем функции $(g_{2i-1} \oplus a_{2i-1}) \cdot (g_{2i} \oplus a_{2i})$, $i = 1, \dots, l$. Для этого понадобится l элементов конъюнкции. Затем реализуем функцию

$$\left(\prod_{i=1}^l (g_{2i-1} \oplus a_{2i-1}) \cdot (g_{2i} \oplus a_{2i}) \right) \cdot \left(\prod_{i=2l+1}^n h_i \right).$$

При этом добавим еще $(n - l - 1)$ элементов конъюнкции. Затем реализуем функцию f по формуле (24) без дополнительных элементов конъюнкции.

Получаем, что $\mu(f) \leq n - 1$.

Нижняя оценка. Для произвольной функции алгебры логики f верно, что $\mu(f) \geq \deg(f) - 1$ [195]. Поэтому получаем, что $\mu(f) \geq n - 1$.

Следовательно, $\mu(f) = n - 1$.

2. *Верхняя оценка* $\mu(F) \leq n - 1$ при $n \geq 3$ следует из доказательства п. 1 теоремы 5.1, т.к. по этому доказательству видно, как построить СФЭ с $(n - 1)$ элементами конъюнкции, в которой реализуются функции $x_1 \cdot \dots \cdot x_n$ и $q(x_1, \dots, x_n)$. При $n = 2$ верхняя оценка верна. *Нижняя оценка* $\mu(F) \geq n - 1$ следует из того, что в системе F содержится функция $x_1 \cdot \dots \cdot x_n$ степени n . Следовательно, $\mu(F) = n - 1$.

Теорема 5.1 доказана. □

Напомним, что функция алгебры логики $f(x_1, \dots, x_n)$ называется мультиаффинной, если найдутся такие аффинные функции $h_1, \dots, h_s$, что $f = \prod_{i=1}^s h_i$. Мультиаффинные функции рассматривались в [196] в связи с задачей выполнимости конъюнктивных форм.

В [195] доказано следующее свойство мультиаффинных функций: если функция $f(x_1, \dots, x_n)$ является мультиаффинной, то найдутся такие линейно независимые функции $g_1, \dots, g_l \in L^n$ и такие константы $a_1, \dots, a_l \in E_2$, где

$l = \deg(f)$, что

$$f(x_1, \dots, x_n) = \prod_{i=1}^l (g_i \oplus a_i).$$

Рассмотрим мультиаффинную функцию $f(x_1, \dots, x_n)$, и пусть $\deg(f) = l$, $l \leq n$. Тогда $f(x_1, \dots, x_n) = \prod_{i=1}^l (g_i \oplus a_i)$, где $g_1, \dots, g_l$ – некоторые линейно независимые линейные функции, и $a_1, \dots, a_l \in E_2$ [195]. Добавим к линейным функциям $g_1, \dots, g_l$ такие линейные функции $g_{l+1}, \dots, g_n$, что линейные функции $g_1, \dots, g_n$ являются линейно независимыми. Мы всегда можем так сделать. Рассмотрим аффинные замены переменных:

$$\begin{aligned} y_1 &= g_1 \oplus a_1, \\ &\dots, \\ y_l &= g_l \oplus a_l, \\ y_{l+1} &= g_{l+1}, \\ &\dots, \\ y_n &= g_n. \end{aligned}$$

Это преобразование переменных переводит мультиаффинную функцию f в функцию $y_1 \cdot \dots \cdot y_l$. Кроме того, это преобразование невырожденно (обратимо), так как линейные функции $g_1, \dots, g_n$ – линейно независимы. Поэтому найдутся такие линейно независимые линейные функции $h_1, \dots, h_n$, зависящие от переменных $y_1, \dots, y_n$, и такие $b_1, \dots, b_n \in E_2$, что

$$\begin{aligned} x_1 &= h_1 \oplus b_1, \\ &\dots, \\ x_n &= h_n \oplus b_n. \end{aligned}$$

Эти рассуждения мы будем применять далее в доказательствах теорем.

По свойству из [195] мультипликативная сложность каждой мультиаффинной функции, зависящей от n переменных, не превосходит $(n - 1)$. Мы дока-

зываем (теоремы 5.2, 5.3, 5.4) оценки мультипликативной сложности функций алгебры логики, которые представимы как сумма по модулю два двух мультиаффинных функций.

Теорема 5.2. [269] 1. Если функция алгебры логики $f(x_1, \dots, x_n)$ может быть представлена в виде $f_1(x_1, \dots, x_n) \oplus f_2(x_1, \dots, x_n)$, где f_1, f_2 – мультиаффинные функции, и $\deg(f) = n$, то $\mu(f) = n - 1$ ($n \geq 2$).

2. Если $F = \{x_1 \cdot \dots \cdot x_n, f(x_1, \dots, x_n)\}$, где f – мультиаффинная функция алгебры логики, $\deg(f) < n$, то $\mu(F) = n - 1$ ($n \geq 1$).

Доказательство. 1. *Верхняя оценка.* Так как $\deg(f) = n$, то обратимыми аффинными заменами переменных функцию $f(x_1, \dots, x_n)$ можно преобразовать к виду $x_1 \cdot \dots \cdot x_n \oplus h(x_1, \dots, x_n)$, где h – мультиаффинная функция, и $\deg(h) < n$. По свойству из [195] представим функцию $h(x_1, \dots, x_n)$ в виде $\prod_{i=1}^l g_i$, где $g_1, \dots, g_l \in A^n$, линейные функции $g_1 \oplus g_1(0, \dots, 0), \dots, g_l \oplus g_l(0, \dots, 0)$ линейно независимы, и $l = \deg(h)$. Не ограничивая общности рассуждений, пусть $g_i(1, \dots, 1) = 1$ при $i = 1, \dots, s$, и $g_i(1, \dots, 1) = 0$ при $i = s + 1, \dots, l$.

Воспользуемся леммой 5.1. Найдем такие функции $g_{l+1}, \dots, g_n \in A^n$, что

$$\prod_{i=1}^s g_i \cdot \prod_{i=s+1}^l \bar{g}_i \cdot \prod_{i=l+1}^n g_i = x_1 \cdot \dots \cdot x_n.$$

Тогда

$$\begin{aligned} f(x_1, \dots, x_n) &= x_1 \cdot \dots \cdot x_n \oplus h(x_1, \dots, x_n) = x_1 \cdot \dots \cdot x_n \oplus \prod_{i=1}^l g_i = \\ &= \prod_{i=1}^s g_i \cdot \prod_{i=s+1}^l \bar{g}_i \cdot \prod_{i=l+1}^n g_i \oplus \prod_{i=1}^s g_i \cdot \prod_{i=s+1}^l g_i = \\ &= \prod_{i=1}^s g_i \cdot \left(\prod_{i=s+1}^l \bar{g}_i \cdot \prod_{i=l+1}^n g_i \oplus \prod_{i=s+1}^l g_i \right). \end{aligned} \quad (25)$$

СФЭ с $(n-1)$ элементами конъюнкции для функции $x_1 \cdot \dots \cdot x_n \oplus h(x_1, \dots, x_n)$ будем строить по формуле (25).

Сначала строим произведение $\prod_{i=1}^s g_i$ при помощи $(s-1)$ элементов конъюнкции.

Затем воспользуемся леммой 5.3. Рассмотрим СФЭ S_{l-s} , реализующую функцию $f_{l-s} = y_1 \cdot \dots \cdot y_{l-s} \oplus \bar{y}_1 \cdot \dots \cdot \bar{y}_{l-s}$ с $(l-s-2)$ элементами конъюнкции. На входы $y_1, \dots, y_{l-s}$ подадим аффинные функции $g_{s+1}, \dots, g_l$ соответственно. Полученная новая СФЭ S'_{l-s} реализует функцию $\prod_{i=s+1}^l g_i \oplus \prod_{i=s+1}^l \bar{g}_i$ с $(l-s-2)$ элементами конъюнкции. Добавляя один элемент конъюнкции, строим функцию $\left(\prod_{i=1}^s g_i\right) \cdot \left(\prod_{i=s+1}^l g_i \oplus \prod_{i=s+1}^l \bar{g}_i\right)$. Домножая эту функцию на функцию g_{s+1} , можно построить функцию $\left(\prod_{i=1}^s g_i\right) \cdot \left(\prod_{i=s+1}^l g_i\right)$, а затем при помощи одного сложения по модулю два функцию $\left(\prod_{i=1}^s g_i\right) \cdot \left(\prod_{i=s+1}^l \bar{g}_i\right)$.

Добавляя $(n-l-1)$ элементов конъюнкции, строим произведение $\prod_{i=l+1}^n g_i$.

Добавляя еще 1 элемент конъюнкции и элементы сложения по модулю два, строим искомую функцию.

Всего мы затратили $(s-1) + (l-s-2) + 2 + (n-l-1) + 1 = n-1$ элементов конъюнкции.

Нижняя оценка. Для произвольной функции алгебры логики f верно, что $\mu(f) \geq \deg(f) - 1$ [195]. Поэтому получаем, что $\mu(f) \geq n - 1$.

Следовательно, $\mu(f) = n - 1$.

2. *Верхняя оценка* $\mu(F) \leq n - 1$ при $n \geq 2$ следует из доказательства п. 1 теоремы 5.2, т.к. из этого доказательства видно, как построить СФЭ с $(n-1)$ элементами конъюнкции, в которой реализуются функции $x_1 \cdot \dots \cdot x_n$ и $f(x_1, \dots, x_n)$. При $n = 1$ верхняя оценка верна. *Нижняя оценка* $\mu(F) \geq n - 1$ следует из того, что в системе F содержится функция $x_1 \cdot \dots \cdot x_n$ степени n .

Следовательно, $\mu(F) = n - 1$.

Теорема 5.2 доказана. □

Теорема 5.3. [269] 1. Если функция алгебры логики $f(x_1, \dots, x_n)$ может быть представлена в виде $f_1(x_1, \dots, x_n) \oplus f_2(x_1, \dots, x_n)$, где f_1, f_2 — мультиаффинные функции, $f_1 \neq f_2$, и $\deg(f_1) = \deg(f_2) = n$, то $\mu(f) = n - 2$ ($n \geq 2$).

2. Если $F = \{x_1 \cdot \dots \cdot x_n, f(x_1, \dots, x_n)\}$, где f — мультиаффинная функция алгебры логики, $\deg(f) = n$, то $\mu(F) = n - 1$ ($n \geq 1$).

Доказательство. 1. *Верхняя оценка.* Не ограничивая общности рассуждений, обратимыми аффинными заменами переменных функцию $f(x_1, \dots, x_n)$ можно преобразовать к виду $x_1 \cdot \dots \cdot x_n \oplus x_1 \cdot \dots \cdot x_s \bar{x}_{s+1} \cdot \dots \cdot \bar{x}_n$. Так как $f_1 \neq f_2$, верно $s < n$. Тогда

$$x_1 \cdot \dots \cdot x_n \oplus x_1 \cdot \dots \cdot x_s \bar{x}_{s+1} \cdot \dots \cdot \bar{x}_n = x_1 \cdot \dots \cdot x_s \cdot (x_{s+1} \cdot \dots \cdot x_n \oplus \bar{x}_{s+1} \cdot \dots \cdot \bar{x}_n). \quad (26)$$

СФЭ, реализующую функцию $x_1 \cdot \dots \cdot x_n \oplus x_1 \cdot \dots \cdot x_s \bar{x}_{s+1} \cdot \dots \cdot \bar{x}_n$, с $(n - 2)$ элементами конъюнкции будем строить по формуле (26). По лемме 5.3 функцию $x_{s+1} \cdot \dots \cdot x_n \oplus \bar{x}_{s+1} \cdot \dots \cdot \bar{x}_n$ можно реализовать СФЭ с $(n - s - 2)$ элементами конъюнкции. Добавляя еще s элементов конъюнкции, получаем СФЭ для искомой функции.

Нижняя оценка $\mu(f) \geq n - 2$ следует из [195], т.к. $\deg(f) = n - 1$.

2. Не ограничивая общности рассуждений, при $n \geq 2$ функция $f(x_1, \dots, x_n)$ имеет вид $x_1 \cdot \dots \cdot x_s \bar{x}_{s+1} \cdot \dots \cdot \bar{x}_n$, где $s < n$. По п. 1 теоремы 5.3 для функции $x_1 \cdot \dots \cdot x_n \oplus f(x_1, \dots, x_n)$ можно построить СФЭ с $(n - 2)$ элементами конъюнкции. Тогда

$$\begin{aligned} x_1 \cdot \dots \cdot x_n &= x_{s+1} \cdot (x_1 \cdot \dots \cdot x_n \oplus f(x_1, \dots, x_n)), \\ f(x_1, \dots, x_n) &= x_1 \cdot \dots \cdot x_n \oplus (x_1 \cdot \dots \cdot x_n \oplus f(x_1, \dots, x_n)). \end{aligned}$$

Отсюда $\mu(F) \leq n - 1$. При $n = 1$ верхняя оценка верна.

Нижняя оценка $\mu(F) \geq n - 1$ следует из того, что в системе F содержится функция $x_1 \cdot \dots \cdot x_n$ степени n .

Теорема 5.3 доказана. □

Теорема 5.4. [269] 1. Если функция алгебры логики $f(x_1, \dots, x_n)$ может быть представлена в виде $f_1(x_1, \dots, x_n) \oplus f_2(x_1, \dots, x_n)$, где f_1, f_2 — мультиаффинные функции, и $\deg(f_1) < n$, $\deg(f_2) < n$, то $\mu(f) \leq n - 1$ ($n \geq 2$).

2. Если $F = \{f_1(x_1, \dots, x_n), f_2(x_1, \dots, x_n)\}$, где f_1, f_2 — мультиаффинные функции алгебры логики, то $\mu(F) \leq n - 1$, ($n \geq 1$).

Доказательство. 1. Пусть $\deg(f_1) = m$, $\deg(f_2) = l$, и $m \leq l < n$. Обратимыми аффинными заменами переменных функцию $f(x_1, \dots, x_n)$ преобразуем к виду $x_1 \dots x_m \oplus t(x_1, \dots, x_n)$, где t — мультиаффинная функция, и $\deg(t) = l$. Представим мультиаффинную функцию $t(x_1, \dots, x_n)$ в виде $\prod_{i=1}^l g_i$, где $g_1, \dots, g_l \in A^n$, и линейные функции $g_1 \oplus g_1(0, \dots, 0), \dots, g_l \oplus g_l(0, \dots, 0)$ линейно независимы.

По лемме 5.2 найдем такие функции $h_1, \dots, h_{n-m} \in A^n$ и $h_{n-m+1}, \dots, h_l \in A^m$, что

$$\prod_{i=1}^l g_i = \prod_{i=1}^l h_i.$$

Тогда

$$x_1 \cdot \dots \cdot x_m \oplus t(x_1, \dots, x_n) = x_1 \cdot \dots \cdot x_m \oplus \left(\prod_{i=1}^{n-m} h_i \right) \cdot \left(\prod_{i=1}^{l-(n-m)} h_{n-m+i} \right). \quad (27)$$

СФЭ для функции $x_1 \cdot \dots \cdot x_m \oplus t(x_1, \dots, x_n)$ будем строить по формуле (27).

По теореме 5.2 систему из двух функций $x_1 \cdot \dots \cdot x_m$ и $\prod_{i=1}^{l-(n-m)} h_{n-m+i}$ можно реализовать СФЭ с $(m - 1)$ элементами конъюнкции. Для построения СФЭ

для функции $\prod_{i=1}^{n-m} h_i$ понадобится $((n - m) - 1)$ элементов конъюнкции. Добавляя еще один элемент конъюнкции и элементы сложения по модулю два, получаем СФЭ с $(n - 1)$ элементами конъюнкции для искомой функции.

2. Если степень хотя бы одной из функций f_1, f_2 равна n , то утверждение доказано в теоремах 5.2, 5.3. Если $\deg(f_1) < n, \deg(f_2) < n$, то при $n \geq 2$ оценка $\mu(F) \leq n - 1$ следует из доказательства п. 1 теоремы 5.4, т.к. из этого доказательства видно, как построить СФЭ с $(n - 1)$ элементами конъюнкции, в которой реализуются функции f_1 и f_2 . При $n = 1$ оценка верна.

Теорема 5.4 доказана. □

Отметим, что для рассмотренных функций алгебры логики доказательство нижней оценки их мультипликативной сложности опиралось на степень функции, и задача состояла в построении СФЭ с этой оценкой. Теперь мы рассмотрим квазиквадратичные функции алгебры логики, для которых их мультипликативная сложность оказывается больше их степени.

Функция алгебры логики $f(x_1, \dots, x_n)$ называется *квазиквадратичной*, если ее можно представить в виде $\varphi(x_1, \dots, x_s) \oplus q(x_1, \dots, x_n)$, где φ – произвольная функция, q – квадратичная функция, $s < n$. Мы исследуем мультипликативную сложность квазиквадратичных функций при $s = 3$ и произвольных n .

Сначала докажем верхнюю оценку мультипликативной сложности таких квазиквадратичных функций алгебры логики.

Теорема 5.5. [272] *Если функция алгебры логики $f(x_1, \dots, x_n)$ может быть представлена в виде $x_1x_2x_3 \oplus q(x_1, \dots, x_n)$, где $\deg(q) = 2, n \geq 3$, то $\mu(f) \leq t + 1$ при $n = 2t$ или $n = 2t + 1$.*

Доказательство. Докажем теорему индукцией по n . *Базис индукции:* $n = 3$.

Тогда функция $f(x_1, x_2, x_3)$ имеет вид

$$x_1x_2x_3 \oplus ax_1x_2 \oplus bx_1x_3 \oplus cx_2x_3 \oplus g(x_1, x_2, x_3),$$

где $a, b, c \in B$, $g \in A^3$. Заметим, что

$$x_1x_2x_3 \oplus ax_1x_2 \oplus bx_1x_3 \oplus cx_2x_3 = (x_1 \oplus c)(x_2 \oplus b)(x_3 \oplus a) \oplus h(x_1, x_2, x_3),$$

где $h \in A^3$. Из приведенного тождества видно, что $\mu(f) \leq 2$.

Индуктивный переход: пусть теорема 5.5 верна для всех функций указанного вида, зависящих менее, чем от n переменных. Рассмотрим функцию указанного вида $f(x_1, \dots, x_n)$, $n \geq 4$. Возможны следующие случаи.

1. Полином Жегалкина функции f содержит слагаемое x_ix_j , где $4 \leq i < j \leq n$. Тогда функцию f можно записать в виде

$$x_ix_j \oplus x_ig_1 \oplus x_jg_2 \oplus f_1,$$

где g_1, g_2 – аффинные функции, а f_1 – квазиквадратичная функция указанного в теореме 5.5 вида, и функции g_1, g_2, f_1 зависят от переменных $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{j-1}, x_{j+1}, \dots, x_n$. Заметим, что

$$x_ix_j \oplus x_ig_1 \oplus x_jg_2 = (x_i \oplus g_2)(x_j \oplus g_1) \oplus g_1g_2.$$

Отсюда функцию f можно представить в виде

$$(x_i \oplus g_2)(x_j \oplus g_1) \oplus f_2,$$

где $f_2 = f_1 \oplus g_1g_2$. Функция f_2 является квазиквадратичной указанного в теореме 5.5 вида и зависит от $(n - 2)$ переменных. Значит, для функции f_2 верно предположение индукции, откуда $\mu(f_2) \leq m$ при $n = 2m$ или $n = 2m + 1$. Отсюда для функции f получаем $\mu(f) \leq m + 1$ при $n = 2m$ или $n = 2m + 1$.

2. Полином Жегалкина функции f не содержит слагаемых вида $x_i x_j$, где $4 \leq i < j \leq n$. Тогда полином Жегалкина функции f можно записать в виде

$$x_1 x_2 x_3 \oplus x_1 g_1 \oplus x_2 g_2 \oplus x_3 g_3 \oplus h,$$

где g_1, g_2, g_3 – линейные функции, зависящие от переменных $x_4, \dots, x_n$, а h – аффинная функция, зависящая от переменных $x_1, \dots, x_n$. Если $n \geq 6$, то в этом выражении вынесем x_1 за скобку. Получим выражение, в котором 4 умножения. Заметим, что $4 \leq m + 1$ при $n = 2m$ или $n = 2m + 1$, где $n \geq 6$.

Отдельно рассмотрим случаи $n = 4$ и $n = 5$. Если $n = 4$, то выражение имеет вид

$$x_1 x_2 x_3 \oplus a x_1 x_4 \oplus b x_2 x_4 \oplus c x_3 x_4 \oplus h,$$

где $a, b, c \in B$, а h – аффинная функция, зависящая от переменных $x_1, \dots, x_4$. Заметим, что достаточно рассмотреть случай, когда хотя бы один из элементов a, b, c равен единице. Не ограничивая общности рассуждений, пусть $c = 1$. Преобразуем это выражение к виду

$$(x_1 x_2 \oplus x_4)(a x_1 \oplus b x_2 \oplus x_3) \oplus (a \oplus b)x_1 x_2 \oplus h.$$

При реализации полученного выражения СФЭ достаточно двух элементов конъюнкции.

Если $n = 5$, то выражение имеет вид

$$x_1 x_2 x_3 \oplus x_1 g_1 \oplus x_2 g_2 \oplus x_3 g_3 \oplus h,$$

где g_1, g_2, g_3 – линейные функции, зависящие от переменных x_4, x_5 , h – аффинная функция, зависящая от переменных $x_1, \dots, x_5$. Заметим, что $g_1, g_2, g_3 \in \{0, x_4, x_5, x_4 \oplus x_5\}$. Если среди функций g_1, g_2, g_3 есть две равные, например, $g_1 = g_2$, то преобразуем выражение к виду

$$x_3(x_1 x_2 \oplus g_3) \oplus (x_1 \oplus x_2)g_1 \oplus h.$$

При реализации полученного выражения СФЭ достаточно трех элементов конъюнкции. Аналогично поступим, если хотя бы одна из функций g_1, g_2, g_3 равна нулю.

Если все три функции g_1, g_2, g_3 различны и не равны нулю, то, не ограничивая общности рассуждений, выражение имеет вид

$$x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3(x_4 \oplus x_5) \oplus h.$$

Перепишем это выражение в виде

$$(x_1x_2 \oplus x_4)(x_1 \oplus x_3) \oplus x_1x_2 \oplus x_5(x_2 \oplus x_3) \oplus h.$$

При реализации полученного выражения СФЭ достаточно трех элементов конъюнкции.

Индуктивный переход полностью обоснован.

Теорема 5.5 доказана. □

Теперь исследуем нижнюю оценку мультипликативной сложности некоторых квазиквадратичных функций. Сначала докажем несколько вспомогательных лемм.

Функция алгебры логики $f(x_1, \dots, x_n)$ называется *линейной по переменной* x_i , $1 \leq i \leq n$, если функция f может быть представлена в виде $x_i \oplus f_1(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$, где f_1 – некоторая функция алгебры логики.

Лемма 5.4. [272] *Если функция алгебры логики $\varphi(x_1, \dots, x_k, x_{k+1}, \dots, x_n)$ не является линейной по переменным $x_{k+1}, \dots, x_n$, $1 \leq k \leq n$, то в произвольной СФЭ S в базисе $\{x \& y, x \oplus y, 1\}$, реализующей функцию φ , найдется такая вершина v с приписанным ей элементом конъюнкции, что в нее ведет дуга из вершины v_1 , причем для вершины v_1 выполняются следующие условия:*

1) или вершина v_1 является входной, или вершине v_1 приписан элемент сложения по модулю два;

2) в вершине v_1 реализуется функция вида

$$x_i \oplus h(x_{k+1}, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \oplus \psi(x_1, \dots, x_k)$$

для некоторого i , $k + 1 \leq i \leq n$, где h – аффинная функция;

3) для любого пути из входов СФЭ S в вершину v_1 верно, что во всех вершинах этого пути, которым приписаны элементы конъюнкции, реализуются функции, зависящие только от переменных $x_1, \dots, x_k$.

Доказательство. Докажем, что такая вершина v всегда найдется в СФЭ S . Для этого для каждой вершины u в СФЭ S введем понятие ее *конъюнктивной глубины* $d_{\&}(u)$. Если u – входная вершина, то $d_{\&}(u) = 0$. Если u не является входной вершиной и ей приписан элемент сложения по модулю два, то $d_{\&}(u) = \max(d_{\&}(u_1), \dots, d_{\&}(u_s))$, где $u_1, \dots, u_s$ – все вершины, которые встречаются на всех путях из входов СФЭ S в вершину u . Если u не является входной вершиной и ей приписан элемент конъюнкции, то $d_{\&}(u) = \max(d_{\&}(u_1), \dots, d_{\&}(u_s)) + 1$, где $u_1, \dots, u_s$ – все вершины, которые встречаются на всех путях из входов СФЭ S в вершину u .

Теперь рассмотрим в СФЭ S все такие вершины $u_1, \dots, u_{s_1}$, что им приписаны элементы конъюнкции и $d_{\&}(u_j) = 1$, $j = 1, \dots, s_1$. Если хотя бы в одну из них ведет дуга из вершины, в которой реализуется функция

$$x_i \oplus h(x_{k+1}, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \oplus \psi(x_1, \dots, x_k),$$

где $k + 1 \leq i \leq n$, а h – аффинная функция, то требуемая вершина v найдена. В противном случае во всех вершинах $u_1, \dots, u_{s_1}$ реализуются функции, зависящие только от переменных $x_1, \dots, x_k$. Пусть уже рассмотрены все вершины, которым приписаны элементы конъюнкции, с конъюнктивной глубиной d , но

требуемая вершина v не найдена. Значит, во всех вершинах, которым приписаны элементы конъюнкции и конъюнктивная глубина которых не больше d , реализуются функции, зависящие только от переменных $x_1, \dots, x_k$. Рассмотрим в СФЭ S все такие вершины $u_{s_d+1}, \dots, u_{s_{d+1}}$, что им приписаны элементы конъюнкции и $d_{\&}(u_j) = d + 1, j = s_d + 1, \dots, s_{d+1}$. Если хотя бы в одну из них ведет дуга из вершины, в которой реализуется функция

$$x_i \oplus h(x_{k+1}, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \oplus \psi(x_1, \dots, x_k),$$

где $k + 1 \leq i \leq n$, а h – аффинная функция, то требуемая вершина v найдена. И т.д. в случае, если требуемая вершина не найдена.

Предположим, что мы рассмотрели все вершины СФЭ S , а требуемую вершину v не нашли. Но это означает, что во всех вершинах, которым приписаны элементы конъюнкции, реализуются функции, зависящие только от переменных $x_1, \dots, x_k$. Но функции, которые реализуются в вершинах с приписанными им элементами сложения по модулю два, являются линейными комбинациями переменных и функций, которые реализуются в вершинах с приписанными им элементами конъюнкции. Значит, все функции, которые реализуются в СФЭ S , являются линейными по переменным $x_{k+1}, \dots, x_n$. Получаем противоречие, т.к. функция φ не является линейной по переменным $x_{k+1}, \dots, x_n$. Следовательно, требуемая вершина v в СФЭ S найдется.

Лемма 5.4 доказана. □

Теперь докажем основную лемму 5.5, которую будем применять при доказательстве нижних оценок.

Лемма 5.5. [272] *Если*

$$f_{n,\varphi}(x_1, \dots, x_n) = \varphi(x_1, \dots, x_k) \oplus x_{k+1}x_{k+2} \oplus x_{k+3}x_{k+4} \oplus \dots \oplus x_{n-1}x_n,$$

где $n \geq k$, то $\mu(f_{n,\varphi}) = \mu(\varphi) + (n - k)/2$.

Доказательство. Верхняя оценка. Для того, чтобы получить СФЭ S , реализующую функцию $f_{n,\varphi}$ с мультипликативной сложностью $\mu(\varphi) + (n - k)/2$, достаточно построить в базисе $\{x \& y, x \oplus y, 1\}$ СФЭ S_1 , реализующую функцию φ с мультипликативной сложностью $\mu(\varphi)$, добавить $(n - k)/2$ элементов конъюнкции для реализации произведений $x_{k+1}x_{k+2}, \dots, x_{n-1}x_n$ и элементы сложения по модулю два.

Нижнюю оценку докажем индукцией по n , $n \geq k$. *Базис индукции* $n = k$ выполняется, так как $\mu(f_{k,\varphi}) = \mu(\varphi)$.

Индуктивный переход. Пусть лемма 5.5 верна для всех функций такого вида, зависящих менее, чем от n переменных. Рассмотрим произвольную СФЭ S в базисе $\{x \& y, x \oplus y, 1\}$, реализующую функцию $f_{n,\varphi}$. Рассмотрим в СФЭ S такую вершину v с приписанным ей элементом конъюнкции, что в нее ведет дуга из вершины v_1 , причем для вершины v_1 выполняются следующие условия:

- 1) или вершина v_1 является входной, или вершине v_1 приписан элемент сложения по модулю два;
- 2) в вершине v_1 реализуется функция вида

$$x_i \oplus h(x_{k+1}, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \oplus \psi(x_1, \dots, x_k),$$

где $i \geq k + 1$, h – аффинная функция;

- 3) для любого пути из входов СФЭ S в вершину v_1 верно, что во всех вершинах этого пути, которым приписаны элементы конъюнкции, реализуются функции, зависящие только от переменных $x_1, \dots, x_k$.

По лемме 5.4 такая вершина v всегда найдется в СФЭ S , т.к. функция $f_{\varphi,n}$ не является линейной по переменным $x_{k+1}, \dots, x_n$. Не ограничивая общности рассуждений, пусть $i = n$. Подставим в функцию $f_{n,\varphi}$ вместо переменной x_n функцию $h \oplus \psi$, а вместо переменной x_{n-1} функцию $h \oplus \psi \oplus 1$. Полу-

чим функцию $f_{(n-2),\varphi}$. Пусть $u_1, \dots, u_s$ – все такие вершины СФЭ S , что им приписаны элементы конъюнкции и от каждой из них существует путь в вершину v_1 . Пусть $\psi_1(x_1, \dots, x_k), \dots, \psi_s(x_1, \dots, x_k)$ – функции алгебры логики, которые соответственно реализуются в вершинах $u_1, \dots, u_s$. Заметим, что $\psi = h_1 \oplus \sum_{j=1}^s a_j \psi_j$, где $a_j \in E_2$, $j = 1, \dots, s$, а $h_1(x_1, \dots, x_k)$ – некоторая аффинная функция.

Преобразуем СФЭ S . На вход x_n подадим функцию $h \oplus h_1 \oplus \sum_{j=1}^s a_j \psi_j$. Для этого соединим через элементы сложения по модулю два вершины $u_1, \dots, u_s$ и аффинную функцию $h \oplus h_1$ (ее можно реализовать без элементов конъюнкции). На вход x_{n-1} аналогичным образом подадим функцию $1 \oplus h \oplus h_1 \oplus \sum_{j=1}^s a_j \psi_j$. Тогда на один из входов элемента конъюнкции в вершине v поступит 0. Удалив этот элемент конъюнкции из СФЭ, получим новую СФЭ S' . СФЭ S' реализует функцию $f_{(n-2),\varphi}$. По предположению индукции в любой СФЭ, реализующей функцию $f_{(n-2),\varphi}$, не менее $\mu(\varphi) + (n - k - 2)/2$ элементов конъюнкции, т.е. $\mu(S') \geq \mu(\varphi) + (n - k - 2)/2$. Отсюда получаем, что в произвольной СФЭ S , реализующей функцию $f_{n,\varphi}$, не менее $\mu(\varphi) + (n - k)/2$ элементов конъюнкции, т.е. $\mu(f_{n,\varphi}) \geq (n - k)/2$.

Лемма 5.5 доказана. □

Теорема 5.6. [272] *Если $f_n(x_1, \dots, x_n) = x_1 x_2 x_3 \oplus x_4 x_5 \oplus x_6 x_7 \oplus \dots \oplus x_{n-1} x_n$, где $n = 2m + 1$, $n \geq 3$, то $\mu(f_n) = m + 1$.*

Доказательство. Теорема 5.6 следует из леммы 5.5 при $\varphi(x_1, x_2, x_3) = x_1 x_2 x_3$. В самом деле, докажем, что $\mu(x_1 x_2 x_3) = 2$. Верхняя оценка очевидна. Нижняя оценка следует из свойства $\mu(f) \geq \deg(f) - 1$, верного для произвольной функции f [195].

Теорема 5.6 доказана. □

Лемма 5.6. [272] *Если $\varphi(x_1, \dots, x_5) = x_1 x_2 x_3 \oplus x_1 x_4 \oplus x_2 x_5 \oplus x_3 (a x_4 \oplus b x_5)$,*

где $a, b \in E_2$, то $\mu(\varphi) = 3$.

Доказательство. Верхняя оценка доказана при доказательстве теоремы 5.5.

Докажем нижнюю оценку. Рассмотрим произвольную СФЭ S в базисе $\{x \& y, x \oplus y, 1\}$, реализующую функцию φ . Рассмотрим в СФЭ S такую вершину v с приписанным ей элементом конъюнкции, что в нее ведет дуга из вершины v_1 , причем для вершины v_1 выполняются следующие условия:

- 1) или вершина v_1 является входной, или вершине v_1 приписан элемент сложения по модулю два;
- 2) в вершине v_1 реализуется функция вида $cx_4 \oplus dx_5 \oplus \psi(x_1, x_2, x_3)$, где $c, d \in E_2$, c, d не равны одновременно нулю;
- 3) для любого пути из входов СФЭ S в вершину v_1 верно, что во всех вершинах этого пути, которым приписаны элементы конъюнкции, реализуются функции, зависящие только от переменных x_1, x_2, x_3 .

По лемме 5.4 такая вершина v всегда найдется, т.к. функция φ не является линейной по переменным x_4, x_5 . Пусть, не ограничивая общности рассуждений, $d = 1$. Возможны следующие случаи.

1. $\deg(\psi) \leq 1$. Подставим в функцию φ вместо переменной x_5 функцию $cx_4 \oplus \psi$. Получим функцию φ_1 , такую, что $\deg(\varphi_1) = 3$. Преобразуем СФЭ S : на вход x_5 подадим функцию $cx_4 \oplus \psi$. Тогда на один из входов элемента конъюнкции в вершине v поступит 0. Удалив этот элемент конъюнкции из СФЭ, получим новую СФЭ S' . СФЭ S' реализует функцию φ_1 , а значит, $\mu(S') \geq 2$. Отсюда получаем, что $\mu(S) \geq 3$.

2. $\deg(\psi) = 2$. Тогда в СФЭ S найдется вершина v_2 , которой приписан элемент конъюнкции, в вершину v_2 ведут дуги из двух вершин, в которых реализуются аффинные функции $g_1(x_1, x_2, x_3), g_2(x_1, x_2, x_3)$ соответственно, и найдется путь из вершины v_2 в вершину v_1 . Подставим в функцию φ вместо переменной x_5 функцию $cx_4 \oplus \psi$. Получим функцию φ_1 . Преобразуем СФЭ

S : на вход x_5 подадим функцию $cx_4 \oplus \psi$. Тогда на один из входов элемента конъюнкции в вершине v поступит 0. Удалив этот элемент конъюнкции из СФЭ, получим новую СФЭ S' . Вершина v_2 в СФЭ S' останется. СФЭ S' реализует функцию φ_1 , которая не является линейной по переменной x_4 . Значит, в СФЭ S' есть еще хотя бы одна вершина v_3 , не совпадающая с вершиной v_2 , которой приписан элемент конъюнкции. Отсюда $\mu(S') \geq 2$, и $\mu(S) \geq 3$.

3. $\deg(\psi) \geq 3$. Тогда в СФЭ S найдутся еще две различные вершины, кроме вершины v , которым приписаны элементы конъюнкции и в которых реализуются функции, зависящие только от переменных x_1, x_2, x_3 . Отсюда $\mu(S) \geq 3$.

Лемма 5.6 доказана. □

Теорема 5.7. [272] *Если*

$$f_n(x_1, \dots, x_n) = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3(x_4 \oplus x_5) \oplus x_6x_7 \oplus x_8x_9 \oplus \dots \oplus x_{n-1}x_n,$$

где $n = 2m + 1$, $n \geq 5$, то $\mu(f_n) = m + 1$.

Доказательство. Теорема 5.7 следует из лемм 5.5 и 5.6 при $\varphi(x_1, x_2, x_3) = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3(x_4 \oplus x_5)$.

Теорема 5.7 доказана. □

Лемма 5.7. [272] *Если $\varphi(x_1, \dots, x_n) = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$, то $\mu(\varphi) = 4$.*

Доказательство. Верхняя оценка. Рассмотрим выражение для функции φ :

$$x_1(x_2x_3 \oplus x_4) \oplus x_2x_5 \oplus x_3x_6.$$

По этому выражению можно построить СФЭ S в базисе $\{x \& y, x \oplus y, 1\}$, реализующую функцию φ и содержащую четыре элемента конъюнкции.

Нижняя оценка. Рассмотрим произвольную СФЭ S в базисе $\{x \& y, x \oplus y, 1\}$, реализующую функцию φ . Рассмотрим в СФЭ S такую вершину v с приписанным ей элементом конъюнкции, что в нее ведет дуга из вершины v_1 , причем для вершины v_1 выполняются следующие условия:

1) или вершина v_1 является входной, или вершине v_1 приписан элемент сложения по модулю два;

2) в вершине v_1 реализуется функция вида $c_1x_4 \oplus c_2x_5 \oplus c_3x_6 \oplus \psi(x_1, x_2, x_3)$, где $c_1, c_2, c_3 \in E_2$, и c_1, c_2, c_3 не равны одновременно нулю;

3) для любого пути из входов СФЭ S в вершину v_1 верно, что во всех вершинах этого пути, которым приписаны элементы конъюнкции, реализуются функции, зависящие только от переменных x_1, x_2, x_3 .

По лемме 5.4 такая вершина v всегда найдется, так как функция φ не является линейной по переменным x_4, x_5, x_6 . Пусть, не ограничивая общности рассуждений, $c_3 = 1$. Возможны следующие случаи.

1. $\deg(\psi) \leq 1$. Подставим в функцию φ вместо переменной x_6 функцию $c_1x_4 \oplus c_2x_5 \oplus \psi$. Получим функцию φ_1 , удовлетворяющую условиям леммы 5.6. Преобразуем СФЭ S : на вход x_6 подадим функцию $c_1x_4 \oplus c_2x_5 \oplus \psi$. Тогда на один из входов элемента конъюнкции в вершине v поступит 0. Удалив этот элемент конъюнкции из СФЭ, получим новую СФЭ S' . СФЭ S' реализует функцию φ_1 , а значит, по лемме 5.6 $\mu(S') \geq 3$. Отсюда получаем, что $\mu(S) \geq 4$.

2. $\deg(\psi) = 2$. Тогда в СФЭ S найдется вершина v_2 , которой приписан элемент конъюнкции, в вершину v_2 ведут дуги из двух вершин, в которых реализуются аффинные функции $g_1(x_1, x_2, x_3), g_2(x_1, x_2, x_3)$ соответственно, и найдется путь из вершины v_2 в вершину v_1 . Подставим в функцию φ вместо переменной x_6 функцию $c_1x_4 \oplus c_2x_5 \oplus \psi$. Получим функцию φ_1 . Преобразуем СФЭ S : на вход x_6 подадим функцию $c_1x_4 \oplus c_2x_5 \oplus \psi$. Тогда на один из

входов элемента конъюнкции в вершине v поступит 0. Удалив этот элемент конъюнкции из СФЭ, получим новую СФЭ S' . Вершина v_2 в СФЭ S' останется. СФЭ S' реализует функцию φ_1 , которая имеет вид $x_4x_1 \oplus x_5x_2 \oplus c_1x_3x_4 \oplus c_2x_3x_5 \oplus \varphi_2(x_1, x_2, x_3)$. По лемме 5.4 в СФЭ S' найдется такая вершина v_3 с приписанным ей элементом конъюнкции, что в нее ведет дуга из некоторой вершины v_4 , причем для вершины v_4 выполняются следующие условия:

1) или вершина v_4 является входной, или вершине v_4 приписан элемент сложения по модулю два;

2) в вершине v_4 реализуется функция вида $d_1x_4 \oplus d_2x_5 \oplus \psi_1(x_1, x_2, x_3)$, где $d_1, d_2 \in E_2$, и d_1, d_2 не равны одновременно нулю;

3) для любого пути из входов СФЭ S в вершину v_4 верно, что во всех вершинах этого пути, которым приписаны элементы конъюнкции, реализуются функции, зависящие только от переменных x_1, x_2, x_3 .

Заметим, что вершина v_3 не лежит на путях из входов СФЭ S в вершину v_2 и не совпадает с вершиной v_2 . Пусть, не ограничивая общности рассуждений, $d_2 = 1$. Подставим в функцию φ_1 вместо переменной x_5 функцию $d_1x_4 \oplus \psi_1$. Получим функцию φ_3 , которая имеет вид $x_4x_1 \oplus cx_3x_4 \oplus \varphi_4(x_1, x_2, x_3)$, где $c \in E_2$. Преобразуем СФЭ S' : на вход x_5 подадим функцию $cx_4 \oplus \psi_1$. Тогда на один из входов элемента конъюнкции в вершине v_3 поступит 0. Удалив этот элемент конъюнкции из СФЭ, получим новую СФЭ S'' . Заметим, что вершина v_2 в СФЭ S'' останется. СФЭ S'' реализует функцию φ_3 , которая не является линейной по переменной x_4 . Значит, в СФЭ S'' найдется еще хотя бы одна вершина с приписанным ей элементом конъюнкции, кроме вершины v_2 . Отсюда $\mu(S'') \geq 2$, и $\mu(S) \geq 4$.

3. $\deg(\psi) \geq 3$. Тогда в СФЭ S найдутся две различные вершины v_2, v_3 , лежащие на путях из входов СФЭ S в вершину v_1 , которым приписаны элементы конъюнкции и в которых реализуются функции, зависящие только от

переменных x_1, x_2, x_3 . Подставим в функцию φ вместо переменной x_6 функцию $c_1x_4 \oplus c_2x_5 \oplus \psi$. Получим функцию φ_1 . Преобразуем СФЭ S : на вход x_6 подадим функцию $c_1x_4 \oplus c_2x_5 \oplus \psi$. Тогда на один из входов элемента конъюнкции в вершине v поступит 0. Удалив этот элемент конъюнкции из СФЭ, получим новую СФЭ S' . Вершины v_2, v_3 в СФЭ S' останутся. СФЭ S' реализует функцию φ_1 , которая имеет вид $x_4x_1 \oplus x_5x_2 \oplus c_1x_3x_4 \oplus c_2x_3x_5 \oplus \varphi_2(x_1, x_2, x_3)$. Значит, в СФЭ S' есть еще хотя бы одна вершина, кроме вершин v_2, v_3 , с приписанным ей элементом конъюнкции. Отсюда $\mu(S') \geq 3$, и $\mu(S) \geq 4$.

Лемма 5.7 доказана. □

Теорема 5.8. [272] *Если*

$$f_n(x_1, \dots, x_n) = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_7x_8 \oplus x_9x_{10} \oplus \dots \oplus x_{n-1}x_n,$$

где $n = 2m$, $n \geq 6$, то $\mu(f_n) = m + 1$.

Доказательство. Теорема 5.8 следует из леммы 5.5 при $\varphi(x_1, x_2, x_3) = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$. По лемме 5.7 верно, что $\mu(\varphi) = 4$.

Теорема 5.8 доказана. □

Пусть Q – это множество всех квазиквадратичных функций алгебры логики, имеющих вид $\varphi(x_1, x_2, x_3) \oplus q(x_1, \dots, x_n)$, где $\deg(\varphi) = 3$, а q – квадратичная функция, и $\mu_Q(n) = \max_{f(x_1, \dots, x_n) \in Q} \mu(f)$.

Следствие 5.1. [272] *При $n \geq 5$ справедливо равенство $\mu_Q(n) = \lceil (n+1)/2 \rceil$.*

Доказательство. Следствие 5.1 вытекает из теорем 5.5, 5.6 и 5.8.

Следствие 5.1 доказано. □

Заключение

Основные результаты работы

1. Сформулированы задачи о длине функций k -значной логики в классах поляризованных полиномиальных форм (ППФ), обобщенно поляризованных полиномиальных форм (ОППФ) и полиномиальных нормальных форм (ПНФ) при простых $k \geq 3$. Найдены верхние и нижние оценки наибольшей длины функций k -значной логики в классах ППФ, ОППФ, ПНФ при простых $k \geq 3$ и в классе псевдополиномиальных форм (ПСПФ) при $k = 2$. Предложены методы построения соответствующих полиномиальных форм, обеспечивающие верхние оценки. При каждом простом k , $k \geq 3$, найдено точное значение наибольшей длины функций k -значной логики, зависящих от одной переменной, в классе ППФ.
2. Сформулирована задача о сложности систем функций алгебры логики и функций k -значной логики при простых $k \geq 3$ в классе ППФ. Найдены точные значения сложности самых сложных систем функций k -значной логики, содержащих хотя бы две функции, в классе ППФ при $k = 2$ и $k = 3$.
3. Сформулированы задачи о сложности полиномов, приближающих функции k -значной логики с заданной точностью при простых $k \geq 3$. Найдены оценки, в том числе асимптотически точные для длины и ранга полиномов по модулю k , приближающих с заданной точностью функции k -значной логики при простых k .
4. Найдены функциональные свойства функций k -значной логики, инвариантных относительно связных преобразований, и структурные свойства их полиномов относительно операций конечного поля из k элементов.

При помощи этих свойств доказана полиномиальность задачи распознавания принадлежности функции k -значной логики, заданной полиномом по модулю k , к предполным классам самодвойственных функций (при простых k). На основе полученного доказательства сформулирован подход к построению полиномиальных распознающих алгоритмов.

5. Доказана полиномиальность задачи распознавания сохранения функцией k -значной логики, заданной полиномом по модулю k , вполне рефлексивного и вполне транзитивного отношения (при простых k). Как следствие получена полиномиальность задач распознавания принадлежности функции k -значной логики, заданной полиномом по модулю k , к предполным классам монотонных функций, функций, сохраняющих разбиение, и к предполным классам типа В (при простых k). Доказана полиномиальность задачи распознавания принадлежности функции k -значной логики, заданной полиномом относительно операций конечного поля из k элементов, к предполным классам линейных функций.
6. Предложен канонический вид полиномиальных функций по составному модулю k . При каждом составном k доказана линейная оценка алгоритмической сложности (в алгоритмической модели схем из функциональных элементов, СФЭ) задачи распознавания полиномиальности функции k -значной логики, заданной вектором своих значений, и в случае положительного ответа построения вектора коэффициентов ее канонического полинома по модулю k .
7. Предложена алгоритмическая модель СФЭ с некоторым ограничением структуры – СФЭ с разделенными переменными (СФЭРП). В модели СФЭРП доказаны нелинейные нижние оценки, в том числе достижимые для алгоритмической сложности задачи построения вектора коэффици-

ентов полинома Жегалкина функции алгебры логики, заданной вектором своих значений.

8. Найдены точные значения мультипликативной сложности функций алгебры логики, представимых как сумма по модулю два или произведения всех переменных и квадратичной функции, или двух мультиаффинных функций, а также найдено точное значения наибольшей мультипликативной сложности функций в одном классе квазиквадратичных функций. Разработаны методы построения СФЭ в базисе Жегалкина, обеспечивающие верхние оценки мультипликативной сложности для соответствующих функций.

Можно предложить дальнейшее развитие результатов, полученных в работе, в следующих направлениях.

1. Исследование полиномиальных представлений функций k -значных логик при простых k . Например, получение асимптотики длины функций k -значных логик в классах поляризованных полиномиальных форм и обобщенно поляризованных полиномиальных форм при $k \geq 3$, в классе полиномиальных нормальных форм при $k \geq 2$, обобщение псевдополиномиальных форм на случай произвольного простого k и получение асимптотики длины функций k -значной логики в классе псевдополиномиальных форм при $k \geq 2$; изучение длины в классах полиномиальных форм для функций из определенных множеств, например, симметрических функций или функций определенной степени; рассмотрение новых видов полиномиальных форм, например, арифметических полиномов, и исследование представлений функций k -значных логик ими.
2. Исследование сложности полиномиальных представлений систем функций k -значной логики при простых k . Например, получение асимптотики

сложности систем функций k -значной логики в классе поляризованных полиномиальных форм при $k \geq 5$ и асимптотики сложности систем функций k -значной логики в других классах полиномиальных форм.

3. Исследование полиномиальных представлений функций k -значных логик при составных k . Например, получение асимптотики длины полиномиального представления для полиномиальных функций k -значной логики при составных k или точности приближения всех функций k -значной логики полиномиальными функциями при составных k .
4. Построение полиномиальных алгоритмов для распознавания важных свойств функций k -значных логик, заданных полиномами (при простых k), и разработка подходов к получению таких алгоритмов. Например, исследование алгоритмической сложности распознавания принадлежности функции k -значной логики, заданной полиномом по модулю k , к предполным классам, определяемым центральными отношениями.
5. Исследование мультипликативной сложности функций алгебры логики и разработка методов получения оценок этой сложности. Например, получение асимптотики функции Шеннона мультипликативной сложности функций определенной степени; нахождение мультипликативной сложности функций некоторых видов или функций из некоторых классов.

Список литературы

- [1] Авсаркисян Г.С., Брайловский Г.С. Представление логических функций в виде полиномов Жегалкина // Автоматика и вычислительная техника. 1975. 6. С. 6–10.
- [2] Авсаркисян Г.С. Представление булевых функций суммой по модулю 2 импликаций аргументов // Автоматика и вычислительная техника. 1977. 1. С. 8–11.
- [3] Авсаркисян Г.С. Обобщенные полиномиальные формы булевых функций и синтез многовыходных логических схем // Автоматика и телемеханика. 1983. 11. С. 111–119.
- [4] Айзенберг Н.Н., Семейон И.В., Циткин А.И. Мощность класса функций k -значной логики от n переменных, представимых полиномами по модулю k // В кн. Многоустойчивые элементы и их применение. М.: Сов. радио, 1971. С. 79–83.
- [5] Айзенберг Н.Н., Семейон И.В. Некоторые критерии представимости функций k -значной логики полиномами по модулю k // В кн. Многоустойчивые элементы и их применение. М.: Сов. радио, 1971. С. 84–88.
- [6] Алексеев В.Б. О расшифровке некоторых классов монотонных многозначных функций // ЖВМиМФ. 1976. 16. 1. С. 189–198.
- [7] Алексеев В.Б., Емельянов Н.Р. Метод построения быстрых алгоритмов в k -значной логике // Математические заметки. 1985. 38. 1. С. 148–156.
- [8] Алексеев В.Б. Ступенчатые билинейные алгоритмы и распознавание полноты в k -значных логиках // Известия вузов. Математика. 1988. 7. С. 19–27.

- [9] Алексеев В.Б. Логические полукольца и их использование для построения быстрых алгоритмов // Вестник Московского университета. Серия 1. Математика. Механика. 1997. 1. С. 22–29.
- [10] Алексеев В.Б. От метода Карацубы для быстрого умножения чисел к быстрым алгоритмам для дискретных функций // Труды МИАН. 1997. **218**. С. 20–27.
- [11] Алексеев В.Б., Омаров Р.Р. О приближении максимально-нелинейных булевых функций почти линейными функциями // Дискретная математика. 2012. **24**. 3. С. 73–81.
- [12] Алексеев В.Б., Смирнов А.В. О точной и приближенной билинейной сложности умножения матриц размеров 4×2 и 2×2 // Современные проблемы математики. 2013. 17. С. 135–152.
- [13] Алексеев Е.К. О некоторых алгебраических и комбинаторных свойствах корреляционно-иммунных булевых функций // Дискретная математика. 2010. **22**. 3. С. 110–126.
- [14] Алехина М.А., Барсукова О.Ю. О надежности схем, реализующих функции из P_3 // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. 2012. 1. С. 57–65.
- [15] Алехина М.А., Барсукова О.Ю. Оценки ненадежности схем в базисе Россера–Туркетта // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. 2014. 1(29). С. 5–19.
- [16] Андреев А.Е. Универсальный принцип самокоррекции // Математический сборник. Новая серия. 1985. **127**. 2. С. 147–172.
- [17] Андреев А.Е. Об одном семействе булевых матриц // Вестник МГУ. Серия 1. Математика. Механика. 1986. 2. С. 97–100.

- [18] Артюхов В.Л., Кондратьев В.Н., Шалыто А.А. Реализация булевых функций арифметическими полиномами // Автоматика и телемеханика. 1988. 4. С. 138–147.
- [19] Баев В.В. О некоторых алгоритмах построения аннигиляторов низкой степени для булевых функций // Дискретная математика. 2006. 18. 3. С. 138–151.
- [20] Баев В.В. Усовершенствованный алгоритм поиска аннигиляторов низкой степени для многочлена Жегалкина // Дискретная математика. 2007. 19. 4. С. 132–138.
- [21] Балюк А.С. О верхней оценке сложности задания квазиполиномами функций над конечными полями // Известия Иркутского государственного университета. Серия: Математика. 2014. 10. С. 3–12.
- [22] Бородина Ю.В., Бородин П.А. Синтез легкотестируемых схем в базисе Жегалкина при константных неисправностях типа 0 на выходах элементов // Дискретная математика. 2010. 22. 3. С. 127–133.
- [23] Бруснецов Н.П. Микро-ЭВМ СЕТУНЬ // Вестник МГУ. 1962. N 4. С. 3–12.
- [24] Буряков М.Л., Логачев О.А. Об уровне аффинности булевых функций // Дискретная математика. 2005. 17. 4. С. 98–107.
- [25] Буряков М.Л. О связи уровня аффинности с криптографическими параметрами булевых функций // Дискретная математика. 2008. 20. 2. С. 3–14.
- [26] Бухман А.В. О сложности распознавания сохранения функциями многозначных логик, заданных полиномами, некоторых множеств // Вест-

ник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2011. 3. С. 38–43.

- [27] Бухман А.В. О применении обобщенных полиномов для построения алгоритмов распознавания свойств k -значных функций, заданных полиномами // Дискретная математика. 2012. **24**. 3. С. 51–61.
- [28] Бухман А.В. О свойствах полиномов периодических функций и сложности распознавания периодичности по полиному булевой функции // Дискретная математика. 2014. **26**. 1. С. 21–31.
- [29] Виноградов Ю.А. О конечнозначных моделях схем с дискретным функционированием // Сб. Проблемы кибернетики. Вып. 23. М.: Наука, 1970. С. 119–126.
- [30] Виноградов Ю.А. О k -значных моделях схем ЭВМ // Сб. Проблемы кибернетики. Вып. 26. М.: Наука, 1973. С. 259–263.
- [31] Виноградов Ю.А. О синтезе трехзначных МДП-схем // Сб. Математические вопросы кибернетики. Вып. 3. М.: Наука, Физматлит, 1991. С. 187–198.
- [32] Винокуров С.Ф., Казимиров А.С. Перечисление операторных классов булевых функций // Известия Иркутского государственного университета. Серия: Математика. 2009. 2. С. 40–55.
- [33] Винокуров С.Ф., Перязев Н.А. Полиномиальные разложения булевых функций по невырожденным функциям // Алгебра и логика. 1991. **30**. 6. С. 631–637.
- [34] Винокуров С.Ф., Перязев Н.А. Представление булевых функций полиномиальными формами // Кибернетика и системный анализ. 1992. 2. С. 210–213.

- [35] Винокуров С.Ф., Перязев Н.А. Разложение булевых функций на сумму произведений подфункций // Дискретная математика. 1993. **5**. 3. С. 102–104.
- [36] Винокуров С.Ф., Перязев Н.А. Полиномиальная декомпозиция булевых функций // Математические заметки. 1993. **53**. 2. С. 25–29.
- [37] Винокуров С.Ф., Перязев Н.А. Полиномиальная декомпозиция булевых функций по образам однородных операторов от невырожденных функций // Известия вузов. Математика. 1996. 1. С. 17–21.
- [38] Винокуров С.Ф., Казимиров А.С. О сложности одного класса булевых функций // Известия Иркутского государственного университета. Серия: Математика. 2010. **3**. 4. С. 2–6.
- [39] Вороненко А.А. О сложности распознавания монотонности // Сб. Математические вопросы кибернетики. Вып. 8. М.: Наука, 1999. С. 301–303.
- [40] Вороненко А.А. О методе разложения для распознавания принадлежности инвариантным классам // Дискретная математика. 2002. **14**. 4. С. 110–116.
- [41] Вороненко А.А. Бесповторность распознается схемами линейной сложности // Дискретная математика. 2005. **7**. 4. С. 111–115.
- [42] Вялый М.Н., Леонтьев В.К., Осетров М.В. Монотонные булевы полиномы // Дискретный анализ и исследование операций. Серия 1. 2002. **9**. 4. С. 41–49.
- [43] Вялый М.Н. Алгоритмические задачи с таблицами значений булевых полиномов // Труды Института системного программирования. 2004. 6. С. 51–64.

- [44] Гаврилов Г.П. О надструктуре класса полиномов в многозначных логиках // Дискретная математика. 1996. **8**. 3. С. 90–97.
- [45] Гаврилов Г.П. О замкнутых классах многозначной логики, содержащих класс полиномов // Дискретная математика. 1997. **9**. 2. С. 12–23.
- [46] Гашков С.Б., Сергеев И.С. О сложности линейных булевых операторов с редкими матрицами // Дискретный анализ и исследование операций. 2010. **17**. 3. С. 3–18.
- [47] Герасимов И.Н. Декомпозиционный метод синтеза многозначных логических сетей // Автоматика и телемеханика. 1983. 5. С. 167–171.
- [48] Глаголев В.В. Некоторые оценки дизъюнктивных нормальных форм функций алгебры логики // Сб. Проблемы кибернетики. Вып. 19. М.: Наука, 1967. С. 75–94.
- [49] Горожин А.Д., Крайнов К.С. Построение полностью самопроверяемых комбинационных устройств с использованием полиномиальных форм // Автоматика и телемеханика. 1979. 12. С. 159–166.
- [50] Горожин А.Д. Синтез полностью самопроверяемых синхронных автоматов с использованием полиномиальных форм // Автоматика и телемеханика. 1982. 1. С. 141–150.
- [51] Горшков С.П. О сложности распознавания мультиаффинности, биюнктивности, слабой положительности и слабой отрицательности // Обзор промышленной и прикладной математики. Серия Дискретная математика. 1997. **4**. 2. С. 216–237.
- [52] Горшков С.П. О сложности нахождения приведенных представлений слабо положительных и слабо отрицательных булевых функций // Прикладная дискретная математика. 2008. 1. С. 7–9.

- [53] Гринчук М.И., Сергеев И.С. Редкие циркулянтные матрицы и нижние оценки сложности некоторых булевых операторов // Дискретный анализ и исследование операций. 2011. **18**. 5. С. 38–53.
- [54] Джавадов Р.М. О сложности приближенного задания функций алгебры логики // Доклады АН СССР. 1982. **265**. 1. С. 24–27.
- [55] Дзюжаньски П., Малюгин В., Шмерко В., Янушкевич С.Н. Линейные модели схем на многозначных элементах // Автоматика и телемеханика. 2002. 6. С. 99–119.
- [56] Емельянов Н.Р. О сложности задачи выразимости в многозначных логиках // Доклады АН СССР. 1985. **282**. 3. С. 525–529.
- [57] Емельянов Н.Р. О сложности решения задачи -выразимости в k -значной логике // Дискретная математика. 1989. **1**. 2. С. 65–77.
- [58] Жегалкин И.И. О технике вычислений предложений в символической логике // Математический сборник. 1927. **34**. С. 9–28.
- [59] Жегалкин И.И. Арифметизация символической логики // Математический сборник. 1928. **35**. 3-4. С. 311–377.
- [60] Забалуев Р.Н. О сложности реализации полиномов Жегалкина // Дискретная математика. 2004. **16**. 1. С. 79–94.
- [61] Закревский А.Д. Минимальная реализация частичных булевых функций полиномами Жегалкина // Автоматика и телемеханика. 1996. 5. С. 134–140.
- [62] Закревский А.Д. Алгоритмы синтеза полиномов, реализующих слабо определенные булевы функции и системы // Автоматика и телемеханика. 2004. 6. С. 158–176.

- [63] Зинченко А.С., Пантелеев В.И. Полиномиальные операторные представления k -значной логики // Дискретный анализ и исследование операций. Серия 1. 2006. **13**. 3. С. 13–26.
- [64] Зинченко А.С., Пантелеев В.И. Бинарные термы в полиномиальных представлениях булевых функций // Математические заметки. 2007. **81**. 2. С. 217–225.
- [65] Зубков А.М., Серов А.А. Оценка числа булевых функций, имеющих аффинные приближения заданной точности // Дискретная математика. 2010. **22**. 4. С. 3–19.
- [66] Зыков К.А. О сравнении сложности двух способов реализации некоторых линейных булевых преобразований // Дискретная математика. 1996. **8**. 2. С. 151–159.
- [67] Кабатянский Г.А., Панченко В.И. Упаковки и покрытия пространства Хэмминга шарами единичного радиуса // Проблемы передачи информации. 1988. **XXIV**. 4. С. 3–16.
- [68] Казимиров А.С., Реймеров С.Ю. Вычислительная оценка сложности полиномиальных представлений булевых функций // Известия Иркутского государственного университета. Серия: Математика. 2010. 4. С. 33–43.
- [69] Казимиров А.С., Реймеров С.Ю. Генетический алгоритм поиска минимальных полиномиальных представлений систем булевых функций // Известия Иркутского государственного университета. Серия: Математика. 2011. 4. С. 82–86.
- [70] Карацуба А.А., Офман Ю.П. Умножение многозначных чисел на автоматах // Доклады АН СССР. 1962. **145**. 2. С. 293–294.

- [71] Катериночкина Н.Н. Поиск максимального верхнего нуля монотонной функции алгебры логики // Доклады АН СССР. 1975. **224**. 3. С. 557–560.
- [72] Катериночкина Н.Н. Поиск максимального верхнего нуля для некоторых подклассов монотонных булевых функций // ЖВМиМФ. 1978. **18**. 2. С. 516–519.
- [73] Катериночкина Н.Н. Поиск максимального верхнего нуля для одного класса монотонных функций k -значной логики // ЖВМиМФ. 1981. **21**. 2. С. 470–481.
- [74] Катериночкина Н.Н. О задаче поиска максимального верхнего нуля для ряда подклассов монотонных булевых функций // ЖВМиМФ. 1987. **27**. 9. С. 1402–1411.
- [75] Катериночкина Н.Н. Поиск максимального нуля для некоторых классов монотонных булевых функций из классификации поста // ЖВМиМФ. 1988. **28**. 9. С. 1397–1406.
- [76] Кириченко К.Д. Верхняя оценка сложности полиномиальных нормальных форм булевых функций // Дискретная математика. 2005. **17**. 3. С. 80–88.
- [77] Кондратьев В.Н., Шалито А.А. Реализация систем логических функций арифметическими полиномами // Автоматика и телемеханика. 1993. 3. С. 135–153.
- [78] Коробков В.К. О монотонных функциях алгебры логики // В кн. Проблемы кибернетики. Вып. 13. М.: Наука, 1965. С. 5–28.

- [79] Коробков В.К. Некоторые обобщения задачи расшифровки монотонных функций алгебры логики // Сб. Дискретный анализ. Вып. 5. Новосибирск: Ин-т матем. СО АН СССР, 1965. С. 19–25.
- [80] Коршунов А.Д. О сложности кратчайших дизъюнктивных нормальных форм булевых функций // Сб. Методы дискретного анализа в изучении булевых функций и графов. Вып. 37. Новосибирск, 1981. С. 9–41.
- [81] Краснова Т.И. О конъюнктивной сложности схем в базисе Жегалкина для одной последовательности булевых функций // Материалы XI Международного семинара “Дискретная математика и ее приложения”. М.: Изд-во механико-математического ф-та МГУ, 2012. С. 138–141.
- [82] Крохин А.А., Сафин К.Л., Суханов Е.В. О строении решетки замкнутых классов полиномов // Дискретная математика. 1997. 9. 2. С. 24–39.
- [83] Кузнецов А.В. О проблемах тождества и функциональной полноты алгебраических систем // В кн. Труды 3-го всесоюзного матем. съезда. Т. 2. М.: Изд-во АН СССР, 1956. С. 145–146.
- [84] Кузьмин А.С., Марков В.Т., Нечаев А.А., Шишков А.Б. Приближение булевых функций мономиальными // Дискретная математика. 2006. 18. 1. С. 9–29.
- [85] Ларин М.В. Транзитивные полиномиальные преобразования колец вычетов // Дискретная математика. 2002. 14. 2. С. 20–32.
- [86] Латыпов Р.Х. Программируемые логические матрицы, пригодные для кольцевого тестирования // Автоматика и телемеханика. 1992. 8. С. 170–174.

- [87] Левашенко В., Морага К., Холвински Г., Янушкевич С.Н., Шмерко В.П. Алгоритм тестирования комбинационных схем на многозначных элементах // Автоматика и телемеханика. 2000. 5. С. 141–156.
- [88] Леонтьев В.К., Морено О. О нулях булевых полиномов // ЖВМиМФ. 1998. 38. 9. С. 1606–1613.
- [89] Леонтьев В.К. О некоторых задачах, связанных с булевыми полиномами // ЖВМиМФ. 1999. 39. 6. С. 1045–1054.
- [90] Леонтьев В.К. Симметрические булевы полиномы // ЖВМиМФ. 2010. 50. 8. С. 1520–1531.
- [91] Лобанов М.С. Точное соотношение между нелинейностью и алгебраической иммунностью // Дискретная математика. 2006. 18. 3. С. 152–159.
- [92] Логачев О.А. Нижняя граница уровня аффинности для почти всех булевых функций // Дискретная математика. 2008. 20. 4. С. 85–88.
- [93] Логачев О.А., Смышляев С.В., Яценко В.В. Новые методы изучения совершенно уравновешенных булевых функций // Дискретная математика. 2009. 21. 2. С. 51–74.
- [94] Лупанов О.Б. О синтезе некоторых классов управляющих систем // Сб. Проблемы кибернетики. Вып. 10. М., 1963. С. 63–97.
- [95] Малюгин В.Д. Реализация булевых функций арифметическими полиномами // Автоматика и телемеханика. 1982. 4. С. 84–93.
- [96] Малюгин В.Д. Полиномиальная реализация кортежей логических функций // Доклады АН СССР. 1982. 265. 6. С.

- [97] Малюгин В.Д. Реализация кортежей булевых функций посредством линейных арифметических полиномов // Автоматика и телемеханика. 1984. 2. С. 114–122.
- [98] Мамонтов А.И., Мещанинов Д.Г. Проблема полноты в функциональной системе линейных полиномов с целыми коэффициентами // Дискретная математика. 2010. **22**. 4. С. 64–82.
- [99] Мамонтов А.И., Мещанинов Д.Г. Алгоритм распознавания полноты в функциональной системе $L(Z)$ // Дискретная математика. 2014. **26**. 1. С. 85–95.
- [100] Маркелов Н.К. Нижняя оценка сложности функций трехзначной логики в классе поляризованных полиномов // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2012. 3. С. 40–45.
- [101] Мартынюк В.В. Исследование некоторых классов в многозначных логиках // Сб. Проблемы кибернетики. Вып. 3. М., 1960. С. 49–60.
- [102] Мелузов А.С. Построение эффективных алгоритмов решения систем полиномиальных булевых уравнений методом опробования части переменных // Дискретная математика. 2011. **23**. 4. С. 66–79.
- [103] Мещанинов Д.Г. О полиномиальной реализации функций k -значной логики. Деп. ВИНТИ 23.10.87, N 7441-B87.
- [104] Мещанинов Д.Г. Некоторые условия представимости функций из P_k полиномами по модулю k // Доклады АН СССР. 1988. **299**. 1. С. 50–53.
- [105] Мещанинов Д.Г. О некоторых свойствах надструктуры класса полиномов в P_k // Математические заметки. 1988. **44**. 5. С. 673–681.

- [106] Мещанинов Д.Г. Перестановочные представления функций k -значной логики // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 1988. 3. С. 61–66.
- [107] Мещанинов Д.Г. О вторых p -разностях функций p^α -значной логики // Дискретная математика. 1992. 4. 4. С. 131–139.
- [108] Мещанинов Д.Г. Метод построения полиномов для функций k -значной логики // Дискретная математика. 1995. 7. С. 48–60.
- [109] Нечипорук Э.И. О сложности схем в некоторых базисах, содержащих нетривиальные элементы с нулевыми весами // Сб. Проблемы кибернетики. Вып. 8. М.: Физматлит, 1962. С. 123–160.
- [110] Нечипорук Э.А. Об одной булевой матрице // Доклады АН СССР. 1966. 169. 4. С. 765; Сб. Проблемы кибернетики. Вып. 21. М.: Наука, 1969. С. 237–241.
- [111] Пантелеев В.И. Полиномиальное разложение k -значных функций по невырожденным функциям // Математические заметки. 1994. 55. 1. С. 144–149.
- [112] Пантелеев В.И. Полиномиальные разложения k -значных функций по операторам дифференцирования и нормализации // Известия вузов. Математика. 1998. 1. С. 82–85.
- [113] Пантелеев В.И., Перязев Н.А. О представлении функций k -значной логики суммой произведений остаточных подфункций // Дискретная математика. 2007. 19. 2. С. 94–100.
- [114] Пантелеев В.И. Специальные представления недоопределенных частичных булевых функций // Ученые записки Казанского университета. Серия Физико-математические науки. 2009. 151. Книга 2. С. 114–119.

- [115] Перязев Н.А. Сложность булевых функций в классе полиномиальных поляризованных форм // Алгебра и логика. 1995. **34**. 3. С. 323–326.
- [116] Поспелов Д.А., Томич Ж. Полиномиальное представление в многозначных логиках // Сб. Многозначные элементы и структуры, М.: Сов. радио, 1967. С. 115–121.
- [117] Разборов А.А. Нижние оценки размера схем ограниченной глубины в базисе $\{\&, \vee, \oplus\}$ // Успехи математических наук. 1986. **41**. 4. С. 219–220.
- [118] Разборов А.А. Нижние оценки размера схем ограниченной глубины в полном базисе, содержащем функцию логического сложения // Математические заметки. 1987. **41**. 4. С. 598–607.
- [119] Редькин Н.П. Доказательство минимальности некоторых схем из функциональных элементов // Сб. Проблемы кибернетики. Вып. 23. М.: Наука, 1970. С. 83–101.
- [120] Ремизов А.Б. О надструктуре замкнутого класса полиномов по модулю k // Дискретная математика. 1989. **1**. 1. С. 3–15.
- [121] 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.
- [122] Романов Д.С. Метод синтеза легкотестируемых схем, допускающих единичные проверяющие тесты константной длины // Дискретная математика. 2014. **26**. 2. С. 100–130.

- [123] Романов Д.С. О синтезе контактных схем, допускающих короткие проверяющие тесты // Ученые записки Казанского университета. Серия физико-математические науки. 2014. **156**. 3. С. 110–115.
- [124] Рязанов Б.В., Чечета С.И. О приближении случайной булевой функции множеством квадратичных форм // Дискретная математика. 1995. **7**. 3. С. 129–145.
- [125] Сапоженко А.А. О сложности дизъюнктивных нормальных форм, полученных с помощью градиентного алгоритма // Дискретный анализ. Вып. 21. Новосибирск, 1972. С. 62–71.
- [126] Семенов А.А. Сложность приближенной реализации булевых функций схемами из функциональных элементов // Сб. Математические вопросы кибернетики. Вып. 5. М.: Наука, 1994. С. 262–279.
- [127] Семигродских А.П., Суханов Е.В. О замкнутых классах полиномов над конечными полями // Дискретная математика. 1997. **9**. 4. С. 50–62.
- [128] Серов А.А. Оценка числа булевых функций, имеющих квадратичные приближения заданной точности // Дискретная математика. 2012. **24**. 3. С. 90–107.
- [129] Столов Е.Л. Математическая модель генератора случайных чисел на основе трехзначной логики// Прикладная дискретная математика. 2012. 2. С. 43–49.
- [130] Супрун В.П. Сложность булевых функций в классе канонических поляризованных полиномов // Дискретная математика. 1993. **5**. 2. С. 111–115.

- [131] Супрун В.П., Городецкий Д.А. Метод блочно-структурного синтеза вычислительных устройств модулярной арифметики // Информатика. 2009. 4. С. 74–79.
- [132] Супрун В.П., Городецкий Д.А. Синтез n -операндных сумматоров по модулю три // Автоматика и вычислительная техника. 2010. 3. С. 72–80.
- [133] Супрун В.П. Одноуровневая схемная реализация основных операций модулярной арифметики в унитарных кодах // Автоматика и вычислительная техника. 2011. 2. С. 18–28.
- [134] Таранников Ю.В. О значениях аффинного ранга носителя спектра платовидной функции // Дискретная математика. 2006. 18. 3. С. 120–137.
- [135] Чашкин А.В. О сложности булевых матриц, графов и соответствующих им булевых функций // Дискретная математика. 1994. 6. 2. С. 43–73.
- [136] Черепов А.Н. Описание структуры замкнутых классов в P_k , содержащих класс полиномов // Сб. Проблемы кибернетики. Вып. 40. М., 1983. С. 5–18.
- [137] Черепов А.Н. Надструктура класса отношений сравнения в k -значной логике по всем модулям-делителям k . Автореферат дисс. канд. физ.-мат. наук, М., 1986.
- [138] Черепов А.Н. Надструктура класса сохранения отношений сравнения при $k = p^m$ // В кн. Моделирование и оптимизация вычислительных систем и процессов. Ярославль: Яросл. гос. ун-т, 1988. С. 61–65.
- [139] Яблонский С.В. Функциональные построения в k -значной логике // Труды Математического института им. В.А. Стеклова АН СССР. 1958. 51. С. 5–142.

- [140] Янов Ю.И., Мучник А.А. О существовании k -значных замкнутых классов, не имеющих конечного базиса // Доклады АН СССР. 1959. **127**. 1. С. 44–46.
- [141] Ablayev F., Vasiliev A. Algorithms for quantum branching programs based on fingerprinting // Electronic Proc. in Theoretical Computer Science. 2009. 9. P. 1–11.
- [142] Alekseyev V.B. On the complexity of some algorithms of matrix multiplication // Journal of Algorithms. 1985. **6**. 1. P. 127–148.
- [143] Alon N., Karchmer M., Wigderson A. Linear circuits over $GF(2)$ // SIAM J. Comput. 1990. **19**. 6. P. 1064–1067.
- [144] Anashin V.S. Uniformly distributed sequences in computer algebra, or how to construct program generators of random numbers // J. Math. Sci. 1998. **89**. 4. P. 1355–1390.
- [145] Barrington D.A.M., Beigel R., Rudich S. Representing Boolean functions as polynomials modulo composite numbers // Computational Complexity. 1994. **38**. 1. P. 367–382.
- [146] Boyar J., Peralta R. Short discreet proofs // Lecture Notes in Computer Science. 1996. **1070**. P. 131–142.
- [147] Boyar J., Peralta R., Pochuev D. On the multiplicative complexity of Boolean functions over the basis $\{\wedge, \oplus, 1\}$ // Theor. Comp. Sci. 2000. **235**. P. 43–57.
- [148] Boyar J., Peralta R., Pochuev D. Concrete multiplicative complexity of symmetric functions // Technical Report YALEU/DCS/TR1219. Computer Science Department, Yale University, 2001.

- [149] Boyar J., Find M.G. Cancellation-free circuits in unbounded and bounded depth // *Fundamentals of Computation Theory. Lecture Notes in Computer Science*. 2013. **8070**. P. 159–170
- [150] Bukhman A.V. Recognition of functions invariant under Mobius transformation and even functions defined in polynomial forms // *Computational Mathematics and Modeling*. 2013. **24**. 4. P. 552–557.
- [151] Carlet C., Guillot Ph. A new representation of Boolean functions // *Technical report INRIA Project CODES*. 1999. P. 1–14.
- [152] Carlitz L. Functions and polynomials (mod p^n) // *Acta Arithmetica*. 1964. 9. P. 66–78.
- [153] Cattopadhyay A. Multilinear polynomials modulo composites // *Bulletin of the European Association on Theoretical Computer Science, Computational Complexity*. 2010.
- [154] Cook S.A. The complexity of theorem-proving procedures // *Proc. 3rd Ann. ACM Symp. on Theory of Computing*. Association for Computing Machinery, New York, 1971. P. 151–158.
- [155] Cooper J.N., Ellis R.B., Kahng A.B. Asymmetric binary covering codes. *Journal of Combinatorial Theory. Series A*. 2002. **100**. 2. P. 232–249.
- [156] Drechsler R., Hengster H., Schafer H., Hartmann J., Becker B. Testability of 2-level AND/EXOR circuits // *Journal of Electronic Testing*. 1999. **14**. 3. P. 219–225.
- [157] Dubrova E.V., Muzio J.C. Testability of generalized multiple-valued Reed-Muller circuits // *Proc. 26th Int. Symp. on Multiple-Valued Logic*. Santiago de Compostela, Spain, January 19-31 1991 y. 1996. P. 56–61.

- [158] Dubrova E.V., Muzio J.C. Easily testable multiple-valued logic circuits derived from Reed-Muller circuits // IEEE Trans. Computers. 2000. **49**. 11. P. 1285–1289.
- [159] Ehrenfeucht A., Karpinski M. The computational complexity of (XOR, AND) counting problems. Preprint. Bonn: Univ., 1989.
- [160] Even S., Kohavi I., Paz A. On minimal modulo 2 sums of products for switching functions // IEEE Trans. Elect. Comput. 1967. P. 671–674.
- [161] Hansel G. Sur le nombre des fonctions booléennes monotones des n variables // C.R. Acad. Sci. Paris. 1966. **262**. P. 1088–1090.
- [162] Interlando J.C., Byrne E., Rosental J. The gate complexity of syndrome decoding of Hamming codes // Applications of Computer Algebra (ACA). 2004. P. 1–5.
- [163] Ishikawa R., Hirayama T., Koda G., Shimizu K. New three-level Boolean expression based on *EXOR* gates // IEICE Trans. Inf. & Syst. 2004. **E87-D**. 5. P. 1214–1222.
- [164] Jukna S., Sergeev I. Complexity of linear Boolean operators // Foundations and Trends in Theoretical Computer Science. 2013. **9**. 1. P. 1–123.
- [165] Keller G., Olson F.R. Counting polynomial (mod p^n) // Duke Math. J. 1968. **35**. 4. P. 835–838.
- [166] Kempner A.J. Polynomials and their residue systems // Trans. Amer. Math. Soc. 1921. 22. P. 240–288.
- [167] Kennes R. Computational aspects of the Mobius transformation of graphs // IEEE Transactions on Systems, Man, and Cybernetics. 1992. **22**. 2. P. 201–223.

- [168] Koda N., Sasao T. An upper bound on the number of products in minimum ESOPs // IFIP WG 10.5 Workshop on Applications of the Reed-Muller Expansions in Circuit Design (Reed-Muller 95). 1995. P. 27–29. (Koda N., Sasao T. An upper bound on the number of products in minimum ESOPs. In: Representations of discrete functions (Sasao T., Fujita M., Eds.). Boston: Kluwer, 1996. P. 94–101.)
- [169] Kojevnikov A., Kulikov A.S. Circuit complexity and multiplicative complexity of Boolean functions. Lecture Notes in Computer Science. 2010. **6158**. P. 239–245.
- [170] Kollar J., Ronyai L., Szabo T. Norm-graphs and bipartite Turan numbers // *Combinatorica*. 1996. **16**. 3. P. 399–406.
- [171] Lamagna E.A., Savage J.E. Computational complexity of some monotone functions // 15th SWAT Conference. 1974. P. 140–144.
- [172] Lo Czu Kai. Precompleteness of a set and rings of linear functions // *Acta bf. natur Univ. Jilinensis*. 1963. 2.
- [173] Malyugin V.D., Veits V.A. Intensive calculations in parallel logic // Proc. 5th Int. Workshop on Spectral Techniques. (Beijing, China, March, 1994 y.). 1994. P. 63–64.
- [174] Mehlhorn K. Some remarks on Boolean sums // *Acta Inf.* 1979. 12. P. 371–375.
- [175] Mirwald R., Schnorr C.P. The multiplicative complexity of quadratic boolean forms // *Theoretical Computer Science*. 1992. **102**. P. 307–328.
- [176] Muller D.E. Application of Boolean algebra to switching circuits design and to error detection // *IRE Trans. Electron. Comp.* EC-3. 1954. P. 6–12.

- [177] Muzio J.C. Stuck fault sensitivity of Reed-Muller and arithmetic coefficients // In Theory and Applications of Spectral Techniques, C. Moraga Ed. Dortmund, 1989. P. 36–45.
- [178] Niven I., Warren L.J. A generalization of Fermat's theorem // Proc. Amer. Math. Soc. 1957. 8. P. 306–313.
- [179] Paterson M. Bounded depth circuits over $\{\oplus, \vee\}$ // Preprint. University of Warwick, 1986.
- [180] Pippenger N. Information theory and the complexity of Boolean functions // Mathematical Systems Theory. 1977. **10**. P. 129–167.
- [181] Post E. Introduction to a general theory of elementary propositions // Amer. Journ. Mathem. 1921. 43. P. 163–185.
- [182] Post E. Two-valued iterative systems of mathematical logic. Princeton, 1941.
- [183] Redei L., Szele T. Algebraisch-zahlentheoretische betrachtungen über ringe // Acta Math. 1947. **79**. P. 291–320.
- [184] Reddy S.M. Easily testable realizations for logic functions // IEEE Trans. Computers. 1972. **21**. 11. P. 1183–1188.
- [185] Reed S.M. A class of multiple error correcting codes and their decoding scheme // IRE Trans. Inf. Th. 1954. PGIT-4. P. 38–49.
- [186] Rosenberg I. La structur des fonctions de plusieurs variables sur un ensemble fini // Comptes Rendus, de l'Academ. Paris, 1965. 260. P. 3817–3819.
- [187] Rosenberg I. Über die funktionale Vollständigkeit in der mehrwertigen Logiken. Rozpravy Česko-slovenské Academie věd // Rada matematických a přírodních věd. Praga, 1970, ročnic 80, Sešit 4. P. 3–93.

- [188] Rosenberg I.G. Polynomial functions over finite rings // *Glasnik Matematiki*. 1975. **10**. 1. P. 25–33.
- [189] Saluja K.K., Reddy S.M. Fault detecting test sets for Reed-Muller canonic networks // *IEEE Trans. Computers*. 1975. **24**. 1. P. 995–998.
- [190] Sarabi A., Perkowski M.A. Fast exact and quasi-minimal minimization of highly testable fixed polarity AND/EXOR canonical networks // *Proc. 29th ACM/IEEE Design Automation Conf.* 1992. P. 20–35.
- [191] Sasao T., Besslich P. On the complexity of mod-2 sum PLA's // *IEEE Trans. on Comput.* 1990. **39**. 2. P. 262–266.
- [192] Sasao T. Representations of logic functions by using EXOR operators // In *Representations of Discrete Functions*. Boston, Kluwer Academic Publishers, 1996. P. 29–54.
- [193] Sasao T. Easily testable realizations for generalized Reed-Muller expressions // *IEEE Trans. Computers*. 1997. **46**. 6. P. 709–716.
- [194] Schnorr C.P. Zwei lineare Schranken für die Komplexität Boolescher Funktionen // *Computing. Archiv für elektronischer Rechnen*. 1974. **13**. 2. P. 155–171.
- [195] Schnorr C.P. The multiplicative complexity of Boolean functions // *Proc. 1st Internat. Joint Conf of ISSAC '88 and AAECC-6, Rome (1988)*. *Lecture Notes in Computer Science*. 1989. **357**. P. 45–58.
- [196] Schaefer T. Complexity of satisfiability problems // *Proceedings of the 10 Annual ACM Symposium on Theory of Computing Machinery*. 1978. P. 216–226.

- [197] Singmaster D. On polynomial functions (mod m) // J. Number Theory. 1974. **6**. 5. P. 345–352.
- [198] Smolensky R. Algebraic methods in the theory of lower bounds for Boolean circuit complexity // Preprint. Berkeley, 1986.
- [199] Strassen V. Gaussian elimination is not optimal // Number. Math. 1969. **13**. P. 354–356.
- [200] Tardos G., Barrington D.A.M. A lower bound on the MOD-6 degree of the OR function // Computational Complexity. 1998. **7**. 2. P. 99–108.
- [201] Yamada T. Easily testable AND/XOR combinational logic circuits // Trans. IECE. 1983. J.66-D. 1. P. 105–110.
- [202] Алексеев В.Б. Введение в теорию сложности алгоритмов. М.: Издательский отдел факультета вычислительной математики и кибернетики МГУ им. М.В. Ломоносова, 2002.
- [203] Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М., Мир, 1979.
- [204] ван дер Варден. Алгебра. М.: Наука, 1979.
- [205] Гаврилов Г.П., Сапоженко А.А. Сборник задач по дискретной математике. М.: Наука, 1977 (1-е изд.), Гаврилов Г.П., Сапоженко А.А. Задачи и упражнения по дискретной математике. М.: Физматлит, 2004 (3-е изд., перераб.).
- [206] Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.
- [207] Зыков А. А. Основы теории графов. М.: Наука, 1987.

- [208] Избранные вопросы теории булевых функций. Под ред. С.Ф. Винокурова и Н.А. Перязева. М.: Физматлит, 2001.
- [209] Кметь А.Б. Четырехзначная логика. Реализация операций. М.: Радио и связь, 1991.
- [210] Курош А.Г. Курс высшей алгебры. М.: Наука, 1971.
- [211] Кухарев Г.А., Шмерко В.П., Зайцева Е.Н. Алгоритмы и систолические процессоры для обработки многозначных данных. Минск: Наука и техника, 1990.
- [212] Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988.
- [213] Логачев О.А., Сальников А.А., Яценко В.В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004 (1-е изд.), Логачев О.А., Сальников А.А., Смышляев С.В., Яценко В.В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012 (2-е изд., дополн.)
- [214] Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
- [215] Поспелов Д.А. Логические методы анализа и синтеза схем. М.: Энергия, 1974.
- [216] Сапоженко А.А. Проблема Дедекинда и метод граничных функционалов. М.: Физматлит, 2009.
- [217] Угрюмов Е.П. Цифровая схемотехника. СПб.: БХВ-Петербург, 2004.
- [218] Яблонский С.В. Введение в дискретную математику. М.: Высшая школа, 2001.
- [219] Яблонский С.В., Гаврилов Г.П., Набебин А.А. Предполные классы в многозначных логиках. М.: Изд-во МЭИ, 1997.

- [220] Astola J.T., Stankovich R.S. Fundamentals of Switching Theory and Logic Design. Dordrecht, Netherlands: Springer, 2006.

Публикации автора по теме работы

- [221] Селезнева С.Н. Некоторые классы формул, допускающие полиномиальное распознавание полноты систем функций // Тезисы докладов XI Международной конференции “Проблемы теоретической кибернетики” (Ульяновск, 1996 г.). М: Изд-во РГГУ, 1996. С. 181–182.
- [222] Селезнева С.Н. О свойствах полиномов самодвойственных и четных функций // Сб. Труды II Международной конференции “Дискретные модели в теории управляющих систем” (Красновидово, 1997 г.). М.: Диалог-МГУ, 1997. С. 51–53.
- [223] Селезнева С.Н. О сложности распознавания полноты множеств булевых функций, реализованных полиномами Жегалкина // Дискретная математика. 1997. **9**. 4. С. 24–31. (Перевод: Selezneva S.N. On the complexity of completeness recognition of systems of Boolean functions realized in the form of Zhegalkin polynomials // Discrete Mathematics and Applications. 1997. **7**. 6. P. 565–572).
- [224] Селезнева С.Н. О свойствах многочленов от многих переменных над конечными полями // Сб. Труды III Международной конференции “Дискретные модели в теории управляющих систем” (Красновидово, 1998 г.). М.: Диалог-МГУ, 1998. С. 102–104.
- [225] Селезнева С.Н. Полиномиальный алгоритм для распознавания принадлежности реализованной полиномом функции k -значной логики предполным классам самодвойственных функций // Дискретная математика. 1998. **10**. 3. С. 64–72. (Перевод: Selezneva S.N. A polynomial algorithm

- for the recognition of belonging a function of k -valued logic realized by a polynomial to precomplete classes of self-dual functions // *Discrete Mathematics and Applications*. 1998. 8. 5. P. 483–492.)
- [226] Селезнева С.Н. Полиномиальный алгоритм распознавания свойства функций многозначных логик, представленных полиномом, сохранять рефлексивный и транзитивный предикат // Сб. Тезисы докладов XII Международной конференции “Проблемы теоретической кибернетики” (Нижний Новгород, 1999 г.). М.: Изд-во МГУ, 1999. С. 207–207.
- [227] Селезнева С.Н. О сложности распознавания функций многозначных логик, сохраняющих некоторые предикаты // Сб. Труды IV Международной конференции “Дискретные модели в теории управляющих систем” (Красновидово, 2000 г.). М.: МАКС Пресс Москва, 2000. С. 119–122.
- [228] Селезнева С.Н. Полиномиальный алгоритм для распознавания принадлежности представленной полиномом функции k -значной логики предполным классам линейных функций // Сб. Материалы Четвертой молодежной научной школы по дискретной математике и ее приложениям. М.: Изд-во МГУ, 2000. С. 69–73.
- [229] Селезнева С.Н. О некоторых свойствах многочленов над конечными полями // Сб. Материалы IV Международного семинара “Дискретная математика и ее приложения” (Москва, 29 января – 2 февраля 2001 г.). М.: Изд-во МГУ Москва, 2001. С. 120–121.
- [230] Селезнева С.Н. О сложности функций многозначной логики в классе поляризованных полиномов // Сб. Дискретная математика и математическая кибернетика. Труды Международной школы-семинара (Ратмино, 31 мая – 3 июня, 2001 г.). М.: МАКС Пресс Москва, 2001. С. 24–25.

- [231] Selezneva S.N. Polynomial-time algorithms for verification of some properties of k -valued functions represented by polynomials // Proceedings of 31th International Symposium of Multiple-Valued Logic (Poland, Warsaw, May 22 – 24, 2001 y.). Washington, Brussels, Tokyo: IEEE Computer Society, 2001. P. 233–238.
- [232] Селезнева С.Н. Полиномиальный алгоритм распознавания принадлежности функций k -значных логик, представленных полиномами, к предполным классам линейных функций // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2001. 3. С. 40–43.
- [233] Селезнева С.Н. О некоторых свойствах многочленов над конечным полем // Дискретная математика. 2001. **13**. 2. С. 111–119. (Перевод: Selezneva S.N. On some properties of polynomials over finite fields // Discrete Mathematics and Applications. 2001. **11**. 2. P. 189–197.)
- [234] Селезнева С.Н. О сложности представления функций многозначных логик поляризованными полиномами // Сб. Тезисы докладов XIII Международной конференции “Проблемы теоретической кибернетики” (Казань, 27–31 мая 2002 г.). М.: Изд-во МГУ, 2002. С. 164–164.
- [235] Селезнева С.Н. О сложности представления функций многозначных логик поляризованными полиномами // Дискретная математика. 2002. **14**. 2. С. 48–53. (Перевод: Selezneva S.N. On the complexity of the representation of functions of many-valued logics by polarized polynomials // Discrete Mathematics and Applications. 2002. **12**. 3. P. 229–234.)
- [236] Селезнева С.Н. О сложности поляризованных полиномов функций k -значных логик, зависящих от одной переменной // Сб. Труды V Меж-

- дународной конференции “Дискретные модели в теории управляющих систем” (Ратмино, 26–29 мая 2003 г.). М.: МАКС Пресс, 2003. С. 80–81.
- [237] Алексеев В.Б., Вороненко А.А., Селезнева С.Н. О сложности реализации функций k -значной логики поляризованными полиномами // Сб. Труды V Международной конференции “Дискретные модели в теории управляющих систем” (Ратмино, 26–29 мая 2003 г.). М.: МАКС Пресс, 2003. С. 8–9.
- [238] Селезнева С.Н. О сложности распознавания полноты систем функций k -значной логики, заданных полиномами // Сб. Труды VI Международной конференции “Дискретные модели в теории управляющих систем” (7 – 11 декабря 2004 г.). М.: МАКС Пресс, 2004. С. 76–79.
- [239] Селезнева С.Н. О сложности поляризованных полиномов функций многозначных логик, зависящих от одной переменной // Дискретная математика. 2004. **16**. 2. С. 117–121. (Перевод: Selezneva S.N. On the complexity of polarized polynomials of multi-valued logic functions in one variable // Discrete Mathematics and Applications. 2004. **14**. 3. P. 263–266.)
- [240] Селезнева С.Н., Дайняк А.Б. О сложности обобщенных полиномов k -значных функций // Сб. Материалы IX Международного семинара “Дискретная математика и ее приложения”, посв. 75-летию со дня рожд. академика О. Б. Лупанова (Москва, 18–23 июня 2007 г.). М.: Изд-во МГУ, 2007. С. 176–178.
- [241] Селезнева С.Н. Об алгоритмической сложности нахождения остатка от деления на степень двойки веса булевой функции, заданной полиномом // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2007. 1. С. 25–29. (Перевод: Selezneva S.N. On

- algorithmic complexity of finding the residue of division by a power of 2 of the weight of a Boolean function defined by a polynomial // Moscow University Computational Mathematics and Cybernetics. 2007. **31**. 1. P. 21–24.)
- [242] Маркелов Н.К., Селезнева С.Н. Быстрый алгоритм построения векторов коэффициентов поляризованных полиномов k -значных функций // Сб. Тезисы докладов XV Международной конференции “Проблемы теоретической кибернетики” (Казань, 2008 г.). М.: Изд-во МГУ Москва, 2008. С. 81–81.
- [243] Селезнева С.Н. О сложности нахождения некоторых свойств веса булевой функции, заданной полиномом // Сб. Материалы Третьей международной конференции по проблемам безопасности и противодействия терроризму. МГУ имени М.В. Ломоносова. 25–27 октября 2007 г. М.: МЦНМО, 2008. С. 148–152.
- [244] Селезнева С.Н. О приближении с заданной точностью функций k -значных логик полиномами // Дискретная математика. 2008. **20**. 2. С. 32–45. (Перевод: Selezneva S.N. On approximation with given accuracy of functions of k -valued logic by polynomials // Discrete Mathematics and Applications. 2008. **18**. 2. P. 115–129.)
- [245] Селезнева С.Н., Дайняк А.Б. О сложности обобщенных полиномов k -значных функций // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2008. 3. С. 34–39. (Перевод: Selezneva S.N., Dainyak A.B. On the complexity of generalized polynomials of k -valued functions // Moscow University Computational Mathematics and Cybernetics. 2008. **32**. 3. P. 152–158.)

- [246] Селезнева С.Н. Линейный алгоритм, определяющий по вектору значений булевой функции, задается ли она полиномом фиксированной степени // Сб. Материалы Четвертой международной научной конференции по проблемам безопасности и противодействия терроризму. МГУ имени М.В. Ломоносова. 30–31 октября 2008 г. Том 2. Материалы МаБИТ-2008. М.: МЦНМО, 2009. С. 46–49.
- [247] Селезнева С.Н. О сложности задания k -значных функций обобщенно-поляризованными полиномами // Сб. Труды VIII Международной конференции “Дискретные модели в теории управляющих систем”. Москва, 6–9 апреля 2009 г. М.: МАКС Пресс, 2009. С. 256–258.
- [248] Селезнева С.Н., Маркелов Н.К. Быстрый алгоритм построения векторов коэффициентов поляризованных полиномов k -значных функций // Ученые записки Казанского университета. Серия Физико-математические науки. 2009. **151**. Книга 2. С. 151–147.
- [249] Селезнева С.Н. О сложности обобщенно-поляризованных полиномов k -значных функций // Дискретная математика. 2009. **21**. 4. С. 20–29. (Перевод: Selezneva S.N. On the complexity of representation of k -valued functions by generalized polarized polynomials // Discrete Mathematics and Applications. 2009. **19**. 6. P. 653–663.)
- [250] Селезнева С.Н. О нахождении коэффициентов обобщенно-поляризованных полиномов k -значных функций // Сб. Материалы X Международного семинара “Дискретная математика и ее приложения”. Москва, 1–6 февраля 2010 г. М.: Издательство механико-математического факультета МГУ, 2010. С. 206–209.
- [251] Селезнева С.Н. О сложности k -значных функций в одном классе полиномов // Сб. Проблемы теоретической кибернетики. Материалы XVI

- Международной конференции (Нижний Новгород, 20–25 июня 2011 г.).
Нижний Новгород: Издательство Нижегородского университета, 2011.
С. 430–434.
- [252] Селезнева С.Н. Быстрый алгоритм построения для k -значных функций полиномов по модулю k при составных k // Дискретная математика. 2011. **23**. 3. С. 3–22. (Перевод: Selezneva S.N. A fast algorithm for the construction of polynomials modulo k for k -valued functions for composite k // Discrete Mathematics and Applications. 2011. **21**. 5-6. P. 651–674.)
- [253] Селезнева С.Н. Быстрый алгоритм построения полиномов функций по составному модулю // Сб. Десятая общероссийская научная конференция “Математика и безопасность информационных технологий”. Материалы секции “Математические проблемы информационной безопасности”. М.: МАКС Пресс Москва, 2012. С. 75–92.
- [254] Селезнева С.Н. Нижняя оценка сложности нахождения полиномов булевых функций в одном классе схем с разделенными переменными // Сб. Материалы XI Международного семинара “Дискретная математика и ее приложения”, посвященного 80-летию со дня рождения академика О.Б. Лупанова (Москва, МГУ, 18–23 июня 2012 г.). М.: Изд-во механико-математического ф-та МГУ, 2012. С. 216–218.
- [255] Селезнева С.Н. О системе образующих идеала нулевых полиномов нескольких переменных над кольцом вычетов по составному модулю // Сб. Синтаксис и семантика логических систем: Материалы 4-й Российской школы-семинара. Иркутск: Из-во ФГБОУ ВПО “Восточно-Сибирская государственная академия образования”, 2012. С. 109–112.
- [256] Селезнева С.Н. Нижняя оценка сложности нахождения полиномов булевых функций в классе схем с разделенными переменными // При-

- кладная математика и информатика. Труды факультета ВМК МГУ. М.: МАКС Пресс, 2012. 40. С. 97–104. (Перевод: Selezneva S.N. Lower bound on the complexity of finding polynomials of Boolean functions in the class of circuits with separated variables // Computational Mathematics and Modeling. 2013. **24**. 1. P. 146–152.)
- [257] Selezneva S.N. Constructing polynomials for functions over residue rings modulo a composite number in linear time // Lecture Notes in Computer Science. 2012. **7353**. P. 303–312.
- [258] Селезнева С.Н. Быстрый алгоритм построения для k -значных функций полиномов по составному модулю k // Интеллектуальные системы. 2013. **17**. 1-4. С. 393–397.
- [259] Селезнева С.Н. О сложности булевых функций в классе полилинейных полиномиальных форм // Сб. Тихоновские чтения: Научная конференция, Москва, МГУ имени М.В. Ломоносова, 28 октября – 1 ноября 2013 г.: Тезисы докладов. М.: МАКС Пресс, 2013. С. 81–81.
- [260] Селезнева С.Н. О схемной сложности нахождения полиномов булевых функций // Сб. Комбінаторна оптимізація та нечіткі множини: матеріали III Всеукр. семінару. Полтава: ПУЕТ, 2013. С. 77–80.
- [261] Селезнева С.Н. Линейная оценка схемной сложности распознавания полиномиальности функций над кольцом вычетов по составному модулю // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2013. 1. С. 27–31. (Перевод: Selezneva S.N. The Circuit complexity of checking polynomiality for functions over a residue ring modulo a composite number is linear // Moscow University Computational Mathematics and Cybernetics. 2013. **37**. 1. С. 21–25.)

- [262] Селезнева С.Н. Мультипликативная сложность некоторых булевых функций // Сб. Ломоносовские чтения: Научная конференция, Москва, факультет ВМК МГУ имени М. В. Ломоносова, 14–23 апреля 2014 г.: Тезисы докладов. М.: МАКС Пресс, 2014. С. 79–80.
- [263] Селезнева С.Н. О сложности функций двузначной и трехзначной логик в классах поляризованных полиномиальных форм // Сб. Тихоновские чтения: Научная конференция, 2014 г.: Тезисы докладов. М.: МАКС Пресс, 2014. С. 43.
- [264] Бухман А.В., Селезнева С.Н. Полиномиальность задачи проверки совпадения множества единиц полинома Жегалкина с образцом // Сб. Тихоновские чтения: Научная конференция, 2014 г.: Тезисы докладов. М.: МАКС Пресс, 2014. С. 45.
- [265] Селезнева С.Н. О мультипликативной сложности некоторых булевых функций // Сб. Проблемы теоретической кибернетики. Материалы XII международной конференции (Казань, 16–20 июня 2014 г.). Казань: Отечество, 2014. С. 252–254.
- [266] Селезнева С.Н., Башов М.А. Порядок функции Шеннона длины функций k -значной логики в классе полиномиальных нормальных форм по модулю k // Сб. Проблемы теоретической кибернетики. Материалы XII международной конференции (Казань, 16–20 июня 2014 г.). Казань: Отечество Казань, 2014. С. 254–256.
- [267] Селезнева С.Н. О длине булевых функций в классе полиномиальных форм с аффинными множителями в слагаемых // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2014. 2. С. 34–38. (Перевод: Selezneva S.N. On the length of Boolean

- functions in the class of exclusive-OR sums of pseudoproducts // Moscow University Computational Mathematics and Cybernetics. 2014. **38**. 2. P. 64–68.)
- [268] Башов М.А., Селезнева С.Н. О длине функций k -значной логики в классе полиномиальных нормальных форм по модулю k // Дискретная математика. 2014. **26**. 3. С. 3–9. (Перевод: Bashov M.A., Selezneva S.N. On the length of functions of k -valued logic in the class of polynomial normal forms modulo k // Discrete Mathematics and Applications. 2015. **25**. 3. P. 131–136.)
- [269] Селезнева С.Н. Мультипликативная сложность некоторых функций алгебры логики // Дискретная математика. 2014. **26**. 4. С. 100–109. (Перевод: Selezneva S.N. Multiplicative complexity of some Boolean functions // Discrete Mathematics and Applications. 2015. **25**. 2. P. 101–108.)
- [270] Selezneva S.N., Bukhman A.V. Polynomial-time algorithms for checking some properties of Boolean functions given by polynomials // Theory of Computing Systems. 2014. P. 1–9.
- [271] Selezneva S.N. On the multiplicative complexity of some Boolean functions // Proc. of Third Russian Finnish Symposium on Discrete Mathematics. Petrozavodsk: Karelian Research Center RAS, 2014. P. 93–95.
- [272] Селезнева С.Н. О мультипликативной сложности квазиквадратичных функций алгебры логики // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2015. 1. С. 23–29. (Перевод: Selezneva S.N. On the multiplicative complexity of quasi-quadratic Boolean functions // Moscow University Computational Mathematics and Cybernetics. 2015. **39**. 1. P. 18–25.)

- [273] Селезнева С.Н. Сложность систем функций алгебры логики и систем функций трехзначной логики в классах поляризованных полиномиальных форм // Дискретная математика. 2015. **27**. 1. С. 111–122.
- [274] Селезнева С.Н. О мультипликативной сложности некоторых функций алгебры логики // Журнал вычислительной математики и математической физики. 2015. **55**. 4. С. 730–736. (Перевод: Selezneva S.N. On the multiplicative complexity of some Boolean functions // Computational Mathematics and Mathematical Physics. 2015. **55**. 4. P. 724–730.)
- [275] Селезнева С.Н. Сложность систем функций алгебры логики и функций трехзначной логики в классах поляризованных полиномиальных форм // Сб. Дискретные модели в теории управляющих систем. IX Международная конференция, Москва и Подмосковье, 20-22 мая 2015 г. М.: МАКС Пресс, 2015. С. 217–219.