МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М. В. ЛОМОНОСОВА

На правах рукописи

Тарannиков Юрий Валерьевич

КОНСТРУКЦИИ И СВОЙСТВА КОРРЕЛЯЦИОННО-ИММУННЫХ И ПЛАТОВИДНЫХ БУЛЕВЫХ ФУНКЦИЙ

2.3.6 — методы и системы защиты информации, информационная безопасность

ДИССЕРТАЦИЯ

на соискание ученой степени

доктора физико–математических наук

Москва 2023

Оглавление

Введение

Одной из фундаментальных проблем, имеющихся в области информационной безопасности, является обеспечение стойкости систем защиты информации против криптографических атак, среди которых выделяются различные виды корреляционных атак. Признанным и распространенным средством противостояния указанным криптографическим атакам является использование в качестве криптографического примитива булевых функций, обладающих хорошими специфическими характеристиками, включающими степень корреляционной иммунности, нелинейность, глобальную автокорреляционную характеристику и другими. Большое число криптографически важных булевых функций строится на основе платовидных функций — функций с трехуровневым носителем спектра. Про некоторые функции с оптимальными криптографическими свойствами доказано, что они обязаны быть платовидными. В связи с этим являются актуальными задачи изучения возможности построения, разработки конструкций и исследования свойств булевых функций, в том числе корреляционно-иммунных и платовидных, противостоящих в качестве криптографического примитива различным видам корреляционных атак на системы защиты информации. Методы решения этих задач имеют математическую природу и используют математический аппарат и подходы различных разделов математики, в том числе методы арифметики, элементарной, линейной и высшей алгебры, теории функций, перечислительной и словарной комбинаторики, теории комбинаторных дизайнов, теории сложности вычислений.

Диссертация представляет результаты исследований в области информационной безопасности. Тема, объект и предмет исследований диссертации соответствуют паспорту специальности 2.3.6 (физико-математические науки) по следующим **областям исследования**:

1. Теория и методология обеспечения информационной безопасности и защиты информации.

9. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности.

10. Модели и методы оценки защищенности информации и информационной безопасности объекта.

15. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

19. Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.

Актуальность темы.

Булевы функции имеют много применений в криптологии, однако одним из важнейших является их использование в качестве нелинейного фильтра или комбинатора для регистров сдвига с линейной обратной связью в поточных шифрах.

Поточным шифром, говоря немного упрощенно, как правило, называется устройство с памятью, которое после введения в него «ключа», определяющего начальные значения ячеек памяти, действует автономно и производит псевдослучайную последовательность, которая преобразует исходное сообщение побитово или побайтово в зашифрованное сообщение, например, складываясь с ним побитово по модулю 2. Главными требованиями к поточным шифрам являются скорость их работы и надежность. Под надежностью понимается невозможность для противника за разумное время по некоторой имеющейся у него информации, например по схеме шифра и перехваченным кускам выданной им псевдослучайной последовательности, определить всю псевдослучайную последовательность целиком, или, что равнозначно, раскрыть «ключ», что позволило бы противнику моментально читать все наши сообщения, зашифрованные с помощью этого ключа.

Одним из наиболее часто использующихся составных частей поточных шиф-

ров является Регистр Сдвига с Линейной Обратной Связью (РСЛОС), очень просто реализующийся как элемент микросхемы и очень быстро работающий. Однако использование одного только РСЛОС недостаточно, потому что существует много атак, позволяющих раскрывать «ключ» РСЛОС (начальные состояния его ячеек) за полиномиальное время относительно N — длины ключа, в то время как в идеале хотелось бы, чтобы противник не имел бы никакого более простого способа, чем перебирать все возможные варианты ключей, которых 2^N, и сравнивать производимые ими псевдослучайные последовательности с перехваченной. То есть не хотелось бы, чтобы существовала атака сложности меньше чем примерно 2^N операций. Поэтому для того, чтобы избавиться от линейной зависимости выдаваемой РСЛОС псевдослучайной последовательности от начальных состояний ячеек, значения некоторых n ячеек РСЛОС в каждый момент времени подают на нелинейный фильтр, представляющий собой булеву функцию от n переменных. И уже выходное значение булевой функции является очередным элементом псевдослучайной последовательности. Модель поточного шифра, основанная на РСЛОС и нелинейном фильтре, показана на Рис. 1.

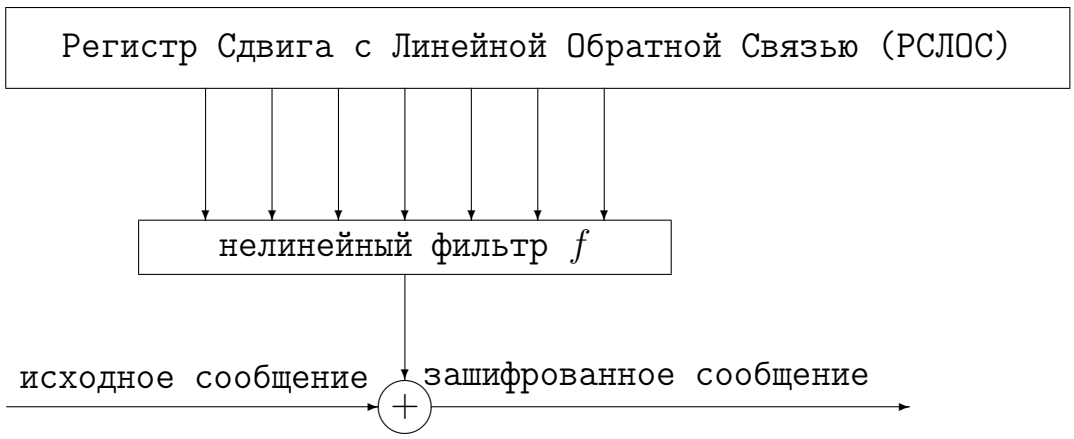


Рис 1. Поточный шифр, состоящий из РСЛОС и нелинейного фильтра.

Нелинейный комбинатор, в свою очередь, комбинирует выходы различных РСЛОС. При этом различные входы нелинейного комбинатора являются полностью независимыми, однако и суммарное число ячеек памяти требуется большее. Общая схема нелинейного комбинатора изображена на рис. 3. в параграфе 2.4.

Существуют, конечно, и другие модели, однако указанные являются одними из самых распространенных.

В зависимости от типов рассматриваемых шифров, на них предложены различные криптографические атаки. Эти атаки используют определенные параметры входящих в шифр компонент, в частности, булевых функций, как средство для эффективного нахождения ключа. Существует много криптографических атак, которые позволяют противнику, если фильтр f выбран неподходящим образом, эффективно раскрыть ключ. Среди таких атак наиболее распространены корреляционные, линейные (быстрые корреляционные), дифференциальные (автокорреляционные) и другие. Поэтому был сформулирован ряд свойств, которым должны удовлетворять используемые в шифрах булевы функции, чтобы успешно противостоять таким атакам. Наиболее важными свойствами являются уравновешенность, высокие нелинейность, алгебраическая степень, корреляционная иммунность, глобальная автокорреляционная характеристика. Кроме того, конечно, для практического использования и быстродействия шифра фильтр должен иметь простую реализацию. Перечисленные требования часто противоречат друг другу, о чем свидетельствуют и теоретические результаты.

Корреляционно-иммунные и устойчивые булевы функции являются хорошо известным объектом в математике и ее приложениях. Обладая тем свойством, что их выход статистически не зависит от некоторых комбинаций входов, эти функции широко используются в потоковых шифрах и других криптографических схемах. Под названием простых ортогональных массивов эти функции изучались в комбинаторике и статистике для дизайна статистических экспериментов, а под названием кодов с некоторым (ненулевым) дуальным расстоянием — в теории кодирования. Рассматриваемым объектам посвящена обширная литература. Частично корреляционно-иммунные и устойчивые булевы функции затрагивались в обзорной статье [16] в шестом выпуске «Математических вопросов кибернетики». Ортогональным массивам посвящена недавно вышедшая специальная монография [69], дуальное расстояние названо Филиппом Дельсартом в [60] одним из «четырех основных параметров кода». Стоит также упомянуть обзорную статью [103], в которой приведены и некоторые результаты

автора диссертации.

Для построения булевых функций с высокой нелинейностью широко применяются конструкции, использующие бент-функции и платовидные функции. Бент-функции — функции с максимально возможной нелинейностью. Напрямую они не используются в шифрах из-за неуравновешенности, но есть конструкции, где из них легко строятся уравновешенные. Платовидные функции представляют большой интерес в криптографии для изучения бент-функций и в силу того, что многие криптографически важные функции являются платовидными. Кроме того, бент-функции строятся через платовидные.

Центральное место в данной диссертационной работе занимает изучение и построение функций, одновременно являющихся устойчивыми высокого порядка и платовидными. Следствие 1.7 утверждает, что m-устойчивые булевы функции от n переменных обязаны одновременно быть платовидными. Самой большой в работе и одной из важнейших (можно сказать, центральной) является глава 2, в которой исследуются методы построения таких функций.

Степень разработанности темы.

Рассматриваемым в диссертации объектам посвящена обширная литература, как со стороны чистой математики, так и со стороны приложений. Криптографическим свойствам булевых функций посвящены монографии [19], [58] и [51]. Корреляционно-иммунные функции параллельно изучались в математике в эквивалентных или близких формулировках как ортогональные массивы, коды с некоторым дуальным расстоянием и др. Платовидные функции также получили широкое изучение, особенно их частный случай — бент-функции, которым посвящены монографии по бент-функциям: [23] и [84]. Но, несмотря на большую разработанность как всей темы, так и отдельных разделов, имелись и до сих пор имеются многочисленные подобласти, которых либо почти не касались исследователи, либо полученные результаты не были достаточно глубокими.

Цель диссертационной работы. Анализ возможности построения, разработка эффективных конструкций и исследование свойств булевых функций, в первую очередь корреляционно-иммунных и платовидных, для противодействия в качестве криптографического примитива различным видам корреляци-

онных атак на системы защиты информации.

Для достижения поставленной цели были **решены задачи**:

1. получения точных оценок нелинейности для корреляционно-иммунных и устойчивых булевых функций;

2. разработки методов построения устойчивых функций, достигающих верхней оценки нелинейности;

3. построения устойчивых функций, достигающих верхней оценки нелинейности, с использованием оригинальных разработанных методов;

4. нахождения эффективных схемных и программных реализаций устойчивых функций с максимально возможной нелинейностью;

5. получения нижней оценки глобальной автокорреляционной характеристики для устойчивых функций высокого порядка; 6. получения верхней оценки на число нелинейных переменных в устойчивых булевых функциях высокого порядка;

7. получения и уточнения вида формул для числа корреляционно-иммунных и устойчивых булевых функций высокого порядка;

8. установления для регулярных булевых функций теоремы типа теоремы Симона–Вегенера;

9. нахождения всех возможных значений аффинного ранга платовидной функции с носителем спектра мощности 16;

10. построения платовидных функций с заданной мощностью носителя спектра и аффинным рангом, принимающим все возможные значения из широкого диапазона;

11. исследования вопроса существования A-примитивных разбиений пространства векторов над конечным полем на конечное число аффинных подпространств и граней одинаковой размерности и получения оценок на параметры таких разбиений; 12. получения вида асимптотических формул для числа разбиений пространства векторов над конечным полем на конечное число аффинных подпространств и граней одинаковой размерности;

13. нахождения всех возможных предельных значений плотности l-уравновешенных функций;

14. описания всех булевых функций, равномерно распределенных по шарам

со степенью 1, и точного подсчета их количества;

15. получения критерия, позволяющий по системе запрещенных подфункций, задающих инвариантный класс, и определения, содержит ли этот класс бесконечное число существенно разных функций;

16. описания всех минимальных бесконечных инвариантных классов и доказательства континуальности числа таких классов.

Методы исследования. В рамках исследования применяется математический аппарат и подходы различных разделов математики, в том числе — методы арифметики, элементарной, линейной и высшей алгебры, теории функций, перечислительной и словарной комбинаторики, теории комбинаторных дизайнов, теории сложности вычислений. Особую роль играет искусство разработки конструкций.

Объект исследований. Булевы функции, их криптографически важные свойства: корреляционная иммунность, устойчивость, нелинейность, автокорреляционные характеристики, аффинный ранг. Множества коэффициентов Уолша булевой функции, их структура и характеристики. Булевы функции с единичными значениями, равномерно распределенными по подкубам или шарам. Булевы функции из специальных классов: корреляционно-иммунные, устойчивые, платовидные, бент-функции. Инвариантные классы булевых функций. Обобщения на многозначные функции. Смежные объекты: различные виды комбинаторных дизайнов, коды, упаковки подкубов, упаковки продуктов.

Предмет исследований. Свойства параметров криптографически важных функций, установление оценок на эти параметры и на их взаимосвязь между собой. Анализ возможностей построения функций, обладающих «криптографически хорошими» параметрами, в том числе — экстремальными. Достижение эффективной схемной и программной реализации таких конструкций. Оценки числа функций из криптографически важных классов, получение эффективных оценок, асимптотических и точных формул для числа функций и вспомогательных комбинаторных объектов, включая разбиения пространства на аффинные подпространства, упаковки продуктов, упаковки подкубов.

Научная новизна работы характеризуется следующими результатами.

1. Установлен факт, что верхняя оценка нелинейности $2^{n-1} - 2^{m+1}$ для m-

устойчивых функций от n переменных может достигаться только на функциях, достигающих равенства в неравенстве Зигенталера.

2. Разработаны методы построения m-устойчивых функций от n переменных с максимально возможной нелинейностью $2^{n-1} - 2^{m+1}$, в частности, с использованием введенных подходящих и обобщенных подходящих матриц.

3. С помощью разработанных методов построены m-устойчивые функции от n переменных с нелинейностью $2^{n-1} - 2^{m+1}$ при всех парах (m, n), удовлетворяющих неравенству $0{,}6n - 1 \leq m \leq n - 2$, а асимптотически при $0,5789\ldots(1 + o(1)) \leq m/n$.

4. Получена нижняя оценка автокорреляционной характеристики m-устойчивой функции от n переменных.

5. Получен вид формул для числа корреляционно-иммунных и устойчивых порядка $m = n - k$ булевых функций от n переменных; доказано, что эта формула является полиномом степени $p(k)$; получены оценки на величину $p(k)$.

6. Построены платовидные функции с носителем спектра мощности 4^h и аффинным рангом $\mathbf{k}$ для любого натурального $\mathbf{k}$, удовлетворяющего неравенствам $2h \leq \mathbf{k} \leq 2^{h+1} - 2$.

7. Установлен факт, что при q, равном степени простого числа, для любого натурального m существует наименьшее натуральное $N = N_q(m)$, что при $n > N$ не существует A-примитивных разбиений $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n - m$. Получены нижние и верхние оценки на величину $N_q(m)$, найдено точное значение $N_q(2) = q + 1$; результаты того же типа получены для разбиений на грани.

8. Установлен факт, что при больших n плотности l-уравновешенных функций близки к одному из следующих пяти чисел: 0, 1/3, 1/2, 2/3 или 1.

9. Получен критерий, позволяющий по системе запрещенных подфункций, задающих инвариантный класс, определить, содержит ли этот класс бесконечное число существенно разных функций. Критерий сводит рассматриваемую задачу для функций к соответствующей задаче для множеств слов.

Теоретическая значимость. Результаты могут найти применение в теории защиты информации, теории синтеза схем, теории кодирования, математической кибернетике, дискретной математике.

Практическая значимость. Разработанные в ходе диссертационных исследований методы, построенные функции и смежные объекты, установленные свойства, в частности разработанные эффективные схемные и программные методы реализации m-устойчивых функций от n переменных, могут применяться в криптографических примитивах и системах защиты информации, в частности, в поточных шифрах. Не исключено приложение метода, включающего обобщенные подходящие матрицы, для построения систем функций, а также в блочных шифрах. Результаты по корреляционно-иммунным функциям могут быть задействованы при разработке криптографических масок.

На защиту выносятся: обоснование актуальности, научная новизна, теоретическая и практическая значимость работы, а также положения, которые подтверждаются результатами исследования, представленными в Заключении диссертации. В их числе следующие далее.

1. Эффективные схемные и программные методы реализации m-устойчивых функций от n переменных для криптографических примитивов и систем защиты информации.

2. Верхняя оценка на число нелинейных переменных в устойчивых булевых функциях высокого порядка.

3. Теорема для регулярных булевых функций типа теоремы Симона–Вегенера.

4. Описание всех возможных значений аффинного ранга платовидной функции с носителем спектра мощности 16.

5. Установление вида асимптотических формул для числа разбиений пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств и граней при $m = \mathrm{const}$, $n \to \infty$.

6. Описание всех булевых функций, равномерно распределенных по шарам со степенью 1, и точный подсчет их количества.

7. Описание всех минимальных бесконечных инвариантных классов; доказательство, что число таких классов — континуум.

Публикации. Перечень публикаций приведен в конце работы; в научных изданиях, индексируемых в базах данных Web of Science (WoS), Scopus, а также в научных изданиях из списка ВАК опубликовано 20 работ.

Степень достоверности и апробация результатов. Результаты диссер-

тации математически строго доказаны. Они неоднократно докладывались на научных семинарах «Булевы функции в криптологии», «Математические вопросы кибернетики», «Синтез и сложность управляющих систем» на механико-математическом факультете МГУ, «Теория кодирования», «2022-арные квазигруппы и смежные вопросы» в ИМ им. С. Л. Соболева, семинаре по теории кодирования Института проблем передачи информации им. А. А. Харкевича, научных семинарах в Индийском статистическом институте (Колката), Институте индустриальных наук университета Токио, технологическом университете Квинсленда, на конференциях «Синтез и сложность управляющих систем», «Проблемы теоретической кибернетики», «Межгосударственный семинар по дискретной математике и ее приложениям», «Математика и безопасность информационных технологий», «Международная научная конференция по проблемам безопасности и противодействия терроризму», «Сибирская конференция по исследованию операций», «Институт продвинутого изучения по разностным множествам, последовательностям и их корреляционным свойствам» (Германия), «Институт продвинутого изучения по булевым функциям в криптологии», «Индо-российская конференция по алгебре, теории чисел и дискретной математике», Международная конференция «Графы и группы, спектры и симметрии», «Международный симпозиум по комбинаторной оптимизации», Международный семинар «Алгебраическая и комбинаторная теория кодирования» (Болгария), «Индокрипт», «Азиякрипт», Семинар «Быстрое программное шифрование» (Япония).

Структура и объем работы.

Диссертация состоит из введения, семи глав, разбитых на параграфы, заключения и списка литературы из 189 наименований. Работа изложена на 287 страницах.

Содержание работы.

Глава 1 диссертации начинается с параграфа 1.1, в котором даются основные определения и понятия, принятые в литературе по булевым функциям и используемые в настоящей диссертации. В параграфе 1.2 приводятся базовые результаты. Эти результаты широко известны и содержатся в монографиях [19], [58], [51], обзорной статье автора [146]. Приведенные базовые результаты

для полноты изложения снабжены доказательствами, как правило, в изложении диссертанта. В параграфе 1.3 описывается связь корреляционно-иммунных функций с ортогональными массивами, описываются известные результаты для ортогональных массивов, уже без доказательств. В параграфе 1.4 устанавливается верхняя оценка нелинейности корреляционно-иммунной порядка m и m-устойчивой функций от n переменных.

Теорема 1.2. *Пусть $f(x_1, \ldots, x_n)$ является m-устойчивой булевой функцией, $m \leq n-2$. Тогда*

$$nl(f) \leq 2^{n-1} - 2^{m+1}. \tag{1.8}$$

Теорема 1.2 была доказана автором в [159] и [134] и независимо Саркаром и Майтрой в [109] и Зенгом и Зангом в [126]. Заметим, что в каждой из указанных работ есть дополнительные результаты, не содержащиеся в других работах. В частности, автором была установлена следующая далее теорема 1.3, которая в параллельных работах Саркара–Майтры и Зенга–Занга получена не была.

Теорема 1.3. *Пусть $f(x_1, \ldots, x_n)$ является m-устойчивой неоптимальной булевой функцией, $m \leq n-3$. Тогда*

$$nl(f) \leq 2^{n-1} - 2^{m+2}.$$

Неоптимальной здесь называется функция, для которой не достигается равенство в неравенстве Зигенталера (1.1).

В заключении параграфа 1.4 приводится верхняя оценка нелинейности неуравновешенных корреляционно-иммунных функций. Следующая теорема 1.6 была доказана автором в [159]. Этот же результат получен и в параллельных работах Саркара и Майтры [109] и Зенга и Занга [126].

Теорема 1.6. *Пусть $f(x_1, \ldots, x_n)$ — неуравновешенная корреляционно-иммунная порядка m булева функция, $m < n$. Тогда*

$$nl(f) \leq 2^{n-1} - 2^m. \tag{1.12}$$

Заметим, что из следствия 1.7 вытекает, что m-устойчивая функция, на которой достигается равенство в оценке (1.8), обязана быть платовидной; конструкциям таких функций будет посвящена следующая глава 2. Глава же 1 заканчивается параграфом 1.5, в котором рассматриваются линейные и квазилинейные переменные и свойства обладающих такими переменными функций. Эти факты пригодятся при изучении конструкций в следующей главе 2.

Глава 2 диссертации посвящена конструкциям m-устойчивых булевых функций от n переменных, нелинейность которых достигает верхней границы $2^{n-1} - 2^{m+1}$. До того, как была установлена оценка (1.8), такие функции специально не изучались, однако изучение существовавших конструкций показывает, что они позволяли построить функции, нелинейность которых достигает оценки (1.8), лишь для m не меньше, чем примерно $n - \log_2 n$. На протяжении главы излагаются последовательно улучшающиеся автором методы, позволяющие построить m-устойчивые функции для все большего диапазона параметров. Несмотря на последовательное улучшение методов, результаты более ранних параграфов не вкладываются полностью в последующие результаты, поскольку последующие результаты приобретают все более асимптотический характер.

В параграфе 2.1 представлена предложенная автором рекурсивная конструкция, в которой из двух функций, связанных определенными условиями, строятся две новых. Эта конструкция позволила построить m-устойчивые булевы функции от n переменных, нелинейность которых достигает верхней границы $2^{n-1} - 2^{m+1}$, при $\frac{2n-7}{3} \le m \le n-2$. В параграфе 2.2 конструкция предыдущего параграфа была доработана и установлена следующая теорема.

Теорема 2.2. *Для целых m и n, удовлетворяющих неравенствам $\frac{2n-7}{3} \le m \le n - \log_2 \frac{n+2}{3} - 2$, существует m-устойчивая булева функция на $\mathbf{F}_2^n$ с нелинейностью $2^{n-1} - 2^{m+1}$, достигающая неравенства Зигенталера для каждой отдельной переменной.*

Заметим, что на самом деле не просто установлен факт существования, а предложен конструктивный и эффективный метод построения таких криптографически важных функций, полезных в системах защиты информации.

В параграфе 2.3 из множества построенных в предыдущих двух параграфах функций выделены две специальные последовательности регулярных функций,

обладающих экстремальными свойствами.

В параграфе 2.4 рассматриваются аспекты схемной реализации функций, построенных в предыдущих параграфах. Показано, что такая реализация может быть осуществлена с линейными по числу переменных сложностью и временем, что делает применение построенных функций перспективным для использования в криптографических примитивах и системах защиты информации.

В параграфе 2.5 предлагается усовершенствованный по сравнению с параграфом 2.1 метод построения устойчивых функций, достигающих верхней границы нелинейности. Вводится и подробно описывается центральное для этого метода понятие **подходящей** (k_0, k, p, t)**-матрицы.** В параграфе 2.6 строятся эффективные примеры подходящих матриц, удовлетворяющих определениям, данным в параграфе 2.5. С их помощью строятся m-устойчивые функции от n переменных с максимальной нелинейностью $2^{n-1} - 2^{m+1}$ для более широкого, чем в предыдущих параграфах, диапазона значений. В частности, доказана следующая теорема.

Теорема 2.8. $\mathrm{nlmax}(n, m) = 2^{n-1} - 2^{m+1}$ *для* $0.6n - 1 \leq m \leq n - 2$.

В параграфе 2.7 излагается следующее усовершенствование. Понятие подходящей матрицы обобщается до **обобщенной** (k_0, k, p, t)**-подходящей матрицы.** Изучаются свойства обобщенных подходящих матриц и возможность их использования для построения m-устойчивых функций с максимальной возможной нелинейностью. В частности, доказана следующая теорема.

Теорема 2.9. *Если существует обобщенная* (k, k, p, t)*-походящая матрица, то можно построить последовательность* m*-устойчивых функций на* $\mathbf{F}_2^n$*, достигающих границы (1.8), при* $n \to \infty$, $\frac{m}{n} \to \frac{t}{t+k}$.

В параграфе 2.8 предлагаются и исследуются рекурсивные конструкции на основе обобщенных подходящих матриц. В результате доказывается следующее утверждение.

Следствие 2.3. *Пусть* α *— действительная константа,* $0.5789... \leq \alpha \leq 1$*. Тогда существует последовательность* m*-устойчивых функций на* $\mathbf{F}_2^n$*, достигающих границы (1.8), для которой* $\frac{m}{n} \to \alpha$.

В параграфе 2.9 обсуждается сложность реализации функций из предложенных в параграфе 2.8 конструкций. Показывается, как эффективно вычислить

значение реализуемой функции ветвящейся программой, имеющей небольшую вычислительную сложность. Отмечено, что если зафиксировать обобщенную (k, k, p, t)-подходящую матрицу, и последовательно применять ее в конструкции растущее число раз, а перестановки переменных на каждом шаге ограничить последними не более чем $2p$ разрядами, то сложность вычисления значения построенной функции ветвящейся программой будет линейной.

В параграфе 2.10 решается комбинаторная задача, тесно связанная с существованием и построением *подходящих матриц,* рассматривавшихся в параграфах 2.5 и 2.6 для построения устойчивых функций, достигающих верхней границы нелинейности. Помимо вышесказанного результаты этого параграфа имеют и общекомбинаторное значение. В параграфе 2.10 устанавливается максимальное число непересекающихся граней с нижним уровнем $l_1 = 1$ и верхним уровнем l_2 в булевом кубе B^n и строится пример, показывающий, что попытка казалось бы естественного обобщения теоремы о максимальном паросочетании в двух соседних слоях булева куба является, вообще говоря, несостоятельной.

В параграфе 2.11 элементы техники, использовавшейся для построения обобщенных подходящих матриц в параграфе 2.8, выделены в самостоятельный комбинаторный объект: *упаковки* (n, k)*-продуктов*. Введено понятие *совершенной упаковки* (n, k)*-продуктов,* которую можно рассматривать как разновидность комбинаторных дизайнов, близкую вист-турнирам. Отметим, что существование совершенной упаковки $(10, 3)$-продуктов позволило ранее установить основные результаты параграфа 2.8. Приведены некоторые оценки величин $A_{n,k}$ — максимальной мощности упаковки (n, k)-продуктов.

В параграфе 2.12 показано, что, ограничиваясь средствами, предложенными в предыдущих параграфах этой главы, нельзя построить m-устойчивые функции от n переменных с оптимальной нелинейностью при $m/n \leq \frac{1}{1+\log_2(1.971044...)}(1+o(1)) = 0.505316...(1+o(1))$. Впрочем, сказанное не исключает дальнейшего совершенствования методов. Заметим, что отношение m/n, близкое к 0.505316..., для многих практических целей является хорошим, поэтому построения в рамках техники [184] тоже представляют интерес.

В то время, как в главе 2 исследовалась связь корреляционной иммунности булевых функций с их нелинейностью, **глава 3** посвящена анализу взаи-

мосвязей корреляционной иммунности с другими криптографически важными свойствами булевых функций, в частности, с их автокорреляционными характеристиками. Главным методом изучения в этой главе является спектральный анализ, т. е. использование коэффициентов Уолша и их свойств, а также автокорреляционных коэффициентов.

В параграфе 3.1 представлена нижняя оценка для абсолютной автокорреляционной характеристики Δ_f устойчивых функций, сформулированная в следующей теореме.

Теорема 3.2. *Пусть f является m-устойчивой булевой функцией на $\mathbf{F}_2^n$. Тогда $\Delta_f \geq \left(\frac{2m-n+3}{n+1}\right) 2^n$.*

Эта оценка является нетривиальной при $2m - n + 3 > 0$ и в указанном диапазоне лучшей из известных.

В параграфе 3.2 доказывается верхняя оценка на число нелинейных переменных в устойчивых булевых функциях высокого порядка. Функции, которые зависят от некоторых переменных линейно, являются во многих приложениях криптографически слабыми, поэтому их использование на практике нежелательно. Кроме того, такие функции не представляют интереса и с теоретической точки зрения, поскольку линейные переменные можно просто отбросить (удалив их в полиноме функции или, что то же самое, подставив вместо них константу 0). Тогда и число переменных функции, и степень ее устойчивости уменьшатся на число отброшенных линейных переменных и задача сведется к исследованию функции без линейных переменных. Поэтому важным вопросом является здесь существование устойчивых функций, которые зависят от всех своих переменных нелинейно. Первоначально автором было доказано [157, 156, 133], что для любого натурального k существует минимальное неотрицательное целое $p(k)$, любая $(n-k)$-устойчивая функция от n переменных зависит нелинейно от не более чем $p(k)$ переменных. Позднее в [164] и [161] автором совместно с его студентом Денисом Кириенко было доказано, что $p(k) \leq (k-1)4^{k-2}$. В этом параграфе доказывается оценка $p(k) \leq (k-1)2^{k-2}$, полученная автором в 2001 году в работе [166] (результаты этой работы содержится в также в [136]). При $k = 3$ эта оценка достигается на функции $f_3(x_1, \ldots, x_4)$, приведенной в параграфе 2.3. При $k = 4$ оценка уже не точна, поскольку в работах [164] и [161]

показано, что $p(4) = 10$; однако отличается от нижней оценки $p(k) \geq 3 \cdot 2^{k-2} - 2$, достигаемой на специальной последовательности функций, впервые построенной автором в работе [158] и приведенной в параграфе 2.3, в линейное по k число раз. Результаты параграфа опубликованы в работе автора [166] и входят в состав работы [136].

Помимо представления булевой функции полиномом Жегалкина, существует также единственное представление булевой функции f мультилинейным полиномом над $\mathbf{R}$. Степень этого полинома (т. е. длина самого длинного монома) называется *действительной степенью* функции f. В 1994 году Нисан и Сегеди доказали [88], что у булевой функции с действительной степенью не выше d число существенных переменных не превосходит $d \cdot 2^{d-1}$. Оказалось, что этот результат эквивалентен оценке автора $p(k) \leq (k-1)2^{k-2}$. Насколько известно автору, факт эквивалентности этих задач в явном виде до сих пор не опубликован. В неявном виде указание на эквивалентность задач было опубликовано в 2014 году О'Доннеллом в качестве непронумерованного замечания между утверждениями 6.23 и 6.24 в монографии [89].

В 2020 году результат Нисана–Сегеди был усилен до $n \leq C \cdot 2^d$, где $C = 6.614\ldots$ [53] и $C = 4.416\ldots$ [122]. Заметим, что это автоматически означает усиление оценки теоремы 3.4 до $p(k) \leq C \cdot 2^{k-1}$ с тем же самым значением $C = 4.416\ldots$. Отметим, что авторы статьи [53] наряду с верхней оценкой $n \leq 6.614 \cdot \cdots \cdot 2^d$, доказывают также и нижнюю, эквивалентную оценке автора $p(k) \geq 3 \cdot 2^{k-2} - 2$ и достигающуюся на той же самой последовательности функций (только заданной в другой форме), что свидетельствует о том, что эквивалентность двух указанных выше задач и статьи по параллельной тематике были еще в 2020 году неизвестны даже некоторым активно работающим в этой области исследователям.

В параграфе 3.3 коэффициенты Уолша применяются для исследования корреляционно-иммунных и устойчивых булевых функций. В параграфе устанавливаются необходимые условия, связывающие число переменных, устойчивость и вес неуравновешенных неконстантных корреляционно-иммунных функций и доказывается, что такие функции не существуют при $m > 0.75n - 1.25$. Похожие утверждения известны для функций с несколькими выходами (операторов)

(см. [38], [77]), но для обычных булевых функций до работ автора утверждения такого типа не были сформулированы даже как гипотезы. Для высоких порядков m этот неожиданный факт превзошел хорошо известное неравенство Бирбрауэра–Фридмана [64], [37]. Одновременно главный результат параграфа явился новым необходимым условием на число строк простого двоичного ортогонального массива. Заметим, что это необходимое условие впервые (если не считать очевидного факта, что число строк должно делиться на двойку в степени, равной силе массива) имеет немонотонное по числу строк поведение. До настоящего времени все усилия исследователей в этой области были направлены исключительно на получение нижних оценок для числа строк в массиве (или как иногда любят говорить, для «мощности дизайна»).

В 2007 году Дмитрий Германович Фон-Дер-Флаасс усилил главный результат этого параграфа и доказал [63], что неуравновешенные неконстантные корреляционно-иммунные функции порядка m от n переменных не существуют при $m > \frac{2}{3}n - 1$, назвав свой результат доказательством «гипотезы Таранникова». Этот результат Фон-Дер-Флаасса является во многих отношениях окончательным, поскольку известны бесконечные семейства функций с $m = \frac{2}{3}n - 1$. В 2010 году А. В. Халявин обобщил [27] результат Фон-Дер-Флаасса на ортогональные массивы, доказав, что если при $m > \frac{2}{3}n - 1$ существует $OA(N, n, 2, m)$, то $N \geq 2^{n-1}$; причем если $N = 2^{n-1}$, то ортогональный массив является простым.

В теореме 3.5 параграфа 3.3 дано необходимое условие существования неуравновешенных неконстантных корреляционно-иммунных булевых функций высокого порядка. В теореме 3.4 параграфа 3.2 дана верхняя оценка для числа нелинейных переменных в устойчивых функциях высокого порядка. Однако в некоторых случаях эти оценки можно улучшить более тонким исследованием. Элементы такого подхода разрабатываются в параграфе 3.4. Приведенные в нем результаты содержатся в работах [164] и [161].

В параграфе 3.4 результаты о спектральной структуре корреляционно-иммунных и устойчивых булевых функций используются для исследования корреляционно-иммунных функций высокого порядка. Вводится матрица ненулевых коэффициентов Уолша и устанавливаются важные свойства этой матрицы.

Эти свойства применяются для доказательства несуществования неуравновешенной неконстантной корреляционно-иммунной порядка $n-4$ функции от $n \geq 10$ переменных.

Асимптотики числа корреляционно-иммунных функций и устойчивых от n переменных малого порядка k (т. е. когда k или константа, или растет достаточно медленно по отношению к n) были получены в работах [5] и [44]. В параграфе 3.5 изучаются количества таких функций высокого порядка, а именно устанавливается вид точных и асимптотических формул для числа корреляционно-иммунных и устойчивых порядка $n-k$ функций от n переменных при $k = \text{const}$, $n \to \infty$.

Обозначим через $A(k,i)$ число $(i-k)$-устойчивых булевых функций на $\mathbf{F}_2^i$.

Теорема 3.12. *Число $R(n, n-k)$ устойчивых порядка $n-k$ функций на $\mathbf{F}_2^n$ выражается формулой*

$$R(n,n-k) = \sum_{i=0}^{p(k)} A(k,i) \binom{n}{i};$$

при $n > 3k-3$ число $K(n,n-k)$ корреляционно-иммунных порядка $n-k$ функций на $\mathbf{F}_2^n$ выражается формулой

$$K(n,n-k) = 2 + R(n,n-k) = 2 + \sum_{i=0}^{p(k)} A(k,i) \binom{n}{i}.$$

Следствие 3.4. *Асимптотика числа $R(n,n-k)$ устойчивых порядка $n-k$ функций на $\mathbf{F}_2^n$, так же как и асимптотика числа $K(n,n-k)$ корреляционно-иммунных порядка $n-k$ функций на $\mathbf{F}_2^n$ при $k = const$, $n \to \infty$, выражается следующей формулой*

$$R(n,n-k) \sim K(n,n-k) \sim \frac{A(k,p(k))}{p(k)!} n^{p(k)}.$$

Основное содержание параграфа 3.6 составляет теорема для регулярных функций типа теоремы Симона–Вегенера.

Следствие 3.6. *Для заданного натурального n минимальное возможное c, такое что существует c-регулярная булева функция на $\mathbf{F}_2^n$, существенно*

зависящая от всех своих переменных, удовлетворяет соотношению

$$\min c = \log_2 n + O(\log_2 \log_2 n).$$

Теорему Симона–Вегенера можно наглядно сформулировать следующим образом.

Теорема Симона–Вегенера 3.14. [115], [121] *Для заданного натурального n минимальное $c(n)$, такое что существует булева функция, существенно зависящая от всех своих n переменных, у которой любой набор имеет* **не более** *$c(n)$ соседних с ним, на которых функция принимает другое значение, удовлетворяет асимптотическому соотношению*

$$c(n) = (1/2) \log_2 n + O(\log_2 \log_2 n).$$

Основной результат параграфа 3.6 переформулируется в стиле теоремы Симона–Вегенера следующим образом.

Теорема 3.15. *Для заданного натурального n минимальное $c(n)$, такое что существует булева функция, существенно зависящая от всех своих n переменных, у которой любой набор имеет* **ровно** *$c(n)$ соседних с ним, на которых функция принимает другое значение, удовлетворяет асимптотическому соотношению*

$$c(n) = \log_2 n + O(\log_2 \log_2 n).$$

Глава 4 посвящена исследованию свойств платовидных функций, основное внимание уделяется значению их аффинного ранга в зависимости от мощности носителя спектра.

Платовидные функции представляют большой интерес сами по себе и для построения различных классов криптографически важных функций. Так, бент-функции можно рассматривать как частный случай платовидных. Специально подчеркнем, что изучавшиеся в предыдущих главах корреляционно-иммунные и устойчивые булевы функции при накладывании разнообразных дополнитель-

ных требований во многих случаях могут быть лишь платовидными. Так, например, из следствия 1.7 вытекает, что m-устойчивая функция, на которой достигается равенство в оценке (1.8), и, тем самым, обладающая максимально возможной нелинейностью при заданном порядке устойчивости, обязана быть платовидной; конструкциям таких функций почти целиком посвящена самая большая глава 2.

Толчком к исследованиям аффинного ранга платовидных функций для автора послужила статья [49], в которой рассматривался аффинный ранг только кубических функций с максимальной устойчивостью, но эти функции, как было несложно показано, обязаны были быть платовидными. Поэтому при исследовании аффинного ранга переходим к рассмотрению всех платовидных функций.

В параграфе 4.1 напоминаются основные понятия и используемые в главе 4 определения, дается описание направления исследований и полученных в главе результатов.

В параграфе 4.2 исследуется аффинные преобразования в $\mathbf{F}_2^n$; причем как аффинные преобразования самой функции, так и аффинные преобразования ее носителя спектра. В частности, доказана следующая лемма.

Лемма 4.2. *Пусть $W_f(x) \to W'(x) = W_f(\mathbf{A}x)$ — аффинное преобразование спектра функции f, заданной на $\mathbf{F}_2^n$. Тогда коэффициенты $W'(x)$ являются коэффициентами Уолша некоторой функции f', причем*

$$f'(x) = f(xA^{-1}) + < a, xA^{-1} > .$$

Лемма 4.2 показывает, что можно работать с булевой функцией, осуществляя аффинные преобразования ее носителя спектра. Многие свойства функции при этом, выраженные через ее коэффициенты Уолша, либо не меняются, либо меняются контролируемым образом. Особенно удобны аффинные преобразования носителя спектра при преобразованиях платовидных функций. Лемма 4.2 используется как на протяжении данной главы, так и в последующих работах.

В параграфе 4.3 доказываются различные утверждения, касающиеся платовидных функций, ранга и аффинного ранга и их взаимосвязей. Эти утверждения являются вспомогательными в рамках главы 4, но представляют также и

самостоятельный интерес.

В параграфе 4.4 представлены все возможные значения аффинного ранга $\mathbf{k}$ платовидных булевых функций с носителем спектра мощности 16. Ранее в работе [49] для подкласса платовидных функций с носителем спектра мощности 16 (более точно, для кубических устойчивых порядка $n-4$ функций) была получена оценка $\mathbf{k} \leq k \leq 9$. В параграфе 4.4 доказано, что аффинный ранг любой платовидной функции с носителем спектра мощности 16 равен 4, 5 или 6.

В параграфе 4.5 рассматриваются полученные автором оценки аффинного ранга платовидной булевой функции с произвольной мощностью $|S_f|$ носителя спектра. В частности, установлена следующая теорема.

Теорема 4.2. *Для любого натурального* $\mathbf{k}$*, удовлетворяющего неравенствам* $2h \leq \mathbf{k} \leq 2^{h+1}-2$ *существует платовидная функция с носителем спектра мощности* 4^h *и аффинным рангом* $\mathbf{k}$*.*

Из более поздних результатов Саньяла [105, 106] следует асимптотическая оценка $\mathbf{k} = O(h \cdot 2^h)$.

В **главе 5** рассматриваются разбиения пространства $\mathbf{F}_q^n$ на аффинные подпространства, приведены результаты о числе таких разбиений. Эти вопросы связаны с основной темой диссертации следующим образом. Среди конструкций платовидных вообще и бент-функций в частности, есть конструкции, в которых функция строится путем сборки из подфункций с непересекающимися носителями спектра. Если все исходные функции являются платовидными с одинаковым значением модуля ненулевых коэффициентов Уолша, то полученная функция снова будет платовидной. Если при этом объединение носителей спектра подфункций есть все пространство $\mathbf{F}_2^n$, то получается бент-функция. Однако задачей является нахождение подходящего множества платовидных функций с непересекающимися носителями спектра. Оказывается, что если взять в качестве носителя спектра аффинное подпространство, то каждая платовидная функция с таким носителем спектра эквивалентна бент-функции от числа переменных, равных размерности аффинного подпространства; более того, между множествами таких функций существует взаимно-однозначное соответствие, которое задается аффинным преобразованием носителя спектра, описанным в

лемме 4.2 главы 4.

Во вступлении к главе 5 описана конструкция K, предложенная Баксовой и Таранниковым в [187], где показано, что конструкция задает бент-функцию. Более того, из описания конструкции K следует, что число бент-функций от n переменных, порождаемых конструкцией K, при заданном параметре n_1 и $n_2 = n - n_1$ равно

$$L = b_{n_2-n_1}^{2^{n_1}} \cdot N_{n_2}^{n_2-n_1}, \tag{5.1}$$

где $b_{n_2-n_1}$ — число бент-функций от $n_2 - n_1$ переменных, $N_{n_2}^{n_2-n_1}$ — число упорядоченных разбиений $\mathbf{F}_2^{n_2}$ на 2^{n_1} классов смежности линейных подпространств размерности $n_2 - n_1$.

Ту же конструкцию, но в другой терминологии предложил ранее С. В. Агиевич [34], который также получил формулу (5.1).

В параграфе 5.1 обсуждаются задачи разбиения пространства $\mathbf{F}_q^n$ на линейные и аффинные подпространства в разных их формулировках, вводится понятие разбиений, примитивных по Агиевичу (или A-примитивных разбиений).

Пусть $\bigsqcup\limits_i E_i = \mathbf{F}_q^n$, где E_i — аффинные подпространства пространства $\mathbf{F}_q^n$, $E_i = L_i + b_i$, L_i — соответствующие линейные подпространства пространства $\mathbf{F}_q^n$, $b_i \in \mathbf{F}_q^n$. Обозначим $\bigcap\limits_i L_i = W$. Агиевич назвал разбиение $\{E_i\}$ *примитивным,* если $W = \{\vec{0}\}$. Мы будем называть такое разбиение *примитивным по Агиевичу* или *A-примитивным.*

В параграфе 5.2 описываются свойства скалярных произведений векторов, когда один из векторов фиксирован, а второй пробегает аффинное подпространство.

В параграфе 5.3 представлены результаты о существовании A-примитивных разбиений.

Теорема 5.2. *Пусть q — степень простого числа. Для любого натурального m существует наименьшее натуральное $N = N_q(m)$, что при $n > N$ не существует A-примитивных разбиений $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n - m$.*

Верхняя оценка на величину $N_q(m)$ дается следующей теоремой.

Теорема 5.3. *Пусть q — степень простого числа. Тогда $N_q(m) \leq m \cdot q^{m-1}$.*

Рекуррентная оценка на величину $N_q(m)$ дается следующей теоремой.

Теорема 5.4. *Пусть q — степень простого числа. Тогда*

$$N_q(m+1) \geq q \cdot N_q(m) + 1.$$

Нижняя оценка на величину $N_q(m)$ дается следующей теоремой.

Теорема 5.5. *Пусть q — степень простого числа. Тогда*

$$N_q(m) \geq \frac{q^m - 1}{q - 1}.$$

Установленное точное значение величины $N_q(2)$ дается следующей теоремой. Ранее Агиевич в [34] фактически доказал, что $N_2(2) = 3$.

Теорема 5.7. *Пусть q — степень простого числа. Тогда*

$$N_q(2) = q + 1.$$

В параграфе 5.4 результаты того же типа, что и в параграфе 5.3, установлены для разбиений на грани (они же координатные подпространства, или подкубы). Разбиения на грани можно рассматривать для произвольного q, поэтому результаты параграфа установлены для q, не обязательно являющихся степенью простого, для чего пришлось преодолеть дополнительные технические сложности.

В параграфе 5.5 изучается число разбиений (не обязательно A-примитивных) пространства F_q^n на q^m аффинных подпространств размерности $n-m$, а также на такое же число граней той же размерности в случае $m = \text{const}$, $n \to \infty$. Установлены асимптотики для числа таких разбиений, которые даны в следующих теоремах.

Теорема 5.14. *Пусть q (степень простого числа) и m фиксированы, $n \to \infty$. Тогда*

$$c_q(n,m) \sim C q^{N_q(m) \cdot n},$$

где $C = \frac{c_q^*(N_q(m),m)}{q^{(N_q(m))^2} \cdot \left(\frac{1}{q};\frac{1}{q}\right)_{N_q(m)}}$; величина $\left(\frac{1}{q};\frac{1}{q}\right)_{N_q(m)} = \prod\limits_{i=1}^{N_q(m)} \left(1 - \frac{1}{q^i}\right)$ известна как q-символ Почхаммера.

Теорема 5.15. *Пусть q и m фиксированы, $n \to \infty$. Тогда*

$$c_q^{\mathrm{coord}}(n, m) \sim C' n^{N_q^{\mathrm{coord}}(m)},$$

где $C' = \frac{c_q^{\mathrm{coord}*}(N_q^{\mathrm{coord}}(m), m)}{N_q^{\mathrm{coord}}(m)!}$.

В главах 2 и 4 главное внимание уделено корреляционно-иммунным и устойчивым булевым функциям, т. е. функциям, единичные значения которых абсолютно равномерно распределены по подкубам заданной размерности $(n - m)$. Не всегда такое абсолютно равномерное распределение достижимо, особенно когда оно должно удовлетворять каким-то дополнительным требованиям. В то же время с практической точки зрения часто достаточно иметь не абсолютно равномерное, а почти равномерное распределение. В **главе 6** рассматриваются булевы функции, количество единичных значений которых в однотипных подмножествах (подкубах и шарах) одинакового размера (но зато любого) различается не более чем на заданную величину l.

В параграфе 6.1 приводятся доказательства теорем рамсеевского типа о симметрических подфункциях. Результаты данного параграфа используются в этой и последующей главах, однако они представляют и самостоятельный интерес.

В параграфе 6.2 представлены результаты изучения l-уравновешенных булевых функций. Пусть l — целое неотрицательное число. Булева функция $f(x_1, x_2, \ldots, x_n)$ называется *l-уравновешенной,* если для любых ее подфункций f_1 и f_2 от одинакового числа переменных выполнено неравенство $|wt(f_1) - wt(f_2)| \leq l$. Величина $\rho(f) = wt(f)/2^n$ называется плотностью n-местной булевой функции f.

В [21] описаны все 1-уравновешенные булевы функции. Некоторые оценки веса l-уравновешенных булевых функций приведены в [128]. Главной целью настоящего параграфа является доказательство того, что при больших n плотности l-уравновешенных функций близки к одному из следующих пяти чисел: 0, 1/3, 1/2, 2/3 или 1. Главный результат параграфа сформулирован в следующей теореме.

Теорема 6.5. *Для любого натурального l и любого положительного ε существует такое натуральное N, что для любого натурального n, не меньше*

шего N, и для любой l-уравновешенной булевой функции f от n переменных имеет место одно из следующих пяти неравенств:

$$\begin{aligned} &wt(f) \le 2l; \\ &|\rho(f) - 1/3| < \varepsilon; \\ &|\rho(f) - 1/2| < \varepsilon; \\ &|\rho(f) - 2/3| < \varepsilon; \\ &wt(f) \ge 2^n - 2l. \end{aligned}$$

Шаром радиуса r с центром α будем называть множество наборов, отстоящих от α на расстояние, не большее r. Весом функции f на шаре (или для краткости просто весом шара) будем называть число 1-наборов функции f, принадлежащих этому шару. Шар радиуса r веса m будем для краткости называть (r, m)-шаром. Шар радиуса r веса не меньшеm будем называть $(r, m)^*$-шаром.

Пусть l — целое неотрицательное число. Булеву функцию $f(x_1, x_2, \ldots, x_n)$ будем называть *равномерно распределенной по шарам со степенью l (l-РРШ функцией),* если модуль разности весов любых двух шаров одинакового радиуса не превосходит l.

В параграфе 6.3 представлены результаты исследования функций, равномерно распределенных по шарам со степенью 1, и дано полное описание таких функций. Равномерное распределение единичных значений булевых функций по шарам ранее не изучалось интенсивно, хотя представляется, что булевы функции, единичные значения которых равномерно распределены по шарам, могут иметь разнообразные полезные приложения, например, когда булева функция играет роль хеширующей функции, или когда мы хотим, чтобы при использовании характеристического кода этой функции все возможные слова на выходе канала связи имели бы приблизительно одинаковое количество способов подходящего декодирования. Такие булевы функции имеют в качестве комбинирующих функций в потоковых шифрах хорошую устойчивость против статистических атак, когда противник имеет возможность изменять некоторое (ограниченное) число входов функции, поэтому доказательство несуществования таких функций в некоторых случаях (для некоторых значений параметров)

доказывает и то, что упомянутые статистические атаки в таких случаях могут иметь гарантированный успех.

В качестве возможного объяснения того, почему подобными вопросами не занимались ранее, можно отметить, что полученный результат является достаточно неожиданным, а используемая техника — неочевидной. Действительно, равномерно распределить наборы по шарам какого-го одного радиуса возможно. Несложно заметить, что характеристическая функция совершенного кода с кодовым расстоянием 3 (например, кода Хэмминга) и функция $f(x_1, \ldots, x_{2n+1}) = \bigoplus_{i=1}^{n+1} x_i$ абсолютно равномерно распределены по шарам радиуса 1; функция от нечетного числа переменных n, которая принимает одинаковые значения на противоположных наборах, абсолютно равномерно распределена по шарам радиуса $\frac{n-1}{2}$. Однако оказывается, что равномерно распределить единичные значения по шарам разных радиусов (даже не абсолютно, а приблизительно) во многих случаях оказывается уже невозможно.

Основной результат параграфа 6.3 сформулирован в следующей теореме.

Теорема 6.6. *Если n-местная булева функция f с весом $wt(f) \leq 2^{n-1}$ является 1-РРШ функцией, то имеет место хотя бы один из следующих трех случаев:*

$$\begin{aligned} &1)\ wt(f) \leq 2;\\ &2)\ n \leq 4;\\ &3)\ n = 6, wt(f) = 4. \end{aligned}$$

Как следствие, подсчитано число 1-РРШ функций.

Следствие 6.7. *Число 1-РРШ функций от n переменных равно*

$$\begin{cases} 2^{2^n} & \text{при } n \leq 2,\\ 80 & \text{при } n = 3,\\ 334 & \text{при } n = 4,\\ 2818 & \text{при } n = 6,\\ 3 \cdot 2^n + 2 & \text{при } n \geq 5, n \text{ нечетно},\\ (n+3)2^n + 2 & \text{при } n \geq 8, n \text{ четно}. \end{cases}$$

Глава 7 посвящена результатам исследований инвариантных классов дискретных функций. Инвариантные классы булевых функций были введены С. В. Яблонским в [30], но более известна его последующая работа [31]. В этой главе рассматриваются не только инвариантные классы булевых функций, но и классы функций, заданных на двоичных наборах и принимающих k значений. Булевы функции из инвариантных классов не являются, вообще говоря, функциями с равномерно распределенными единичными значениями. Однако, тем не менее, многие рассматриваемые в предыдущих главах работы классы функций с равномерно распределенными единичными значениями являются инвариантными. Так, инвариантными являются класс $(n-k)$-устойчивых функций от n переменных (для заданного k) и класс l-уравновешенных функций (для заданного l). Тут, впрочем, надо сделать оговорку, что эти классы не являются инвариантными по классическому определению С. В. Яблонского, потому что они не замкнуты относительно добавления фиктивных переменных. Поэтому надо или делать оговорку о том, что включаем вместе с функцией в класс все функции, получающиеся из нее добавлением фиктивной переменной, или просто исключить такое добавление из определения инвариантного класса. Этим главным образом и объясняется то, что наряду с классическим определением инвариантного класса по С. В. Яблонскому, в этой главе рассматриваются и неклассические определения инвариантного класса, в которых операция добавления несущественной переменной не учитывается.

Помимо того, что некоторые классы функций с равномерно распределенными единичными значениями являются инвариантными, важна также и общность методов и подходов. Так во многих рассуждениях предыдущих глав являлось важным, что если перейти от функции к ее подфункции, подставив, например, вместо переменной константу, или удалив линейную переменную из ее полинома, то получится снова функция из того же класса. Этим и вызван интерес к инвариантным классам в данной работе, для которой, таким образом, инвариантные классы являются идейно близким объектом.

В параграфе 7.1 дается общее понятие инвариантного класса и некоторые определения, в том числе обсуждаются различные способы определения инвариантного класса.

В параграфе 7.2 даются краткие сведения из теории слов, избегающих запреты.

В параграфе 7.3 предлагается критерий, позволяющий по системе запрещенных подфункций, задающих инвариантный класс, определить, содержит ли этот класс бесконечное число существенно разных функций. Критерий сводит рассматриваемую задачу для функций к соответствующей задаче для множеств слов. Задание инвариантных классов через множества запрещенных подфункций использовалось уже при введении инвариантных классов С. В. Яблонским, однако до работы автора [146] такой критерий предложен не был.

В параграфе 7.4 рассматриваются минимальные бесконечные инвариантные классы функций, т. е. такие классы, что при добавлении к множеству запрещенных функций любой функции из класса класс перестает быть бесконечным. Представлено описание всех минимальных бесконечных инвариантных классов и доказательство теоремы, что число таких классов — континуум.

1 Корреляционно-иммунные и устойчивые булевы функции

Глава 1 диссертации носит вводный характер, в ней даются основные определения и понятия, принятые в литературе по булевым функциям и используемые в настоящей диссертации, приводятся базовые результаты, описывается связь корреляционно-иммунных функций с ортогональными массивами. Однако уже в главе 1 приводится новый результат — в теореме 1.2 устанавливается верхняя оценка $nl(f) \leq 2^{n-1} - 2^{m+1}$ для нелинейности корреляционно-иммунной порядка m-устойчивой функции от n переменных, $m \leq n-2$. Теорема 1.2 была доказана автором в [159] и [134] и независимо Саркаром и Майтрой в [109] и Зенгом и Зангом в [126]. Из этих соображений результат теоремы 1.2 не включен в основные результаты диссертации. Заметим, что в каждой из указанных работ есть дополнительные результаты, не содержащиеся в других работах. В частности, автором доказана теорема 1.3, которая в параллельных работах Саркара–Майтры и Зенга–Занга получена не была.

1.1 Предварительные определения и понятия

Рассматривается $\mathbf{F}_2^n$, векторное пространство наборов длины n с компонентами из $\mathbf{F}_2$ — конечного поля из двух элементов 0 и 1, операции сложения и умножения в котором вводятся как обычные операции сложения и умножения чисел 0 и 1 по модулю 2. Для элементов $\mathbf{F}_2$ устанавливается естественный порядок предшествования: $0 < 1$. *Булева функция* от n переменных — это отображение из $\mathbf{F}_2^n$ в $\mathbf{F}_2$. Функцию f от n переменных будем также записывать в виде $f(x) = f(x_1, x_2, \ldots, x_n)$, считая при этом, что переменные x_1, x_2, …, x_n однозначно соответствуют компонентам $\mathbf{F}_2^n$. В дальнейшем будем обозначать

набор из $\mathbf{F}_2^n$ буквой без нижнего индекса, а компоненту этого набора — той же буквой с нижним индексом, указывающим на порядковый номер этой компоненты в наборе. Наборы x' и x'' называются *соседними,* если они различаются только в i-й компоненте. Обозначим через x^i набор, который отличается от x только в i-й компоненте, $i = 1, \ldots, n$. Переменная x_i называется *фиктивной* для функции f, если для любых наборов x' и x'', соседних по i-й компоненте, выполнено $f(x') = f(x'')$. Переменные булевой функции иногда будем называть ее *входами,* а принимаемое булевой функцией значение – ее *выходом.*

Весом $|x|$ набора x из $\mathbf{F}_2^n$ называется число единиц в x. Мы говорим, что набор x длины n *предшествует* набору y длины n и обозначаем это $x \preceq y$, если $x_i \leq y_i$ для любого натурального i от 1 до n. Если наборы x и y не совпадают и $x \preceq y$, то будем говорить, что набор x *строго предшествует* набору y, и писать $x \prec y$. *Вес* $wt(f)$ функции f над $\mathbf{F}_2^n$ — это число наборов x из $\mathbf{F}_2^n$, для которых $f(x) = 1$. Функция f называется *уравновешенной,* если $wt(f) = wt(f \oplus 1) = 2^{n-1}$ (т. е. функция принимает значения 0 и 1 на одинаковом числе наборов). *Подфункцией* булевой функции f называется функция f', полученная подстановкой в f некоторых констант 0 или 1 вместо некоторых переменных. Если подставлять в функцию f константы $\sigma_{i_1}, \ldots, \sigma_{i_s}$ вместо переменных $x_{i_1}, \ldots, x_{i_s}$ соответственно, то полученная подфункция обозначается $f^{\sigma_{i_1},\ldots,\sigma_{is}}_{x_{i_1},\ldots,x_{i_s}}$. Если вместо переменной x_i константа не подставлена, то x_i называется *свободной* переменной для f'.

Расстоянием Хэмминга $d(x', x'')$ между двумя наборами x' и x'' называют число компонент, в которых наборы x' и x'' различаются. Для заданной функции f из $\mathbf{F}_2^n$ минимум расстояний $d(f, l)$, где l пробегает множество всех аффинных функций из $\mathbf{F}_2^n$ называется *нелинейностью* функции f и обозначается через $\mathrm{nl}(f)$. *Подфункцией* булевой функции f называется функция f', полученная подстановкой в f некоторых констант 0 или 1 вместо некоторых переменных.

Хорошо известно, что функция f, заданная на $\mathbf{F}_2^n$, имеет единственное полиномиальное представление над $\mathbf{F}_2$, степень которого по каждой переменной

не превосходит 1, а именно

$$f(x_1, \ldots, x_n) = \bigoplus_{(a_1,\ldots,a_n)\in \mathbf{F}_2^n} g(a_1, \ldots, a_n) x_1^{a_1} \ldots x_n^{a_n}$$

где g это также функция над $\mathbf{F}_2^n$. Такое полиномиальное представление f называется *алгебраической нормальной формой* (сокращенно АНФ) функции, а каждое выражение $x_1^{a_1} \ldots x_n^{a_n}$ называется *слагаемым* в АНФ функции f (в русскоязычной литературе АНФ иногда называют полиномом Жегалкина). Отображение $f(x) \to g(x)$ иногда называют *преобразованием Мебиуса.*

Алгебраическая степень функции f, обозначаемая через $\deg(f)$, определяется как число переменных в самом длинном слагаемом в АНФ функции f. *Алгебраическая степень переменной* x_i функции f, обозначаемая через $\deg(f, x_i)$, это число переменных в самом длинном слагаемом в АНФ функции f, содержащем x_i. Если $\deg(f, x_i) = 0$, то переменная x_i называется *фиктивной,* или *несущественной* для функции f. Если $\deg(f, x_i) = 1$, то говорим, что f зависит от x_i *линейно.* Если $\deg(f, x_i) \neq 1$, то говорим, что f зависит от x_i *нелинейно.* Слагаемое длины 1 называется *линейным* слагаемым. Если $\deg(f) \leq 1$, то f называется *аффинной* функцией. Если f является аффинной функцией и $f(0) = 0$, то f называется *линейной* функцией. (Заметим, что в русскоязычной литературе по дискретной математике в силу исторически сложившейся практики линейной чаще всего называют аффинную функцию.)

Расстоянием Хэмминга $d(x', x'')$ между двумя наборами x' и x'' называют число компонент, в которых наборы x' и x'' различаются. различаются. Наборы x' и x'' называются *соседними,* если $d(x', x'') = 1$. Обозначим через x^i набор, который отличается от x только в i-й компоненте, $i = 1, \ldots, n$. Для двух булевых функций f_1 и f_2 на $\mathbf{F}_2^n$ расстояние между f_1 и f_2 определяется как $d(f_1, f_2) = \#\{x \in \mathbf{F}_2^n | f_1(x) \neq f_2(x)\}$. Легко заметить, что $d(f_1, f_2) = wt(f_1 \oplus f_2)$. Для заданной функции f из $\mathbf{F}_2^n$ минимум расстояний $d(f, l)$, где l пробегает множество всех аффинных функций из $\mathbf{F}_2^n$ называется *нелинейностью* функции f и обозначается через $nl(f)$.

Булева функция f, заданная на $\mathbf{F}_2^n$, называется *корреляционно-иммунной порядка* m, $1 \leq m \leq n$, если выход f и любое множество из m ее входных переменных являются статистически независимыми. Это понятие было

введено Зигенталером [113]. В эквивалентной невероятностной формулировке булева функция f называется корреляционно-иммунной порядка m, если $wt(f') = wt(f)/2^m$ для любой ее подфункции f' от $n-m$ переменных. Уравновешенная корреляционно-иммунная функция порядка m называется *m-устойчивой.* Другими словами, булева функция f называется m-устойчивой, если $wt(f') = 2^{n-m-1}$ для любой ее подфункции f' от $n-m$ переменных. С этой точки зрения можно рассматривать формально любую уравновешенную булеву функцию как 0-устойчивую (это понятие принято в [42], [108], [90]) и произвольную булеву функцию как (-1)-устойчивую (у функции от n переменных подфункции от $n+1$ переменной не существует, поэтому для любой ее подфункции справедливо все, что угодно). Понятие m-устойчивой функции было введено в [54].

Булева функция f на $\mathbf{F}_2^n$ называется *(c_0, c_1)-регулярной* (или просто *регулярной*), если 1) для любого набора $x \in \mathbf{F}_2^n$, такого что $f(x) = 0$, имеем $\#\{y \in \mathbf{F}_2^n \,|\, d(x,y) = 1, f(y) = 1\} = c_0$; 2) для любого набора $x \in \mathbf{F}_2^n$, такого что $f(x) = 1$, имеем $\#\{y \in \mathbf{F}_2^n \,|\, d(x,y) = 1, f(y) = 0\} = c_1$. Булеву функцию, являющуюся (c,c)-регулярной, будем называть *c-регулярной* функцией.

Пусть $x = (x_1, \ldots, x_n)$ и $u = (u_1, \ldots, u_n)$ — это наборы длины n над $\mathbf{F}_2$. *Скалярное произведение* x и u — это целочисленная функция которая определяется как

$$< x, u >= \sum_{i=1}^{n} x_i u_i.$$

(сложение в скалярном произведении берется обычное целочисленное, а не по модулю 2). Под сложением $x + u$ двух двоичных наборов x и u понимается их покомпонентное сложение по модулю 2.

Преобразованием Фурье булевой функции f называется целочисленная функция над $\mathbf{F}_2^n$, определяемая следующим образом

$$F_f(u) = \sum_{x \in \mathbf{F}_2^n} f(x)(-1)^{<u,x>}.$$

Для каждого $u \in \mathbf{F}_2^n$ значение $F_f(u)$ называется *коэффициентом Фурье. Преобразованием Уолша* булевой функции f называется целочисленная функция над

$\mathbf{F}_2^n$, определяемая следующим образом

$$W_f(u) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+<u,x>}.$$

Для каждого $u \in \mathbf{F}_2^n$ значение $W_f(u)$ называется *коэффициентом Уолша.* Заметим, что в различных работах каждый из коэффициентов $F_f(u)$ и $W_f(u)$ называется и коэффициентом Фурье, и коэффициентом Уолша, и коэффициентом Уолша–Адамара, и коэффициентом Адамара. Однако в последнее время прослеживается тенденция называть их именно так, как это было сделано выше. Коэффициенты Уолша будем называть *спектральными коэффициентами,* а совокупность всех 2^n коэффициентов Уолша — *спектром* булевой функции.

Множество S_f всех наборов u, таких что $W_f(u) \neq 0$, называется *носителем спектра* функции f.

Булева функция от n переменных называется *бент-функцией,* если значение коэффициентов Уолша на всех наборах равно $\pm 2^{n/2}$.

Булева функция называется *платовидной,* если ее коэффициенты Уолша принимают ровно три возможных значения: 0 и $\pm 2^c$ для некоторого c. Платовидные функции представляют большой интерес для изучения бент-функций (например, потому, что при разложении бент-функции по переменной возникают две платовидные функции), а также потому, что многие криптографически важные функции являются платовидными.

Бент-функции и платовидные функции будут играть важнейшую роль в диссертационном исследовании, однако в полной мере смысл их определений будет раскрыт только в следующем параграфе после формулировки и осмысления ряда вспомогательных результатов, в частности, равенства Парсеваля,

Пусть f — это булева функция на $\mathbf{F}_2^n$. Для каждого $u \in \mathbf{F}_2^n$ *автокорреляционный коэффициент* функции f на наборе u определяется как $\Delta_f(u) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+f(x+u)}$. *Абсолютная автокорреляционная характеристика* [124] функции f определяется как $\Delta_f = \max_{x \in \mathbf{F}_2^n \setminus \{0\}} |\Delta_f(x)|$. Функция $D_u f = f(x) + f(x+u)$ называется *производной* функции f по направлению u. Множество наборов $u \in {F_2}^n$, таких что $D_u f \equiv \text{const}$, называется *линейной структурой* функции f. Легко проверить, что линейная структура функции f образует ли-

нейное пространство в $\mathbf{F}_2^n$. Наличие у функции линейных структур в некоторых случаях (но не всех) является криптографической слабостью.

1.2 Базовые результаты

В этом параграфе приведены базовые результаты, связанные с корреляционной иммунностью и устойчивостью булевых функций, их алгебраической степенью, нелинейностью и спектральными коэффициентами. Эти результаты будут активно использоваться в последующих параграфах. Большинство результатов являются классическими (см. например [79]), однако для полноты изложения будем излагать их, как правило, с полными доказательствами. Основой этого параграфа является работа автора [165], в которой впервые были представлены доказательства многих известных фактов, доказанных ранее более сложно.

Лемма 1.1. *Корреляционно-иммунная порядка m функция является также корреляционно-иммунной любого меньшего порядка.*

Доказательство. Действительно, пусть f' — произвольная подфункция от $n-m+1$ переменной корреляционно-иммунной порядка m функции f. Пусть x_i — произвольная переменная функции f'. Тогда $f' = x_i(f')^1_{x_i} \oplus (x_i \oplus 1)(f')^0_{x_i}$ и $wt(f') = wt((f')^1_{x_i}) + wt((f')^0_{x_i})$. Однако веса обоих подфункций $(f')^1_{x_i}$ и $(f')^0_{x_i}$ от $n-m$ переменных функции f равны $wt(f)/2^m$ в силу корреляционной иммунности порядка m последней. Поэтому, $wt(f') = wt(f)/2^{m-1}$. Таким образом, функция f является корреляционно-иммунной и порядка $m-1$, и любого меньшего порядка. □

Лемма 1.2. *Для любой булевой функции f на $\mathbf{F}_2^n$ и для любого двоичного набора $u \in \mathbf{F}_2^n$ значение коэффициента $g(u)$ АНФ функции f можно вычислить по формуле*

$$g(u) = \bigoplus_{\substack{x \in \mathbf{F}_2^n \\ x \preceq u}} f(x).$$

Доказательство. Проведем доказательство индукцией по весу набора u. Если $u = 0$, то очевидно, что $g(0) = f(0)$. Пусть формула справедлива для всех

наборов с весом меньше $|u|$. Тогда по определению функции $g(x)$, а далее по предположению индукции имеем

$$f(u) = \bigoplus_{\substack{x \in \mathbf{F}_2^n \\ x \preceq u}} g(x) = \bigoplus_{\substack{x \in \mathbf{F}_2^n \\ x \prec u}} \bigoplus_{\substack{y \in \mathbf{F}_2^n \\ y \preceq x}} f(y) \oplus g(u).$$

Несложно видеть, что в сумме $\bigoplus\limits_{\substack{x \in \mathbf{F}_2^n \\ x \prec u}} \bigoplus\limits_{\substack{y \in \mathbf{F}_2^n \\ y \preceq x}} f(y)$ каждое слагаемое $f(y)$ присутствует только если $y \prec u$, более того, встречается ровно $2^{|u|-|y|} - 1$, то есть нечетное число раз. Поэтому $\bigoplus\limits_{\substack{x \in \mathbf{F}_2^n \\ x \prec u}} \bigoplus\limits_{\substack{y \in \mathbf{F}_2^n \\ y \preceq x}} f(y) = \bigoplus\limits_{\substack{y \in \mathbf{F}_2^n \\ y \prec u}} f(y)$. Отсюда

$$g(u) = \bigoplus_{\substack{y \in \mathbf{F}_2^n \\ y \preceq u}} f(y),$$

что и требовалось доказать. □

Следствие 1.1. *Из формул* $f(u) = \bigoplus\limits_{\substack{x \in \mathbf{F}_2^n \\ x \preceq u}} g(x)$ *и* $g(u) = \bigoplus\limits_{\substack{x \in \mathbf{F}_2^n \\ x \preceq u}} f(x)$ *видно, что преобразование Мебиуса обратно само себе. Если* $u = \widetilde{1} = (1, \ldots, 1)$ *— набор, состоящий из одних единиц, то* $g(1) = \bigoplus\limits_{x \in \mathbf{F}_2^n} f(x)$. *Поэтому* $g(\widetilde{1}) = 1$ *тогда и только тогда, когда вес функции* f *нечетен.*

Лемма 1.3. *Пусть* f *является булевой функцией на* $\mathbf{F}_2^n$, $\deg(f) = d \geq 1$. *Тогда* $2^{n-d} \leq wt(f) \leq 2^n - 2^{n-d}$.

Доказательство. Пусть $x_{i_1} x_{i_2} \ldots x_{i_d}$ — некоторое слагаемое длины d в АНФ функции f. Тогда подставляя всеми возможными способами константы 0 и 1 вместо оставшихся $n - d$ переменных, мы разложим f на 2^{n-d} подфункций $f_1, \ldots, f_{2^{n-d}}$. Каждая из этих подфункций содержит в АНФ слагаемое $x_{i_1} x_{i_2} \ldots x_{i_d}$. Поэтому $1 \leq wt(f_i) \leq 2^d - 1$, $i = 1, \ldots, 2^{n-d}$. Очевидно, $wt(f) = \sum\limits_{i=1}^{2^{n-d}} wt(f_i)$. Следовательно, $2^{n-d} \leq wt(f) \leq 2^n - 2^{n-d}$. □

Для корреляционно-иммунных функций имеет место *неравенство Зигенталера:*

Лемма 1.4. *Если f — корреляционно-иммунная порядка m функция на $\mathbf{F}_2^n$, то $\deg(f) \leq n - m$. Более того, если f является m-устойчивой, $m \leq n - 2$, то*

$$\deg(f) \leq n - m - 1. \tag{1.1}$$

Доказательство. Пусть f — корреляционно-иммунная порядка m функция на $\mathbf{F}_2^n$. Предположим, что $\deg(f) > n - m$. Рассмотрим в АНФ функции f слагаемое X самой большой длины (то есть включающее в себя наибольшее число переменных). Длина X, очевидно, равна $\deg(f)$. Если таких слагаемых несколько, то выберем одно из них произвольно. Подставим в f константы вместо всех переменных, не вошедших в X, а переменные, вошедшие в X, оставим свободными. Получится подфункцию f' от $\deg(f)$ переменных функции f, причем $\deg(f') = \deg(f)$. Поэтому по следствию 1.1 вес функции f' нечетен. Разложим функцию f' по одной из ее переменных на две подфункции от $\deg(f) - 1$ переменных. Очевидно, что вес одной из этих двух подфункций будет нечетен, а другой — четен. Если $\deg(f) - 1 > n - m$, то возьмем подфункцию от $\deg(f) - 1$ переменных с нечетным весом и снова разложим ее. Будем продолжать этот процесс до тех пор, пока в конце концов не получим две подфункции от $n - m$ переменных, причем вес одной из этих двух подфункций будет нечетен, а другой — четен. Это противоречит определению корреляционной иммунности. Таким образом, $\deg(f) \leq n - m$. Если функция f является к тому же и m-устойчивой, $m \leq n - 2$, и $\deg(f) \geq n - m$, то по предыдущему построению получим подфункцию f'' от $n - m$ переменных с нечетным весом. Однако $wt(f'') = wt(f)/2^m = 2^{n-1-m}$. Из того, что $m \leq n - 2$, следует, что величина $wt(f'')$ является четной. Полученное противоречие полностью доказывает неравенство Зигенталера. □

Пусть $m \leq n - 2$. Тогда m-устойчивая булева функция f называется *оптимальной,* если $\deg(f) = n-m-1$ (т. е. для функции f в неравенстве Зигенталера достигается равенство).

Лемма 1.5. *Пусть f является произвольной булевой функцией на $\mathbf{F}_2^n$. Тогда*

$$wt(f) = 2^{n-1} - \frac{1}{2}W_f(0).$$

Доказательство. Следует непосредственно из определения коэффициентов Уолша. □

Лемма 1.6. *Коэффициенты Фурье и Уолша связаны соотношением*

$$W_f(u) = 2^n \delta_u^0 - 2F_f(u).$$

Доказательство. Действительно,

$$F_f(u) = \sum_{x \in \mathbf{F}_2^n} f(x)(-1)^{<u,x>} = \sum_{\substack{x \in \mathbf{F}_2^n \\ f(x)=1}} (-1)^{<u,x>}.$$

Поэтому

$$W_f(u) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+<u,x>} = \sum_{\substack{x \in \mathbf{F}_2^n \\ f(x)=0}} (-1)^{<u,x>} - \sum_{\substack{x \in \mathbf{F}_2^n \\ f(x)=1}} (-1)^{<u,x>} =$$
$$\sum_{x \in \mathbf{F}_2^n} (-1)^{<u,x>} - 2 \sum_{\substack{x \in \mathbf{F}_2^n \\ f(x)=1}} (-1)^{<u,x>} = 2^n \delta_u^0 - 2F_f(u).$$

(Сумма $\sum\limits_{x \in \mathbf{F}_2^n} (-1)^{<u,x>}$ равна $\sum\limits_{x \in \mathbf{F}_2^n} 1 = 2^n$, если $u = 0$. Если же $u \neq 0$, то $u_i = 1$ для некоторого i. В этом случае все наборы $x \in \mathbf{F}_2^n$ можно разбить на пары (x', x'') наборов, различающихся только в i-й компоненте. Тогда $(-1)^{<u,x'>} + (-1)^{<u,x''>} = 0$. Поэтому $\sum\limits_{x \in \mathbf{F}_2^n} (-1)^{<u,x>} = 0$.) □

Использование коэффициентов Фурье или Уолша в различных случаях имеет свои преимущества. В дальнейшем будем рассматривать только коэффициенты Уолша.

Следующая лемма связывает коэффициенты Уолша булевой функции с коэффициентами Уолша ее подфункций.

Лемма 1.7. *Пусть* $X = (x_1, \ldots, x_n)$, $Y = (y_1, \ldots, y_k)$ — *наборы переменных,* $\sigma = (\sigma_1, \ldots, \sigma_k)$, $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_k)$. *Пусть имеет место представление*

$$g(X, Y) = \bigoplus_{\sigma \in \mathbf{F}_2^k} \left(\prod_{i=1}^{k} (y_i \oplus \sigma_i) \right) f_\sigma(X).$$

Тогда

$$W_g(uv) = \sum_{\sigma \in \mathbf{F}_2^k} (-1)^{<\sigma,v>} W_{f_{\sigma+(1,\ldots,1)}}(u).$$

Доказательство. Имеем

$$W_g(uv) = \sum_{X\sigma \in \mathbf{F}_2^{n+k}} (-1)^{g(X\sigma)+<X\sigma,uv>} =$$

$$\sum_{\sigma \in \mathbf{F}_2^k} (-1)^{<\sigma,v>} \sum_{X \in \mathbf{F}_2^n} (-1)^{g(X\sigma)+<X,u>} = \sum_{\sigma \in \mathbf{F}_2^k} (-1)^{<\sigma,v>} W_{f_{\sigma+(1,\ldots,1)}}(u).$$

□

Для коэффициентов Уолша справедлива следующая **формула обращения**.

Лемма 1.8. *Имеет место тождество.*

$$(-1)^{f(x)} = 2^{-n} \sum_{u \in \mathbf{F}_2^n} W_f(u)(-1)^{<u,x>}.$$

Доказательство. Преобразуем выражение, пользуясь определением коэффициентов Уолша:

$$2^{-n} \sum_{u \in \mathbf{F}_2^n} W_f(u)(-1)^{<u,x>} = 2^{-n} \sum_{u \in \mathbf{F}_2^n} \sum_{y \in \mathbf{F}_2^n} (-1)^{f(y)+<u,y>}(-1)^{<u,x>} =$$
$$2^{-n} \sum_{y \in \mathbf{F}_2^n} (-1)^{f(y)} \sum_{u \in \mathbf{F}_2^n} (-1)^{<u,x+y>} = 2^{-n}(-1)^{f(x)} \sum_{u \in \mathbf{F}_2^n} (-1)^{<u,x+x>} +$$
$$2^{-n} \sum_{\substack{y \in \mathbf{F}_2^n \\ y \neq x}} (-1)^{f(y)} \sum_{u \in \mathbf{F}_2^n} (-1)^{<u,x+y>} = 2^{-n}(-1)^{f(x)} \sum_{u \in \mathbf{F}_2^n} 1 + 0 =$$
$$2^{-n}(-1)^{f(x)} 2^n = (-1)^{f(x)}.$$

(В случае $y \neq x$ у набора $x + y$ найдется некоторая i-я компонента, равная 1. В этом случае все наборы $u \in \mathbf{F}_2^n$ можно разбить на пары (u', u'') наборов, различающихся только в i-й компоненте. Тогда $(-1)^{<u',x+y>} + (-1)^{<u'',x+y>} = 0$. Поэтому $\sum_{u \in \mathbf{F}_2^n} (-1)^{<u,x+y>} = 0$). □

Из формулы обращения видно, что по набору коэффициентов Уолша булева функция восстанавливается не более чем одним способом. А именно, если для всех 2^n наборов $x \in \mathbf{F}_2^n$ выражение

$$2^{-n} \sum_{u \in \mathbf{F}_2^n} W_f(u)(-1)^{<u,x>}$$

принимает значения ± 1, то булева функция восстанавливается однозначно. Если же хотя бы одно из этих выражений не равно ± 1, то данному набору коэффициентов Уолша никакая булева функция не соответствует.

Лемма 1.9. *Коэффициенты Уолша удовлетворяют* **равенству Парсеваля.**

$$\sum_{u \in \mathbf{F}_2^n} W_f^2(u) = 2^{2n}.$$

Доказательство.

$$\sum_{u \in \mathbf{F}_2^n} W^2(u) = \sum_{u \in \mathbf{F}_2^n} \left(\sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+<u,x>} \right)^2 =$$

$$\sum_{u \in \mathbf{F}_2^n} \left(2^n + \sum_{\substack{x', x'' \in \mathbf{F}_2^n, \\ x' \neq x''}} (-1)^{f(x')+f(x'')+<u,x'+x''>} \right) =$$

$$2^{2n} + \sum_{\substack{x', x'' \in \mathbf{F}_2^n, \\ x' \neq x''}} (-1)^{f(x')+f(x'')} \sum_{u \in \mathbf{F}_2^n} (-1)^{<u,x'+x''>} = 2^{2n}.$$

(В случае $x' \neq x''$ у набора $x' + x''$ найдется некоторая i-я компонента, равная 1. В этом случае все наборы $u \in \mathbf{F}_2^n$ можно разбить на пары (u', u'') наборов, различающихся только в i-й компоненте. Тогда $(-1)^{<u',x'+x''>} + (-1)^{<u'',x'+x''>} = 0$. Поэтому $\sum\limits_{u \in \mathbf{F}_2^n} (-1)^{<u,x'+x''>} = 0$). □

Докажем также полезное в дальнейшем *тождество Саркара.* Это тождество было доказано в [107]. Заметим, что в [107] доказательство тождества занимает три страницы. Здесь будет дано простое доказательство, впервые приведенное автором в [161], [164].

Лемма 1.10. (Тождество Саркара, [107]) *Пусть f — булева функция на $\mathbf{F}_2^n$. Тогда для любого $w \in \mathbf{F}_2^n$*

$$\sum_{\substack{u \in \mathbf{F}_2^n \\ u \preceq w}} W_f(u) = 2^n - 2^{|w|+1} wt(f_w), \tag{1.2}$$

где f_w это функция, полученная из f подстановкой $0 \to x_i$ для всех таких i, что $w_i = 1$.

Доказательство.

$$\sum_{\substack{u\in\mathbf{F}_2^n\\ u\preceq w}} W_f(u) = \sum_{\substack{u\in\mathbf{F}_2^n\\ u\preceq w}} \sum_{x\in\mathbf{F}_2^n} (-1)^{f(x)+<x,u>} = \sum_{x\in\mathbf{F}_2^n} (-1)^{f(x)} \sum_{\substack{u\in\mathbf{F}_2^n\\ u\preceq w}} (-1)^{<x,u>} =$$

$$\sum_{\substack{x\in\mathbf{F}_2^n\\ <x,w>=0}} (-1)^{f(x)} \sum_{\substack{u\in\mathbf{F}_2^n\\ u\preceq w}} (-1)^{<x,u>} + \sum_{\substack{x\in\mathbf{F}_2^n\\ <x,w>>0}} (-1)^{f(x)} \sum_{\substack{u\in\mathbf{F}_2^n\\ u\preceq w}} (-1)^{<x,u>} =$$

$$2^{|w|} \sum_{\substack{x\in\mathbf{F}_2^n\\ <x,w>=0}} (-1)^{f(x)} + \sum_{\substack{x\in\mathbf{F}_2^n\\ <x,w>>0}} (-1)^{f(x)} \cdot 0 =$$

$$2^{|w|} W_{f_w}(0) = 2^{|w|}(2^{n-|w|} - 2wt(f_w)) = 2^n - 2^{|w|+1} wt(f_w).$$

(Если $< x, w >= 0$ и $u \preceq w$, то $< x, u >= 0$. Поэтому $\sum\limits_{\substack{u\in\mathbf{F}_2^n\\ u\preceq w}} (-1)^{<x,u>} = \sum\limits_{\substack{u\in\mathbf{F}_2^n\\ u\preceq w}} 1 = 2^{|w|}$. Если же $< x, w >> 0$, то тогда найдется такое i, что $x_i = 1$ и $w_i = 1$. Объединим все $2^{|w|}$ наборов u, $u \preceq w$, в пары так, чтобы каждая пара (u', u'') содержала наборы u' и u'', различающиеся в i-й компоненте и совпадающие во всех остальных компонентах. Тогда $(-1)^{<x,u'>} + (-1)^{<x,u''>} = 0$. Поэтому $\sum\limits_{\substack{u\in\mathbf{F}_2^n\\ u\preceq w}} (-1)^{<x,u>} = 0$.) □

Пусть $u \in \mathbf{F}_2^n$. Обозначим через l_u линейную функцию $l_u(x_1, \ldots, x_n) = \bigoplus\limits_{i=1}^{n} u_i x_i$. Из определения коэффициентов Уолша легко видеть, что

Лемма 1.11. $W_f(u) = W_{f\oplus l_u}(0) = 2^n - 2wt(f \oplus l_u) = 2^n - 2d(f, l_u)$.

Следствие 1.2. *Функция f на $\mathbf{F}_2^n$ является уравновешенной тогда и только тогда, когда $W_f(0) = 0$.*

Имеет место характеризация корреляционно-иммунных функций с помощью коэффициентов Уолша. Впервые эта характеризация была получена в [68]. Здесь приводится основанное на тождестве Саркара более простое доказательство, впервые данное автором в [165].

Лемма 1.12. *Функция f на $\mathbf{F}_2^n$ является корреляционно-иммунной функцией порядка m тогда и только тогда, когда $W_f(w) = 0$ для всех наборов $w \in \mathbf{F}_2^n$, для которых $1 \le |w| \le m$.*

Доказательство. Пусть булева функция f является корреляционно-иммунной функцией порядка m. Докажем утверждение индукцией по величине

$|w|$. Пусть утверждение верно для всех ненулевых наборов с весом меньше $|w|$. (Если $|w| = 1$, то основание индукции тривиально верно, потому что в этом случае требуется справедливость утверждения для пустого множества наборов.) В силу тождества Саркара имеем

$$\sum_{\substack{u \in \mathbf{F}_2^n \\ u \preceq w}} W_f(u) = 2^n - 2^{|w|+1} wt(f_w).$$

В левой части этого выражения ненулевыми по предположению индукции являются максимум два слагаемых: $W_f(0) = 2^n - 2wt(f)$ и $W_f(w)$. Величина $wt(f_w)$ в силу корреляционной иммунности функции f равна $wt(f)/2^{|w|}$. Поэтому правая часть выражения равна $2^n - 2wt(f)$. Отсюда $W_f(w) = 0$, что нам и требовалось.

Пусть теперь $W_f(w) = 0$ для всех наборов $w \in \mathbf{F}_2^n$, для которых $1 \leq |w| \leq m$. Тогда в силу тождества Саркара

$$\sum_{\substack{u \in \mathbf{F}_2^n \\ u \preceq w}} W_f(u) = 2^n - 2^{|w|+1} wt(f_w).$$

Левая часть этого выражения равна $W_f(0) = 2^n - 2wt(f)$. Отсюда $wt(f_w) = wt(f)/2^{|w|}$. Следовательно, вес любой подфункции f' функции f, полученной подстановкой в f констант 0 вместо любых h, $0 \leq h \leq m$, переменных, равен $wt(f)/2^h$. Нам нужно доказать этот факт в случае, когда подставляются не только нули, но и единицы. Будем проводить это доказательство двойной индукцией. Внешняя индукция будет осуществляться по количеству h подставляемых констант, а внутренняя — по количеству l подставляемых единиц. Основание внешней индукции — случай $h = 0$ — справедливо, потому что вес самой функции f равен $wt(f) = wt(f)/2^0$. Основание внутренней индукции — случай $l = 0$ — справедливо в силу ранее доказанного равенства $wt(f_w) = wt(f)/2^{|w|}$. Пусть утверждение доказано, если подставляется менее h констант, а также если подставляется h констант, из которых менее l единиц. Докажем утверждение в случае, когда подставляется в точности h констант, среди которых в точности l единиц. Пусть некоторая такая подстановка дает подфункцию f' от $n-h$ переменных. Пусть x_i — переменная функции f, вместо которой была подставлена еди-

ница. Тогда можно записать $f' = (f'')^1_{x_i}$, где f'' — функция, полученная из f подстановкой $h-1$ констант, среди которых в точности ровно $l-1$ единицы. Очевидно, что $f'' = x_i(f')^1_{x_i} \oplus (x_i \oplus 1)(f')^0_{x_i}$ и $wt(f'') = wt((f')^1_{x_i}) + wt((f')^0_{x_i})$. По предположению индукции мы имеем, что $wt(f'') = wt(f)/2^{h-1}$, $wt((f')^0_{x_i}) = wt(f)/2^h$. Тогда $wt(f') = wt((f')^1_{x_i}) = wt(f)/2^h$, что и требовалось доказать. Шаг индукции доказан, что доказывает и все утверждение. □

Следствие 1.3. *Функция f на $\mathbf{F}_2^n$ является m-устойчивой тогда и только тогда, когда $W_f(w) = 0$ для всех наборов $w \in \mathbf{F}_2^n$, для которых $|w| \leq m$.*

Справедливо также следующее свойство коэффициентов Уолша корреляционно-иммунной функции, полученное в [109]. Здесь оно приводится с доказательством автора.

Лемма 1.13. [109] *Если f является корреляционно-иммунной функцией порядка m на $\mathbf{F}_2^n$, $m \leq n-1$, то для любого $w \in \mathbf{F}_2^n$ выполнено $W_f(w) \equiv 0 \pmod{2^{m+1}}$. Более того, если f является m-устойчивой, $m \leq n-2$, то $W_f(w) \equiv 0 \pmod{2^{m+2}}$.*

Доказательство. Рассмотрим сначала корреляционно-иммунную порядка m функцию f. Докажем утверждение индукцией по $|w|$. Если $w = 0$, то $W_f(0) = 2^n - 2wt(f)$. По условию $n - m \geq 1$, поэтому 2^n делится на 2^{m+1}. По определению корреляционной иммунности число $wt(f)/2^m$ целое, поэтому величина $2wt(f)$ также делится на 2^{m+1}. Поэтому $W_f(0) \equiv 0 \pmod{2^{m+1}}$. Для $1 \leq |w| \leq m$ все коэффициенты Уолша $W_f(w)$ по ранее доказанному равны 0. Пусть утверждение справедливо для всех наборов с весом меньше $|w|$, $|w| \geq m+1$. По тождеству Саркара

$$\sum_{\substack{u \in \mathbf{F}_2^n \\ u \preceq w}} W_f(u) = 2^n - 2^{|w|+1} wt(f_w).$$

Правая часть равенства, очевидно, делится на 2^{m+1}. В левой части по индуктивному предположению на 2^{m+1} делятся все слагаемые, кроме, может быть, $W_f(w)$. Однако тогда и $W_f(w) \equiv 0 \pmod{2^{m+1}}$.

Пусть теперь f является m-устойчивой функцией, $n - m \geq 2$. Докажем утверждение индукцией по $|w|$. Если $w = 0$, то $W_f(0) = 0$ в силу уравновешенности функции f. Для $1 \leq |w| \leq m$ все коэффициенты Уолша $W_f(w)$ по ранее доказанному равны 0. Пусть утверждение справедливо для всех наборов с весом меньше $|w|$, $|w| \geq m + 1$. По тождеству Саркара

$$\sum_{\substack{u \in \mathbf{F}_2^n \\ u \preceq w}} W_f(u) = 2^n - 2^{|w|+1} wt(f_w).$$

Правая часть равенства, очевидно, делится на 2^{m+2}. В левой части по индуктивному предположению на 2^{m+2} делятся все слагаемые, кроме, может быть, $W_f(w)$. Однако тогда и $W_f(w) \equiv 0 \pmod{2^{m+2}}$. □

Следующее небольшое усиление леммы 1.13 дано в [126]. Оно приводится здесь с доказательством автора, которое полностью аналогично предыдущему.

Лемма 1.14. [126] *Если f является корреляционно-иммунной функцией порядка m на $\mathbf{F}_2^n$, $m \leq n - 2$, и $W_f(0) \equiv 0 \pmod{2^{m+2}}$, то для любого $w \in \mathbf{F}_2^n$ выполнено $W_f(w) \equiv 0 \pmod{2^{m+2}}$.*

Доказательство. Пусть f является корреляционно-иммунной функцией порядка m на $\mathbf{F}_2^n$, $m \leq n - 2$, и $W_f(0) \equiv 0 \pmod{2^{m+2}}$. Докажем утверждение индукцией по $|w|$. Если $w = 0$, то утверждение леммы справедливо по ее условию. Для $1 \leq |w| \leq m$ все коэффициенты Уолша $W_f(w)$ по ранее доказанному равны 0. Пусть утверждение справедливо для всех наборов с весом меньше $|w|$, $|w| \geq m + 1$. По тождеству Саркара

$$\sum_{\substack{u \in \mathbf{F}_2^n \\ u \preceq w}} W_f(u) = 2^n - 2^{|w|+1} wt(f_w).$$

Правая часть равенства, очевидно, делится на 2^{m+2}. В левой части по индуктивному предположению на 2^{m+2} делятся все слагаемые, кроме, может быть, $W_f(w)$. Однако тогда и $W_f(w) \equiv 0 \pmod{2^{m+2}}$. □

Две следующие леммы хорошо известны.

Лемма 1.15. *Пусть $f(x_1, \ldots, x_n)$ — булева функция, заданная на $\mathbf{F}_2^n$. Тогда $\deg(f) = n$ в том и только том случае, когда $wt(f)$ нечетно.*

Доказательство. Функция f может быть представлена в виде

$$f(x_1,\dots,x_n)=\bigoplus_{\substack{(\sigma_1,\dots,\sigma_n)\in\mathbf{F}_2^n\\ f(\sigma_1,\dots,\sigma_n)=1}}(x_1\oplus\sigma_1\oplus 1)\dots(x_n\oplus\sigma_n\oplus 1).$$

Число слагаемых в этой сумме равно весу f. Поэтому после раскрытия скобок и приведения подобных слагаемых слагаемое длины n будет присутствовать в полиноме f, тогда и только тогда, когда $wt(f)$ нечетно. □

Лемма 1.16. *Пусть $f(x_1,\dots,x_n)$ — булева функция, представленная в виде*

$$f(x_1,\dots,x_n)=\bigoplus_{(\sigma_1,\dots,\sigma_l)}(x_1\oplus\sigma_1)\dots(x_l\oplus\sigma_l)f(\sigma_1\oplus 1,\dots,\sigma_l\oplus 1,x_{l+1},\dots,x_n).$$

Предположим, что все 2^l подфункций $f(\sigma_1\oplus 1,\dots,\sigma_l\oplus 1,x_{l+1},\dots,x_n)$ являются m-устойчивыми. Тогда функция f также является m-устойчивой.

Лемма 1.16 была доказана во множестве статей, включая (для случая $l=1$) основополагающую статью Зигенталера (теорема 2 в [113]). Общий случай следует из случая $l=1$ немедленно.

Лемма 1.17. *Пусть $g(x_1,\dots,x_n,y)=f(x_1,\dots,x_n)$ (переменная y является фиктивной для функции $g(x_1,\dots,x_n,y)$). Тогда $wt(g(x_1,\dots,x_n,y))=2wt(f(x_1,\dots,x_n))$.*

Доказательство. Для любого набора $x\in\mathbf{F}_2^n$ имеем $g(x,0)=g(x,1)=f(x)$. Поэтому $wt(g)=2wt(f)$. □

Лемма 1.18. *Пусть $f(x_1,\dots,x_n)$ — произвольная функция на $\mathbf{F}_2^n$, и пусть $g(x_1,\dots,x_{n-1},z_1,z_2)=f(x_1,\dots,x_{n-1},z_1\oplus z_2)$ — функция на $\mathbf{F}_2^{n+1}$. Тогда $wt(g)=2wt(f)$.*

Доказательство. Равенства $f(x_1,\dots,x_{n-1},0)=g(x_1,\dots,x_{n-1},0,0)=g(x_1,\dots,x_{n-1},1,1)$ и $f(x_1,\dots,x_{n-1},1)=g(x_1,\dots,x_{n-1},0,1)=g(x_1,\dots,x_{n-1},1,0)$ доказывают эту лемму. □

Лемма 1.19. *Пусть $f(x_1,\dots,x_n)$ — произвольная булева функция. Тогда функция $g(x_1,\dots,x_n,y)=f(x_1,\dots,x_n)\oplus y$ является уравновешенной.*

Доказательство. Объединим все 2^{n+1} наборов функции g в пары, так чтобы любая пара (x', x'') содержала наборы x' и x'', которые различаются в $(n+1)$-й компоненте и совпадают во всех остальных компонентах. Тогда $f(x') = f(x'')$ и $g(x') \neq g(x'')$. Таким образом, $wt(g) = 2^n$ и функция g — уравновешенная. □

Лемма 1.20. *Пусть* $g(x_1, \ldots, x_n, y) = f(x_1, \ldots, x_n) \oplus cy$, *где* $c \in \{0, 1\}$. *Тогда* $nl(g) = 2nl(f)$.

Доказательство. Нелинейность функции $g(x_1, \ldots, x_n, y)$ это минимум весов функций

$$g_\alpha = \bigoplus_{i=1}^{n} \alpha_i x_i \oplus \beta y \oplus f(x_1, \ldots, x_n)$$

на множестве всех двоичных наборов $\alpha = (\alpha_1, \ldots, \alpha_n, \beta)$ длины $n+1$. Если $\beta = 1$, то функция g_α является уравновешенной по лемме 1.19. Поэтому в этом случае $wt(g_\alpha) = 2^n$. Если $\beta = 0$, то по лемме 1.17 мы имеем $wt(g_\alpha) = 2wt\left(f(x_1, \ldots, x_n) \bigoplus_{i=1}^{n} \alpha_i x_i\right) \geq 2nl(f)$. Последнее неравенство достигается для некоторого набора α. Таким образом, $nl(g) = \min\{2^n, 2nl(f)\} = 2nl(f)$. □

Лемма 1.21. *Пусть* $f(x_1, \ldots, x_n)$ — *произвольная булева функция на* $\mathbf{F}_2^n$ *и* $g(x_1, \ldots, x_{n-1}, z_1, z_2) = f(x_1, \ldots, x_{n-1}, z_1 \oplus z_2) \oplus z_1$. *Тогда функция* g *на* $\mathbf{F}_2^{n+1}$ *является уравновешенной.*

Доказательство. Объединим все 2^{n+1} наборов функции g в пары, так чтобы любая пара (x', x'') содержала наборы x' и x'', которые различаются в n-й и $(n+1)$-й компонентах и совпадают во всех остальных компонентах. Тогда $g(x') \neq g(x'')$. Таким образом, функция g является уравновешенной. □

Лемма 1.22. *Пусть* $f(x_1, \ldots, x_n)$ — *произвольная булева функция на* $\mathbf{F}_2^n$ *и* $g(x_1, \ldots, x_{n-1}, z_1, z_2) = f(x_1, \ldots, x_{n-1}, z_1 \oplus z_2) \oplus c_1 z_1 \oplus c_2 z_2$, *где* $c_1, c_2 \in \{0, 1\}$. *Тогда* $nl(g) = 2nl(f)$.

Доказательство. Нелинейность функции g равна минимуму весов функций

$$g_\alpha = f(x_1, \ldots, x_{n-1}, z_1 \oplus z_2) \oplus \bigoplus_{i=1}^{n-1} \alpha_i x_i \oplus \gamma_1 z_1 \oplus \gamma_2 z_2 \oplus \delta$$

на множестве всех двоичных наборов $\alpha = (\alpha_1, \ldots, \alpha_{n-1}, \gamma_1, \gamma_2, \delta)$ длины $n+2$. Если $\gamma_1 \neq \gamma_2$, то по лемме 1.21 функция g_α является уравновешенной. Но нелинейность функции на $\mathbf{F}_2^{n+1}$ всегда меньше чем 2^n. Поэтому можно исключить случай $\gamma_1 \neq \gamma_2$ из нашего рассмотрения. Таким образом, предполагаем, что $\gamma_1 = \gamma_2 = \gamma$. В этом случае $g_\alpha = f'(x_1, \ldots, x_{n-1}, z_1 \oplus z_2)$ для некоторой функции f' на $\mathbf{F}_2^n$, $nl(f') = nl(f)$. По лемме 1.18 имеем $wt(g_\alpha) = 2wt(f') \geq 2nl(f)$, поэтому $nl(g) \geq 2nl(f)$. С другой стороны, для некоторого набора α вес соответствующей функции f' достигает минимума нелинейности для f. Таким образом, $nl(g) = 2nl(f)$. $\square$

Коэффициенты Уолша удовлетворяют формуле обращения $(-1)^{f(x)} = 2^{-n} \sum\limits_{u \in F_2^n} W_f(u)(-1)^{<u,x>}$ и равенству Парсеваля $\sum\limits_{u \in F_2^n} W_f^2(u) = 2^{2n}$. Нелинейность булевой функции f выражается через ее коэффициенты Уолша следующим образом: $nl(f) = 2^{n-1} - \frac{1}{2} \max\limits_{u \in \mathbf{F}_2^n} |W_f(u)|$.

Бент-функции существуют при всех четных n, а при нечетных — не существуют. Бент-функция является функцией с максимально возможной нелинейностью $2^{n-1} - 2^{(n/2)-1}$ среди всех функций от n переменных при четном n.

1.3 О связи корреляционно-иммунных булевых функций с кодами и ортогональными массивами

В данном параграфе будет указано на тесную связь корреляционно-иммунных булевых функций с кодами, особенно в том случае, когда, рассматриваются вопросы, связанные с дуальными расстояниями кодов, и с ортогональными массивами. Также дается обзор некоторых результатов на стыке этих областей. Основой параграфа послужила статья автора [160].

Произвольное множество наборов $C \in \mathbf{F}_2^n$ называется *(двоичным) кодом*. Понятия булевой функции и кода тесно связаны. Произвольная булева функция f на $\mathbf{F}_2^n$ ассоциируется с ее *характеристическим множеством* — кодом C: $\{x \in \mathbf{F}_2^n \,|\, f(x) = 1\}$. Наоборот, произвольный код $C \in \mathbf{F}_2^n$ ассоциируется с его *характеристической функцией* — функцией f: $f(x) = \begin{cases} 1 & \text{если } x \in C, \\ 0 & \text{если } x \notin C. \end{cases}$ Код C называется *линейным,* если для любых x, y, $z \in \mathbf{F}_2^n$, таких что $z = x \oplus y$, имеем $z \in C$, если x, $y \in C$. *(Кодовым) расстоянием* $d = d(C)$ кода C называется минимум по всем попарным расстояниям между различными наборами из C. *Распределение весов* кода C по отношению к вектору $x \in \mathbf{F}_2^n$ — это набор $A(C, x) = (A_0(x), A_1(x), \ldots, A_n(x))$, где $A_i(x)$ — это число векторов в C, расстояние Хэмминга от которых до x в точности равно i. *Распределение весов* кода C — это распределение весов этого кода по отношению к нулевому вектору.

(Двоичный) *ортогональный массив* $OA(h, n, 2, m)$ — это матрица размера $h \times n$, клетки которой заполнены элементами из множества $\{0, 1\}$, так что внутри любых m столбцов каждый упорядоченный поднабор двоичных символов встречается в точности в $\lambda = h/2^m$ строках. Ортогональный массив называется *простым,* если все строки в этом массиве попарно различны. Параметр m называется *силой* ОА. Любая двоичная матрица может рассматриваться как ортогональный массив (может быть, силы 0). Если двоичная матрица является $OA(h, n, 2, m)$, но не является $OA(h, n, 2, m + 1)$, то говорим, что максимальная сила этого ОА равна m. Ортогональные массивы были введены в 1947 году индийским статистиком Рао [97] при изучении задачи планирования статистических экспериментов. Недавно вышла монография [69], целиком посвященная ортогональным массивам.

Простому $OA(h, n, 2, m)$ можно сопоставить код C в $\mathbf{F}_2^n$, где C — это множество всех наборов из $\mathbf{F}_2^n$, заданных строками ОА. Хорошо известно, что если код C является линейным, то максимальная сила соответствующего ему ОА равна $d' - 1$, где d' — это *дуальное расстояние* C (т. е. кодовое расстояние кода $C^\perp$, дуального к C). Распределение весов $A(C^\perp)$ кода $C^\perp$, дуального к линейному коду C может быть найдено из распределения весов $A(C)$ кода C с помощью тождеств Мак-Вильямс [78], и минимальное натуральное число i, такое что $A_i(C^\perp) \neq 0$, равно дуальному расстоянию d'. Если код C не является линейным, то понятие дуального кода $C^\perp$ не определено. Тем не менее, Дельсарт показал [60], что если вычислить формально распределение весов $A(C^\perp)$ через тождества Мак-Вильямс и положить d' равным минимальному натуральному i, такому что $A_i(C^\perp) \neq 0$, то максимальная сила ОА, соответствующего коду C будет равна $d' - 1$ так же, как и для линейного кода.

В [42] было показано, что корреляционно-иммунная функция является частным случаем ортогонального массива (ОА), а именно, корреляционно-иммунная порядка m функция от n переменных с весом $wt(f)$ соответствует простому $OA(wt(f), n, 2, m)$ (все наборы x, для которых $f(x) = 1$, задаются строками ОА). Таким образом, максимальный порядок корреляционной иммунности булевой функции равен максимальной силе соответствующего ей ОА, и равен дуальному расстоянию ее характеристического кода, уменьшенному на 1.

Напомним, что булева функция f на $\mathbf{F}_2^n$ называется (c_0, c_1)-регулярной (или просто регулярной), если 1) для любого набора $x \in \mathbf{F}_2^n$, такого что $f(x) = 0$, имеем $\#\{y \in \mathbf{F}_2^n \,|\, d(x,y) = 1, f(y) = 1\} = c_0$; 2) для любого набора $x \in \mathbf{F}_2^n$, такого что $f(x) = 1$, имеем $\#\{y \in \mathbf{F}_2^n \,|\, d(x,y) = 1, f(y) = 0\} = c_1$. Булева функция, являющаяся (c,c)-регулярной, называется c-регулярной функцией. Характеристический код регулярной булевой функции — это частный случай *полностью регулярного кода* [59], а также частный случай *дизайна r-разбиения* [43] (при $r = 1$). Характеристический код C регулярной (c_0, c_1)-функции удовлетворяет соотношению $A_1(C,x) = \begin{cases} c_0 & \text{если } x \notin C, \\ c_1 & \text{если } x \in C. \end{cases}$ Для устойчивых функций более общее понятие покрывающих последовательностей булевых функций обсуждается в [131]. Частным случаем теоремы 3.1, пункт 1 в [56] является следующее утверждение.

Теорема 1.1. *[56] Дуальное расстояние d' характеристического кода (c_0, c_1)-регулярной функции равно $d' = \frac{c_0+c_1}{2}$.*

Следствие 1.4. *Из теоремы 1.1 следует, что максимальный порядок корреляционной иммунности (c_0, c_1)-регулярной булевой функции равен $\frac{c_0+c_1}{2} - 1$.*

Если f является c-регулярной функцией на $\mathbf{F}_2^n$, то функция f является уравновешенной; кроме того функция $f \oplus \bigoplus_{i=1}^{n}$ является $(n-c)$-регулярной. Из этого следует, что любая уравновешенная регулярная функция от n переменных порождает устойчивую булеву функцию порядка не менее чем $\lceil \frac{n}{2} \rceil - 1$.

Обозначим через $\Phi = \Phi(x_1, \ldots, x_6)$ булеву функцию

$$\Phi = \bigoplus_{1 \le i < j < k \le 6} x_i x_j x_k \oplus x_1x_2 \oplus x_2x_3 \oplus x_3x_4 \oplus x_4x_5 \oplus x_1x_5 \oplus \bigoplus_{i=1}^{5} x_i \oplus 1.$$

Эта функция впервые приведена в работе автора [157], а также упоминается в работах автора [159], [160] и [134]. Функция Φ имеет множество замечательных свойств и будет обсуждаться в последующих параграфах. В частности, непосредственной проверкой легко убедиться, что функция Φ является $(3,5)$-регулярной. Вес функции Φ равен 24. Все 24 единичные значения функции Φ

разбиваются на 12 пар соседних наборов, которые в свою очередь объединяются в шесть пар параллельных ребер, идущих вдоль каждого из шести направлений.

Как было отмечено выше, существует соответствие между корреляционно-иммунными функциями, кодами (относительно их дуальных расстояний) и простыми ортогональными массивами. Таким образом, результаты существования (или несуществования), полученные в одной из этих трех областей, могут быть перенесены в другие. Легко видеть из определения, что для $OA(h, n, 2, m)$ величина 2^m делит h. В теории ортогональных массивов одной из наиболее популярных задач является получение нижней оценки для h. Наиболее знаменитыми и важными нижними оценками являются классическое неравенство Рао [97] $h \geq \sum_{i=0}^{\lfloor m/2 \rfloor} \binom{n}{i}$ и неравенство Бирбрауэра–Фридмана [64, 37] $h \geq 2^n \left(1 - \frac{n}{2(m+1)}\right)$. Для корреляционно-иммунных булевых функций последнее неравенство может быть переписано в форме $wt(f) \geq 2^n \left(1 - \frac{n}{2(m+1)}\right)$. Положим $k = n - m$. Правая часть последнего неравенства больше чем $\frac{2^{k-1}-1}{2^k} 2^n$ при $n > (2^{k-1}+1)(k-1)$. Следовательно, не существует неуравновешенной неконстантной корреляционно-иммунной функции порядка $n - k$ от n переменных при $n \geq (k-1)2^{k-1} + k$. [157] В параграфе 3.3 мы существенно улучшим эту оценку, показав, что не существует таких функций при $n \geq 4(k-1)$. Заметим, что для заданного k максимально известное на настоящий момент автору n, такое что существует неуравновешенная неконстантная корреляционно-иммунная функция порядка $n - k$ от n переменных равно $3k - 3$. Это значение достигается по крайней мере на трех семействах функций (с точностью до линейных трансформаций и отрицания). Одно из них может быть задано характеристическим линейным кодом с проверочной матрицей

$$\left(\begin{array}{cccccccccccc} 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 \\ \underbrace{0}_{k-1} & \underbrace{0}_{} & \dots & \underbrace{0}_{} & \underbrace{1}_{k-1} & \underbrace{1}_{} & \dots & \underbrace{1}_{} & \underbrace{1}_{k-1} & \underbrace{1}_{} & \dots & \underbrace{1}_{} \end{array} \right).$$

Легко видеть, что дуальное расстояние этого кода длины $n = 3k - 3$ равно $2k - 2$, таким образом, максимальный порядок корреляционной иммунности равен $2k - 3$, а вес функции равен $2^n/4$. Кроме того, несложно видеть, что эта функция является $(n/3, n)$-регулярной. Рассматривая проверочные матрицы,

нетрудно понять, что для заданного k величина $n = 3k - 3$ является максимальной в классе неуравновешенных неконстантных корреляционно-иммунных порядка $n - k$ от n переменных характеристических функций линейных кодов. Второе семейство было найдено автором и задается следующими функциями: $\Phi_s = \Phi(x_{11} \oplus \cdots \oplus x_{1s}, \ldots, x_{61} \oplus \cdots \oplus x_{6s})$, $s = 1, 2, \ldots$. Функция Φ_s является корреляционно-иммунной функцией порядка $(4s-1)$ от $6s = 3(2s+1)-3$ переменных, а вес функции равен $(3/8)2^n$. Третье семейство было построено студентом автора Денисом Кириенко в [11]. Основой семейства является 5-устойчивая функция от 9 переменных $\Psi(x_1, \ldots, x_9) = (x_1 \oplus x_2 \oplus x_3 \oplus 1)(x_4 \oplus x_5 \oplus x_6) \oplus (x_1 \oplus x_4)(x_2 \oplus x_5)(x_3 \oplus x_6) \oplus (x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6)(x_7 \oplus x_8 \oplus x_9)$. В качестве базисной можно взять и любую функцию, получающуюся из Ψ автоморфизмами булева куба, сохраняющими расстояния. Семейство $(6s-1)$-устойчивых функций от $9s$ переменных, $s = 1, 2, \ldots$, строится следующим образом: $g(x_{11}, \ldots, x_{1s}, \ldots, x_{91}, \ldots, x_{9s}) = \Psi(x_{11} \oplus \ldots \oplus x_{1s}, \ldots, x_{91} \oplus \ldots \oplus x_{9s})$. Существование неуравновешенной неконстантной корреляционно-иммунной функции порядка $n - k$ от n переменных при $n > 3k - 3$ является открытым вопросом.

Простой $OA(h, n, 2, m)$ при $h = 2^{m-1}$ не является интересным объектом для исследования в теории ортогональных массивов. Очевидно, что такой ОА существует даже при $m - 1$ (ОА, соответствующий коду проверки на четность). Однако для корреляционно-иммунных функций ситуация противоположна. Уравновешенные корреляционно-иммунные (устойчивые) функции наиболее важны для приложений, в то время как линейная сумма всех переменных по модулю 2 не является криптографически хорошей функцией по другим критериям (например, алгебраической степени и нелинейности). Поэтому важным вопросом является здесь существование устойчивых функций, которые зависят от всех своих переменных нелинейно. Автором доказано, [157, 156, 133] что для любого натурального k существует минимальное неотрицательное целое $p(k)$, такое что любая $(n-k)$-устойчивая функция от n переменных зависит нелинейно от не более чем $p(k)$ входов. Позднее в [164] и [161] автором совместно с его студентом Денисом Кириенко было доказано, что $p(k) \leq (k-1)4^{k-2}$. Наилучший на данный момент результат $p(k) \leq (k-1)2^{k-2}$ получен автором

в [166] (результаты этой работы содержится в также в [136]) и излагается в параграфе 3.2. Заметим, впрочем, что в [164] и [161] показано, что $p(4) = 10$. Нижняя оценка $p(k) \geq 3 \cdot 2^{k-2} - 2$ для $k \geq 3$ [158] получается в параграфах 2.2 и 2.3 с помощью рекурсивной конструкции $f_3 = (x_1 \oplus x_2)(x_3 \oplus x_4) \oplus x_1 \oplus x_3$, $f_{k+1}(x_1, \ldots, x_{2n(k)+2})(x_{2n(k)+1} \oplus x_{2n(k)+2}) \left(f_k(x_1, \ldots, x_{n(k)}) \oplus \bigoplus_{i=n(k)+1}^{2n(k)} x_i \right) \oplus (x_{2n(k)+1} \oplus x_{2n(k)+2} \oplus 1) \left(f_k(x_{n(k)+1}, \ldots, x_{2n(k)}) \oplus \bigoplus_{i=1}^{n(k)} x_i \right) \oplus x_{2n(k)+1}$.

1.4 Верхняя оценка для нелинейности устойчивых функций

В этом параграфе устанавливаются верхние оценки для нелинейности устойчивых, а также неоптимальных устойчивых, регулярных и корреляционно-иммунных функций.

Пусть $u \in \mathbf{F}_2^n$. Обозначим через l_u линейную функцию $l_u(x_1, \ldots, x_n) = \bigoplus_{i=1}^{n} u_i x_i$. Из определения коэффициентов Уолша и леммы 1.11 легко видеть, что $W_f(u) = W_{f \oplus l_u}(0) = 2^n - 2wt(f \oplus l_u)2^n - 2d(f, l_u)$. Поэтому,

$$d(f, l_u) = 2^{n-1} - \tfrac{1}{2} W_f(u),$$
$$d(f, l_u \oplus 1) = 2^{n-1} + \tfrac{1}{2} W_f(u).$$

Отсюда следует, что

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbf{F}_2^n} |W_f(u)|. \tag{1.3}$$

Из этого равенства видно, что нелинейность функции f равна 0 (то есть функция аффинная) тогда и только тогда, когда $\max\limits_{u \in \mathbf{F}_2^n} |W_f(u)| = 2^n$, то есть один из коэффициентов Уолша равен $\pm 2^n$, а все остальные нулевые. Из равенства Парсеваля вытекает, что $\max\limits_{u \in \mathbf{F}_2^n} |W_f(u)| \geq 2^{n/2}$, поэтому

$$nl(f) \leq 2^{n-1} - 2^{n/2-1}. \tag{1.4}$$

Функция, нелинейность которой достигает верхней границы $2^{n-1} - 2^{n/2-1}$, называется *бент-функцией*. Из того, что при нечетном n величина $2^{n-1} - 2^{n/2-1}$ не является целым числом, следует, что бент-функций от нечетного числа переменных не существует. Для любого четного n бент-функции существуют.

Пусть m и n — целые числа, $-1 \leq m \leq n$. Обозначим через $\mathrm{nlmax}(n, m)$ максимально возможную нелинейность m-устойчивой булевой функции, заданной на $\mathbf{F}_2^n$. Из сказанного выше следует, что

$$\mathrm{nlmax}(n, -1) \leq 2^{n-1} - 2^{\frac{n}{2}-1}, \tag{1.5}$$

Это значение может достигаться только для четных n. Таким образом, для четных n имеем $\mathrm{nlmax}(n,-1) = 2^{n-1} - 2^{\frac{n}{2}-1}$. Известно, [92, 93, 62] что для нечетных n, $n \le 7$, $\mathrm{nlmax}(n,-1) = 2^{n-1} - 2^{(n-1)/2}$, а для нечетных n, $n \ge 15$, справедливо неравенство $\mathrm{nlmax}(n,-1) > 2^{n-1} - 2^{(n-1)/2}$. Бент функции всегда неуравновешены, поэтому для уравновешенной (0-устойчивой) функции f от n переменных имеем $nl(f) < 2^{n-1} - 2^{\frac{n}{2}-1}$, и

$$\mathrm{nlmax}(n,m) < 2^{n-1} - 2^{\frac{n}{2}-1} \text{ при } m \ge 0. \tag{1.6}$$

Если f является m-устойчивой функцией от n переменных, $m \ge n-2$, то по неравенству Зигенталера [113] выполнено $\deg(f) \le 1$, отсюда $\mathrm{nlmax}(n,m) = 0$. В [90] было доказано, что $\mathrm{nlmax}(n,n-3) = 2^{n-2}$ и высказана гипотеза, что $\mathrm{nlmax}(n,n-4) = 2^{n-1} - 2^{n-3}$. Для некоторых малых значений параметров n и m точные значения максимальной нелинейности известны. Так, $\mathrm{nlmax}(4,0) = 4$, $\mathrm{nlmax}(5,-1) = \mathrm{nlmax}(5,0) = \mathrm{nlmax}(5,1) = 12$, $\mathrm{nlmax}(6,0) = 26$ [61], $\mathrm{nlmax}(6,1) = \mathrm{nlmax}(6,2) = 24$ [90], $\mathrm{nlmax}(7,-1) = 56$ [86], $\mathrm{nlmax}(7,0) = \mathrm{nlmax}(7,1) = 56$ [52]. Все эти значения получены соединением конструкций конкретных функций с верхними оценками (1.5), (1.6) или, может быть, [61], [90], с помощью исчерпывающего поиска.

Из леммы 1.13 и равенства Парсеваля следует, что для коэффициентов Уолша m-устойчивой булевой функции на $\mathbf{F}_2^n$ справедливо неравенство $\max\limits_{u \in \mathbf{F}_2^n} |W_f(u)| \ge 2^{m+2}$. Отсюда, учитывая (1.3), имеем

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbf{F}_2^n} |W_f(u)| \le 2^{n-1} - 2^{m+1}. \tag{1.7}$$

Приведенное рассуждение (включая доказанную в параграфе 1.2 лемму 1.13) следует доказательству верхней оценки (1.7), данной Саркаром и Майтрой в [109]. Одновременно и независимо этот же результат был получен другими методами автором в [159] и [134], и Зенгом и Зангом в [126]. Ниже приводится этот результат, доказанный методом автора (теорема 1.2). Заметим, что метод автора позволил получить следующую ниже теорему 1.3, которая в параллельных работах Саркара–Майтры и Зенга–Занга получена не была.

Теорема 1.2. *Пусть $f(x_1, \ldots, x_n)$ является m-устойчивой булевой функцией, $m \leq n-2$. Тогда*

$$nl(f) \leq 2^{n-1} - 2^{m+1}. \tag{1.8}$$

Доказательство. Если $m = n-2$, то по неравенству Зигенталера $\deg(f) \leq 1$, поэтому f является аффинной функцией и $nl(f) = 0$. Если $m \leq n-3$, то тогда без потери общности можно предположить, что f является m-устойчивой, но не $(m+1)$-устойчивой (в противном случае мы будем доказывать более строгое неравенство $nl(f) \leq 2^{n-1} - 2^{m+2}$). Тогда f имеет подфункцию от $n-m-1$ переменных $f^{\sigma_{i_1},\ldots,\sigma_{i_{m+1}}}_{x_{i_1},\ldots,x_{i_{m+1}}}$, такую что $wt\left(f^{\sigma_{i_1},\ldots,\sigma_{i_{m+1}}}_{x_{i_1},\ldots,x_{i_{m+1}}}\right) = h \neq 2^{n-m-2}$. Можно принять, что $h < 2^{n-m-2}$, потому что

$$wt(f) = \sum_{(\delta_{i_1},\ldots,\delta_{i_{m+1}})} wt\left(f^{\delta_{i_1},\ldots,\delta_{i_{m+1}}}_{x_{i_1},\ldots,x_{i_{m+1}}}\right) 2^{n-1},$$

где сумма берется по всем двоичным наборам $\delta = (\delta_{i_1}, \ldots, \delta_{i_{m+1}})$ длины $m+1$, и если эта сумма содержит слагаемое, большее чем 2^{n-m-2}, то эта сумма содержит также и слагаемое, меньшее чем 2^{n-m-2}.

Рассмотрим функцию $f^{\delta_{i_1},\ldots,\delta_{i_{m+1}}}_{x_{i_1},\ldots,x_{i_{m+1}}}$, где наборы $\sigma = (\sigma_{i_1}, \ldots, \sigma_{i_{m+1}})$ и $\delta = (\delta_{i_1}, \ldots, \delta_{i_{m+1}})$ различаются только в одной j-й компоненте. Тогда

$$wt\left(f^{\sigma_{i_1},\ldots,\sigma_{i_{j-1}},\sigma_{i_j},\sigma_{i_{j+1}},\ldots,\sigma_{i_{m+1}}}_{x_{i_1},\ldots,x_{i_{j-1}},x_{i_j},x_{i_{j+1}},\ldots,x_{i_{m+1}}}\right) + wt\left(f^{\delta_{i_1},\ldots,\delta_{i_{j-1}},\delta_{i_j},\delta_{i_{j+1}},\ldots,\delta_{i_{m+1}}}_{x_{i_1},\ldots,x_{i_{j-1}},x_{i_j},x_{i_{j+1}},\ldots,x_{i_{m+1}}}\right) =$$
$$wt\left(f^{\sigma_{i_1},\ldots,\sigma_{i_{j-1}},\sigma_{i_{j+1}},\ldots,\sigma_{i_{m+1}}}_{x_{i_1},\ldots,x_{i_{j-1}},x_{i_{j+1}},\ldots,x_{i_{m+1}}}\right) = 2^{n-m-1},$$

потому что функция f является m-устойчивой. Поэтому,

$$wt\left(f^{\delta_{i_1},\ldots,\delta_{i_{j-1}},\delta_{i_j},\delta_{i_{j+1}},\ldots,\delta_{i_{m+1}}}_{x_{i_1},\ldots,x_{i_{j-1}},x_{i_j},x_{i_{j+1}},\ldots,x_{i_{m+1}}}\right) = 2^{n-m-1} - h.$$

Рассуждая подобным образом, получаем, что

$$wt\left(f^{\delta_{i_1},\ldots,\delta_{i_{j-1}},\delta_{i_j},\delta_{i_{j+1}},\ldots,\delta_{i_{m+1}}}_{x_{i_1},\ldots,x_{i_{j-1}},x_{i_j},x_{i_{j+1}},\ldots,x_{i_{m+1}}}\right) = \begin{cases} h, & \text{если } d(\sigma,\delta) \text{ четно}, \\ 2^{n-m-1} - h, & \text{если } d(\sigma,\delta) \text{ нечетно}. \end{cases}$$

Рассмотрим аффинную функцию l,

$$l = \bigoplus_{j=1}^{m+1} x_{i_j} \oplus (|\sigma| \pmod 2).$$

Тогда

$$d(f,l) = \sum_{(\delta_{i_1},\ldots,\delta_{i_{m+1}})} d\left(f^{\delta_{i_1},\ldots,\delta_{i_{m+1}}}_{x_{i_1},\ldots,x_{i_{m+1}}}, \bigoplus_{j=1}^{m+1}\delta_{i_j} \oplus (|\sigma| \pmod 2)\right) =$$

$$\sum_{\substack{\delta \\ d(\sigma,\delta)\ \text{четно}}} wt\left(f^{\delta_{i_1},\ldots,\delta_{i_{m+1}}}_{x_{i_1},\ldots,x_{i_{m+1}}}\right) +$$

$$\sum_{\substack{\delta \\ d(\sigma,\delta)\ \text{нечетно}}} \left(2^{n-m-1} - wt\left(f^{\delta_{i_1},\ldots,\delta_{i_{m+1}}}_{x_{i_1},\ldots,x_{i_{m+1}}}\right)\right) = h2^m + h2^m = h2^{m+1}.$$

Поэтому,

$$nl(f) \le d(f,l) = h2^{m+1} \le (2^{n-m-2}-1)2^{m+1} = 2^{n-1} - 2^{m+1}.$$

□

Следствие 1.5. $\mathrm{nlmax}(n,m) \le 2^{n-1} - 2^{m+1}$ *при* $m \le n-2$.

Если $m \le \frac{n}{2}-2$, то неравенство (1.7) не дает нам никакой новой информации в силу хорошо известного неравенства (1.5). Однако в последующих параграфах будет показано, что неравенство (1.7) достижимо для широкого спектра больших m.

Теорема 1.3. *Пусть* $f(x_1,\ldots,x_n)$ *является* m*-устойчивой неоптимальной булевой функцией,* $m \le n-3$*. Тогда*

$$nl(f) \le 2^{n-1} - 2^{m+2}.$$

Доказательство. Как и в доказательстве теоремы 1.2 пусть $f^{\sigma_{i_1},\ldots,\sigma_{i_{m+1}}}_{x_{i_1},\ldots,x_{i_{m+1}}}$ будет подфункцией f, такой что $wt\left(f^{\sigma_{i_1},\ldots,\sigma_{i_{m+1}}}_{x_{i_1},\ldots,x_{i_{m+1}}}\right) = h < 2^{n-m-2}$. Функция f не является оптимальной. Следовательно, $\deg\left(f^{\sigma_{i_1},\ldots,\sigma_{i_{m+1}}}_{x_{i_1},\ldots,x_{i_{m+1}}}\right) \le \deg(f) \le n-m-2$. По 1.15 это дает, что h четно. Поэтому, $h \le 2^{n-m-2}-2$ и $nl(f) \le h2^{m+1} \le (2^{n-m-2}-2)2^{m+1} = 2^{n-1} - 2^{m+2}$. □

Следствие 1.6. *Неравенство (1.8) может достигаться только для оптимальных функций.*

Таким образом, неравенство (1.7) может достигаться, только если достигается и неравенство Зигенталера.

Теорема 1.3 и следствие 1.6 были доказаны нами в [159]. Заметим, что в параллельных работах [109] и [126] этот результат получен не был. Позднее в [47] (работа автора [159] в [47] процитирована) Клодом Карле была получена верхняя оценка на нелинейность m-устойчивой функции f на $\mathbf{F}_2^n$, учитывающая алгебраическую степень функции:

$$nl(f) \leq 2^{n-1} - 2^{m+1+\left\lfloor \frac{n-m-2}{\deg(f)} \right\rfloor}. \tag{1.9}$$

Теорема 1.3 является частным случаем неравенства (1.9) при $\deg(f) \leq n-m-2$.

Следствие 1.7. *Если в условиях теоремы 1.2 в формуле (1.8) достигается точное равенство, то функция f обязана быть платовидной.*

Доказательство. Пусть имеют место условия теоремы 1.2, т. е. функция $f(x_1, \ldots, x_n)$ является m-устойчивой булевой функцией, $m \leq n-2$, и пусть $nl(f) = 2^{n-1} - 2^{m+1}$. Отсюда из (1.7) вытекает, что для всех $u \in \mathbf{F}_2^n$ выполнено $|W_f(u)| \leq 2^{m+2}$.

В то же время по лемме 1.13 для всех $u \in \mathbf{F}_2^n$ выполнено $W_f(u) \equiv 0 \pmod{2^{m+2}}$. Отсюда для всех $u \in \mathbf{F}_2^n$ имеем $W_f(u) \in \{0, \pm 2^{m+2}\}$. Таким образом, заключаем, что функция f является платовидной. □

Следующее полученное автором простое следствие теоремы 1.2, касающееся регулярных функций, приведено в совместной работе [131].

Теорема 1.4. *Нелинейность любой c-регулярной функции удовлетворяет неравенству*

$$nl(f) \leq 2^{n-1} - 2^{\max\{c, n-c\}}. \tag{1.10}$$

Доказательство. Пусть $f(x_1, \ldots, x_n)$ является c-регулярной функцией. Функция $g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \oplus \bigoplus_{i=1}^{n} x_i$ принимает на любых двух соседних наборах одинаковые значения тогда и только тогда, когда f принимает на этих наборах различные значения. Поэтому функция g является $(n-c)$-регулярной. В то же время для любой аффинной функции l имеем $d(f, l) =$

$d\left(g, l \oplus \bigoplus_{i=1}^{n} x_i\right)$. Поэтому $nl(f) = nl(g)$. Следовательно, в силу 1.2 и следствия 1.4 выполнены неравенства $nl(f) \leq 2^{n-1} - 2^c$ и $nl(f) \leq 2^{n-1} - 2^{n-c}$. □

В той же совместной работе [131] приведена и другая верхняя оценка нелинейности регулярных функций, полученная Клодом Карле:

Теорема 1.5. *Нелинейность любой c-регулярной функции удовлетворяет неравенству*

$$nl(f) \leq 2^{n-1} - \frac{2^{n-1}}{\sqrt{\binom{n}{c}}}. \tag{1.11}$$

Замечание 1.1. Используя формулу Стирлинга легко видеть, что $\frac{2^{n-1}}{\sqrt{\binom{n}{c}}}$ больше $2^{\max\{c,n-c\}}$, когда c близко к $n/2$ (наименьшими значениями, когда это так, являются $n = 10$, $c = 5$), и меньше в остальных случаях.

В конце параграфа затронем вопрос о максимальной нелинейности неуравновешенных корреляционно-иммунных функций. Следующая теорема доказана автором в [159]. Этот же результат получен и в параллельных работах Саркара и Майтры [109] и Зенга и Занга [126].

Теорема 1.6. *Пусть $f(x_1, \ldots, x_n)$ — неуравновешенная корреляционно-иммунная порядка m булева функция, $m < n$. Тогда*

$$nl(f) \leq 2^{n-1} - 2^m. \tag{1.12}$$

Доказательство. Очевидно, $nl(f) = nl(f \oplus 1)$. Поэтому без ограничения общности можно допустить, что $wt(f) < 2^{n-1}$. Вес f может быть вычислен как

$$wt(f) = \sum_{(\delta_1,\ldots,\delta_m)} wt\left(f_{x_1,\ldots,x_m}^{\delta_1,\ldots,\delta_m}\right).$$

Однако вес всех функций $f_{x_1,\ldots,x_m}^{\delta_1,\ldots,\delta_m}$ один и тот же. Поэтому

$$nl(f) \leq wt(f) = 2^m wt\left(f_{x_1,\ldots,x_m}^{0,\ldots,0}\right) \leq 2^m(2^{n-m-1} - 1) = 2^{n-1} - 2^m.$$

□

Верхняя оценка (1.12) в теореме 1.6 слабее, чем соответствующая верхняя оценка (1.7) в теореме 1.2. Тем не менее, эта оценка достигается для некоторых функций.

Примеры. Если $m = n - 1$, то по неравенству Зигенталера $\deg(f) \leq 1$, поэтому $nl(f) = 0$ и оценка (1.12) достигается. Однако если $\deg(f) = 1$, то f является уравновешенной. Единственный оставшийся случай $f \equiv \text{const}$ может рассматриваться как вырожденный.

$n = 2$, $m = 0$. Возьмем $g_2(x_1, x_2) = x_1 x_2$. Заметим, что ранее мы рассматривали g_2 как (-1)-устойчивую функцию, но также g_2 может рассматриваться как неуравновешенная корреляционно-иммунная функция порядка 0. Ее нелинейность $nl(g_2) = 1$, поэтому g_2 достигает оценки (1.12).

$n = 3$, $m = 1$. Возьмем $g_3(x_1, x_2, x_3) = \bigoplus\limits_{1 \leq i < j \leq 3} x_i x_j \oplus \bigoplus\limits_{1 \leq i \leq 3} x_i \oplus 1$. Функция g_3 является неуравновешенной корреляционно-иммунной порядка 1, $nl(g_3) = 2^2 - 2^1 = 2$, поэтому g_3 достигает оценки (1.12). Заметим, что $g_2 = (g_3)^1_{x_3}$.

$n = 6$, $m = 3$. Возьмем $\Phi(x_1, x_2, x_3, x_4, x_5, x_6) \bigoplus\limits_{1 \leq i < j < k \leq 6} x_i x_j x_k \oplus x_1 x_2 \oplus x_2 x_3 \oplus x_3 x_4 \oplus x_4 x_5 \oplus x_1 x_5 \oplus \bigoplus\limits_{i=1}^{5} x_i \oplus 1$. (Функция Φ уже упоминалась нами в параграфе 1.3). Функция Φ является неуравновешенной корреляционно-иммунной порядка 3, $nl(\Phi) = 2^5 - 2^3 = 24$, таким образом, Φ достигает оценки (1.12).

$n = 5$, $m = 2$. Возьмем $g_5(x_1, x_2, x_3, x_4, x_5, x_5) = (\Phi)^{\sigma}_{x_i}$ для произвольного $i \in \{1, \ldots, 6\}$, $\sigma \in \{0, 1\}$. Очевидно, что функция g_5 является неуравновешенной корреляционно-иммунной порядка 2, непосредственно можно проверить, что $nl(g_5) = 2^4 - 2^2 = 12$, таким образом, g_5 достигает оценки (1.12).

Примеры, приведенные выше, являются единственными известными нам функциями, на которых достигается неравенство (1.12) (с точностью до перестановок переменных и линейных трансформаций). Существование функций, достигающих оценки (1.12), при $n \geq 7$ является открытым вопросом. Следующей парой значений, для которой существование таких функций возможно, является пара $n = 9$, $m = 4$.

В работе Зенга и Занга [126] было доказано, что если $m \geq 0.6n - 0.4$, то для корреляционно-иммунных порядка m булевых функций на $\mathbf{F}_2^n$ справед-

ливо неравенство $nl(f) \leq 2^{n-1} - 2^{m+1}$. Этот результат был усилен в работе студента автора Антона Ботева [3], результат включен также в состав работы [136], который доказал, что для корреляционно-иммунной порядка m булевой функции f на $\mathbf{F}_2^n$ если $m \geq \frac{1}{2}n + \frac{1}{2}\log_2 n + \frac{1}{2}\log_2\left(\frac{\pi}{2}e^{8/9}\right) - 1$, $n \geq 12$, то $nl(f) \leq 2^{n-1} - 2^{m+1}$, и если $m \geq \frac{1}{2}n + \frac{3}{2}\log_2 n + \log_2\left(\frac{1}{4} + \frac{1}{n}\right) + \frac{1}{2}\log_2\left(\frac{\pi}{2}e^{8/9}\right) - 2$, $n \geq 24$, то $nl(f) \leq 2^{n-1} - 2^{m+2}$.

1.5 О линейных и квазилинейных переменных

В этом параграфе рассматривается понятие линейных и квазилинейных переменных и устанавливаются некоторые свойства функций, обладающих такими переменными. Понятие пары квазилинейных переменных было введено автором в работах [159] и [134] для построения устойчивых функций, достигающих верхней границы нелинейности (1.7).

Напомним, что переменная x_i называется *линейной* для функции $f = f(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n)$ если $\deg(f, x_i) = 1$. Кроме того, будем говорить, что функция f зависит от переменной x_i *линейно*. Если переменная x_i является линейной для функции f, то можно представить f в виде

$$f(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n) = g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \oplus x_i.$$

Следующая лемма описывает изменения коэффициентов Уолша булевой функции при добавлении к ней линейной переменной.

Лемма 1.23. *Пусть $f(x_1, \ldots, x_n)$ — булева функция на $\mathbf{F}_2^n$, и пусть $g(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n) \oplus x_{n+1}$, $u = (u_1, \ldots, u_n)$. Тогда*
а) $W_g(u0) = 0$, $W_g(u1) = 2W_f(u)$;
б) если f является m-устойчивой, то g является $(m+1)$-устойчивой.

Доказательство. а) Обозначим $X = (x_1, \ldots, x_n)$. Имеем

$$W_g(uu_{n+1}) = \sum_{Xx_{n+1} \in \mathbf{F}_2^{n+1}} (-1)^{g(Xx_{n+1}) + <Xx_{n+1}, uu_{n+1}>} =$$

$$= \sum_{X \in \mathbf{F}_2^n} (-1)^{g(X0) + <X,u>} + (-1)^{u_{n+1}} \sum_{X \in \mathbf{F}_2^n} (-1)^{g(X1) + <X,u>} = W_f(u) - (-1)^{u_{n+1}} W_f(u),$$

откуда следует утверждение.

б) Любой набор из носителя спектра функции f имел по следствию 1.3 вес больше m и, как видим из утверждения пункта а), любой набор из носителя спектра функции g имеет единицу в $(n+1)$-й компоненте. Отсюда по следствию 1.3 функция g является $(m+1)$-устойчивой. □

Следствие 1.8. *Если функция* $(x_1, \ldots, x_n)$ *достигает равенства в оценке (1.8), то функция* $g(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n) \oplus x_{n+1}$ *тоже достигает равенства в оценке (1.8).*

Следствие 1.9. *Все наборы из спектра функции* $g(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n) \oplus x_{n+1}$ *имеют* 1 *в* $(n+1)$*-й компоненте.*

Другим эквивалентным определением линейной переменной является следующее: переменная x_i называется линейной для функции f, если $f(x') \neq f(x'')$ для любых двух наборов x' и x'', различающихся только в i-й компоненте. По аналогии с последним определением дадим новое определение пары квазилинейных переменных.

Определение 1.1. *Будем говорить, что булева функция* $f = f(x_1, \ldots, x_n)$ *зависит от пары своих переменных* (x_i, x_j) квазилинейно, *если* $f(x') \neq f(x'')$ *для любых двух наборов* x' *и* x'' *длины* n*, различающихся только в* i*-й и* j*-й компонентах. Пара* (x_i, x_j) *в этом случае называется* парой квазилинейных переменных *в* f*.*

Лемма 1.24. *Пусть* $f(x_1, \ldots, x_n)$ *— булева функция. Тогда* (x_i, x_j)*,* $i < j$*, является парой квазилинейных переменных в* f *тогда и только тогда, когда* f *может быть представлена в виде*

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n, x_i \oplus x_j) \oplus x_i. \quad (1.13)$$

Доказательство. Если f представлена в форме (1.13), то, очевидно, пара переменных (x_i, x_j) является квазилинейной для f. Предположим, что пара переменных (x_i, x_j) является квазилинейной для f. Функция f может быть записана в виде $f = g_1 x_i x_j \oplus g_2 x_i \oplus g_3 x_j \oplus g_4 = h(x_i, x_j)$, где g_k — это функция от остальных переменных. Имеем $h(0,0) \neq h(1,1)$ и $h(0,1) \neq h(1,0)$. Следовательно, $g_1 \oplus g_2 \oplus g_3 \neq 0$ и $g_3 \neq g_2$. Таким образом, $g_1 \oplus g_2 \oplus g_3 = 1$ и $g_2 \oplus g_3 = 1$, поэтому $g_1 = 0$. Кроме того, $g_2 = g_3 \oplus 1$. Поэтому $f = (g_3 \oplus 1)x_i \oplus g_3 x_j \oplus g_4 = (g_3(x_i \oplus x_j) \oplus g_4) \oplus x_i$, что и требовалось. □

Лемма 1.25. *Пусть* $f(x_1, \ldots, x_n)$ *— булева функция. Если* f *зависит от некоторой переменной* x_i *линейно, то* f *является уравновешенной.*

Доказательство. Объединим все 2^n наборов функции f в пары так, чтобы каждая пара (x', x'') содержала наборы x' и x'', различающиеся в i-й компоненте и совпадающие во всех остальных компонентах. Тогда $f(x') \neq f(x'')$. Таким образом, $wt(f) = 2^{n-1}$ и f является уравновешенной. □

Следствие 1.10. *Пусть $f(x_1, \ldots, x_n)$ — булева функция. Если f зависит от некоторых переменных x_{i_1}, x_{i_2}, …, x_{i_s} линейно, то f является $(s-1)$-устойчивой.*

Заметим, что следствие 1.10 находится в соответствии с нашим предположением, что уравновешенная функция является 0-устойчивой, а произвольная булева функция является (-1)-устойчивой. (В последнем случае $s = 0$.)

Лемма 1.26. *Пусть $f(x_1, \ldots, x_n)$ — булева функция. Если f зависит от некоторой пары переменных (x_i, x_j) квазилинейно, тогда f является уравновешенной.*

Доказательство. Объединим все 2^n наборов функции g в пары так, чтобы любая пара (x', x'') содержала наборы x' и x'', различающиеся в i-й и j-й компонентах, и совпадающие во всех остальных компонентах. Тогда $f(x') \neq f(x'')$. Таким образом, функция f является уравновешенной. □

Лемма 1.27. *Пусть $f(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n) \oplus cx_{n+1}$, где $c \in \{0, 1\}$. Тогда $nl(f) = 2nl(g)$.*

Доказательство. Нелинейность функции $f(x_1, \ldots, x_n, x_{n+1})$ равна минимуму весов функций

$$f_\alpha = \bigoplus_{i=1}^{n} \alpha_i x_i \oplus \alpha_{n+1} x_{n+1} \oplus g(x_1, \ldots, x_n) \oplus \delta$$

по множеству всех двоичных наборов $\alpha(\alpha_1, \ldots, \alpha_n, \alpha_{n+1}, \delta)$ длины $n+2$. Если $\alpha_{n+1} = 1$, то функция f_α является уравновешенной по лемме 1.25. Таким образом, в этом случае $wt(f_\alpha) = 2^n$. Если $\alpha_{n+1} = 0$, то имеем $wt(f_\alpha) = 2wt\left(g(x_1, \ldots, x_n) \bigoplus_{i=1}^{n} \alpha_i x_i \oplus \delta\right) \geq 2nl(f)$. Последнее неравенство достигается на некотором наборе α. Поэтому $nl(f) = \min\{2^n, 2nl(g)\} = 2nl(g)$. □

Лемма 1.28. *Пусть $f(x_1, \ldots, x_n)$ — булева функция, заданная на $\mathbf{F}_2^n$. Кроме того, пусть f зависит от некоторой пары переменных (x_i, x_j) квазилинейно. Тогда $nl(f) = 2nl(g)$, где g — функция, участвовавшая в представлении f в виде (1.13) в лемме 1.24.*

Доказательство. Нелинейность функции f равна минимуму весов функций

$$f_\alpha = g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n, x_i \oplus x_j) \oplus \bigoplus_{i=1}^{n} \alpha_i x_i \oplus \delta$$

по множеству всех двоичных наборов $\alpha = (\alpha_1, \alpha_n, \delta)$ длины $n+1$. Если $\alpha_i \neq \alpha_j$, то тогда по лемме 1.25 функция f_α является уравновешенной. Однако для функции, заданной на $\mathbf{F}_2^n$, нелинейность всегда меньше чем 2^{n-1}. Поэтому мы можем исключить случай $\alpha_1 \neq \alpha_2$ из нашего рассмотрения. Таким образом, предполагаем, что $\alpha_1 = \alpha_2 = \alpha$. В этом случае $f_\alpha = g'(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n, x_i \oplus x_j)$ для некоторой функции g', заданной на $\mathbf{F}_2^{n-1}$, $nl(g') = nl(g)$. Легко видеть, что $wt(f_\alpha)2wt(g') \geq 2nl(g)$, поэтому $N(g) \geq 2N(f)$. С другой стороны, для некоторого набора α вес соответствующей функции g' равен минимуму нелинейности для g. Таким образом, $nl(f) = 2nl(g)$. □

Лемма 1.29. *Пусть f_1 и f_2 — это две булевых функции на $\mathbf{F}_2^n$. Более того, существуют переменные x_i и x_j, такие что f_1 зависит от пары переменных (x_i, x_j) квазилинейно, в то время как f_2 зависит от переменных x_i и x_j линейно. Пусть l является произвольной аффинной функцией на $\mathbf{F}_2^n$. Тогда по крайней мере одна из двух функций $f_1 \oplus l$ и $f_2 \oplus l$ является уравновешенной.*

Доказательство. Пусть $l = \bigoplus_{r=1}^{n} u_r x_r \oplus u_0$, $u_r \in \{0, 1\}$, $r = 0, 1, \ldots, n$. Если $u_i = 0$ (соответственно, $u_j = 0$), тогда $f_2 \oplus l$ зависит от переменной x_i (соответственно, x_j) линейно, поэтому функция $f_2 \oplus l$ является уравновешенной. Оставшийся случай — это $u_i = u_j = 1$. Однако здесь легко видеть, что функция $f_1 \oplus l$ зависит от пары переменных (x_i, x_j) квазилинейно, поэтому $f_1 \oplus l$ является уравновешенной. □

Лемма 1.30. *Пусть* $f(x_1, \ldots, x_n)$ *— булева функция на* $\mathbf{F}_2^n$*, и пусть* $g(x_1, \ldots, x_{n-1}, x_n, x_{n+1}) = f(x_1, \ldots, x_{n-1}, x_n \oplus x_{n+1}) \oplus x_{n+1}$*,* $u = (u_1, \ldots, u_{n-1})$*. Тогда*
$W_g(uu_nu_{n+1}) = 0$*, если* $u_n = u_{n+1}$*, и* $W_g(uu_nu_{n+1}) = 2W_f(uu_n)$*, если* $u_n \neq u_{n+1}$*.*

Доказательство. Обозначим $X = (x_1, \ldots, x_n)$. Имеем

$$W_g(uu_nu_{n+1}) = \sum_{Xx_{n+1} \in \mathbf{F}_2^{n+1}} (-1)^{g(Xx_{n+1}) + <Xx_{n+1}, uu_nu_{n+1}>} =$$

$$= \sum_{X \in \mathbf{F}_2^n} (-1)^{g(X0) + <X, uu_n>} + (-1)^{u_{n+1}} \sum_{X \in \mathbf{F}_2^n} (-1)^{g(X1) + <X, uu_n>} =$$

$$W_f(uu_n) - (-1)^{u_n \oplus u_{n+1}} W_f(uu_n),$$

откуда следует утверждение. □

Следствие 1.11. *Все наборы из носителя спектра функции* $g(x_1, \ldots, x_{n-1}, x_n, x_{n+1}) = f(x_1, \ldots, x_{n-1}, x_n \oplus x_{n+1}) \oplus x_{n+1}$ *имеют в паре компонент* $(n, n+1)$ *либо комбинацию* 01*, либо комбинацию* 10*.*

Следствие 1.12. *Если функция* $(x_1, \ldots, x_n)$ *достигает равенства в оценке (1.8) и является* m*-устойчивой, а функция* $g(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_{n-1}, x_n \oplus x_{n+1}) \oplus x_{n+1}$ *является* $(m+1)$*-устойчивой, то функция* g *тоже достигает равенства в оценке (1.8).*

Заметим, что преобразование одной из переменных в пару квазилинейных, вообще говоря, не гарантирует роста устойчивости функции. Однако в следующих параграфах будут представлены рекурсивные конструкции, при использовании которых преобразование одной из только что добавленных переменных в пару квазилинейных переменных приводит к росту устойчивости.

2 Методы построения устойчивых функций, достигающих верхней границы нелинейности

Эта глава занимает в диссертации центральное место и посвящена конструкциям m-устойчивых булевых функций от n переменных, нелинейность которых достигает верхней границы $2^{n-1}-2^{m+1}$, установленной в предыдущей главе. До того, как была установлена оценка (1.8), такие функции специально не изучались, однако изучение существовавших конструкций показывает, что они позволяли построить функции, нелинейность которых достигает оценки (1.8), лишь для m не меньше, чем примерно $n-\log_2 n$. На протяжении главы излагаются последовательно улучшающиеся автором методы, позволяющие построить m-устойчивые функции для все большего диапазона параметров. Несмотря на последовательное улучшение методов, результаты более ранних параграфов не вкладываются полностью в последующие результаты, поскольку последующие результаты приобретают все более асимптотический характер.

2.1 Метод построения устойчивых функций, достигающих верхней границы нелинейности

Теорема 1.2 показывает, что нелинейность m-устойчивой булевой функции, заданной на $\mathbf{F}_2^n$, не может превосходить $2^{n-1}-2^{m+1}$. Ранее в статьях [111], [52], [83], [108] развивались методы построения m-устойчивых булевых функций от n переменных с высокой нелинейностью, и, в частности, нелинейность $2^{n-1}-2^{m+1}$ в этих четырех статьях может быть достигнута при $m+3\geq 2^{n-m-2}$. Методы, предложенные в этих статьях, достаточно различны, однако в части спектра, заданной неравенством $m+3\geq 2^{n-m-2}$, они дают фактически одну и ту же

конструкцию. Соединение этих результатов с нашей верхней оценкой (1.7) из теоремы 1.2 доказывает, что $\mathrm{nlmax}(n,m) = 2^{n-1} - 2^{m+1}$ при $m+3 \geq 2^{n-m-2}$. В этом параграфе будет приведен более сильный результат, содержащийся в работах автора [159] и [134], а именно, будет доказано, что $\mathrm{nlmax}(n,m) = 2^{n-1} - 2^{m+1}$ при $\frac{2n-7}{3} \leq m \leq n-2$. Таким образом, m-устойчивые функции на $\mathbf{F}_2^n$ с максимально возможной нелинейностью $2^{n-1} - 2^{m+1}$ были впервые построены для ненулевой меры пар (n,m).

Лемма 2.1. *Пусть n — натуральное число. Пусть $f_1(x_1,\ldots,x_n)$ и $f_2(y_1,\ldots,y_n)$ — это m-устойчивые булевы функции, заданные на $\mathbf{F}_2^n$, причем $nl(f_1) \geq N_0$, $nl(f_2) \geq N_0$. Более того, существуют две переменные x_i и x_j, такие что f_1 зависит от переменных x_i и x_j линейно, а f_2 зависит от пары переменных (x_i,x_j) квазилинейно. Тогда функция*

$$f_1'(x_1,\ldots,x_n,x_{n+1}) = (x_{n+1}\oplus 1)f_1(x_1,\ldots,x_n) \oplus x_{n+1}f_2(x_1,\ldots,x_n) \tag{2.1}$$

является m-устойчивой функцией на $\mathbf{F}_2^{n+1}$ с нелинейностью $nl(f_1') \geq 2^{n-1} + N_0$, и функция

$$\begin{gathered} f_2'(x_1,\ldots,x_n,x_{n+1},x_{n+2}) = (x_{n+1}\oplus x_{n+2}\oplus 1)f_1(x_1,\ldots,x_n)\oplus \\ (x_{n+1}\oplus x_{n+2})f_2(x_1,\ldots,x_n)\oplus x_{n+1} \end{gathered} \tag{2.2}$$

является $(m+1)$-устойчивой булевой функцией на $\mathbf{F}_2^{n+2}$ с нелинейностью $nl(f_2') \geq 2^n + 2N_0$. Более того, f_2' зависит от пары переменных (x_{n+1},x_{n+2}) квазилинейно.

Доказательство. Во первых, рассмотрим выражение (2.1). Обе подфункции $(f_1')^0_{x_{n+1}} = f_1(x_1,\ldots,x_n)$ и $(f_1')^1_{x_{n+1}} = f_2(x_1,\ldots,x_n)$ являются m-устойчивыми, следовательно по лемме 1.16 функция f_1' также является m-устойчивой. Пусть $l = \bigoplus_{i=1}^{n+1} c_i x_i \oplus c_0$ — это произвольная аффинная функция, заданная на $\mathbf{F}_2^{n+1}$. Тогда $d(f_1',l) = d(f_1,l^0_{x_{n+1}}) + d(f_2,l^1_{x_{n+1}}) = wt(f_1\oplus l^0_{x_{n+1}}) + wt(f_2\oplus l^1_{x_{n+1}})$. Мы утверждаем, что по крайней мере одна из двух функций $f_1\oplus l^0_{x_{n+1}}$ и $f_2\oplus l^1_{x_{n+1}}$ является уравновешенной. Действительно, если $c_i = 0$ или $c_j = 0$, то тогда функция $f_1\oplus l^0_{x_{n+1}}$ зависит от x_i или x_j линейно, следовательно, по лемме 1.25 функция $f_1\oplus l^0_{x_{n+1}}$ является уравновешенной. В оставшемся случае $c_i = 1$ и

$c_j = 1$ легко видеть из представления (1.13), что функция $f_2 \oplus l^1_{x_{n+1}}$ зависит от пары переменных (x_i, x_j) квазилинейно, поэтому по лемме 1.26 функция $f_2 \oplus l^1_{x_{n+1}}$ является уравновешенной. Таким образом, $d(f_1', l) \geq 2^{n-1} + N_0$. Аффинная функция l была выбрана произвольно, поэтому, $nl(f_1') \geq 2^{n-1} + N_0$.

Далее, рассмотрим выражение (2.2). Из конструкции (2.2) и представления (1.13) видим, что f_2' зависит от пары переменных (x_{n+1}, x_{n+2}) квазилинейно. Теперь хотим доказать, что функция f_2' является $(m+1)$-устойчивой. Заменим произвольные $m+1$ переменных константами, порождая подфункцию $\hat{f}$. Если обе переменные x_{n+1} и x_{n+2} являются свободными в $\hat{f}$, тогда $\hat{f}$ зависит от пары (x_{n+1}, x_{n+2}) квазилинейно, поэтому по лемме 1.26 функция $\hat{f}$ является уравновешенной. Если хотя бы одна из двух переменных x_{n+1} и x_{n+2} была заменена константой, то константами было бы заменено не более m из первых n переменных $x_1, \ldots, x_n$. Однако функции $\hat{f}^{0\ 0}_{x_{n+1},x_{n+2}} = f_1$, $\hat{f}^{0\ 1}_{x_{n+1},x_{n+2}} = f_2$, $\hat{f}^{1\ 0}_{x_{n+1},x_{n+2}} = f_2 \oplus 1$, $\hat{f}^{1\ 1}_{x_{n+1},x_{n+2}} = f_1 \oplus 1$ являются m-устойчивыми, следовательно, по лемме 1.16 функция $\hat{f}$ является уравновешенной. Подфункция $\hat{f}$ была выбрана произвольно, поэтому функция f_2' является $(m+1)$-устойчивой.

Наконец, нам нужно доказать нижнюю оценку для нелинейности функции f_2'. Пусть $l = \bigoplus_{i=1}^{n+2} c_i x_i \oplus c_0$ — это произвольная аффинная функция на $\mathbf{F}_2^{n+2}$. Тогда $d(f_2', l) = d(f_1, l^{0\ 0}_{x_{n+1},x_{n+2}}) + d(f_2, l^{0\ 1}_{x_{n+1},x_{n+2}}) + d(f_2 \oplus 1, l^{1\ 0}_{x_{n+1},x_{n+2}}) + d(f_1 \oplus 1, l^{1\ 1}_{x_{n+1},x_{n+2}}) = wt(f_1 \oplus l^{0\ 0}_{x_{n+1},x_{n+2}}) + wt(f_2 \oplus l^{0\ 1}_{x_{n+1},x_{n+2}}) + wt(f_2 \oplus l^{1\ 0}_{x_{n+1},x_{n+2}} \oplus 1) + wt(f_1 \oplus l^{1\ 1}_{x_{n+1},x_{n+2}} \oplus 1)$. По той же самой причине, что и выше, по крайней мере одна из двух функций $f_1 \oplus l^{0\ 0}_{x_{n+1},x_{n+2}}$ и $f_2 \oplus l^{0\ 1}_{x_{n+1},x_{n+2}}$ является уравновешенной, и по крайней мере одна из двух функций $f_2 \oplus l^{1\ 0}_{x_{n+1},x_{n+2}} \oplus 1$ и $f_1 \oplus l^{1\ 1}_{x_{n+1},x_{n+2}} \oplus 1$ является уравновешенной. Таким образом, $d(f_2', l) \geq 2^n + 2N_0$. Аффинная функция l была выбрана произвольно, поэтому $nl(f_2') \geq 2^n + 2N_0$. □

Лемма 2.2. *Предположим, что существуют m-устойчивая булева функция $f_{n,1}$ на $\mathbf{F}_2^n$, $nl(f_{n,1}) \geq N_0$, и $(m+1)$-устойчивая булева функция $f_{n+1,2}$ на $\mathbf{F}_2^{n+1}$, $nl(f_{n+1,2}) \geq 2N_0$, кроме того функция $f_{n+1,2}$ зависит от некоторой пары своих переменных (x_i, x_j) квазилинейно. Тогда существуют $(m+2)$-устойчивая булева функция $f_{n+3,1}$ на $\mathbf{F}_2^{n+3}$, $nl(f_{n+3,1}) \geq 2^{n+1} + 4N_0$, и $(m+3)$-устойчивая булева функция $f_{n+4,2}$ на $\mathbf{F}_2^{n+4}$, $nl(f_{n+4,2}) \geq 2^{n+2} + 8N_0$, кроме того функция*

$f_{n+4,2}$ *зависит от некоторой пары своих переменных квазилинейно.*

Доказательство. Можно положить, что $i < j$. Обозначим

$$f_1(x_1, \ldots, x_{n+2}) = f_{n,1}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_{n+2}) \oplus x_i \oplus x_j,$$

$$f_2(x_1, \ldots, x_{n+2}) = f_{n+1,2}(x_1, \ldots, x_{n+1}) \oplus x_{n+2}.$$

По леммам 1.25 и 1.27 функции f_1 и f_2 являются $(m+2)$-устойчивыми функциями на $\mathbf{F}_2^{n+2}$, $nl(f_1) \geq 4N_0$, $nl(f_2) \geq 4N_0$. Более того, f_1 зависит от переменных x_i и x_j линейно, и f_2 зависит от пары переменных (x_i, x_j) квазилинейно. Подставляя f_1 и f_2 в (2.1) и (2.2) (мы сдвигаем $n \to n+2$), имеем

$$f_1'(x_1, \ldots, x_{n+2}, x_{n+3}) = (x_{n+3} \oplus 1) f_1(x_1, \ldots, x_{n+2}) \oplus x_{n+3} f_2(x_1, \ldots, x_{n+2})$$

и

$$f_2'(x_1, \ldots, x_{n+2}, x_{n+3}, x_{n+4}) = (x_{n+3} \oplus x_{n+4} \oplus 1) f_1(x_1, \ldots, x_{n+2}) \oplus$$
$$(x_{n+3} \oplus x_{n+4}) f_2(x_1, \ldots, x_{n+2}) \oplus x_{n+3}.$$

По лемме 2.1 мы построили $(m+2)$-устойчивую булеву функцию $f_{n+3,1} = f_1'$ на $\mathbf{F}_2^{n+3}$, $nl(f_{n+3,1}) \geq 2^{n+1} + 4N_0$, и $(m+3)$-устойчивую булеву функцию $f_{n+4,2} = f_2'$ на $\mathbf{F}_2^{n+4}$, $nl(f_{n+4,2}) \geq 2^{n+2} + 8N_0$, кроме того функция $f_{n+4,2}$ зависит от пары переменных (x_{n+3}, x_{n+4}) квазилинейно. □

Следствие 2.1. *Предположим, что при* $m \leq n-2$ *существует* m*-устойчивая булева функция* $f_{n,1}$ *на* $\mathbf{F}_2^n$, $nl(f_{n,1}) = 2^{n-1} - 2^{m+1}$, *и* $(m+1)$*-устойчивая булева функция* $f_{n+1,2}$ *на* $\mathbf{F}_2^{n+1}$, $nl(f_{n+1,2}) = 2^n - 2^{m+2}$, *кроме того, функция* $f_{n+1,2}$ *зависит от некоторой пары своих переменных* (x_i, x_j) *квазилинейно. Тогда существует* $(m+2)$*-устойчивая булева функция* $f_{n+3,1}$ *на* $\mathbf{F}_2^{n+3}$, $nl(f_{n+3,1}) = 2^{n+2} - 2^{m+3}$, *и* $(m+3)$*-устойчивая булева функция* $f_{n+4,2}$ *на* $\mathbf{F}_2^{n+4}$, $nl(f_{n+4,2}) = 2^{n+3} - 2^{m+4}$, *кроме того, функция* $f_{n+4,2}$ *зависит от некоторой пары своих переменных квазилинейно.*

Доказательство. Предположение следствия 2.1 является предположением леммы 2.2 для $N_0 = 2^{n-1} - 2^{m+1}$. По лемме 2.2 можно построить функции $f_{n+3,1}$ и f_{n+4} с требуемыми свойствами и нелинейностями $nl(f_{n+3,1}) \geq 2^{n+1} + 4N_0 =$

$2^{n+2}-2^{m+3}$, $nl(f_{n+4,2}) \geq 2^{n+2}+8N_0 = 2^{n+3}-2^{m+4}$, соответственно. По теореме 1.2 правые части двух последних неравенств являются также верхними оценками. Поэтому, имеем точные равенства $nl(f_{n+3,1}) = 2^{n+2} - 2^{m+3}$, $nl(f_{n+4,2}) = 2^{n+3} - 2^{m+4}$. □

Теорема 2.1. $\mathrm{nlmax}(n, m) = 2^{n-1} - 2^{m+1}$ *при* $\frac{2n-7}{3} \leq m \leq n-2$.

Доказательство. Если $m = n-2$, то по неравенству Зигенталера любая $(m-2)$-устойчивая функция, заданная на $\mathbf{F}_2^n$, является аффинной. Таким образом, $\mathrm{nlmax}(n, n-2) = 0$. Далее, положим $f_{2,1} = x_1x_2$, $f_{3,2} = x_1(x_2 \oplus x_3) \oplus x_2$. Эти функции удовлетворяют предположению следствия 2.1 при $n = 2$, $m = -1$. По следствию 2.1 мы можем построить функции $f_{5,1}$ и $f_{6,2}$, такие что функция $f_{5,1}$ является 1-устойчивой булевой функцией на $\mathbf{F}_2^5$, $nl(f_{5,1}) = 2^4-2^2$, а функция $f_{6,2}$ является 2-устойчивой булевой функцией на $\mathbf{F}_2^6$, $nl(f_{6,2}) = 2^5 - 2^3$, кроме того $f_{6,2}$ зависит от пары переменных (x_5, x_6) квазилинейно. Подставим функции $f_{5,1}$ и $f_{6,2}$ в предположение следствия 2.1, и так далее. Действуя таким образом, для любого целого k, $k \geq 3$, мы построим m-устойчивую булеву функцию $f_{n,1}$ на $\mathbf{F}_2^n$ с нелинейностью $2^{n-1}-2^{m+1}$, где $n = 3k-7$, $m = 2k-7$. Пусть $\frac{2n-7}{3} \leq m \leq n-3$. Положим

$$f(x_1, \ldots, x_n) = f_{3(n-m)-7,1}(x_1, \ldots, x_{3(n-m)-7}) \oplus \bigoplus_{i=3(n-m)-6}^{n} x_i.$$

По предположению теоремы 2.1 мы имеем $3(n-m)-7 \leq n$. Устойчивость функции f равна $(2(n-m)-7) + (n-(3(n-m)-7)) = m$, нелинейность функции f равна $2^{n-(3(n-m)-7)}\left(2^{(3(n-m)-7)-1} - 2^{(2(n-m)-7)+1}\right) = 2^{n-1} - 2^{m+1}$. Таким образом, при $\frac{2n-7}{3} \leq m \leq n-2$ построена m-устойчивая булева функция на $\mathbf{F}_2^n$ с нелинейностью $2^{n-1} - 2^{m+1}$. Принимая во внимание верхнюю оценку (1.7) из теоремы 1.2, полностью завершаем доказательство. □

Заметим, что недавняя гипотеза $\mathrm{nlmax}(n, n-4) = 2^{n-1} - 2^{n-3}$ (при $n \geq 5$) в [90] есть частный случай нашей теоремы 2.1.

Примеры. Уже было отмечено, что мы берем $f_{2,1} = x_1x_2$, $f_{3,2} = x_1(x_2 \oplus x_3) \oplus x_2 = x_1x_2 \oplus x_1x_3 \oplus x_2$. Далее, $f_{5,1} = (x_5 \oplus 1)(x_1x_4 \oplus x_2 \oplus x_3) \oplus x_5(x_1x_2 \oplus x_1x_3 \oplus x_2 \oplus x_4) = x_1x_2x_5 \oplus x_1x_3x_5 \oplus x_1x_4x_5 \oplus x_1x_4 \oplus x_3x_5 \oplus x_4x_5 \oplus x_2 \oplus x_3$,

$f_{6,2} = (x_5 \oplus x_6 \oplus 1)(x_1x_4 \oplus x_2 \oplus x_3) \oplus (x_5 \oplus x_6)(x_1x_2 \oplus x_1x_3 \oplus x_2 \oplus x_4) \oplus x_5 = x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6 \oplus x_2 \oplus x_3 \oplus x_5$.

На следующем шаге имеем $f_{8,1} = (x_8 \oplus 1)(x_1x_2x_7 \oplus x_1x_3x_7 \oplus x_1x_4x_7 \oplus x_1x_4 \oplus x_3x_7 \oplus x_4x_7 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6) \oplus x_8(x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_7) = x_1x_2x_5x_8 \oplus x_1x_2x_6x_8 \oplus x_1x_2x_7x_8 \oplus x_1x_3x_5x_8 \oplus x_1x_3x_6x_8 \oplus x_1x_3x_7x_8 \oplus x_1x_4x_5x_8 \oplus x_1x_4x_6x_8 \oplus x_1x_4x_7x_8 \oplus x_1x_2x_7 \oplus x_1x_3x_7 \oplus x_1x_4x_7 \oplus x_3x_5x_8 \oplus x_3x_6x_8 \oplus x_3x_7x_8 \oplus x_4x_5x_8 \oplus x_4x_6x_8 \oplus x_4x_7x_8 \oplus x_1x_4 \oplus x_3x_7 \oplus x_4x_7 \oplus x_6x_8 \oplus x_7x_8 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6$.

Функция $f_{8,1}$ является 3-устойчивой функцией от 8 переменных с нелинейностью 112. Заметим, что до работ [159] и [134] максимальное известное значение нелинейности 3-устойчивой функции на $\mathbf{F}_2^8$ было равно 96 [52],[108],[90].

Построение в качестве примера 29-устойчивых булевых функций на $\mathbf{F}_2^{50}$ с как можно большей нелинейностью в течение какого-то времени было достаточно популярно в литературе. Заметим, что метод в [52] позволяет строить 29-устойчивые булевы функции на $\mathbf{F}_2^{50}$ с нелинейностью $2^{49} - 2^{34}$ и алгебраической степенью 16. В [83] и [108] изучались оптимальные функции, т. е. функции, на которых достигается неравенство Зигенталера. В [83] была построена 29-устойчивая булева функция на $\mathbf{F}_2^{50}$ с алгебраической степенью 20 и нелинейностью $2^{49} - 2^{39} - 2^{30}$, и в [83] была построена такая функция с нелинейностью $2^{49} - 2^{37} - 2^{30}$. Заметим, что при помощи метода, развитого в этом параграфе, можно построить функцию $f_{50,1}$. Эта функция является 31-устойчивой функцией на $\mathbf{F}_2^{50}$ с алгебраической степенью 18 и нелинейностью $2^{49} - 2^{32}$ (мы доказали, что эта нелинейность является максимально возможной). Конечно, эту функцию можно также рассматривать и как 29-устойчивой (в любом случае, функция $f_{50,1} \oplus x_1 \oplus x_2$ является 29-устойчивой в силу спектральных свойств корреляционно-иммунных функций, см. [68]). Если нужны оптимальные функции, то можно взять функцию $f_{47,1}$. Эта функция является 29-устойчивой функцией на $\mathbf{F}_2^{47}$ с алгебраической степенью 17 и нелинейностью $2^{46} - 2^{30}$. Положим $f(x_1, \ldots, x_{50}) = \bigoplus_{(\sigma_{48},\sigma_{49},\sigma_{50})} (x_{48} \oplus \sigma_{48})(x_{49} \oplus \sigma_{49})(x_{50} \oplus \sigma_{50}) f_{47,1}^{\sigma_{48},\sigma_{49},\sigma_{50}}(x_1, \ldots, x_{47})$, где $f_{47,1}^{\sigma_{48},\sigma_{49},\sigma_{50}}(x_1, \ldots, x_{47})$ — это функции, полученные из $f_{47,1}(x_1, \ldots, x_{47})$ некоторы-

ми перестановками переменных. Легко обеспечить, чтобы алгебраическая степень f была равна 20 (например, если некоторое слагаемое длины 17 будет содержаться в полиноме только одной из восьми функций $f_{47,1}^{\sigma_{48},\sigma_{49},\sigma_{50}}(x_1,\ldots,x_{47})$). Таким образом, построенная функция f является 29-устойчивой оптимальной булевой функцией на $\mathbf{F}_2^{50}$ с нелинейностью не менее $8(2^{46}-2^{30}) = 2^{49}-2^{33}$. Видим, что рассматриваемый метод позволил строить функции с лучшими параметрами, чем в предшествовавших работах [52],[108],[90]. Заметим, что усовершенствованный метод построения, развитый автором в параграфе 2.5 и работах [162] и [137], позволил построить 29-устойчивую функцию на $\mathbf{F}_2^{50}$ с максимально возможной нелинейностью $2^{49}-2^{30}$.

2.2 Оптимизация неравенства Зигенталера для каждой отдельной переменной

Некоторым недостатком конструкции, приведенной в доказательстве теоремы 2.1, является то, что при $\frac{2n-7}{3} < m$ построенная функция зависит от некоторых переменных линейно. Заметим, что функции с нелинейностью $2^{n-1} - 2^{m+1}$, построенные в [111], [52], [83], [108] (при $m + 3 \geq 2^{n-m-2}$), зависят нелинейно от всех своих переменных только в некоторых случаях, когда $m + 3 = 2^{n-m-2}$ или $m + 2 = 2^{n-m-2}$. В целом,эти функции зависят нелинейно от $2^{n-m-2} + n - m - 4$ или $2^{n-m-2} + n - m - 3$ переменных. В этом параграфе при $\frac{2n-7}{3} \leq m \leq n - \log_2 \frac{n+2}{3} - 2$ предлагается метод построения m-устойчивой булевой функции на $\mathbf{F}_2^n$, которая достигает неравенства Зигенталера по каждой своей переменной (т. е. $\deg(f, x_i) = n - m - 1$ для всех переменных x_i). Одновременно дается более общий метод построения по сравнению с тем, который был дан в предыдущем параграфе. Результаты параграфа содержатся в работах автора [159] и [134].

Будем говорить, что переменная x_i является *покрывающей* для функции f, если каждая другая переменная функции f содержится вместе с x_i в некотором слагаемом максимальной длины в полиноме f. Будем говорить, что пара переменных (x_i, x_j) является *покрывающей* для функции f, если каждая другая переменная функции f содержится вместе с x_i в некотором слагаемом максимальной длины в полиноме f (и соответственно вместе с x_j в некотором слагаемом максимальной длины в полиноме f).

Лемма 2.3. *Для целых k и n, удовлетворяющих неравенствам $k \geq 3$, $3k - 7 \leq n < 3 \cdot 2^{k-2} - 2$, существует булева функция $f_{n,1}^k$ на $\mathbf{F}_2^n$, для которой выполняются следующие свойства:*

(1 i) $f_{n,1}^k$ является $(n-k)$-устойчивой;

(1 ii) $nl(f_{n,1}^k) = 2^{n-1} - 2^{n-k+1}$;

(1 iii) $\deg(f_{n,1}^k, x_i) = k - 1$ для каждой переменной x_i;

(1 iv) $f_{n,1}^k$ имеет покрывающую переменную.

Для целых k и n, удовлетворяющих неравенствам $k \geq 3$, $3k - 7 < n \leq$

$3 \cdot 2^{k-2} - 2$, *существует булева функция* $f^k_{n,2}$ *на* $\mathbf{F}_2^n$, *для которой выполняются следующие свойства:*

(2 i) $f^k_{n,2}$ *является* $(n-k)$*-устойчивой;*

(2 ii) $nl(f^k_{n,2}) = 2^{n-1} - 2^{n-k+1}$*;*

(2 iii) $\deg(f^k_{n,2}, x_i) = k-1$ *для каждой переменной* x_i*;*

(2 iv) $f^k_{n,2}$ *имеет квазилинейную пару покрывающих переменных.*

Доказательство. Будем проводить доказательство индукцией по k. При $k = 3$ можно положить $f^3_{2,1} = x_1x_2$, $f^3_{3,1} = f^3_{3,2} = x_1(x_2 \oplus x_3) \oplus x_2$, $f^3_{4,2} = (x_1 \oplus x_2)(x_3 \oplus x_4) \oplus x_1 \oplus x_3$. Легко проверить, что эти функции удовлетворяют всем требуемым условиям.

Предположим, что утверждение справедливо для k. Будем доказывать его для $k+1$. Будем искать функции $f^{k+1}_{n,1}$ и $f^{k+1}_{n,2}$ в виде

$$\begin{gathered} f^{k+1}_{n,1} = (x_n \oplus 1)\left(f^k_{n_1}(x_1, \ldots, x_{n_1}) \oplus \bigoplus_{i=n_1+1}^{n-1} x_i\right) \\ \oplus x_n\left(\bigoplus_{i=1}^{n-1-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2}, \ldots, x_{n-1})\right), \\ n_1 + n_2 \geq n-1, \quad n_1 \leq n-3, \quad n_2 \leq n-2, \end{gathered} \tag{2.3}$$

и

$$\begin{gathered} f^{k+1}_{n,2} = (x_{n-1} \oplus x_n \oplus 1)\left(f^k_{n_1}(x_1, \ldots, x_{n_1}) \oplus \bigoplus_{i=n_1+1}^{n-2} x_i\right) \\ \oplus (x_{n-1} \oplus x_n)\left(\bigoplus_{i=1}^{n-2-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2-1}, \ldots, x_{n-2})\right) \oplus x_{n-1}, \\ n_1 + n_2 \geq n-2, \quad n_1 \leq n-4, \quad n_2 \leq n-3, \end{gathered} \tag{2.4}$$

где $f^k_{n_1}(x_1, \ldots, x_{n_1})$ — это $f^k_{n_1,1}(x_1, \ldots, x_{n_1})$ или $f^k_{n_1,2}(x_1, \ldots, x_{n_1})$ (если $f^k_{n_1} = f^k_{n_1,2}$, то $n_2 \neq n-2$ в (2.3) и $n_2 \neq n-3$ в (2.4)). Кроме того, предполагаем, что покрывающей переменной в $f^k_{n_1}$ является x_1 (или квазилинейной парой покрывающих переменных в $f^k_{n_1,2}$ является (x_1, x_2)), и предполагаем, что квазилинейными парами покрывающих переменных в $f^k_{n_2,2}$ являются (x_{n-2}, x_{n-1}) в (2.3) или (x_{n-3}, x_{n-2}) в (2.4).

Функции $f^{k+1}_{n,1}$ и $f^{k+1}_{n,2}$ удовлетворяют всем требуемым свойствам. Действительно:

(1 i) Устойчивость функции $f^k_{n_1}(x_1,\dots,x_{n_1}) \oplus \bigoplus\limits_{i=n_1+1}^{n-1} x_i$ равна $(n_1-k)+(n-1-n_1)=n-k-1$, устойчивость функции $\bigoplus\limits_{i=1}^{n-1-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2},\dots,x_{n-1})$ равна $n-1-n_2+(n_2-k)=n-k-1$. Таким образом, по лемме 2.1 устойчивость функции $f^{k+1}_{n,1}$ равна $n-(k+1)$.

(2 i) Устойчивость функции $f^k_{n_1}(x_1,\dots,x_{n_1}) \oplus \bigoplus\limits_{i=n_1+1}^{n-2} x_i$ равна $(n_1-k)+(n-2-n_1)=n-k-2$, устойчивость функции $\bigoplus\limits_{i=1}^{n-2-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2-1},\dots,x_{n-2})$ равна $n-2-n_2+(n_2-k)=n-k-2$. Таким образом, по лемме 2.1 устойчивость функции $f^{k+1}_{n,1}$ равна $n-(k+1)$.

(1 ii) Нелинейность функции $f^k_{n_1}(x_1,\dots,x_{n_1}) \oplus \bigoplus\limits_{i=n_1+1}^{n-1} x_i$ равна

$$(2^{n_1-1}-2^{n_1-k+1})\cdot 2^{n-1-n_1}=2^{n-2}-2^{n-k},$$

нелинейность функции $\bigoplus\limits_{i=1}^{n-1-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2},\dots,x_{n-1})$ равна

$$2^{n-1-n_2}(2^{n_2-1}-2^{n_2-k+1})=2^{n-2}-2^{n-k}.$$

Функция $f^k_{n_1}(x_1,\dots,x_{n_1}) \oplus \bigoplus\limits_{i=n_1+1}^{n-1} x_i$ зависит от переменных x_{n-2} и x_{n-1} линейно, в то время как функция $\bigoplus\limits_{i=1}^{n-1-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2},\dots,x_{n-1})$ зависит от пары переменных (x_{n-2},x_{n-1}) квазилинейно. Таким образом, по лемме 2.1 нелинейность функции $f^{k+1}_{n,1}$ равна $2^{n-2}+(2^{n-2}-2^{n-k})=2^{n-1}-2^{n-(k+1)+1}$.

(2 ii) Нелинейность функции $f^k_{n_1}(x_1,\dots,x_{n_1}) \oplus \bigoplus\limits_{i=n_1+1}^{n-2} x_i$ равна

$$(2^{n_1-1}-2^{n_1-k+1})\cdot 2^{n-2-n_1}=2^{n-3}-2^{n-k-1},$$

нелинейность функции $\bigoplus\limits_{i=1}^{n-2-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2-1},\dots,x_{n-2})$ равна

$$2^{n-2-n_2}(2^{n_2-1}-2^{n_2-k+1})=2^{n-3}-2^{n-k-1}.$$

Функция $f^k_{n_1}(x_1,\dots,x_{n_1}) \oplus \bigoplus\limits_{i=n_1+1}^{n-2} x_i$ зависит от переменных x_{n-3} и x_{n-2} линейно, в то время как функция $\bigoplus\limits_{i=1}^{n-1-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2},\dots,x_{n-1})$ зависит от пары пере-

менных (x_{n-3}, x_{n-2}) квазилинейно. Таким образом, по лемме 2.1 нелинейность функции $f^{k+1}_{n,2}$ равна $2^{n-2} + 2(2^{n-3} - 2^{n-k-1}) = 2^{n-1} - 2^{n-(k+1)+1}$.

(1 iii), (1 iv) Каждая переменная из множества $\{x_2, x_3, \ldots, x_{n_1}\}$ содержится вместе с x_1 в некотором слагаемом длины $k-1$ в полиноме функции $f^k_{n_1,1}(x_1, \ldots, x_{n_1})$, если $f^k_{n_1} = f^k_{n_1,1}$ или каждая переменная из множества $\{x_3, x_4, \ldots, x_{n_1}\}$ содержится вместе с x_1 в некотором слагаемом длины $k-1$ (а также вместе с x_2 в некотором слагаемом такой длины) в полиноме функции $f^k_{n_1,2}(x_1, \ldots, x_{n_1})$, если $f^k_{n_1} = f^k_{n_1,2}$. Функция $\bigoplus_{i=1}^{n-1-n_2} x_i \oplus f^k_{n_2,2}(x_{n-n_2}, \ldots, x_{n-1})$ зависит от переменной x_1 линейно (а также от переменной x_2, если $f^k_{n_1} = f^k_{n_1,2}$). Следовательно, после раскрытия скобок и приведения подобных слагаемых каждая переменная из множества $\{x_1, x_2, x_3, \ldots, x_{n_1}\}$ будет содержаться вместе с x_n в некотором слагаемом длины k в полиноме функции $f^{k+1}_{n,1}$. Аналогично, каждая переменная из множества $\{x_{n-n_2}, \ldots, x_{n-3}\}$ содержится вместе с x_{n-2} в некотором слагаемом длины $k-1$ (а также вместе с x_{n-1} в некотором слагаемом такой длины) в полиноме функции $f^k_{n_2,2}(x_{n-n_2}, \ldots, x_{n-1})$. Функция $f^k_{n_1}(x_1, \ldots, x_{n_1}) \oplus \bigoplus_{i=n_1+1}^{n-1} x_i$ зависит от переменных x_{n-2} и x_{n-1} линейно. Поэтому после раскрытия скобок и приведения подобных слагаемых каждая переменная из множества $\{x_{n-n_2}, \ldots, x_{n-1}\}$ будет содержаться вместе с x_n в некотором слагаемом длины k в полиноме функции $f^{k+1}_{n,1}$. По условию, $n_1 + n_2 \le n-1$, поэтому объединение множеств $\{x_1, x_2, x_3, \ldots, x_{n_1}\}$ и $\{x_{n-n_2}, \ldots, x_{n-1}\}$ есть множество $\{x_1, \ldots, x_{n-1}\}$. Таким образом, x_n является покрывающей переменной в $f^k_{n,1}$.

Доказательство свойств (2 iii) и (2 iv) проводится аналогично.

Наконец, заметим, что в соответствии с (2.3) можно построить функцию $f^k_{n,1}$, если $n \ge n_1 + 3 \ge (3k-7) + 3 = 3(k+1) - 7$ и если $n \le n_1 + n_2 + 1 \le 2(3 \cdot 2^{k-2} - 2) + 1 \le 3 \cdot 2^{(k+1)-2} - 3$, а в соответствии с (2.4) можно построить функцию $f^k_{n,2}$, если $n \ge n_1 + 4 \ge (3k-7) + 4 = 3(k+1) - 4$ и если $n \le n_1 + n_2 + 2 \le 2(3 \cdot 2^{k-2} - 2) + 2 \le 3 \cdot 2^{(k+1)-2} - 2$. Таким образом, индуктивный переход полностью доказан. □

Теорема 2.2. *Для целых m и n, удовлетворяющих неравенствам $\frac{2n-7}{3} \le m \le n - \log_2 \frac{n+2}{3} - 2$, существует m-устойчивая булева функция на $\mathbf{F}_2^n$ с нели-*

нейностью $2^{n-1} - 2^{m+1}$*, достигающая неравенства Зигенталера для каждой отдельной переменной.*

Доказательство. Непосредственное следствие из леммы 2.3. □

Примеры. Пусть $n = 7$, $m = 3$. Выбираем $n_1 = 3$, $n_2 = 4$, и строим в соответствии с (2.3):

$$f^4_{7,1} = (x_7 \oplus 1)\left(f^3_{3,1}(x_1, x_2, x_3)\bigoplus_{i=4}^{6} x_i\right) \oplus x_7\left(\bigoplus_{i=1}^{2} x_i \oplus f^3_{4,2}(x_3, x_4, x_5, x_6)\right) =$$
$$(x_7 \oplus 1)(x_1x_2 \oplus x_1x_3 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_6) \oplus$$
$$x_7(x_1 \oplus x_2 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6 \oplus x_3 \oplus x_5) =$$
$$x_1x_2x_7 \oplus x_1x_3x_7 \oplus x_3x_5x_7 \oplus x_3x_6x_7 \oplus x_4x_5x_7 \oplus x_4x_6x_7 \oplus$$
$$x_1x_2 \oplus x_1x_3 \oplus x_1x_7 \oplus x_3x_7 \oplus x_4x_7 \oplus x_6x_7 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_6.$$

Функция $f^4_{7,1}$ является 3-устойчивой булевой функцией на $\mathbf{F}_2^7$ с нелинейностью $2^6 - 2^4 = 48$, алгебраическая степень каждой переменной в $f^4_{7,1}$ равна 3.

Пусть $n = 10$, $m = 6$. Выбираем $n_1 = 4$, $n_2 = 4$, и строим в соответствии с (2.4):

$$f^4_{10,2} = (x_9 \oplus x_{10} \oplus 1)\left(f^3_{4,2}(x_1, x_2, x_3, x_4)\bigoplus_{i=5}^{8} x_i\right) \oplus$$
$$(x_9 \oplus x_{10})\left(\bigoplus_{i=1}^{4} x_i \oplus f^3_{4,2}(x_5, x_6, x_7, x_8)\right) \oplus x_9 =$$
$$(x_9 \oplus x_{10} \oplus 1)(x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_1 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8) \oplus$$
$$(x_9 \oplus x_{10})(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5x_7 \oplus x_5x_8 \oplus x_6x_7 \oplus x_6x_8 \oplus x_5 \oplus x_7) \oplus x_9 =$$
$$x_1x_3x_9 \oplus x_1x_3x_{10} \oplus x_1x_4x_9 \oplus x_1x_4x_{10} \oplus x_2x_3x_9 \oplus x_2x_3x_{10} \oplus x_2x_4x_9 \oplus$$
$$x_2x_4x_{10} \oplus x_5x_7x_9 \oplus x_5x_7x_{10} \oplus x_5x_8x_9 \oplus x_5x_8x_{10} \oplus x_6x_7x_9 \oplus x_6x_7x_{10} \oplus$$
$$x_6x_8x_9 \oplus x_6x_8x_{10} \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2x_9 \oplus x_2x_{10} \oplus x_4x_9 \oplus$$
$$x_4x_{10} \oplus x_6x_9 \oplus x_6x_{10} \oplus x_8x_9 \oplus x_8x_{10} \oplus x_1 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus x_9.$$

Функция $f^4_{10,2}$ является 6-устойчивой булевой функцией на $\mathbf{F}_2^{10}$ с нелинейностью $2^9 - 2^7 = 384$, алгебраическая степень каждой переменной в $f^4_{10,2}$ равна 3.

2.3 Две специальные последовательности регулярных булевых функций

В этом параграфе будут отдельно описаны две последовательности булевых функций, являющихся частными случаями нашей конструкции из параграфа 2.2, и доказано, что все функции в этих последовательностях являются регулярными. Вторая последовательность функций дает нам достижимость верхней оценки для нелинейности c-регулярных функций, доказанной в параграфе 1.4 при $1 \le \min\{c, n-c\} \le (n/4)+1$. Первую последовательность будем использовать в последующих параграфах.

Начальной функцией (для $k=3$) в обеих последовательностях будет служить функция $f_3(x_1,\dots,x_4) = f'_3(x_1,\dots,x_4) = (x_1 \oplus x_2)(x_3 \oplus x_4) \oplus x_1 \oplus x_3$. Эта функция, очевидно, является 2-регулярной, поскольку на любых двух наборах, отличающихся ровно в двух компонентах x_1 и x_2, а также на любых двух наборах, отличающихся ровно в двух компонентах x_3 и x_4, функция $f_3(x_1,\dots,x_4)$ принимает разные значения. По следствию 1.4 функция $f_3(x_1,\dots,x_4)$ является 1-устойчивой. Нелинейность функции f достигает максимально возможного значения для 1-устойчивых функций от 4 переменных и равна 4. Положим $n(3) = n'(3) = 4$. (Далее величины $n(k)$ и $n'(k)$ будут соответствовать количеству переменных в функциях f_k и f'_k, соответственно).

Строим далее для $k = 3, 4, \dots$ рекурсивно:

$$\begin{gathered} f_{k+1}(x_1,\dots,x_{2n(k)+2}) = \\ (x_{2n(k)+1} \oplus x_{2n(k)+2}) \left(f_k(x_1,\dots,x_{n(k)}) \oplus \bigoplus_{i=n(k)+1}^{2n(k)} x_i \right) \oplus \\ (x_{2n(k)+1} \oplus x_{2n(k)+2} \oplus 1) \left(f_k(x_{n(k)+1},\dots,x_{2n(k)}) \oplus \bigoplus_{i=1}^{n(k)} x_i \right) \oplus x_{2n(k)+1} \end{gathered} \tag{2.5}$$

и

$$\begin{gathered} f'_{k+1}(x_1,\dots,x_{n'(k)+4}) = (x_{n'(k)+3} \oplus x_{n'(k)+4}) \cdot \\ \left(f_k(x_{n'(k)-1}, x_{n'(k)}, x_1, \dots, x_{n'(k)-2}) \oplus x_{n'(k)+1} \oplus x_{n'(k)+2}\right) \oplus \\ (x_{n'(k)+3} \oplus x_{n'(k)+4} \oplus 1) \left(f_k(x_3,\dots,x_{n'(k)+2}) \oplus x_1 \oplus x_2\right) \oplus x_{n'(k)+3}. \end{gathered} \tag{2.6}$$

Нетрудно найти, что $n(k) = 3 \cdot 2^{k-2} - 2$ и $n'(k) = 4(k-2)$.

Приведенные конструкции (2.5) и (2.6) являются частными случаями конструкций из параграфа 2.2, поэтому функции $f_k(x_1,\ldots,x_{n(k)})$ и $f'_k(x_1,\ldots,x_{n'(k)})$ являются соответственно $(n(k)-k)$-устойчивой и $(n'(k)-k)$-устойчивой функциями с максимально возможной для данных числа переменных и устойчивости нелинейностью, соответственно $2^{n(k)-1}-2^{n(k)-k+1}$ и $2^{n'(k)-1}-2^{n'(k)-k+1}$. Кроме того, функции f_k и f'_k достигают неравенства Зигенталера по всем своим переменным. Осталось только показать, что эти функции являются соответственно $(n(k)-k+1)$-регулярной и $(n'(k)-k+1)$-регулярной.

Теорема 2.3. *Если функция $f_k(x_1,\ldots,x_{n(k)})$ в конструкции (2.5) является $(n(k)-k+1)$-регулярной, то функция $f_{k+1}(x_1,\ldots,x_{n(k+1)})$ является $(n(k+1)-(k+1)+1)$-регулярной.*

Доказательство. Рассмотрим произвольный набор $\sigma(x_1,\ldots,x_{n(k)},\ x_{n(k)+1},\ldots,\ x_{2n(k)},\ x_{2n(k)+1},x_{2n(k)+2})$ на $\mathbf{F}_2^{2n(k)+2}$. Из (2.5) имеем

$$f_{k+1}(\sigma)=\begin{cases}\bigoplus\limits_{i=n(k)+1}^{2n(k)} x_i\oplus x_{2n(k)+1}\oplus f_k(x_1,\ldots,x_{n(k)}),\\ \qquad\text{если } x_{2n(k)+1}\oplus x_{2n(k)+2}=1,\\ \bigoplus\limits_{i=1}^{n(k)} x_i\oplus x_{2n(k)+1}\oplus f_k(x_{n(k)+1},\ldots,x_{2n(k)}),\\ \qquad\text{если } x_{2n(k)+1}\oplus x_{2n(k)+2}=0.\end{cases}\tag{2.7}$$

Из (2.7) видим, что $f_{k+1}(\sigma^{2n(k)+1})\neq f_{k+1}(\sigma^{2n(k)+2})$. Если $x_{2n(k)+1}\oplus x_{2n(k)+2}=1$, то $f_{k+1}(\sigma)\neq f_{k+1}(\sigma^i)$ для всех $i=n(k)+1,\ldots,2n(k)$, и $f_{k+1}(\sigma)=f_{k+1}(\sigma^{n+i})$ для $i=1,\ldots,n(k)$ тогда и только тогда, когда $f_k(x_1,\ldots,x_{n(k)})=f_k^i(x_1,\ldots,x_{n(k)})$. Если $x_{2n(k)+1}\oplus x_{2n(k)+2}=0$, то $f_{k+1}(\sigma)\neq f_{k+1}(\sigma^{n+i})$ для всех $i=1,\ldots,n(k)$, и $f_{k+1}(\sigma)=f_{k+1}(\sigma^i)$ для $i=n(k)+1,\ldots,2n(k)$ тогда и только тогда, когда $f_k(x_{n(k)+1},\ldots,x_{2n(k)})=f_k^i(x_{n(k)+1},\ldots,x_{2n(k)})$. Поэтому, $|\{i|f_{k+1}(\sigma^i)=f_{k+1}(\sigma)\}|=|\{i|f_k(\sigma^i)=f_k(\sigma)\}|+1=(k-1)+1=k$. Таким образом, функция f_{k+1} является $(n(k+1)-k)$-регулярной. □

Теорема 2.4. *Если функция $f'_k(x_1,\ldots,x_{n'(k)})$ в конструкции (2.6) является $(n(k)-k+1)$-регулярной, то функция $f'_{k+1}(x_1,\ldots,x_{n'(k+1)})$ является $(n'(k+1)-(k+1)+1)$-регулярной.*

Доказательство. Рассмотрим произвольный набор $\sigma(x_1, \ldots, x_{n(k)+4}$ на $\mathbf{F}_2^{n(k)+4}$). Из (2.6) имеем

$$f'_{k+1}(\sigma) = \begin{cases} x_1 \oplus x_2 \oplus x_{n'(k)+3} \oplus f'_k(x_3, \ldots, x_{n'(k)+2}), \\ \text{если } x_{n'(k)+3} \oplus x_{n'(k)+4} = 0, \\ x_{n'(k)+1} \oplus x_{n'(k)+2} \oplus x_{n'(k)+3} \oplus f'_k(x_{n'(k)-1}, x_{n'(k)}, x_1, \ldots, x_{n'(k)-2}), \\ \text{если } x_{n'(k)+3} \oplus x_{n'(k)+4} = 1. \end{cases} \tag{2.8}$$

Из (2.8) видим, что $f'_{k+1}(\sigma^{n'(k)+3}) \neq f_{k+1}(\sigma^{n'(k)+4})$. Если $x_{n'(k)+3} \oplus x_{n'(k)+4} = 0$, то $f'_{k+1}(\sigma) \neq f'_{k+1}(\sigma^i)$ для $i = 1, 2$, и $f'_{k+1}(\sigma) = f'_{k+1}(\sigma^{n+i})$ для $i = 1, \ldots, n(k)$ тогда и только тогда, когда $f'_k(x_3, \ldots, x_{n'(k)+2}) = f'^i_k(x_3, \ldots, x_{n'(k)+2})$. Если $x_{n'(k)+3} \oplus x_{n'(k)+4} = 1$, то $f'_{k+1}(\sigma) \neq f'_{k+1}(\sigma^i)$ для $i = n'(k)+1, n'(k)+2$, и $f'_{k+1}(\sigma) = f'_{k+1}(\sigma^i)$ для $i = 1, \ldots, n'(k)$ тогда и только тогда, когда $f'_k(x_{n'(k)-1}, x_{n'(k)}, x_1, \ldots, x_{n'(k)-2}) = f'^i_k(x_{n'(k)-1}, x_{n'(k)}, x_1, \ldots, x_{n'(k)-2})$. Поэтому, $|\{i | f'_{k+1}(\sigma^i) = f'_{k+1}(\sigma)\}| = |\{i | f'_k(\sigma^i) = f'_k(\sigma)\}| + 1 = (k-1) + 1 = k$. Таким образом, функция f'_{k+1} является $(n'(k+1) - k)$-регулярной. □

Теорема 2.4 дает достижимость верхней оценки для нелинейности регулярных функций из теоремы 1.4 при $1 \leq \min\{c, n-c\} \leq (n/4) + 1$. Следующее полученное автором утверждение содержится в работе [131].

Теорема 2.5. *Максимальная нелинейность c-регулярных функций на $\mathbf{F}_2^n$ при $1 \leq \min\{c, n-c\} \leq (n/4) + 1$ равна $2^{n-1} - 2^{\max\{c, n-c\}}$.*

Доказательство. Мы уже знаем, что максимальная нелинейность ограничена сверху величиной $2^{n-1} - 2^{\max\{c,n-c\}}$ в соответствии с теоремой 1.4. Пусть $n'L - 4 \leq n$. Тогда по теореме 2.4 существует c-регулярная функция $f'(x_1, \ldots, x_{n'})$ на $\mathbf{F}_2^{n'}$ с нелинейностью $N_{f'} = 2^{n'-1} - 2^{n'-c}$. Добавив $n - n'$ новых фиктивных переменных, мы получим c-регулярную функцию $f(x_1, \ldots, x_n)$ на $\mathbf{F}_2^n$ с нелинейностью $N_f = 2^{n-1} - 2^{n-c}$. Если $n - c \leq (n/4) + 1$, то построим тем же самым путем $(n-c)$-регулярную функцию $f(x_1, \ldots, x_n)$ на $\mathbf{F}_2^n$ с нелинейностью $N_f = 2^{n-1} - 2^c$. Тогда функция $g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \oplus x_1 \oplus \cdots \oplus x_n$ является, очевидно, c-регулярной функцией на $\mathbf{F}_2^n$ с нелинейностью $N_f = 2^{n-1} - 2^c$, и $nl(f) = nl(g)$. □

2.4 Схемная реализация

Проблема схемной реализации булевых функций является очень важной. Даже если некоторая функция обладает совокупностью наилучших криптографических свойств, но требует для своей реализации слишком много элементов, практическое использование такой функции может оказаться слишком дорогим. Заметим, что схемная сложность непосредственной реализации функций, построенных обычными методами, вообще говоря, экспоненциальна по n. В [108] обсуждается схемная сложность функций, построенных изложенными в той работе методами, и дается экспоненциальная оценка. Замечательно, что схемная сложность некоторых функций, строящихся методами, развитыми в настоящей работе, *линейна* по n. Результаты параграфа содержатся в работе автора [159].

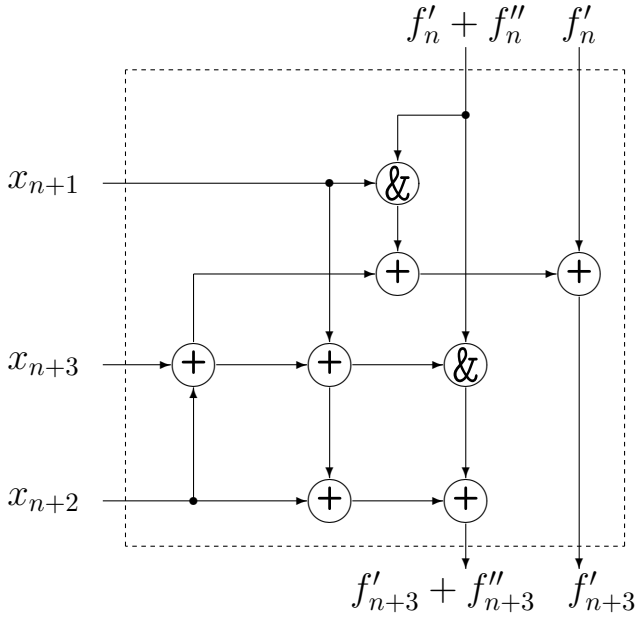


Рис 2. Схема блока B

Дадим конкретные детали такой реализации. Положим

$$\begin{aligned} f'_{n+3} &= (x_{n+1} \oplus 1) f'_n \oplus x_{n+1} f''_n \oplus x_{n+2} \oplus x_{n+3}, \\ f''_{n+3} &= (x_{n+2} \oplus x_{n+3} \oplus 1) f'_n \oplus (x_{n+2} \oplus x_{n+3}) f''_n \oplus x_{n+1} \oplus x_{n+2} \end{aligned} \tag{2.9}$$

По лемме 2.1 если f'_n и f''_n являются m-устойчивыми булевыми функциями на $\mathbf{F}_2^n$ с максимально возможной нелинейностью $(2^{n-1} - 2^{m+1})$, причем f'_n

зависит от двух своих последних переменных линейно, а f''_n зависит от пары своих последних переменных квазилинейно, то f''_{n+3} и f''_{n+3} являются $(m+2)$-устойчивыми булевыми функциями на $\mathbf{F}_2^{n+3}$ с максимально возможной нелинейностью $(2^{n+2} - 2^{m+3})$, причем f'_n зависит от двух своих последних переменных линейно, а f''_n зависит от пары своих последних переменных квазилинейно.

Чуть более удобно переписать соотношения (2.9) в виде

$$\begin{aligned} f'_{n+3} &= x_{n+1}(f'_n \oplus f''_n) \oplus f'_n \oplus x_{n+2} \oplus x_{n+3}, \\ f'_{n+3} \oplus f''_{n+3} &= (x_{n+1} \oplus x_{n+2} \oplus x_{n+3})(f'_n \oplus f''_n) \oplus x_{n+1} \oplus x_{n+3}. \end{aligned} \tag{2.10}$$

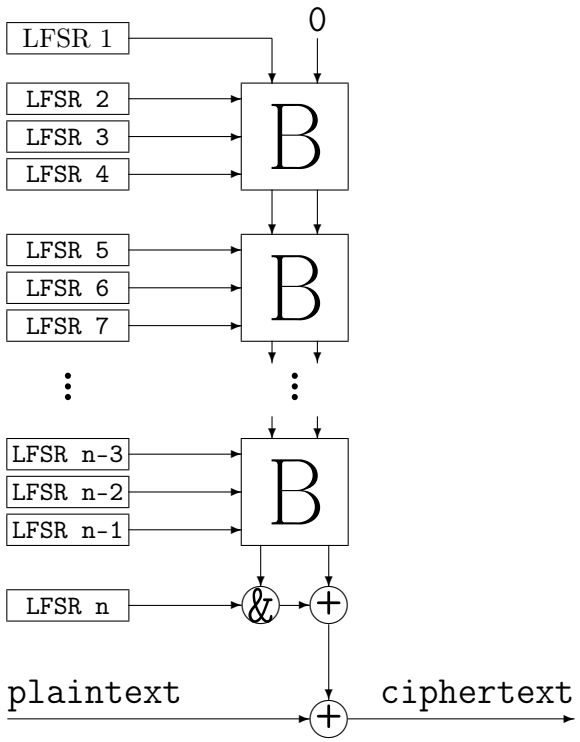


Рис 3. Потоковый шифр, основанный на функции f_n

Соотношения (2.10) позволяют реализовать f'_{n+3} и $f'_{n+3} \oplus f''_{n+3}$ как две функции от пяти значений f'_n, $f'_n \oplus f''_n$, x_{n+1}, x_{n+2}, x_{n+3} с помощью блока B (см. Рис 2). Блок B содержит 8 двухвходовых элементов. В качестве начальных функций могут быть выбраны

$$\begin{aligned} f'_4 &= x_1x_2 \oplus x_3 \oplus x_4, \\ f''_4 &= x_2 \oplus x_1(x_3 \oplus x_4) \oplus x_3, \\ f'_4 \oplus f''_4 &= x_1(x_2 \oplus x_3 \oplus x_4) \oplus x_2 \oplus x_4. \end{aligned}$$

Сравнение с (2.10) показывает, что можно взять $f_1' = 0$, $f_1'' = x_1$. Наконец, положим

$$f_n = x_n(f_{n-1}' \oplus f_{n-1}'') \oplus f_{n-1}', \quad n \equiv 2 \pmod 3.$$

В действительности, функция f_n это функция $f_{n,1}$ из параграфа 2.1 (с точностью до некоторой перестановки переменных). В силу параграфа 2.1 функция f_n является $\frac{2n-7}{3}$-устойчивой функцией на $\mathbf{F}_2^n$, $n \equiv 2 \pmod 3$, с нелинейностью $2^{n-1} - 2^{\frac{2n-4}{3}}$, алгебраическая степень каждой переменной в f_n равна $\frac{n+4}{3}$. Полная схема псевдослучайного генератора для потокового шифра, основанного на функции f_n показана на Рис. 3 (один элемент в первом блоке B, получающий на один из входов 0, может быть удален). Схема функции f_n содержит $2n-4$ элементов XOR и $\frac{2n-1}{3}$ элементов AND. Заметим, что эта схема имеет сильно регулярную каскадную структуру. Для практического применения достаточно штамповать блок B, и варьируя число таких блоков в схеме, мы будем получать функции от различного числа переменных, в зависимости от наших потребностей.

Если $\frac{2n-7}{3} < m$, то можно добавить к предыдущей конструкции недостающие переменные линейно, как это было сделано в доказательстве теоремы 2.1 Если $\frac{2n-7}{3} < m \leq n - \log_2 \frac{n+2}{3} - 2$, и нам нужно построить схему для функции с максимально возможной нелинейностью, достигающей неравенства Зигенталера для каждой отдельной переменной, то также можно сделать это со схемной сложностью, линейной по n, следуя технике, развитой в параграфе 2.2 настоящей работы.

2.5 Усовершенствованный метод построения устойчивых функций, достигающих верхней границы нелинейности

В этом параграфе будет обобщена конструкция построения устойчивых функций, достигающих верхней границы нелинейности, изложенная в параграфе 2.1. С помощью этой конструкции в параграфе 2.6 будут построены m-устойчивые функции на $\mathbf{F}_2^n$ с максимально возможной нелинейностью $2^{n-1} - 2^{m+1}$ для более широкого спектра значений m и n, чем это было сделано в параграфе 2.1. Заметим, что конструкция параграфа 2.1, опубликованная автором в [159] и [134], была модифицирована в [91] в конструкцию, как было сказано, «более удобную для понимания», хотя последнее утверждение очень спорно. Однако изложенную в этом параграфе обобщенную конструкцию никому пока модифицировать не удалось. Результаты параграфа содержатся в статье автора [137].

Предположим,что $f_0, f_1, \ldots, f_{2^k-1}$ — это булевы функции на $\mathbf{F}_2^n$. Будем обозначать f_r также как $f_{\sigma_1 \ldots \sigma_k}$, где $\sigma_1 \ldots \sigma_k$ — это двоичное представление числа r. Предположим, что $c = (c_1, \ldots, c_k)$ — это произвольный двоичный набор. Пусть $s = \sum\limits_{i=1}^{k} c_i$. Обозначим $X = \{x_i \,|\, i = 1, \ldots, n\}$, $Y = \{y_i \,|\, i = 1, \ldots, k\}$, $Z = \{z_i \,|\, c_i = 1,\ i = 1, \ldots, k\}$. Определим

$$f(X, Y, Z) = \left(\bigoplus_{(\sigma_1, \ldots, \sigma_k) \in \mathbf{F}_2^k} \left(\prod_{i=1}^{k} (y_i \oplus c_i z_i \oplus \sigma_i) \right) f_{\sigma_1 \ldots \sigma_k}(X) \right) \oplus \bigoplus_{i=1}^{k} c_i z_i. \quad (2.11)$$

По построению функция f в (2.11) зависит от $n + k + s$ переменных. Ниже сформулируем некоторые свойства конструкции (2.11).

Замечание 2.1. Некоторые детали конструкции (2.11) можно понять более легко, если положить $c_1 = \cdots = c_s = 1$, $c_{s+1} = \cdots = c_k = 0$. Однако для эффективной реализации важно в некоторых случаях варьировать вектор c.

Лемма 2.4. *Предположим, что все* 2^k *булевых функций* f_0, f_1, ..., f_{2^k-1} *в*

(2.11) являются m-устойчивыми. Тогда функция $f(X,Y,Z)$ является $(m+s)$-устойчивой.

Доказательство. Подставим в (2.11) произвольные $m+s$ констант вместо произвольных $m+s$ переменных. Тем самым получим некоторую подфункцию f' от $(n+k-m)$ переменных. Если $c_i = 1$ для некоторого i и если обе переменные y_i и z_i являются свободными в f', то пара переменных (y_i, z_i) является квазилинейной парой в f', поэтому по лемме 1.26 подфункция f' является уравновешенной). Таким образом, можем принять, что для каждого i, такого что $c_i = 1$, по крайней мере одна из двух переменных y_i и z_i замещена константой. Тогда не более m переменных из X замещены константами в (2.11). Все функции $f_0, f_1, \ldots, f_{2^k-1}$ являются уравновешенными, поэтому функция $f(X,Y,Z)$ также является уравновешенной. Тем самым доказано, что произвольная подфункция функции $f(X,Y,Z)$ от $(n+k-m)$ переменных является уравновешенной. □

Лемма 2.5. *Предположим, что нелинейность всех 2^k булевых функций f_0, f_1, …, f_{2^k-1} в (2.11) не менее чем N_0. Более того, для любых двух функций f_{r_1} и f_{r_2}, $0 \le r_1 \ne r_2 \le 2^k-1$, существует пара переменных (x_i, x_j), такая что одна из этих двух функций, скажем f_{r_1}, зависит линейно от переменных x_i и x_j, в то время как другая функция f_{r_2} зависит квазилинейно от пары (x_i, x_j). Тогда $nl(f) \ge 2^s(2^{n-1}(2^k-1)+N_0)$.*

Доказательство. Очевидно, что если мы заменим $c_i = 0$ на $c_i = 1$, то мы умножим нелинейность на 2 (добавляя новую переменную). Таким образом, мы можем считать, что $s = 0$. Рассмотрим произвольную аффинную функцию l. Обозначим $l_r = l_{y_1,\ldots,y_k}^{\sigma_1\oplus 1,\ldots,\sigma_k\oplus 1}$, где $\sigma_1 \ldots \sigma_k$ — это двоичное представление числа r. Заметим, что для любого $r = 0, \ldots, 2^k-1$, имеем $l_r = l_0$ или $l_r = l_0 \oplus 1$. Тогда $d(f,l) = \sum\limits_{r=0}^{2^k-1} d(f_r, l_r)$. По лемме 1.29 и предположению этой леммы имеем что $d(f_r, l_r) \ne 2^{n-1}$ для не более чем одного значения r. Таким образом, $d(f,l) \ge 2^{n-1}(2^k-1)+N_0$. Аффинная функция l была выбрана произвольно. Поэтому $nl(f) \ge 2^{n-1}(2^k-1)+N_0$. □

Конструкция (2.11) является обобщением конструкции в [159], где рассматривался только случай $k = 1$.

Проблема заключается в том, чтобы найти функции $f_0, f_1, \ldots, f_{2^k-1}$ с требуемым распределением линейных и квазилинейных переменных. Ниже будет дан некоторый подход, который позволяет строить такие системы функций.

Определение 2.1. *Пусть $B = (b_{ij})$ — это $(2^k \times p)$ матрица с 2^k строками и p столбцами, клетки которой заполнены символами из множества $\{1, 2, *\}$. Пусть k_0 и t — это натуральные числа. Мы предполагаем, что*

(i) для любых двух строк i_1 и i_2 существует столбец j, такой что $b_{i_1 j} = 1$, $b_{i_2 j} = 2$ или $b_{i_1 j} = 2$, $b_{i_2 j} = 1$.

(ii) для любой строки i выполняется неравенство $\sum_{j=1}^{p} b_{ij} \leq t$ (знаки $*$ не дают в суммы никакого вклада).

(iii) в каждой строке число единиц не превосходит k_0.

Если матрица B удовлетворяет всем свойствам (i), (ii), (iii), то мы говорим, что B является подходящей *(k_0, k, p, t)-матрицей.*

Определение 2.2. *Пусть F является множеством булевых функций, таким что для каждого s, $0 \leq s \leq k$, множество F содержит $(m+s)$-устойчивую функцию на $\mathbf{F}_2^{n+s}$ с нелинейностью не менее $2^s(2^{n-1} - 2^{m+\lambda})$ (λ не обязательно целое), которая имеет s непересекающихся пар квазилинейных переменных. Тогда мы говорим, что F является $S_{n,m,k,\lambda}$-*системой *булевых функций.*

Замечание 2.2. Для того, чтобы обеспечить существование $S_{n,m,k,\lambda}$-системы булевых функций, достаточно иметь только $(m+k)$-устойчивую функцию f на $\mathbf{F}_2^{n+k}$ с нелинейностью не менее $2^k(2^{n-1} - 2^{m+\lambda})$, которая содержит k непересекающихся пар квазилинейных переменных. Все остальные требуемые функции $S_{n,m,k,\lambda}$-системы могут быть получены из f подстановками констант вместо некоторых переменных из различных непересекающихся пар квазилинейных переменных. Заметим, однако, что последний путь не является эффективным с точки зрения схемной реализации.

Лемма 2.6. *Существует $S_{2,-1,2,1}$-система булевых функций.*

Доказательство. Пусть $f_0' = x_1 x_2$, $f_1' = (x_1 \oplus x_2)x_3 \oplus x_1$, $f_2' = (x_1 \oplus x_2)(x_3 \oplus x_4) \oplus x_1 \oplus x_3$. Легко проверить, что f_s', $s = 0, 1, 2$, — это $(-1+s)$-устойчивая

функция на $\mathbf{F}_2^{2+s}$ с нелинейностью $2^s(2^{2-1} - 2^{-1+1})$, более того f'_s содержит s непересекающихся пар квазилинейных переменных. □

Теорема 2.6. *Предположим, существует $S_{n,m,k_0,\lambda}$-система булевых функций F и существует подходящая (k_0, k, p, t)-матрица B, $n \geq 2p - t$. Тогда существует $S_{n+k+t,m+t,k,\lambda}$-система булевых функций.*

Доказательство. Рассмотрим i-ю строку матрицы B, $i = 0, 1, \ldots, 2^k - 1$. Предположим, что эта строка содержит $s = s(i)$ единиц. Матрица B является подходящей, поэтому $s \leq k_0$, $s \leq t$. По предположению существует $(m + s)$-устойчивая функция f'_i на $\mathbf{F}_2^{n+s}$, которая содержит s непересекающихся пар квазилинейных переменных, с нелинейностью не менее $2^s(2^{n-1} - 2^{m+\lambda})$. Добавим $t - s$ новых линейных переменных к функции f'_i. В результате получим функцию f''_i на $\mathbf{F}_2^{n+t}$. Легко видеть, что функция f''_i является $(m+t)$-устойчивой функцией с нелинейностью не менее $2^t(2^{n-1} - 2^{m+\lambda})$, более того, f''_i содержит s непересекающихся пар квазилинейных переменных, и кроме того $t-s$ линейных переменных. Заметим, что по свойству (ii) подходящей матрицы величина $t - s$ не меньше, чем число двоек в i-й строке B, умноженное на 2. Таким способом строим функции f''_i на $\mathbf{F}_2^{n+t}$ для каждого i, $i = 0, 1, \ldots, 2^k - 1$. По предположению, $n + t \geq 2p$. Далее, для каждого i, $i = 0, 1, \ldots, 2^k - 1$, переставляем переменные в $f''_i(x_1, \ldots, x_{n+t})$, получая функцию f_i, такую что функция f_i зависит от пары переменных (x_{2j-1}, x_{2j}) квазилинейно, если $b_{ij} = 1$, и функция f_i зависит от переменных x_{2j-1} и x_{2j} линейно, если $b_{ij} = 2$. В силу приведенных выше аргументов, имеем для этой процедуры достаточно число квазилинейных и линейных переменных. Теперь мы готовы применить конструкцию (2.11). С помощью этой конструкции, варьируя число единиц в векторе $(c_1, \ldots, c_k)$, получаем функции $f(X, Y, Z_s)$, $s = 0, 1, \ldots, k$. Функция $f(X, Y, Z_s)$ по леммам 2.4 и 2.5 является $(m + t + s)$-устойчивой функцией на $\mathbf{F}_2^{n+k+t+s}$ с нелинейностью не менее чем $2^s(2^{n+k+t-1} - 2^{m+t+\lambda})$. Более того, функция $f(X, Y, Z_s)$ содержит s непересекающихся пар квазилинейных переменных. Таким образом, построена $S_{n+k+t,m+t,k,\lambda}$-система булевых функций. □

Применение конструкции, данной в теореме 2.6, обозначим через

$$S_{n,m,k_0,\lambda} T_{k_0,k,p,t} = S_{n+k+t,m+t,k,\lambda}.$$

Если добавить новую линейную переменную к m-устойчивой функции f на $\mathbf{F}_2^n$, то получится $(m+1)$-устойчивая функция f' на $\mathbf{F}_2^{n+1}$ с нелинейностью $2nl(f)$. Обозначим эту процедуру через

$$S_{n,m,0,\lambda}T_{0,0,0,1} = S_{n+1,m+1,0,\lambda}.$$

2.6 Примеры подходящих матриц, эффективных для нашей конструкции, и новые устойчивые булевы функции с максимальной нелинейностью

Напомним, что в параграфе 2.1 были построены m-устойчивые функции на $\mathbf{F}_2^n$, достигающие верхней оценки нелинейности $2^{n-1} - 2^{m+1}$, при $\frac{2n-7}{3} \leq m \leq n-2$. Этот результат был несколько улучшен в [91], где с помощью некоторой модификации нашей конструкции и компьютерного нахождения 2-устойчивой функции от 7 переменных с нелинейностью 56, имеющей *подходящий вид,* были построены искомые функции для $\frac{2n-9}{3} \leq m \leq n-2$. В этом параграфе с помощью конструкции, изложенной в параграфе 2.5, и некоторых конкретных *подходящих матриц* будут построены m-устойчивые функции на $\mathbf{F}_2^n$ для более широкого спектра значений m и n, чем это было сделано в параграфе 2.1 и статье [91], а именно для $\frac{5n-14}{8} \leq m \leq n-2$ и для $0.6n-1 \leq m \leq n-2$. В конце параграфа будут сделаны некоторые замечания по комбинаторной задаче, связанной с *подходящими матрицами* и даем геометрические интерпретации. Результаты параграфа содержатся в статье автора [137].

Дадим сначала некоторые примеры подходящих матриц, эффективных для построения булевых функций с хорошей комбинацией параметров. Обозначим подходящую (k_0, k, p, t)-матрицу через $B_{k_0,k,p,t}$.

$$B_{1,1,1,2} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \; B_{2,2,2,4} = \begin{pmatrix} 2 & 2 \\ 2 & 1 \\ 1 & 2 \\ 1 & 1 \end{pmatrix}, \; B_{3,2,3,3} = \begin{pmatrix} 2 & 1 & * \\ * & 2 & 1 \\ 1 & * & 2 \\ 1 & 1 & 1 \end{pmatrix},$$

$$B_{2,3,5,6} = \begin{pmatrix} 2 & 2 & 1 & 1 & * \\ 2 & 1 & 1 & 2 & * \\ 2 & 1 & * & 1 & 2 \\ 2 & 1 & 2 & * & 1 \\ 1 & 1 & * & 2 & 2 \\ 1 & 2 & 1 & * & 2 \\ 1 & * & 2 & 1 & 2 \\ 1 & * & 2 & 2 & 1 \end{pmatrix}, \; B_{3,3,4,5} = \begin{pmatrix} * & 1 & 2 & 2 \\ 2 & * & 1 & 2 \\ 2 & 2 & * & 1 \\ 1 & 2 & 2 & * \\ 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix},$$

$$B_{2,4,7,8} = \begin{pmatrix} 1 & 1 & * & * & 2 & 2 & 2 \\ * & 2 & 1 & 1 & * & 2 & 2 \\ * & * & 2 & 2 & 1 & 1 & 2 \\ 1 & * & * & 2 & 2 & 2 & 1 \\ 2 & 1 & 1 & * & * & 2 & 2 \\ * & * & 2 & 1 & 1 & 2 & 2 \\ * & * & 2 & 2 & 2 & 1 & 1 \\ 1 & 2 & 2 & 1 & 2 & * & * \\ * & 1 & 2 & 2 & 1 & 2 & * \\ * & * & 1 & 2 & 2 & 1 & 2 \\ 2 & * & * & 1 & 2 & 2 & 1 \\ 1 & 2 & * & 2 & 1 & 2 & * \\ * & 1 & 2 & * & 2 & 1 & 2 \\ 2 & * & 1 & 2 & * & 2 & 1 \\ 2 & 2 & * & 1 & * & 1 & 2 \\ 2 & 2 & 2 & * & 1 & * & 1 \end{pmatrix}, B_{4,4,6,6} = \begin{pmatrix} 2 & 2 & 2 & * & * & * \\ 1 & 2 & * & 1 & 2 & * \\ 1 & 2 & * & * & 1 & 2 \\ 1 & 2 & * & 2 & * & 1 \\ * & 1 & 2 & 1 & 2 & * \\ * & 1 & 2 & * & 1 & 2 \\ * & 1 & 2 & 2 & * & 1 \\ 2 & * & 1 & 1 & 2 & * \\ 2 & * & 1 & * & 1 & 2 \\ 2 & * & 1 & 2 & * & 1 \\ 2 & * & 1 & 1 & 1 & 1 \\ 1 & 2 & * & 1 & 1 & 1 \\ * & 1 & 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & * & 1 \\ 1 & 1 & 1 & 1 & 2 & * \\ 1 & 1 & 1 & * & 1 & 2 \end{pmatrix}.$$

Легко проверить, что все приведенные выше матрицы являются подходящими матрицами с соответствующими параметрами.

Теперь применим подходящие матрицы для построения устойчивых функций с максимально возможной нелинейностью, используя конструкцию параграфа 2.5.

Простейшим примером подходящей матрицы является матрица $B_{1,1,1,2}$. Если $\frac{2n-7}{3} \leq m \leq n-3$, то числа n и m могут быть представлены в виде $n = 3r+s+2$,

$m = 2r + s - 1$, где r и s — это неотрицательные целые (существование этого представления, так же как и существование представлений в теоремах 2.7 и 2.8 может быть доказано с помощью аргументов из элементарной арифметики). По лемме 2.6 существует система $S_{2,-1,2,1}$. Применяем

$$S_{2,-1,2,1}(T_{1,1,1,2})^r(T_{0,0,0,1})^s = S_{n,m,0,1}.$$

Поэтому $\mathrm{nlmax}(n,m) \geq 2^{n-1} - 2^{m+1}$ для $m \geq \frac{2n-7}{3}$. Ранее было указано, что $\mathrm{nlmax}(n,m) \leq 2^{n-1} - 2^{m+1}$ для $m \leq n-2$. Поэтому $\mathrm{nlmax}(n,m) = 2^{n-1} - 2^{m+1}$ для $\frac{2n-7}{3} \leq m \leq n-2$. Приведенная выше конструкция была дана в [159].

Теорема 2.7. $\mathrm{nlmax}(n,m) = 2^{n-1} - 2^{m+1}$ *для* $\frac{5n-14}{8} \leq m \leq n-2$.

Доказательство. Пусть n, m — это целые числа. Заметим, что $\lceil \frac{5n-14}{8} \rceil \geq \lceil \frac{2n-7}{3} \rceil$ при $n < 17$. Если $n \geq 17$, $m > n-8$, то $m \geq \frac{2n-7}{3}$. Если $n \geq 17$, $\frac{5n-13}{8} \leq m \leq n-8$, то числа n и m могут быть представлены в форме $n = 8r_1 + 3r_2 + s + 17$, $m = 5r_1 + 2r_2 + s + 9$, где r_1, r_2 и s — это неотрицательные целые. Применяем

$$S_{2,-1,2,1}T_{2,2,2,4}T_{2,3,5,6}(T_{3,3,4,5})^{r_1}(T_{1,1,1,2})^{r_2}(T_{0,0,0,1})^s = S_{n,m,0,1}.$$

Если $n \geq 17$, $\frac{5n-14}{8} = m$, то числа n и m могут быть представлены в форме $n = 8r + 22$, $m = 5r + 12$, где r — это неотрицательное целое. В этом случае применяем

$$S_{2,-1,2,1}T_{2,2,2,4}T_{2,3,5,6}(T_{3,3,4,5})^r T_{3,2,3,3} = S_{n,m,2,1}.$$

□

Теорема 2.8. $\mathrm{nlmax}(n,m) = 2^{n-1} - 2^{m+1}$ *для* $0.6n - 1 \leq m \leq n-2$.

Доказательство. Пусть n, m — это целые числа. Заметим, что $0.6n - 1 \geq \frac{2n-7}{3}$ для $n \leq 20$. Если $n \geq 20$, $m > n-9$, то $m \geq \frac{2n-7}{3}$. Если $n \geq 20$, $0.6n - 1 \leq m \leq n-9$, исключая случай $m = 0.6n-1$, $n \equiv 5 \pmod{10}$, то числа n и m могут быть представлены в форме $n = 10r_1+8r_2+3r_3+s+20$, $m = 6r_1+5r_2+2r_3+s+11$, где r_1, r_2, r_3 и s — это неотрицательные целые. Применяем

$$S_{2,-1,2,1}T_{2,2,2,4}T_{2,4,7,8}(T_{4,4,6,6})^{r_1}(T_{3,3,4,5})^{r_2}(T_{1,1,1,2})^{r_3}(T_{0,0,0,1})^s = S_{n,m,0,1}.$$

В случае $n = 10r + 25$, $m = 6r + 14$, где r — это неотрицательное целое, применяем

$$S_{2,-1,2,1}T_{2,2,2,4}T_{2,4,7,8}(T_{4,4,6,6})^r T_{3,2,3,3} = S_{n,m,2,1}.$$

□

Сделаем некоторые замечания по комбинаторной задаче, связанной с подходящими матрицами и дадим геометрические интерпретации. Если существует подходящая (k, k, p, t)-матрица, то используя технику, описанную в предыдущем параграфе, можно доказать, что $\mathrm{nlmax}(n, m) = 2^{n-1} - 2^{m+1}$ для $m > \frac{t}{t+k}n - c'$, где c' это некоторая константа. Заметим, что конструкция в [52] позволяет достигнуть такой нелинейности только для $m \leq c''\frac{n}{4}(1 + o(1))$. Поэтому мы заинтересованы в нахождении подходящей (k, k, p, t)-матрицы с как можно меньшим отношением $\frac{t}{k}$.

Для заданного натурального k обозначим через $t(k)$ минимальное натуральное t, такое что для некоторого p существует подходящая (k, k, p, t)-матрица. Ясно, что можно рассматривать только матрицы без столбцов из одних звездочек. Тогда, очевидно, $p \leq t \cdot 2^k$. Существует подходящая $(k, k, k, 2k)$-матрица (все строки различны и не содержат звездочек). Таким образом, для того, чтобы найти $t(k)$, достаточно рассмотреть только конечное множество матриц.

Утверждение 2.1. *Пусть k_1 и k_2 являются натуральными числами. Тогда $t(k_1 + k_2) \leq t(k_1) + t(k_2)$.*

Доказательство. По определению для некоторых p_1 и p_2 существуют подходящая $(k_1, k_1, p_1, t(k_1))$-матрица B' и подходящая $(k_2, k_2, p_2, t(k_2))$-матрица B''. Составим матрицу B размера $(2^{k_1+k_2} \times (p_1 + p_2))$, где строки B представляют из себя всевозможные конкатенации строк матриц B' и B''. Легко видеть, что B является подходящей $(k_1 + k_2, k_1 + k_2, p_1 + p_2, t(k_1) + t(k_2))$-матрицей. Поэтому $t(k_1 + k_2) \leq t(k_1) + t(k_2)$. □

Достаточно очевидно, что

Утверждение 2.2. $t(k) \geq k$.

Из утверждений 2.1 и 2.2 следует, что существует предел $\lim\limits_{k\to\infty} \frac{t(k)}{k}$.

Подходящая (k_0, k, p, t)-матрица B может быть проинтерпретирована как совокупность 2^k непересекающихся подкубов булева куба $\{1,2\}^p$. Действительно, строка B может быть проинтерпретирована как подкуб, где компоненты со звездочками соответствуют свободным переменным, в то время как компоненты с 1 или 2 соответствуют переменным, замещенным соответствующими константами. Проиллюстрируем это на примере матрицы $B_{3,3,4,5}$:

строка B_{3345}	наборы подкуба
$*122$	$\{(1,1,2,2),(2,1,2,2)\}$
$2*12$	$\{(2,1,1,2),(2,2,1,2)\}$
$22*1$	$\{(2,2,1,1),(2,2,2,1)\}$
$122*$	$\{(1,2,2,1),(1,2,2,2)\}$
2111	$\{(2,1,1,1)\}$
1211	$\{(1,2,1,1)\}$
1121	$\{(1,1,2,1)\}$
1112	$\{(1,1,1,2)\}$

Свойство (i) подходящей матрицы обеспечивает то, что подкубы не пересекаются. Свойства (ii) и (iii) характеризуют расположение подкубов в кубе и размер подкубов.

Оценивая числа наборов на различных уровнях булева куба, которые принадлежат некоторым непересекающимся подкубам, можно показать, что

Утверждение 2.3. *$t(1) = 2$, $t(2) = 4$, $t(3) = 5$, $t(4) = 6$, $t(5) = 8$, $t(6) = 9$, $t(7) = 11$, $t(8) = 12$, $t(10) = 15$.*

Позднее в работах студентки автора Марии Федоровой [24] и [25] и ее совместной статье с автором [132] (полной версией статьи является [168]) было показано, что не существует подходящих (k_0, k, p, t)-матриц при $\frac{t}{t+k} < \frac{1}{\log_2\left(\sqrt{5}+1\right)} = 0.5902\ldots$ Отсюда следует, что используя только метод подходящих матриц, нельзя построить m-устойчивые функции на $\mathbf{F}_2^n$ с максимально возможной нелинейностью $2^{n-1} - 2^{m+1}$ при $m < 0.5902\ldots n + O(1)$. В то же время в работе [25] доказано, что $\lim\limits_{k\to\infty} \frac{t(k)}{k} \frac{1}{\log_2\left(\sqrt{5}+1\right)} = 0.5902\ldots$, а в работе

[132] построена бесконечная последовательность таких функций, для которых $m = 0.5902\ldots n + O(\log_2 n)$.

2.7 Разделимые наборы и обобщение подходящих матриц

Для того, чтобы дальнейшее изложение было более понятно, формализуем главное содержание параграфа 2.5 в следующих двух конструкциях и соответствующих им леммах.

Конструкция 1. Пусть $X = (x_1, \ldots, x_{n+t})$, $Y = (y_1, \ldots, y_k)$ — наборы булевых переменных. Пусть $\{f_\sigma(X)\}_{\sigma \in \mathbf{F}_2^k}$ — множество из 2^k функций, обладающих следующими свойствами:
1) каждая $f_\sigma(X)$ является $(m+t)$-устойчивой булевой функцией на $\mathbf{F}_2^{n+t}$;
2) каждая $f_\sigma(X)$ достигает границы (1.8);
3) для любых двух функций $f_{\sigma'}(X)$ и $f_{\sigma''}(X)$, $\sigma' \neq \sigma''$, носители спектра функций $f_{\sigma'}(X)$ и $f_{\sigma''}(X)$ не пересекаются.

Лемма 2.7. *В обозначениях конструкции 1 функция*

$$g(X,Y) = \bigoplus_{\sigma \in \mathbf{F}_2^k} \left(\prod_{i=1}^{k} (y_i \oplus \sigma_i) \right) f_\sigma(X)$$

является $(m+t)$-устойчивой булевой функцией на $\mathbf{F}_2^{n+t+k}$, достигающей границы (1.8).

Доказательство. По следствию 1.7 каждая из функций $f_\sigma(X)$ является платовидной, и все ненулевые коэффициенты Уолша каждой из этих функций по модулю равны 2^{m+t+2}. Отсюда из попарного непересечения носителей спектра функций $f_\sigma(X)$ по лемме 1.7 следует, что все ненулевые коэффициенты Уолша функции g тоже по модулю равны 2^{m+t+2}. Из того, что все $f_\sigma(X)$ являются $(m+t)$-устойчивыми, следует, что и g является $(m+t)$-устойчивой. Поэтому g действительно достигает границы (1.8). □

Конструкция 2. Пусть $X = (x_1, \ldots, x_{n+t})$, $Y = (y_1, \ldots, y_k)$, $Z = (z_1, \ldots, z_k)$ — наборы булевых переменных. Пусть $c = (c_1, \ldots, c_k) \in \mathbf{F}_2^k$, — фиксированный двоичный вектор, $|c| = s$. Пусть $\{f_\sigma(X)\}_{\sigma \in \mathbf{F}_2^k}$ — множество из 2^k функций, обладающих теми же свойствами, что и в конструкции 1:

1) каждая $f_\sigma(X)$ является $(m+t)$-устойчивой булевой функцией на $\mathbf{F}_2^{n+t}$;
2) каждая $f_\sigma(X)$ достигает границы (1.8);
3) для любых двух функций $f_{\sigma'}(X)$ и $f_{\sigma''}(X)$, $\sigma' \neq \sigma''$, носители спектра функций $f_{\sigma'}(X)$ и $f_{\sigma''}(X)$ не пересекаются.

Лемма 2.8. *В обозначениях конструкции 2 функция*

$$g_c(X,Y,Z_c) = \bigoplus_{\sigma\in\mathbf{F}_2^k} \left(\prod_{i=1}^{k} (y_i \oplus c_i z_i \oplus \sigma_i) \right) f_\sigma(X) \oplus \bigoplus_{i=1}^{k} c_i z_i$$

является $(m+t+s)$-устойчивой булевой функцией на $\mathbf{F}_2^{n+t+k+s}$, достигающей границы (1.8), имеющей s непересекающихся пар квазилинейных переменных. Будем считать, что если $c_i = 0$, то переменная z_i не входит во множество Z_c переменных функции g_c.

Доказательство. Если $s = 0$, то утверждение уже доказано в лемме 2.7 для функции g_0, которая по следствию 1.7 является платовидной. Если $s > 0$, то будем последовательно заменять в g_0 для всех i, что $c_i = 1$, переменные y_i на пары квазилинейных переменных (y_i, z_i). На каждом шаге такой замены по лемме 1.30 все ненулевые коэффициенты Уолша у новой функции будут по модулю в 2 раза больше, чем у предыдущей. Поэтому на каждом шаге снова будет получаться платовидная функция. Сделав все s шагов, получим, что у функции g_c все коэффициенты Уолша принадлежат множеству $\{0, \pm 2^{m+t+s+2}\}$. Покажем, что функция g_c является $(m+t+s)$-устойчивой. Рассмотрим произвольный набор α из носителя спектра функции g_c. В первых $(n+t)$ компонентах α по лемме 1.7 имеет более $m+t$ единиц, потому что каждая из функций $f_\sigma(X)$ является $(m+t)$-устойчивой. В каждой из пар компонент, соответствующих парам переменным (y_i, z_i) для $c_i = 1$ набор α имеет одну единицу по следствию 1.11. Поэтому набор α имеет вес больше $m+t+s$. Отсюда функция g_c является $(m+t+s)$-устойчивой и, по сказанному выше, достигает границы (1.8). Лемма доказана. □

Имея m-устойчивую функцию на $\mathbf{F}_2^n$, достигающую границы (1.8), можно получить из нее $(m+t)$-устойчивую функцию на $\mathbf{F}_2^{n+t}$, достигающую границы

(1.8), добавив к ней t' новых линейных переменных и преобразовав s переменных, $t' + s = t$, в пары квазилинейных переменных. Нужная нелинейность гарантируется леммами 1.23 и 1.30, а нужный рост устойчивости может быть достигнут согласно лемме 2.8, если заменить на пару квазилинейных переменных только что добавленные переменные y_i.

Однако для применения конструкции 2 нужно добиться того, чтобы носители спектра любых двух разных функций f_σ не пересекались. В [137] для этой цели были введены (k_0, k, p, t)-подходящие матрицы. Здесь не будем повторять здесь определение этих матриц, а дадим его обобщение, после чего поясним различия между старым и новым определениями.

Рассмотрим множество наборов V длины p, компонентами которых являются символы $1/2$, 1 или $*$, причем все символы $1/2$ объединены в пары (таким образом, общее число символов $1/2$ в каждой строке четно). Каждый набор α из V будем ассоциировать с состояниями последних p переменных $v_1, \ldots, v_k$ некоторой булевой функции $f_\alpha(u_1, \ldots, u_{n-p}, v_1, \ldots, v_p)$, а именно, если $\alpha_i = 1$, то соответствующая переменная v_i функции f_α является линейной; если $\alpha_i = \alpha_j = 1/2$ и разряды i и j в наборе α объединены в пару, то переменные (v_i, v_j) являются парой квазилинейных переменных функции f_α.

Два набора α и β из множества V назовем *разделимыми,* если носители спектра соответствующих функций f_α и f_β гарантированно не пересекаются.

Пример 1. Пусть $\alpha_i = \alpha_j = 1$, $\beta_i = \beta_j = 1/2$ и разряды i и j в наборе β объединены в пару. Тогда носители спектра соответствующих функций f_α и f_β гарантированно не пересекаются. Действительно, любой набор из носителя спектра f_α по следствию 1.9 имеет единицы в разрядах, соответствующих переменным v_i и v_j, а любой набор из носителя спектра f_β по следствию 1.11 имеет в одном из разрядов, соответствующих переменным v_i и v_j, единицу, а в другом — ноль. На этом фактически и основывалось использование конструкции 2 в [137] (но на другом языке — без использования коэффициентов Уолша), однако этим примером и ограничивалось. Сейчас покажем, что разделимые наборы могут иметь более общий вид.

Лемма 2.9. *Пусть α и β — два набора из V длины p. Пусть I — множе-*

ство индексов, $I \subseteq \{1, \ldots, p\}$. Пусть наборы α и β не содержат символов $*$ в компонентах из I, а каждый символ $1/2$ в компоненте из I объединен в каждом из этих наборов в пару с символом $1/2$ также в компоненте из I. Пусть, кроме того, наборы α и β содержат разное число пар символов $1/2$ в компонентах из I. Тогда наборы α и β являются разделимыми.

Доказательство. Пусть в наборе α в точности a пар символов $1/2$ в компонентах из I и, соответственно, в точности $|I| - 2a$ единиц в компонентах из I. Тогда по следствиям 1.9 и 1.11 любой набор из носителя спектра функции f_α в компонентах из I содержит в точности $|I| - a$ единиц. Поэтому если в наборе β в точности b пар символов $1/2$ в компонентах из I, $a \neq b$, то спектры функций f_α и f_β не пересекаются, что доказывает лемму. □

Следствие 2.2. *Пусть α и β — два набора из V длины p, причем найдутся разряды $i_1, \ldots, i_{2d}$, такие что $\alpha_{i_1} = \alpha_{i_{2d}} = 1$, $\alpha_{i_j} = 1/2$, $j = 2, \ldots, 2d-1$; $\beta_{i_j} = 1/2$, $j = 1, \ldots, 2d$. Кроме того, в пары объединены разряды (i_{2j}, i_{2j+1}), $j = 1, \ldots, d-1$, в наборе α и разряды (i_{2j-1}, i_{2j}), $j = 1, \ldots, d$, в наборе β. Тогда наборы α и β являются разделимыми.*

Лемма 2.10. *Пусть α и β — два набора из V длины $p = n + k$. Пусть I — множество индексов, $I \subseteq \{1, \ldots, p\}$, $|I| = n$. Обозначим через α_I и β_I ограничения α и β на I, соответственно. Предположим, что в наборе α каждый символ $1/2$ в разряде из I объединен в пару с некоторым символом $1/2$ также в разряде из I, пусть то же самое верно для набора β. Кроме того, предположим, что поднаборы α_I и β_I являются разделимыми. Тогда наборы α и β также являются разделимыми.*

Доказательство. По определению разделимых наборов для заданного $u \in \mathbf{F}_2^n$ либо $W_{f_{\alpha(I)}}(u) = 0$ для любой функции $f_{\alpha(I)}$, ассоциированной с $\alpha(I)$, либо $W_{f_{\beta(I)}}(u) = 0$ для любой функции $f_{\beta(I)}$, ассоциированной с $\beta(I)$. Отсюда по лемме 1.7 следует, что либо $W_{f_\alpha}(uv) = 0$ для любого $v \in \mathbf{F}_2^k$ и любой функции f_α на $\mathbf{F}_2^{n+k}$, ассоциированной с α, либо $W_{f_\beta}(uv) = 0$ для любого $v \in \mathbf{F}_2^k$ и любой функции f_β на $\mathbf{F}_2^{n+k}$, ассоциированной с β. □

Понятие разделимых наборов полезно для построения множеств разделимых функций, требующихся в конструкции 2. Введем понятие обобщенной подходящей матрицы.

Матрица A размера $2^k \times p$ называется *обобщенной* (k_0, k, p, t)*-подходящей матрицей,* если в ее клетках записаны символы из множества $\{1/2, 1, *\}$, причем все символы $1/2$ внутри каждой строки объединены в непересекающиеся пары и, кроме того, выполнены следующие условия:

1) каждая строка матрицы A содержит не более k_0 пар символов $1/2$;

2) сумма всех числовых символов в каждой строке равна t (звездочки не считаются);

3) любые две разные строки матрицы A являются разделимыми.

Отличие обобщенных подходящих матриц от просто подходящих матриц, введенных в [137], следующее. Во-первых, в [137] все столбцы были жестко объединены в пары, и два столбца из одной пары совпадали (в обозначениях [137] они объединялись в один столбец с удвоенными значениями символов), а символы $1/2$ автоматически объединялись в пару внутри пары столбцов. Во-вторых, в [137] разделимыми де факто считались только пары строк, для которых имела место конфигурация примера 1. В-третьих, в [137] условие 2) было ослабленным, — требовалось, чтобы соответствующая сумма не превосходила t; но это малосущественное ослабление приводило к дополнительным построениям в дальнейшем.

Следующая лемма является переформулировкой для обобщенных подходящих матриц утверждения из [137].

Лемма 2.11. *Пусть A — обобщенная (k_0, k, p, t)-подходящая матрица. Пусть n и m — натуральные числа, $p \le n+t$. Предположим, что для каждого целого i, такого что*

(a) $0 \le i \le k_0$;

(b) в матрице A есть строка α, содержащая в точности i пар символов $1/2$ выполняется следующее условие: существует $(m+i)$-устойчивая функция на $\mathbf{F}_2^{n+i}$, имеющая i непересекающихся пар квазилинейных переменных и достигающая границы (1.8). Тогда для каждого целого s, $0 \le s \le k$, можно построить

$(m+t+s)$-устойчивую функцию на $\mathbf{F}_2^{n+t+k+s}$, имеющую s непересекающихся пар квазилинейных переменных и достигающую границы (1.8).

Доказательство. Пусть строка α матрицы A содержит в точности i пар символов $1/2$. Возьмем соответствующую этой строке функцию f_α, существование которой гарантировано условием леммы. К f добавим $t-i$ новых линейных переменных. Переставим у получившейся $(m+t)$-устойчивой функции на $\mathbf{F}_2^{n+t}$ переменные так, чтобы последние p переменных пришли в соответствие с видом строки α: в разряды, где в α находится 1, поставим линейные переменные, а в разряды, соответствующие паре символов $1/2$, поместим пару квазилинейных переменных. Легко видеть, что от перестановки переменных нелинейность и устойчивость функции не изменяются. Проделаем это для каждой строки матрицы A. В результате получим семейство функций, удовлетворяющих условию конструкции 2, что по лемме 2.8 гарантирует построение требуемых новых функций. Лемма доказана. □

Пример 2. Пусть p четно, $\binom{p/2}{2} \geq 2^k$. Тогда существует обобщенная $(2, k, p, p-2)$-подходящая матрица. Действительно, объединим жестко в пары разряды $(2i-1, 2i)$, $i = 1, \ldots, p/2$. В качестве строк будем выбирать только строки ровно с двумя парами символов $1/2$ (внутри жестко скрепленных пар) и единицами в остальных разрядах. Всего существует $\binom{p/2}{2}$ строк такого вида. Легко видеть, что любые две разные строки такого вида разделимы. Поскольку по условию $\binom{p/2}{2} \geq 2^k$, мы сможем написать 2^k разных строк такого вида, что и требуется для построения обобщенной $(2, k, p, p-2)$-подходящей матрицы.

Функция $f(x_1, x_2, x_3, x_4) = (x_1 \oplus x_2)(x_3 \oplus x_4) \oplus x_2 \oplus x_4$ имеет две непересекающиеся пары квазилинейных переменных и является 1-устойчивой, достигая равенства в оценке (1.8). Условие $p \leq n+t = 4+(p-2)$ тоже выполнено. Поэтому используя в лемме 2.11 для функции f только что построенную обобщенную $(2, k, p, p-2)$-подходящую матрицу для любого фиксированного k при p, удовлетворяющем неравенству $\binom{p/2}{2} \geq 2^k$, получим (m_0+s)-устойчивые функции на $\mathbf{F}_2^{n_0+s}$, достигающие границы (1.8) с любым числом s непересекающихся пар квазилинейных переменных от 0 до k для некоторых n_0 и m_0.

Теорема 2.9. *Если существует обобщенная (k, k, p, t)-походящая матрица, то можно построить последовательность m-устойчивых функций на $\mathbf{F}_2^n$, достигающих границы (1.8), при $n \to \infty$, $\frac{m}{n} \to \frac{t}{t+k}$.*

Доказательство. В примере 2 построены $(m_0 + s)$-устойчивые функции на $\mathbf{F}_2^{n_0+s}$, достигающие границы (1.8) с любым числом s непересекающихся пар квазилинейных переменных от 0 до k для некоторых n_0 и m_0. Применяя теперь r раз конструкцию 2, получим (m_0+s+rt)-устойчивую функцию на $\mathbf{F}_2^{n_0+s+r(t+k)}$, достигающую границы (1.8). Очевидно, при $r \to \infty$ имеем $\frac{m}{n} \to \frac{t}{t+k}$, что и требовалось. □

Заметим, что конструкция примера 2 не является эффективной и приведена здесь лишь для обеспечения простоты доказательства теоремы 2.9. С практической точки зрения выгоднее делать не один большой переход от k_0 к k, а много маленьких. Примеры таких последовательностей переходов приведены в [132]. Заметим также, что в примере 2 де факто использовались подходящие матрицы в их старом определении, поскольку столбцы были жестко скреплены и разделимость любых двух строк обеспечивалась всего двумя столбцами из жесткой пары. Целесообразность введения определения обобщенных подходящих матриц будет показана в следующих параграфах.

2.8 Конструкции на основе обобщенных подходящих матриц

Назовем матрицу M *разделяющей,* если в ее клетках записаны символы из множества $\{1/2, 1, *\}$, причем в каждой строке все символы $1/2$ объединены в пары, а любые две строки являются разделимыми. Таким образом, разделяющие матрицы отличаются от обобщенных подходящих матриц тем, что для них отсутствуют жесткие ограничения на число строк и значения сумм числовых символов по строкам. Если сумма числовых значений в каждой строке разделяющей матрицы равна в точности t, то такую матрицу назовем t*-разделяющей.*

Конструкция 3. Пусть разделяющая матрица M имеет h строк и сумма число-

вых символов в i-й строке равна t_i, $i = 1, \ldots, h$. Обозначим $t_{\max} = \max\limits_{1 \le i \le h} t_i$. Будем строить последовательность t-разделяющих матриц $A(t)$, $t = 0, 1, \ldots$ Обозначим через $s(t)$ число строк в матрице $A(t)$. Зададим начальные t-разделяющие матрицы $A(t)$, $t = 0, 1, \ldots, t_{\max -1}$, произвольно (например, заведомо можно взять в качестве начальной матрицы $A(t)$ строку из t единиц, хотя из практических соображений желательно, чтобы матрица $A(t)$ содержала как можно больше строк). Определим при $t \ge t_{\max}$ матрицу $A(t)$ рекурсивно следующим образом. Для строки α с номером i, $i = 1, \ldots, h$, матрицы M запишем в $A(t)$ строки, являющиеся конкатенацией α с каждой из строк матрицы $A(t - t_i)$. Поскольку строки получившейся матрицы $A(t)$, вообще говоря, могут иметь разную длину, допишем для выравнивания справа звездочки в недостающие разряды. Таким образом, легко видеть, что $A(t)$ является t-разделяющей матрицей и имеет место рекуррентное соотношение

$$s(t) = \sum_{i=1}^{h} s(t - t_i),$$

которому соответствует характеристический многочлен

$$x^{t_{\max}} - \sum_{i=1}^{h} x^{t_{\max} - t_i}. \tag{2.12}$$

Старший корень характеристического многочлена (2.12) является действительным и положительным, за исключением некоторых вырожденных случаев. Классификация вырожденных и невырожденных случаев тесно связано с условиями теоремы Перрона–Фробениуса для неотрицательных матриц [85]. В невырожденных случаях если $X_{\max}$ — старший корень характеристического многочлена (2.12), то асимптотика величины $s(t)$ имеет вид $s(t) = CX_{\max}^t(1 + o(1))$, где константа C определяется начальными условиями. Если в матрице $A(t)$ отбросить строки до ближайшей степени двойки, оставив 2^k строк, где $k = \lfloor \log_2 s(t) \rfloor = t \log_2 X_{\max}(1 + o(1))$, то получившаяся матрица является, как легко видеть, обобщенной подходящей (t, k, p, t)-матрицей, где p — число столбцов в матрице $A(t)$. Однако если нам нужна обобщенная подходящая (k_0, k, p, t)-матрица для $k = t \log_2 X_{\max}(1 + o(1))$, то нам надо отбросить в матрице $A(t)$

все строки с числом пар символов $1/2$ больше k_0 и доказать, что число таких строк асимптотически мало по сравнению с $s(t)$.

Заметим, что в [132] в качестве матрицы M фактически использовалась матрица

$$\begin{pmatrix} 1 & 1 \\ (1/2)_2 & (1/2)_1 \end{pmatrix},$$

что дало рекурректное соотношение $s(t) = s(t-2) + s(t-1)$ и характеристический многочлен $x^2 - x - 1$ со старшим корнем $X_{\max} = \frac{\sqrt{5}+1}{2} = 1.6180...$ Это дало возможность построить подходящую (k_0, k, p, t)-матрицу для $k_0 < k$, $k = \log_2 X_{\max}(1 + o(1))$, и, таким образом, с соотношением $\frac{t}{t+k} = \frac{1}{1+\log_2 X_{\max}}(1 + o(1)) = 0.5902...(1 + o(1))$.

Можно развить эту конструкцию следующим образом. Будем пользоваться нашей новой терминологией, но пока фактически не выходя за рамки старых подходящих матриц.

Конструкция 4. Пусть n четное. Объединим столбцы в пары $(2i-1, 2i)$, $i = 1, \ldots, n/2$, и включим в матрицу M_n по одному разу те и только те строки $a = (a_1, \ldots, a_n)$ из символов $1/2$ и 1, для которых $a_{2i-1} = a_{2i}$, $i = 1, \ldots, n/2$. В результате получим матрицу из $2^{n/2}$ строк. Например, при $n = 4$ имеем

$$M_n = \begin{pmatrix} 1 & 1 & 1 & 1 \\ (1/2)_2 & (1/2)_1 & 1 & 1 \\ 1 & 1 & (1/2)_4 & (1/2)_3 \\ (1/2)_2 & (1/2)_1 & (1/2)_4 & (1/2)_3 \end{pmatrix}.$$

Легко видеть, что таким образом построенная матрица M_n содержит в точности $\binom{n/2}{j}$ строк с j парами симвлов $1/2$, суммой числовых значений, равной $n - j$, и является разделяющей. Поэтому рекуррентной конструкции для $A(t)$, использующей матрицу M_n, соответствует характеристический многочлен

$$x^n - \sum_{j=0}^{n/2} \binom{n/2}{j} x^{\frac{n}{2}-j} = \left(x^2\right)^{n/2} - (x+1)^{n/2} = (x^2 - x - 1)\left(\sum_{j=0}^{\frac{n}{2}-1} x^{2(\frac{n}{2}-1-j)}(x+1)^j\right). \tag{2.13}$$

Старший корень характеристического многочлена (2.13) является действительным и положительным, что легко вытекает из теоремы Перрона–

Фробениуса. Все действительные корни многочлена в самой правой скобке в (2.13) отрицательны, поэтому старший корень всего многочлена такой же, как и у $x^2 - x - 1$. Однако конструкцию матрицы M_n можно попытаться улучшить.

Конструкция 5. Из леммы 2.9 видно, что если хотя бы для одной пары n и k, где n четно, а $0 \le k \le n/2$, построим множество V попарно разделимых строк длины n из символов множества $\{1, 1/2\}$ (без звездочек), в каждой из которых все символы $1/2$ объединены в пары, а число таких пар в точности k, и мощность множества V будет больше $\binom{n/2}{k}$, то заменяя в M_n все строки, содержащие в точности k пар символов $1/2$ на строки из V, получим матрицу M, для которой в характеристическом многочлене (2.13) коэффициент при $x^{\frac{n}{2}-k}$ по модулю увеличится, а остальные коэффициенты не изменятся. Поэтому старший корень $X_{\max}$ увеличится, а, стало быть, увеличится порядок величины $s(t)$.

Поиск множества попарно разделимых строк можно осуществлять на языке теории графов. Каждой из $\binom{n}{2k}(2k-1)!!$ возможных строк сопоставляем вершину графа, две вершины графа соединены ребром тогда и только тогда, когда соответствующие им строки разделимы. Задачу поиска максимального (большого) множества попарно разделимых строк можно решать путем поиска максимальной (большой) клики в соответствующем графе. Несложно показать, что при $k = 0, 1, 2, \frac{n}{2} - 1, \frac{n}{2}$ построить больше, чем $\binom{n/2}{k}$ попарно разделимых строк нельзя. Для $n = 10$, $k = 3$ был предпринят компьютерный поиск градиентным алгоритмом со случайным выбором первых нескольких строк. На градиентных шагах алгоритма выбиралась вершина графа (строка), соединенная с наибольшим количеством находящихся в рассмотрении вершин (т. е. еще не выбранных и не забракованных), все не соединенные с ней еще находящиеся в рассмотрении вершины после этого забраковывались. В результате работы алгоритма было получено множество из 15 строк, которое приведено ниже:

$$V = \begin{pmatrix}
(1/2)_2 & (1/2)_1 & (1/2)_4 & (1/2)_3 & (1/2)_6 & (1/2)_5 & 1 & 1 & 1 & 1 \\
(1/2)_2 & (1/2)_1 & 1 & (1/2)_6 & 1 & (1/2)_4 & 1 & (1/2)_9 & (1/2)_8 & 1 \\
(1/2)_2 & (1/2)_1 & 1 & 1 & 1 & 1 & (1/2)_9 & (1/2)_{10} & (1/2)_7 & (1/2)_8 \\
(1/2)_3 & (1/2)_5 & (1/2)_1 & 1 & (1/2)_2 & 1 & (1/2)_8 & (1/2)_7 & 1 & 1 \\
(1/2)_4 & 1 & 1 & (1/2)_1 & (1/2)_7 & (1/2)_9 & (1/2)_5 & 1 & (1/2)_6 & 1 \\
(1/2)_5 & (1/2)_3 & (1/2)_2 & 1 & (1/2)_1 & 1 & 1 & 1 & (1/2)_{10} & (1/2)_9 \\
(1/2)_6 & 1 & (1/2)_{10} & (1/2)_8 & 1 & (1/2)_1 & 1 & (1/2)_4 & 1 & (1/2)_3 \\
(1/2)_7 & (1/2)_{10} & 1 & 1 & (1/2)_6 & (1/2)_5 & (1/2)_1 & 1 & 1 & (1/2)_2 \\
(1/2)_{10} & (1/2)_7 & (1/2)_4 & (1/2)_3 & 1 & 1 & (1/2)_2 & 1 & 1 & (1/2)_1 \\
1 & (1/2)_8 & (1/2)_7 & (1/2)_9 & 1 & 1 & (1/2)_3 & (1/2)_2 & (1/2)_4 & 1 \\
1 & (1/2)_9 & 1 & 1 & (1/2)_{10} & (1/2)_8 & 1 & (1/2)_6 & (1/2)_2 & (1/2)_5 \\
1 & 1 & (1/2)_5 & (1/2)_9 & (1/2)_3 & 1 & (1/2)_{10} & 1 & (1/2)_4 & (1/2)_7 \\
1 & 1 & (1/2)_5 & 1 & (1/2)_3 & (1/2)_8 & (1/2)_{10} & (1/2)_6 & 1 & (1/2)_7 \\
1 & 1 & (1/2)_8 & (1/2)_6 & (1/2)_9 & (1/2)_4 & 1 & (1/2)_3 & (1/2)_5 & 1 \\
1 & 1 & 1 & (1/2)_7 & 1 & (1/2)_{10} & (1/2)_4 & (1/2)_9 & (1/2)_8 & (1/2)_6
\end{pmatrix}.$$

В следующей таблице на пересечении i-й строки и j-го столбца указаны номера разрядов, которые обеспечивают разделимость i-й и j-й строк из V.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	X	8 9	3 4	7 8	2 1 4 3	9 10	2 1 6 5	3 4	5 6	5 6	3 4	1 2	1 2	1 2	1 2
2		X	4 6	4 6	5 7	4 6	3 10	8 9	8 9	3 7	4 6	1 2	1 2	1 2	1 2
3			X	3 1 2 5	8 10	5 1 2 3	7 9	5 6	3 4	3 7 9 4	1 2 9 7	1 2	1 2	1 2	1 2
4				X	6 9	7 8	2 5	3 1 7 8	5 2 7 8	4 9	1 3	4 9	1 3 5 2	4 6	1 3
5					X	2 3	5 7	2 10	6 9	2 8	1 4	1 4 9 6	1 4	3 8	1 4 7 5
6						X	4 8	7 1 5 6	7 2 3 4	1 5	6 8	1 5 3 2	6 8	4 6	1 5
7							X	4 8	4 8	1 6	2 9	1 6	1 6 8 4	5 9	7 4 8 9
8								X	5 6	5 6	1 7	4 9	3 5 6 8	1 7	8 9
9									X	1 10	3 4	5 3 4 9	6 8	1 10	8 9
10										X	3 7	2 8	4 9	2 8 3 7	6 10
11											X	6 8	2 9	3 8 6 4	4 7
12												X	4 9	7 10	3 5
13													X	7 10	3 5
14														X	3 8 9 5
15															X

Конструкция 6. Заменяя в M_{10} подматрицу, составленную из 10 строк, содержащих в точности 3 пары символов $1/2$, на множество строк V, получаем матрицу M', при использовании которой в конструкции 3 для числа строк $s(t)$ матрицы $A(t)$ получается рекуррентное соотношение

$$s(t) = s(t-5) + 5s(t-6) + 15s(t-7) + 10s(t-8) + 5s(t-9) + s(t-10)$$

с характеристическим многочленом

$$x^{10} - x^5 - 5x^4 - 15x^3 - 10x^2 - 5x - 1,$$

старший корень которого равен $X_{\max} = 1.6556...$ Тогда соотношение $\frac{t}{t+k}$ для обобщенных подходящих матриц, построенных с помощью $A(t)$, стремится к $\frac{1}{1+\log_2 X_{\max}} = 0.5789...$

Остается доказать, что число строк с числом пар символов $1/2$, асимптотически превосходящим $t \log_2 X_{\max} = 0.7274...$, мало по сравнению с $s(t)$. В [132] при соответствующем доказательстве для рекуррентного соотношения $s(t) = s(t-1) + s(t-2)$ использовалась простота этого уравнения, в результате решение выписывалось почти в явном виде, что для характеристического многочлена 10-й степени представляется проблематичным. Не будем сейчас строить какой-то общей теории и для простоты изложения приведем доказательство исключительно для конструкции 6 с использованием матрицы M'.

Рекурсивная конструкция, использующая матрицу M', действует, начиная с $t = 10$. В качестве начальных матриц $A(t)$, $t = 0, 1, \ldots, 9$, можно взять произвольные t-разделяющие матрицы; главное, чтобы они не были одновременно пустыми; выбор этих матриц будет влиять на асимптотику, но не на порядок роста величины $s(t)$, поскольку асимптотика величины $s(t)$ равна $CX_{\max}^t$, и начальные матрицы влияют только на константу C. Конечно, из практических соображений лучше взять матрицы $A(t)$, $t = 0, 1, \ldots, 9$, с максимально возможным числом строк.

По построению строки матрицы $A(t)$ представляют собой всевозможные конкатенации допустимых кусков длины 10, соответствующих шагам применения рекурсивной конструкции и завершаются суффиксом, являющимся строкой одной из начальных матриц. По строке матрицы $A(t)$ ее суффикс определяется однозначно, а именно, последовательно откладывая с левого края строки куски длины 10, следим за суммой числовых символов в префиксе, и как только эта сумма становится не меньше чем $t - 9$, объявляем, что все оставшаяся правая часть строки является ее суффиксом.

Из вида M' следует, что множество допустимых кусков длины 10 состоит из 1 набора с 0 пар символов $1/2$ и суммой символов, равной 10; 5 наборов

с 1 парой символов 1/2 и суммой символов, равной 9; 10 наборов с 2 парами символов 1/2 и суммой символов, равной 8; 15 наборов с 3 парами символов 1/2 и суммой символов, равной 7; 5 наборов с 4 парами символов 1/2 и суммой символов, равной 6; 1 набора с 5 парами символов 1/2 и суммой символов, равной 5.

Обозначим через $l_j(t)$ число строк матрицы $A(t)$, содержащих в точности j пар символов 1/2.

Лемма 2.12. *Пусть $\varepsilon > 0$. Для матрицы $A(t)$ из конструкции 3, построенной с помощью матрицы M' из конструкции 6, при $j \geq (2/3+\varepsilon)t(1+o(1))$ начиная с некоторого t выполнено*

$$\frac{l_{j-2}(t+2)}{l_j(t)} > 15.$$

Доказательство. Для произвольной строки α матрицы $A(t)$ обозначим через $n_i(\alpha)$, $i = 0, 1, 2, 3, 4, 5$, число кусков длины 10 в строке α (не считая суффикса), содержащих в точности i пар символов 1/2. Пусть $j_0(\alpha)$ — число пар символов 1/2 в суффиксе α), а $t_0(\alpha)$ — сумма числовых символов в суффиксе α). Для соотношения числа $j(\alpha)$ пар символов 1/2 к сумме $t(\alpha)$ числовых символов в строке α имеем

$$\frac{j(\alpha)}{t(\alpha)} = \frac{5n_5(\alpha) + 4n_4(\alpha) + 3n_3(\alpha) + 2n_2(\alpha) + n_1(\alpha) + j_0(\alpha)}{5n_5(\alpha) + 6n_4(\alpha) + 7n_3(\alpha) + 8n_2(\alpha) + 9n_1(\alpha) + 10n_0(\alpha) + t_0(\alpha)}. \quad (2.14)$$

Нас интересуют только такие строки α из множества $A^*(t)$ «плохих» строк из $A(t)$, для которых, начиная с некоторого t, выполнено $\frac{j(\alpha)}{t(\alpha)} > \frac{2}{3} + \varepsilon'$, $0 < \varepsilon' < \varepsilon$. Поэтому, исходя из (2.14), можно считать, что $\min\limits_{\alpha \text{ из } A(t)} n_5(\alpha) \to \infty$ при $t \to \infty$ и, начиная с некоторого t, для любой строки α из $A^*(t)$ выполнено $n_5(\alpha) > n_3(\alpha) + 1$.

Обозначим через $S(t, j, n_5)$ множество строк матрицы $A(t)$, содержащих в точности j пар символов 1/2 и в точности n_5 кусков длины 10, состоящих из 5 пар символов 1/2. Для заданных j и достаточно большого t для всех значений n_5, для которых множество $S(t, j, n_5)$ непусто, заменим в каждой строке α из $S(t, j, n_5)$ один из кусков длины 10 с 5 парами символов 1/2 на допустимый кусок длины 10 с 3 парами символов 1/2. Это можно сделать $15n_5$ способами.

Тем самым получим строку матрицы $A(t+2)$, содержащую в точности $j-2$ пар символов $1/2$, которая могла быть получена таким способом из $n_3(\alpha)+1<n_5$ строк из $S(t,j,n_5)$. Поэтому множеству $S(t,j,n_5)$ сопоставлено множество строк $S(t+2,j-2,n_5-1)$, превосходящее его по мощности более чем в 15 раз. Пробегая все значения n_5, доказываем утверждение леммы. □

Лемма 2.13. *В матрице $A(t)$ из конструкции 3, построенной с помощью матрицы M' из конструкции 6, число строк с числом пар символов $1/2$, не меньшим $k_0=\lfloor 0.70t\rfloor$, асимптотически мало по сравнению с числом всех строк.*

Доказательство. Оценим отношение числа указанных в условии леммы строк к числу всех строк. Выберем d так, чтобы $d\to\infty$ при $t\to\infty$, но $\frac{\lfloor 0.70t\rfloor-2d}{t+2d}>2/3+\varepsilon$. Используя лемму 2.12, начиная с некоторого t, имеем

$$\frac{\sum\limits_{j=k_0}^{t} l_j(t)}{s(t)}<\frac{\sum\limits_{j=k_0-2d}^{t-2d} l_j(t+2d)}{15^d s(t)}<\frac{s(t+2d)}{15^d s(t)}\le\left(\frac{X_{\max}^2}{15}\right)^d(1+o(1))\to 0.$$

Лемма доказана. □

Таким образом, показано, что число строк с числом пар символов $1/2$, асимптотически превосходящим $t\log_2 X_{\max}=0.7274...$, действительно мало по сравнению с $s(t)$. Тем самым лемма 2.13 и теорема 2.9 доказывают следующую теорему.

Теорема 2.10. *Конструкция 6 с использованием матрицы M' позволяет построить последовательность m-устойчивых функций на $\mathbf{F}_2^n$, достигающих границы (1.8), для которой $m=\frac{1}{1+\log_2 X_{\max}}n(1+o(1))=0.5789...n(1+o(1))$, где $X_{\max}=1.6556...$ — старший корень характеристического многочлена $x^{10}-x^5-5x^4-15x^3-10x^2-5x-1$.*

Следствие 2.3. *Пусть α — действительная константа, $0.5789...\le\alpha\le 1$. Тогда существует последовательность m-устойчивых функций на $\mathbf{F}_2^n$, достигающих границы (1.8), для которой $\frac{m}{n}\to\alpha$.*

Следствие 2.3 легко вытекает из того факта, что, беря функции из последовательности из формулировки теоремы 2.10 и прибавляя к ним t новых линейных переменных, мы увеличиваем порядок устойчивости и число переменных на t, в то время как будет сохраняться равенство в оценке (1.8). Такие функции имеют криптографические слабости, поэтому из практических соображений разумнее использовать чуть более сложные конструкции, используя результаты и методы этой или цитированных статей.

2.9 О сложности реализации

В этом параграфе обсудим вкратце сложность реализации функций из предложенных нами конструкций. Существует предрассудок, что применение в шифрах функций от большого числа переменных практически невыгодно ввиду большой вычислительной сложности. Однако в ряде случаев, в том числе и нашем, функции от большого числа переменных могут иметь небольшую вычислительную сложность.

Покажем, как эффективно вычислить значение нашей функции ветвящейся программой. Посмотрим на функции $g(X,Y)$ и $g(X,Y,Z)$ из конструкций 1 и 2. Значение на каждом такте работы шифра надо вычислять на каком-то конкретном наборе (X,Y) или (X,Y,Z). Зная поднаборы Y и Z, мы сводим вычисление функции $g(X,Y)$ (или $g(X,Y,Z)$) к вычислению единственной подфункции $f_\sigma(X)$, где индекс σ однозначно немедленно находится из Y и Z. Для вычисления значения $f_\sigma(X)$ нам сначала надо посмотреть, как переставлялись переменные в наборе X для получения $f_\sigma(X)$ из функции, построенной на предыдущем шаге рекурсии. В доказательстве леммы 2.11 мы описывали процесс перестановки переменных в соответствии с видом соответствующей обобщенной подходящей матрицы, но не специфицировали этот процесс, поскольку для доказательства леммы он был неважен. В целях эффективности реализации этот процесс следует строго задать. Можно переставлять переменные только для того, чтобы придать последним p переменным функции необходимый статус (линейности или квазилинейности), хотя может оказаться, что в целях стойкости шифра (запутывания) полезна и более масштабная пе-

рестановка. Так или иначе, после обратной перестановки переменных получаем функцию $f'(X)$, построенную на предыдущем шаге рекурсии, и применяем к ней уже приведенные выше операции. Легко видеть, что если зафиксировать обобщенную (k, k, p, t)-подходящую матрицу, и последовательно применять ее в конструкции 2 растущее число раз, а перестановки переменных на каждом шаге ограничить последними не более чем $2p$ разрядами, то сложность вычисления значения построенной функции ветвящейся программой будет линейной.

2.10 Необходимое условие упаковки непересекающихся интервалов между двумя слоями булева куба не является достаточным

В этом параграфе рассматривается одна комбинаторная задача, тесно связанная с существованием и построением *подходящих матриц,* применявшихся в параграфах 2.5 и 2.6 для построения устойчивых функций, достигающих верхней границы нелинейности. Как несложно следует из геометрической интерпретации подходящих матриц на языке булева куба и непересекающихся подкубов в нем, данной в конце параграфа 2.6, для существования подходящей (k_0, k, p, t)-матрицы необходимо существование натуральных чисел C_0, C_1, ..., C_{k_0}, таких что

$$\sum_{j=0}^{k_0} C_j \geq 2^k, \tag{2.15}$$

и удовлетворяющих кроме того для любого i неравенству

$$\sum_{j=0}^{k_0} C_j \binom{p - \lfloor \frac{t+j}{2} \rfloor}{i - \lfloor \frac{t-j}{2} \rfloor} \leq \binom{p}{i}. \tag{2.16}$$

Здесь C_j — это число строк подходящей матрицы ровно с j единицами; неравенство (2.16) получается из подсчета общего числа точек i-го уровня булева куба, содержащегося во всех подкубах, соответствующих строкам подходящей матрицы, принимая во внимание, что если размерность подкуба мала, то его

можно расширить, заменив некоторые звездочки двойками. На самом деле, достаточно считать коэффициенты C_j ненулевыми только для j той же четности, что и t, а также для $j = k_0$.

Несуществование набора натуральных чисел C_0, C_1, ..., C_{k_0}, удовлетворяющих неравенствам (2.15) и (2.16) влечет за собой несуществование подходящей (k_0, k, p, t)-матрицы. Но означает ли, что подходящая (k_0, k, p, t)-матрица с соответствующим распределением строк по числу единиц в них существует, если набор таких чисел найдется? В этом параграфе показывается, что ответ на этот вопрос вообще говоря отрицательный даже если ненулевым является только один из коэффициентов C_j.

Помимо вышесказанного результаты этого параграфа имеют и общекомбинаторное значение. В этом параграфе устанавливается максимальное число непересекающихся граней с нижним уровнем $l_1 = 1$ и верхним уровнем l_2 в булевом кубе B^n и строится пример, показывающий, что попытка казалось бы естественного обобщения теоремы о максимальном паросочетании в двух соседних слоях булева куба является, вообще говоря, несостоятельной. Результаты параграфа опубликованы в работе автора [163].

Дадим теперь определения комбинаторных объектов, о которых пойдет речь в этом параграфе, и которые уже затрагивались мимоходом выше, более строго.

Вектор $(x_1, \ldots, x_n)$, координаты которого принимают значения из множества $\{0, 1\}$ называется *двоичным набором.* Весом $|x|$ двоичного набора x называется число его компонент, равных единице. Множество $\{0, 1\}^n$ всех двоичных наборов длины n называется *булевым кубом* B^n. Множество всех двоичных наборов длины n с весом l называется *l-м слоем булева куба* и обозначается через B_l^n. Наборы x' и x'' из B^n называются *соседними,* если они различаются ровно в одной компоненте. Неупорядоченная пара соседних вершин называется *ребром* булева куба. Множество $(B^n)_{i_1 \ldots i_k}^{\sigma_1 \ldots \sigma_k}$ всех наборов из B^n, у которых $x_{i_j} = \sigma_j$, $j = 1, \ldots, k$, называется *гранью* куба B^n. Число k называется *рангом грани,* а число $(n - k)$ — *размерностью грани.* Грань $(B^n)_{i_1 \ldots i_k}^{\sigma_1 \ldots \sigma_k}$ можно задать как набор $b = b((B^n)_{i_1 \ldots i_k}^{\sigma_1 \ldots \sigma_k}) = (b_1, \ldots, b_n)$, компонентами которого являются символы из множества $\{0, 1, *\}$, причем $b_i = \sigma_s$, если индекс i совпадает с индексом i_s, и $b_i = *$, если индекс i отличен от всех индексов $i_1, \ldots, i_k$. Очевидно, что набор

b содержит ровно $n-k$ звездочек. Число единиц в наборе b назовем *нижним уровнем грани,* а суммарное число единиц и звездочек в наборе b назовем *верхним уровнем грани.* Две грани назовем *непересекающимися,* если они не содержат общих наборов.

Утверждение 2.4. *Грани B' и B'' не пересекаются тогда и только тогда, когда в соответствующих им наборах $b(B')$ и $b(B'')$ найдется такая компонента, что один из этих наборов содержит в этой компоненте единицу, а другой — ноль.*

Доказательство. Если бы такой компоненты не нашлось, то доопределяя звездочки в наборах $b(B')$ и $b(B'')$ нулями и единицами, можно было бы получить одинаковые наборы, что означало бы то, что грани B' и B'' пересекаются. □

Утверждение 2.5. *Пусть C, l_1, l_2 и n — целые неотрицательные числа и $0 \le l_1 \le l_2 \le n$. Для того, чтобы в булевом кубе B^n существовало C непересекающихся граней с нижним уровнем l_1 и верхним уровнем l_2, необходимо, чтобы*

$$\forall i \qquad C\binom{l_2-l_1}{i-l_1} \le \binom{n}{i}. \tag{2.17}$$

Доказательство. Легко видеть, что i-й слой булева куба содержит $\binom{n}{i}$ двоичных наборов. В то же время, в этот слой должны попасть $\binom{l_2-l_1}{i-l_1}$ наборов каждой из C граней. □

Широко известная **теорема о существовании максимального паросочетания в двух соседних слоях булева куба**, доказанная в [67], утверждает, что для любых двух соседних слоев $B^n_{l_1}$ и $B^n_{l_1+1}$ булева куба B^n можно составить попарно непересекающиеся двухэлементные множества (x', x''), $x' \in B^n_{l_1}$, $x'' \in B^n_{l_1+1}$, являющиеся ребрами булева куба, в количестве, равном мощности меньшего из этих двух слоев (говоря языком теории графов, в двудольном графе, образованном двумя соседними слоями булева куба, существует паросочетание, покрывающее наименьшую долю вершин). Ребро булева куба можно рассматривать как грань размерности 1. Поэтому можно переформулировать теорему о существовании максимального паросочетания в терминах нашего утверждения 2.5.

Утверждение 2.6. *Для того, чтобы в булевом кубе B^n существовало C непересекающихся граней с нижним уровнем l_1 и верхним уровнем l_2, $l_2 - l_1 = 1$, условие (2.17) является необходимым и достаточным.*

В связи с вышесказанным естественно возникает вопрос, не является ли необходимое условие (2.17) в утверждении 2.5 также и достаточным при любых C, l_1, l_2 и n. Ниже будет показано, что это, вообще говоря, не так.

Теорема 2.11. *Максимальное число непересекающихся граней с нижним уровнем $l_1 = 1$ и верхним уровнем l_2 в булевом кубе B^n равно* $\min\{2(n - l_2) + 1, n\}$.

Доказательство. Пусть в булевом кубе B^n существует C непересекающихся граней $B_1, \ldots, B_C$ с нижним уровнем $l_1 = 1$ и верхним уровнем l_2. Образуем матрицу B с C строками и n столбцами, записав в строках этой матрицы наборы $b_i = b(B_i)$. Заметим, что каждая строка b_i матрицы B содержит ровно одну единицу и ровно $n - l_2$ нулей, остальные символы — звездочки. Две разные строки матрицы B не могут содержать единицу в одном и том же столбце, потому что в противном случае не нашлось бы такого столбца, в котором одна из этих строк содержала единицу, а другая — ноль, и тогда в силу утверждения (2.17) грани, соответствующие этим двум строкам, пересекались бы. Поэтому все единицы в матрице B содержатся в разных столбцах и, следовательно, $C \leq n$. Далее, каждая строка b_i матрицы B содержит ровно $n - l_2$ нулей, которые обеспечивают в силу утверждения (2.17) непересечение грани B_i максимум с $n - l_2$ другими гранями. Все нули матрицы B обеспечивают непересечение между собой максимум $C(n - l_2)$ пар граней. Всего пар граней ровно $\frac{C(C-1)}{2}$. Поэтому $C(n - l_2) \geq \frac{C(C-1)}{2}$ и, следовательно, $C \leq 2(n - l_2) + 1$. Таким образом, $C \leq \min\{2(n - l_2) + 1, n\}$.

С другой стороны, пусть $C = \min\{2(n - l_2) + 1, n\}$. Образуем квадратную матрицу порядка C, записав в ее строки всевозможные циклические сдвиги строки

$$(1\underbrace{00\ldots0}_{n-l_2}\underbrace{*\,*\cdots*}_{C-n+l_2-1}).$$

Если $C < n$, то добавим недостающие до n столбцы, целиком заполненные звездочками. Несложно убедиться, что в получившейся матрице B для любых двух строк найдется такой столбец, в котором одна из этих строк содержит единицу, а другая — ноль. Поэтому по утверждению (2.17) строки матрицы B задают C непересекающихся граней в булевом кубе B^n с нижним уровнем $l_1 = 1$ и верхним уровнем l_2. □

Из соображений симметрии из теоремы 2.11 немедленно вытекает следующее следствие.

Следствие 2.4. *Максимальное число непересекающихся граней с нижним уровнем* l_1 *и верхним уровнем* $l_2 = n-1$ *в булевом кубе* B^n *равно* $\min\{2l_1+1, n\}$.

Теорема 2.12. *Необходимое условие (2.17) в утверждении 2.5 не является достаточным.*

Доказательство. Положим $n = 14, l_1 = 1, l_2 = 12, C = 6$. Непосредственной проверкой несложно убедиться в справедливости условия (2.17). В то же время в силу теоремы 2.11 в булевом кубе B^{14} найдется не более пяти непересекающихся граней с нижним уровнем 1 и верхним уровнем 12. □

Другим набором параметров, доказывающим теорему 2.12, является следующий: $n = 14$, $l_1 = 1$, $l_2 = 11$, $C = 8$. Условие (2.17) соблюдается, в то время как в силу теоремы 2.11 в булевом кубе B^{14} найдется не более семи непересекающихся граней с нижним уровнем 1 и верхним уровнем 11. Этот пример интересен тем, что здесь C является степенью двойки, что требуется в определении подходящей матрицы.

Интересно было бы определить более точно, в каких случаях условие (2.17) является достаточным, а в каких — нет. В частности, заслуживают внимания случаи, когда $l_2 - l_1 = 2$, а также когда $l_1 = 2$.

2.11 Упаковки продуктов

Пусть $n, k \in \mathbf{Z}$, $0 \leq 2k \leq n$. Будем называть (n,k)-продуктом (или просто *продуктом*) произведение двучленов: $P = \prod_{i=1}^{k}(x_{i,1} + x_{i,2})$, где $x_{i,1}, x_{i,2}$, $i = 1, \ldots, k$, — неповторяющиеся переменные из множества $x_1, \ldots, x_n$. *Разложением* (n,k)-продукта P назовем совокупность 2^k мономов длины k, получающихся после раскрытия скобок в продукте P. Считаем, что разложением $(n,0)$-продукта является моном длины 0. Будем говорить, что разложение суммы продуктов $\sum_{i=1}^{s} P_i$ *несократимо*, если разложения никаких двух продуктов P_i и P_j, $i \neq j$, не содержат общих мономов. Число s продуктов в сумме назовем *длиной* суммы продуктов. Через $A_{n,k}$ обозначим максимально возможное значение длины суммы (n,k)-продуктов с несократимым разложением.

В [184] автором были указаны следующие несложные соотношения на величины $A_{n,k}$.

Утверждение 2.7. *Справедливы следующие соотношения:*
а) $A_{n,k} \leq \frac{\binom{n}{k}}{2^k}$;
б) $A_{n,k} \leq \binom{n}{2k}$;
в) $A_{n,k} \geq \binom{\lfloor \frac{n}{2} \rfloor}{k}$;
г) $A_{n,k} \geq A_{n-2,k} + A_{n-2,k-1}$ *при* $2 \leq 2k \leq n-2$;
д) $A_{n,0} = 1$;
е) $A_{n,1} = \lfloor \frac{n}{2} \rfloor$;
ж) $A_{n,2} = \binom{\frac{n}{2}}{2}$ *при четном* n;
з) $A_{n,\lfloor \frac{n}{2} \rfloor} = 1$;
и) $A_{n,\frac{n}{2}-1} = \frac{n}{2}$ *при четном* n;
к) $A_{10,3} = 15$.

Пример суммы продуктов, на которой достигается значение $A_{10,3} = 15$ (в несколько иной терминологии этот пример приведен автором в [140] и в параграфе 2.8 настоящей диссертации):

$$(x_1+x_2)(x_3+x_4)(x_5+x_6)+(x_1+x_2)(x_4+x_6)(x_8+x_9)+(x_1+x_2)(x_7+x_9)(x_8+x_{10})+$$

$$+(x_1+x_3)(x_2+x_5)(x_7+x_8)+(x_1+x_4)(x_5+x_7)(x_6+x_9)+(x_1+x_5)(x_2+x_3)(x_9+x_{10})+$$
$$(x_1+x_6)(x_3+x_{10})(x_4+x_8)+(x_1+x_7)(x_2+x_{10})(x_5+x_6)+(x_1+x_{10})(x_2+x_7)(x_3+x_4)+ \quad (2.18)$$
$$+(x_2+x_8)(x_3+x_7)(x_4+x_9)+(x_2+x_9)(x_5+x_{10})(x_6+x_8)+(x_3+x_5)(x_4+x_9)(x_7+x_{10})+$$
$$+(x_3+x_5)(x_6+x_8)(x_7+x_{10})+(x_3+x_8)(x_4+x_6)(x_5+x_9)+(x_4+x_7)(x_6+x_{10})(x_8+x_9).$$

Верхняя оценка в утверждении 2.7, к) следует из оценки утверждения 2.7, а). Пример (2.18) можно рассматривать как *совершенную упаковку* продуктов, поскольку каждый из $\binom{10}{3} = 120 = 15 \cdot 2^3$ мономов длины 3 от 10 переменных встречается в разложении ровно одного продукта.

Совершенную упаковку (n, k)-продуктов можно рассматривать как разновидность комбинаторных дизайнов, близкую вист-турнирам и их обобщениям [36].

Исследованию упаковок продуктов (в частности, совершенных упаковок продуктов) и получению оценок на величины $A_{n,k}$ посвящена работа [142], в которой представлены рекурсивные конструкции упаковок продуктов (включая совершенные упаковки продуктов) и соответствующие рекурсивные оценки на их длину. В [142] доказаны следующие утверждения.

Утверждение 2.8. *Справедливо неравенство*

$$A_{n_1+n_2,k} \geq \sum_{i=0}^{k} A_{n_1,i} \cdot A_{n_2,k-i}.$$

Утверждение 2.9. *Справедливо неравенство*

$$A_{n-1,k-1} \geq \frac{2k}{n} A_{n,k}.$$

Следствие 2.5. *Если существует совершенная упаковка (n, k)-продуктов, то существует и совершенная упаковка $(n-1, k-1)$-продуктов.*

Теорема 2.13. *Если существует совершенная упаковка (n, k)-продуктов, $k \geq 1$, то*

$$n \equiv k - 1 \pmod{2^{d_k}}$$

где $d_k = \max\{d_{k-1}, k + p(k)\}$, $d_0 = 0$, $p(k)$ — максимальная степень двойки, которая делит k.

Теорема 2.14. *Пусть существуют совершенная упаковка (n_1, k)-продуктов и совершенная упаковка (n_2, k)-продуктов. Тогда существует и совершенная упаковка $(n_1 + n_2 - k + 1, k)$-продуктов.*

Теорема 2.15. *Совершенная упаковка $(n, 3)$-продуктов, $n \geq 6$, существует тогда и только тогда, когда $n \equiv 2 \pmod 8$.*

Следствие 2.6. *Совершенная упаковка $(n, 2)$-продуктов, $n \geq 4$, существует тогда и только тогда, когда $n \equiv 1 \pmod 8$.*

Утверждение 2.10. *Имеет место следующее рекуррентное неравенство:*

$$A_{n_1+n_2-k+1,k} \geq \sum_{i=0}^{k} A_{n_1-k+i,i} \cdot A_{n_2-i,k-i}.$$

Теорема 2.16. *Величина $A_{n,2}$ выражается следующими рекуррентными неравенствами:*

$$A_{n,2} = \begin{cases} \frac{n(n-2)}{8} & \text{if } n \text{ is even,} \\ \frac{n(n-1)}{8} & \text{if } n \equiv 1 \pmod 8, \\ \frac{(n+2)(n-3)}{8} & \text{if } n \equiv 3 \pmod 8, \\ \frac{(n+3)(n-4)}{8} & \text{if } n \equiv 5 \pmod 8, \\ \frac{(n+1)(n-2)}{8} - 1 & \text{if } n \equiv 7 \pmod 8. \end{cases}$$

2.12 О возможностях метода из параграфа 2.8

В начале этого параграфа вкратце подведем итоги всей главы.

Нелинейность и корреляционная иммунность (m-устойчивость) относятся к числу наиболее важных криптографических характеристик булевых функций, обладание которыми необходимо для противостояния криптосистем, использующих булевы функции, в частности, шифров, линейным, корреляционным и другим видам криптографических атак. поэтому крайне желательно, чтобы функции, использующиеся в шифрах, обладали одновременно высокими нелинейностью и устойчивостью. В 2000 в [159, 134, 109, 126] была доказана верхняя оценка (1.7) нелинейности m-устойчивых функций на $\mathbf{F}_2^n$:

$$\mathrm{nl}(f) \leq 2^{n-1} - 2^{m+1} \tag{1.7}$$

при $m \leq n-2$ (см. параграф 1.4), в которой если и может достигаться равенство, то только при $\frac{n-3}{2} \leq m \leq n-2$. Одновременно в [159, 134] были построены функции, для которых достигалось равенство в (1.7) при $\frac{2n-7}{3} \leq m \leq n-2$. Отсюда актуальной стала задача построения функций, достигающих равенства в оценке (1.7) (как говорили, построения функций с максимально возможной нелинейностью). После ряда последовательных улучшений в 2001 Федорова и Таранников получили [132] лучший на долгое время результат: используя подходящие матрицы (см. определение 2.1) построили m-устойчивые функции на $\mathbf{F}_2^n$ с максимально возможной нелинейностью для $0.5902...n(1 + o(1)) \leq m \leq n - 2$, но одновременно показали, что с помощью использовавшейся техники подходящих матриц улучшить константу 0.5789... нельзя. В 2014 году автор обобщил понятие подходящей матрицы, введя обобщенные подходящие матрицы (см. параграф 2.7) и в [140] построил m-устойчивые функции от n переменных с нелинейностью, достигающей равенства в оценке (1.7), для которых $\frac{m}{n} \to \alpha$, где α — действительная константа, $0.5789... \leq \alpha \leq 1$ (см. следствие 2.3). Поскольку $0.5789... < 0.5789...$, метод с использованием обобщенных подходящих матриц позволил построить функции, которые нельзя было построить, используя просто подходящие матрицы. Тем не менее, оставался открытым вопрос о возможности достичь для отношения $\frac{m}{n}$ величины $\frac{1}{2}$.

С практической точки зрения важна не столько нелинейность, сколько *относительная нелинейность,* т. е. величина $\frac{\mathrm{nl}(f)}{2^n}$, точнее, отклонение относительной нелинейности от 0.5. Отклонение относительной нелинейности любой булевой функции на $\mathbf{F}_2^n$ от 0.5 не меньше $\frac{1}{2^{\frac{n}{2}+1}}$, в то же время, если построить m-устойчивую функцию на $\mathbf{F}_2^n$ с максимально возможной нелинейностью $2^{n-1}-2^{m+1}$ при m, близком к $0.5n$, то отклонение ее относительной нелинейности от 0.5 будет равно $\frac{1}{2^{n-m-1}}$, т. е. близко к нижней оценке наилучшего возможного отклонения. Поэтому прогресс в задаче построения m-устойчивых функций на $\mathbf{F}_2^n$ с максимально возможной нелинейностью $2^{n-1}-2^{m+1}$ при m, близких к $0.5n$, по прежнему является важным, потому что позволит соединить нелинейность, близкую к оптимальной, с очень высокой устойчивостью. Область значений параметров, для которых построены функции, на которых достигается равенство в (1.7), неоднократно расширялась. В 2014 году с помощью техники *обобщенных подходящих матриц* в [140] построены функции, достигающие равенства в (1.7), для $m \geq 0.5789...n(1+o(1))$. В [184] техника рекурсивного построения обобщенных подходящих матриц была сформулирована на языке несократимых разложений сумм продуктов.

Пусть $n, C_k \in \mathbf{N}$, $C_k \leq A_{n,k}$, $k = 0, 1, 2, \ldots, \lfloor \frac{n}{2} \rfloor$, где $A_{n,k}$ — максимально возможное значение длины суммы (n,k)-продуктов с несократимым разложением. Положим $C = \frac{1}{1+\log_2 X_{max}}$, где X_{max} — старший корень многочлена $x^n - \sum\limits_{k=0}^{\lfloor \frac{n}{2} \rfloor} C_k x^k$. Тогда для функций, построенных с помощью с помощью обобщенных подходящих матриц аналогично конструкции 6 из параграфа 2.8, выполнено $\frac{m}{n} \leq C$.

В связи с этим становится понятно, что для того, чтобы с помощью техники рекурсивного построения обобщенных подходящих матриц работ [140] и [184] была возможность построить m-устойчивые функции на $\mathbf{F}_2^n$ с оптимальной нелинейностью с отношением m/n, стремящимся к 0.5, необходимо, чтобы старший корень X_{max} уравнения

$$x^n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} A_{n,k} x^k \tag{2.19}$$

с ростом n стремился к 2.

В работе [185] автор показал, что X_{max} не стремится к 2.

Пусть $k/n \to \lambda$; предположим, что k-е слагаемое — максимальное в правой части (2.19).

Из $A_{n,k} \le \frac{\binom{n}{k}}{2^k}$ следует, что $X^n_{max} \le X^k_{max} \cdot \frac{2^{nH(k/n)}}{2^k} \cdot Pol(n)$, т. е.

$$X_{max} \le 2^{(H(\lambda)-\lambda)/(1-\lambda)}.$$

Аналогично из $A_{n,k} \le \binom{n}{2k}$ следует, что $X^n_{max} \le X^k_{max} \cdot 2^{nH(2k/n)} \cdot Pol(n)$, т. е.

$$X_{max} \le 2^{H(2\lambda)/(1-\lambda)}.$$

Таким образом, $X_{max} \le \min\{2^{(H(\lambda)-\lambda)/(1-\lambda)}, 2^{H(2\lambda)/(1-\lambda)}\}$.

Равенство $H(\lambda) - \lambda = H(2\lambda)$ достигается при $\frac{H(\lambda)-\lambda}{1-\lambda} = 0.97896...$, что с учетом поведения графиков функций дает $X_{max} \le 1.971044...$

Отсюда следует, что ограничиваясь средствами, предложенными в [140] и [184], нельзя построить m-устойчивые функции от n переменных с оптимальной нелинейностью при $m/n \le \frac{1}{1+\log_2(1.971044...)}(1+o(1)) = 0.505316...(1+o(1))$. Впрочем, сказанное не исключает дальнейшего совершенствования методов. Заметим, что отношение m/n, близкое к 0.505316..., для многих практических целей является хорошим, поэтому построения в рамках техники [184] тоже представляют интерес.

3 Свойства корреляционно-иммунных и устойчивых булевых функций

В предыдущей главе 2 была изучена связь корреляционной иммунности булевых функций с их нелинейностью. Однако существует ряд других важных характеристик булевых функций, важных при использовании булевой функции в качестве криптографического примитива в системах защиты информации. Поэтому начинающаяся с этих строк глава 3 посвящена анализу взаимосвязей корреляционной иммунности с другими криптографически важными свойствами булевых функций, в частности, с их автокорреляционными характеристиками. Главным методом изучения в этой главе является спектральный анализ, т. е. использование коэффициентов Уолша и их свойств, а также автокорреляционных коэффициентов.

3.1 Об автокорреляционных свойствах корреляционно-иммунных функций

Дифференциальные (или автокорреляционные) характеристики (критерий распространения, критерий SAC, абсолютная автокорреляционная характеристика, индикатор «сумма квадратов» и другие) наряду с нелинейностью считаются важнейшими свойствами, которыми должны обладать функции, использующиеся в блоковых шифрах. В последних исследованиях дифференциальные характеристики рассматриваются как важные и для потоковых шифров.

Многие работы (например, [46]) показывают, что корреляционная иммунность и автокорреляционные характеристики находятся в сильном противоречии, т. е. хорошие значения этих величин плохо совместимы. Результаты этого

параграфа подтверждают это. Тем не менее оказывается, что автокорреляционные коэффициенты булевой функции являются мощным средством для изучения корреляционной иммунности и других свойств даже без прямого отношения к дифференциальным характеристикам. Результаты последующих параграфов подтверждают это.

В этом параграфе доказывается новая нижняя оценка для абсолютной автокорреляционной характеристики [124] устойчивых функций.

В [127] Зенг и Занг доказали, что для уравновешенной корреляционно-иммунной порядка m булевой функции f на $\mathbf{F}_2^n$ справедливо неравенство $\Delta_f \geq \frac{2^n}{2^{n-m}-1}$. Из него сразу следует, что $\Delta_f \geq 2^m + 2$. В этом параграфе в теореме 3.2 доказывается, что $\Delta_f \geq \left(\frac{2m-n+3}{n+1}\right) 2^n$. Эта оценка является намного более сильной для высоких порядков устойчивости (при $m > (n-3)/2$).

Результаты параграфа опубликованы в работе автора [166] и входят в состав работы [136].

Докажем сначала важную техническую формулу. Заметим, что эта формула может быть выведена из соотношения

$$W_f^2(x) = \sum_{u \in \mathbf{F}_2^n} (-1)^{<x,u>} \Delta_f(u),$$

которое приводится в [46] и [45], однако здесь будет приведено прямое доказательство.

Теорема 3.1. $\Delta_f(u) = -2^n + 2^{1-n} \sum\limits_{\substack{x \in \mathbf{F}_2^n \\ <x,u> \equiv 0 \pmod 2}} W_f^2(x).$

Доказательство. Если $u = 0$, то, очевидно, $\Delta_f(u) = 2^n$, и

$$\sum_{\substack{x \in \mathbf{F}_2^n \\ <x,u> \equiv 0 \pmod 2}} W_f^2(x) = \sum_{x \in \mathbf{F}_2^n} W_f^2(x) = 2^{2n},$$

поэтому равенство выполняется. Таким образом, можно считать, что $u \neq 0$.

Далее,

$$\sum_{\substack{x\in\mathbf{F}_2^n \\ <x,u>\equiv 0 \pmod 2}} W_f^2(x) = \sum_{\substack{x\in\mathbf{F}_2^n \\ <x,u>\equiv 0 \pmod 2}} \left(\sum_{y\in\mathbf{F}_2^n} (-1)^{f(y)+<x,y>} \right)^2 =$$

$$\sum_{\substack{x\in\mathbf{F}_2^n \\ <x,u>\equiv 0 \pmod 2}} \left(2^n + \sum_{y'\neq y''\in\mathbf{F}_2^n} (-1)^{f(y')+f(y'')+<x,y'+y''>} \right) =$$

$$2^{2n-1} + \sum_{y'\neq y''\in\mathbf{F}_2^n} (-1)^{f(y')+f(y'')} \sum_{x\in\mathbf{F}_2^n} \left(\tfrac{1}{2} + \tfrac{1}{2}(-1)^{<x,u>}\right) (-1)^{<x,y'+y''>} =$$

$$2^{2n-1} + \tfrac{1}{2} \sum_{y'\neq y''\in\mathbf{F}_2^n} (-1)^{f(y')+f(y'')} \cdot$$

$$\cdot \left(\sum_{x\in\mathbf{F}_2^n} (-1)^{<x,y'+y''>} + \sum_{x\in\mathbf{F}_2^n} (-1)^{<x,u+y'+y''>} \right) =$$

$$2^{2n-1} + \tfrac{1}{2} \sum_{\substack{y',y''\in\mathbf{F}_2^n \\ y'+y''=u}} (-1)^{f(y')+f(y'')} \left(0 + \sum_{x\in\mathbf{F}_2^n} 1 \right) =$$

$$2^{2n-1} + 2^{n-1} \sum_{y\in\mathbf{F}_2^n} (-1)^{f(y)+f(y+u)} = 2^{2n-1} + 2^{n-1}\Delta_f(u).$$

□

Обозначим через e^i вектор длины n, который имеет единицу в i-й компоненте и нули во всех остальных компонентах.

Лемма 3.1. *Пусть f является m-устойчивой булевой функцией на $\mathbf{F}_2^n$. Тогда $\Delta_f \geq \left(\frac{2m-n+2}{n}\right) 2^n$.*

Доказательство. Образуем матрицу B с n столбцами, выписывая по строкам B каждый двоичный набор u из $\mathbf{F}_2^n$ в точности $W_f^2(u)$ раз. По равенству Парсеваля матрица B содержит в точности 2^{2n} строк. По спектральной характеризации [68] каждая строка матрицы B содержит не более $n-m-1$ нулей. Следовательно, общее число нулей в B не более $(n-m-1)2^{2n}$. Поэтому, найдется некоторый i-й столбец в B, который содержит не более $\frac{(n-m-1)2^{2n}}{n}$ нулей. Из построения следует, что $\sum\limits_{\substack{x\in\mathbf{F}_2^n \\ x_i=0}} W_f^2(x) \leq \frac{(n-m-1)2^{2n}}{n}$. Тогда по теореме 3.1 имеем

$$\Delta_f(e^i) = -2^n + 2^{1-n} \sum_{\substack{x\in\mathbf{F}_2^n \\ x_i=0}} W_f^2(x) \leq -2^n + \frac{(n-m-1)}{n} 2^{n+1} \leq \frac{(n-2m-2)}{n} 2^n.$$

Отсюда следует, что $\Delta_f \geq \left(\frac{2m-n+2}{n}\right) 2^n$. □

Нижняя оценка в лемме 3.1 может быть улучшена. Следующая теорема дает рекордную нижнюю оценку для абсолютной автокорреляционной характеристики m-устойчивой функции от n переменных при $m > (n-3)/2$.

Теорема 3.2. *Пусть f является m-устойчивой булевой функцией на $\mathbf{F}_2^n$. Тогда $\Delta_f \geq \left(\frac{2m-n+3}{n+1}\right) 2^n$.*

Доказательство. Предположим, что в доказательстве леммы 3.1 матрица B содержит в точности $h2^{2n}$ строк с менее чем $n-m-1$ нулями для некоторого действительного h. Тогда повторяя аргументы из доказательства леммы 3.1, имеем

$$\Delta_f \geq \left(\frac{2m-n+2+2h}{n}\right) 2^n. \tag{3.1}$$

В то же самое время нетрудно видеть, что

$$\Delta_f((1\ldots1)) = -2^n + 2^{1-n} \sum_{\substack{x\in\mathbf{F}_2^n \\ |x|\equiv 0 \pmod 2}} W_f^2(x)$$

и

$$\Delta_f \geq |\Delta_f((1\ldots1))| \geq (1-2h)2^n. \tag{3.2}$$

Правая часть в (3.1) возрастает по h в то время как правая часть в (3.2) убывает по h. Правые части в (3.1) и (3.2) равны при

$$h = \frac{n-m-1}{n+1}.$$

Поэтому,

$$\Delta_f \geq \left(\frac{2m-n+3}{n+1}\right) 2^n. \tag{3.3}$$

□

Несколько позднее Майтра в работе [82] улучшил оценку Зенга и Занга и для малых порядков устойчивости (для $m \leq \frac{n}{2}-2$). Более точно, Майтра доказал, что

$$\Delta_f \geq \sqrt{\frac{1}{2^n-1}} \cdot \frac{2^{2n} \sum\limits_{i=0}^{m} \binom{n}{i}}{2^n - \sum\limits_{i=0}^{m} \binom{n}{i}}. \tag{3.4}$$

Оценивать качество формулы (3.4) достаточно трудно ввиду ее громоздкости, однако вычисления, проведенные в [82] показывают, что она существенно превосходит оценку Зенга и Занга. Заметим, что при $m > (n-3)/2$ наша оценка (3.3) все равно лучше.

3.2 Верхняя оценка для числа нелинейных переменных в устойчивых булевых функциях высокого порядка

В этом параграфе доказывается верхняя оценка для числа нелинейных переменных в устойчивых булевых функциях высокого порядка. Функции, которые зависят от некоторых переменных линейно, являются во многих приложениях криптографически слабыми, поэтому их использование на практике нежелательно. Кроме того, такие функции не представляют интереса и с теоретической точки зрения, поскольку линейные переменные можно просто отбросить (удалив их в полиноме функции или, что то же самое, подставив вместо них константу 0). Тогда и число переменных функции, и степень ее устойчивости уменьшатся на число отброшенных линейных переменных (здесь мы как и во всей работе считаем уравновешенную неустойчивую функцию 0-устойчивой, а неуравновешенную функцию — (-1)-устойчивой) и задача сведется к исследованию функции без линейных переменных. Поэтому важным вопросом является здесь существование устойчивых функций, которые зависят от всех своих переменных нелинейно. Первоначально автором было доказано [157, 156, 133], что для любого натурального k существует минимальное неотрицательное целое $p(k)$, любая $(n-k)$-устойчивая функция от n переменных зависит нелинейно от не более чем $p(k)$ переменных. Позднее в [164] и [161] автором совместно с его студентом Денисом Кириенко было доказано, что $p(k) \leq (k-1)4^{k-2}$. В этом параграфе доказывается оценка $p(k) \leq (k-1)2^{k-2}$, полученная автором в работе [166] (результаты этой работы содержится в также в [136]). При $k = 3$ эта оценка достигается на функции $f_3(x_1, \ldots, x_4)$, приведенной в параграфе 2.3. При $k = 4$ оценка уже не точна, поскольку в работах [164] и [161] показано, что $p(4) = 10$; однако отличается от нижней оценки $p(k) \geq 3 \cdot 2^{k-2} - 2$, достигаемой на специальной последовательности функций, впервые построенной автором в работе [158] и приведенной в параграфе 2.3, в линейное по k число раз. Результаты параграфа опубликованы в работе автора [166] и входят в состав работы [136].

Помимо представления булевой функции полиномом Жегалкина, существует также единственное представление булевой функции f мультилинейным полиномом над $\mathbf{R}$. Степень этого полинома (т. е. длина самого длинного монома) называется *действительной степенью функции* f. В 1994 году Нисан и Сегеди доказали [88], что у булевой функции с действительной степенью не выше d число существенных переменных не превосходит $d \cdot 2^{d-1}$. Оказалось, что этот результат эквивалентен результату теоремы 3.4. Насколько известно автору, факт эквивалентности этих задач в явном виде до сих пор не опубликован. В неявном виде указание на эквивалентность задач было опубликовано в 2014 году О'Доннеллом в качестве непронумерованного замечания между утверждениями 6.23 и 6.24 в монографии [89].

В 2020 году результат Нисана–Сегеди был усилен до $n \leq C \cdot 2^d$, где $C = 6.614\ldots$ [53] и $C = 4.416\ldots$ [122]. Заметим, что это автоматически означает усиление оценки теоремы 3.4 до $n \leq C \cdot 2^{k-1}$ с теми же самыми значениями C. Отметим, что авторы статьи [53] наряду с верхней оценкой $n \leq 6.614 \cdot \ldots \cdot 2^d$, доказывают также и нижнюю, эквивалентную оценке автора $p(k) \geq 3 \cdot 2^{k-2} - 2$ и достигающуюся на той же самой последовательности функций (только заданной в другой форме). Это свидетельствует о том, что эквивалентность двух указанных выше задач и статьи по параллельной тематике были еще в 2020 году неизвестны даже некоторым активно работающим в этой области исследователям.

Следующая лемма очевидна.

Лемма 3.2. *Пусть f является булевой функцией на $\mathbf{F}_2^n$, $\deg(f) \geq 1$. Тогда* $\deg(f(x) \oplus f(x + e^i)) \leq \deg(f(x)) - 1$.

Автокорреляционные коэффициенты и теорема 3.1 применяются при доказательстве следующей леммы.

Лемма 3.3. *Пусть f является булевой функцией на $\mathbf{F}_2^n$, $\deg(f, x_i) \geq 2$. Тогда* $\sum\limits_{\substack{u \in \mathbf{F}_2^n \\ u_i = 0}} W_f^2(u) \geq 2^{2n - \deg(f) + 1}$.

Доказательство. По теореме 3.1, используя леммы 1.3 и 3.2, имеем

$$-2^n + 2^{1-n} \sum_{\substack{u \in \mathbf{F}_2^n \\ u_i = 0}} W_f^2(u) = \Delta_f(e^i) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+f(x+e^i)} =$$

$$2^n - 2wt(f(x) \oplus f(x+e^i)) \geq 2^n - 2\left(2^n - 2^{n-(\deg(f)-1)}\right) = -2^n + 2^{n-\deg(f)+2}.$$

Отсюда следует, что $\sum\limits_{\substack{u \in \mathbf{F}_2^n \\ u_i = 0}} W_f^2(u) \geq 2^{2n-\deg(f)+1}$. □

Лемма 3.4. *Пусть f является булевой функцией на $\mathbf{F}_2^n$, $\deg(f, x_i) = 0$ (т. е. переменная x_i является фиктивной для функции f). Тогда $\sum\limits_{\substack{u \in \mathbf{F}_2^n \\ u_i = 0}} W_f^2(u) = 2^{2n}$.*

Доказательство. По условию переменная x_i является фиктивной для функции f. Поэтому $f(x) \equiv f(x+e^i)$. По теореме 3.1, имеем

$$-2^n + 2^{1-n} \sum_{\substack{u \in \mathbf{F}_2^n \\ u_i = 0}} W_f^2(u) = \Delta_f(e^i) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+f(x+e^i)} = 2^n.$$

Отсюда $\sum\limits_{\substack{u \in \mathbf{F}_2^n \\ u_i = 0}} W_f^2(u) = 2^{2n}$. □

Теорема 3.3. *Пусть f является $(m = n-k)$-устойчивой булевой функцией на $\mathbf{F}_2^n$, $k \geq 2$, и $\deg(f, x_i) \neq 1$ для каждого $i = 1, \ldots, n$. Тогда $n \leq (k-1)2^{\deg(f)-1}$.*

Доказательство. Образуем матрицу B с n столбцами, выписывая в строках B каждый двоичный набор u из $\mathbf{F}_2^n$ в точности $W_f^2(u)$ раз. По равенству Парсеваля матрица B содержит в точности 2^{2n} строк. По спектральной характеризации [68] каждая строка матрицы B содержит не более $k-1$ нулей. Следовательно, общее число нулей в B не более $(k-1)2^{2n}$. По леммам 3.3 и 3.4 каждый столбец B содержит не менее $2^{2n-\deg(f)+1}$ нулей. Поэтому $n \leq \frac{(k-1)2^{2n}}{2^{2n-\deg(f)+1}} = (k-1)2^{\deg(f)-1}$. □

Теорема 3.4. *Пусть f — это $(m = n-k)$-устойчивая булева функция на $\mathbf{F}_2^n$, $k \geq 2$, и $\deg(f, x_i) \neq 1$ для каждого $i = 1, \ldots, n$. Тогда $n \leq (k-1)2^{k-2}$.*

Доказательство. По неравенству Зигенталера [113] имеем $\deg(f) \leq k-1$. Этот факт вместе с теоремой 3.3 доказывают результат. □

В [161] доказано, что $n \leq (k-1)4^{k-2}$. Теорема 3.4, доказанная автором в 2001 году, существенно улучшает этот результат. Заметим, что существуют $(n-k)$-устойчивые функции на $\mathbf{F}_2^n$, $n = 3 \cdot 2^{k-2} - 2$, которые зависят нелинейно от всех своих n переменных. (см. параграф 2.3, в котором приведены конструкции автора из [158, 134]).

Существуют также $(n-k)$-устойчивые функции на $\mathbf{F}_2^n$, которые зависят от всех своих n переменных квадратично, при $n = 2(k-1)$, т. е. достигающие верхней оценки в теореме 3.3. Из леммы 1.21 несложно видеть, что если алгебраическая степень всех переменных функции $g(y_1, \ldots, y_n)$ на $\mathbf{F}_2^n$ равна двум, то функция $f(x_1, \ldots, x_{2n})g(x_1 \oplus x_{n+1}, x_2 \oplus x_{n+2}, \ldots, x_n \oplus x_{2n}) \oplus x_1 \oplus x_2 \oplus \cdots \oplus x_n$ является $(n-1)$-устойчивой, и алгебраическая степень всех $2n$ переменных функции f равна двум. Таким образом, функция f достигает верхней оценки в теореме 3.3. Студент автора Петр Королев в работе [13] (результаты включены также в состав работы [136]) доказал, что указанными выше функциями с точностью до перестановок переменных (без отождествления) и взятия отрицания у всей функции ограничивается множество всех квадратичных по всем своим переменным функций, достигающих верхней оценки в теореме 3.3.

Следствие 3.1. *Пусть f является m-устойчивой булевой функцией на $\mathbf{F}_2^n$. Если $n \geq (n-m-1)2^{n-m-2}$, то $\Delta_f = 2^n$.*

Доказательство. Если $n > (n-m-1)2^{n-m-2}$, то по теореме 3.4 функция f зависит линейно от некоторой переменной, следовательно, $\Delta_f = 2^n$. Если $n = (n-m-1)2^{n-m-2}$ и f зависит нелинейно от всех своих переменных, то в соответствии с доказательствами теорем 3.3 и 3.4 имеем, что каждая строка матрицы B содержит ровно $n-m-1$ нулей. Однако в этом случае по теореме 3.1 $|\Delta_f((1 \ldots 1))| = 2^n$, таким образом, $\Delta_f = 2^n$. □

3.3 Отсутствие неуравновешенных неконстантных корреляционно-иммунных порядка m булевых функций от n переменных при $m > 0.75n - 1.25$

В этом параграфе применяются коэффициенты Уолша для исследования корреляционно-иммунных и устойчивых булевых функций. Устанавливаются новые необходимые условия, связывающие число переменных, устойчивость и вес неуравновешенных неконстантных корреляционно-иммунных функций и доказываем, что такие функции не существуют при $m > 0.75n - 1.25$. Похожие утверждения известны для функций с несколькими выходами (операторов) (см. [38], [77]). Однако для обычных булевых функций до работ автора утверждения такого типа не были сформулированы даже как гипотезы. Для высоких порядков m этот неожиданный факт превзошел хорошо известное неравенство Бирбрауэра–Фридмана [64], [37]. Одновременно главный результат параграфа явился новым необходимым условием на число строк простого двоичного ортогонального массива. Заметим, что это необходимое условие впервые (если не считать очевидного факта, что число строк должно делиться на двойку в степени, равной силе массива) имеет немонотонное по числу строк поведение. До сих пор все усилия исследователей в этой области были направлены исключительно на получение нижних оценок для числа строк в массиве (или как иногда любят говорить, для «мощности дизайна»).

Результаты параграфа опубликованы в работе автора [167] и входят в состав работы [136].

В 2007 году Дмитрий Германович Фон-Дер-Флаасс усилил главный результат этого параграфа и доказал [63], что неуравновешенные неконстантные корреляционно-иммунные функции порядка m от n переменных не существуют при $m > \frac{2}{3}n - 1$, назвав свой результат доказательством «гипотезы Таранникова». Этот результат Фон-Дер-Флаасса является во многих отношениях окончательным, поскольку известны бесконечные семейства функций с $m = \frac{2}{3}n - 1$. В

2010 году А. В. Халявин обобщил [27] результат Фон-Дер-Флаасса на ортогональные массивы, доказав, что если при $m > \frac{2}{3}n - 1$ существует $OA(N, n, 2, m)$, то $N \geq 2^{n-1}$; причем если $N = 2^{n-1}$, то ортогональный массив является простым.

Лемма 3.5. *Пусть f — это произвольная булева функция на $\mathbf{F}_2^n$. Тогда*

$$\sum_{\substack{x \in \mathbf{F}_2^n \\ <x,w>=0}} W_f^2(x) = 2^{n-|w|+2} \sum_{f'} \left(2^{|w|-1} - wt(f')\right)^2,$$

где последняя сумма берется по всем $2^{n-|w|}$ подфункциям f' от $|w|$ переменных, полученным из f подстановкой констант вместо всех x_i, таких что $w_i = 0$.

Доказательство. Имеем

$$\sum_{\substack{x \in \mathbf{F}_2^n \\ <x,w>=0}} W_f^2(x) = \sum_{\substack{x \in \mathbf{F}_2^n \\ <x,w>=0}} \left(\sum_{u \in \mathbf{F}_2^n} (-1)^{f(u)+<u,x>} \right)^2 = \sum_{u', u'' \in \mathbf{F}_2^n} (-1)^{f(u')+f(u'')} \sum_{\substack{x \in \mathbf{F}_2^n \\ <x,w>=0}} (-1)^{<u' \oplus u'', x>}.$$

Если найдется i, такое что $u'_i \oplus u''_i = 1$, а $w_i = 0$, то все наборы x из $\mathbf{F}_2^n$, такие что $< x, w >= 0$, можно разбить на пары наборов (x', x''), различающихся только в i-й компоненте и совпадающих во всех остальных компонентах. Тогда $(-1)^{<u' \oplus u'', x'>} + (-1)^{<u' \oplus u'', x''>} = 0$ и $\sum\limits_{\substack{x \in \mathbf{F}_2^n \\ <x,w>=0}} (-1)^{<u' \oplus u'', x>} = 0$. Следовательно, сумма $\sum\limits_{\substack{x \in \mathbf{F}_2^n \\ <x,w>=0}} (-1)^{<u' \oplus u'', x>}$ может быть ненулевой, только если $u' \oplus u'' \preceq w$. В этом случае для любого набора x из $\mathbf{F}_2^n$, такого что $< x, w >= 0$, выполнено $(-1)^{<u' \oplus u'', x>} = 1$ и, таким образом, $\sum\limits_{\substack{x \in \mathbf{F}_2^n \\ <x,w>=0}} (-1)^{<u' \oplus u'', x>} = 2^{n-|w|}$. Поэтому

$$\sum_{\substack{x \in \mathbf{F}_2^n \\ <x,w>=0}} W_f^2(x) = 2^{n-|w|} \sum_{\substack{u', u'' \in \mathbf{F}_2^n \\ u' \oplus u'' \preceq w}} (-1)^{f(u')+f(u'')}.$$

Заметим, что $u' \oplus u'' \preceq w$ тогда и только тогда, когда наборы u' и u'' принадлежат одной подфункции f' от $|w|$ переменных, полученной из f подстановкой

соответствующих констант вместо всех x_i, таких что $w_i = 0$. Поэтому

$$\sum_{\substack{x\in\mathbf{F}_2^n \\ <x,w>=0}} W_f^2(x) = 2^{n-|w|}\sum_{f'}\sum_{u',u''\text{из } f'}(-1)^{f(u')+f(u'')} =$$

$$2^{n-|w|}\sum_{f'}\left(wt^2(f') + \left(2^{|w|} - wt(f')\right)^2 - 2wt(f')\left(2^{|w|} - wt(f')\right)\right) =$$

$$2^{n-|w|+2}\sum_{f'}\left(2^{|w|-1} - wt(f')\right)^2.$$

□

Замечание 3.1. Если f является корреляционно-иммунной порядка $n-k$ функцией на $\mathbf{F}_2^n$, то по (1.13) имеем $W_f(0) \equiv 0 \pmod{2^{n-k+1}}$. Поэтому $W_f(0) \equiv 2^{n-i} \pmod{2^{n-i+1}}$ для некоторого i, $i \in \{1, 2, \ldots, k-1\}$.

Теорема 3.5. *Пусть f является неуравновешенной неконстантной корреляционно-иммунной порядка $n-k$ функцией на $\mathbf{F}_2^n$. Пусть $W_f(0) = \pm p\cdot 2^{n-i}$, где p — некоторое нечетное натуральное число, $i \in \{1, 2, \ldots, k-1\}$. Тогда*

$$\binom{n}{i} \le (2^{2i} - p^2)\binom{k-1}{i}. \tag{3.5}$$

Доказательство. По лемме 1.5 имеем, что $\left|2^{n-1} - wt(f)\right| = p\cdot 2^{n-i-1}$. Пусть $w \in \mathbf{F}_2^n$ — это произвольный набор, такой что $|w| = i$. Тогда

$$\sum_{f'}\left|2^{i-1} - wt(f')\right| \ge \left|2^{n-1} - wt(f)\right| = p\cdot 2^{n-i-1},$$

где сумма берется по всем 2^{n-i} подфункциям f' от i переменных, полученным из f подстановкой констант вместо всех x_i, таких что $w_i = 0$. Все слагаемые в сумме целые. Отсюда следует, что

$$\sum_{f'}\left(2^{i-1} - wt(f')\right)^2 \ge \left(\left(\frac{p+1}{2}\right)^2 + \left(\frac{p-1}{2}\right)^2\right)\cdot 2^{n-i-1}.$$

Поэтому по лемме 3.5 имеем

$$\sum_{\substack{x\in\mathbf{F}_2^n \\ <x,w>=0}} W_f^2(x) \ge 2^{n-i+2}\cdot\left(\frac{p^2+1}{2}\right)\cdot 2^{n-i-1} = (p^2+1)\cdot 2^{2n-2i}.$$

Следовательно,

$$\sum_{\substack{x\in\mathbf{F}_2^n \\ <x,w>=0}} W_f^2(x) - W_f^2(0) \geq 2^{2n-2i}. \tag{3.6}$$

Далее, образуем матрицу B с n столбцами, записывая в строках B каждый двоичный набор $x \in \mathbf{F}_2^n$ в точности $W_f^2(x)$ раз. По равенству Парсеваля матрица B содержит в точности 2^{2n} строк. Общее число ненулевых строк в B равно $2^{2n} - p^2 \cdot 2^{2n-2i}$. По спектральной характеризации Гуо-Чжена–Мэсси [68] каждая ненулевая строка матрицы B содержит не более $k-1$ нулей. Отсюда следует, что каждая ненулевая строка в B содержит не более $\binom{k-1}{i}$ подмножеств из i нулей. Все ненулевые строки в B содержат не более $(2^{2n} - p^2 \cdot 2^{2n-2i})\binom{k-1}{i}$ подмножеств из i нулей. В то же самое время по (3.6) для любых i столбцов в B существует не менее 2^{2n-2i} ненулевых строк, содержащих только нули в этих i столбцах. Поэтому,

$$\frac{(2^{2n} - p^2 \cdot 2^{2n-2i})\binom{k-1}{i}}{2^{2n-2i}} \geq \binom{n}{i}.$$

□

В частном случае $i = k-1$, $p = 1$ неравенство (3.5) встречалось в работе Зенга и Занга [126].

Следствие 3.2. *Пусть f является корреляционно-иммунной булевой функцией порядка m на $\mathbf{F}_2^n$. Пусть $wt(f) = u \cdot 2^h$, где u — некоторое нечетное натуральное число, h — натуральное число. Тогда*

$$\binom{n}{h+1} \leq u(2^{n-h} - u)\binom{n-m-1}{h-m}.$$

Доказательство. Немедленно вытекает из теоремы 3.5 и леммы 1.5. □

Теорема 3.6. *Пусть f является неуравновешенной неконстантной корреляционно-иммунной порядка $(n-k)$ булевой функцией на $\mathbf{F}_2^n$. Тогда $n \leq 4k-5$.*

Доказательство. По замечанию 3.1 мы можем считать, что $W_f(0) \equiv 2^{n-i} \pmod{2^{n-i+1}}$ для некоторого i, $i \in \{1, 2, \ldots, k-1\}$. Тогда по теореме 3.5 мы имеем

$$n(n-1)\ldots(n-i+1) \leq (2^{2i}-1)(k-1)(k-2)\ldots(k-i). \tag{3.7}$$

Предположим, что $n \geq 4(k-1)$. Тогда, $n(n-1)\dots(n-i+1) \geq 2^{2i}(k-1)(k-2)\dots(k-i)$, что противоречит (3.7). □

Следствие 3.3. *При* $m > 0.75n - 1.25$ *не существует неуравновешенной неконстантной корреляционно-иммунной порядка* m *булевой функцией на* $\mathbf{F}_2^n$.

Легко видеть, что функция f от 3 переменных, которая принимает значение 1 только на двух наборах $(0,0,0)$ и $(1,1,1)$, является корреляционно-иммунной порядка 1. Поэтому оценка в следствии 3.3 является точной.

Замечание 3.2. Некоторое время неравенство Бирбрауэра–Фридмана [64], [37]

$$wt(f) \geq 2^n \frac{2(m+1)-n}{2(m+1)} \tag{3.8}$$

было лучшей известной нижней оценкой для веса корреляционно-иммунных неконстантных функций высокого порядка. Если подставить $m > 0.75n - 1.25$ в (3.8), то получим $wt(f) > 2^n \frac{n-1}{3n-1}$. На самом деле, из следствия 3.3 вытекает, что в этом случае $wt(f) = 2^{n-1}$.

Используя формулу (3.5) для $i = k-1$ и $i = k-2$ студент автора Антон Ботев получил в [3] (результаты этой статьи входят также в состав работы [136]) новые верхние оценки для нелинейности неуравновешенных корреляционно-иммунных функций высокого порядка.

3.4 Спектральный анализ корреляционно-иммунных функций высокого порядка

В теореме 3.5 параграфа 3.3 дано необходимое условие существования неуравновешенных неконстантных корреляционно-иммунных булевых функций высокого порядка. В теореме 3.4 параграфа 3.2 дана верхняя оценка для числа нелинейных переменных в устойчивых функциях высокого порядка. Однако в некоторых случаях эти оценки можно улучшить более тонким исследованием. Элементы такого подхода разрабатываются в этом параграфе. Приведенные в нем результаты содержатся в работах [164] и [161].

В этом параграфе результаты о спектральной структуре корреляционно-иммунных и устойчивых булевых функций используются для исследования корреляционно-иммунных функций высокого порядка. Вводится матрица ненулевых коэффициентов Уолша и устанавливаются важные свойства этой матрицы. Эти свойства применяются для доказательства несуществования неуравновешенной неконстантной корреляционно-иммунной порядка $n-4$ функции от $n \geq 10$ переменных.

В следующей лемме дается спектральная характеризация линейной зависимости функции f от переменной x_i.

Лемма 3.6. *Функция f зависит от переменной x_i линейно тогда и только тогда, когда $W_f(u) = 0$ для всех u, таких что $u_i = 0$.*

Доказательство. Функция f зависит от переменной x_i линейно тогда и только тогда, когда $f(x) \oplus f(x + e^i) \equiv 1$. По теореме 3.1, имеем

$$-2^n + 2^{1-n} \sum_{\substack{u \in \mathbf{F}_2^n \\ u_i = 0}} W_f^2(u) = \Delta_f(e^i) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+f(x+e^i)}.$$

Отсюда $\sum\limits_{\substack{u \in \mathbf{F}_2^n \\ u_i = 0}} W_f^2(u) = 0$ тогда и только тогда, когда функция f зависит от переменной x_i линейно. Отсюда немедленно следует заключение леммы. □

Ниже через $M = M(f)$ обозначаем $(0,1)$-матрицу с n столбцами, которая получается выписыванием по строкам всех наборов u, таких что $W_f(u) \neq 0$.

Лемма 3.7. *Пусть f является булевой функцией на $\mathbf{F}_2^n$. Пусть $M = M(f)$ является матрицей ненулевых коэффициентов Уолша функции f, введенной выше. Если M содержит столбец с ровно одним символом 0, то f имеет только один ненулевой коэффициент Уолша и f является аффинной функцией.*

Доказательство. Предположим, что i-й столбец M содержит в точности один символ 0. Рассмотрим набор w из $\mathbf{F}_2^n$, который содержит нуль в i-й компоненте и единицы во всех остальных компонентах. По конструкции $|w| = n - 1$. По теореме 1.10 выполняется соотношение (1.2). По предположению леммы левая часть (1.2) содержит ровно одно ненулевое слагаемое. Правая часть (1.2) делится на 2^n. Поэтому существует ненулевой коэффициент Уолша, который делится на 2^n. Тогда по равенству Парсеваля этот коэффициент является единственным ненулевым коэффициентом Уолша функции f. Отсюда ясно, что f является аффинной функцией. □

Пусть f является корреляционно-иммунной порядка m неаффинной функцией на $\mathbf{F}_2^n$, такой что $W_f(u) \equiv 0 \pmod{2^{m+2}}$ для каждого $u \in \mathbf{F}_2^n$. Из того факта, что f неаффинная, следует, что $n-m \geq 2$. Разложим матрицу $M = M(f)$ на матрицы $M_1, M_2, \ldots$, где матрица M_i содержит все строки M, которые соответствуют наборам u, таким что $W_f(u) \equiv 2^{m+1+i} \pmod{2^{m+2+i}}$. Пусть r_i это число строк в M_i. Из равенства Парсеваля следует, что $r_1 + 4r_2 + 16r_3 + \cdots \leq 4^{n-m-2}$.

Теорема 3.7. *В матрице M_1 внутри любых h столбцов, $h \leq n-m-2$, каждая возможная h-ка встречается в четном числе строк.*

Доказательство. Возьмем произвольное множество S из h столбцов в матрице M_1, $0 \leq h \leq n - m - 2$. Пусть w является набором из $\mathbf{F}_2^n$, таким что $w_i = 0$, если i-й столбец принадлежит S, и $w_i = 1$ в противоположном случае. Ясно, что $|w| = n - h \geq m + 2$. По теореме 1.10 выполняется тождество (1.2). Правая часть (1.2) делится на 2^{m+3}. По предположению все слагаемые в левой части (1.2) делятся на 2^{m+2}. Поэтому число слагаемых в левой части (1.2), которые сравнимы с 2^{m+2} по модулю 2^{m+3}, четно. Таким образом, в выбранных h столбцах h-ка из одних нулей встречается в четном числе строк. Заметим, что возможность $h = 0$ показывает, что M_1 содержит четное число строк. Отсюда

легко следует, что в M_1 внутри любых h столбцов, $h \le n-m-2$, каждая h-ка встречается в четном числе строк. □

Следующая теорема является обобщением теоремы 3.7.

Теорема 3.8. *В матрице M_i внутри любых h столбцов, $0 < h \le n-m-i-1$, которые содержат в матрицах M_1, M_2, ..., M_{i-1} только единицы, h-ка из одних нулей содержится в четном числе строк.*

Доказательство. Доказательство аналогично доказательству теоремы 3.7. Возьмем в матрице M_i произвольное множество S из h столбцов, $0 < h \le n-m-i-1$, таких что каждый из этих столбцов содержит в матрицах M_1, M_2, ..., M_{i-1} только единицы. Пусть w является набором из $\mathbf{F}_2^n$, таким что $w_i = 0$, если i-й столбец принадлежит S, и $w_i = 1$ в противоположном случае. Ясно, что $|w| = n - h \ge m + i + 1$. По теореме 1.10 выполняется соотношение (1.2). Правая часть (1.2) делится на 2^{m+i+2}. По предположению все слагаемые в левой части (1.2) делятся на 2^{m+i+1}. Поэтому число слагаемых в левой части (1.2), сравнимых с 2^{m+i+1} по модулю 2^{m+i+2}, четно. Таким образом, в выбранных h столбцах h-ка из одних нулей встречается в четном числе строк. □

Лемма 3.8. *Пусть f является корреляционно-иммунной порядка $(m = n-4)$ функцией на $\mathbf{F}_2^n$, такой что $W_f(u) \equiv 0 \pmod{2^{m+2}}$ для всех $u \in \mathbf{F}_2^n$, и матрица $M_1 = M_1(f)$ не содержит строки из одних нулей. Тогда если некоторый столбец матрицы M_1 содержит не менее одного символа 0, то этот столбец содержит не менее четырех нулей.*

Доказательство. Предположим, что f является корреляционно-иммунной порядка $(m = n-4)$ функцией на $\mathbf{F}_2^n$, такой что $W_f(u) \equiv 0 \pmod{2^{m+2}}$ и матрица $M_1 = M_1(f)$ не содержит строки из одних нулей. Рассмотрим произвольный (скажем, i-й) столбец матрицы M_1, содержащий нуль. Тогда по теореме 3.7 этот i-й столбец содержит не менее двух нулей. Матрица M_1 не содержит одинаковых строк, поэтому некоторая строка содержит нули в i-м и некотором другом (скажем, j-м) разрядах. Тогда по теореме 3.7 существует не менее двух строк в M_1, которые содержат нули в i-й и j-й компонентах. Матрица M_1 не содержит одинаковых строк, поэтому строка l_1 содержит нули в i-м, j-м и некотором

другом (скажем, k-м) разрядах, в то время как строка l_2 содержит нули и i-м и j-м разрядах и не содержит нуль в k-м разряде. Однако по теореме 3.7 четное число строк содержит нули в i-м и k-м столбцах одновременно. Поэтому в M_1 существует строка l_3, которая содержит нули в i-м и k-м столбцах. Таким образом, мы имеем по крайней мере три строки, которые содержат нуль в i-м столбце. Тогда по теореме 3.7 этот i-й столбец должен содержать не менее четырех нулей. □

Теорема 3.9. *При $n \geq 10$ не существует неуравновешенной неконстантной корреляционно-иммунной порядка $(n-4)$ функции на $\mathbf{F}_2^n$.*

Доказательство. Пусть f является неуравновешенной неконстантной корреляционно-иммунной порядка ($m = n-4$) функцией на $\mathbf{F}_2^n$. Если $W_f(u) \equiv 2^{m+1} \pmod{2^{m+2}}$ для некоторого $u \in \mathbf{F}_2^n$, то по лемме 1.14 имеем, что $W_f(0) \equiv 2^{m+1} \pmod{2^{m+2}}$. Однако тогда $i = k - 1 = 3$ в формулировке теоремы 3.5, и имеем $\binom{n}{3} \leq 63$. Отсюда $n \leq 8$. Стало быть, можно считать, что $W_f(u) \equiv 0 \pmod{2^{m+2}}$ для каждого $u \in \mathbf{F}_2^n$. Если $W_f(u) = \pm 2^n$ для некоторого $u \in \mathbf{F}_2^n$, то f является аффинной функцией и, следовательно, не может быть неуравновешенной неконстантной. Таким образом, $W_f(u) \equiv 2^{n-2} \pmod{2^{n-1}}$ для r_1 наборов $u \in \mathbf{F}_2^n$, $W_f(u) = \pm 2^{n-1}$ для r_2 наборов $u \in \mathbf{F}_2^n$, и $W_f(u) = 0$ для всех остальных наборов. По равенству Парсеваля $r_1 + 4r_2 \leq 16$. Разложим матрицу $M = M(f)$ на матрицу M_1 с r_1 строками и матрицу M_2 с r_2 строками. Одна из двух матриц M_1 и M_2 содержит строку из одних нулей. Если матрица M_2 содержит строку из одних нулей, то $W_f(0) = \pm 2^{n-1}$, поэтому $i = 1$ в формулировке теоремы 3.5, и имеем $n \leq 9$. Таким образом, осталось разобрать случай, когда матрица M_1 содержит строку из одних нулей. Тогда по теореме 3.7 любые два столбца в M_1 должны иметь нули одновременно и в некоторой другой строке. Каждая строка в M_1 с единицами содержит не более трех нулей, поэтому $r_1 - 1$ строк дают не более $3(r_1 - 1)$ комбинаций из двух нулей в одной строке. Следовательно, $\frac{n(n-1)}{2} \leq 3(r_1 - 1) \leq 45$. Таким образом, $n \leq 10$. (Такой же результат дает и теорема 3.5 при $i = 2$.) Однако если $n = 10$, то $r_1 - 1 = 15$ и 15 строк M_1 задают систему троек Штейнера. Хорошо известно, что не существует системы троек Штейнера для четного n. Например потому, что тогда $n - 1$

нечетно, и все столбцы кроме произвольно выбранного невозможно разбить на попарно непересекающиеся пары столбцов, содержащих ноль в одной строке с выбранным. Поэтому и в этом случае $n \leq 9$. □

Заметим, что существует неуравновешенная неконстантная корреляционно-иммунная порядка $(9-4)$ функция на $\mathbf{F}_2^9$ (см. [158]). Используя изложенные в этом параграфе методы, студент автора Денис Кириенко дал в работах [11] и [12] полное описание неуравновешенных неконстантных корреляционно-иммунная порядка 5 функций на $\mathbf{F}_2^9$, найдя при этом новое, ранее неизвестное семейство таких функций.

В работах [164] и [161], используя развитую в этом параграфе технику и элементы компьютерного поиска, доказано, что при $n \geq 11$ не существует $(n-4)$-устойчивой функции на $\mathbf{F}_2^n$, которая зависит нелинейно от всех своих n переменных. Таким образом, учитывая существование такой функции от 10 переменных, построенной автором и приведенной в параграфе 2.3, было доказано, что максимально возможное число $p(4)$ переменных в $(n-4)$-устойчивых функциях от n переменных равно 10. Заметим, что результат $p(3) = 4$ был получен еще в [42], однако следующий шаг (для $k = 4$) удалось осуществить только через десять лет.

3.5 О числе корреляционно-иммунных и устойчивых булевых функций высокого порядка

Для числа n-местных корреляционно-иммунных функций порядка k при $k = \text{const}$, $n \to \infty$ в [5] Денисовым при помощи сложных выкладок, использующих вероятностный аппарат, получена асимптотическая формула

$$N(n,k) \sim \frac{2^{2^n}}{2^k \exp\left(\sum\limits_{i=1}^{k} \left(\ln \sqrt{\frac{\pi}{2}} + \left(\frac{n}{2} - i\right) \ln 2\right) \binom{n}{i}\right)}. \tag{3.9}$$

Спустя девять лет в статье [6] Денисов признал, что формула (3.9) неточна при $k \geq 2$, и доказал для $n \to \infty$, $k(n) = o(\sqrt{n})$, уточненные асимптотические формулы для числа k-устойчивых от n переменных

$$R(n,k) \sim \exp_2\left(2^n - \frac{n-k}{2}\binom{n}{k} - M(n,k)\log_2\sqrt{\pi/2}\right)$$

и корреляционно-иммунных порядка k от n переменных

$$K(n,k) \sim \frac{\exp_2\left(2^n - \binom{n}{k}\frac{n-k}{2} - (M(n,k)-1)\log_2\sqrt{\pi/2} + n/2 - k\right)}{\left(1 + \sum\limits_{i=2}^{k}(i-1)^2\binom{n}{i}\right)^{1/2}}$$

функций, где

$$M(n,k) = \sum_{i=0}^{k}\binom{n}{i}.$$

В [44] было показано, что результат первой статьи Денисова [5] был верен, а вторая [6] содержала ошибку. Основным вкладом статьи [44] является асимптотическая оценка величины $K(n,k)$, которая верна, если k возрастает вместе с n в достаточно широких пределах. Кроме того, в [44] получены оценки на функции с заданным весом, включая устойчивые функции.

Если в упомянутых выше статьях изучались асимптотики для числа корреляционно-иммунных функций и устойчивых функций порядка, достаточно малого по сравнению с числом переменных, то в этом параграфе изучаются количества таких функций высокого порядка, а именно устанавливается

вид формул для числа корреляционно-иммунных и устойчивых порядка $n-k$ функций от n переменных при $k=\text{const}$, $n\to\infty$.

Сформулируем важные для достижения цели диссертации утверждения, уже многократно упоминавшиеся в предыдущих параграфах.

Теорема 3.10. *Для любого натурального k существует минимальное неотрицательное целое $p(k)$, такое что любая $(n-k)$-устойчивая функция от n переменных зависит нелинейно от не более чем $p(k)$ переменных. При этом $3\cdot 2^{k-2}-2\le p(k)\le (k-1)2^{k-2}$.*

Доказательство. Нижняя оценка следует из конструкции (2.5) параграфа 2.3 и теоремы 2.3. Верхняя оценка доказана в теореме 3.4. □

Теорема 3.11. *Для любого натурального k существует минимальное неотрицательное целое $p_{ub}(k)$, такое что любая неуравновешенная неконстантная корреляционно-иммунная порядка $(n-k)$ булева функция зависит от $n\le p_{ub}(k)$ переменных. При этом $3k-3\le p_{ub}(k)\le 4k-5$.*

Доказательство. Конструкции, на которых достигается нижняя оценка, приведены в параграфе 1.3. Верхняя оценка доказана в теореме 3.6. □

В 2007 году Фон-Дер-Флаасс доказал [63], что $p_{ub}(k)=3k-3$.

Обозначим через $A(k,i)$ число $(i-k)$-устойчивых булевых функций на $\mathbf{F}_2^i$. Как обычно, считаем, что уравновешенная булева функция является 0-устойчивой, а произвольная булева функция является устойчивой любого целого отрицательного порядка.

Теорема 3.12. *Число $R(n,n-k)$ устойчивых порядка $n-k$ функций на $\mathbf{F}_2^n$ выражается формулой*

$$R(n,n-k)=\sum_{i=0}^{p(k)}A(k,i)\binom{n}{i};$$

при $n>3k-3$ число $K(n,n-k)$ корреляционно-иммунных порядка $n-k$ функций на $\mathbf{F}_2^n$ выражается формулой

$$K(n,n-k)=2+R(n,n-k)=2+\sum_{i=0}^{p(k)}A(k,i)\binom{n}{i}.$$

Доказательство. По теореме 3.10 любая $(n-k)$-устойчивая функция f зависит нелинейно от i переменных, $i \in \{0, \ldots, p(k)\}$, а от остальных $n-i$ переменных f зависит линейно. Выбрать $n-i$ переменных из n можно $\binom{n}{i}$ способами. Каждая из выбранных $n-i$ линейных переменных однозначно входит в полином функции в виде единственного линейного члена. От каждой же из оставшихся i переменных функция, получившаяся отбрасыванием линейных слагаемых, должна зависеть нелинейно, причем быть на множестве из этих i переменных устойчивой порядка $(n-k)-(n-i) = i-k$. Число таких функций как раз и равно $A(k,i)$.

Если $n > p_{ub}(k)$, то по теореме 3.11 неуравновешенных неконстантных корреляционно-иммунных порядка $(n-k)$ булевых функций от n переменных не существует. Поэтому кроме устойчивых корреляционно-иммунными такого порядка будут только две константные функции. □

Следствие 3.4. *Асимптотика числа $R(n, n-k)$ устойчивых порядка $n-k$ функций на $\mathbf{F}_2^n$, так же как и асимптотика числа $K(n, n-k)$ корреляционно-иммунных порядка $n-k$ функций на $\mathbf{F}_2^n$ при $k = const$, $n \to \infty$, выражается следующей формулой*

$$R(n, n-k) \sim K(n, n-k) \sim \frac{A(k, p(k))}{p(k)!} n^{p(k)}.$$

Помимо нижних и верхних оценок на величину $p(k)$ и p_{ub}, данных в теоремах 3.10 и 3.11, известны также следующие точные значения этих величин:

$p(1) = 0$, $p(2) = 1$, $p(3) = 4$, $p(4) = 10$, $p_{ub}(k) = 3k - 3$.

При $k = 1, 2$ эти значения тривиальны. Величина $p(3) = 4$ была фактически найдена в [42]. Значение $p_{ub}(3) = 6$ было впервые приведено в работах автора [156] и [157]. Величина $p_{ub}(4) = 9$ была найдена автором в работах [161], [164] и [135], доказательство этого факта приведено в параграфе 3.4. То, что $p(4) \geq 10$, было показано автором в [155]. Точное же значение $p(4) = 10$ было установлено студентом автора Денисом Кириенко и опубликовано в работах [161], [164] и [135]. Равенство $p_{ub}(k) = 3k - 3$ установлено Фон-Дер-Флаассом в [63].

Что касается формул для числа корреляционно-иммунных функций, то на сегодняшний день известно следующее:

$$
\begin{aligned}
&K(n, n-1) = 4 && \text{при } n > 0,\\
&K(n, n-2) = 2n + 4 && \text{при } n > 3,\\
&K(n, n-3) = n^4 - (2/3)n^3 + (5/3)n + 4 && \text{при } n > 6,\\
&K(n, n-4) = (1/2)n^{10} + O(n^9) && \text{при } n \to \infty.
\end{aligned}
$$

Первые две формулы тривиальны, третья впервые выписана автором в [156] и [157], хотя соответствующая формула для числа $(n-3)$-устойчивых функций на $\mathbf{F}_2^n$ алгебраической степени 2 встречается в [42]. Наконец, последняя асимптотическая формула получена в [135].

3.6 Теорема для регулярных функций типа теоремы Симона–Вегенера

Пусть c и n — целые неотрицательные числа, $0 \leq c \leq n$. Напомним, что булева функция $f(x_1, \ldots, x_n)$ называется c-регулярной, если для любого $x \in \mathbf{F}_2^n$ выполнено равенство $\#\{i | i \in \{1, \ldots, n\},\ f(x) \neq f(x^i)\} = c$.

Легко видеть, что если $f(x_1, \ldots, x_n)$ является c-регулярной функцией на $\mathbf{F}_2^n$, то $f(x_1, \ldots, x_n) \oplus x_{n+1}$ является $(c+1)$-регулярной функцией на $\mathbf{F}_2^{n+1}$, и $f(x_1, \ldots, x_n)$ является c-регулярной функцией на $\mathbf{F}_2^{n+1}$ (здесь переменная x_{n+1} является фиктивной). Поэтому если регулярная функция зависит от некоторых переменных несущественно или линейно, то она может рассматриваться как вырожденная. В этом отношении целесообразно изучать только регулярные функции, зависящие существенно и нелинейно от всех своих переменных. В этом параграфе покажем, что для таких функций существует взаимосвязь между значениями параметров c и n. Содержание параграфа составляет теорема для регулярных функций типа теоремы Симона–Вегенера. Результаты этого параграфа были включены автором в состав работы [131]. При подготовке параграфа первоначальные доказательства были сильно упрощены.

Теорема 3.13. *Пусть f является c-регулярной булевой функцией на $\mathbf{F}_2^n$, $0 < c < n$. Если f зависит существенно от всех своих переменных, то $n \leq c \cdot 2^{c-1}$.*

Доказательство. Рассмотрим функцию

$$g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \oplus \bigoplus_{i=1}^{n} x_i.$$

Легко видеть, что функция g является $(n-c)$-регулярной и зависит от всех своих n переменных нелинейно. Поэтому по следствию 1.4 функция g является $(n-c-1)$-устойчивой функцией, поэтому по теореме 3.4 мы имеем $n \leq c2^{c-1}$. □

Заметим, что теорема 3.13 доказана в [131] без ссылки на следствие 1.4, однако это делает доказательство длиннее и требует введения дополнительных понятий.

Следствие 3.5. *Для заданного натурального c, $c \geq 2$, максимальное возможное n, такое что существует c-регулярная булева функция на $\mathbf{F}_2^n$, зависящая от всех своих переменных существенно, удовлетворяет соотношениям*

$$3 \cdot 2^{c-1} - 2 \leq \max n \leq c \cdot 2^{c-1}.$$

Доказательство. Нижняя оценка следует из примера, приведенного в [157] и параграфе 2.3 настоящей работы. Действительно, из теоремы 2.3 следует существование $(n(k)-k+1)$-регулярной функции f, нелинейно зависящей от всех своих $n(k)$ переменных, $k \geq 3$, где $n(k) = 3 \cdot 2^{k-2} - 2$. Обозначим $c = k - 1$ и рассмотрим функцию $g(x_1, \ldots, x_{n(k)}) = f(x_1, \ldots, x_n) \oplus \bigoplus_{i=1}^{n(k)} x_i$. Легко видеть, что g является c-регулярной функцией, существенно зависящей от всех своих $n(k) = 3 \cdot 2^{c-1} - 2$ переменных. Этот пример и доказывает нижнюю оценку теоремы. Верхняя оценка следует из теоремы 3.13. □

Следствие 3.6. *Для заданного натурального n минимальное возможное c, такое что существует c-регулярная булева функция на $\mathbf{F}_2^n$, существенно зависящая от всех своих переменных, удовлетворяет соотношению*

$$\min c = \log_2 n + O(\log_2 \log_2 n).$$

Доказательство. Доказательство вытекает из следствия 3.5. Неравенство $3 \cdot 2^{\min c - 1} - 2 \leq n$ дает $\min c \leq \log_2 n$. Неравенство $n \leq \min c \cdot 2^{\min c - 1}$ дает $\min c \geq \log_2 n - \log_2 \log_2 n + 1$. □

Замечание 3.3. В оригинальной теореме Симона–Вегенера [115, 121] использовались обозначения:

$$\begin{aligned} c(f, x) &= \#\{i \mid f(x) \neq f(x^i), i = 1, \ldots, n\}, \\ c(f) &= \max_{x \in \mathbf{F}_2^n} c(f, x), \\ c(n) &= \min c(f). \end{aligned}$$

Последний минимум брался над множеством всех булевых функций на $\mathbf{F}_2^n$, которые зависят от всех своих переменных существенно. Теорема Симона–Вегенера (верхняя оценка получена Симоном в [115], нижняя — Вегенером в [121]) утверждает, что $c(n) = (1/2) \log_2 n + O(\log_2 \log_2 n)$.

Более наглядно теорему Симона–Вегенера можно сформулировать так:

Теорема 3.14. Симона–Вегенера [115], [121] *Для заданного натурального n минимальное $c(n)$, такое что существует булева функция, существенно зависящая от всех своих n переменных, у которой любой набор имеет* **не более** *$c(n)$ соседних с ним, на которых функция принимает другое значение, удовлетворяет асимптотическому соотношению*

$$c(n) = (1/2)\log_2 n + O(\log_2 \log_2 n).$$

Тогда наш результат будет иметь следующую формулировку:

Теорема 3.15. *Для заданного натурального n минимальное $c(n)$, такое что существует булева функция, существенно зависящая от всех своих n переменных, у которой любой набор имеет* **ровно** *$c(n)$ соседних с ним, на которых функция принимает другое значение, удовлетворяет асимптотическому соотношению*

$$c(n) = \log_2 n + O(\log_2 \log_2 n).$$

4 О значениях аффинного ранга носителя спектра платовидной функции

В этой главе изучаются платовидные функции, основное внимание уделяется значению их аффинного ранга в зависимости от мощности носителя спектра.

Платовидные функции представляют большой интерес сами по себе и для построения различных классов криптографически важных функций. Так, бент-функции можно рассматривать как частный случай платовидных. Специально подчеркнем, что изучавшиеся в предыдущих главах корреляционно-иммунные и устойчивые булевы функции при накладывании разнообразных дополнительных требований во многих случаях могут быть лишь платовидными. Так, например, из следствия 1.7 вытекает, что m-устойчивая функция, на которой достигается равенство в оценке (1.8), и, тем самым, обладающая максимально возможной нелинейностью при заданном порядке устойчивости, обязана быть платовидной; конструкциям таких функций почти целиком посвящена самая большая глава 2.

Толчком к исследованиям аффинного ранга платовидных функций для автора послужила статья [49], в которой рассматривался аффинный ранг только кубических функций с максимальной устойчивостью, но эти функции, как было несложно показано, обязаны были быть платовидными. Поэтому при исследовании аффинного ранга переходим к рассмотрению всех платовидных функций.

4.1 Определения и анонс результатов главы

В этой главе доказывается, что аффинный ранг любой платовидной функции с носителем спектра мощности 16 равен 4, 5 или 6. Также для любого натурального h рассматриваются платовидные функции с носителем спектра

мощности 4^h, даются оценки аффинного ранга для таких функций и строятся функции, аффинный ранг которых принимает все возможные значения от $2h$ до $2^{h+1}-2$.

Платовидные функции представляют большой интерес в криптографии для изучения бент функций и в силу того, что многие криптографически важные функции являются платовидными. В этой главе изучаются возможные значения аффинного ранга носителя спектра платовидных функций. Автор рассмотрел для любого натурального h платовидные функции с носителем спектра мощности 4^h (мощность обязана иметь такой вид), даем оценки аффинного ранга для таких функций и строим функции, аффинный ранг которых принимает все возможные целые значения от $2h$ до $2^{h+1}-2$. Проблема была полностью решена для $h=2$, а именно, было доказано, что аффинный ранг любой платовидной функции с носителем спектра мощности 16 равен 4, 5 или 6.

Множество S_f всех наборов u, таких что $W_f(u)\neq 0$, называется *носителем спектра* функции f.

Напомним, что булева функция называется *бент-функцией,* если значение коэффициентов на всех наборах равно $\pm 2^{n/2}$. Бент-функции существуют при всех четных n, а при нечетных — не существуют. Бент-функция является функцией с максимально возможной нелинейностью $2^{n-1}-2^{(n/2)-1}$ среди всех функций от n переменных при четном n. Напомним, что булева функция называется *платовидной,* если ее коэффициенты Уолша принимают ровно три возможных значения: 0 и $\pm 2^c$ для некоторого c. Платовидные функции представляют большой интерес для изучения бент-функций (например, потому, что при разложении бент-функции по переменной возникают две платовидные функции), а также потому, что многие криптографически важные функции являются платовидными (например, m-устойчивые функции с максимально возможной для них нелинейностью $2^{n-1}-2^{m+1}$). Обозначим для платовидных функций $\phi(x)=2^{-c}W_f(x)$. Тогда для любого $x\in \mathbf{F}_2^n$ величина $\phi(x)$ может принимать только три значения: 0, -1 и 1. Множество S_f всех наборов u, таких что $W_f(u)\neq 0$, называется *носителем спектра* платовидной функции. Множество всех наборов, на которых $\phi(x)=-1$, будем обозначать через T^-, а множество всех наборов, на которых $\phi(x)=1$, будем обозначать через T^+. Из равенства

Парсеваля сразу следует, что мощность носителя спектра равна 4^{n-c}. Бент-функцию удобно рассматривать как частный случай платовидной при $c = n/2$ и $|S_f| = 2^n$, что и будем часто делать с оговорками. (Хотя часто формально бент-функции к платовидным не относят.) Платовидные функции изучались в большом числе работ, см., например, [17, 172, 125].

Напомним, что для каждого $u \in {F_2}^n$ *автокорреляционный коэффициент* функции f на наборе u определяется как $\Delta_f(u) = \sum\limits_{x \in {F_2}^n} (-1)^{f(x)+f(x+u)}$. Функция $D_u f = f(x) + f(x+u)$ называется *производной* функции f по направлению u. Набор $u \in {F_2}^n$, такой что $D_u f \equiv \mathrm{const}$, называется *линейной структурой* функции f. Легко проверить, что линейные структуры функции f образуют линейное пространство в $\mathbf{F}_2^n$. Наличие у функции нетривиальной линейной структуры в некоторых случаях (но не всех) является криптографической слабостью.

Пусть E — произвольное подмножество $\mathbf{F}_2^n$. *Рангом* множества E называется называется размерность подпространства, порожденного E в $\mathbf{F}_2^n$. *Аффинным рангом* множества E называется называется размерность наименьшего класса смежности в $\mathbf{F}_2^n$, содержащего E. Ранг и аффинный ранг носителя спектра булевой функции будем обозначать через k и $\mathbf{k}$, соответственно. Для краткости в данной главе аффинный ранг и ранг носителя спектра булевой функции будем называть просто ее *аффинным рангом* и *рангом,* соответственно. Легко убедиться, что $\mathbf{k} \in \{k, k-1\}$. Известно (см., например, [49]), что размерность линейной структуры функции f равна $n - \mathbf{k}$. Если существует набор $u \in {F_2}^n$, такой что $D_u f \equiv 1$, то $k = \mathbf{k} + 1$. Если такого набора не существует, то $k = \mathbf{k}$.

Дополнительные сведения о свойствах булевых функций можно найти в [19] и [146].

Из изложенного выше следует, что аффинный ранг является важной характеристикой платовидных функций. Очевидно, что аффинный ранг любой платовидной функции с носителем спектра мощности 4^h не меньше $2h$, потому что меньшие классы смежности не содержат 4^h наборов. Любой платовидная функция с носителем спектра мощности 1 есть аффинная функция и, очевидно, ее аффинный ранг равен 0. Аффинный ранг любой платовидной функции с носителем спектра мощности 4 равен 2. Этот факт доказан в [94], но, по-

видимому, был известен намного раньше. Платовидные функции с носителем спектра мощности 16 (не называясь платовидными) фактически рассматривались в [72], а в работе [49] для подкласса платовидных функций с носителем спектра мощности 16 (более точно, для кубических устойчивых порядка $n-4$ функций) была получена оценка $\mathbf{k} \leq k \leq 9$. Автором было доказано, [139] что аффинный ранг любой платовидной функции с носителем спектра мощности 16 равен 4, 5 или 6. Кроме того, в [139] были рассмотрены для любого натурального h платовидные функции с носителем спектра мощности 4^h, даны оценки аффинного ранга для таких функций и построены функции, аффинный ранг которых принимает все возможные значения от $2h$ до $2^{h+1}-2$. Более точно результаты этой главы формулируются в следующих утверждениях.

Теорема 4.1. *Пусть f является платовидной функцией, $|S_f| = 16$. Тогда для аффинного ранга $\mathbf{k}$ носителя спектра S_f справедливо неравенство $\mathbf{k} \leq 6$.*

Из этой теоремы следует, что аффинный ранг платовидных функций с носителем спектра мощности 16 не может принимать никаких значений, кроме 4, 5 и 6. Функции с такими параметрами известны, и их примеры приводились, например, в [49], поэтому здесь не будут отдельно приводиться примеры. Эти примеры будут построены в следующем разделе в рамках общей конструкции.

Теорема 4.2. *Для любого натурального $\mathbf{k}$, удовлетворяющего неравенствам $2h \leq \mathbf{k} \leq 2^{h+1}-2$ существует платовидная функция с носителем спектра мощности 4^h и аффинным рангом $\mathbf{k}$.*

Следствие 4.1. *Аффинный ранг платовидной функции с носителем спектра мощности 16 может принимать только значения 4, 5 и 6.*

Тривиальной верхней оценкой аффинного ранга $\mathbf{k}$ платовидной функции с носителем спектра мощности 4^h является $\mathbf{k} \leq 4^h - 1$. Приведем несколько улучшенную оценку.

Теорема 4.3. *Пусть f является платовидной функцией, $|S_f| = 4^h$. Тогда для аффинного ранга $\mathbf{k}$ носителя спектра S_f справедливо неравенство $\mathbf{k} \leq 2^{2h-1} - 2^{h-1} + h$.*

При $h = 2$ оценка теоремы 4.3 не достигается. Осмелимся выдвинуть гипотезу.

Гипотеза. Для любого натурального h максимально возможный аффинный

ранг платовидной функции с носителем спектра мощности 4^h равен $2^{h+1}-2$.

Обозначим для платовидных функций $\phi(x) = 2^{-c}W_f(x)$. Тогда для любого $x \in \mathbf{F}_2^n$ величина $\phi(x)$ может принимать только три значения: 0, -1 и 1. Множество S_f всех наборов u, таких что $W_f(u) \neq 0$, называется *носителем спектра* платовидной функции. Множество всех наборов, на которых $\phi(x) = -1$, будем обозначать через T^-, а множество всех наборов, на которых $\phi(x) = 1$, будем обозначать через T^+. Из равенства Парсеваля сразу следует, что мощность носителя спектра равна 4^{n-c}. Бент-функцию удобно рассматривать как частный случай платовидной при $c = n/2$ и $|S_f| = 2^n$, что и будем часто делать с оговорками. (Хотя часто формально бент-функции к платовидным не относят.) Платовидные функции изучались в большом числе работ, см., например, [17, 172, 125].

4.2 Об аффинных преобразованиях в $\mathbf{F}_2^n$

Аффинным преобразованием в $\mathbf{F}_2^n$ называется отображение $x \to x' = \mathbf{A}x = xA^T + a$, где A — квадратная двоичная невырожденная над $\mathbf{F}_2$ матрица порядка n, а a — вектор длины n. Аффинное преобразование является автоморфизмом $\mathbf{F}_2^n$, при котором все классы смежности переходят в классы смежности той же размерности. Если $a = 0$, то аффинное преобразование называется также *линейным.*

Аффинным преобразованием функции f, заданной на $\mathbf{F}_2^n$, называется преобразование $f(x) \to f'(x) = f(\mathbf{A}x)$. Если для функций f и f' существует аффинное преобразование функции, переводящее f в f', то f и f' называются *аффинное эквивалентными.* Если для функций f и f' существует линейное преобразование функции, переводящее f в f', то f и f' называются *линейно эквивалентными.*

Лемма 4.1. *Пусть* $f(x) \to f'(x) = f(\mathbf{A}x)$ — *аффинное преобразование функции* f, *заданной на* $\mathbf{F}_2^n$. *Тогда*

$$W_{f'(x)}(u) = (-1)^{<a,uA^{-1}>} \cdot W_f(uA^{-1}).$$

Доказательство. По формуле для коэффициентов Уолша имеем

$$W_{f'(x)}(u) = \sum_{x\in\mathbf{F}_2^n}(-1)^{f'(x)+<x,u>} = \sum_{x\in\mathbf{F}_2^n}(-1)^{f(\mathbf{A}x)+<x,u>} =$$
$$\sum_{x\in\mathbf{F}_2^n}(-1)^{f(x)+<\mathbf{A}^{-1}x,u>} = \sum_{x\in\mathbf{F}_2^n}(-1)^{f(x)+<x,uA^{-1}>+<a,uA^{-1}>} =$$
$$(-1)^{<a,uA^{-1}>}\cdot\sum_{x\in\mathbf{F}_2^n}(-1)^{f(x)+<x,uA^{-1}>} = (-1)^{<a,uA^{-1}>}\cdot W_f(uA^{-1}).$$

□

Пусть булева функция f задана на $\mathbf{F}_2^n$. *Аффинным преобразованием спектра* функции f называется преобразование $W_f(x) \to W'(x) = W_f(\mathbf{A}x)$. Можно показать, что коэффициенты $W'(x)$ являются коэффициентами Уолша некоторой функции f', которая, вообще говоря, не является аффинно эквивалентной функции f.

Лемма 4.2. *Пусть $W_f(x) \to W'(x) = W_f(\mathbf{A}x)$ — аффинное преобразование спектра функции f, заданной на $\mathbf{F}_2^n$. Тогда коэффициенты $W'(x)$ являются коэффициентами Уолша некоторой функции f', причем*

$$f'(x) = f(xA^{-1}) + < a, xA^{-1} > .$$

Доказательство. Проверим, что для всех $x \in \mathbf{F}_2^n$ суммы в формуле обращения для гипотетически существующей функции $f'(x)$ равны ± 1. Обозначим

$$F(x) = 2^{-n}\sum_{u\in\mathbf{F}_2^n} W'(u)(-1)^{<u,x>}.$$

Имеем

$$F(x) = 2^{-n}\sum_{u\in\mathbf{F}_2^n} W'(u)(-1)^{<u,x>} = 2^{-n}\sum_{u\in\mathbf{F}_2^n} W_f(\mathbf{A}u)(-1)^{<u,x>} =$$
$$2^{-n}\sum_{v\in\mathbf{F}_2^n} W_f(v)(-1)^{<\mathbf{A}^{-1}v,x>} = 2^{-n}\sum_{v\in\mathbf{F}_2^n} W_f(v)(-1)^{<v,xA^{-1}>+<a,xA^{-1}>} =$$
$$(-1)^{<a,xA^{-1}>}\cdot 2^{-n}\sum_{v\in\mathbf{F}_2^n} W_f(v)(-1)^{<v,xA^{-1}>} = (-1)^{f(xA^{-1})+<a,xA^{-1}>}.$$

Таким образом, для всех $x \in \mathbf{F}_2^n$ выполнено $F(x) = \pm 1$. Поэтому функция $f'(x)$ существует, более того, $f'(x) = f(xA^{-1}) + < a, xA^{-1} >$. □

Спектры функций f и f', переводимых один в другой аффинным преобразованием спектра, называются *аффинно эквивалентными.* Спектры функций f и f', переводимых один в другой линейным преобразованием спектра, называются *линейно эквивалентными.* Аналогично, из аффинной эквивалентности функций не следует аффинная эквивалентность их спектров. Например, потому, что при аффинном преобразовании функции f величина $wt(f)$ остается неизменной, но $wt(f) = 2^{n-1} - \frac{1}{2}W_f(0)$, поэтому переводя при аффинном преобразовании спектра в 0 набор с другим значением коэффициента Уолша, получим функцию, не являющуюся аффинно эквивалентной f. В то же время из лемм 4.1 и 4.2 видно, что линейное преобразование спектра является линейным преобразованием функции, и наоборот.

Очевидно, аффинное преобразование спектра платовидной функции f переводит его в спектр также платовидной некоторой функции f' с той же мощностью носителя спектра, а аффинное преобразование платовидной функции f переводит ее в платовидную функцию f' с той же мощностью носителя спектра.

Лемма 4.3. *Пусть f — булева функция, заданная на $\mathbf{F}_2^n$, причем носитель спектра этой функции лежит в $\mathbf{F}_2^l \otimes (\underbrace{0\ldots0}_{n-l})$. Тогда функция f зависит от переменных $x_{l+1}, \ldots, x_n$ фиктивно. Пусть f' — функция на $\mathbf{F}_2^n$, полученная из f удалением фиктивных переменных $x_{l+1}, \ldots, x_n$. Тогда для любого u из $\mathbf{F}_2^l$ выполнено $W_{f'}(u) = 2^{-(n-l)}W_f(u\underbrace{0\ldots0}_{n-l})$.*

Доказательство. Пусть x и x^i — произвольная пара наборов, соседних по i-й компоненте, $i \in \{l+1, \ldots, n\}$. По формуле обращения имеем

$$(-1)^{f(x)} - (-1)^{f(x^i)} = 2^{-n}\sum_{u\in\mathbf{F}_2^n} W_f(u)\left[(-1)^{<x,u>} - (-1)^{<x^i,u>}\right] =$$

$$2^{-n}\sum_{u\in\mathbf{F}_2^l\otimes(\underbrace{0\ldots0}_{n-l})} W_f(u)\left[(-1)^{<x,u>} - (-1)^{<x^i,u>}\right] = 0.$$

Поэтому $f(x) = f(x^i)$, и переменные $x_{l+1}, \ldots, x_n$, таким образом, действительно являются фиктивными. Рассмотрим теперь функцию f' на $\mathbf{F}_2^n$, полученную из f удалением фиктивных переменных $x_{l+1}, \ldots, x_n$. Для любого ее коэффициента

Уолша $u \in \mathbf{F}_2^l$ имеем

$$W_{f'}(u) = \sum_{x \in \mathbf{F}_2^l} (-1)^{f'(x)+<x,u>} =$$

$$2^{-(n-l)} \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+<x,u\underbrace{0\ldots0}_{n-l}>} = 2^{-(n-l)} W_f(u\underbrace{0\ldots0}_{n-l}).$$

□

Лемма 4.4. *Пусть f — булева функция, заданная на $\mathbf{F}_2^n$. Пусть f' — функция на $\mathbf{F}_2^{n+1}$, определенная как $f'(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n) + x_{n+1}$. Тогда если u — набор из $\mathbf{F}_2^{n+1}$, принадлежащий носителю спектра функции f', то $u_{n+1} = 1$ и $W_{f'}(u_1, \ldots, u_n, 1) = 2W_f(u_1, \ldots, u_n)$.*

Доказательство. Пусть $u \in \mathbf{F}_2^{n+1}$. Сгруппируем в сумме $W_{f'}(u) = \sum_{x \in \mathbf{F}_2^{n+1}} (-1)^{f(x)+<x,u>}$ в пары наборы x и x^{n+1}, различающиеся только в $(n+1)$-й компоненте. Для определенности пусть $x_{n+1} = 0$. Для этих наборов выполнено $f'(x) = f'(x^{n+1}) + 1$ Если $u_{n+1} = 0$, то $< x, u >=< x^{n+1}, u >$. Отсюда получаем, что $(-1)^{f'(x)+<x,u>} + (-1)^{f'(x^{n+1})+<x^{n+1},u>} = 0$. Поэтому и $W_{f'}(u) = 0$. Если $u_{n+1} = 1$, то $< x, u >=< x^{n+1}, u > +1$. Отсюда получаем, что $(-1)^{f'(x)+<x,u>} + (-1)^{f'(x^{n+1})+<x^{n+1},u>} = 2 \cdot (-1)^{f'(x)+<x,u>} = 2 \cdot (-1)^{f(x_1,\ldots,x_n)+<(x_1,\ldots,x_n),(u_1,\ldots,u_n)>}$. Поэтому $W_{f'}(u) = 2W_f(u_1, \ldots, u_n)$. □

Из лемм 4.1, 4.2 и 4.3 следует, что изучение платовидных функций на $\mathbf{F}_2^n$ с носителем спектра мощности 4^h можно в некотором смысле свести к изучению платовидных функций с носителем спектра той же мощности 4^h, заданных на $\mathbf{F}_2^{\mathbf{k}}$. Более того, если $\mathbf{k} > 2h$, то любую платовидную функцию f' на $\mathbf{F}_2^n$ с носителем мощности 4^h можно получить из некоторой функции f на $\mathbf{F}_2^{\mathbf{k}}$ с носителем той же мощности 4^h, добавив $n - \mathbf{k}$ фиктивных переменных и выполнив некоторое линейное преобразование функции. Того же можно добиться и в случае, если $\mathbf{k} = 2h$ и $W_{f'}(0) \neq 0$ (в этом случае функция f будет бент-функцией). Если $\mathbf{k} = 2h$ и $W_{f'}(0) = 0$, то указанного линейного преобразования функции не существует, но можно использовать аффинное преобразование спектра, либо же взять функцию f от $\mathbf{k} + 1$ переменной.

Заметим, что указанного сведения может быть недостаточно, если требуется исследовать дополнительные свойства функций, не сохраняющиеся при аффинных преобразованиях (например, корреляционную иммунность).

Укажем также на следующее свойство, позволяющее не рассматривать специально вопрос о возможных значениях, принимаемых рангом k.

Лемма 4.5. *Если существует платовидная функция с носителем спектра мощности 4^h и аффинным рангом, равным $\mathbf{k}$, то существуют платовидные функции с носителем спектра той же мощности 4^h и рангами, равными и $k = \mathbf{k}$, и $k = \mathbf{k} + 1$.*

Доказательство. По лемме 4.2 аффинное преобразование носителя спектра платовидной функции снова дает платовидную функцию с носителем спектра той же мощности и с тем же аффинным рангом. Если аффинным преобразованием перевести в ноль один из наборов, входящий в наименьший класс смежности, содержащий S_f, то для получившейся функции, очевидно, будет выполнено $k = \mathbf{k}$. Если же перевести в ноль набор, не принадлежащий наименьшему классу смежности, содержащему S_f, то для получившейся функции $k = \mathbf{k} + 1$. Если для исходной функции не было наборов, не принадлежащих наименьшему классу смежности, содержащему S_f (т. е. если $\mathbf{k}$ совпадало с числом переменных), то можно просто добавить фиктивную переменную и такие наборы появятся, а функция останется платовидной с той же мощностью спектра. □

Из вышесказанного следует, что аффинный ранг является важной характеристикой платовидных функций. Очевидно, что аффинный ранг любой платовидной функции с носителем спектра мощности 4^h не меньше $2h$, потому что меньшие классы смежности не содержат 4^h наборов. Любой платовидная функция с носителем спектра мощности 1 есть аффинная функция и, очевидно, ее аффинный ранг равен 0. Аффинный ранг любой платовидной функции с носителем спектра мощности 4 равен 2. Этот факт доказан в [94], но, по-видимому, был известен намного раньше. Платовидные функции с носителем спектра мощности 16 (не называясь платовидными) фактически рассматривались в [72], а в работе [49] для подкласса платовидных функций с носителем спектра мощно-

сти 16 (более точно, для кубических устойчивых порядка $n-4$ функций) была получена оценка $\mathbf{k} \leq k \leq 9$. В настоящей главе доказывается, что аффинный ранг любой платовидной функции с носителем спектра мощности 16 равен 4, 5 или 6. Кроме того, для любого натурального h рассматриваются платовидные функции с носителем спектра мощности 4^h, даются оценки аффинного ранга для таких функций и строятся функции, аффинный ранг которых принимает все возможные значения от $2h$ до $2^{h+1}-2$.

4.3 Вспомогательные результаты

Следующее утверждение хорошо известно (см., например, соотношение (2.15) в [19]). Ранее его доказательство было дано в [50].

Лемма 4.6. *Пусть f — булева функция на $\mathbf{F}_2^n$. Пусть U является линейным подпространством в $\mathbf{F}_2^n$ размерности l, а $U^\perp$ — пространство, ортогональное к U в $\mathbf{F}_2^n$. Пусть v — произвольный вектор из $\mathbf{F}_2^n$. Тогда*

$$\sum_{u \in U+v} W_f(u) = 2^l \sum_{x \in U^\perp} (-1)^{f(x)+<x,v>}.$$

Лемма 4.7. *Пусть f — платовидная функция с носителем спектра мощности 4^h, заданная на $\mathbf{F}_2^n$. Тогда $\sum\limits_{a \in \mathbf{F}_2^n} \phi(a) \in \{-2^h, 2^h\}$.*

Доказательство. Возьмем в лемме 4.6 в качестве подпространства U все $\mathbf{F}_2^n$. В обозначениях леммы 4.6 имеем $W_f(u) = \phi(u) \cdot 2^{n-h}$, $l = n$. Тогда $U^\perp = \{0\}$. Поэтому

$$\sum_{u \in \mathbf{F}_2^n} W_f(u) = 2^n (-1)^{f(0)}.$$

Отсюда для функции f имеем

$$\sum_{u \in \mathbf{F}_2^n} \phi(u) = 2^h (-1)^{f(0)} \in \{-2^h, 2^h\}.$$

□

Лемма 4.8. *Пусть f — платовидная функция с носителем спектра мощности 4^h, заданная на $\mathbf{F}_2^n$. Пусть $\sum\limits_{a\in\mathbf{F}_2^n}\phi(a)=2^h$. Пусть H является $(n-1)$-мерным классом смежности в $\mathbf{F}_2^n$. Тогда $\sum\limits_{a\in H}\phi(a)\in\{0,2^h\}$.*

Доказательство. В обозначениях леммы 4.6 имеем $W_f(u)=\phi(u)\cdot 2^{n-h}$, $l=n-1$. Поэтому из леммы 4.6 следует, что $\sum\limits_{a\in H}\phi(a)\in\{-2^h,0,2^h\}$. Однако если сумма равна -2^h, то $\sum\limits_{a\in\mathbf{F}_2^n\setminus H}\phi(a)=2^{h+1}$, что невозможно по сказанному выше. □

Следующее утверждение также хорошо известно (см., например, теорему 2.91 в [19]).

Лемма 4.9. *Пусть f — булева функция на $\mathbf{F}_2^n$. Пусть U является линейным подпространством в $\mathbf{F}_2^n$ размерности l, а $U^\perp$ — пространство, ортогональное к U в $\mathbf{F}_2^n$. Тогда*

$$\sum_{u\in U}W_f^2(u)=2^l\sum_{v\in U^\perp}\Delta_f(v).$$

Лемма 4.10. *Пусть f — булева функция на $\mathbf{F}_2^n$, $n\geq 1$. Тогда $wt(f)$ нечетно тогда и только тогда, когда $\deg(f)=n$.*

Доказательство очевидно (см., например, следствие 1 в [146]). □

Лемма 4.11. *Пусть f — булева функция на $\mathbf{F}_2^n$, $f\not\equiv\mathrm{const}$. Тогда $2^{n-\deg(f)}\leq wt(f)\leq 2^n-2^{n-\deg(f)}$.*

Доказательство очевидно (см., например, лемму 5.6 в [19] или лемму 3 в [146]). □

Лемма 4.12. *[125] Пусть f — платовидная булева функция на $\mathbf{F}_2^n$ с носителем спектра мощности 4^h. Тогда $\deg(f)\leq h+1$.*

Доказательство. Коэффициенты Уолша функции f принимают значения из множества $\{0,\pm 2^{n-h}\}$. Рассмотрим самое длинное слагаемое $x_{i_1}x_{i_2}\ldots x_{i_s}$ функции f (если таких слагаемых несколько, берем любое из них). Можно считать, что $s\geq 2$, иначе утверждение автоматически является верным.

Воспользуемся леммой 4.6. Возьмем в качестве U линейное подпространство $U = \{x \in \mathbf{F}_2^n \,|\, x_{i_1} = 0, \ldots, x_{i_s} = 0\}$ размерности $l = n - s$, вектор v возьмем нулевым. Тогда ортогональное пространство $U^\perp$ по лемме 4.10 содержит нечетное число наборов x, таких что $f(x) = 1$. Поэтому сумма $\sum\limits_{x \in U^\perp} (-1)^{f(x)}$ при $s \geq 2$ не делится на 4. Следовательно, в равенстве

$$\sum_{u \in U} W_f(u) = 2^{n-s} \sum_{x \in U^\perp} (-1)^{f(x)}$$

левая часть делится на 2^{n-h}, а правая часть не делится на 2^{n-s+2}. Отсюда $n-h < n-s+2$, а учитывая целочисленность, получаем, что $s \leq h+1$, что и требовалось доказать. □

Лемма 4.13. *Пусть f — платовидная булева функция на $\mathbf{F}_2^n$ с носителем спектра мощности 4^h. Пусть H является $(n-1)$-мерным классом смежности в $\mathbf{F}_2^n$. Тогда либо $\sum\limits_{u \in H} |\phi(u)| = 0$, либо $\sum\limits_{u \in H} |\phi(u)| = 4^h$, либо $2^h \leq \sum\limits_{u \in H} |\phi(u)| \leq 4^h - 2^h$.*

Доказательство. Пусть сначала H — линейное подпространство в $\mathbf{F}_2^n$. Тогда $H^\perp = \{0, v\}$ для некоторого ненулевого $v \in \mathbf{F}_2^n$. Очевидно, $\Delta_f(0) = 2^n$. По лемме 4.9 имеем

$$4^{n-h} \sum_{u \in H} |\phi(u)| = 2^{n-1}(2^n + \Delta_f(v)) = 4^n - 2^n wt(D_v f).$$

По лемме 4.12 выполнено $\deg(f) \leq h + 1$. Функция $D_v f$ является производной функции f, поэтому $\deg(D_v f) \leq h$. Если $D_v f \equiv 0$, то $\sum\limits_{u \in H} |\phi(u)| = 4^h$. Если $D_v f \equiv 1$, то $\sum\limits_{u \in H} |\phi(u)| = 0$. Если $D_v f \not\equiv \text{const}$, то по лемме 4.11 имеем $2^{n-h} \leq wt(D_v f) \leq 2^n - 2^{n-h}$. Отсюда $2^h \leq \sum\limits_{u \in H} |\phi(u)| \leq 4^h - 2^h$, что и требовалось. Для класса смежности $\mathbf{F}_2^n \setminus H$ точно такие же три случая имеют место в силу только что доказанного и равенства Парсеваля. □

Лемма 4.14. *Пусть f_1, f_2 — булевы функции на $\mathbf{F}_2^n$, а f — булева функция на $\mathbf{F}_2^{n+1}$, причем $f(xx_{n+1}) = (x_{n+1} + 1)f_1(x) + x_{n+1}f_2(x)$. Тогда $W_f(u0) = W_{f_1}(u) + W_{f_2}(u)$, а $W_f(u1) = W_{f_1}(u) - W_{f_2}(u)$.*

Эта лемма очень хорошо известна. Фактически на ее применении основано быстрое преобразование Уолша. □

4.4 Об аффинном ранге платовидных булевых функций с носителем спектра мощности 16

В этом параграфе найдены все возможные значения аффинного ранга $\mathbf{k}$ платовидных булевых функций с носителем спектра мощности 16.

Ранее в работе [49] для подкласса платовидных функций с носителем спектра мощности 16 (более точно, для кубических устойчивых порядка $n-4$ функций) была получена оценка $\mathbf{k} \leq k \leq 9$. В этом параграфе доказано, что аффинный ранг любой платовидной функции с носителем спектра мощности 16 равен 4, 5 или 6.

Во всех утверждениях этого параграфа предполагается, что f – платовидная булева функция на $\mathbf{F}_2^n$ и $|S_f| = 16$. В этом случае $c = n - 2$. По лемме 4.7 имеет место один из двух случаев $|T^+| = 10$, $|T^-| = 6$, или же $|T^+| = 6$, $|T^-| = 10$. Учитывая, что для всех u выполнено $W_f(u) = -W_{f+1}(u)$, можно без ограничения общности считать, что $|T^+| = 10$, $|T^-| = 6$, что и будем делать в дальнейшем в этом параграфе. Таким образом, имеем $|S_f| = 16$, $|T^+| = 10$, $|T^-| = 6$.

Нашей целью является доказательство следующей теоремы.

Теорема 4.1. *Пусть f является платовидной функцией, $|S_f| = 16$. Тогда для аффинного ранга $\mathbf{k}$ носителя спектра S_f справедливо неравенство $\mathbf{k} \leq 6$.*

Доказательство теоремы 4.1 будет получено путем доказательства серии лемм.

Предположим, что аффинный ранг носителя спектра S_f равен $\mathbf{k}$ и аффинный ранг T^- равен $\mathbf{k}^-$. Очевидно, $3 \leq \mathbf{k}^- \leq 5$. Легко видеть, что с помощью некоторого аффинного отображения в $\mathbf{F}_2^n$ можно вложить наименьший класс смежности, содержащий носитель спектра S_f, в $\mathbf{F}_2^{\mathbf{k}} \otimes (\underbrace{0 \ldots 0}_{n-\mathbf{k}})$, так чтобы некоторые $\mathbf{k}^- + 1$ наборов из T^- перешли в наборы $(0, 0, 0, \ldots, 0)$, $(1, 0, 0, \ldots, 0)$,

$(0,1,0,\ldots,0)$, $\ldots$, $(\underbrace{0,0,\ldots,0,1}_{\mathbf{k}^-},0,\ldots,0)$. Заметим, что после такого отображения все наборы из T^- перейдут в наборы, имеющие только нули во всех компонентах i, $i > \mathbf{k}^-$. Отметим, что описанное выше аффинное отображение спектра не является, вообще говоря, аффинным преобразованием функции f, однако нам этого и не нужно. Нам достаточно того, что получившаяся в результате отображения булева функция будет платовидной с тем же наборов значений, принимаемых коэффициентами Уолша, и тем же значениями $\mathbf{k}$ и $\mathbf{k}^-$. По лемме 4.3 переменные с $(\mathbf{k}+1)$-й по n-ю у получившейся функции будут фиктивными. Отбрасывая их и деля все коэффициенты Уолша на $2^{n-\mathbf{k}}$, по леммам 4.2 и 4.3 получим платовидную функцию, заданную на $\mathbf{F}_2^{\mathbf{k}}$, с носителем спектра той же мощности 16. Таким образом, без потери общности в оставшейся части этого параграфа будем рассматривать именно такой носитель спектра.

Лемма 4.15. *Пусть H является $(\mathbf{k}-1)$-мерным классом смежности в $\mathbf{F}_2^{\mathbf{k}}$. Тогда $\sum\limits_{a\in H}\phi(a) \in \{0,4\}$.*

Доказательство. Утверждение леммы является частным случаем леммы 4.8. □

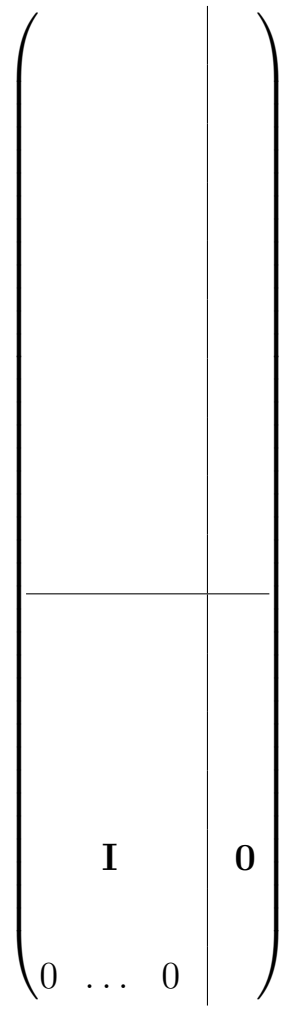
Лемма 4.16. *[49] Пусть H является $(\mathbf{k}-1)$-мерным классом смежности в $\mathbf{F}_2^{\mathbf{k}}$. Тогда H содержит 4, 6, 8, 10 или 12 наборов из S_f.*

Доказательство. В силу леммы 4.15 класс H содержит четное число наборов из S_f. Случаи 2 и 14 невозможны в силу леммы 4.13. Если H содержит 16 наборов из S_f, то S_f содержится в H; если H содержит 0 наборов из S_f, то S_f содержится в $\mathbf{F}_2^{\mathbf{k}} \setminus H$. Оба последних случая невозможны в силу того, что $\mathbf{F}_2^{\mathbf{k}}$ — наименьший класс смежности, содержащий носитель спектра S_f. □

Нашей целью является доказать, что $\mathbf{k} \le 6$. Предположим противное. Пусть $\mathbf{k} \ge 7$. Докажем, что это невозможно.

Образуем матрицу M размера 16×7. В строках M будем записывать слева направо первые 7 компонент наборов из S_f (в случае $\mathbf{k} > 7$ мы опустим все компоненты после седьмой). В первых 10 строках M запишем наборы из T^+, а в последних 6 строках M запишем наборы из T^-. Левые $\mathbf{k}^-$ столбцов M назовем

левой частью M, оставшиеся $7 - \mathbf{k}^-$ столбцов назовем *правой частью* M.



Обозначим через γ_i столбцы из левой части M, а через x_i — соответствующие этим столбцам переменные. Обозначим через δ_j столбцы из правой части M, а через y_j — соответствующие этим столбцам переменные. Обозначим через γ_i^+ и δ_j^+ подстолбцы, содержащие верхние 10 элементов столбцов γ_i и δ_j, соответственно.

Лемма 4.17. *Для любого множества* $\delta_{j_1}, \ldots, \delta_{j_s}$, $1 \le s \le 7 - \mathbf{k}^-$, *различных столбцов из правой части* M *выполнено* $wt(\delta_{j_1}^+ + \cdots + \delta_{j_s}^+) = 4$.

Доказательство. Обозначим $H = \{F_2^{\mathbf{k}} \mid y_{j_1} + \cdots + y_{j_s} = 0\}$. Гиперплоскость H содержит все 6 наборов из T^-, поэтому по лемме 4.15 гиперплоскость H должна содержать 6 или 10 наборов из T^+. Однако если H содержит 10 наборов из T^+, то H содержит S_f. Это невозможно, поскольку $\mathbf{k}$ есть размерность наименьшего класса смежности, содержащего S_f. Поэтому H содержит 12 наборов из S_f и $\mathbf{F}_2^n \setminus H$ содержит в точности 4 набора из S_f. □

Лемма 4.18. *Существует не более* 3 *столбцов, удовлетворяющих условию леммы 4.17. Без потери общности можно выбрать в качестве этих столбцов* $\delta_1^+ = (0,0,0,0,0,0,1,1,1,1)^T$, $\delta_2^+ = (0,0,0,0,1,1,0,0,1,1)^T$, $\delta_3^+ = (0,0,0,1,0,1,0,1,0,1)^T$.

Доказательство. Легко проверить, что наборы $\delta_1^+, \delta_2^+, \delta_3^+$, указанные в условии, могут быть взяты без потери общности. Предположим, что можно добавить к этому множеству некоторый набор δ_4^+. Для $c_1, c_2, c_3 \in \{0,1\}$ обозначим $\delta^+(c_1,c_2,c_3) = c_1\delta_1^+ + c_2\delta_2^+ + c_3\delta_3^+$. Рассмотрим сумму

$$S = \sum_{c_1,c_2,c_3 \in \{0,1\}} d(\delta_4^+, \delta^+(c_1,c_2,c_3)).$$

Заметим, что для любой строки с 4-й по 10-ю в точности 4 из 8 наборов $\delta^+(c_1,c_2,c_3)$ имеют единицу в этой строке. Поэтому $S = 28 + 8w_0 = 32$, где w_0 — это число единиц в δ_4^+ в строках с 1-й по 3-ю. Отсюда следует, что $w_0 = 0,5$, но w_0 должно быть целым числом. Это противоречие доказывает лемму 4.18. □

Лемма 4.19. *Правая часть матрицы* M *содержит не более* 3 *столбцов.*

Доказательство следует из лемм 4.17 и 4.18. □

Из леммы 19 следует, что случай $\mathbf{k}^- = 3$ невозможен. Остались случаи $\mathbf{k}^- = 4$ и $\mathbf{k}^- = 5$.

Лемма 4.20. *Пусть* γ_i *— столбец из левой части матрицы* M*. Предположим, что* γ_i *содержит* 1 *единицу и* 5 *нулей в нижних* 6 *строках. Тогда* $wt(\gamma_i^+) = 5$.

Доказательство. Обозначим $H = \{F_2^{\mathbf{k}} \mid x_i = 0\}$. Гиперплоскость H содержит в точности 5 наборов из T^-, поэтому по лемме 4.15 гиперплоскость H должна содержать 5 или 9 наборов из T^+. Однако если H содержит 9 наборов из T^+, то H содержит в точности 14 наборов из S_f. Это невозможно по лемме 4.16. Отсюда следует, что $wt(\gamma_i^+) = 5$. □

Лемма 4.21. *Пусть* γ_i *— столбец из левой части матрицы* M*. Предположим, что* γ_i *содержит* 2 *единицы и* 4 *нуля в нижних* 6 *компонентах. Тогда* $wt(\gamma_i^+) \in \{2,6\}$.

Доказательство. Обозначим $H = \{F_2^{\mathbf{k}} \,|\, x_i = 0\}$. Гиперплоскость H содержит в точности 4 набора из T^-, поэтому по лемме 4.15 гиперплоскость H должна содержать 4 или 8 наборов из T^+. Отсюда следует, что $wt(\gamma_i^+) = 2$ или 6. □

Рассмотрим теперь отдельно случаи $\mathbf{k}^- = 4$ и $\mathbf{k}^- = 5$.

Случай $\mathbf{k}^- = 5$.

В этом случае правая часть матрицы M содержит два столбца. По лемме 4.18 без ограничения общности можно предположить, что эти столбцы есть $\delta_1 = (0,0,0,0,0,0,1,1,1,1)^T$ и $\delta_2 = (0,0,0,0,1,1,0,0,1,1)^T$. Без ограничения общности можно считать, что матрица M имеет вид

$$\left(\begin{array}{ccccc|cc}
* & * & * & * & * & 0 & 0 \\
* & * & * & * & * & 0 & 0 \\
* & * & * & * & * & 0 & 0 \\
* & * & * & * & * & 0 & 0 \\
* & * & * & * & * & 0 & 1 \\
* & * & * & * & * & 0 & 1 \\
* & * & * & * & * & 1 & 0 \\
* & * & * & * & * & 1 & 0 \\
* & * & * & * & * & 1 & 1 \\
* & * & * & * & * & 1 & 1 \\
\hline
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right).$$

По лемме 4.20 все столбцы γ_i^+, $i = 1,2,3,4,5$, содержат в точности 5 единиц.

Лемма 4.22. *Пусть* $\mathbf{k}^- = 5$. *Тогда для* $1 \le i_1 < i_2 \le 5$, *имеем* $d(\gamma_{i_1}^+, \gamma_{i_2}^+) \in \{2,6\}$.

Доказательство. Обозначим $H = \{F_2^{\mathbf{k}} \,|\, x_{i_1} + x_{i_2} = 0\}$. Гиперплоскость H содержит в точности 4 набора из T^-, поэтому по лемме 4.15 гиперплоскость

H должна содержать 4 или 8 наборов из T^+. Отсюда следует, что $d(\gamma_{i_1}^+, \gamma_{i_2}^+) = wt(\gamma_{i_1}^+ + \gamma_{i_2}^+) \in \{2, 6\}$. □

Лемма 4.23. *Пусть* $\mathbf{k}^- = 5$. *Тогда для любых* $i \in \{1, 2, 3, 4, 5\}$, $c_1, c_2 \in \{0, 1\}$, *имеем* $d(\gamma_i^+, c_1\delta_1^+ + c_2\delta_2^+) = 5$.

Доказательство. Обозначим $H = \{F_2^{\mathbf{k}} \mid x_i + c_1 y_1 + c_2 y_2 = 0\}$. Гиперплоскость H содержит в точности 5 наборов из T^-, поэтому по лемме 4.15 гиперплоскость H должна содержать 5 или 9 наборов из T^+. Однако если H содержит 9 наборов из T^+, то H содержит в точности 14 наборов из S_f. Это невозможно по лемме 4.16. Отсюда следует, что $d(\gamma_i^+, c_1\delta_1^+ + c_2\delta_2^+) = wt(\gamma_i^+ + c_1\delta_1^+ + c_2\delta_2^+) = 5$. □

Лемма 4.24. *Пусть* $\mathbf{k}^- = 5$. *Тогда для любого* i, $i \in \{1, 2, 3, 4, 5\}$, *столбец* γ_i^+ *содержит в точности* 2 *единицы в строках с* 1*-й по* 4*-ю, в точности* 1 *единицу в строках* $5, 6$, *в точности* 1 *единицу в строках* $7, 8$, *в точности* 1 *единицу в строках* $9, 10$.

Доказательство. Если γ_i^+ содержит 0 единиц в строках $9, 10$, то из равенства $d(\gamma_i^+, \delta_1^+) = d(\gamma_i^+, \delta_2^+) = 5$ следует, что γ_i^+ содержит только единицы в строках $5, 6, 7, 8$. Однако в этом случае $d(\gamma_i^+, \delta_1^+ + \delta_2^+) = 1$, что дает противоречие с леммой 4.23. Если γ_i^+ содержит 2 единицы в строках $9, 10$, то из равенства $d(\gamma_i^+, \delta_1^+) = d(\gamma_i^+, \delta_2^+) = 5$ следует, что γ_i^+ содержит только нули в строках $5, 6, 7, 8$. Однако в этом случае $d(\gamma_i^+, \delta_1^+ + \delta_2^+) = 9$, что дает противоречие с леммой 4.23. Поэтому γ_i^+ содержит в точности 1 единицу в строках $9, 10$. Отсюда следует, что γ_i^+ содержит в точности 1 единицу в строках $7, 8$, в точности 1 единицу в строках $5, 6$ и в точности 2 единиц в строках с 1-й по 4-ю. □

Лемма 4.25. *Случай* $\mathbf{k}^- = 5$ *невозможен.*

Доказательство. Существует ровно 3 пары противоположных наборов длины 4 с в точности 2 единицами. Поэтому в левой части M найдутся два столбца γ_{i_1} и γ_{i_2}, которые либо идентичны, либо противоположны в верхних 4 строках. Пусть γ_{i_3} — еще какой-то столбец в левой части M, $i_1 \neq i_3$, $i_2 \neq i_3$. Тогда из леммы 4.24 легко видеть, что каждая группа строк (1–4), $(5, 6)$, $(7, 8)$, $(9, 10)$

дает в сумму $S = d(\gamma_{i_1}^+, \gamma_{i_2}^+) + d(\gamma_{i_1}^+, \gamma_{i_3}^+) + d(\gamma_{i_2}^+, \gamma_{i_3}^+)$ вклад, делящийся на 4. Поэтому сумма S делится на 4. С другой стороны, по лемме 4.22 все слагаемые в S сравнимы с 2 по модулю 4. Поэтому S также сравнима с 2 по модулю 4. Это противоречие доказывает лемму 4.25. □

Таким образом, доказано, что случай $\mathbf{k}^- = 5$ невозможен.

Случай $\mathbf{k}^- = 4$.

В этом случае правая часть матрицы M содержит в точности три столбца. По лемме 18 без ограничения общности можем предположить, что эти столбцы есть $\delta_1 = (0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 1,\ 1)^T$, $\delta_2 = (0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 1,\ 1)^T$, $\delta_3 = (0, 0, 0, 1, 0, 1, 0, 1, 0, 1)^T$. Без ограничения общности можем предположить, что матрица M имеет вид

$$\left(\begin{array}{cccc|ccc} * & * & * & * & 0 & 0 & 0 \\ * & * & * & * & 0 & 0 & 0 \\ * & * & * & * & 0 & 0 & 0 \\ * & * & * & * & 0 & 0 & 1 \\ * & * & * & * & 0 & 1 & 0 \\ * & * & * & * & 0 & 1 & 1 \\ * & * & * & * & 1 & 0 & 0 \\ * & * & * & * & 1 & 0 & 1 \\ * & * & * & * & 1 & 1 & 0 \\ * & * & * & * & 1 & 1 & 1 \\ \hline * & * & * & * & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Пусть $c_1, c_2, c_3 \in \{0, 1\}$. Обозначим $\delta^+(c_1, c_2, c_3) = c_1\delta_1^+ + c_2\delta_2^+ + c_3\delta_3^+$.

Лемма 4.26. *Пусть $\mathbf{k}^- = 4$. Тогда никакой столбец γ_i в левой части матрицы M не может иметь ноль в 11-й строке.*

Доказательство. Предположим, что некоторый столбец γ_i имеет ноль в 11-

й строке. Тогда по лемме 4.20 имеет место $wt(\gamma_i^+) = 5$. Тем же самым путем, что и в лемме 4.23, можно показать, что для любых $c_1, c_2, c_3 \in \{0,1\}$ выполнено $d(\gamma_i^+, \delta^+(c_1,c_2,c_3)) = 5$. Рассмотрим сумму

$$S = \sum_{c_1,c_2,c_3 \in \{0,1\}} d(\gamma_i^+, \delta^+(c_1,c_2,c_3)).$$

Заметим, что для любой строки с 4-й по 10-ю в точности 4 из 8 наборов $\delta^+(c_1,c_2,c_3)$ имеют единицу в этой строке. Поэтому $S = 28+8w_0 = 40$, где w_0 — это число единиц в γ_i в строках с 1-й по 3-ю. Отсюда следует, что $w_0 = 1{,}5$, но w_0 должно быть целым числом. Это противоречие доказывает лемму 4.26. □

Из леммы 4.26 следует, что без ограничения общности матрица M имеет вид

$$\left(\begin{array}{cccc|ccc}
* & * & * & * & 0 & 0 & 0 \\
* & * & * & * & 0 & 0 & 0 \\
* & * & * & * & 0 & 0 & 0 \\
* & * & * & * & 0 & 0 & 1 \\
* & * & * & * & 0 & 1 & 0 \\
* & * & * & * & 0 & 1 & 1 \\
* & * & * & * & 1 & 0 & 0 \\
* & * & * & * & 1 & 0 & 1 \\
* & * & * & * & 1 & 1 & 0 \\
* & * & * & * & 1 & 1 & 1 \\
\hline
1 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right).$$

Лемма 4.27. *Пусть* $\mathbf{k}^- = 4$. *Тогда для любых* $1 \le i_1 < i_2 \le 4$ *выполнено* $d(\gamma_{i_1}^+, \gamma_{i_2}^+) \in \{2,6\}$.

Доказательство. Обозначим $H = \{F_2^{\mathbf{k}} \mid x_{i_1} + x_{i_2} = 0\}$. Гиперплоскость H содержит в точности 4 набора из T^-, поэтому по лемме 4.15 гиперплоскость

H должна содержать 4 или 8 наборов из T^+. Отсюда следует, что $d(\gamma_{i_1}^+, \gamma_{i_2}^+) \in \{2, 6\}$. □

Лемма 4.28. *Пусть* $\mathbf{k}^- = 4$. *Тогда любой столбец* γ_i *в левой части матрицы* M *имеет в точности* 2 *единицы в строках с* 1*-й по* 3*-ю и совпадает в строках с* 4*-й по* 10*-ю с вектор-столбцом* $\delta^+(c_1, c_2, c_3)$ *при некоторых* $c_1, c_2, c_3 \in \{0, 1\}$.

Доказательство. По лемме 4.21 имеем $wt(\gamma_i^+) \in \{2, 6\}$. Тем же самым способом можно показать, что для любых $c_1, c_2, c_3 \in \{0, 1\}$ выполнено $d(\gamma_i^+, \delta^+(c_1, c_2, c_3)) \in \{2, 6\}$.

Предположим, что $wt(\gamma_i^+) = 2$. Если γ_i^+ не содержит обе свои единицы в строках с 1-й по 3-ю, то легко найти некоторые $c_1, c_2, c_3 \in \{0, 1\}$, такие что набор $\delta^+(c_1, c_2, c_3)$ содержит в точности 1 единицу в тех строках, где и γ_i^+ имеет единицу. Тогда будет выполнено $d(\gamma_i^+, \delta^+(c_1, c_2, c_3)) = 4$, что невозможно. Поэтому γ_i^+ содержит обе свои единицы в строках с 1-й по 3-ю и совпадает в строках с 4-й по 10-ю с набором $\delta^+(0, 0, 0)$, т. е. имеет требуемый вид.

Теперь предположим, что $wt(\gamma_i^+) = 6$. Рассмотрим сумму

$$S = \sum_{c_1, c_2, c_3 \in \{0,1\}} d(\gamma_i^+, \delta^+(c_1, c_2, c_3)).$$

Заметим, что для любой строки с 4-й по 10-ю в точности 4 из 8 наборов $\delta^+(c_1, c_2, c_3)$ имеют единицу в этой строке. Поэтому $S = 28 + 8w_0$, где w_0 — это число единиц в γ_i в строках с 1-й по 3-ю. Если для любых $c_1, c_2, c_3 \in \{0, 1\}$ выполнено $d(\gamma_i^+, \delta^+(c_1, c_2, c_3)) = 6$, то $S = 48$ и $w_0 = 2{,}5$. Однако w_0 должно быть целым числом. Поэтому существует набор значений $c_1, c_2, c_3 \in \{0, 1\}$, такой что $d(\gamma_i^+, \delta^+(c_1, c_2, c_3)) = 2$. Обозначим $\delta^+(c_1, c_2, c_3)$ через δ_0^+. Тогда $wt(\gamma_i^+ + \delta_0^+) = 2$ и для любых $c_1, c_2, c_3 \in \{0, 1\}$ имеет место $d(\gamma_i^+ + \delta_0^+, \delta^+(c_1, c_2, c_3)) \in \{2, 6\}$. Как было указано в начале этого доказательства, набор $\gamma_i^+ + \delta_0^+$ должен иметь в точности 2 единицы в строках с 1-й по 3-ю и одни нули в строках с 4-й по 10-ю. Следовательно, набор γ_i^+ имеет в точности 2 единиц в строках с 1-й по 3 и совпадает с набором δ_0^+ в строках с 4-й по 10-ю. □

Лемма 4.29. *Случай* $\mathbf{k}^- = 4$ *невозможен.*

Доказательство. По лемме 4.28 все столбцы γ_i в левой части M имеют в точности 2 единицы в строках с 1-й по 3-ю. Левая часть M содержит 4 столбца, поэтому среди них найдутся столбцы γ_{i_1} и γ_{i_2}, $1 \le i_1 < i_2 \le 4$, совпадающие в строках с 1-й по 3-ю). В строках с 4-й по 10-ю столбцы γ_{i_1} и γ_{i_2} совпадают по лемме 4.28 с некоторыми вектор-столбцами $\delta^+(c'_1, c'_2, c'_3)$ и $\delta^+(c''_1, c''_2, c''_3)$, соответственно. По лемме 4.17 имеем $d(\delta^+(c'_1, c'_2, c'_3), \delta^+(c''_1, c''_2, c''_3)) \in \{0, 4\}$. Отсюда $d(\gamma^+_{i_1}, \gamma^+_{i_2}) \in \{0, 4\}$, что противоречит лемме 4.27. □

Все случаи рассмотрены. Теорема 4.1 доказана.

Таким образом, показано, что аффинный ранг платовидных функций с носителем спектра мощности 16 не может принимать никаких значений, кроме 4, 5 и 6. Функции с такими параметрами известны, и их примеры приводились, например, в [49], поэтому здесь не будут отдельно приводиться примеры. Эти примеры будут построены в следующем параграфе в рамках общей конструкции.

4.5 Оценки для аффинного ранга платовидных функций с произвольной мощностью носителя спектра

Лемма 4.30. *Пусть существует платовидная функция с носителем спектра мощности 4^h и аффинным рангом $\mathbf{k}$. Тогда для любого натурального s, удовлетворяющего неравенствам $\mathbf{k} + 2 \le s \le 2\mathbf{k} + 2$ существует платовидная функция с носителем спектра мощности 4^{h+1} и аффинным рангом s.*

Доказательство. Если существует платовидная функция с носителем спектра мощности 4^h и аффинным рангом $\mathbf{k}$, то из нее по леммам 4.2 и 4.3 аффинным преобразованием спектра и последующим удалением фиктивных переменных можно получить платовидную функцию f на $\mathbf{F}_2^{\mathbf{k}}$ с носителем спектра мощности 4^h, причем так, чтобы спектру функции f принадлежал и нулевой набор, и все наборы веса 1. Рассмотрим функцию $f_1(x_1, \ldots, x_s) = f(x_{s-\mathbf{k}}, \ldots, x_{s-1}) + x_s$ на $\mathbf{F}_2^s$ (переменные x_1, …, $x_{s-\mathbf{k}-1}$ у функции f_1 будут

фиктивными). По леммам 4.3 и 4.4 функция f_1 снова будет платовидной с той же мощностью носителя, причем ко всем наборам из S_f в носителе спектра S_{f_1} слева припишется $s-\mathbf{k}-1$ нулей, а справа припишется единица. Линейное подпространство размерности $\mathbf{k}$ в $\mathbf{F}_2^{\mathbf{k}}$, содержавшее S_f при переходе к функции f_1 перейдет в класс смежности размерности $\mathbf{k}$ в $\mathbf{F}_2^s$, содержащий S_{f_1}, но линейным подпространством не являющийся. Поэтому ранг функции f_1 равен $\mathbf{k}+1$. Заметим, что носителю спектра S_{f_1} принадлежат следующие наборы: все наборы веса 2 с единицами в компонентах i и s, $i = s-\mathbf{k},\ldots,s-1$, а также набор веса 1 с единицей в компоненте s. Образуем функцию $f_2(x_1,\ldots,x_s) = f_1(x_s,\ldots,x_1)$ на $\mathbf{F}_2^s$, переименовав все переменные в обратном порядке. Ясно, что функция f_2 будет обладать свойствами, аналогичными свойствам функции f_1. Носителю спектра S_{f_2} принадлежат в числе прочих следующие наборы: все наборы веса 2 с единицами в компонентах 1 и i, $i = 2,\ldots,\mathbf{k}+1$, а также набор веса 1 с единицей в компоненте 1. Заметим, что во всех наборах из S_{f_1} в первой компоненте ноль, а во всех наборах из S_{f_2} в первой компоненте единица. Поэтому множества S_{f_1} и S_{f_2} в $\mathbf{F}_2^s$ не пересекаются.

Образуем функцию

$$f'(x_1,\ldots,x_{s+1}) = (x_{s+1}+1)f_1(x_1,\ldots,x_s) + x_{s+1}f_2(x_1,\ldots,x_s)$$

на $\mathbf{F}_2^{s+1}$. По лемме 4.14 для любого $u \in \mathbf{F}_2^s$ выполнено $W_{f'}(u0) = W_{f_1}(u)+W_{f_2}(u)$, $W_f(u1) = W_{f_1}(u)-W_{f_2}(u)$. Как было указано выше, множества S_{f_1} и S_{f_2} в $\mathbf{F}_2^s$ не пересекаются. Поэтому каждый набор u из S_{f_1} и S_{f_2} в $\mathbf{F}_2^s$ даст ровно два набора $u0$ и $u1$, входящие в носитель спектра $S_{f'}$ функции f' на $\mathbf{F}_2^{s+1}$, причем значения ненулевых коэффициентов Уолша функции f' будут теми же самыми, что и значения ненулевых коэффициентов Уолша функций f_1 и f_2. Таким образом, мощность $S_{f'}$ равна 4^{h+1}, и функция f' также является платовидной функцией.

Из сказанного выше следует, что $S_{f'}$ принадлежат все наборы веса 2 с единицами в компонентах 1 и i, $i = 2,\ldots,\mathbf{k}+1$, все наборы веса 2 с единицами в компонентах i и s, $i = s-\mathbf{k},\ldots,s-2,s-1,s+1$, а также наборы веса 1 с единицей в компонентах 1, s. Легко видеть, что ранг вышеуказанной системы наборов равен $s+1$. Поэтому ранг функции f' на $\mathbf{F}_2^{s+1}$ равен $s+1$. В то же время для любого набора из $S_{f'}$ сумма значений 1-й и s-й компонент равна 1.

Поэтому S_f принадлежит гиперплоскости $H = \{x \in \mathbf{F}_2^{s+1} \mid x_1 + x_s = 1\}$, и аффинный ранг функции f' меньше, чем $s+1$, но он не меньше чем ранг функции f' без единицы, и поэтому аффинный ранг функции f' равен s. Таким образом, требуемая функция построена. □

Теорема 4.2. *Для любого натурального* $\mathbf{k}$*, удовлетворяющего неравенствам* $2h \le \mathbf{k} \le 2^{h+1} - 2$ *существует платовидная функция с носителем спектра мощности* 4^h *и аффинным рангом* $\mathbf{k}$*.*

Доказательство. Проведем доказательство индукцией по h. При $h = 1$ величина $\mathbf{k}$ может быть равна только 2. Такой функцией является, например, бент-функция x_1x_2 на $\mathbf{F}_2^2$. (Если не хотим считать бент-функцию платовидной функцией, то добавим к ней фиктивную переменную.) Если утверждение теоремы верно для h, то его справедливость для $h+1$ немедленно следует из леммы 4.30. □

Следствие 4.1. *Аффинный ранг платовидной функции с носителем спектра мощности* 16 *может принимать только значения* 4, 5 *и* 6*.*

Доказательство. Верхняя оценка $\mathbf{k} \le 6$ доказана в теореме 4.1. Нижняя оценка $\mathbf{k} \ge 4$ очевидна. Существование функций с $\mathbf{k} = 4, 5, 6$ следует из теоремы 4.2. Заметим, что примеры таких функций даны в [49]. □

Тривиальной верхней оценкой аффинного ранга $\mathbf{k}$ платовидной функции с носителем спектра мощности 4^h является $\mathbf{k} \le 4^h - 1$. Приведем несколько улучшенную оценку.

Теорема 4.3. *Пусть* f *является платовидной функцией,* $|S_f| = 4^h$*. Тогда для аффинного ранга* $\mathbf{k}$ *носителя спектра* S_f *справедливо неравенство* $\mathbf{k} \le 2^{2h-1} - 2^{h-1} + h$*.*

Доказательство. Будем следовать путем, аналогичным доказательству теоремы 4.1. По лемме 4.8 выполнено $|T^+|, |T^-| \in \{2^{2h-1} + 2^{h-1}, 2^{2h-1} - 2^{h-1}\}$. Без ограничения общности можно считать, что $|T^+| = 2^{2h-1} + 2^{h-1}$, $|T^-| = 2^{2h-1} - 2^{h-1}$. Предположим, что аффинный ранг носителя спектра S_f равен

$\mathbf{k}$ и аффинный ранг T^- равен $\mathbf{k}^-$. Очевидно, $\mathbf{k}^- \leq 2^{2h-1} - 2^{h-1} - 1$. Легко видеть, что с помощью некоторого аффинного отображения в $\mathbf{F}_2^n$ можно вложить наименьший класс смежности, содержащий носитель спектра S_f, в $\mathbf{F}_2^{\mathbf{k}} \otimes (\underbrace{0 \ldots 0}_{n-\mathbf{k}})$, так чтобы некоторые $\mathbf{k}^- + 1$ наборов из T^- перешли в наборы $(0,0,0,\ldots,0), (1,0,0,\ldots,0), (0,1,0,\ldots,0), \ldots, (\underbrace{0,0,\ldots,0,1}_{\mathbf{k}^-},0,\ldots,0)$. Получившаяся в результате отображения булева функция будет платовидной с тем же наборов значений, принимаемых коэффициентами Уолша, и тем же значениями $\mathbf{k}$ и $\mathbf{k}^-$. По лемме 4.3 переменные с $(\mathbf{k}+1)$-й по n-ю у получившейся функции будут фиктивными. Отбрасывая их и деля все коэффициенты Уолша на $2^{n-\mathbf{k}}$, по леммам 4.2 и 4.3 получим платовидную функцию, заданную на $\mathbf{F}_2^{\mathbf{k}}$, с носителем спектра той же мощности 2^h. Таким образом, без потери общности в оставшейся части этого параграфа будем рассматривать именно такой носитель спектра.

Образуем матрицу M размера $4^h \times \mathbf{k}$. В строках M будем записывать слева направо наборы из S_f. В первых $2^{2h-1} + 2^{h-1}$ строках M запишем наборы из T^+, а в последних $2^{2h-1} - 2^{h-1}$ строках M запишем наборы из T^-. Левые $\mathbf{k}^-$ столбцов M назовем *левой частью* M, оставшиеся $\mathbf{k} - \mathbf{k}^-$ столбцов назовем *правой частью* M. Из того, что $|T^-| = 2^{2h-1} - 2^{h-1}$, имеем $\mathbf{k}^- \leq 2^{2h-1} - 2^{h-1} - 1$.

Обозначим через δ_j столбцы из правой части M, а через y_j — соответствующие этим столбцам переменные. Обозначим через δ_j^+ подстолбцы, содержащие верхние $2^{2h-1} + 2^{h-1}$ элементов столбцов δ_j соответственно.

Лемма 4.31. *Для любого множества $\delta_{j_1}, \ldots, \delta_{j_s}$, $1 \leq s \leq \mathbf{k} - \mathbf{k}^-$, различных столбцов из правой части M выполнено $wt(\delta_{j_1}^+ + \cdots + \delta_{j_s}^+) = 2^h$.*

Доказательство. Обозначим $H = \{(x,y) \in F_2^{\mathbf{k}} \,|\, y_{j_1} + \cdots + y_{j_s} = 0\}$. Гиперплоскость H содержит все $2^{2h-1} - 2^{h-1}$ наборов из T^-, поэтому по лемме 4.8 гиперплоскость H должна содержать $2^{2h-1} - 2^{h-1}$ или $2^{2h-1} + 2^{h-1}$ наборов из T^+. Однако если H содержит $2^{2h-1} + 2^{h-1}$ наборов из T^+, то H содержит S_f. Это невозможно, поскольку $\mathbf{k}$ есть размерность наименьшего класса смежности, содержащего S_f. Поэтому H содержит $4^h - 2^h$ наборов из S_f и $\mathbf{F}_2^n \setminus H$ содержит в точности 2^h наборов из S_f. $\square$

Лемма 4.32. *Правая часть матрицы M содержит не более $h+1$ столбцов.*

Доказательство. Пусть правая часть матрицы M содержит m столбцов $\delta_1, \ldots, \delta_m$. Для $c_1, \ldots, c_m \in \{0,1\}$ обозначим $\delta^+(c_1, \ldots, c_m) = c_1\delta_1^+ \cdots + c_m\delta_m^+$. Рассмотрим сумму

$$S = \sum_{c_1,\ldots,c_m \in \{0,1\}} wt(\delta^+(c_1, \ldots, c_m)).$$

Каждое слагаемое в S, кроме слагаемого, соответствующего нулевому набору, равно 2^h по лемме 4.31. Обозначим через r число строк среди верхних $2^{2h-1} + 2^{h-1}$ строк матрицы M, содержащих хотя бы одну единицу в правой части матрицы M. Заметим, что если строка в верхней части матрицы M содержит хотя бы одну такую единицу, то в точности 2^{m-1} из $2^m - 1$ ненулевых наборов $\delta^+(c_1, \ldots, c_3)$ имеют единицу в этой строке. Поэтому $S = 2^h(2^m - 1) = r \cdot 2^{m-1}$. Отсюда $r = 2^{h+1} - 2^{h-m+1}$. В силу целочисленности r имеем $m \leq h+1$, что и требовалось доказать. □

Доказательство теоремы 4.3 немедленно следует из структуры матрицы M и леммы 4.32. □

При $h = 2$ оценка теоремы 4.3 не достигается. Осмелимся выдвинуть гипотезу.

Гипотеза. Для любого натурального h максимально возможный аффинный ранг платовидной функции с носителем спектра мощности 4^h равен $2^{h+1} - 2$.

В 2015 году Саньял получил [105, 106] сильный асимптотический результат. Он доказал, что ранг (и аффинный ранг, как отличающийся от ранга не более чем на 1) произвольной булевой функции с мощностью носителя спектра $s = |S_f|$ есть $O(\sqrt{s}\log_2 s)$. Поскольку для платовидной булевой функции в наших обозначениях $s = |S_f| = 4^h$, мы получаем, что применительно к платовидной функции результат Саньяла выгладит так:

$$\mathbf{k} = O(h \cdot 2^h).$$

5 О существовании разбиений, примитивных по Агиевичу

В этой главе рассматриваются разбиения пространства $\mathbf{F}_q^n$ на аффинные подпространства. Укажем связь этого направления с основной темой диссертации. Среди конструкций платовидных вообще и бент-функций в частности, есть конструкции, в которых функция строится путем сборки из подфункций с непересекающими носителями спектра. Если все исходные функции являются платовидными с одинаковым значением модуля ненулевых коэффициентов Уолша, то полученная функция снова будет платовидной. Если при этом объединение носителей спектра подфункций есть все пространство $\mathbf{F}_2^n$, то получается бент-функция. Однако задачей является нахождение подходящего множества платовидных функций с непересекающимися носителями спектра. Оказывается, что если взять в качестве носителя спектра аффинное подпространство, то каждая платовидная функция с таким носителем спектра эквивалентна бент-функции от числа переменных, равных размерности аффинного подпространства. Более того, между множествами таких функций существует взаимно-однозначное соответствие, которое задается аффинным преобразованием носителя спектра, описанным в лемме 4.2 главы 4.

Приведем более точное задание описанной выше конструкции.

Конструкция К. Рассмотрим $\mathbf{F}_2^n$ — линейное n-мерное векторное пространство над $\mathbf{F}_2$. Булева функция от n-переменных — это отображение из $\mathbf{F}_2^n$ в $\mathbf{F}_2$. Пусть $n = n_1 + n_2$, $n_1 \leq n_2$, где n_1 и n_2 — целые неотрицательные числа одной четности. Рассмотрим разложение n-местной булевой функции f по

первым n_1 переменным:

$$f(x_1,\ldots,x_n)=\bigoplus_{\sigma\in\mathbf{F}_2^{n_1}}\left(\left(\mathop{\&}_{i=1}^{n_1}(x_i\sim\sigma_i)\right)f(\sigma_1,\ldots,\sigma_{n_1},x_{n_1+1},\ldots,x_{n_1+n_2})\right)=$$
$$\overline{x}_1\cdot\ldots\cdot\overline{x}_{n_1-1}\overline{x}_{n_1}f_1(x)\oplus\overline{x}_1\cdot\ldots\cdot\overline{x}_{n_1-1}x_{n_1}f_2(x)\oplus\overline{x}_1\cdot\ldots\cdot x_{n_1-1}\overline{x}_{n_1}f_3(x)\oplus$$
$$x_1\cdot\ldots\cdot x_{n_1-1}x_{n_1}f_{2^{n_1}}(x).$$

где f_i — функции от правых n_2 переменных.

Пространство $\mathbf{F}_2^{n_2}$ от правых n_2 переменных разбиваем на 2^{n_1} классов смежности линейных подпространств размерности n_2-n_1 каждый. Пусть C_i — i-й класс смежности в разбиении, $C_i\subseteq\mathbf{F}_2^{n_2}$. Класс C_i объявляем носителем спектра своей платовидной подфункции f_i. Подфункцию f_i зададим так: к произвольной бент-функции g_i от n_2-n_1 переменных добавим n_1 фиктивных переменных и осуществим аффинное преобразование спектра $\mathbf{F}_2^{n_2}\to\mathbf{F}_2^{n_2}$ так, чтобы носитель спектра функции g_4 перешел в C_i (подробнее об аффинных преобразованиях носителя спектра см. параграф 4.2 главы 4).

Описанная выше конструкция К предложена в [187], где показано, что конструкция задает бент-функцию. Более того, из описания конструкции К следует следующая теорема.

Теорема 5.1. *[187] Пусть n четно. Число бент-функций от n переменных, порождаемых конструкцией К, при заданном параметре n_1 и $n_2=n-n_1$ равно*

$$L=b_{n_2-n_1}^{2^{n_1}}\cdot N_{n_2}^{n_2-n_1},\qquad(5.1)$$

где $b_{n_2-n_1}$ — число бент-функций от n_2-n_1 переменных, $N_{n_2}^{n_2-n_1}$ — число упорядоченных разбиений $\mathbf{F}_2^{n_2}$ на 2^{n_1} классов смежности линейных подпространств размерности n_2-n_1.

О конструкции, доказательстве теорем и некоторых свойств можно прочитать в [188]. По сути ту же конструкцию, но в другой терминологии предложил ранее С. В. Агиевич [34], который также установил результат, аналогичный теореме 5.1.

В связи со сказанным выше, является актуальной задача о разбиении пространства $\mathbf{F}_2^n$ на аффинные подпространства и подсчете числа таких разбиений.

Поскольку существуют обобщения бент-функций с двоичного на q-ичный случай, будем также рассматривать разбиения пространства $\mathbf{F}_q^n$.

В этой главе доказано, что для любого натурального m существует наименьшее натуральное $N = N_q(m)$, что при $n > N$ не существует A-примитивных разбиений пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n - m$. Получены нижние и верхние оценки на величину $N_q(m)$. Доказано, что $N_q(2) = q + 1$. Результаты того же типа установлены для разбиений на грани.

5.1 Задачи разбиения на подпространства

Пусть q — степень простого числа. Достаточно широко известна задача разбиения пространства $\mathbf{F}_q^n$ на линейные подпространства L_i:

$$\{L_i\}: \qquad \bigsqcup_i (L_i \setminus \{0\}) = \mathbf{F}_q^n \setminus \{0\},$$

где L_i — линейные подпространства, как правило, одинаковой размерности, но рассматривались и наборы различных размерностей. Задача это не такая простая, но интересная, с большим числом приложений и активно изучавшаяся (см., например, [70, 35]). Исследователей интересовало в основном существование разбиений и их структура; количество разбиений, как правило, не оценивалось.

В отличие от упомянутой выше задачи, практически не изучалась задача о разбиении $\mathbf{F}_q^n$ на аффинные подпространства $E_i = L_i + b_i$, где L_i — линейное подпространство, $b_i \in \mathbf{F}_q^n$:

$$\{E_i\}: \qquad \bigsqcup_i E_i = \mathbf{F}_q^n;$$

может быть, потому, что она имеет тривиальное решение. Достаточно взять все $L_i = L$, а в качестве b_i — представителей классов смежности (такое разбиение указано в начале работы [2], где в качестве L выступает q-ичный код Хэмминга, после чего рассмотрение переходит к разбиению $\mathbf{F}_q^n$ на неэквивалентные совершенные коды — тоже достаточно популярной теме). А раз задача тривиальная

и не было приложений, требующих нетривиальных разбиений, то ее и не рассматривали.

В 2008 году такое приложение обнаружил Агиевич, исследуя построения бент-функций в работе [34]; там же он исследовал некоторые количественные и структурные свойства разбиений $\mathbf{F}_q^n$ на аффинные подпространства.

В последние годы появилось несколько новых публикаций на эту тему. В [187, 144] получены оценки на число разбиений $\mathbf{F}_2^n$ на аффинные подпространства, а в [188] найдена асимптотика логарифма числа разбиений $\mathbf{F}_2^n$ на аффинные подпространства размерности два. Эти результаты позволили улучшить асимптотическую нижнюю оценку на логарифм число булевых бент-функций, превзойдя асимптотику логарифма числа бент-функций из пополненного семейства Майораны–МакФарланда, которое до этого считалось самым большим из известных.

Подробнее о бент-функциях и других криптографически важных функциях см. в [19].

В [34] Агиевич ввел понятие примитивного разбиения. Пусть $\bigsqcup\limits_i E_i = \mathbf{F}_q^n$, где E_i — аффинные подпространства пространства $\mathbf{F}_q^n$, $E_i = L_i + b_i$, L_i — соответствующие линейные подпространства пространства $\mathbf{F}_q^n$, $b_i \in \mathbf{F}_q^n$. Обозначим $\bigcap\limits_i L_i = W$. Агиевич назвал разбиение $\{E_i\}$ *примитивным,* если $W = \{\vec{0}\}$.

С нашей точки зрения в данном контексте использование термина «примитивный» небесспорно, поскольку он характеризует скорее некоторую невырожденность разбиения. Кроме того, подобного рода невырожденность разбиения можно определять разными способами, а слово «примитивный» в математике вообще перегружено. В то же время давать другой термин тоже представляется неправильным, поэтому будем в дальнейшем называть такое разбиение *примитивным по Агиевичу* или *A-примитивным.*

Обратим также внимание на еще одну подсерию публикаций. Как было упомянуто выше, в ряде работ рассматривались разбиения пространства $\mathbf{F}_q^n$ (как правило, при $q = 2$) на совершенные коды. Поскольку совершенные коды могут быть нелинейными, это несколько другая задача. Однако в нескольких статьях рассматривались разбиения только на сдвиги совершенных **линейных** кодов

(т. е. кодов Хэмминга), и вот это уже подзадача задачи о разбиении на аффинные подпространства с ограничением на вид L_i. При этом в [71] Хеден и Соловьева рассматривали разбиение на «*взаимно непараллельные*» коды Хэмминга; под «*взаимной непараллельностью*» понималось требование, чтобы $L_i \neq L_j$ при $i \neq j$. Кротов пошел еще дальше и изучал в [75] разбиения на «максимально непараллельные» коды Хэмминга, ставя задачей максимизацию величины $\min\limits_{i \neq j} (\dim \langle L_i \cup L_j \rangle - \dim L_i)$.

Заметим, что для задачи разбиения на произвольные аффинные пространства свойства A-примитивности и взаимной непараллельности не вкладываются друг в друга. Так, увеличивая n на 1 и добавляя ко всем подпространствам взаимно непараллельного разбиения новый базисный вектор, получим снова взаимно непараллельное разбиение, которое при этом не будет A-примитивным. При этом некоторые из A-примитивных разбиений, приводимых ниже, будут содержать повторяющиеся L_i, т. е. не будут взаимно непараллельными.

Еще одним частным случаем разбиений на аффинные подпространства, получившим внимание исследователей, являются ассоциативные блок-дизайны (АБД). В контексте настоящей работы удобнее обсудить их в разделе 5.4.

В настоящей главе главное внимание уделяется вопросу существования A-примитивных разбиений.

5.2 Технические сведения и вспомогательные результаты

Приведем необходимые определения. Определения, уже данные во введении, повторять не будем.

Пусть q — степень простого. Конечное поле порядка q обозначается через $\mathbf{F}_q$. Линейное пространство векторов длины n над $\mathbf{F}_q$ обозначается через $\mathbf{F}_q^n$. Сумма векторов u и v из $\mathbf{F}_q^n$ обозначается через $u + v$, а произведение вектора u на константу $\lambda \in \mathbf{F}_q$ — через λu. Если L — линейное подпространство пространства $\mathbf{F}_q^n$, а $b \in \mathbf{F}_q^n$, то под аффинным подпространством $E = L + b$ понимается множество всех векторов вида $u + b$, где $u \in L$.

Для любой пары $u = (u_1, \ldots, u_n)$ и $v = (v_1, \ldots, v_n)$ векторов из $\mathbf{F}_q^n$ их *скалярное произведение,* которое в этой главе, чтобы не путать с линейной оболочкой множества векторов, переименуем и будем обозначать через

$$(u, v) = u_1 \cdot v_1 + \cdots + u_n \cdot v_n, \tag{5.2}$$

где умножение и сложение выполняются над $\mathbf{F}_q$. Говорят, что векторы u и v *ортогональны* и пишут $u \perp v$, если $(u, v) = 0$. Если L — линейное подпространство в $\mathbf{F}_q^n$, то через $L^\perp$ обозначается множество всех таких наборов v, что $v \perp u$ для любого $u \in L$. Легко понять и широко известно, что $L^\perp$ само является линейным подпространством в $\mathbf{F}_q^n$. Подпространство $L^\perp$ называется *ортогональным* к L. Напомним, что для пространств над конечными полями ортогональное подпространство не обязательно является ортогональным дополнением, в отличие, например, от евклидова случая.

Если C — произвольное подмножество $\mathbf{F}_q^n$, то его *линейной оболочкой* (или *линейным замыканием*) $\langle C \rangle$ называется множество всех векторов, представимых в виде линейных комбинаций над $\mathbf{F}_q$ векторов из C. Легко понять, что $\langle C \rangle$ является линейным подпространством пространства $\mathbf{F}_q^n$.

Следующая лемма широко известна, но докажем ее для полноты изложения.

Лемма 5.1. *Пусть q — степень простого числа. Пусть L — линейное подпространство пространства $\mathbf{F}_q^n$. Пусть $u \notin L^\perp$. Тогда скалярное произведение (x, u) при x, пробегающем L, принимает каждое из q значений одинаковое число раз.*

Доказательство. Из $u \notin L^\perp$ следует, что существует $x_0 \in L$, такое что $(x_0, u) = \mu_0 \neq 0$. Тогда для любого $\mu \in \mathbf{F}_q$, $\mu \neq 0$, отображение $x \to \mu \cdot x$ переводит L в себя, причем скалярное произведение $(x, u) = \mu_0$ переходит в $(\mu \cdot x, u) = \mu\mu_0$. Отсюда следует, что любое ненулевое значение скалярного произведения встречается не реже, чем любое другое ненулевое значение, поэтому все ненулевые значения принимаются как результат скалярного произведения одинаковое количество раз.

Далее, рассмотрим отображение $x \to x - x_0$. Это отображение переводит L в себя, причем скалярное произведение $(x, u) = \mu_0$ переходит в $(x - x_0, u) =$

$\mu_0 - \mu_0 = 0$. В свою очередь отображение $x \to x + x_0$ переводит L в себя, причем скалярное произведение $(x, u) = 0$ переходит в $(x + x_0, u) = \mu_0$. Отсюда следует, что нулевое значение скалярного произведения встречается столько же раз, сколько любое ненулевое, и, таким образом, скалярное произведение (x, u) при x, пробегающем все L, принимает каждое из q значений одинаковое число раз. □

Следствие 5.1. *Пусть q — степень простого числа. Пусть $E = L + b$ — аффинное подпространство пространства $\mathbf{F}_q^n$. Пусть $u \notin L^\perp$. Тогда скалярное произведение (x, u) при x, пробегающем E, принимает каждое из q значений одинаковое число раз.*

Доказательство. Немедленное следствие леммы 5.1. □

5.3 А-примитивные разбиения

В этом разделе получаем результаты о существовании А-примитивных разбиений.

Лемма 5.2. *Пусть q — степень простого числа. Пусть $\{E_i = L_i + b_i\}$ — А-примитивное разбиение пространства $\mathbf{F}_q^n$. Тогда* $\dim \left\langle \bigcup_{i=1}^{q^m} L_i^\perp \right\rangle = n$.

Доказательство. Предположим противное. Пусть $\dim \left\langle \bigcup_{i=1}^{q^m} L_i^\perp \right\rangle < n$. Тогда найдется ненулевой набор $u \in \mathbf{F}_q^n$, такой что $u \perp \left\langle \bigcup_{i=1}^{q^m} L_i^\perp \right\rangle$. Отсюда u принадлежит всем L_i, что противоречит А-примитивности разбиения $\{E_i\}$. Полученное противоречие доказывает лемму. □

Теорема 5.2. *Пусть q — степень простого числа. Для любого натурального m существует наименьшее натуральное $N = N_q(m)$, что при $n > N$ не существует А-примитивных разбиений $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n - m$.*

Доказательство. Пусть $\{E_i = L_i + b_i\}$ — А-примитивное разбиение пространства $\mathbf{F}_q^n$. Из леммы 5.2 следует, что $n = \dim \left\langle \bigcup_{i=1}^{q^m} L_i^\perp \right\rangle \leq m \cdot q^m$. □

Следствие 5.2. $N_q(m) \leq m \cdot q^m$.

Заметим, что Агиевич в [34] фактически доказал, что $N_q(1) = 1$ для любого q (равного степени простого числа) и $N_2(2) = 3$.

Для дальнейшего усиления верхней оценки на $N_q(m)$ сформулируем два дополнительных соображения (леммы).

Лемма 5.3. *Пусть $\{E_i\}$ — разбиение $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n-m$, $n \geq 2m$. Тогда для любых $i, j (i \neq j)$ выполнено $L_i^\perp \cap L_j^\perp \neq \{0\}$.*

Доказательство. Предположим противное. Пусть для некоторых i, j выполнено $L_i^\perp \cap L_j^\perp = \{0\}$. Пусть $L_i^\perp = \left\langle \{l^{i,1}, \ldots, l^{i,m}\} \right\rangle$, $L_j^\perp = \left\langle \left\{l^{j,1}, \ldots, l^{j,m}\right\} \right\rangle$. Тогда множество наборов из $E_i \cap E_j$ есть множество решений системы из $2m$ уравнений с n неизвестными:

$$\left\{(x - b_i, l^{i,t}) = 0,\ t = 1, \ldots, m, \quad (x - b_j, l^{j,t}) = 0,\ t = 1, \ldots, m\right\}.$$

В силу линейной независимости системы векторов $\{l^{i,t}, l^{j,t}\}$, $t = 1, \ldots, m$, и условия $n \geq 2m$ (неизвестных не меньше, чем уравнений), эта система имеет решение. Следовательно, аффинные подпространства E_i и E_j пересекаются, что противоречит тому, что они входят в разбиение. Полученное противоречие доказывает лемму. □

Лемма 5.4. *Пусть $\{E_i\}$ — разбиение $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n - m$. Тогда для любого $u \in \mathbf{F}_q^n$ число содержащих набор u ортогональных подпространств $L_i^\perp$ делится на q.*

Доказательство. Нулевой набор, очевидно, принадлежит всем q^m подпространствам $L_i^\perp$. Пусть $u \in \mathbf{F}_q^n$, $u \neq \vec{0}$. Если $u \notin L_i^\perp$, то скалярное произведение (x, u) при x, пробегающем E_i, в силу следствия 5.1 принимает каждое из q значений одинаковое число раз. Если же $u \in L_i^\perp$, то скалярное произведение (x, u) при x, пробегающем E_i, принимает фиксированное значение и, стало быть, при $y = x + b_i$, пробегающем E_i, скалярное произведение (y, u) принимает также фиксированное значение. В силу того, что $u \notin \left(\mathbf{F}_q^n\right)^\perp = \{\vec{0}\}$, по лемме 5.1 имеем, что скалярное произведение (x, u) при x, пробегающем $\mathbf{F}_q^n$, принимает каждое

из q значений одинаковое число раз. Отсюда число $L_i^\perp$, содержащих u, должно делиться на q. □

Теорема 5.3. *Пусть q — степень простого числа. Тогда $N_q(m) \le m \cdot q^{m-1}$.*

Доказательство. Пусть $\{E_i\}$ — A-примитивное разбиение $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n-m$. В силу леммы 5.2 выполнено $\dim \left\langle \bigcup_{i=1}^{q^m} L_i^\perp \right\rangle = n$. Построим базис $U = \{u_1, \ldots, u_n\}$ пространства $\mathbf{F}_q^n$ следующим образом. Будем последовательно просматривать подпространства $L_j^\perp$, $j = 1, 2, \ldots$, и если $\dim \left\langle \bigcup_{i=1}^{j} L_i^\perp \right\rangle - \dim \left\langle \bigcup_{i=1}^{j-1} L_i^\perp \right\rangle = \delta > 0$, то в U добавим δ линейно независимых векторов, принадлежащих $L_j^\perp$, но не принадлежащих $\left\langle \bigcup_{i=1}^{j-1} L_i^\perp \right\rangle$.

По построению каждый из базисных векторов $u_1, \ldots, u_n$ принадлежит хотя бы одному $L_i^\perp$ и, стало быть, по лемме 5.4 принадлежит не менее q подпространствам $L_i^\perp$. Поэтому общее число вхождений базисных векторов из U в $\bigcup_{i=1}^{q^m} L_i^\perp$ не меньше qn. С другой стороны, каждое $L_i^\perp$ содержит не более m векторов из U. Отсюда для числа S вхождений векторов из U в $\bigcup_{i=1}^{q^m} L_i^\perp$ имеем

$$qn \le S \le m \cdot q^m$$

и, следовательно,

$$n \le m \cdot q^{m-1}.$$

□

Лемма 5.5. *Пусть q — степень простого числа. Тогда $N_q(2) \le q+1$.*

Доказательство. Пусть $\{E_i\}$ — A-примитивное разбиение $\mathbf{F}_q^n$ на q^2 аффинных подпространств размерности $n-2$. В силу леммы 5.2 выполнено $\dim \left\langle \bigcup_{i=1}^{q^2} L_i^\perp \right\rangle = n$. Поменяем, если нужно, нумерацию подпространств $L_j^\perp$, $j = 1, \ldots, q^2$, так, чтобы для первых j, пока можно, возрастало значение величины $\dim \left\langle \bigcup_{i=1}^{j} L_i^\perp \right\rangle$,

т. е. выполнялось

$$\dim\left\langle\bigcup_{i=1}^{j}L_i^{\perp}\right\rangle-\dim\left\langle\bigcup_{i=1}^{j-1}L_i^{\perp}\right\rangle>0.$$

В силу леммы 5.3 при $j\geq 2$ выполнено $\dim\left(L_j^{\perp}\bigcap L_1^{\perp}\right)>0$, поэтому при $j=2,\ldots,n-1$ подпространство $L_j^{\perp}$ будет иметь вид $L_j^{\perp}=\langle v_{j,1},v_{j,2}\rangle$, где $v_{j,1}\in\left(L_1^{\perp}\setminus\vec{0}\right)$, $v_{j,2}\notin\left\langle\bigcup\limits_{i=1}^{j-1}L_i^{\perp}\right\rangle$.

Подпространство $L_1^{\perp}$ содержит q^2-1 ненулевых наборов, каждое из подпространств $L_2^{\perp},\ldots,L_{n-1}^{\perp}$ по построению содержит q^2-q наборов, не содержащихся в уже рассмотренных подпространствах. Отсюда объединение подпространств $\bigcup\limits_{i=1}^{n-1}L_i^{\perp}$ содержит не менее $(q^2-1)+(n-2)(q^2-q)$ различных ненулевых наборов из $\mathbf{F}_q^n$, поэтому по лемме 5.4 общее число вхождений ненулевых векторов из $\mathbf{F}_q^n$ в $\bigcup\limits_{i=1}^{q^2}L_i^{\perp}$ не меньше $q((q^2-1)+(n-2)(q^2-q))$. С другой стороны, каждое $L_i^{\perp}$ содержит в точности q^2-1 ненулевых векторов из $\mathbf{F}_q^n$. Поэтому для числа S вхождений ненулевых векторов из $\mathbf{F}_q^n$ в $\bigcup\limits_{i=1}^{q^2}L_i^{\perp}$ имеем

$$q((q^2-1)+(n-2)(q^2-q))\leq S=(q^2-1)q^2.$$

Отсюда

$$n\leq q+2-\frac{1}{q}.$$

Учитывая целочисленность n, получаем

$$n\leq q+1.$$

□

Заметим, что непосредственное применение техники доказательства леммы 5.5 позволяет улучшить и оценку теоремы 5.3, но незначительно, поэтому не будем приводить соответствующие достаточно громоздкие рассуждения и выкладки.

Справедливо следующее рекуррентное неравенство.

Теорема 5.4. *Пусть q — степень простого числа. Тогда*

$$N_q(m+1)\geq q\cdot N_q(m)+1.$$

Доказательство. Элементы поля $\mathbf{F}_q$ обозначим через $\mathbf{F}_q = \{a_0, a_1, \ldots, a_{q-1}\}$. Пусть $\{E_i\} = \{L_i + b_i\}$, $i = 1, \ldots, q^m$, — A-примитивное разбиение $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n - m$. Построим A-примитивное разбиение $\{E_i\}$ пространства $\mathbf{F}_q^{qn+1}$ на q^{m+1} аффинных подпространств размерности $qn - m$. Множество базисных векторов пространства $\mathbf{F}_q^{qn+1}$ обозначим через U, $U = \{e_1, \ldots, e_{qn+1}\}$.

Определим $\mathbf{S}_j$, $j \in \{0, 1, \ldots, q-1\}$, как копию пространства $\mathbf{F}_q^n$, натянутую на множество базисных векторов $U_j = \{e_{jn+1}, e_{jn+2}, \ldots, e_{(j+1)n}\}$ и являющуюся подпространством пространства $\mathbf{F}_q^{qn+1}$ (во всех компонентах, не вошедших в U_j все вектора из $\mathbf{S}_j$ имеют нулевые значения).

Подпространство L и вектор b, взятые в j-й копии $\mathbf{S}_j$ пространства $\mathbf{F}_q^n$, будем обозначать как $L[\mathbf{S}_j]$ и $b[\mathbf{S}_j]$, соответственно. Сами $L[\mathbf{S}_j]$ и $b[\mathbf{S}_j]$ будем рассматривать как лежащие уже в $\mathbf{F}_q^{qn+1}$.

Определим $\widehat{\mathbf{S}}_j$, $j \in \{0, 1, \ldots, q-1\}$, как копию пространства $\mathbf{F}_q^{(q-1)n}$, натянутую на множество базисных векторов $\widehat{U}_j = U \setminus (U_j \cup e_{qn+1})$ и являющуюся подпространством пространства $\mathbf{F}_q^{qn+1}$ (во всех компонентах, не вошедших в $\widehat{U}_j$ все вектора из $\mathbf{S}_j$ имеют нулевые значения).

Зададим совокупность из q^{m+1} аффинных подпространств: $\{E_{i,j}\} = \{L_{i,j} + b_{i,j}\}$, $i = 1, \ldots, q^m$; $j = 0, 1, \ldots, q-1$, где $L_{i,j} = \left\langle L_i[\mathbf{S}_j], \widehat{\mathbf{S}}_j \right\rangle$, $b_{i,j} = b_i[\mathbf{S}_j] + a_j e_{qn+1}$.

По построению каждое из заданных подпространств имеет размерность $(n - m) + (q-1)n = qn - m$.

Пусть $(i', j') \neq (i'', j'')$. Если $j' \neq j''$, то аффинные подпространства $E_{i',j'}$ и $E_{i'',j''}$ не пересекаются, потому что в последней $(qn+1)$-й компоненте все вектора из $E_{i',j'}$ имеют значение $a_{j'}$, а все вектора из $E_{i'',j''}$ имеют значение $a_{j''}$. Если же $j' = j'' = j$ и $i' \neq i''$, то аффинные подпространства $E_{i',j}$ и $E_{i'',j}$ не пересекаются, потому что совокупность аффинных подпространств $\{E_i\}$ является разбиением $\mathbf{F}_q^n$. Следовательно, совокупность аффинных подпространств $\{E_{i,j}\}$ действительно является разбиением $\mathbf{F}_q^{qn+1}$.

Покажем теперь, что никакой ненулевой вектор w из $\mathbf{F}_q^{qn+1}$ не принадлежит одновременно всем $\{L_{i,j}\}$. У ненулевого вектора w есть ненулевая компонента. Можно считать, что эта компонента не последняя, потому что по построению у всех наборов из всех $L_{i,j}$ последняя компонента нулевая. Тогда ненуле-

вая компонента вектора w принадлежит какому-то множеству компонент U_j, $j \in \{0, 1, \ldots, q-1\}$. Вектор w при ограничении на множество компонент U_j дает ненулевой набор $\widetilde{w}$ длины n. Из A-примитивности разбиения $\{E_i\}$ следует, что некоторое L_i не содержит набор $\widetilde{w}$. Отсюда вытекает, что линейное подпространство $L_{i,j}$ не содержит набор w. Это доказывает, что разбиение $\{E_{i,j}\}$ является A-примитивным. □

Из рекуррентной оценки теоремы 5.4 вытекает следующая нижняя оценка на величину $N_q(m)$.

Теорема 5.5. *Пусть q — степень простого числа. Тогда*

$$N_q(m) \geq \frac{q^m - 1}{q - 1}.$$

Доказательство. В качестве основания индукции можно взять значение $L_q(1) = 1$ [34] или даже $L_q(0) = 0$ (очевидно, хотя и вычурно).

Индуктивный переход заключается в использовании теоремы 5.4. Пусть $N_q(m) \geq \frac{q^m-1}{q-1}$. Тогда

$$N_q(m+1) \geq q \cdot N_q(m) + 1 \geq q \cdot \frac{q^m - 1}{q - 1} + 1 = \frac{q^{m+1} - 1}{q - 1}.$$

□

Заметим, что в конструкции из теоремы 5.4 можно сделать множества U_j пересекающимися. Тогда при переходе от m к $m+1$ размерность пространства можно увеличить с n до любого числа из отрезка от $n+1$ до $qn+1$. Отсюда легко следует следующая теорема.

Теорема 5.6. *Пусть q — степень простого числа, m — натуральное число. Тогда A-примитивное разбиение пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n - m$ существует при любом натуральном n в отрезке от m до $\frac{q^m-1}{q-1}$.*

Заметим, что при $n > \frac{q^m-1}{q-1}$ отсутствие «дырок» во множестве значений размерности пространств, для которых существует A-примитивное разбиение, не является априори очевидным.

Полученные результаты позволяют установить точное значение величины $N_q(2)$ для любого q, являющегося степенью простого числа (напомним, в [34] Агиевич фактически сделал это для $q = 2$).

Теорема 5.7. *Пусть q — степень простого числа. Тогда*

$$N_q(2) = q + 1.$$

Доказательство. Следствие из леммы 5.5 и теоремы 5.5. □

5.4 A-примитивные разбиения на грани

Аффинное подпространство $E = L + b$ называется *координатным* (и известно также как *гранью*), если базисные вектора подпространства L содержатся среди фиксированных базисных векторов $e_1, \ldots, e_n$ всего пространства $\mathbf{F}_q^n$.

Предполагается, что базис $\{e_1, \ldots, e_n\}$ пространства $\mathbf{F}_q^n$ задан и зафиксирован. Тогда линейное подпространство L размерности $n - m$ определяется выбором $n - m$ из n базисных векторов. Для задания аффинного подпространства нужно дополнительно задать вектор b, $b \in \mathbf{F}_q^n$. Несложно понять, что вектор b можно выбрать таким образом, чтобы он имел нули во всех компонентах, соответствующих базисным векторам подпространства L.

Разбиение на грани является частным случаем разбиения на аффинные подпространства, но разбиение на грани можно рассматривать и для q, не являющихся степенью простого. Действительно, базисные вектора $\{e_1, \ldots, e_n\}$ не содержат компонент, отличных от 0 и 1, поэтому в их линейных комбинациях не используется умножение, отличное от умножения на 0 и 1. Ортогональным к координатному линейному подпространству L объявляется координатное линейное подпространство $L^\perp$, базис которого состоит из тех и только тех векторов из $\{e_1, \ldots, e_n\}$, которые не входят в базис L (и поэтому для координатных подпространств, в отличие от произвольных подпространств, ортогональное подпространство можно называть ортогональным дополнением). Внутреннее произведение двух q-значных векторов при q, не являющемся степенью простого, в общем случае не для всех целей может быть задано соотношением (5.2),

поскольку умножение не будет групповым, но при проверке ортогональности векторов u и v, $u \in L$, $v \in L^\perp$, формулу (5.2) можно использовать, поскольку при ее применении не возникнет произведения ненулевых элементов.

Исходя из сказанного выше, можно говорить о разбиении на аффинные координатные подпространства (грани) и при q, не являющемся степенью простого, только рассматриваться эти подпространства будут не в $\mathbf{F}_q^n$, а в $\mathbf{Z}_q^n$. Также можно применять использовавшуюся в предыдущих разделах технику работы с ортогональными подпространствами.

Каждую грань $E = L + b$ размерности $n - m$ в $\mathbf{Z}_q^n$ можно задать как набор длины n из звездочек и чисел из $\mathbf{Z}_q$, причем чисел в точности m. Звездочки стоят в компонентах, соответствующих базисным векторам подпространства L, числа стоят в остальных компонентах, причем число, стоящее в j-й компоненте, равно значению j-й компоненты набора b.

Разбиение $\{E_i\}$ пространства $\mathbf{Z}_q^n$ на грани можно задать матрицей размера $q^m \times n$. Для того, чтобы такая матрица задавала разбиение, она должна удовлетворять **критерию непересечения граней:** для каждой пары строк должен быть столбец с разными числами в этих строках.

Действительно, все наборы, содержащиеся в грани, можно получить произвольными доопределениями всех звездочек строки числами из $\mathbf{Z}_q^n$. Для того, чтобы из двух строк доопределениями не получился один набор (и тем самым эти две грани не пересеклись бы), как раз необходим и достаточен критерий непересечения граней.

Тот факт, что каждый набор из $\mathbf{Z}_q^n$ попадет в какую-то грань, гарантируется числом строк в матрице. В матрице в точности q^m строк, каждая задает грань с q^{n-m} наборами, все грани вместе содержат $q^m \cdot q^{n-m} = q^n$ наборов, грани не пересекаются, поэтому каждый набор попадет ровно в одну грань и, таким образом, матрица действительно задаст разбиение на грани.

Для того, чтобы разбиение, задаваемое матрицей, являлось A-примитивным разбиение, матрица должна удовлетворять **критерию A-примитивности:** в матрице не должно быть столбца из одних звездочек.

Действительно, если j-й столбец матрицы состоит из одних звездочек, то базисный вектор e_j принадлежит всем L_i, и поэтому разбиение на является A-

примитивным. Если же i-я строка матрицы содержит в j-м столбце число, то базисный вектор e_j не принадлежит L_i вместе со всеми линейными комбинациями базисных векторов, в которые он входит с ненулевым коэффициентом (напомним, умножения на 0 и 1 у нас разрешены).

Заметим, что частным случаем разбиения на грани являются *ассоциативные блок-дизайны (АБД),* которые были введены Ривестом [100] для использования в алгоритмах хэширования и изучались в ряде работ (см., например, [39, 118]). АБД — это разбиение $\mathbf{Z}_2^n$ на грани одинаковой размерности с дополнительным требованием: в матрице разбиения каждый столбец содержит одно и то же число звездочек. Из определения очевидно, что АВД является А-примитивным разбиением.

При переносе результатов со случая разбиения $\mathbf{F}_q^n$ на аффинные подпространства на случай разбиения $\mathbf{Z}_q^n$ на грани небольшую техническую трудность представляет использование скалярного произведения. Будем продолжать его использование в соответствии с формулой (5.2), следя за тем, чтобы не возникало произведения элементов $\mathbf{Z}_q$, одновременно отличных и от нуля, и от единицы. В последующих леммах этого раздела под L_i и $L_i^\perp$ понимаются только координатные линейные подпространства.

Лемма 5.6. *Пусть q — натуральное число, $q \geq 2$. Пусть L — линейное координатное подпространство пространства $\mathbf{Z}_q^n$. Пусть u — вектор из $\mathbf{Z}_q^n$, все компоненты которого принимают только значения из множества $\{0, 1\}$. Пусть $u \notin L^\perp$. Тогда скалярное произведение (x, u) при x, пробегающем L, принимает каждое из q значений одинаковое число раз.*

Доказательство. Из $u \notin L^\perp$ следует, что существует компонента j, в которой значение вектора u равно 1, а $e_j \in L$. Сгруппируем наборы координатного подпространства L в группы по q наборов, отличающихся только в j-й компоненте. Пусть G — одна из таких групп. Тогда легко видеть, что при x, пробегающем G, скалярное произведение (x, u) принимает каждое из q значений ровно один раз. Рассмотрев все группы, получаем, что при x, пробегающем L, скалярное произведение (x, u) принимает каждое из q значений одинаковое число раз. □

Следствие 5.3. *Пусть q — натуральное число, $q \geq 2$. Пусть $E = L + b$ — аффинное координатное подпространство пространства $\mathbf{Z}_q^n$. Пусть u — вектор из $\mathbf{Z}_q^n$, все компоненты которого принимают только значения из множества $\{0, 1\}$. Пусть $u \notin L^\perp$. Тогда скалярное произведение (x, u) при x, пробегающем E, принимает каждое из q значений одинаковое число раз.*

Доказательство. Следствие леммы 5.6. □

Лемма 5.7. *Пусть $\{E_i\}$ — разбиение $\mathbf{Z}_q^n$ на q^m координатных аффинных подпространств размерности $n - m$. Пусть u — вектор из $\mathbf{Z}_q^n$, все компоненты которого принимают только значения из множества $\{0, 1\}$. Тогда число содержащих набор u ортогональных подпространств $L_i^\perp$ делится на q.*

Доказательство. Нулевой набор, очевидно, принадлежит всем q^m подпространствам $L_i^\perp$. Пусть $u \neq \vec{0}$. Если $u \notin L_i^\perp$, то скалярное произведение (x, u) при x, пробегающем E_i, в силу следствия 5.3 принимает каждое из q значений одинаковое число раз. Если же $u \in L_i^\perp$, то скалярное произведение (x, u) при x, пробегающем E_i, принимает фиксированное значение и, стало быть, при $y = x + b_i$, пробегающем E_i, скалярное произведение (y, u) принимает также фиксированное значение. В силу того, что $u \notin \left(\mathbf{Z}_q^n\right)^\perp = \{\vec{0}\}$, по лемме 5.6 имеем, что скалярное произведение (x, u) при x, пробегающем $\mathbf{Z}_q^n$, принимает каждое из q значений одинаковое число раз. Отсюда число $L_i^\perp$, содержащих u, должно делиться на q. □

Лемма 5.8. *Пусть $\{E_i\}$ — разбиение $\mathbf{Z}_q^n$ на q^m координатных аффинных подпространств размерности $n - m$. Пусть $u \in \mathbf{Z}_q^n$. Тогда число содержащих набор u ортогональных подпространств $L_i^\perp$ делится на q.*

Доказательство. По вектору u построим набор $\delta(u)$, заменив все ненулевые компоненты вектора u на 1. Для вектора $\delta(u)$ заключение леммы 5.8 справедливо в силу леммы 5.7. Легко видеть, что наборы u и $\delta(u)$ принадлежат или не принадлежат каждому из координатных линейных подпространств $L_i^\perp$ одновременно. Следовательно, заключение леммы 5.8 справедливо и для вектора u. □

Следствие 5.4. *Пусть $\{E_i = L_i + b_i\}$ — разбиение пространства $\mathbf{Z}_q^n$ на грани одинаковой размерности. Тогда множество $\{L_i\}$ соответствующих этому разбиению координатных линейных подпространств распадается на группы из q совпадающих.*

Доказательство. Пусть $E = L + b$ — грань из разбиения $\{E_i\}$. Рассмотрим вектор u, равный 0 в компонентах, соответствующих базисным векторам подпространства L, и равный 1 в компонентах, соответствующих базисным векторам подпространства $L^\perp$. По построению $u \in L^\perp$. По лемме 5.7 вектор u должен содержаться в делящемся на q числе подпространств $L_i^\perp$, но, очевидно, в силу того, что u имеет m ненулевых компонент, он не может содержаться ни в каком координатном линейном подпространстве размерности m, кроме $L^\perp$. Поэтому подпространство L входит в $\{L_i\}$ делящееся на q число раз. □

Следствие 5.5. *Не существует взаимно непараллельных разбиений пространства $\mathbf{Z}_q^n$ на грани одинаковой размерности.*

Утверждение следствия 5.4 ранее сформулировано и доказано Потаповым (Proposition 4 в [95]) для $q = 2$, но доказательство дословно проходит для любого q. Еще раньше аналогичное утверждение было сформулировано и доказано для АБД (теорема 9.7(4) в [119], доказательство дословно проходит для любого разбиения на грани и для любого q).

Заметим, что утверждения, аналогичные следствиям 5.4 и 5.5, не будут верными для разбиений пространства $\mathbf{F}_q^n$ на произвольные (не обязательно координатные) аффинные подпространства в силу того, что в рассуждениях из доказательства утверждения 5.4 вектор u может содержаться в этом случае в разных подпространствах $L_i^\perp$.

Пример 5.1. Существует взаимно непараллельное A-примитивное разбиение пространства $\mathbf{F}_2^3$ на 2^2 аффинных подпространств размерности $3 - 2 = 1$:

$$\begin{aligned} E_1 &= \{(000),(001)\} &&= \langle e_3 \rangle, \\ E_2 &= \{(100),(110)\} &&= \langle e_2 \rangle + e_1, \\ E_3 &= \{(011),(111)\} &&= \langle e_1 \rangle + e_2 + e_3, \\ E_4 &= \{(010),(101)\} &&= \langle e_1 + e_2 + e_3 \rangle + e_2. \end{aligned}$$

Рекурсивно подставляя это разбиение в конструкцию из теоремы 5.4, получаем взаимно непараллельные A-примитивные разбиения пространства $\mathbf{F}_2^n$ на 2^m аффинных подпространств размерности $n-m$ для $n=2^m-1$, $m=2,3,\ldots$

Для удобства будущих ссылок сформулируем в явном виде утверждения предыдущих разделов, перенесенные на разбиения на грани.

Лемма 5.9. *Пусть $\{E_i = L_i + b_i\}$ — A-примитивное разбиение пространства $\mathbf{Z}_q^n$ на грани. Тогда* $\dim \left\langle \bigcup_{i=1}^{q^m} L_i^{\perp} \right\rangle = n$.

Теорема 5.8. *Пусть $q \geq 2$. Для любого натурального m существует наименьшее натуральное $N = N_q^{\mathrm{coord}}(m)$, что при $n > N$ не существует A-примитивных разбиений $\mathbf{Z}_q^n$ на q^m граней размерности $n-m$.*

Поскольку при q, являющемся степенью простого числа, разбиение на грани является частным случаем разбиения на аффинные подпространства, справедливо следующее утверждение.

Утверждение 5.1. *Пусть q — степень простого числа. Тогда*

$$N_q^{\mathrm{coord}}(m) \leq N_q(m).$$

Теорема 5.9. *Пусть $q \geq 2$. Тогда $N_q^{\mathrm{coord}}(m) \leq m \cdot q^{m-1}$.*

Доказательство. Аналогично доказательству теоремы 5.3 с использованием леммы 5.8. При формировании множества U дополнительно требуем, чтобы во множество U включались только базисные вектора пространства. Таким образом, после окончания процедуры формирования множества U будем иметь $U = \{e_1, \ldots, e_n\}$. □

Можно переформулировать доказательство теоремы 5.9 на языке матрицы разбиения на грани. Зададим A-примитивное разбиение на грани матрицей размера $q^m \times n$. В каждой строке ровно m чисел, всего чисел в матрице $m \cdot q^m$, в матрице нет столбца из одних звездочек, а количество чисел в каждом столбце делится на q. Поэтому число столбцов не превышает $m \cdot q^{m-1}$.

Несложно видеть, что конструкция теоремы 5.4 сохраняет свойство разбиения быть координатным. Поэтому такая же рекуррентная оценка верна и для разбиения на грани.

Теорема 5.10. *Пусть $q \geq 2$. Тогда $N_q^{\mathrm{coord}}(m+1) \geq q \cdot N_q^{\mathrm{coord}}(m) + 1$.*

Теорема 5.11. *Пусть $q \geq 2$. Тогда $N_q^{\mathrm{coord}}(m) \geq \frac{q^m-1}{q-1}$.*

Теорема 5.12. *Пусть $q \geq 2$, m — натуральное число. Тогда A-примитивное разбиение пространства $\mathbf{Z}_q^n$ на q^m граней размерности $n-m$ существует при любом натуральном n в отрезке от m до $\frac{q^m-1}{q-1}$.*

Лемма 5.10. *Пусть $q \geq 2$. Тогда $N_q^{\mathrm{coord}}(2) \leq q+1$.*

Доказательство. Можно действовать аналогично доказательству леммы 5.5 с использованием леммы 5.8, в качестве базисных векторов подпространств $L_i^\perp$ выбирая базисные вектора пространства, а можно поступить проще. По следствию 5.4 множество из всех q^2 граней разобьется на q групп из q параллельных граней в каждой группе. Первая из этих групп даст вклад в $\dim \left\langle \bigcup L_i^\perp \right\rangle$, равный 2, каждая из последующих групп в силу критерия непересечения граней будет добавлять к этой величине не более единицы. Отсюда $n \leq q+1$. □

Теорема 5.13. *Пусть $q \geq 2$. Тогда $N_q^{\mathrm{coord}}(2) = q+1$.*

Доказательство. Следствие из леммы 5.10 и теоремы 5.11. □

Из доказательства леммы 5.10 несложно видеть, что максимальное значение $N_q^{\mathrm{coord}}(2) = q+1$ будет достигаться только на таких разбиениях $\mathbf{Z}_q^n$ на грани размерности $n-2$, в которых все $L_i^\perp$ содержат общий базисный вектор пространства $\mathbf{Z}_q^n$, а каждый из остальных $n-1=q$ базисных векторов $\mathbf{Z}_q^n$ является вторым базисным вектором в точности в q подпространствах $L_i^\perp$.

Заметим, что для АВД при $m > 3$ доказано неравенство $n \leq \binom{m}{2}$ [76]. Сравнение этой квадратичной по m верхней оценки с экспоненциальной нижней оценкой $N_2^{\mathrm{coord}}(m) \geq 2^m - 1$ теоремы 5.11 представляется сильным аргументом в пользу того, что в матрицах разбиений на грани, на которых достигаются величины $N_q^{\mathrm{coord}}(m)$, распределение звездочек по столбцам очень неравномерно.

5.5 О числе разбиений на аффинные подпространства

Пусть q — степень простого числа. Агиевич в [34] привел формулу для числа различных неупорядоченных разбиений пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n-m$:

$$c_q(n,m) = \sum_{d=0}^{n-m} \binom{n}{d}_q c_q^*(n-d,m), \tag{5.3}$$

где $c_q(n,m)$ — число различных неупорядоченных разбиений пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n-m$; $c_q^*(n,m)$ — число различных неупорядоченных A-примитивных разбиений пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n-m$; $\binom{n}{d}_q$ — число различных d-мерных подпространств пространства $\mathbf{F}_q^n$. Хорошо известно, что

$$\binom{n}{d}_q = \frac{\prod\limits_{i=0}^{d-1}(q^n - q^i)}{\prod\limits_{i=0}^{d-1}(q^d - q^i)}. \tag{5.4}$$

Делая в (5.3) замену $h = n-d$, учитывая, что $\binom{n}{d}_q = \binom{n}{n-d}_q$ (поскольку d-мерное подпространство однозначно задается ортогональным к нему $(n-d)$-мерным подпространством, и наоборот), а также принимая во внимание, что по теореме 5.2 при $n > N_q(m)$ не существует A-примитивных разбиений $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n-m$, получаем

$$c_q(n,m) = \sum_{h=m}^{N_q(m)} \binom{n}{h}_q c_q^*(h,m). \tag{5.5}$$

Заметим, что при фиксированных q и m сумма в (5.5) содержит конечное число слагаемых.

Пусть q (степень простого числа) и m фиксированы, $n \to \infty$. Легко видеть, что $\binom{n}{h}_q = o\left(\binom{n}{h'}_q\right)$ при фиксированных натуральных $h < h'$. Отсюда

$$c_q(n,m) \sim \binom{n}{N_q(m)}_q c_q^*(N_q(m),m). \tag{5.6}$$

Раскрывая число подпространств в (5.6) по формуле (5.4) и переходя к асимптотике, устанавливаем следующую теорему.

Теорема 5.14. *Пусть q (степень простого числа) и m фиксированы, $n \to \infty$. Тогда*

$$c_q(n,m) \sim C q^{N_q(m)\cdot n},$$

где $C = \frac{c_q^*(N_q(m),m)}{q^{(N_q(m))^2}\cdot\left(\frac{1}{q};\frac{1}{q}\right)_{N_q(m)}}$; величина $\left(\frac{1}{q};\frac{1}{q}\right)_{N_q(m)} = \prod\limits_{i=1}^{N_q(m)}\left(1-\frac{1}{q^i}\right)$ известна как q-символ Почхаммера.

Как видим, асимптотика числа разбиений пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств одинаковой размерности при $m = \text{const}$, $n \to \infty$, в огромной степени определяется величиной $N_q(m)$, что является еще одним аргументом в пользу ее изучения.

Для разбиений на грани аналогичными рассуждениями получаем формулу

$$c_q^{\text{coord}}(n,m) = \sum_{h=m}^{N_q^{\text{coord}}(m)} \binom{n}{h} c_q^{\text{coord}*}(h,m), \tag{5.7}$$

где $c_q^{\text{coord}}(n,m)$ — число различных неупорядоченных разбиений пространства $\mathbf{Z}_q^n$ на q^m граней размерности $n-m$; $c_q^{\text{coord}*}(n,m)$ — число различных неупорядоченных A-примитивных разбиений пространства $\mathbf{Z}_q^n$ на q^m граней размерности $n-m$; $\binom{n}{h}$ — обычный биномиальный коэффициент.

Заметим, что при фиксированных q и m сумма в (5.7) содержит конечное число слагаемых.

Пусть q и m фиксированы, $n \to \infty$. Легко видеть, что $\binom{n}{h} = o\left(\binom{n}{h'}\right)$ при фиксированных натуральных $h < h'$. Отсюда

$$c_q^{\text{coord}}(n,m) \sim \binom{n}{N_q^{\text{coord}}(m)} c_q^{\text{coord}*}(N_q^{\text{coord}}(m),m),$$

и устанавливаем следующую теорему.

Теорема 5.15. *Пусть q и m фиксированы, $n \to \infty$. Тогда*

$$c_q^{\text{coord}}(n,m) \sim C' n^{N_q^{\text{coord}}(m)},$$

где $C' = \frac{c_q^{\text{coord}*}(N_q^{\text{coord}}(m),m)}{N_q^{\text{coord}}(m)!}$.

Как видим, величину $N_q^{\text{coord}}(m)$ тоже изучалась не зря.

6 О булевых функциях с единичными значениями почти равномерно распределенными по подфункциям и шарам

В предыдущих главах основное внимание уделялось корреляционно-иммунным и устойчивым булевым функциям, т. е. функциям, единичные значения которых абсолютно равномерно распределены по подкубам заданной размерности $(n - m)$. Не всегда такое абсолютно равномерное распределение достижимо, особенно когда оно должно удовлетворять каким-то дополнительным требованиям. В то же время, с практической точки зрения часто достаточно иметь не абсолютно равномерное, а почти равномерное распределение. В этой главе рассматриваются булевы функции, количество единичных значений которых в однотипных подмножествах (подкубах и шарах) одинакового размера (но зато любого) различается не более чем на заданную величину l.

Рассмотрение предваряет параграф о рамсеевских теоремах для симметрических подфункциях, играющий во всем изложении вспомогательную роль, но представляющий самостоятельное значение.

6.1 Рамсеевские теоремы о симметрических подфункциях

В этом параграфе доказываются теоремы рамсеевского типа о симметрических подфункциях. Результаты данного параграфа будут использованы в этой и последующей главах, однако они представляют и самостоятельный интерес. Основой параграфа является четвертый параграф статьи автора [146], однако некоторые его результаты публиковались автором и ранее в [129], [156], [157].

Пусть A_n — конечное множество, состоящее из n различимых элементов, $A = \{a_1, a_2, \ldots, a_n\}$. Неупорядоченное подмножество множества A_n, состоящее ровно из r элементов (без повторений), будем называть *r-подмножеством.* Пусть $f^{r,t}_{A_n}$ — некоторая функция, ставящая в соответствие любому из r-подмножеств A_n одно из t значений $0, 1, \ldots, t-1$. Такую функцию также будем называть *t-раскраской.*

Теорема Рамсея [96] Пусть $r \geq 1$, $q_i \geq r$ $(i = 0, \ldots, t-1)$. Тогда существует такое наименьшее натуральное $\mathcal{N} = \mathcal{N}(q_0, \ldots, q_{t-1}; r)$, что для любого $n \geq \mathcal{N}$ и любой t-раскраски $f^{r,t}_{A_n}$ найдется (при некотором $i \in \{0, 1, \ldots, t-1\}$) такое q_i-подмножество множества A_n, всем r-подмножествам которого сопоставлено значение i.

Замечание 6.1. Теорема Рамсея была бы неверна, если бы элементам было разрешено входить в подмножества с повторениями. В качестве контрпримера можно привести функцию $f^{r,t}_{A_n}$,

$$f^{r,t}_{A_n}(a_{i_1}, a_{i_2}, \ldots, a_{i_r}) = 1 \Leftrightarrow a_{i_1} = a_{i_2} = \cdots = a_{i_r}$$

и $f^{r,t}_{A_n}$ принимает значение 0 в противном случае. Точно так же теорема Рамсея была бы неверна, если бы подмножества были упорядоченными. Для построения контрпримера достаточно сопоставить различные значения наборам, получающимся друг из друга перестановкой двух первых компонент.

Мы будем рассматривать дискретные отображения (функции) вида $f : \{0, 1, \ldots, q-1\}^n \to \{0, 1, \ldots, k-1\}$. Множество всех таких функций обозначается через $P^n_{q,k}$. Объединение множеств $P^n_{q,k}$ для всех целых неотрицательных n обозначается через $P_{q,k}$: $P_{q,k} = \bigcup\limits_{n=0}^{\infty} P^n_{q,k}$. В случае $q = k$ множества $P^n_{q,k}$ и $P_{q,k}$ принято обозначать P^n_k и P_k соответственно. Множество P_k обычно называют классом всех функций k-значной логики, а функции из этого класса — функциями k-значной логики или k-значными функциями. При $q = k = 2$ класс P_2 является классом всех булевых функций, а функции из этого класса — булевыми функциями. Функцию f из множества $P^n_{q,k}$ часто записывают в виде $f(x_1, x_2, \ldots, x_n)$. При этом считается, что переменные x_1, x_2, …, x_n однозначно соответствуют компонентам декартова произведения $\{0, 1, \ldots, q-1\}^n$.

Совокупность значений переменных x_1, x_2, ..., x_n называется *набором* значений переменных, или просто *набором*. Если $q = 2$, то набор иногда называют *двоичным* набором.

Функция $f(x_1, x_2, \ldots, x_n)$ из множества $P^n_{q,k}$ называется *симметрической*, если для произвольного взаимно однозначного отображения $\phi : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ (или, иными словами, для произвольной *перестановки переменных*) функция f не меняется: $f(x_1, x_2, \ldots, x_n) \equiv f(x_{\phi(1)}, x_{\phi(2)}, \ldots, x_{\phi(n)})$. Хорошо известно, что симметрическая функция f из $P^n_{2,k}$ полностью определяется своей *характеристической последовательностью* $\pi(f) = (\pi_0, \pi_1, \ldots, \pi_n)$, где π_i — это значение функции f на любом наборе, содержащем ровно i единиц (и соответственно $n-i$ нулей), $i = 0, 1, \ldots, n$. При $q \geq 3$ множество *характеристических коэффициентов*, полностью определяющих симметрическую функцию f из $P_{q,k}$ имеет более сложную структуру. В общем случае это множество можно определить как $\{\pi_{i_1,i_2,\ldots,i_{q-1}} \,|\, 0 \leq i_1, i_2, \ldots, i_{q-1}; \sum\limits_{j=1}^{q-1} i_j \leq n\}$, где $\pi_{i_1,i_2,\ldots,i_{q-1}}$ — это значение функции f на любом наборе, содержащем ровно i_j значений j, $j = 1, 2, \ldots, q-1$, (и соответственно ровно $n - \sum\limits_{j=1}^{q-1} i_j$ значений 0). Геометрически множество характеристических коэффициентов симметрической функции из $P^n_{q,k}$ можно представлять себе как треугольник при $q = 3$, тетраэдр при $q = 4$ и $(q-1)$-мерный гипертетраэдр при $q \geq 5$.

Сужением $f[k_1, k_2]$, $0 \leq k_1 \leq k_2 \leq n$ симметрической функции f из класса $P^n_{2,k}$ будем называть функцию из класса $P^{k_2-k_1}_{2,k}$, полученную из функции $f^{i_1,i_2,\ldots,i_{n-k_2+k_1}}_{\sigma_1,\sigma_2,\ldots,\sigma_{n-k_2+k_1}}(x_1, x_2, \ldots, x_n)$ с удалением фиктивных переменных x_{i_1}, $x_{i_2}, \ldots,$ $x_{i_{n-k_2+k_1}}$, где $(\sigma_1, \sigma_2, \ldots, \sigma_{n-k_2+k_1})$ — набор длины $n - k_2 + k_1$, содержащий ровно k_1 единиц и ровно $n - k_2$ нулей. В дальнейшем в этом параграфе, говоря о подстановке констант вместо переменных, будем подразумевать, что переменные, ставшие фиктивными после того, как вместо них подставили константы, удаляются. В каком именно порядке будут при этом переупорядочиваться оставшиеся свободные переменные, нам не важно, потому что главное для нас, получится ли в результате всех подстановок констант симметрическая подфункция.

Теорема 6.1. *Для любого натурального n_1 найдется минимальное натуральное $N = N(n_1)$ такое, что из любой функции f из класса $P^n_{2,k}$ от $n \geq N(n_1)$*

переменных подстановками только констант 0 *вместо некоторых переменных можно получить симметрическую подфункцию от* n_1 *переменных.*

Формулировка теоремы 6.1 приведена в [87]. Другой вариант доказательства этой теоремы дан в [129].

Доказательство. Сопоставим переменным $x_1, x_2, \ldots, x_n$ функции $f(x_1, x_2, \ldots, x_n)$ элементы $a_1, a_2, \ldots, a_n$, соответственно, множества A_n, а набору значений переменных $x = (x_1, x_2, \ldots, x_n)$ сопоставим подмножество $A(x)$ множества A следующим образом:

$$a_i \in A(x) \Leftrightarrow x_i = 1.$$

Тогда набору x, содержащему r единиц и $n - r$ нулей сопоставляется r-подмножество множества A_n. Обозначим $\mathcal{N}(q_0, q_0; r) = N(q_0, r)$. Покажем, что $N(n_1)$ существует и удовлетворяет неравенству

$$N(n_1) \leq N(N(N(\ldots N(N(n_1, n_1 - 1), n_1 - 2)\ldots, 3), 2), 1).$$

Чтобы не работать с таким длинным выражением, введем обозначения $n^{(n_1-1)} = n_1$, $n^{(n_1-i-1)} = N(n^{(n_1-i)}, n_1 - i)$, $i = 1, 2, \ldots, n_1 - 1$. Теперь нам надо доказать, что $N(n_1) \leq n^{(0)}$.

Рассмотрим произвольную функцию $f = f^{(0)}$ из $P^n_{2,k}$ от $n = n^{(0)}$ переменных. Сопоставим этой функции множество $A_{n^{(0)}}$ указанным выше способом. Зададим на $A_{n^{(0)}}$ функцию $g^{1,k}_{A_{n^{(0)}}}(A_{n^{(0)}}(x)) = f^{(0)}(x)$, где x пробегает множество всех наборов, содержащих ровно одну единицу. По теореме Рамсея для числа $n^{(0)}$ данного вида у $A_{n^{(0)}}$ найдется $n^{(1)}$-подмножество, на любом 1-подмножестве которого $g^{1,k}_{A_{n^{(0)}}}$ принимает одно и то же значение, обозначим его π_1. Подставим вместо всех переменных функции $f^{(0)}$, соответствующих элементам множества $A_{n^{(0)}}$, не вошедшим в $n^{(1)}$-подмножество, константу 0. Получится функция $f^{(1)}$ из $P^{n^{(1)}}_{2,k}$ от $n^{(1)}$ переменных, которая на всех наборах, содержащих в точности одну единицу, принимает одно и то же значение π_1. Сопоставим однозначно всем переменным функции $f^{(1)}$ элементы множества $A_{n^{(1)}}$. Зададим на $A_{n^{(1)}}$ функцию $g^{2,k}_{A_{n^{(1)}}}(A_{n^{(1)}}(x)) = f^{(1)}(x)$, где x пробегает множество всех наборов, содержащих ровно две единицы. По теореме Рамсея для числа $n^{(1)}$ данного

вида у $A_{n^{(1)}}$ найдется $n^{(2)}$-подмножество, на любом 2-подмножестве которого $g^{2,k}_{A_{n^{(1)}}}$ принимает одно и то же значение, обозначим его π_2. Подставим вместо всех переменных функции $f^{(1)}$, соответствующих элементам множества $A_{n^{(1)}}$, не вошедшим в $n^{(2)}$-подмножество, константу 0. Получится функция $f^{(2)}$ из $P^{n^{(2)}}_{2,k}$ от $n^{(2)}$ переменных, которая на всех наборах, содержащих в точности одну единицу, принимает значение π_1, а на всех наборах, содержащих в точности две единицы, принимает значение π_2. Сопоставим однозначно всем переменным функции $f^{(2)}$ элементы множества $A_{n^{(2)}}$ и продолжим действовать подобным образом. Наконец, на (n_1-1)-м шаге, сопоставим однозначно всем переменным функции $f^{(n_1-2)}$ элементы множества $A_{n^{(n_1-2)}}$, $n^{(n_1-2)} = N(n_1, n_1-1)$. Зададим на $A_{n^{(n_1-2)}}$ функцию $g^{n_1-1,k}_{A_{n^{(n_1-2)}}}(A_{n^{(n_1-2)}}(x)) = f^{(n_1-2)}(x)$, где x пробегает множество всех наборов, содержащих ровно n_1-1 единиц. По теореме Рамсея для числа $n^{(n_1-2)}$ данного вида у $A_{n^{(n_1-2)}}$ найдется $n^{(n_1-1)}$-подмножество, $n^{(n_1-1)} = n_1$, на любом (n_1-1)-подмножестве которого $g^{n_1-1,k}_{A_{n^{(n_1-2)}}}$ принимает одно и то же значение, обозначим его π_{n_1-1}. Подставим вместо всех переменных функции $f^{(n_1-2)}$, соответствующих элементам множества $A_{n^{(n_1-2)}}$, не вошедшим в $n^{(n_1-2)}$-подмножество, константу 0. Получится функция $f^{(n_1-1)}$ из $P^{n^{(n_1-1)}}_{2,k}$ от $n^{(n_1-1)} = n_1$ переменных, которая на всех наборах, содержащих в точности i единиц, $i = 1, 2, \ldots, n_1-1$, принимает соответственно значения π_i. Кроме этих наборов функция $f^{(n_1-1)}$ определена еще на наборе из одних нулей, на котором значение функции $f^{(n_1-1)}$ равно, скажем π_0, и на наборе из n_1 единиц, значение функции $f^{(n_1-1)}$ на котором обозначим через π_{n_1}. Таким образом, функция $f^{(n_1-1)}$ является симметрической функцией от n_1 переменных. Теорема 6.1 доказана. □

Следствие 6.1. *Для любого натурального n_1 найдется минимальное натуральное $N = N(n_1)$ такое, что из любой функции f из класса $P^n_{2,k}$ от $n \geq N(n_1)$ переменных подстановками только констант 1 вместо некоторых переменных можно получить симметрическую подфункцию от n_1 переменных.*

Обобщение теоремы 6.1 на функции из множества $P^n_{q,k}$, $q \geq 3$, $k \geq 2$, неверно. Пусть $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ — набор длины n, где $\sigma_i \in \{0, 1, \ldots, q-1\}$. Всякую

неупорядоченную пару (i,j) такую, что $x_i > x_j$ и $i < j$ назовем *беспорядком* в наборе σ. Введем величину $s_{ij}(\sigma)$, равную 1, если пара (i,j) является беспорядком в наборе σ, и 0, если пара (i,j) не является беспорядком в наборе σ. Общее число беспорядков в наборе σ обозначим через $s(\sigma)$, $s(\sigma) = \sum\limits_{1\le i<j\le n} s_{ij}(\sigma)$.

Теорема 6.2. *Пусть $f(x) = s(x) \pmod 2$ — функция из $P^n_{q,k}$, $q \ge 3$, $k \ge 2$. Тогда функция f не содержит симметрических подфункций от двух переменных.*

Доказательство. Рассмотрим произвольную подфункцию функции $f(x_1, x_2, \ldots, x_n)$, зависящую от двух переменных. Пусть x_l и x_m — единственные две переменные, вместо которых не были подставлены константы, $1 \le l < m \le n$. Обозначим через $x^{\sigma_1\sigma_2}$ наборы длины n, в которых во всех компонентах i, $1 \le i \le n$, $i \ne l, m$, стоят подставленные вместо переменных x_i константы, а в l-й и m-й компонентах стоят соответственно константы σ_1 и σ_2. Тогда

$$
\begin{aligned}
&f(x^{01}) + f(x^{02}) + f(x^{10}) + f(x^{12}) + f(x^{20}) + f(x^{21}) \pmod 2 = \\
&s(x^{01}) + s(x^{02}) + s(x^{10}) + s(x^{12}) + s(x^{20}) + s(x^{21}) \pmod 2 = \\
&= \sum_{\substack{1\le i<j\le n\\ i,j\ne l,m}} \big(s_{ij}(x^{01}) + s_{ij}(x^{02}) + s_{ij}(x^{10}) + s_{ij}(x^{12}) + s_{ij}(x^{20}) + s_{ij}(x^{21})\big) + \\
&\sum_{\substack{1\le i\le n\\ i\ne l,m}} \big(s_{il}(x^{01}) + s_{il}(x^{02}) + s_{il}(x^{10}) + s_{il}(x^{12}) + s_{il}(x^{20}) + s_{il}(x^{21})\big) + \\
&\sum_{\substack{1\le i\le n\\ i\ne l,m}} \big(s_{im}(x^{01}) + s_{im}(x^{02}) + s_{im}(x^{10}) + s_{im}(x^{12}) s_{im}(x^{20}) + s_{im}(x^{21})\big) + \\
&s_{lm}(x^{01}) + s_{lm}(x^{02}) + s_{lm}(x^{10}) + s_{lm}(x^{12}) + s_{lm}(x^{20}) + s_{lm}(x^{21}) \pmod 2 = \\
&= 6 \sum_{\substack{1\le i<j\le n\\ i,j\ne l,m}} s_{ij}(x^{01}) + 2 \sum_{\substack{1\le i\le n\\ i\ne l,m}} s_{il}(x^{01}) + 2 \sum_{\substack{1\le i\le n\\ i\ne l,m}} s_{il}(x^{10}) + 2 \sum_{\substack{1\le i\le n\\ i\ne l,m}} s_{il}(x^{20}) + \\
&2 \sum_{\substack{1\le i\le n\\ i\ne l,m}} s_{im}(x^{10}) + 2 \sum_{\substack{1\le i\le n\\ i\ne l,m}} s_{im}(x^{01}) + 2 \sum_{\substack{1\le i\le n\\ i\ne l,m}} s_{im}(x^{02})(s_{lm}(x^{01}) + s_{lm}(x^{10})) + \\
&(s_{lm}(x^{02}) + s_{lm}(x^{20})) + (s_{lm}(x^{12}) + s_{lm}(x^{21})) \pmod 2 = 3 \pmod 2 = 1.
\end{aligned}
$$

Поэтому, хотя бы на одной из трех пар наборов x^{01} и x^{10}, x^{02} и x^{20}, x^{12} и x^{21} функция f принимает разные значения. Следовательно, рассматриваемая нами подфункция не является симметрической. Теорема 6.2 доказана. □

Теорема 6.3. *(Симона–Вегенера) [115], см. также [121] Для любого натурального n_1 существует такое натуральное n_2, что для любой невырожденной функции f из $P_{2,k}^n$ при $n \geq n_2$ найдется такой набор констант $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_{n_2})$, что $f(\sigma) \neq f(\sigma^i)$ для по крайней мере n_1 значений индекса i, $i = 1, 2, \ldots, n_2$.*

Замечание 6.2. Теорема 6.3 доказана в [115] и [121] для булевых функций, т. е. для случая $k = 2$. Однако приведенные там доказательства можно дословно повторить и для случая произвольного k.

Теорема 6.4. *Для любого натурального n_1 существует такое натуральное n_2, что из любой невырожденной функции f из $P_{2,k}^n$ при $n \geq n_2$ подстановками констант 0 и 1 можно получить невырожденную симметрическую подфункцию от n_1 переменных.*

Доказательство. Для заданного n_1 выберем $N(n_1)$ из теоремы 6.1. По теореме 6.3 для натурального $2N(n_1)$ существует такое натуральное n_2, что для произвольной невырожденной функции f из $P_{2,k}^n$, $n \geq n_2$ найдется такой набор констант $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n)$, что $f(\sigma) \neq f(\sigma^i)$ для $2N(n_1)$ значений индекса i, а именно для значений из множества $A = \{i_1, i_2, \ldots, i_{2N(n_1)}\}$ мощности $2N(n_1)$. Разобьем множество A на два непересекающихся подмножества A_0 и A_1, $A = A_0 \bigcup A_1$, так что $i_j \in A_0$, если $\sigma_{i_j} = 0$, и $i_j \in A_1$, если $\sigma_{i_j} = 1$. Мощность по крайней мере одного из множеств A_0 и A_1 не меньше чем $N(n_1)$. Пусть $|A_0| \geq N(n_1)$. Выделим в A_0 подмножество A_0', $|A_0'| = N(n_1)$, и подставим в f константы σ_i вместо переменных x_i соответственно, $i \notin A_0'$; переменные x_i, $i \in A_0'$, оставим свободными. В результате таких подстановок получим функцию f' из $P_{2,k}^{N(n_1)}$, причем $f'(\widetilde{0}) \neq f'(0^i)$ для всех $i = 1, 2, \ldots, N(n_1)$. По теореме 6.1, учитывая выбор числа $N(n_1)$, из функции f' путем подстановок констант 0 вместо некоторых переменных можно получить симметрическую подфункцию f'' из $P_{2,k}^{n_1}$, причем причем $f''(\widetilde{0}) \neq f''(0^i)$ для всех $i = 1, 2, \ldots, n_1$. Таким образом, функция f'' зависит существенно от всех своих переменных, т. е. невырождена. В случае, если $|A_1| \geq N(n_1)$, действуем аналогичным образом. Выделим в A_1 подмножество A_1', $|A_1'| = N(n_1)$, и подставим в f константы σ_i вместо

переменных x_i соответственно, $i \notin A'_1$; переменные x_i, $i \in A'_1$, оставим свободными. В результате таких подстановок получим функцию f' из $P_{2,k}^{N(n_1)}$, причем $f'(\widetilde{1}) \neq f'(1^i)$ для всех $i = 1, 2, \ldots, N(n_1)$. По следствию 6.1, учитывая выбор числа $N(n_1)$, из функции f' путем подстановок констант 1 вместо некоторых переменных можно получить симметрическую подфункцию f'' из $P_{2,k}^{n_1}$, причем $f''(\widetilde{1}) \neq f''(1^i)$ для всех $i = 1, 2, \ldots, n_1$. Таким образом, функция f'' зависит существенно от всех своих переменных, т. е. невырождена. Тем самым теорема 6.4 доказана. □

6.2 О некоторых оценках для веса l-уравновешенных булевых функций

Напомним, что весом булевой функции f называется величина $wt(f)$, равная числу наборов, на которых функция f принимает значение 1. Величину $\rho(f) = wt(f)/2^n$ назовем плотностью n-местной булевой функции f.

Пусть l — целое неотрицательное число. Булева функция $f(x_1, x_2, \ldots, x_n)$ называется *l-уравновешенной,* если для любых ее подфункций f_1 и f_2 от одинакового числа переменных выполнено неравенство $|wt(f_1) - wt(f_2)| \leq l$.

В [21] описаны все 1-уравновешенные булевы функции. Некоторые оценки веса l-уравновешенных булевых функций приведены в [128]. Главной целью настоящего параграфа является доказательство того, что при больших n плотности l-уравновешенных функций близки к одному из следующих пяти чисел: 0, 1/3, 1/2, 2/3 или 1. Результаты параграфа изложены в работе автора [129].

Теорема 6.5. *Для любого натурального l и любого положительного ε существует такое натуральное N, что для любого натурального n, не меньшего N, и для любой l-уравновешенной булевой функции f от n переменных имеет место одно из следующих пяти неравенств:*

$$wt(f) \leq 2l;$$
$$|\rho(f) - 1/3| < \varepsilon;$$
$$|\rho(f) - 1/2| < \varepsilon;$$
$$|\rho(f) - 2/3| < \varepsilon;$$
$$wt(f) \geq 2^n - 2l.$$

Для доказательства теоремы докажем серию лемм.

Лемма 6.1. *Для любого натурального m найдется такое $N(m)$, что при $n > N(m)$ и $l < m/2$ не существует l-уравновешенных n-местных функций, имеющих вес m.*

Доказательство. Сопоставим функции f с весом m матрицу размера $m \times n$, в строках которой записаны все m наборов длины n, на которых функция

f принимает единичное значение. При $n \geq 2^m + 1$ в матрице найдутся два совпадающих столбца. Пусть эти столбцы соответствуют переменным x_i и x_j. Тогда вес подфункций $f|_{x_i=0,x_j=1}$ и $f|_{x_i=1,x_j=0}$ равен 0, а вес одной из подфункций $f|_{x_i=0,x_j=0}$ и $f|_{x_i=1,x_j=1}$ не меньше $l+1$. Следовательно, функция f не является l-уравновешенной. Таким образом, утверждение леммы 6.1 справедливо при $N(m) = 2^m$. □

Лемма 6.2. *Для любого натурального l существует такая положительная константа $c(l)$, что для любой l-уравновешенной булевой функции f с весом $wt(f)$, $wt(f) > 2l$, справедливо неравенство $\rho(f) \geq c(l)$.*

Доказательство. Пусть $f = f_0$ — функция, удовлетворяющая условиям леммы. Если $wt(f) > 5l$, то разложим функцию f по любой переменной на две подфункции от $n-1$ переменной и обозначим через f_1 ту из этих подфункций, которая имеет меньший вес (если веса равны, выбираем f_1 произвольно). Из свойства l-уравновешенности вытекает, что $wt(f_1) > 2l$; кроме того, очевидно, что $\rho(f) \geq \rho(f_1)$. Далее, если $wt(f_1) > 5l$, разложим функцию f_1 по любой переменной на две подфункции от $n-2$ переменных и обозначим через f_2 ту, которая имеет меньший вес (если веса равны, выбираем f_2 произвольно) и т. д. На некотором (s-м) шаге, $s \geq 0$, получим функцию f_s, вес которой удовлетворяет неравенствам $2l+1 \leq wt(f_s) \leq 5l$, и для плотности которой справедливо неравенство $\rho(f) \geq \rho(f_s)$.

По лемме 6.1 для любого m, $m > 2l$, существует лишь конечное число l-уравновешенных функций с весом m, поэтому определена величина $c(l) = \min\limits_{g} \rho(g)$, где минимум берется по всем l-уравновешенным функциям g, для которых выполнены неравенства $2l+1 \leq wt(g) \leq 5l$.

Из определения величины $c(l)$ очевидно, что $c(l) > 0$ и $\rho(f_s) \geq c(l)$. Тем самым $\rho(f) \geq c(l)$. Лемма 6.2 доказана. □

Лемма 6.3. *Для любого натурального n_1 существует такое натуральное N, что у любой булевой функции f от N переменных найдется симметрическая подфункция от n_1 переменных.*

Proof. Данная лемма является частным случаем теоремы 6.1. □

Будем говорить, что симметрическая булева функция от n переменных имеет *период* T, если при всех i, $0 \le i \le n-T$, имеет место соотношение $\pi_i = \pi_{i+T}$.

Лемма 6.4. *Для любых натуральных l и n_2 существует такое натуральное N, что у любой l-уравновешенной булевой функции f от N переменных найдется n_2-местная симметрическая периодическая подфункция с периодом T, не превосходящим 2^{l+1}.*

Доказательство. Положим $n_1 = \max\{n_2+2, 2^{l+1}+l+3\}$. В силу леммы 6.3 существует такое натуральное N, что у любой булевой функции f от N переменных найдется симметрическая подфункция f_1 от n_1 переменных. Рассмотрим характеристическую последовательность $\pi = (\pi_0, \pi_1, \ldots, \pi_{n_1})$ этой подфункции. Среди ее первых $2^{l+1}+l+1$ элементов по принципу Дирихле найдутся два совпадающих отрезка длины $l+1$: $(\pi_h, \pi_{h+1}, \ldots, \pi_{h+l})$ и $(\pi_{h+T}, \pi_{h+T+1}, \ldots, \pi_{h+T+l})$, где $T \le 2^{l+1}$, $h \ge 0$, $h+T+l \le 2^{l+1}+l+1$. Совпадение отрезков означает, что $\pi_i = \pi_{T+i}$ при $i = h, h+1, \ldots, h+l$. Докажем, что равенство $\pi_i = \pi_{T+i}$ верно для всех i, $i = 1, 2, \ldots, n_1 - T - 1$.

Пусть равенство $\pi_i = \pi_{T+i}$ установлено для всех таких натуральных i, что $h \le i \le j$, где j удовлетворяет неравенствам $h+l \le j \le n_1 - 2$. Установим равенство $\pi_{j+1} = \pi_{T+j+1}$. Для этого рассмотрим функции $f' = f_1[j-l,\, j+2]$ и $f'' = f_1[T+j-l,\, T+j+2]$. Эти функции являются подфункциями функции f, поэтому они сами l-уравновешены. Для весов функций f_1 и f_2 имеем $wt(f_1) = \sum\limits_{i=0}^{l+2} \binom{l+2}{i} \pi_{j-l+i}$, $wt(f_2) = \sum\limits_{i=0}^{l+2} \binom{l+2}{i} \pi_{T+j-l+i}$ и

$$|wt(f_1) - wt(f_2)| = \left| \sum_{i=0}^{l+2} \binom{l+2}{i} (\pi_{j-l+i} - \pi_{T+j-l+i}) \right| =$$
$$\left| \binom{l+2}{l+1} (\pi_{j+1} - \pi_{T+j+1}) + \binom{l+2}{l+2} (\pi_{j+2} - \pi_{T+j+2}) \right| =$$
$$|(l+2)(\pi_{j+1} - \pi_{T+j+1}) + (\pi_{j+2} - \pi_{T+j+2})| \ge (l+2)|\pi_{j+1} - \pi_{T+j+1}| - 1.$$

Поэтому если $\pi_{j+1} \ne \pi_{T+j+1}$, то $|wt(f_1) - wt(f_2)| \ge l+1$, что противоречит l-уравновешенности функции f. Следовательно, $\pi_{j+1} = \pi_{T+j+1}$.

Аналогично, пусть равенство $\pi_i = \pi_{T+i}$ установлено для всех таких целых i, что $j \le i \le h+l$, где $2 \le j \le h$. Установим равенство $\pi_{j-1} = \pi_{T+j-1}$. Для этого

рассмотрим функции $f' = f_1[j-2, j+l]$ и $f'' = f_1[T+j-2, T+j+l]$. Эти функции являются подфункциями функции f, потому они l-уравновешены. Подобно рассмотренному выше, имеем $wt(f_1) = \sum\limits_{i=0}^{l+2} \binom{l+2}{i} \pi_{j-2+i}$, $wt(f_2) = \sum\limits_{i=0}^{l+2} \binom{l+2}{i} \pi_{T+j-2+i}$ и

$$|wt(f_1) - wt(f_2)| = \left| \sum_{i=0}^{l+2} \binom{l+2}{i} (\pi_{j-2+i} - \pi_{T+j-2+i}) \right| =$$

$$\left| \binom{l+2}{0} \cdot (\pi_{j-2} - \pi_{T+j-2}) + \binom{l+2}{1} (\pi_{j-1} - \pi_{T+j-1}) \right| =$$

$$|(l+2)(\pi_{j-1} - \pi_{T+j-1}) + (\pi_{j-2} - \pi_{T+j-2})| \geq (l+2)|\pi_{j-1} - \pi_{T+j-1}| - 1.$$

Поэтому если $\pi_{j-1} \neq \pi_{T+j-1}$, то $|wt(f_1) - wt(f_2)| \geq l+1$, что противоречит l-уравновешенности функции f. Следовательно, $\pi_{j-1} = \pi_{T+j-1}$.

Таким образом, равенство $\pi_i = \pi_{T+i}$ установлено для всех целых i, удовлетворяющих неравенствам $1 \leq i \leq n_1 - T - 1$. Рассмотрим функцию $f_2 = f_1[1, n_2 + 1]$ от n_2 переменных. (Задание функции f_2 корректно, так как $n_1 \geq n_2 + 2$.) Функция f_2, очевидно, является симметрической периодической функцией с периодом, не превосходящим 2^{l+1}, и по построению является подфункцией функции f, что доказывает лемму 6.4.

Утверждение 6.1. *Симметрическая периодическая (с периодом T) булева функция от заданного числа переменных полностью определяется начальным отрезком характеристической последовательности (который в дальнейшем будем называть характеристическим отрезком), включающим в себя ее первые T элементов. Обозначим его $\pi[T] = (\pi_0, \pi_1, \ldots, \pi_{T-1})$.*

Через ε_k будем обозначать k-й корень степени T из единицы, $\varepsilon_k = \cos \frac{2\pi k}{T} + i \sin \frac{2\pi k}{T}$. Обозначим $r_k = |1 + \varepsilon_k|$.

Утверждение 6.2. *Если a, b, c, d — целые числа, то, как известно, $\varepsilon_{ab}^{cd} = \varepsilon_{abc}^{d} = \varepsilon_{a}^{bcd}$.*

Утверждение 6.3. *При $0 \leq k_1 < k_2 \leq \lfloor (T-1)/2 \rfloor$ выполняется неравенство $r_{k_1} > r_{k_2}$.*

Утверждение 6.4. *При $k < T/3$ выполняется неравенство $r_k > 1$.*

Утверждение 6.5. *При четных T выполняется равенство $r_{T/2} = 0$.*

Лемма 6.5. *При целых n, T и j, удовлетворяющих неравенствам $n > 0$ и $0 \le j < T$, справедлива формула*

$$\sum_{i=0}^{\lfloor (n-j)/T \rfloor} \binom{n}{j+iT} = \frac{2^n}{T} + \frac{2}{T} \sum_{k=1}^{\lfloor (T-1)/2 \rfloor} r_k^n \cos \frac{\pi k(n-2j)}{T}.$$

Формулы подобного вида встречаются в [98], [99] и [4].

Доказательство. Обозначим $a_j(n) = \sum\limits_{i=0}^{\lfloor (n-j)/T \rfloor} \binom{n}{j+iT}$, $j = 0, 1, \ldots, T-1$, $\overrightarrow{a}(n) = (a_0(n), a_1(n), \ldots, a_{T-1}(n))$. Тогда $\overrightarrow{a}^T(n) = A \cdot \overrightarrow{a}^T(n-1)$, где A — матрица порядка T,

$$A = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 & 1 \\ 1 & 1 & 0 & \ldots & 0 & 0 & 0 \\ 0 & 1 & 1 & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 & 0 \\ 0 & 0 & 0 & \ldots & 1 & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 & 1 \end{pmatrix}.$$

Матрица A имеет собственные значения $\lambda_k = 1 + \varepsilon_k$, $k = 0, 1, \ldots, T-1$, и собственные векторы $\overrightarrow{c}_k = (c_k^0, c_k^1, \ldots, c_k^{T-1})$, где $c_k^j = \varepsilon_{-kj}$, $k, j = 0, 1, \ldots, T-1$.

Учитывая утверждение 6.5, при $n > 0$, $j = 0, 1, \ldots, T-1$, имеем $a_j(n) = \sum\limits_{k=0}^{T-1} \frac{(\overrightarrow{a}(0), \overrightarrow{\overline{c_k}})}{(\overrightarrow{c_k}, \overrightarrow{\overline{c_k}})} c_k^j \cdot \lambda_k^n = \sum\limits_{k=0}^{T-1} \frac{1}{T} \varepsilon_{-kj} (1 + \varepsilon_k)^n = \frac{1}{T} \sum\limits_{k=0}^{T-1} r_k^n \varepsilon_{k(n-2j)/2} = \frac{2^n}{T} + \frac{1}{T} \cdot \sum\limits_{k=1}^{\lfloor (T-1)/2 \rfloor} r_k^n \left(\varepsilon_{k(n-2j)/2} + \varepsilon_{(T-k)(n-2j)/2} \right) = \frac{2^n}{T} + \frac{2}{T} \sum\limits_{k=1}^{\lfloor (T-1)/2 \rfloor} r_k^n \cos \frac{\pi k(n-2j)}{T}$, что доказывает лемму. □

Лемма 6.6. *Пусть $F = \{f_n\}$, $n = 1, 2, \ldots,$ — бесконечная последовательность симметрических периодических булевых функций, где f_n — n-местная функция, задаваемая характеристическим отрезком $\pi[T] = (\pi_0, \pi_1, \ldots, \pi_{T-1})$. Если все функции из последовательности F являются l-уравновешенными, то для любого натурального k, меньшего $T/3$, выполняется равенство $\sum\limits_{j=0}^{T-1} \pi_j \varepsilon_{kj} = 0$.*

Доказательство. Предположим, что утверждение леммы неверно. Обозначим через K минимальное k, для которого $\sum\limits_{j=0}^{T-1} \pi_j \varepsilon_{kj} \neq 0$; при этом $K < T/3$. Тогда равенство $\sum\limits_{j=0}^{T-1} \pi_j \varepsilon_{kj} = 0$ выполняется для всех натуральных k, меньших K, и справедливо соотношение $\sum\limits_{j=0}^{T-1} \pi_j \varepsilon_{Kj} \neq 0$.

Рассмотрим последовательность булевых функций $F' = \{f'_n\}$, $n = 1, 2, \ldots$, такую, что $f'_n = f_{n'+T-1}$, где $n' = 2nT$. Обозначим $f_n^m = f'_n[m, n'+m]$, $m = 0, 1, \ldots, T-1$. Все функции f_n^m, очевидно, являются l-уравновешенными симметрическими периодическими функциями с периодом T.

Для веса функции f_n^m, используя лемму 6.5, имеем

$$wt(f_n^m) = \sum_{i=0}^{n'} \binom{n'}{i} \pi_{i+m} = \sum_{j=0}^{T-1} \sum_{i=0}^{\lfloor (n'-j)/T \rfloor} \binom{n'}{j+iT} \pi_{j+m} =$$

$$= \sum_{j=0}^{T-1} \pi_{j+m} \sum_{i=0}^{\lfloor (n'-j)/T \rfloor} \binom{n'}{j+iT} =$$

$$= \sum_{j=0}^{T-1} \pi_{j+m} \left(\frac{2^{n'}}{T} + \frac{2}{T} \sum_{k=1}^{\lfloor (T-1)/2 \rfloor} r_k^{n'} \cos \frac{\pi k (n'-2j)}{T} \right) =$$

$$= \sum_{j=0}^{T-1} \pi_{j+m} \left(\frac{2^{n'}}{T} + \frac{2}{T} \sum_{k=1}^{\lfloor (T-1)/2 \rfloor} r_k^{n'} \cos \frac{2\pi k j}{T} \right) =$$

$$= \frac{2^{n'}}{T} \sum_{j=0}^{T-1} \pi_{j+m} + \sum_{k=1}^{\lfloor (T-1)/2 \rfloor} r_k^{n'} \cdot \frac{2}{T} \sum_{j=0}^{T-1} \pi_{j+m} \cos \frac{2\pi k j}{T} =$$

$$= \frac{2^{n'}}{T} \sum_{j=0}^{T-1} \pi_j + \sum_{k=1}^{\lfloor (T-1)/2 \rfloor} r_k^{n'} \cdot \frac{2}{T} \sum_{j=0}^{T-1} \pi_j \cos \frac{2\pi k (j-m)}{T}.$$

По предположению $\sum\limits_{j=0}^{T-1} \pi_j \varepsilon_{kj} = 0$ для всех натуральных k, меньших K. Отсюда $\sum\limits_{j=0}^{T-1} \pi_j \varepsilon_{kj} \varepsilon_{-km} = 0$ для любого m и, таким образом,

$$\sum_{j=0}^{T-1} \pi_j \cos \frac{2\pi k (j-m)}{T} = 0.$$

Далее, из того, что $\sum\limits_{j=0}^{T-1} \pi_j \varepsilon_{Kj} \neq 0$ и $K < T/3$, следует, что значения трех сумм $\sum\limits_{j=0}^{T-1} \pi_j \varepsilon_{Kj} \varepsilon_{-Km}$, $m = 0, 1, 2$, попарно различны. Однако значения этих трех сумм равны по абсолютной величине, поэтому среди значений их действительных частей $\sum\limits_{j=0}^{T-1} \pi_j \cos \dfrac{2\pi K(j-m)}{T}$, $m = 0, 1, 2$, найдутся по крайней мере два различных. Пусть различны значения сумм $\sum\limits_{j=0}^{T-1} \pi_j \cos \dfrac{2\pi K(j-m_1)}{T}$ и $\sum\limits_{j=0}^{T-1} \pi_j \cos \dfrac{2\pi K(j-m_2)}{T}$, $m_1, m_2 \in \{0, 1, 2\}$. Тогда, используя утверждения 6.3 и 6.4, имеем

$$
\begin{aligned}
|wt(f_n^{m_1}) - wt(f_n^{m_2})| = \Bigg| \sum_{k=K}^{\lfloor (T-1)/2 \rfloor} r_k^{n'} \cdot \frac{2}{T} \sum_{j=0}^{T-1} \pi_j \cos \frac{2\pi k(j-m_1)}{T} - \\
- \sum_{k=K}^{\lfloor (T-1)/2 \rfloor} r_k^{n'} \cdot \frac{2}{T} \sum_{j=0}^{T-1} \pi_j \cos \frac{2\pi k(j-m_2)}{T} \Bigg| \geq \\
\geq \left| r_K^{n'} \cdot \frac{2}{T} \left(\sum_{j=0}^{T-1} \pi_j \cos \frac{2\pi K(j-m_1)}{T} - \sum_{j=0}^{T-1} \pi_j \cos \frac{2\pi K(j-m_2)}{T} \right) \right| - \\
- \left| \sum_{k=K+1}^{\lfloor (T-1)/2 \rfloor} r_k^{n'} \cdot \frac{2}{T} \sum_{j=0}^{T-1} \pi_j \cos \frac{2\pi k(j-m_1)}{T} - \right. \\
\left. - \sum_{k=K+1}^{\lfloor (T-1)/2 \rfloor} r_k^{n'} \cdot \frac{2}{T} \sum_{j=0}^{T-1} \pi_j \cos \frac{2\pi k(j-m_2)}{T} \right| \geq \\
\geq r_K^{n'} \cdot \frac{2}{T} \left| \sum_{j=0}^{T-1} \pi_j \cos \frac{2\pi K(j-m_1)}{T} - \sum_{j=0}^{T-1} \pi_j \cos \frac{2\pi K(j-m_2)}{T} \right| - \\
- r_{K+1}^{n'} \cdot \frac{T-1}{2} \cdot \frac{2}{T} \cdot 2T = C_1 r_K^{n'} - C_2 r_{K+1}^{n'},
\end{aligned}
$$

где C_1 и C_2 не зависят от n', причем $C_1 > 0$. При $n' \to \infty$, поскольку $r_K > r_{K+1}$ и $r_K > 1$, имеем $C_1 r_K^{n'} - C_2 r_{K+1}^{n'} \to \infty$. Следовательно, все функции из последовательности F', а, следовательно, и из последовательности F, не могут быть одновременно l-уравновешенными, что противоречит условию леммы. $\square$

Утверждение 6.6. *Каждая функция из последовательности F является*

подфункцией всех последующих функций из F, поскольку получается из них подстановкой константы 0 вместо лишних переменных. Поэтому если в F найдется функция, не являющаяся l-уравновешенной, то F содержит лишь конечное число l-уравновешенных функций.

Лемма 6.7. *Пусть f — симметрическая периодическая булева функция с периодом $T = 6$, задаваемая характеристическим отрезком $\pi[6] = (\pi_0, \pi_1, \ldots, \pi_5)$, и пусть выполняется равенство $\sum_{j=0}^{5} \pi_j \varepsilon_j = 0$. Тогда функция f имеет период $T' \le 3$.*

Доказательство. Отрицание симметрической периодической булевой функцией является симметрической периодической булевой функцией с тем же периодом. Поэтому достаточно ограничиться случаем $\sum_{j=0}^{5} \pi_j \le 3$. Заметим также, что достаточно обнаружить период T' в последовательности $(\pi_0, \pi_1, \ldots, \pi_5)$.

1. Пусть $\sum_{j=0}^{5} \pi_j = 0$. Тогда, очевидно, все π_j имеют значение 0, и функция f имеет период 1.

2. Пусть $\sum_{j=0}^{5} \pi_j = 1$, т. е. отлично от 0 только одно из π_j. Тогда $\sum_{j=0}^{5} \pi_j \varepsilon_j \ne 0$, поэтому такой случай невозможен.

3. Пусть $\sum_{j=0}^{5} \pi_j = 2$, и пусть $\pi_{m_1} = \pi_{m_2} = 1$, $0 \le m_1 < m_2 \le 5$. Тогда из $\sum_{j=0}^{5} \pi_j \varepsilon_j = 0$ следует $\varepsilon_{m_1} = -\varepsilon_{m_2}$. Отсюда $m_2 - m_1 = 3$ и, таким образом, равенство $\pi_j = \pi_{j+3}$ выполняется для $j = 0, 1, 2$. Поэтому функция f имеет период 3.

4. Пусть $\sum_{j=0}^{5} \pi_j = 3$. Легко видеть, что при этом соотношение $\sum_{j=0}^{5} \pi_j \varepsilon_j = 0$ выполнено только в двух случаях: $\pi[6] = (0, 1, 0, 1, 0, 1)$ и $\pi[6] = (1, 0, 1, 0, 1, 0)$. Поэтому функция f имеет период 2.

Все случаи рассмотрены. Лемма 6.7 доказана. □

Корень h-й степени из единицы ξ называется *примитивным,* если все корни h-й степени из единицы представимы в виде ξ^i, $i \in \{0, 1, \ldots, h-1\}$.

Лемма 6.8. *[117], с. 203. Пусть корнем многочлена с рациональными коэффициентами $F(x)$ является примитивный корень ξ из единицы степени h.*

Тогда все примитивные корни h-й степени из единицы являются корнями многочлена $F(x)$.

Лемма 6.9. *Пусть f — симметрическая периодическая булева функция с периодом T, задаваемая характеристическим отрезком $\pi[T] = (\pi_0, \pi_1, \ldots, \pi_{T-1})$, и пусть для любого натурального k, меньшего $T/3$, выполняется равенство $\sum\limits_{j=0}^{T-1} \pi_j \varepsilon_{kj} = 0$. Тогда функция f имеет период $T' \leq 3$.*

Доказательство. Рассмотрим многочлен $\Pi(x) = \sum\limits_{j=0}^{T-1} \pi_j x^j$; его степень по построению не превосходит $T-1$. При $k < T/3$ по условию леммы $\sum\limits_{j=0}^{T-1} \pi_j \varepsilon_{kj} = 0$. По утверждению 6.2 имеем $\varepsilon_{kj} = \varepsilon_k^j$, поэтому ε_k — корень многочлена $\Pi(x)$.

Каждый корень степени T из единицы является примитивным корнем из единицы некоторой натуральной степени h, делящей T нацело, причем примитивным корнем 1-й степени из единицы является лишь ε_0, 2-й степени — лишь $\varepsilon_{T/2}$ (если T делится на 2), 3-й степени — лишь $\varepsilon_{T/3}$ и $\varepsilon_{2T/3}$ (если T делится на 3). Пусть ε_j — произвольный примитивный корень из единицы степени h, большей чем 3. Тогда $\varepsilon_{T/h}$ — также примитивный корень из единицы степени h, а так как $T/h < T/3$, число $\varepsilon_{T/h}$ является по доказанному выше корнем многочлена $\Pi(x)$; по лемме 6.8 получаем, что ε_j также является корнем многочлена $\Pi(x)$. Следовательно, корнями многочлена $\Pi(x)$ являются все корни из единицы степени T, за исключением, быть может, ε_0, $\varepsilon_{T/2}$ (если T делится на 2), $\varepsilon_{T/3}$ и $\varepsilon_{2T/3}$ (если T делится на 3).

Обозначим через $\Psi(x)$ многочлен $\prod\limits_{\substack{j=1 \\ j \neq T/3, T/2, 2T/3}}^{T-1} (x - \varepsilon_j)$. Все корни многочлена $\Psi(x)$ являются корнями многочлена $\Pi(x)$ и в поле многочленов с комплексными коэффициентами нет делителей нуля, поэтому $\Pi(x)$ делится на $\Psi(x)$. Частное обозначим через $\Theta(x)$: $\Pi(x) = \Psi(x)\Theta(x)$, $\deg \Theta(x) \leq \deg \Pi(x) - \deg \Psi(x)$ (Знак неравенства поставлен с тем, чтобы не исключать возможный случай $\Pi(x) \equiv 0$). В зависимости от того, делится ли T на 2 и 3, возможны четыре случая.

1. Пусть T не делится ни на 2, ни на 3. Тогда

$$\Psi(x) = \prod_{j=1}^{T-1}(x - \varepsilon_j) = \frac{\prod_{j=0}^{T-1}(x - \varepsilon_j)}{x - \varepsilon_0} = \frac{x^T - 1}{x - 1} = \sum_{j=0}^{T-1} x^j.$$

Отсюда имеем $\Pi(x) = \sum_{j=0}^{T-1} x^j \cdot \Theta(x)$. Из того, что $\deg\Theta(x) \le \deg\Pi(x) - \deg\Psi(x) \le 0$, следует, что многочлен $\Theta(x)$ равен некоторой константе a. Следовательно, $\Pi(x) = a\sum_{j=0}^{T-1} x^j$ и, таким образом, коэффициенты при всех степенях многочлена $\Pi(x)$ равны. Тогда, очевидно, равенство $\pi_j = \pi_{j+1}$ выполняется для любого целого неотрицательного j. Поэтому функция f имеет период 1.

2. Пусть $T = 2t$, T не делится на 3. Тогда

$$\Psi(x) = \prod_{\substack{j=1\\ j\ne t}}^{T-1}(x - \varepsilon_j) = \frac{\prod_{j=0}^{T-1}(x - \varepsilon_j)}{(x - \varepsilon_0)(x - \varepsilon_t)} = \frac{x^{2t} - 1}{(x - 1)(x + 1)} = \sum_{j=0}^{t-1} x^{2j}.$$

Отсюда имеем $\Pi(x) = \sum_{j=0}^{t-1} x^{2j} \cdot \Theta(x)$. Из того, что $\deg\Theta(x) \le \deg\Pi(x) - \deg\Psi(x) \le 2t - 1 - (2t - 2) = 1$, следует, что многочлен $\Theta(x)$ имеет вид $ax + b$. Следовательно, $\Pi(x) = (ax + b)\sum_{j=0}^{t-1} x^{2j}$ и, таким образом, последовательность коэффициентов многочлена $\Pi(x)$ имеет период 2. Поэтому функция f также имеет период 2.

3. Пусть $T = 3t$, T не делится на 2. Тогда

$$\Psi(x) = \prod_{\substack{j=1\\ j\ne t,2t}}^{T-1}(x - \varepsilon_j) = \frac{\prod_{j=0}^{T-1}(x - \varepsilon_j)}{(x - \varepsilon_0)(x - \varepsilon_t)(x - \varepsilon_{2t})} =$$

$$= \frac{x^{3t} - 1}{(x - 1)(x^2 + x + 1)} = \sum_{j=0}^{t-1} x^{3j}.$$

Отсюда имеем $\Pi(x) = \sum_{j=0}^{t-1} x^{3j} \cdot \Theta(x)$. Из того, что $\deg\Theta(x) \le \deg\Pi(x) - \deg\Psi(x) \le 3t - 1 - (3t - 3) = 2$, следует, что многочлен $\Theta(x)$ имеет вид

ax^2+bx+c. Следовательно, $\Pi(x) = (ax^2+bx+c)\sum\limits_{j=0}^{t-1} x^{3j}$ и последовательность коэффициентов многочлена $\Pi(x)$ имеет период 3. Поэтому функция f также имеет период 3.

4. Пусть $T = 6t$. Тогда

$$\Psi(x) = \prod_{\substack{j=1\\ j\neq 2t,3t,4t}}^{T-1}(x-\varepsilon_j) = \frac{\prod\limits_{j=0}^{T-1}(x-\varepsilon_j)}{(x-\varepsilon_0)(x-\varepsilon_{2t})(x-\varepsilon_{3t})(x-\varepsilon_{4t})} =$$

$$= \frac{x^{6t}-1}{(x-1)(x+1)(x^2+x+1)} =$$

$$= \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)}\sum_{j=0}^{t-1} x^{6j} = (x^2-x+1)\sum_{j=0}^{t-1} x^{6j}.$$

Отсюда имеем $\Pi(x) = (x^2-x+1)\sum\limits_{j=0}^{t-1} x^{6j}\Theta(x)$. Из того, что $\deg\Theta(x) \leq \deg\Pi(x) - \deg\Psi(x) \leq 6t-1-(6t-4) = 3$, следует, что многочлен $\Theta(x)$ имеет вид ax^3+bx^2+cx+d. Следовательно, $\Pi(x) = \big((ax^3+bx^2+cx+d)(x^2-x+1)\big)\sum\limits_{j=0}^{t-1} x^{6j}$ и последовательность коэффициентов многочлена $\Pi(x)$ имеет период 6. Поэтому функция f также имеет период 6. Покажем, что 6 — не минимальный период. Из равенства $\sum\limits_{j=0}^{6t-1}\pi_j\varepsilon_{tj} = 0$ следует, что $\sum\limits_{j=0}^{6t-1}\pi_j\varepsilon_{tj} = \sum\limits_{i=0}^{t-1}\sum\limits_{j=0}^{5}\pi_{j+6i}\varepsilon_{t(j+6i)} = \sum\limits_{i=0}^{t-1}\sum\limits_{j=0}^{5}\pi_j\varepsilon_{tj} = t\sum\limits_{j=0}^{5}\pi_j\varepsilon_j^t = 0$ и, таким образом, $\sum\limits_{j=0}^{5}\pi_j\varepsilon_j^t = 0$. Поскольку ε^t является первым корнем 6-й степени из единицы, условия леммы 6.7 полностью соблюдены, и, таким образом, функция f имеет период не более 3.

Все случаи рассмотрены. Лемма 6.9 доказана. □

Обозначим через $\mathcal{F}(l, T_{\max})$ множество, состоящее из всех l-ура новешенных симметрических периодических булевых функций с периодом, не превосходящим $T_{\max}$.

Лемма 6.10. *Для любого натурального l множество $\mathcal{F}(l, 2^{l+1})\setminus\mathcal{F}(l,3)$ конечно.*

Доказательство. Пусть $\pi[T]$ — некоторый характеристический отрезок дли-

ны T, где $T \leq 2^{l+1}$. Рассмотрим последовательность симметрических периодических булевых функций $F(\pi[T]) = \{f_n\}$, $n = 1, 2, \ldots$, задаваемую характеристическим отрезком $\pi[T]$. Если последовательность $F(\pi[T])$ содержит бесконечное число l-уравновешенных функций, то по леммам 6.6 и 6.9 и утверждению 6.6 все функции из последовательности $F(\pi[T])$ являются симметрическими периодическими булевыми функциями с периодом, не превосходящим 3. Таким образом, последовательность $F(\pi[T])$ в любом случае содержит лишь конечное число функций из множества $\mathcal{F}(l, 2^{l+1}) \setminus \mathcal{F}(l, 3)$.

Существует лишь конечное число характеристических отрезков длины, не превосходящей 2^{l+1}, и, значит, множество $\mathcal{F}(l, 2^{l+1}) \setminus \mathcal{F}(l, 3)$ покрывается конечным числом последовательностей $F(\pi[T])$. Следовательно, множество $\mathcal{F}(l, 2^{l+1}) \setminus \mathcal{F}(l, 3)$ конечно. □

Лемма 6.11. *Для любых натуральных l и n' существует такое натуральное N, что у любой l-уравновешенной булевой функции f от N переменных найдется симметрическая периодическая подфункция f' от n' переменных с периодом, не превосходящим* 3.

Доказательство. По лемме 10 найдется такое натуральное n_2, не меньшее n', для которого не существует булевых функций, принадлежащих множеству $\mathcal{F}(l, 2^{l+1}) \setminus \mathcal{F}(l, 3)$ и имеющих не менее n_2 переменных. По лемме 6.4 существует такое натуральное N, что у любой l-уравновешенной булевой функции f от N переменных найдется симметрическая периодическая подфункция f' от n_2 переменных с периодом, не превосходящим 2^{l+1}, и, следовательно, не превосходящим 3. Функция $f'[0, n']$ является, очевидно, симметрической периодической подфункцией от n' переменных с периодом, не превосходящим 3. Лемма 6.11 доказана. □

Лемма 6.12. *Пусть функция f является симметрической периодической булевой функцией от n' переменных с периодом T, не превосходящим* 3. *Тогда* $wt(f) \in \{0, \lfloor 2^{n'}/3 \rfloor, \lceil 2^{n'}/3 \rceil, 2^{n'}/2, \lfloor 2^{n'+1}/3 \rfloor, \lceil 2^{n'+1}/3 \rceil, 2^{n'}\}$.

Доказательство. 1. Пусть $T = 1$. Тогда

$$wt(f) = \sum_{i=0}^{n'} \binom{n'}{i} \pi_i = \pi_0 \sum_{i=0}^{n'} \binom{n'}{i} = \pi_0 \cdot 2^{n'}$$

и, следовательно, в этом случае $wt(f) \in \{0, 2^{n'}\}$.

2. Пусть $T = 2$. Тогда по лемме 6.5 имеем

$$wt(f) = \sum_{i=0}^{n'} \binom{n'}{i} \pi_i = \pi_0 \sum_{i=0}^{\lfloor n'/2 \rfloor} \binom{n'}{2i} + \pi_1 \sum_{i=0}^{\lfloor (n'-1)/2 \rfloor} \binom{n'}{1+2i} =$$
$$= \frac{2^{n'}}{2}\pi_0 + \frac{2^{n'}}{2}\pi_1 = (\pi_0 + \pi_1)\frac{2^{n'}}{2}$$

и, следовательно, в этом случае $wt(f) \in \{0, 2^{n'}/2, 2^{n'}\}$.

3. Пусть $T = 3$. По лемме 6.5, учитывая, что $r_1 = 1$, имеем

$$wt(f) = \sum_{i=0}^{n'} \binom{n'}{i} \pi_i = \pi_0 \sum_{i=0}^{\lfloor n'/3 \rfloor} \binom{n'}{3i} + \pi_1 \sum_{i=0}^{\lfloor (n'-1)/3 \rfloor} \binom{n'}{1+3i} +$$
$$+ \pi_2 \sum_{i=0}^{\lfloor (n'-2)/3 \rfloor} \binom{n'}{2+3i} = \left(\frac{2^{n'}}{3} + \frac{2}{3}\cos\frac{\pi n'}{3}\right)\pi_0 +$$
$$+ \left(\frac{2^{n'}}{3} + \frac{2}{3}\cos\frac{\pi(n'-2)}{3}\right)\pi_1 +$$
$$+ \left(\frac{2^{n'}}{3} + \frac{2}{3}\cos\frac{\pi(n'-4)}{3}\right)\pi_2 = \frac{2^{n'}}{3}(\pi_0 + \pi_1 + \pi_2) +$$
$$+ \frac{2}{3}\left(\pi_0 \cos\frac{\pi n'}{3} + \pi_1 \cos\frac{\pi(n'-2)}{3} + \pi_2 \cos\frac{\pi(n'-4)}{3}\right).$$

Из того, что $\cos\frac{\pi n'}{3} + \cos\frac{\pi(n'-2)}{3} + \cos\frac{\pi(n'-4)}{3} = 0$, заключаем, что $\left|\pi_0 \cos\frac{\pi n'}{3} + \pi_1 \cos\frac{\pi(n'-2)}{3} + \pi_2 \cos\frac{\pi(n'-4)}{3}\right| \le 1$. Отсюда получаем неравенства

$$\left\lfloor \frac{2^{n'}(\pi_0 + \pi_1 + \pi_2)}{3} \right\rfloor \le wt(f) \le \left\lceil \frac{2^{n'}(\pi_0 + \pi_1 + \pi_2)}{3} \right\rceil.$$

Следовательно, в этом случае $wt(f) \in \{0, \lfloor 2^{n'}/3 \rfloor, \lceil 2^{n'}/3 \rceil, \lfloor 2^{n'+1}/3 \rfloor, \lceil 2^{n'+1}/3 \rceil, 2^{n'}\}$.

Все случаи рассмотрены. Лемма 6.12 доказана. □

Лемма 6.13. *Для любого натурального l и любого положительного ε существует такое натуральное N, что для любого натурального n, не меньшего N, и для любой l-уравновешенной булевой функции f от n переменных имеет место одно из следующих пяти неравенств:*

$$\rho(f) < \varepsilon;$$
$$|\rho(f) - 1/3| < \varepsilon;$$
$$|\rho(f) - 1/2| < \varepsilon;$$
$$|\rho(f) - 2/3| < \varepsilon;$$
$$\rho(f) > 1 - \varepsilon.$$

Доказательство. По леммам 6.11 и 6.12 для любых натуральных l и n' существует такое натуральное N, что у любой l-уравновешенной булевой функции f от N переменных найдется симметрическая периодическая подфункция f' от n' переменных, вес которой $wt(f')$ принадлежит множеству $\{0, \lfloor 2^{n'}/3 \rfloor, \lceil 2^{n'}/3 \rceil, 2^{n'}/2, \lfloor 2^{n'+1}/3 \rfloor, \lceil 2^{n'+1}/3 \rceil, 2^{n'}\}$. Тогда из свойства l-уравновешенности следует, что веса всех n-местных подфункций f'' функции f должны одновременно удовлетворять одному из неравенств

$$wt(f'') < l + 1;$$
$$\left|wt(f'') - 2^{n'}/3\right| < l + 1;$$
$$\left|wt(f'') - 2^{n'-1}\right| < l + 1;$$
$$\left|wt(f'') - 2^{n'+1}/3\right| < l + 1;$$
$$wt(f'') > 2^{n'} - (l + 1).$$

Положим $n' = \left\lceil \log_2 \frac{l+1}{\varepsilon} \right\rceil$ и разделим обе части каждого из пяти неравенств на $2^{n'}$. Учитывая, что $\min\limits_{f''} \rho(f'') \le \rho(f) \le \max\limits_{f''} \rho(f'')$, получим заключение леммы 6.13.

Доказательство теоремы 6.5 непосредственно следует из лемм 6.2 и 6.13.

□

Следствие 6.2. *Пусть $F = \{f_k\}$, $k = 1, 2, \ldots$ — последовательность различных l-уравновешенных булевых функций для некоторого заданного l, причем число переменных, от которых зависят функции этой последовательности, не убывает. Тогда множество предельных значений плотности функций из последовательности F содержится во множестве* $\{0,\ 1/3,\ 1/2,\ 2/3,\ 1\}$.

Следствие 6.3. *Пусть $F = \{f_k\}$, $k = 1, 2, \ldots$ — последовательность булевых функций , причем число переменных, от которых зависят функции этой*

последовательности, не убывает и стремится к бесконечности. Пусть множество предельных значений плотности функций из последовательности F не пересекается со множеством $\{1/3, 1/2, 2/3\}$ и пусть веса функций из последовательности F и их отрицаний стремятся к бесконечности. Тогда для любого натурального l найдется такое натуральное $k(l)$, что все функции из последовательности F, начиная с $f_{k(l)}$, не являются l-уравновешенными.

Результат теоремы 6.5 был обобщен автором в работах [153] и [154] для k-значных функций, заданных на булевом кубе, т. е. для функций из $P^n_{2,k}$. Пусть $f(x_1, x_2, \ldots, x_n)$ — это функция из $\{0,1\}^n$ в $\{0, 1, \ldots, k-1\}$. Мы говорим, что сумма $\sum\limits_{\alpha} f(\alpha)$ по всем n-местным двоичным наборам α называется *весом* функции f и обозначается через $wt(f)$. Величина $\rho(f) = wt(f)/2^n$ называется *плотностью* n-местной функции f. Функция f', полученная из f подстановкой констант 0 и 1 вместо некоторых переменных называется *подфункцией* f. Будем говорить, что функция f называется *l-уравновешенной,* если $|wt(f_1) - wt(f_2)| \leq l$ для любых двух ее подфункций f_1 и f_2 от одинакового числа аргументов.

В статьях автора [153] и [154] описано множество всех возможных предельных значений плотности l-уравновешенных k-значных функций n-местных функций при n, стремящемся к бесконечности. Это обобщает результаты [129]. Более точно, доказано, что множество всех возможных предельных значений плотности l-уравновешенных n-местных функций при n, стремящемся к бесконечности, есть

$$\begin{cases} \{0, i, k-1\}, & \text{если } l = 0, \\ \{0, \frac{1}{3}, \frac{1}{2}, i - \frac{1}{3}, i, i + \frac{1}{3}, i + \frac{1}{2}, k - 1 - \frac{1}{3}, k - 1\}, & \text{если } l = 1, \\ \{0, \frac{1}{3}, \frac{1}{2}, i - \frac{1}{3}, i - \frac{1}{6}, i, i + \frac{1}{6}, i + \frac{1}{3}, i + \frac{1}{2}, k - 1 - \frac{1}{3}, k - 1\}, & \text{если } l \geq 2, \end{cases}$$

$i = 1, 2, \ldots, k-2$.

Для любого возможного предельного значения построена последовательность 1-уравновешенных функций (или 2-уравновешенных функций, если в знаменателе стоит 6), плотность которых стремится к этому значению.

Доказательство этого утверждения почти полностью аналогично доказательству теоремы 6.5. Нельзя лишь перенести доказательство леммы 6.7, потому что, к примеру, симметрическая периодическая булева функция с периодом $T = 6$, задаваемая характеристическим отрезком $\pi[6] = (i, i, i, i - 1, i + 1, i - 1)$, $i \in \{1, \ldots, k - 2\}$, удовлетворяет всем требованиям и является 2-уравновешенной. Поэтому в качестве предельного значения плотности l-уравновешенных (при $l \geq 2$) функций из $P^n_{2,k}$ достигается любая дробь между 0 и $k - 1$ со знаменателем 6, кроме $\frac{1}{6}$ и $\frac{6k-7}{6}$.

6.3 О классе булевых функций, равномерно распределенных по шарам со степенью 1

Во многих разделах математики и ее приложениях, например, в теории кодирования, криптографии и пр., важной задачей является изучение классов булевых функций, единичные значения которых равномерно распределены по некоторым однотипным подмножествам булева куба.

Булевы функции, единичные значения которых равномерно или почти равномерно распределены по подкубам (а также характеристические коды таких функций и массивы, в строках которых записаны наборы, на которых функция принимает единичные значения) интенсивно изучались в различных разделах математики и ее приложений. Такие структуры известны как коды с большим дуальным расстоянием, корреляционно-иммунные, устойчивые и ε-отклоненные булевы функции, ортогональные массивы и т. д. Такие структуры важны в статистике для планирования экспериментов, в криптографии для сокрытия секретов и для порождения псевдослучайных последовательностей. Равномерное распределение единичных значений булевых функций по шарам ранее не изучалось интенсивно (мы можем упомянуть только работу автора [130], хотя представляется, что булевы функции, единичные значения которых равномерно распределены по шарам, могут иметь разнообразные полезные приложения, например, когда булева функция играет роль хеширующей функции, или когда желательно, чтобы при использовании характеристического кода этой функции все возможные слова на выходе канала связи имели бы приблизительно одинаковое количество способов подходящего декодирования. Такие булевы функции имеют в качестве комбинирующих функций в потоковых шифрах хорошую устойчивость против статистических атак, когда противник имеет возможность изменять некоторое (ограниченное) число входов функции, поэтому доказательство несуществования таких функций в некоторых случаях (для некоторых значений параметров) доказывает и то, что упомянутые статистические атаки в таких случаях могут иметь гарантированный успех.

В работах [21], [128] и [129] рассматривались классы l-уравновешенных буле-

вых функций, единичные значения которых равномерно распределены по подкубам одинаковой размерности (этим функциям посвящен параграф 6.2. В [21] был полностью описан класс 1-уравновешенных функций, определена мощность этого класса и доказано, что любую 1-уравновешенную функцию можно реализовать схемой из функциональных элементов с линейной относительно числа переменных сложностью. В данном параграфе аналогичные задачи ставятся и решаются для класса функций, равномерно распределенных по шарам со степенью 1, в частности, полностью описан класс функций, равномерно распределенных по шарам со степенью 1 и найдено их число. В качестве возможного объяснения того, почему подобной задачей не занимались ранее, можно отметить, что полученный результат является достаточно неожиданным, а используемая техника — неочевидной. Действительно, равномерно распределить наборы по шарам какого-го одного радиуса возможно. Так, несложно видеть, что характеристическая функция совершенного кода с кодовым расстоянием 3 (например, кода Хэмминга) и функция $f(x_1, \ldots, x_{2n+1}) = \bigoplus_{i=1}^{n+1} x_i$ абсолютно равномерно распределены по шарам радиуса 1; функция от нечетного числа переменных n, которая принимает одинаковые значения на противоположных наборах, абсолютно равномерно распределена по шарам радиуса $\frac{n-1}{2}$. Однако оказывается, что равномерно распределить единичные значения по шарам разных радиусов (даже не абсолютно, а приблизительно) во многих случаях оказывается уже невозможно.

Результаты этого параграфа опубликованы в работе автора [130].

Наборы, на которых функция принимает значение 1 в этом параграфе будем называть 1-наборами.

Шаром радиуса r с центром α будем называть множество наборов, отстоящих от α на расстояние, не большее r. Весом функции f на шаре (или для краткости просто весом шара) будем называть число 1-наборов функции f, принадлежащих этому шару. Шар радиуса r веса m будем для краткости называть (r, m)-шаром. Шар радиуса r веса не меньше m будем называть $(r, m)^*$-шаром.

Пусть l — целое неотрицательное число. Булеву функцию $f(x_1, x_2, \ldots, x_n)$ будем называть *равномерно распределенной по шарам со степенью l (l-РРШ*

функцией), если модуль разности весов любых двух шаров одинакового радиуса не превосходит l.

Очевидно, 0-РРШ функциями являются только константы. В этом параграфе рассматривается случай $l = 1$.

Если булева функция f является l-РРШ функцией, то очевидно, что $\overline{f}$ также есть l-РРШ функция. Поэтому достаточно рассматривать только такие функции f, для которых $wt(f) \leq 2^{n-1}$.

Теорема 6.6. *Если n-местная булева функция f с весом $wt(f) \leq 2^{n-1}$ является 1-РРШ функцией, то имеет место хотя бы один из следующих трех случаев:*

$$1)\ wt(f) \leq 2;$$
$$2)\ n \leq 4;$$
$$3)\ n = 6, wt(f) = 4.$$

Для доказательства теоремы 6.6 будет показано, что не существует n-местных 1-РРШ функций f для каждого из случаев I–IV):

$$I)\ wt(f) = 3, n \geq 4;$$
$$II)\ 3 < wt(f) < \frac{2^{n+1}}{\sum\limits_{i=0}^{4}\binom{n}{i}};$$
$$III)\ \frac{2^{n+1}}{\sum\limits_{i=0}^{4}\binom{n}{i}} \leq wt(f) < \frac{2^{n+2}}{n^2}, n \geq 7;$$
$$III')\ wt(f) = 5, n = 6;$$
$$IV)\ \frac{2^{n+2}}{n^2} \leq wt(f) \leq 2^{n-1}, n \geq 5.$$

Нетрудно видеть, что случаи I–IV покрывают все множество пар n и $wt(f)$, $wt(f) \leq 2^{n-1}$, не перечисленных в теореме 6.6.

Введем некоторые вспомогательные обозначения. Через S_f^r обозначим сумму весов всех 2^n шаров радиуса r. Каждый набор входит в точности в $\sum\limits_{i=0}^{r}\binom{n}{i}$ шаров радиуса r, поэтому $S_f^r = wt(f)\sum\limits_{i=0}^{r}\binom{n}{i}$. Через R_f^r обозначим величину $\frac{S_f^r}{2^n}$. Величина R_f^r есть средний вес шара радиуса r, поэтому если f является 1-РРШ функцией, то вес любого шара радиуса r равен либо $\lfloor R_f^r \rfloor$, либо $\lceil R_f^r \rceil$. Величину $\lfloor R_f^1 \rfloor$ будем для краткости обозначать просто R.

Докажем сначала две технические леммы.

Лемма 6.14. *При $n \geq 4k+2, k \geq 2$, выполняется неравенство*

$$\sum_{i=0}^{2k} \binom{n}{i} > 2 \sum_{i=0}^{k+1} \binom{n}{i}.$$

Доказательство леммы проведем индукцией по k. Сначала рассмотрим случай $k = 2$.

Имеем

$$\sum_{i=0}^{4} \binom{n}{i} = \frac{n^4 - 2n^3 + 11n^2 + 14n + 24}{24}, \qquad \sum_{i=0}^{3} \binom{n}{i} = \frac{n^3 + 5n + 6}{6}.$$

Разность левой и правой частей устанавливаемого неравенства будет равна

$$\sum_{i=0}^{4} \binom{n}{i} - 2 \sum_{i=0}^{3} \binom{n}{i} = \frac{1}{24}(n^4 - 10n^3 + 11n^2 - 26n - 24) > 0 \text{ при } n \geq 10.$$

Пусть теперь утверждение леммы справедливо для $k-1$. Тогда имеем

$$\sum_{i=0}^{2k} \binom{n}{i} - 2 \sum_{i=0}^{k+1} \binom{n}{i} = \sum_{i=0}^{2(k-1)} \binom{n}{i} - 2 \sum_{i=0}^{k} \binom{n}{i} + \\ + \binom{n}{2k-1} + \binom{n}{2k} - 2 \binom{n}{k+1} > \binom{n+1}{2k} - \binom{n+1}{k+2}.$$

Последнее выражение больше 0, поскольку $k > 2$ и $n + 1 > 4k$. Лемма 6.14 доказана.

Следствие 6.4. *При $n \geq 4k+2, k \geq 2$, для любой n-местной функции f, не равной тождественно 0, выполняется неравенство $R_f^{2k} > 2R_f^{k+1}$.*

Лемма 6.15. *а) При натуральных n и m, удовлетворяющих условиям $n \geq 7$, $\frac{2^{n+1}}{n^2+n+2} \leq m \leq \frac{2^{n+2}}{n^2+n+2}$, справедливо неравенство*

$$3m \left(\left\lfloor \frac{(n^4 - 2n^3 + 11n^2 + 14n + 24)m}{24 \cdot 2^n} \right\rfloor - 1 \right) > \frac{n^2+n+2}{2} m - 2^n.$$

б) При натуральных n и m, удовлетворяющих условиям $n \geq 5$, $\frac{2^{n+2}}{n^2+n+2} \leq m \leq 2^{n-1}$, справедливо неравенство

$$m \left(\left\lfloor \frac{(n^2+n+2)m}{2^{n+1}} \right\rfloor - 1 \right) > \left\lfloor \frac{(n+1)m}{2^n} \right\rfloor \left((n+1)m - 2^{n-1} \left(\left\lfloor \frac{(n+1)m}{2^n} \right\rfloor + 1 \right) \right).$$

Доказательство. Во избежание громоздких выкладок установим выполнение неравенств лишь при $n \geq 16$. Справедливость утверждений при $n \leq 15$ легко проверить на компьютере перебором всех допустимых пар n и m.

а) Положим $m = \rho\frac{2^{n+1}}{n^2+n+2}$, где $1 \leq \rho \leq 2$. Разделим обе части неравенства на $3m$ и вычтем из левой части правую. Имеем

$$\begin{gathered}
\left\lfloor \frac{(n^4-2n^3+11n^2+14n+24)m}{24\cdot 2^n} \right\rfloor - 1 - \frac{n^2+n+2}{6} + \frac{2^n}{3m} \geq \\
\geq \frac{\rho((n^2+n+2)(n^2-3n+12)+8n)}{12(n^2+n+2)} - 2 - \frac{n^2+n+2}{6} + \frac{n^2+n+2}{6\rho} \geq \\
\geq \frac{\rho}{12}(n^2-3n+12) - 2 - \left(\frac{n^2+n+2}{6}\right)\left(1-\frac{1}{\rho}\right) = \\
= \frac{n^2}{12\rho}(\rho^2-2\rho+2) + n\left(-\frac{\rho}{4}-\frac{1}{6}+\frac{1}{6\rho}\right) + \left(\rho-2-\frac{1}{3}+\frac{1}{3\rho}\right) \geq \\
\geq \frac{n^2}{12\rho}((\rho-1)^2+1) + n\left(-\frac{1}{2}-\frac{1}{6}+\frac{1}{12}\right) + \left(1-2-\frac{1}{3}+\frac{1}{6}\right) \geq \\
\geq \frac{1}{24}(n^2-14n-28) > 0 \quad \text{при} \quad n \geq 16.
\end{gathered}$$

б) Если $\frac{2^{n+2}}{n^2+n+2} \leq m < \frac{2^n}{n+1}$, то левая часть неравенства, очевидно, больше 0, а правая часть равна 0. Пусть $m \geq \frac{2^n}{n+1}$ и $\left\lfloor \frac{(n+1)m}{2^n} \right\rfloor = h$, $1 \leq h \leq \frac{n+1}{2}$. Положим $m = \rho\frac{2^n}{n+1}$, где $h \leq \rho < h+1$. Разделим обе части неравенства на m и вычтем из левой части правую. Имеем

$$\begin{gathered}
\left\lfloor \frac{(n^2+n+2)m}{2^{n+1}} \right\rfloor - 1 - h\left((n+1) - \frac{2^{n-1}(h+1)}{m}\right) \geq \\
\geq \frac{\rho}{2}\cdot\frac{n(n+1)+2}{n+1} - 2 - h(n+1) + \frac{h(h+1)}{2\rho}(n+1) \geq \\
\geq \frac{\rho n}{2} - 2 - h(n+1) + \frac{h(h+1)}{2\rho}(n+1) = \\
= \frac{n}{2\rho}(\rho^2 - 2\rho h + h^2 + h) + \left(-2 - h + \frac{h(h+1)}{2\rho}\right) \geq \\
\geq \frac{n}{2(h+1)}\left((\rho-h)^2+h\right)\big) - \left(2+\frac{h}{2}\right) \geq \frac{nh}{2(h+1)} - \left(2+\frac{h}{2}\right).
\end{gathered}$$

Последнее выражение при $h \leq 3$ не меньше чем $\frac{n}{4} - \frac{7}{2} = \frac{1}{4}(n-14) > 0$ при $n \geq 15$, а при $h > 3$ оно не меньше чем $\frac{2n}{5} - \frac{9}{4} - \frac{n}{4} \geq \frac{3}{20}(n-15) > 0$ при $n \geq 16$.

Лемма 6.15 доказана.

Рассмотрим теперь последовательно случаи I–IV.

Лемма 6.16. *При $n \geq 4$ не существует n-местных 1-РРШ функций f с весом $wt(f) = 3$.*

Доказательство. Пусть такая функция f существует, и пусть α^1, α^2 и α^3 — все три 1-набора функции f. Обозначим через n_0 число разрядов, в которых все

три набора α^i, $i = 1, 2, 3$, совпадают, через n_{ij}, $1 \le i < j \le 3$, обозначим число разрядов, в которых наборы α^i и α^j совпадают и отличаются от третьего 1-набора. Обозначим $H = \max\{n_{12}, n_{13}, n_{23}\}$, $h = n - H$. Очевидно, что найдутся два 1-набора, расстояние между которыми не больше чем h, и, следовательно, существует $\left(\lceil \frac{h}{2} \rceil, 2\right)^*$-шар. Рассмотрим теперь набор γ, отличающийся в каждом разряде по крайней мере от двух из наборов α^i, $i = 1, 2, 3$. Ясно, что расстояние от набора γ до каждого из 1-наборов не меньше h и, таким образом, существует $(h-1, 0)$-шар. Для того, чтобы f была 1-РРШ функцией необходимо, чтобы выполнялось неравенство $h - 1 < \lceil \frac{h}{2} \rceil$. Однако это возможно только если $h \le 1$. Однако тогда существует $(1, 2)^*$-шар. В то же время при $n \ge 4$, $wt(f) = 3$ справедливо неравенство $R_f^1 < 1$, поэтому найдется $(1, 0)$-шар. Полученное противоречие доказывает лемму 6.16.

Лемма 6.17. *Не существует n-местных 1-РРШ функций f при $3 < wt(f) < \frac{2^{n+1}}{\sum\limits_{i=0}^{4} \binom{n}{i}}$.*

Доказательство леммы проведем от противного. Пусть функция f с таким весом найдется. Тогда покажем по индукции, что для любого k, $k \ge 3$, найдется $(k, 0)$-шар. Заметим, что при $n \le 9$ выполняется неравенство $\frac{2^{n+1}}{\sum\limits_{i=0}^{4} \binom{n}{i}} \le 4$. Таким образом, достаточно ограничиться случаем $n \ge 10$. Из условия леммы 6.17 следует, что $R_f^4 < 2$. По следствию из леммы 6.14 при $n \ge 10$, $wt(f) > 0$ имеем $R_f^4 > 2R_f^3$. Поэтому $R_f^3 < 1$ и, следовательно, найдется $(3, 0)$-шар. Основание индукции доказано.

Покажем теперь, что если существует $(k, 0)$-шар, $k \ge 3$, то найдется и $(k+1, 0)$-шар. В самом деле, в любом шаре радиуса k содержится не более одного 1-набора. Следовательно, расстояние между любыми двумя 1-наборами больше чем $2k$. Поэтому шар радиуса $2k$ с центром в 1-наборе α имеет вес 1 и, таким образом, $R_f^{2k} < 2$. Рассмотрим шар радиуса $2k$ с центром в наборе $\overline{\alpha}$. Его вес не больше чем 2. Если $n \le 4k + 1$, то эти два шара покрывают весь булев куб и тогда $wt(f) \le 3$, что неверно по предположению леммы. Следовательно, достаточно ограничиться случаем $n \ge 4k + 2$. Однако тогда по следствию из леммы 6.14 имеем $R_f^{k+1} < R_f^{2k}/2 < 1$ и, таким образом, существует $(k+1, 0)$-

шар.

Однако если положить $k = n$, то по доказанному имеем $wt(f) = 0$. Полученное противоречие доказывает лемму 6.17.

Лемма 6.18. *При $n \geq 7$ не существует n-местных 1-РРШ функций f с весом, удовлетворяющим неравенствам $\frac{2^{n+1}}{\sum_{i=0}^{4}\binom{n}{i}} \leq wt(f) < \frac{2^{n+2}}{n^2+n+2}$. Случай $n = 6$, $wt(f) = 5$ также невозможен.*

Доказательство. Пусть такая функция f существует.

а) Если $wt(f) < \frac{2^{n+1}}{n^2+n+2}$, то $R_f^2 < 1$, поэтому существует $(2,0)$-шар, но тогда не существует $(2,2)^*$-шара, следовательно, расстояние между любыми двумя 1-наборами не меньше чем 5. Поэтому любой шар радиуса 4 с центром в 1-наборе имеет вес 1. Однако по условию леммы 6.18 имеем $R_f^4 \geq 2$. Следовательно, случай а) невозможен.

б) Пусть $\frac{2^{n+1}}{n^2+n+2} \leq wt(f) < \frac{2^{n+2}}{n^2+n+2}$. Тогда $1 \leq R_f^2 < 2$ и существует в точности $S_f^2 - 2^n$ штук $(2,2)$-шаров, остальные шары радиуса 2 имеют вес 1.

Для каждого 1-набора найдется по крайней мере $\lfloor R_f^4 \rfloor - 1$ различных 1-наборов, находящихся от него на расстоянии, не большем чем 4. В то же время $R_f^1 = \frac{wt(f)(n+1)}{2^n} < \frac{4}{n} < 1$ при $n \geq 6$, поэтому расстояние между любыми двумя 1-наборами не меньше чем 3. Следовательно, для каждой пары 1-наборов, расстояние между которыми не больше чем 4, найдутся в точности шесть шаров радиуса 2, содержащих оба эти 1-набора. Ушестеренное число пар 1-наборов, расстояние между которыми не больше чем 4, не меньше чем $N_1 = 3wt(f)(\lfloor R_f^4 \rfloor - 1)$.

С другой стороны, в точности $N_2 = S_f^2 - 2^n$ шаров радиуса 2 содержат ровно одну пару 1-наборов, расстояние между которыми не больше чем 4, остальные шары радиуса 2 таких пар не содержат. Следовательно, ушестеренное число пар 1-наборов, расстояние между которыми не больше чем 4, в точности равно N_2. Однако по лемме 6.15, п. а) при $n \geq 7$ и $m = wt(f)$ выполнено неравенство $N_1 > N_2$, что немедленно дает противоречие. Таким образом, случай III невозможен.

Если же $n = 6$, $wt(f) = 5$, то имеем $N_2 = S_f^2 - 2^n = 46$. Однако 46 не делится на 6. Это показывает, что случай III' также невозможен. Лемма 6.18 доказана.

Лемма 6.19. *При $n \geq 5$ не существует n-местных 1-РРШ функций f с весом, удовлетворяющим неравенствам $\frac{2^{n+2}}{n^2+n+2} \leq wt(f) \leq 2^{n-1}$.*

Доказательство. Пусть такая функция f существует. Для каждого 1-набора найдется по крайней мере $\lfloor R_f^2 \rfloor - 1$ различных 1-наборов, находящихся от него на расстоянии, не большем чем 2. Для каждой пары 1-наборов, расстояние между которыми не больше чем 2, найдутся в точности два шара радиуса 1, содержащих оба эти 1-набора. Удвоенное число пар 1-наборов, расстояние между которыми не больше чем 2, не меньше чем $N_1 = wt(f)(\lfloor R_f^2 \rfloor - 1)$.

С другой стороны, каждый шар радиуса 1 содержит в точности $\frac{R(R-1)}{2}$ пар 1-наборов, расстояние между которыми не больше чем 2, за исключением $S_f^1 - 2^n \cdot R$ шаров, которые содержат ровно $\frac{R(R+1)}{2}$ пар таких наборов. Следовательно, удвоенное число пар 1-наборов, расстояние между которыми не больше чем 2, равно в точности

$$N_2 = 2^n \frac{R(R-1)}{2} + (S_f^1 - 2^n \cdot R)R = R(S_f^1 - 2^{n-1}(R+1)).$$

Однако по лемме 6.15, п. б) при $n \geq 5$ и $m = wt(f)$ выполнено неравенство $N_1 > N_2$, что немедленно дает доказывающее лемму 6.19 противоречие.

Последовательное рассмотрение случаев I–IV закончено. Теорема 6.6 доказана.

Очевидно, что все булевы функции с весом 0 или 1 являются 1-РРШ функциями. Если же $wt(f) = 2$, то легко видеть, что f является 1-РРШ функцией тогда и только тогда, когда расстояние между ее 1-наборами равно n, если n нечетно, и не меньше чем $n-1$, если n четно.

Все 1-РРШ функции при $n \leq 4$ и при $n = 6$, $wt(f) = 4$ легко перечислить на компьютере. Таким образом можно установить справедливость следующей теоремы.

Теорема 6.7. *Число* 1-*РРШ функций от* n *переменных равно*

$$\begin{cases} 2^{2^n} & \textit{при } n \le 2, \\ 80 & \textit{при } n = 3, \\ 334 & \textit{при } n = 4, \\ 2818 & \textit{при } n = 6, \\ 3 \cdot 2^n + 2 & \textit{при } n \ge 5, n \textit{ нечетно}, \\ (n+3)2^n + 2 & \textit{при } n \ge 8, n \textit{ четно}. \end{cases}$$

Теорема 6.6 позволяет установить следующий результат.

Теорема 6.8. *Множество* 1-*РРШ функций от* n *переменных реализуется схемами из функциональных элементов в базисе* $\{\&, \vee, \neg\}$ *с линейной относительно числа переменных сложностью.*

По мотивам исследований этого параграфа была составлена следующая задача повышенной трудности (почти никто из студентов старших курсов, которым она предлагалась, не сумел решить ее без многочисленных подсказок), опубликованная в [152], которая хорошо характеризует различные аспекты рассматриваемой тематики. Задача представляет самостоятельное научное значение.

Задача 6.1. Пусть A — некоторое множество двоичных наборов длины 6. Известно, что шар радиуса 2 с центром в любом наборе содержит ровно 1 или 2 набора из A. Найти мощность множества A.

Решение. Назовем число наборов из множества A, содержащихся в некотором шаре, весом этого шара. Обозначим через N число шаров радиуса 2 с весом 2. Рассмотрим сумму весов всех $2^6 = 64$ шаров радиуса 2. Эта сумма, очевидно, равна $64 + N$. С другой стороны, каждый набор из A дает в эту сумму вклад, равный объему шара радиуса 2, т. е. равный $\sum\limits_{i=0}^{2} \binom{6}{i} = 22$. Поэтому $64 + N = 22|A|$. Из неравенств $0 \le N \le 64$ следует, что возможны только следующие три случая: 1) $N = 2$, $|A| = 3$; 2) $N = 24$, $|A| = 4$; 3) $N = 46$, $|A| = 5$.

Рассмотрим два набора α и β из множества A, содержащиеся в некотором шаре радиуса 2. Очевидно, что число шаров, одновременно содержащих α и β зависит от $\rho(\alpha, \beta)$. Геометрическое рассмотрение показывает, что это число равно 12, если $\rho(\alpha, \beta)$ есть 1 или 2, и равно 6, если $\rho(\alpha, \beta)$ есть 3 или 4. Таким образом, число N должно делиться на 6, что оставляет возможным только случай $N = 24$, $|A| = 4$.

Осталось только убедиться, что случай $|A| = 4$ действительно реализуем. В качестве примера рассмотрим множество $A = \{(000000), (000111), (111000), (111111)\}$. Легко убедиться, что условия задачи для множества A выполнены. Таким образом, $|A| = 4$. □

В работе [32] ученицы автора М. С. Ярыкиной доказано, что при фиксированном натуральном l, начиная с некоторого достаточно большого n, не существует l-РРШ функций f веса $wt(f)$, где $2l < wt(f) < 2^n - 2l$.

7 О критериях бесконечности инвариантных классов дискретных функций

Инвариантные классы булевых функций были введены С. В. Яблонским в [30], но более известна его последующая работа [31]. В этой главе рассматриваются не только инвариантные классы булевых функций, но и классы функций, заданных на двоичных наборах и принимающих k значений. Булевы функции из инвариантных классов не являются, вообще говоря, функциями с равномерно распределенными единичными значениями. Достаточно упомянуть класс монотонных функций — у них все единичные значения вверху, а все нулевые значения — внизу, какое уж тут равномерное распределение. Однако тем не менее многие (хотя, конечно, не все) рассматриваемые в предыдущих главах работы классы функций с равномерно распределенными единичными значениями являются инвариантными. Так, инвариантными являются класс $(n-k)$-устойчивых функций от n переменных (для заданного k) и класс l-уравновешенных функций (для заданного l). Тут, впрочем, надо сделать оговорку, что эти классы не являются инвариантными по классическому определению С. В. Яблонского, потому что они не замкнуты относительно добавления фиктивных переменных. Поэтому надо или делать оговорку о том, что включаем вместе с функцией в класс все функции, получающиеся из нее добавлением фиктивной переменной, или просто исключить такое добавление из определения инвариантного класса. Этим главным образом и объясняется то, что наряду с классическим определением инвариантного класса по С. В. Яблонскому, в этой главе рассматриваются и неклассические определения инвариантного класса, в которых операция добавления несущественной переменной не учитывается.

Помимо того, что некоторые классы функций с равномерно распределенными единичными значениями являются инвариантными, важна также и общ-

ность методов и подходов. Так во многих рассуждениях предыдущих глав являлось важным, что если перейти от функции к ее подфункции, подставив, например, вместо переменной константу, или удалив линейную переменную из ее полинома, то снова получится функция из того же класса. Этим и вызван интерес к инвариантным классам в данной работе, для которой, таким образом, инвариантные классы являются идейно близким объектом.

В этой главе предлагается критерий, позволяющий по системе запрещенных подфункций, задающих инвариантный класс, определить, содержит ли этот класс бесконечное число существенно разных функций. Критерий сводит рассматриваемую задачу для функций к соответствующей задаче для множеств слов. Задание инвариантных классов через множества запрещенных подфункций использовалось уже при введении инвариантных классов С. В. Яблонским, однако до работы автора [146] такой критерий предложен не был. Далее проводится изучение минимальных бесконечных инвариантных классов функций, т. е. таких классов, что при добавлении к множеству запрещенных функций любой функции из класса класс перестает быть бесконечным. Будет предложено описание всех минимальных бесконечных инвариантных классов и доказано, что число таких классов — континуум.

С. В. Яблонский в своей основополагающей работах [30] и [31] при исследовании алгоритмических трудностей синтеза минимальных контактных схем ввел понятие инвариантного класса. Слово «инвариантный» здесь подразумевало замкнутость класса функций относительно операций подстановки константы вместо переменной, переименования переменных без отождествления, а также удаления и добавления несущественных переменных. Как отмечалось в [31], инвариантные классы представляют собой «достаточно мощное семейство классов, содержащее, повидимому, все классы, возникающие в практике синтеза схем». В [31] детально исследованы различные способы задания инвариантных классов, оценена мощность как множества всех инвариантных классов, так и различных его подклассов, для так называемых *ненулевых* инвариантных классов найдена асимптотика реализации функций из этих классов контактными схемами. Фигурирующие при определении в [30] и [31] инвариантного класса операции подстановки константы вместо переменной, переименования перемен-

ных без отождествления и удаления и добавления несущественных переменных часто относят к классу так называемых *унарных* операций, имея в виду, что они применяются к *одной* функции (недетерминированным образом) в отличие, например, от операции суперпозиции, которая применяется одновременно к *нескольким* функциям. В связи с этим естественными выглядят попытки обобщений понятия инвариантного класса на другие наборы унарных операций. С. В. Яблонский поддерживал такие исследования, являясь, например, научным руководителем диссертационной работы [15]. Целесообразность таких обобщений с точки зрения приложений к синтезу схем вызывалась тем, что инвариантные классы в их классическом определении [30], [31] являлись слишком общим объектом, что не давало возможности учета конкретной специфики важных на практике классов. Кроме того, наиболее важными на практике оказывались функции из как раз *нулевых* инвариантных классов, для которых требовалась более детальная классификация. Обобщения инвариантных классов исследовались в работах [10], [14], [15], где в качестве дополнительных операций рассматривались отождествление переменных и подстановка вместо переменной функции от одной переменной. Вместе с тем, в некоторых случаях, не связанных с синтезом схем, представляет интерес и отказ при определении инвариантного класса от некоторых из трех основополагающих операций, в частности, от операции добавления несущественных переменных. Если с точки зрения синтеза схем функции, различающиеся лишь множествами несущественных переменных, могут считаться абсолютно идентичными, поскольку реализуются одной и той же схемой, то в ситуациях, когда нам важна геометрическая структура функции, ее подфункции от разного числа переменных естественно считать различными, даже если они различаются лишь множествами несущественных переменных. Тогда если нас интересует класс функций, не содержащий «запрещенных» подфункций, то требования к этому классу будут, вообще говоря, менее жесткими, чем требования к инвариантному классу в его классическом определении [30], [31], потому что в число запрещенных функций может входить функция, имеющая фиктивные переменные, в то время как функция, полученная из нее удалением этих фиктивных переменных, вполне может быть для нас допустима. Поэтому в этой главе наряду с классическим определени-

ем инвариантного класса будут также рассматриваться два альтернативных (неэквивалентных) определения инвариантного класса, соответствующие «геометрическому» взгляду на функцию. Заметим, что некоторые из полученных в этой главе результатов формулируются для «геометрических» инвариантных классов чуть более просто, чем для классических, и поэтому «геометрические» инвариантные классы могут рассматриваться как промежуточное звено при получении соответствующих результатов для классических инвариантных классов Яблонского.

Далее эта глава организована следующим образом. В параграфе 7.1 даются предварительные определения и понятия, включая три альтернативных неэквивалентных определения инвариантного класса. В параграфе 7.2 приводятся краткие сведения из теории слов, избегающих запреты. Параграф 7.3 посвящен задаче определения по множеству запрещенных подфункций G, является ли заданный множеством G инвариантный класс бесконечным. Дается критерий, позволяющий для функций из класса $P_{2,k}$ свести эту задачу к хорошо известной задаче из теории слов. Параграф 7.4 посвящен исследованию минимальных бесконечных инвариантных классов. Для функций из множества $P_{2,k}$ предложено описание всех таких классов. Доказано, что мощность множества минимальных бесконечных инвариантных классов равна континууму. Результаты этой главы опубликованы в статье автора [146].

7.1 Общее понятие инвариантного класса и некоторые определения

Важные для изложения в этой главе определения множеств функций $P^n_{q,k}$ и P_k, а также симметрических функций в этих множествах, были даны нами в параграфе 6.1.

Пусть $f(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, x_n)$ — функция из множества $P^n_{q,k}$. Переменная x_i называется *несущественной* или *фиктивной* для функции f, если $f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, x_n) \equiv f(x_1, \ldots, x_{i-1}, j, x_{i+1}, x_n)$ для любого j, $j = 1, 2, \ldots, q-1$. Про функцию f в этом случае говорят, что f зависит от переменной x_i *несущественно* или *фиктивно*. Переменная, которая не является фиктивной, называется *существенной*. Функция, которая зависит существенно от всех своих переменных, называется *невырожденной*. Две функции f и g из $P^n_{q,k}$ называются *равными*, если множества их существенных переменных совпадают, и на любых двух наборах, различающихся, быть может, только значениями фиктивных переменных, значения функций совпадают. Часто запись $f(x_1, x_2, \ldots, x_n)$ используют не только для обозначения конкретной функции из множества $P^n_{q,k}$, но и для обозначения целого класса равных ей функций. Это, однако, во многих случаях приводит к путанице. Так, записи $f(x_1, x_2, \ldots, x_n)$ и $f(y_1, y_2, \ldots, y_n)$ приходится считать тогда обозначениями двух разных функций. В этой главе мы будем осторожными и не станем пользоваться данным соглашением.

Наборы одинаковой длины будем называть *соседними*, если они отличаются только в одной компоненте. *Соседним по i-й компоненте* для двоичного набора $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ будем называть набор $\sigma^i = (\sigma_1, \sigma_2, \ldots, \sigma_{i-1}, \sigma_i \oplus 1, \sigma_{i+1}, \ldots, \sigma_n)$.

Пусть $f(x_1, x_2, \ldots, x_n)$ — функция из $P^n_{q,k}$ и пусть $1 \le i_1 < i_2 < \cdots < i_l \le n$. Через $f^{i_1,i_2,\ldots,i_l}_{\sigma_1,\sigma_2,\ldots,\sigma_l}(x_1, x_2, \ldots, x_n)$ обозначается функция из $P^n_{q,k}$, полученная из $f(x_1, x_2, \ldots, x_n)$ подстановкой на места переменных x_{i_1}, x_{i_2}, $\ldots$, x_{i_l} соответственно констант σ_1, σ_2, $\ldots$, σ_l. Отметим, что функция $f^{i_1,i_2,\ldots,i_l}_{\sigma_1,\sigma_2,\ldots,\sigma_l}(x_1, x_2, \ldots, x_n)$ по-прежнему зависит от переменных x_1, x_2, $\ldots$, x_n, только от переменных x_{i_1},

$x_{i_2}, \ldots, x_{i_l}$ она зависит фиктивно.

Определение 7.1. *Функция* $f^{i_1,i_2,\ldots,i_l}_{\sigma_1,\sigma_2,\ldots,\sigma_l}(x_1, x_2, \ldots, x_n)$ *называется подфункцией (в главном смысле) функции* $f(x_1, x_2, \ldots, x_n)$.

Часто по разным причинам представляется более удобным рассматривать подфункцию $f^{i_1,i_2,\ldots,i_l}_{\sigma_1,\sigma_2,\ldots,\sigma_l}(x_1, x_2, \ldots, x_n)$ функции $f(x_1, x_2, \ldots, x_n)$ из $P^n_{q,k}$ не как функцию из $P^n_{q,k}$, а как функцию из $P^{n-l}_{q,k}$, произведя *удаление фиктивных переменных*, однако здесь возникает серьезная трудность. Дело в том, что в декартовом произведении $\{0, 1, \ldots, q-1\}^n$ все компоненты формально равноправны, и установленный нами линейный порядок соответствующих этим компонентам переменных $x_1, x_2, \ldots, x_n$ есть результат чистого соглашения. Если мы захотим функцию из $P^n_{q,k}$ после удаления l фиктивных переменных рассматривать как функцию из $P^{n-l}_{q,k}$, то перед нами встанет задача установления нового порядка переменных, который a priori ни из чего не следует (заметим, что такая задача перед нами не стоит, если функция f является симметрической). Чуть более естественно сохранить имевший место линейный порядок, считая, что фиктивные переменные просто «выпадают» из набора, не меняя порядка оставшихся переменных. Другой подход заключается в том, чтобы считать функции из $P^{n-l}_{q,k}$, получающиеся после любого переупорядочивания переменных, подфункциями исходной функции f. В интересах дальнейшего рассмотрения дадим два альтернативных определения.

Определение 7.2. *Функция* $g(y_1, y_2, \ldots, y_{n-l})$ *из* $P^{n-l}_{q,k}$ *называется подфункцией (в первом смысле) функции* $f(x_1, x_2, \ldots, x_n)$ *из* $P^n_{q,k}$, *если существует такое разбиение множества переменных* $\{x_1, x_2, \ldots, x_n\}$ *на два подмножества* $\{x_{i_1}, x_{i_2}, \ldots, x_{i_l}\}$, $i_1 < i_2 < \cdots < i_l$, *и* $\{x_{i'_1}, x_{i'_2}, \ldots, x_{i'_{n-l}}\}$, $i'_1 < i'_2 < \cdots < i'_{n-l}$, *что* $g(x_{i'_1}, x_{i'_2}, \ldots, x_{i'_{n-l}}) \equiv f^{i_1,i_2,\ldots,i_l}_{\sigma_1,\sigma_2,\ldots,\sigma_l}(x_1, x_2, \ldots, x_n)$.

Определение 7.3. *Функция* $g(y_1, y_2, \ldots, y_{n-l})$ *из* $P^{n-l}_{q,k}$ *называется подфункцией (во втором смысле) функции* $f(x_1, x_2, \ldots, x_n)$ *из* $P^n_{q,k}$, *если существует разбиение множества переменных* $\{x_1, x_2, \ldots, x_n\}$ *на два подмножества* $\{x_{i_1}, x_{i_2}, \ldots, x_{i_l}\}$, $i_1 < i_2 < \cdots < i_l$, *и* $\{x_{i'_1}, x_{i'_2}, \ldots, x_{i'_{n-l}}\}$, $i'_1 < i'_2 < \cdots < i'_{n-l}$, *и существует взаимно однозначное отображение* $\phi : \{i'_1, i'_2, \ldots, i'_{n-l}\} \to \{i'_1, i'_2, \ldots, i'_{n-l}\}$ *такие, что* $g(x_{\phi(i'_1)}, x_{\phi(i'_2)}, \ldots, x_{\phi(i'_{n-l})}) \equiv f^{i_1,i_2,\ldots,i_l}_{\sigma_1,\sigma_2,\ldots,\sigma_l}(x_1, x_2, \ldots, x_n)$.

Отметим, что по нашим определениям всякая подфункция в первом смысле является также подфункцией во втором смысле.

Следствие 7.1. *Нетрудно видеть, что подфункция (в первом или втором смысле) симметрической функции из $P_{q,k}$ также является симметрической функцией. Поэтому для симметрических функций понятие подфункции в первом и втором смыслах совпадают.*

Процесс перехода от функции к ее подфункции (в одном из смыслов) часто называют *подстановкой констант вместо переменной.*

Перестановкой (без отождествления) переменных функции f из $P^n_{q,k}$ называется изменение линейного порядка следования компонент декартова произведения $\{0, 1, \ldots, q-1\}^n$ в записи $f(x_1, x_2, \ldots, x_n)$.

Теперь подходим к понятию *инвариантного класса.* Начнем с классического определения С. В. Яблонского (в [30] и [31] это определение было дано для случая $q = k = 2$).

Определение 7.4. *Множество $I \subset P_{q,k}$ называется инвариантным классом (по С. В. Яблонскому), если:*

(1) для каждой функции $f \in I$ классу I принадлежат все равные ей функции;

(2) для каждой функции $f \in I$ классу I принадлежат также все функции, получающиеся из f путем перестановки (без отождествления) переменных;

(3) для каждой функции $f \in I$ классу I принадлежат все подфункции f (в главном смысле).

Заметим, что в [31] п.(3) был сформулирован через подстановку константы вместо переменной. Однако при таком определении не вполне ясно, подразумевается ли удаление фиктивной переменной после подстановки (видимо, нет). В контексте задания инвариантного класса по С. В. Яблонскому это не имеет существенного значения, потому что по п.(1) равные функции должны одновременно принадлежать или не принадлежать инвариантному классу. Однако ниже будут даны альтернативные определения инвариантного класса, и для

этого третий пункт удобнее формулировать именно в таком виде, как в определении 7.4.

Инвариантные классы в [31] были введены при изучении схемной реализации булевых функций. В этом контексте определение 7.4 естественно, потому что, как отмечалось С. В. Яблонским, если построена схема, реализующая функцию f, то без труда получаются схемы, реализующие функции, возникающие из f путем применения операций (1), (2) и (3). В частности, равные функции просто реализуются одной и той же схемой. Однако при исследовании других задач иногда бывает необходимо рассматривать равные функции как существенно разные. Например, это наглядно видно, когда рассматриваются характеристические множества булевых функций (т. е. множества наборов, на которых функция принимает значение 1). Так, характеристическое множество функции $f_1(x_1) = x_1$ представляет собой один набор длины 1, а характеристическое множество функции $f_2(x_1, x_2) = x_1$ представляет из себя два набора длины 2. Если исследуется задачи о структурах дискретных функций без запрещенных подфункций (в первом и втором смыслах), то важное значение имеет, какая именно из равных функций запрещена. В этом контексте важно лишь то, что вместе с любой функцией в классе содержалась и любая ее подфункция (в том или ином смысле). Поэтому дадим два других (не эквивалентных классическому) определения инвариантного класса.

Определение 7.5. *Множество $I \subset P_{q,k}$ называется инвариантным классом (в первом смысле), если для каждой функции $f \in I$ классу I принадлежат все подфункции f (в первом смысле).*

Определение 7.6. *Множество $I \subset P_{q,k}$ называется инвариантным классом (во втором смысле), если для каждой функции $f \in I$ классу I принадлежат все подфункции f (во втором смысле).*

Из определений 7.2, 7.3, 7.5, 7.6 сразу следует, что любой инвариантный класс во втором смысле является также инвариантным классом в первом смысле. Кроме того, несложно видеть, что для инвариантного класса во втором смысле выполняется также условие (2) определения 7.4, поскольку функцию,

получающуюся из f перестановкой переменных без отождествления можно рассматривать как подфункцию f во втором смысле.

Возможно, слова «в первом» и «во втором» смыслах звучат не очень эстетично, однако, без достаточно убедительных аргументов в пользу рассматривающихся названий-кандидатов не будем вводить новые термины.

В [31] произведена характеризация инвариантных классов (по С. В. Яблонскому) в терминах запрещенных функций (порождающих элементов).

Определение 7.7. *[31] Функция g из $P_{q,k}$ называется порождающим элементом для инвариантного класса (по С. В. Яблонскому) I, если $g \notin I$ и любая ее подфункция (в главном смысле) принадлежит I.*

Инвариантный класс $I \subset P_{q,k}$ (в любом смысле) можно задать через его дополнение $CI \equiv P_{q,k} \setminus I$. Такое задание, вообще говоря, является избыточным, потому что если из некоторой функции f из $P_{q,k}$ последовательным применением операций, предусмотренных в определениях 7.4, 7.5, 7.6, удается получить функцию g, $g \notin I$, то f заведомо не принадлежит инвариантному классу. Поэтому для задания класса I достаточно указать лишь такое множество функций $G \subset CI$ по возможности содержащее как можно меньшее количество функций, что для любой функции f, $f \notin I$, применением операций, предусмотренных в определениях 7.4, 7.5, 7.6, удается получить функцию g, $g \in G$. В [31] показано, что в случае инвариантного класса по С. В. Яблонскому в качестве такого множества G можно взять множество всех порождающих элементов. Кроме того, в [31] отмечено, что любое множество $G \in P_{q,k}$ задает некоторый инвариантный класс в $P_{q,k}$ (еще раз напомним, что в работе [31] рассматривался только случай $q = k = 2$, но все приведенные там рассуждения остаются верными и для общего случая).

Аналогичный факт имеет место и для инвариантных классов в первом и втором смыслах. Если задана функция g_i, то обозначим через Π_{g_i} множество всех функций, из которых путем применения операций, предусмотренных определениях 7.4, 7.5, 7.6, удается получить функцию g_i. Множество Π_{g_i} названо в [31] *пучком*, порожденным функцией g_i. Тогда инвариантный класс, задаваемый

множеством G определяется в точности как $I(G) = P_{q,k} \setminus \left(\bigcup_{g_i \in G} \Pi_{g_i} \right)$. В этой главе задание инвариантного класса через множество G мы будем называть заданием инвариантного класса через *множество запрещенных подфункций*, а само множество G будем называть *множеством запрещенных подфункций*.

7.2 Краткие сведения из теории слов, избегающих запреты

Конечное множество A букв называется *алфавитом*. Часто бывает удобно рассматривать алфавит мощности k как множество первых k целых неотрицательных чисел $Z_k = \{0, 1, \ldots, k-1\}$. Последовательность букв из алфавита называется *словом* в этом алфавите. Различают *конечные* слова $(a_0, a_1, \ldots, a_{n-1})$, в этом случае число букв n в слове называют *длиной слова*, и *бесконечные* слова $(a_0, a_1, \ldots)$. Взятая без пропусков подпоследовательность букв слова u называется *подсловом* слова u. Подслово слова u может быть пустым (иметь длину 0), или совпадать с самим словом u. Подслова, отличные от этих двух типов, называются *собственными* подсловами. Слово (конечное или бесконечное) будем называть *константным*, если все входящие в него буквы совпадают между собой. Пусть G — произвольное множество слов в алфавите A (конечное или бесконечное). Говорят, что слово u *избегает* множество G (или *множество запрещенных подслов*, или *систему запретов*), если ни одно из слов, входящих во множество G, не содержится в слове u в качестве подслова. Если в алфавите A существует бесконечное слово, избегающее систему запретов G, то множество G называется *избегаемым*, в противном случае, если в алфавите A не существует бесконечного слова, избегающего G, то множество G называется *блокирующим*.

Проблема определения, является ли множество слов G (конечное или бесконечное) блокирующим или свободным в алфавите A, одна из наиболее интенсивно исследующихся в теории слов, избегающих запреты. Если множество G является конечным, а длина самого длинного его слова равна n, то хорошо известно, что вопрос о том, является ли множество G избегаемым или блокирующим, можно решить с трудоемкостью порядка $|G| \cdot n$ [8]. Весьма удобным при этом является построение конечного автомата и анализ его структуры средствами теории графов. Подробнее об этом можно узнать из работы [7]. Среди многочисленных работ, посвященных вопросам распознавания избегаемости конечного системы запретов G, выделим работу [101].

В случае, когда множество G бесконечно, многое зависит от того, каким

именно образом G задано. Ведь если множество G задано как некоторая бесконечная последовательность слов, то говорить о практических алгоритмах распознавания его избегаемости не приходится. Поэтому важное значение имеют случаи, когда бесконечное множество запрещенных слов G тем не менее как-то задается конечным образом. Способы такого задания опять-таки разнообразны. В современной литературе большой популярностью пользуется изучение избегаемости бесконечных множеств G, заданных с помощью *термов*, т. е. конечных слов в каком-то новом алфавите $\mathcal{X}$, и множество G образуется путем всевозможных подстановок в термы вместо букв алфавита $\mathcal{X}$ конечных слов из нашего алфавита A. Среди работ, связанных с термами, следует отметить работу А. И. Зимина [9], в которой получена характеризация блокирующих термов, однако только таких, которые являются блокирующими в алфавитах любой мощности. Общая же задача характеризации блокирующих систем термов в алфавитах заданной мощности остается открытой.

7.3 Критерии бесконечности инвариантных классов, заданных системой запрещенных подфункций

Как было отмечено в параграфе 7.1, каждый инвариантный класс (по С. В. Яблонскому, в первом или втором смыслах) может быть задан через множество запрещенных подфункций G, более того, произвольное множество G, конечное или бесконечное, если его рассматривать как множество запрещенных подфункций, задает некоторый инвариантный класс. Представляет интерес вопрос, как по множеству запрещенных подфункций можно устанавливать те или иные свойства инвариантного класса. Настоящий параграф посвящен задаче определения по множеству запрещенных подфункций G, является ли задаваемый множеством G инвариантный класс бесконечным. Для инвариантного класса в первом или втором смыслах понятие бесконечности класса можно (и нужно) понимать буквально: инвариантный класс в первом или втором смыслах будем называть *бесконечным*, если он содержит бесконечное число функций из $P_{q,k}$. В случае инвариантного класса по С. В. Яблонскому подобное определение несодержательно, поскольку любой непустой инвариантный класс по С. В. Яблонскому вместе с любой своей функцией содержит и бесконечное число равных ей функций. Заметим, что из любой функции путем удаления фиктивных переменных можно получить невырожденную функцию. Поэтому *бесконечным* инвариантным классом по С. В. Яблонскому назовем инвариантный класс по С. В. Яблонскому, содержащий бесконечное число невырожденных функций. (Напомним, что $f(x_1, x_2, \ldots, x_n)$ и $f(y_1, y_2, \ldots, y_n)$ считаются записями одной и той же функции.)

Пусть G — произвольное (конечное или бесконечное) множество функций из $P_{q,k}$. Через $I(G)$ будем обозначать инвариантный класс (в соответствующем смысле), задаваемый множеством G. (При рассмотрении инвариантного класса по С. В. Яблонскому мы будем считать, что все функции из G невырождены, поскольку в этом случае функцию, зависящую от каких-то переменных фиктивно, можно заменить на равную ей функцию, зависящую от всех переменных

существенно; при этом задаваемый множеством G инвариантный класс не изменится.). Через $S(G)$ обозначим множество, состоящее из всех симметрических функций из G.

Лемма 7.1. *Инвариантные классы (в первом или втором смыслах), задаваемые множествами запрещенных подфункций G и $S(G)$ из $P_{2,k}$, либо одновременно являются бесконечными, либо одновременно не являются бесконечными.*

Доказательство. Заметим сначала, что $S(G) \subseteq G$, поэтому, как легко видеть, $I(G) \subseteq I(S(G))$. Если класс $I(G)$ не является бесконечным, то найдется такое натуральное n_1, что класс $I(G)$ не содержит функций из $P_{2,k}^{n_1}$. Имея число n_1, возьмем число $N(n_1)$ из теоремы 6.1. Рассмотрим произвольную функцию f из $P_{2,k}^{N(n_1)}$. По теореме 6.1 из функции f подстановками констант 0 вместо некоторых переменных можно получить симметрическую функцию f' (в первом или втором смыслах) из $P_{2,k}^{n_1}$. Функция f' не принадлежит классу $I(G)$, следовательно, из нее подстановками констант вместо некоторых переменных можно получить функцию f'' из множества G. Однако по следствию 7.1 функция f'' является также симметрической, стало быть, функция f'' принадлежит и множеству $S(G)$. Тогда функция f не принадлежит инвариантному классу $I(S(G))$. Ввиду произвольности выбора функции f делаем вывод, что класс $I(S(G))$ не содержит функций из $P_{2,k}^{N(n_1)}$, и, таким образом, класс $I(S(G))$, как и класс $I(G)$, не является бесконечным.

Пусть теперь класс $I(S(G))$ является бесконечным. Тогда бесконечным является и множество функций $S(I(S(G)))$ (более того, из следствия 7.1 несложно видеть, что это множество само является инвариантным классом). Действительно, если бы множество $S(I(S(G)))$ не являлось бесконечным, то нашлось бы такое натуральное число n_1, что множество $S(I(S(G)))$ не содержит функций из $P_{2,k}^{n_1}$, но тогда по теореме 6.1 класс $I(S(G))$ не содержал бы функций из $P_{2,k}^{N(n_1)}$ и, стало быть, не являлся бы бесконечным. Однако множество $S(I(S(G)))$ содержится в классе $I(G)$, поскольку противное могло бы быть только в случае существования функции f из $S(I(S(G)))$, содержащей в качестве подфункции (в первом или втором смыслах) функцию из $G \setminus S(G)$, что невозможно в силу

симметричности функции f и следствия 7.1. Таким образом, класс $I(G)$, как и класс $I(S(G))$, является бесконечным. Лемма 7.1 доказана. □

Лемма 7.2. *Инвариантные классы (по С. В. Яблонскому), задаваемые множествами запрещенных подфункций G и $S(G)$ из $P_{2,k}$, либо одновременно являются бесконечными, либо одновременно не являются бесконечными.*

Доказательство. Заметим сначала, что $S(G) \subseteq S$, поэтому, как легко видеть, $I(G) \subseteq I(S(G))$. Если класс $I(G)$ не является бесконечным, то найдется такое натуральное n_1, что класс $I(G)$ не содержит невырожденных функций из $P_{2,k}^{n_1}$. Имея число n_1, возьмем число n_2 из теоремы 6.4. Рассмотрим произвольную невырожденную функцию f из $P_{2,k}^{n}$, $n \geq n_2$. По теореме 6.4 из функции f подстановками констант вместо некоторых переменных с последующим удалением фиктивных переменных можно получить симметрическую функцию f' из $P_{2,k}^{n_1}$. Функция f' не принадлежит классу $I(G)$, следовательно, из нее подстановками констант вместо некоторых переменных с последующим удалением несущественных переменных можно получить функцию f'' из множества G. Однако по следствию 7.1 функция f'' является также симметрической, стало быть, функция f'' принадлежит и множеству $S(G)$. Тогда функция f не принадлежит инвариантному классу $I(S(G))$. Ввиду произвольности выбора функции f делаем вывод, что класс $I(S(G))$ не содержит невырожденных функций из $P_{2,k}^{n_2}$ при $n \geq n_2$ и, таким образом, класс $I(S(G))$, как и класс $I(G)$, не является бесконечным.

Пусть теперь класс $I(S(G))$ является бесконечным. Тогда бесконечным является и множество функций $S(I(S(G)))$ (более того, из следствия 7.1 несложно видеть, что это множество само является инвариантным классом). Действительно, если бы множество $S(I(S(G)))$ не являлось бесконечным, то нашлось бы такое натуральное число n_1, что множество $S(I(S(G)))$ не содержит невырожденных функций из $P_{2,k}^{n_1}$, но тогда по теореме 6.4 класс $I(S(G))$ не содержал бы функций из $P_{2,k}^{n}$ при $n \geq n_2$ и, стало быть, не являлся бы бесконечным. Однако множество $S(I(S(G)))$ содержится в классе $I(G)$, поскольку противное могло бы быть только в случае существования функции f из $S(I(S(G)))$, содержащей в качестве подфункции функцию из $G \setminus S(G)$, что невозможно в силу

симметричности функции f и следствия 7.1. Таким образом, класс $I(G)$, как и класс $I(S(G))$, является бесконечным. Лемма 7.2 доказана. □

Замечание 7.1. Обобщение лемм 7.1 и 7.2 для множества $P_{q,k}$, $q \geq 3$, $k \geq 2$, неверно. Действительно, возьмем в качестве множества G множество всех функций из $P^2_{q,k}$ (в случае инвариантного класса по С. В. Яблонскому берем только невырожденные функции из $P^2_{q,k}$). Очевидно, что класс $I(G)$ не является бесконечным. Пример из теоремы 6.2 убеждает, что класс $I(S(G))$ в этом случае бесконечным является.

Леммы 7.1 и 7.2 показывают, что в случае $q = 2$ при рассмотрении вопроса, является ли класс $I(G)$ бесконечным, можно рассматривать класс $I(S(G))$. Ответ будет тем же. Грубо говоря, из множества G можно удалить все функции, не являющиеся симметрическими (еще раз повторим, что в случае инвариантных классов по С. В. Яблонскому, считаем, что в G входят только невырожденные функции). Это показывает, что ответ на вопрос, будет ли класс $I(G)$ бесконечным, один и тот же, независимо от того, рассматриваем ли мы инвариантные классы в первом или втором смыслах. Для инвариантных классов по С. В. Яблонскому, как увидим ниже, имеется некоторая специфика.

Напомним, что для симметрической функции f из $P^n_{2,k}$ через $\pi(f) = (\pi_0, \pi_1, \ldots, \pi_n)$ обозначаем ее характеристическую последовательность. Пусть G — произвольное множество функций из $P_{2,k}$. Обозначим через $\pi(G)$ множество, состоящее из характеристических последовательностей всех симметрических функций из G. Будем рассматривать такие последовательности как слова в алфавите $Z_k = \{0, 1, \ldots, k-1\}$.

Теорема 7.1. *Инвариантный класс $I(G)$ (в первом или втором смысле) в $P_{2,k}$ бесконечен тогда и только тогда, когда множество $\pi(G)$ не является блокирующим в алфавите Z_k.*

Доказательство. Пусть класс $I(G)$ бесконечен. Тогда по лемме 7.1 бесконечен и класс $I(S(G))$. Инвариантный класс замкнут относительно перехода к подфункции, поэтому по лемме Кенига о бесконечном дереве найдется такая бесконечная последовательность $F = \{f_i\}$, $i = 0, 1, \ldots$, симметри-

ческих функций из $I(S(G))$, что $f_i \in P^i_{2,k}$ и функция f_i может быть получена из функции f_{i+1} подстановкой константы 0 вместо переменной x_{i+1} (с последующим удалением фиктивной переменной). Легко видеть, что с последовательностью функций F ассоциирована бесконечная последовательность $\pi(F) = (\pi_0, \pi_1, \dots)$ в алфавите Z_k, причем для любого целого неотрицательного n начальный кусок длины $n+1$ последовательности $\pi(F)$ является характеристической последовательностью функции f_n из F. Функция f_i не содержит функций из $S(G)$ в качестве подфункций, стало быть последовательность $\pi(F)$ в алфавите Z_k не содержит слов из множества $\pi(G)$ в качестве подслов. Тем самым предъявлено бесконечное слово $\pi(F)$ в алфавите Z_k, избегающее множество запретов $\pi(G)$, поэтому множество $\pi(G)$ не является блокирующим. Пусть теперь множество $\pi(G)$ не является блокирующим. Тогда существует бесконечное слово $\pi(F) = (\pi_0, \pi_1, \dots)$ в алфавите Z_k, избегающее это множество запретов. Рассмотрим множество симметрических функций $F = \{f_i\}$, $i = 0, 1, \dots$, где функция f_i задается через ее характеристическую последовательность $(\pi_0, \pi_1, \dots, \pi_i)$. Рассмотрим множество всевозможных подфункций (в первом или втором смыслах, что, кстати, все равно, поскольку функции симметрические) функций из F. По построению все эти подфункции не содержат подфункций (в первом или втором смыслах) из G и, стало быть, принадлежат $I(G)$. Таким образом, инвариантный класс (в первом или втором смыслах) $I(G)$ бесконечен. Теорема 7.1 доказана. □

Теорема 7.2. *Пусть G — некоторое множество функций из $P_{2,k}$, существенно зависящих от всех своих переменных. Инвариантный класс $I(G)$ (по С. В. Яблонскому) в $P_{2,k}$ бесконечен тогда и только тогда, когда в алфавите Z_k существует бесконечное слово, содержащее по крайней мере две различные буквы, которое избегает множество запрещенных подслов $\pi(G)$.*

Доказательство. Отличие от теоремы 7.1 состоит в том, что бесконечность инвариантного класса подразумевает теперь бесконечность числа содержащихся в нем невырожденных функций. Симметрическая функция, не равная тождественной константе, зависит существенно от всех своих переменных; тождественной же константе симметрическая функция не равна тогда и только тогда,

когда ее характеристическая последовательность содержит по крайней мере два разных числа. Поэтому, если найдется бесконечное слово, содержащее по крайней мере две различные буквы, которое избегает множество запрещенных подслов $\pi(G)$, то с его помощью найдем бесконечное число невырожденных симметрических функций из $I(G)$. Если же множество запрещенных подслов $\pi(G)$ является блокирующим в алфавите Z_k, или же его избегают только бесконечные слова, состоящие ровно из одной буквы, то это означает, что начиная с некоторого натурального n_1 не существует слов длины n_1, содержащих по крайней мере две разные буквы, которые бы не содержали в качестве подслов слов из множества $\pi(G)$. Тогда если взять число n_2 из теоремы 6.4, то любая невырожденная функция f из $P^n_{2,k}$, $n \geq n_2$, содержит в качестве подфункции невырожденную симметрическую функцию из $P^{n_1}_{2,k}$, которая инвариантному классу $I(G)$ не принадлежит. Тем самым функция f также не принадлежит $I(G)$, поэтому класс $I(G)$ не является бесконечным. Теорема 7.2 доказана. □

Пример. Пусть $q = k = 2$ и множество G состоит из одной функции, равной тождественной единице. Тогда $\pi(G) = \{(1)\}$. Эту систему запретов в алфавите Z_2 избегает только одно бесконечное слово, состоящее из одних нулей. Поэтому инвариантный класс в первом или втором смыслах $I(G)$ бесконечен и состоит из функций $f_i(x_1, x_2, \ldots, x_i) \equiv 0$, $i = 0, 1, \ldots$. Инвариантный же класс по С. В. Яблонскому $I(G)$ конечен и состоит функций, равных тождественному нулю.

А. А. Евдокимов сообщил автору, что когда он много лет назад выступал на семинаре С. В. Яблонского с докладом о множествах слов, избегающих запреты, Сергей Всеволодович отметил внутреннее сходство множеств слов, избегающих запреты, с инвариантными классами.

7.4 Минимальные бесконечные инвариантные классы

На задачу, решение которой рассматривается в этом параграфе, внимание автора настоятельно обратил О. М. Касим-Заде.

Определение 7.8. *Бесконечный инвариантный класс (по С. В. Яблонскому, в первом или втором смысле) I в $P_{q,k}$ мы будем называть минимальным, если для любой функции f, $f \in I$, инвариантный класс $I\left((P_{q,k} \setminus I) \bigcup f\right)$ не является бесконечным.*

Лемма 7.3. *Любой минимальный бесконечный инвариантный класс (по С. В. Яблонскому, в первом или втором смысле) в $P_{2,k}$ содержит только симметрические функции (в случае инвариантного класса по С. В. Яблонскому речь идет только о невырожденных функциях).*

Доказательство. Пусть I — произвольный бесконечный инвариантный класс (в любом смысле), содержащий не симметрическую функцию f. Очевидно, что класс I можно задать как $I = I(P_{2,k} \setminus I)$. Рассмотрим класс $I_1 = I\left((P_{2,k} \setminus I) \bigcup f\right)$. По леммам 7.1 и 7.2 если класс I бесконечен, то и класс I_1 тоже бесконечен. Однако тогда по определению 7.8 класс I не является минимальным бесконечным инвариантным классом. Лемма 7.3 доказана. □

Лемма 7.3 показывает, что минимальные бесконечные инвариантные классы в первом и втором смыслах будут в точности одни и те же.

Определение 7.9. *[1] Пусть w — бесконечное слово в алфавите A. Слово w называется плотным, если для любого его конечного подслова u найдется такое натуральное число $n(u)$, что для любого подслова v слова w длины $n(u)$ слово u является подсловом слова v.*

Определение 7.10. *Пусть $\pi = (\pi_0, \pi_1, \dots)$ — бесконечное слово в алфавите $Z_k = \{0, 1, \dots, k-1\}$. Обозначим через $I_{\tilde{\pi}}$ множество всех симметрических функций из $P_{2,k}$, характеристические последовательности которых являются подсловами слова $\tilde{\pi}$.*

Лемма 7.4. *Пусть* $\pi = (\pi_0, \pi_1, \dots)$ *— бесконечное слово в алфавите* $Z_k = \{0, 1, \dots, k-1\}$. *Тогда множество* I_π *является бесконечным инвариантным классом (в первом или втором смыслах).*

Доказательство. Множество I_π состоит только из симметрических функций и вместе с любой своей функцией содержит и любую ее подфункцию (в первом или втором смыслах). Следовательно, I_π — инвариантный класс. Число функций в I_π бесконечно. Лемма 7.4 доказана. □

Лемма 7.5. *Пусть* $\pi = (\pi_0, \pi_1, \dots)$ *— бесконечное плотное слово в алфавите* $Z_k = \{0, 1, \dots, k-1\}$. *Тогда* I_π *является минимальным бесконечным инвариантным классом (в первом или втором смыслах).*

Доказательство. Пусть f — произвольная функция из класса I_π. Рассмотрим инвариантный класс $I_1 = I\left((P_{2,k} \setminus I_\pi) \bigcup f\right)$. По построению класса I_π функция f является симметрической. Пусть $\pi(f)$ — характеристическая последовательность функции f. Слово $\pi(f)$ по заданию класса I_π является подсловом слова π. По определению 7.9 для слова $\pi(f)$ найдется такое натуральное число $n(\pi(f))$, что для любого подслова v слова π длины $n(\pi(f))$ слово $n(\pi(f))$ является подсловом слова v. Отсюда никакая функция из класса I_π, зависящая не менее чем от $n(\pi(f))$ переменных, не принадлежит классу I_1. Поэтому класс I_1 не является бесконечным. Ввиду произвольности выбора функции f в классе I_π заключаем, что класс I_π является минимальным бесконечным инвариантным классом (в первом или втором смыслах). Лемма 7.5 доказана. □

Следствие 7.2. *Пусть* $\pi = (\pi_0, \pi_1, \dots)$ *— бесконечное плотное слово в алфавите* $Z_k = \{0, 1, \dots, k-1\}$. *Тогда бесконечное слово* $\pi'(\pi_m, \pi_{m+1}, \dots)$, *получающееся из* π *отбрасыванием любого его начала, также является плотным и* $I_{\pi'} = I_\pi$. *Действительно, плотность слова* $(\pi_m, \pi_{m+1}, \dots)$ *сразу следует из определения 7.9. Из этого же определения следует и то, что при отбрасывании любого начала* π *всякое подслово, имевшее буквы в отброшенном начале, будет содержаться и в оставшейся (бесконечной) части слова* π *— слове* $(\pi_m, \pi_{m+1}, \dots)$.

Лемма 7.6. *Пусть I — минимальный бесконечный инвариантный класс в $P_{2,k}$ (в первом или втором смыслах). Тогда найдется такое бесконечное плотное слово $\pi = (\pi_0, \pi_1, \dots)$, что класс I можно задать как множество всех симметрических функций из $P_{2,k}$, характеристические последовательности которых являются подсловами слова π.*

Доказательство. То, что класс I состоит только из симметрических функций, уже доказано нами в лемме 7.3. Из бесконечности класса I вытекает, что по лемме Кенига о бесконечном дереве найдется такая бесконечная последовательность $F = \{f_i\}$, $i = 0, 1, \dots$, симметрических функций из I, что $f_i \in P^i_{2,k}$ и функция f_i может быть получена из функции f_{i+1} подстановкой константы 0 вместо переменной x_{i+1} (с последующим удалением фиктивной переменной). Легко видеть, что с последовательностью функций F ассоциировано бесконечное слово $\pi = (\pi_0, \pi_1, \dots)$ в алфавите Z_k, причем для любого целого неотрицательного n начальный кусок длины $n+1$ последовательности π является характеристической последовательностью функции f_n из F. Бесконечное слово π, как видно из леммы 7.4, задает, $I_1 = I_\pi$, который, очевидно, содержится в классе I. Если $I_1 \neq I$, то класс I не является минимальным, поэтому $I_1 = I$. Если слово π не является плотным, то тогда, обращая определение 7.9, получаем, что в слове π найдется такое конечное подслово u, что для любого натурального числа n в слове π найдется такое подслово v длины n, что слово u не является подсловом слова v. Однако тогда возьмем функцию f, характеристической последовательностью которой является слово u, и рассмотрим класс $I_2 = I\left((P_{2,k} \setminus I) \bigcup f\right)$. По сказанному выше класс I_2 является бесконечным инвариантным классом, $I_2 \subset I$ и $I_2 \neq I$. Отсюда следует, что инвариантный класс I не был минимальным. Значит, слово π должно быть плотным. Лемма 7.6 доказана. □

Объединяя результаты лемм 7.4, 7.5 и 7.6, мы получаем следующую теорему о характеризации минимальных бесконечных инвариантных классов в $P_{2,k}$ (в первом или втором смыслах).

Теорема 7.3. *Любое бесконечное плотное слово π в алфавите Z_k задает минимальный бесконечный инвариантный класс в $P_{2,k}$ (в первом или втором смыслах) I_π. В свою очередь любой минимальный бесконечный инвариантный*

класс I в $P_{2,k}$ (в первом или втором смыслах) может быть задан как $I_1 = I_\pi$ через бесконечное плотное слово в алфавите Z_k.

Лемма 7.7. *Пусть I — минимальный бесконечный инвариантный класс в $P_{2,k}$ (по С. В. Яблонскому). Тогда либо класс I можно задать как $I_1 = I_\pi$ для некоторого бесконечного плотного слова $\pi = (\pi_0, \pi_1, \dots)$ в алфавите Z_k, либо класс I есть множество всех симметрических функций из $P_{2,k}$, характеристические последовательности которых имеют вид $(a, b, b, \dots, b, b)$, где a и b — различные фиксированные буквы алфавита Z_k, включающее также функции, равные константам a и b, либо класс I есть множество всех симметрических функций из $P_{2,k}$, характеристические последовательности которых имеют вид $(b, b, \dots, b, b, a)$, где a и b — различные фиксированные буквы алфавита Z_k, включающее также функции, равные константам a и b.*

Доказательство. Как было установлено в лемме 7.3, класс I состоит только из симметрических функций. Число невырожденных функций в классе I по условию леммы бесконечно. Если пытаться составить из характеристических последовательностей этих функций бесконечное слово, пользуясь леммой Кенига о бесконечном дереве, как это было сделано при доказательстве леммы 7.6, то можно получить константное слово, т. е. слово, все буквы которого совпадают. Константное же бесконечное слово в случае инвариантных классов по С. В. Яблонскому задает не бесконечный инвариантный класс. Поэтому чуть усложним построение.

Случай 1. Если инвариантный класс I для некоторого натурального n_0 содержит бесконечное число симметрических функций, у характеристических последовательностей которых среди первых n_0 букв имеются хотя бы две различных, то можно ограничиться только таким множеством функций, и применяя к нему лемму Кенига о бесконечном дереве, получим бесконечное слово π, состоящее из по крайней мере двух разных букв. Множество невырожденных симметрических функций, характеристические последовательности которых являются подсловами слова π, бесконечно, поэтому в силу минимальности бесконечного инвариантного класса I заключаем, что характеристическая последовательность любой функции из I является подсловом слова π. Если сло-

во π является плотным, то все доказано. Пусть слово π не является плотным. Тогда, обращая определение 7.9, получаем, что в слове π найдется такое конечное подслово u, что для любого натурального числа n в слове π найдется такое подслово v длины n, что слово u не является подсловом слова v. Возьмем функцию f, характеристической последовательностью которой является слово u и рассмотрим класс $I_2 = I\left((P_{2,k} \setminus I) \bigcup f\right)$. Очевидно, что $I_2 \subset I$ и $I_2 \neq I$. Поэтому класс I может являться минимальным бесконечным инвариантным классом только если класс I_2 не является бесконечным инвариантным классом. Это может быть только в том случае, если выбиравшиеся для любого натурального числа n подслова v длины n являлись константными словами. Таким образом, для любого n в слове π существует константное подслово длины n. Однако по построению в начальном куске длины n_0 слова π имеются по крайней мере две различные буквы. Поэтому если продолжить константные подслова налево до первой встречи другой буквы, то будет построено бесконечное семейство слов вида $(a, b, b, \ldots, b, b)$, где a и b — различные буквы алфавита Z_k. Заметим, что подслова такого вида могут содержаться в слове π только при фиксированных значениях a и b, в противном случае класс I не является минимальным бесконечным инвариантным классом. Однако множество слов вида $(a, b, b, \ldots, b, b)$ при фиксированных различных буквах a и b, объединенное с константными функциями a и b, в точности совпадает с множеством подслов бесконечной последовательности $(a, b, b, \ldots)$ и является инвариантным классом. Несложно проверить, что этот инвариантный класс является минимальным бесконечным инвариантным классом. Случай 1 полностью разобран.

Случай 2. Инвариантный класс I для любого натурального n содержит лишь конечное число симметрических функций, у характеристических последовательностей которых среди первых n букв имеются хотя бы две различных. Однако инвариантный класс I бесконечен, поэтому для любого натурального числа n он содержит бесконечное число невырожденных симметрических функций, у характеристических последовательностей первые n букв совпадают. Продолжая константные начала вправо до первой встречи другой буквы, построим бесконечное семейство слов вида $(b, b, \ldots, b, b, a)$, где a и b — различные буквы алфавита Z_k. Заметим, что подслова такого вида могут содержаться в слове π

только при фиксированных значениях a и b, в противном случае класс I не является минимальным бесконечным инвариантным классом. Множество слов вида $(b, b, \dots, b, b, a)$ при фиксированных различных буквах a и b, объединенное с константными функциями a и b, можно рассматривать как множество подслов бесконечной последовательности $(\dots, b, b, a)$, идущей в бесконечность не направо, как обычно, а налево. Несложно проверить, что это множество является минимальным бесконечным инвариантным классом. Лемма 7.7 полностью доказана. □

Лемма 7.8. *Пусть $\pi = (\pi_0, \pi_1, \dots)$ — бесконечное плотное слово в алфавите $Z_k = \{0, 1, \dots, k-1\}$, состоящее по крайней мере из двух разных букв. Тогда множество I_π является бесконечным инвариантным классом (по С. В. Яблонскому).*

Доказательство. Множество I_π состоит только из симметрических функций, среди которых имеется бесконечное число невырожденных, и вместе с любой своей функцией содержит и любую ее подфункцию. Следовательно, I_π — инвариантный класс. Число невырожденных функций в I_π бесконечно. Доказательство же минимальности класса I_π почти дословно повторяет доказательство леммы 7.5 (только рассуждение надо применять именно к невырожденным функциям). Лемма 7.8 доказана. □

Объединяя результаты лемм 7.7 и 7.8, получаем следующую теорему о характеризации минимальных бесконечных инвариантных классов в $P_{2,k}$ (по С. В. Яблонскому).

Теорема 7.4. *Любое бесконечное плотное слово π в алфавите Z_k, состоящее по крайней мере из двух разных букв, задает минимальный бесконечный инвариантный класс I в $P_{2,k}$ (по С. В. Яблонскому) I_π. В свою очередь, любой минимальный бесконечный инвариантный класс I в $P_{2,k}$ (по С. В. Яблонскому), может быть задан как $I = I_\pi$ через бесконечное плотное слово в алфавите Z_k, кроме классов всех симметрических функций из $P_{2,k}$, характеристические последовательности которых имеют вид $(a, b, b, \dots, b, b)$, где a и b — различные фиксированные буквы алфавита Z_k, включающих также функции, равные константам a и b, и классов всех всех симметрических*

функций из $P_{2,k}$, характеристические последовательности которых имеют вид $(b, b, \ldots, b, b, a)$, где a и b — различные фиксированные буквы алфавита Z_k, включающих также функции, равные константам a и b.

Следствие 7.3. *Пусть $q = k = 2$. Тогда любое бесконечное плотное слово π в алфавите Z_2, содержащее и нули, и единицы, задает минимальный бесконечный инвариантный класс в P_2 (по С. В. Яблонскому), если рассмотреть множество всех симметрических функций из P_2, характеристические последовательности которых являются подсловами слова π. Кроме того, минимальными бесконечными инвариантными классами в P_2 (по С. В. Яблонскому) являются еще четыре класса, включающие в себя помимо констант 0 и 1, также соответственно:* 1) *всевозможные конъюнкции переменных,* 2) *отрицания всевозможных конъюнкций переменных,* 3) *всевозможные дизъюнкции переменных,* 4) *отрицания всевозможных дизъюнкций переменных.*

Замечание 7.2. Из доказательств лемм 7.6 и 7.7 видно, что для любого бесконечного инвариантного класса I в $P_{2,k}$ (в первом или втором смыслах или по С. В. Яблонскому) найдется минимальный бесконечный инвариантный класс I_1, содержащийся в I.

В [31] С. В. Яблонский доказал, что мощность множества всех инвариантных классов (по С. В. Яблонскому) равна континууму. Очевидно, что мощность множества всех инвариантных классов, не являющихся бесконечными, счетна. Оказывается, что уже мощность множества всех минимальных бесконечных инвариантных классов равна континууму. Доказательству этого факта мы предпошлем несколько лемм.

Лемма 7.9. *Пусть ξ — произвольное иррациональное число из интервала $(0, 1)$. Тогда для любого $\varepsilon > 0$ найдется такое натуральное $m = m(\varepsilon)$, что величина $m\xi$ отличается от ближайшего целого числа меньше чем на ε.*

Доказательство. Очевидно, что дробные части чисел вида $n\xi$ при разных целых n различны ввиду иррациональности числа ξ. Поэтому среди чисел $n\xi$, $n = 0, 1, \ldots, \lceil 1/(\varepsilon + 1) \rceil$, найдутся два таких, скажем, n_1 и n_2, что $0 < (n_2\xi - \lfloor n_2\xi \rfloor) - (n_1\xi - \lfloor n_1\xi \rfloor) < \varepsilon$. Тогда дробная часть числа $(n_2 - n_1)\xi$ меньше чем ε.

Отсюда следует, что в качестве числа $m = m(\varepsilon)$ можно взять число $|n_2 - n_1|$. Лемма 7.9 доказана. □

Лемма 7.10. *Пусть ξ — произвольное иррациональное число из интервала $(0, 1)$. Для любого $\varepsilon > 0$ обозначим через $\mathcal{M}(\varepsilon)$ множество всех таких натуральных чисел n, что дробная часть числа $n\xi$ меньше чем ε. Тогда найдется такое $M = M(\varepsilon)$, что из любых M идущих подряд натуральных чисел найдется хотя бы одно, принадлежащее множеству $\mathcal{M}(\varepsilon)$.*

Доказательство. Возьмем $m = m(\varepsilon)$ из леммы 7.9 и рассмотрим множество чисел вида $nm\xi$, где n пробегает множество всех натуральных чисел. Дробная часть числа $nm\xi$ при увеличении n на единицу циклически сдвигается по отрезку $[0, 1]$ на величину ε', $0 < \varepsilon' < \varepsilon$. Поэтому не реже чем через $\lceil 1/\varepsilon' \rceil$ шагов по n дробная часть числа $nm\xi$ будет попадать в интервал $(0, \varepsilon)$. Поэтому в качестве числа $M(\varepsilon)$ достаточно взять число $m\lceil 1/\varepsilon' \rceil$. Лемма 7.10 доказана.

Для заданного действительного числа ξ, $0 < \xi < 1$, рассмотрим бесконечную последовательность $\pi(\xi)(\pi_0, \pi_1, \dots)$, построенную по правилу $\pi_n = \lfloor (n+1)\xi \rfloor - \lfloor n\xi \rfloor$, $n = 0, 1, \dots$. В работе [18] эта последовательность названа *последовательностью типа Бернулли* или *B-последовательностью*. В современной зарубежной литературе ее принято называть *стандартной последовательностью Штурма*. Легко видеть, что все элементы последовательности $\pi(\xi)$ равны 0 или 1. Таким образом, последовательность $\pi(\xi)$ можно рассматривать как бесконечное слово в алфавите Z_2. Если ξ — рациональное число вида $\frac{s}{t}$, то несложно видеть, что $\pi_i = \pi_{i+t}$ для любого целого неотрицательного i, т. е. слово $\pi(\xi)$ является *периодическим* с периодом t. Тогда если u — произвольное подслово слова $\pi(\xi)$ длины $l(u)$, то u содержится в качестве подслова в любом слове вида $(\pi_{m_1 t}, \pi_{m_1 t+1}, \dots, \pi_{m_2 t-1})$, где m_1 и m_2 — целые неотрицательные числа, и $m_2 = \lfloor \frac{l(u)+2t}{t} \rfloor + m_1$. Последнее же слово в свою очередь содержится в любом подслове v слова $\pi(\xi)$ длины не меньше $l(u)+4t$. Следовательно, полагая $n(u) = l(u) + 4t$, по определению 7.9 устанавливаем, что $\pi(\xi)$ — плотное слово. Таким образом, доказана следующая лемма.

Лемма 7.11. *Пусть ξ — произвольное рациональное число. Тогда бесконечное слово $\pi(\xi)(\pi_0, \pi_1, \dots)$, построенное по правилу $\pi_n = \lfloor (n+1)\xi \rfloor - \lfloor n\xi \rfloor$, $n =$*

$0, 1, \ldots,$ *является плотным.*

Рассмотрим теперь случай, когда число ξ — иррационально.

Лемма 7.12. *Пусть ξ — произвольное иррациональное число. Тогда бесконечное слово $\pi(\xi)(\pi_0, \pi_1, \ldots)$, построенное по правилу $\pi_n = \lfloor (n+1)\xi \rfloor - \lfloor n\xi \rfloor$, $n = 0, 1, \ldots,$ является плотным.*

Доказательство. Пусть $u = (\pi_{n_1}, \pi_{n_1+1}, \ldots, \pi_{n_2})$ — произвольное подслово слова $\pi(\xi)$. Обозначим $\varepsilon = \varepsilon(u) \min\limits_{n_1 \le n \le n_2+1} (\lceil n\xi \rceil - n\xi)$. Число ξ иррационально, поэтому $\varepsilon > 0$. Если $\mathcal{M}(\varepsilon)$ — это множество всех таких натуральных чисел m, что дробная часть числа $m\xi$ меньше чем ε, то для любого $m \in \mathcal{M}$ слово $u(m) = (\pi_{n_1+m}, \pi_{n_1+m+1}, \ldots, \pi_{n_2+m})$ совпадает со словом u. По лемме 7.10 существует такое $M = M(\varepsilon)$, что из любых M идущих подряд натуральных чисел найдется хотя бы одно, принадлежащее множеству $\mathcal{M}(\varepsilon)$. Поэтому в любом подслове v длины $M + (n_2 - n_1 + 1)$ слова $\pi(\xi)$ найдется подслово, совпадающее со словом u. Следовательно, по определению 7.9 слово $\pi(\xi)$ является плотным. Лемма 7.12 доказана. □

Лемма 7.13. *Мощность множества всех бесконечных плотных слов в алфавите Z_k, $k \ge 2$, равно континууму.*

Доказательство. Как следует из лемм 7.11 и 7.12, для любого действительного ξ, $0 < \xi < 1$, бесконечное слово $\pi(\xi)(\pi_0, \pi_1, \ldots)$, построенное по правилу $\pi_n = \lfloor (n+1)\xi \rfloor - \lfloor n\xi \rfloor$, $n = 0, 1, \ldots,$ является плотным. Мощность множества действительных точек в интервале $(0, 1)$ равна континууму. Таким образом, предъявлен континуум бесконечных плотных слов в алфавите Z_2. Всякое такое слово является также и бесконечным плотным словом в алфавите Z_k, $k > 2$. С другой стороны, хорошо известно, что мощность множества всех бесконечных слов в алфавите конечной мощности также равна континууму. Тем самым лемма 7.13 доказана. □

Теорема 7.5. *Мощность множества минимальных бесконечных инвариантных классов (в первом или втором смыслах или по С. В. Яблонскому) равна континууму.*

Доказательство. Каждое бесконечное плотное слово в алфавите Z_k, содержащее по крайней мере две разных буквы, задает по теоремам 7.3 и 7.4 минимальный бесконечный инвариантный класс (в первом или втором смыслах или по С. В. Яблонскому). В лемме 7.13 показано, что мощность множества бесконечных плотных слов равна континууму, среди них из одной буквы состоят только k — конечное число. Проблема может заключаться в том, что разные плотные слова могут задавать один и тот же инвариантный класс. Так в следствии 7.2 указано, что если отбросить у плотного слова любое его начало, то оставшаяся часть будет задавать тот же самый инвариантный класс. Тем не менее оказывается, что плотные слова $\pi(\xi)$ в алфавите Z_2, рассматривавшиеся в леммах 7.11 и 7.12, при разных действительных ξ из интервала $(0,1)$ задают разные инвариантные классы. Заметим сначала, что из задания слова $\pi(\xi)$ видно, что его произвольное подслово $(\pi_m, \pi_{m+1}, \ldots, \pi_{m+s-1})$ длины s содержит ровно $\lfloor (m+s)\xi \rfloor - \lfloor m\xi \rfloor$ единиц. Несложно видеть, что $s\xi - 1 \le \lfloor (m+s)\xi \rfloor - \lfloor m\xi \rfloor \le s\xi + 1$. Пусть теперь ξ_1 и ξ_2 — различные действительные числа из интервала $(0,1)$, и $\xi_2 - \xi_1 = \varepsilon > 0$. Тогда любое подслово длины $\lceil \frac{3}{\varepsilon} \rceil$ слова $\pi(\xi_1)$ содержит не более $\xi_1 \lceil \frac{3}{\varepsilon} \rceil + 1$ единиц, а любое подслово длины $\lceil \frac{3}{\varepsilon} \rceil$ слова $\pi(\xi_2)$ содержит не менее $\xi_2 \lceil \frac{3}{\varepsilon} \rceil - 1 (\xi_1 + \varepsilon) \lceil \frac{3}{\varepsilon} \rceil - 1 > \xi_1 \lceil \frac{3}{\varepsilon} \rceil + 1$ единиц. Следовательно, бесконечные плотные слова $\pi(\xi_1)$ и $\pi(\xi_2)$ имеют разные множества подслов и тем самым задают разные минимальные бесконечные инвариантные классы. Таким образом, предъявлен континуум минимальных бесконечных инвариантных классов. Теорема 7.5 доказана. $\square$

Заключение

Изложенные в работе основные результаты автора состоят в следующем.

1. Установлена теорема, что для m-устойчивой неоптимальной булевой функции f при $m \leq n-3$ выполнено $nl(f) \leq 2^{n-1} - 2^{m+2}$. Корреляционно-иммунные и устойчивые булевы функции активно изучались, были получены некоторые описания, но оставалась, в частности, непроясненной связь с нелинейностью. Оценки $nl(f) \leq 2^{n-1} - 2^{m+1}$ для m-устойчивых и $nl(f) \leq 2^{n-1} - 2^{m+1}$ были получены автором, а также независимо в параллельных работах Саркара–Майтры и Зенга–Занга. В каждой из указанных работ есть дополнительные результаты, не содержащиеся в других работах. В частности, установленная теорема о верхней оценке нелинейности m-устойчивой неоптимальной булевой функции в параллельных работах Саркара–Майтры и Зенга–Занга получена не была.

2. Разработаны методы построения m-устойчивых функций от n переменных с максимально возможной нелинейностью $2^{n-1} - 2^{m+1}$, в частности, с использованием введенных подходящих и обобщенных подходящих матриц, что решило вопросы о существовании m-устойчивых функций, достигающих оценки нелинейности $nl(f) \leq 2^{n-1} - 2^{m+1}$ и эффективном построения таких функций.

3. С помощью этих разработанных автором методов построены m-устойчивые функции от n переменных с нелинейностью $2^{n-1} - 2^{m+1}$ при всех парах (m, n), удовлетворяющих неравенству $0{,}6n - 1 \leq m \leq n-2$, а асимптотически при $0,5789\ldots(1 + o(1)) \leq m/n$. Также автором разработаны эффективные методы схемной и программной реализации m-устойчивых функций от n переменных для криптографических примитивов и систем защиты информации.

4. Получена новая рекордная при $m > (n-3)/2$ нижняя оценка для аб-

солютной автокорреляционной характеристики m-устойчивой функции от n переменных: $\Delta_f \geq \left(\frac{2m-n+3}{n+1}\right) 2^n$. Важное значение имеют связи корреляционной иммунности с другими криптографически важными параметрами булевых функций; в частности, с ее автокорреляционными характеристиками. До автора уже было известно несколько оценок на глобальную автокорреляционную характеристику корреляционно-иммунных и m-устойчивых булевых функций.

5. Получен вид формул для числа корреляционно-иммунных и устойчивых порядка $m = n-k$ булевых функций от n переменных; доказано, что эта формула является полиномом степени $p(k)$; получены оценки на величину $p(k)$. Автор не ограничился получением собственно оценок на автокорреляционные характеристики, но и использовал автокорреляционные коэффициенты как мощное средство для получения других результатов. В частности, автор с их помощью получил верхнюю оценки на число нелинейных переменных в $(m = n - k)$-устойчивых булевых функциях высокого порядка: $n \leq (k-1)2^{k-2}$. Этот результат позволил в свою очередь получить вид формул для числа корреляционно-иммунных и устойчивых порядка $m = n - k$ булевых функций от n переменных; формула оказалась полиномом степени $p(k)$; были также получены оценок на величину $p(k)$. Заметим, что ранее были получены асимптотики лишь для числа корреляционно-иммунных функций малого порядка (константного или медленно растущего).

6. Построены платовидные функции с носителем спектра мощности 4^h и аффинным рангом $\mathbf{k}$ для любого натурального $\mathbf{k}$, удовлетворяющего неравенствам $2h \leq \mathbf{k} \leq 2^{h+1}-2$. Платовидные функции представляют большой интерес сами по себе и для построения различных классов криптографически важных функций. Так, бент-функции можно рассматривать как частный случай платовидных. Также платовидными неизбежно должны быть функции ограниченной алгебраической степенью с максимальной при этом устойчивостью. Шарпин и Карле исследовали кубические функции с максимальной устойчивостью (которые должны быть платовидными с мощностью носителя спектра 16) и получили некоторые оценки на их аффинный ранг. Автор нашел все возможные значения аффинного ранга платовидной функции с носителем спектра мощности 16: а именно 4, 5 и 6, в то время как оценка французов для подмножества функций

давала более широкий диапазон. Автор пошел в этом направлении еще дальше и построил для любого натурального $\mathbf{k}$, удовлетворяющего неравенствам $2h \leq \mathbf{k} \leq 2^{h+1} - 2$, платовидную функцию с носителем спектра мощности 4^h и аффинным рангом $\mathbf{k}$. До сих пор неизвестно, существует ли платовидная функция с параметрами вне этого диапазона.

7. Установлен факт, что при q, равном степени простого числа, для любого натурального m существует наименьшее натуральное $N = N_q(m)$, что при $n > N$ не существует A-примитивных разбиений $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n - m$. Получены нижние и верхние оценки на величину $N_q(m)$, найдено точное значение $N_q(2) = q + 1$; результаты того же типа получены для разбиений на грани. Среди конструкций платовидных вообще и бент-функций в частности, есть конструкции, в которых функция строится путем сборки из подфункций с непересекающимися носителями спектра. Если все исходные функции являются платовидными с одинаковым значением модуля ненулевых коэффициентов Уолша, то полученная функция снова будет платовидной. Если при этом объединение носителей спектра подфункций есть все пространство $\mathbf{F}_2^n$, то получается бент-функция. Однако проблемой является нахождение подходящего множества платовидных функций с непересекающимися носителями спектра. Оказывается, что если взять в качестве носителя спектра аффинное подпространство, то каждая платовидная функция с таким носителем спектра эквивалентна бент-функции от числа переменных, равных размерности аффинного подпространства; более того, между множествами таких функций существует взаимно-однозначное соответствие, которое задается аффинным преобразованием носителя спектра. В связи со сказанным выше, стала актуальной задача о разбиении пространства $\mathbf{F}_2^n$ на аффинные подпространства и подсчете числа таких разбиений. Поскольку существуют обобщения бент-функций с двоичного на q-ичный случай, автор также рассматривал разбиения пространства $\mathbf{F}_q^n$. Автор установил и доказал тот факт, что при q, равном степени простого числа, для любого натурального m существует наименьшее натуральное $N = N_q(m)$, что при $n > N$ не существует примитивных по Агиевичу разбиений $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n - m$. Автор также получил нижние и верхние оценки на величину $N_q(m)$, нашел точное зна-

чение $N_q(2) = q+1$; получил результаты того же типа для разбиений на грани. С помощью этих результатов автор получил вид асимптотических формул для числа разбиений (не обязательно примитивных по Агиевичу) пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств и граней при $m = \text{const}$, $n \to \infty$.

8. Установлен факт, что при больших n плотности l-уравновешенных функций близки к одному из следующих пяти чисел: 0, 1/3, 1/2, 2/3 или 1. Корреляционно-иммунные и устойчивые булевы функции являются функциями, единичные значения которых абсолютно равномерно распределены по подкубам заданной размерности $n - m$. Не всегда такое абсолютно равномерное распределение достижимо, особенно когда оно должно удовлетворять каким-то дополнительным требованиям. В то же время с практической точки зрения часто достаточно иметь не абсолютно равномерное, а почти равномерное распределение. Поэтому автор рассмотрел также булевы функции, количество единичных значений которых в однотипных подмножествах (подкубах и шарах) одинакового размера (но зато любого) различается не более чем на заданную величину l. Автор установил и доказал тот факт, что при больших n плотности l-уравновешенных функций близки к одному из следующих пяти чисел: 0, 1/3, 1/2, 2/3 или 1. Автор описал все булевы функции, равномерно распределенные по шарам со степенью 1, и точно подсчитал их количество.

9. Получен критерий, позволяющий по системе запрещенных подфункций, задающих инвариантный класс, определить, содержит ли этот класс бесконечное число существенно разных функций. Критерий сводит рассматриваемую задачу для функций к соответствующей задаче для множеств слов. Инвариантные классы булевых функций были введены С. В. Яблонским. Булевы функции из инвариантных классов не являются, вообще говоря, функциями с равномерно распределенными единичными значениями. Однако, тем не менее, многие рассматриваемые в предыдущих главах работы классы функций с равномерно распределенными единичными значениями являются инвариантными. Так, инвариантными являются класс $(n-k)$-устойчивых функций от n переменных (для заданного k) и класс l-уравновешенных функций (для заданного l). Тут, впрочем, надо сделать оговорку, что эти классы не являются инвариантными по классическому определению С. В. Яблонского, потому что они не замкнуты

относительно добавления фиктивных переменных. Поэтому надо или делать оговорку о том, что включаем вместе с функцией в класс все функции, получающиеся из нее добавлением фиктивной переменной, или просто исключить такое добавление из определения инвариантного класса. Этим главным образом и объясняется то, что наряду с классическим определением инвариантного класса по С. В. Яблонскому автор рассматривал и неклассические определения инвариантного класса, в которых операция добавления несущественной переменной не учитывается. Помимо того, что некоторые классы функций с равномерно распределенными единичными значениями являются инвариантными, важна также и общность методов и подходов. Так во многих рассуждениях предыдущих глав являлось важным, что если перейти от функции к ее подфункции, подставив, например, вместо переменной константу, или удалив линейную переменную из ее полинома, то снова получится функцию из того же класса. Этим и вызван интерес автора к инвариантным классам в данной работе, для которой, таким образом, инвариантные классы являются идейно близким объектом. Автор получил критерий, позволяющий по системе запрещенных подфункций, задающих инвариантный класс, определить, содержит ли этот класс бесконечное число существенно разных функций. Критерий сводит рассматриваемую задачу для функций к соответствующей задаче для множеств слов. Автор описал все минимальные бесконечные инвариантные классы и доказано, что число таких классов — континуум.

Таким образом, полученные автором в диссертации результаты, являются существенными продвижениями по широкому фронту направлений в решении проблемы обеспечения стойкости систем защиты информации против криптографических атак, среди которых выделяются различные виды корреляционных атак.

Список литературы

[1] Августинович С. В. О множестве запрещенных слов в символьных последовательностях, Второй Сибирский конгресс по прикладной и индустриальной математике (ИНПРИМ-96), Тезисы докладов, Новосибирск, Институт математики СО РАН, 1996, с. 111.

[2] Августинович С. В., Соловьева Ф. И., Хеден У. О разбиениях n-куба на неэквивалентные совершенные коды, Пробл. передачи информ. 2007. Т. 43, №4. С. 45–50.

[3] Ботев А. А., О взаимосвязи корреляционной иммунности и нелинейности для неуравновешенных булевых функций, Материалы XII Международной школы-семинара «Синтез и сложность управляющих систем», Пенза, 15–21 октября 2001 г, М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 1, с. 58–63.

[4] Гаврилов Г. П., Сапоженко А. А. Задачи и упражнения по курсу дискретной математики. 2-е изд. М.: Наука, 1992.

[5] Денисов О. В. Асимптотическая формула для числа корреляционно-иммунных порядка k булевых функций, Дискретная математика, 1991, Т. 3, вып. 2, с. 25–46.

[6] Денисов О. В. Локальная предельная теорема для распределения части спектра случайной двоичной функции, Дискретная математика, 2000, Т. 12, вып. 1, с. 82–95.

[7] Евдокимов А. А. Полные множества слов и их числовые характеристики,

Методы дискретного анализа в исследовании экстремальных структур, вып. 39, Новосибирск, Институт математики СО АН СССР, 1983, с. 7–19.

[8] Евдокимов А. А. Полнота множеств слов, Материалы всесоюзного семинара по дискретной математике и ее приложениям. М.: Изд-во МГУ, 1986, с. 112–116.

[9] Зимин А. И. Блокирующие множества термов, Математический сборник, Т. 119, № 3, 1982, с. 363–375.

[10] Касим-Заде О. М. О классах булевых функций, инвариантных относительно подстановки функций от одной переменной, Вестник Московского Университета, Серия 1, Математика, Механика, №3, 1995, с. 79–82.

[11] Кириенко Д. П. Полное описание неуравновешенных корреляционно-иммунных порядка 5 булевых функций от 9 переменных, Современные исследования в математике и механике. Труды XXIII конференции молодых ученых механико-математического факультета МГУ (9–14 апреля 2001 г.). Москва, 2001 г., Т. 2, с. 153–156.

[12] Кириенко Д. П. О неуравновешенных корреляционно-иммунных порядка 5 булевых функциях от 9 переменных, Материалы XII Международной школы-семинара «Синтез и сложность управляющих систем», Пенза, 15–21 октября 2001 г, М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 1, с. 110–115.

[13] Королев П. С. Квадратичные булевы функции высокого порядка устойчивости, Труды XXIII конференции молодых ученых механико-математического факультета МГУ (9–14 апреля 2001 г.). Москва, 2001 г., Т. 2, с. 186–191.

[14] Кузнецов Ю. В. О классах булевых функций, инвариантных относительно отождествления переменных, Докл. АН СССР, Т. 290, №4, 1986, с. 780–785.

[15] Кузнецов Ю. В. Исследование инвариантных классов, связанных с функциональными системами, Диссертация на соискание ученой степени к. ф.-м. н., М., 1987.

[16] Кузнецов Ю. В., Шкарин С. А. Коды Рида–Маллера (обзор публикаций), Математические вопросы кибернетики, Вып. 6, - М.: Наука, Физматлит, 1996, с. 5–50.

[17] Кузнецов Ю. В. О носителях платовидных функций, Материалы VIII Международного семинара «Дискретная математика и ее приложения» (2–6 февраля 2004 г.), М., Изд-во механико-математического факультета МГУ, 2004, с. 424-426.

[18] Липатов Е. П. Об одной классификации двоичных наборов и свойствах классов однородности, Проблемы кибернетики, вып. 39, М.: Наука, 1982, с. 67–84.

[19] Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В. Булевы функции в теории кодирования и криптологии. М: Ленанд, 2021. 576 с.

[20] Рыбников К. А. Введение в комбинаторный анализ. 2-е изд. М.: Изд. Моск. ун-та, 1985.

[21] Таранников Ю. В. Класс 1-уравновешенных функций и сложность его реализации, М., — Издательство Московского университета, Вестник Московского университета. Серия 1, Математика, Механика. 1991, N 2, с. 83–85.

[22] Таранников Ю. В. О множествах l-уравновешенных булевых наборов и функций, Диссертация на соискание ученой степени к. ф.-м. н., М., 1994.

[23] Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения, Saarbrucken, Germany: LAP LAMBERT Academic Publishing, 2011.

[24] Федорова М. С. О соотношениях между параметрами матриц специального вида, Современные исследования в математике и механике. Труды

XXIII конференции молодых ученых механико-математического факультета МГУ (9–14 апреля 2001 г.). Москва, 2001 г., Т. 3, с. 334–337.

[25] Федорова М. С. О неравенствах для параметров комбинаторных матриц специального вида, — Издательство Московского университета, Вестник Московского университета, Серия 15, Вычислительная математика и кибернетика, 2002, N 2, с. 45–49.

[26] Халявин А. В. О построении и оценках характеристик корреляционно-иммунных булевых функций и смежных комбинаторных объектов. Диссертация, Москва, 2011.

[27] Халявин А. В. Оценка мощности ортогональных массивов большой силы. Вестник Московского университета. Серия 1: Математика. Механика. — 2010. — №3. — с. 49–51.

[Перевод на английский язык: Khalyavin A. V. Estimates of the capacity of orthogonal arrays of large strength. Moscow University Mathematics Bulletin. — 2010. — Vol. 65, — pp. 130–131.]

[28] Халявин А. В. Оценка нелинейности корреляционно-иммунных булевых функций. Прикладная дискретная математика, Т. 11. №1, 2011, с. 34–69.

[29] Халявин А. В. Построение 4-корреляционно-иммунных булевых функций от 9 переменных с нелинейностью 240. Материалы X Международного семинара «Дискретная математика и ее приложения», Москва, МГУ, 1–6 февраля 2010 г. — М.: Изд-во мех-мат ф-та МГУ, 2010, с. 534–537.

[30] Яблонский С. В. О классах функций алгебры логики, допускающих простую схемную реализацию, Успехи матем. наук, 1957, Т. 12, №6, с. 189–196.

[31] Яблонский С. В. Об алгоритмических трудностях синтеза минимальных контактных схем, Проблемы кибернетики, вып. 2, М.: Физматгиз, 1959, с. 75–121.

[32] Ярыкина М. С. Несуществование двоичных кодов, равномерно распределенных по шарам, Дискретный анализ и исследование операций. — 2008. — Т. 15, No 2. — с. 65–97.

[33] Ященко В. В. О двух характеристиках нелинейности булевых отображений, Дискретный анализ и исследование операций, Серия 1, Т. 5, N 2, 1998, с. 90–96.

[34] Agievich S. Bent rectangles, Proceedings of the NATO advanced study institute on Boolean functions in cryptology and information security, Amsterdam: IOS Press, 2008. P. 3–22. (NATO science for peace and security Series D: Information and communication security, Vol. 18).

[35] Akman F., Sissokho P. A. Reconfiguration of subspace partitions, J. Comb. Des. 2022. Vol. 30, No. 1. P. 5–18.

[36] Anderson I., Finizio N. Whist tournaments, in: Colbourn C, L., Dinitz J. H. (Eds.), Handbook of combinatorial designs, 2nd edition, CRC Press, Boca Raton, Fl., 2007, pp. 690–695.

[37] Bierbrauer J. Bounds on orthogonal arrays and resilient functions, Journal of Combinatorial Designs, V. 3, 1995, pp. 179–183.

[38] Bierbrauer J., Gopalakrishnan K., Stinson D. R. Orthogonal arrays, resilient functions, error correcting codes and linear programming bounds, SIAM J. Discr. Math., V. 9, 1996, p. 424–452.

[39] Brouwer A. E. On associative block designs, Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), North-Holland, Amsterdam. 1978. Vol. 18. pp. 173–184.

[40] Brualdi R. A., Cai N., Pless V. S. Orphan structure of the first-order Reed-Muller codes, Discrete Mathematics, V. 102, pp. 239–247, 1992.

[41] Camion P., Canteaut A. Construction of t-resilient functions over a finite alphabet, Advanced in Cryptology, Eurocrypt '96, Lecture Notes in Computer Sciences, V. 1070, 1996, pp. 283–293.

[42] Camion P., Carlet C. , Charpin P., Sendrier N. On correlation-immune functions, Advances in Cryptology: Crypto '91, Proceedings, Lecture Notes in Computer Science, V. 576, 1991, pp. 86–100.

[43] Camion P., Courteau B., Delsarte Ph. On r-partition designs in Hamming spaces, Applicable Algebra in Engineering, Communications and Computing, V. 2, 1992, pp. 147–162.

[44] Canfield E. R., Gao Z., Greenhill C., McKay B. D., Robinson R. W. Asymptotic enumeration of correlation-immune Boolean functions, Cryptogr. Commun., Vol. 2, No 1, 2010, pp. 111–126.

[45] Canteaut A., Carlet C., Charpin P., Fontaine C. Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions, In Advanced in Cryptology: Eurocrypt 2000, Lecture Notes in Computer Science, V. 1807, 2000, pp. 507–522.

[46] Carlet C. Partially-bent functions, In Advanced in Cryptology: Crypto'92, Lecture Notes in Computer Science, V. 740, 1992, Springer-Verlag, pp. 280–291.

[47] Carlet C. On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions, Proceedings of SETA 2001 (Sequences and their Applications 2001), Discrete Mathematics and Theoretical Computer Science, 2001, Springer-Verlag, pp. 131–144.

[48] Carlet C. A larger class of cryptographic Boolean functions via a study of the Maiorana–McFarland construction, In Advanced in Cryptology: Crypto 2002, Lecture Notes in Computer Science, V. 2442, 2002, Springer-Verlag, pp. 549–564.

[49] Carlet C., Charpin P. Cubic Boolean functions with highest resiliency, IEEE Transactions on Information Theory, Vol. 51, No 2, 2005, pp. 562–571.

[50] Carlet C., Sarkar P. Spectral domain analysis of correlation immune and

resilient Boolean functions, Finite fields and Applications, V. 8, 2002, pp. 120–130.

[51] Carlet C. Boolean Functions for Cryptography and Coding Theory. Cambridge: Cambridge University Press, 2020.

[52] Chee S., Lee S., Lee D., Sung S. H. On the Correlation Immune Functions and their Nonlinearity, Advances in Cryptology — Asiacrypt'96, Lecture Notes in Computer Science, V. 1163, 1996, pp. 232–243.

[53] Chiarelli J., Hatami P., Saks M. An asymptotically tight bound on the number of relevant variables in a bounded degree Boolean function, Combinatorica, Vol. 40, 2020, pp. 237–244.

[54] Chor B., Goldreich O., Hastad J., Friedman J., Rudich S., Smolensky R. The bit extraction problem or t-resilient functions, IEEE Symposium on Foundations of Computer Science, V. 26, 1985, pp. 396–407.

[55] Cohen G, Honkala I., Lobstein A., Litsyn S. Covering codes. Elsevier, 1998.

[56] Courteau B., Montpetit A. Dual distances of completely regular codes, Discrete Mathematics V. 89, 1991, pp. 7–15.

[57] Cusick T. W. On constructing balanced correlation immune functions, in Sequences and Their Applications, Proceedings of SETA'98, Springer Discrete Mathematics and Theoretical Computer Science, 1999, pp. 184–190.

[58] Cusick T. W., Stanica P. Cryptographic Boolean Functions and Applications (Second Edition), Academic Press, 2017.

[59] Delsarte Ph. An algebraic approach to the association schemes of coding theory, Philips Research Reports Supplements, V. 10, 1973. [Русский перевод: Дельсарт Ф. Алгебраический подход к схемам отношений теории кодирования, М., Мир, 1976.]

[60] Delsarte Ph. Four fundamental parameters of a code and their combinatorial significance, Information and Control, V. 23, No 5, 1973, p. 407–438. [Русский

перевод: Дельсарт Ф., Четыре основных параметра кода и их комбинаторное значение, Кибернетический сборник, Новая серия, М., Мир, 1977, Вып. 14, с. 46–77.]

[61] Dobbertin H. Construction of bent functions and balanced Boolean functions with high nonlinearity, In B. Preneel, editor, Fast Software Encryption, Lecture Notes in Computer Sciences, Vol. 1008, 1994, pp. 61–74.

[62] Filiol E., Fontaine C. Highly Nonlinear Balanced Boolean Functions with a Good Correlation Immunity, Advanced in Cryptology, Eurocrypt '98, Helsinki, Finland, Lecture Notes in Computer Sciences, Vol. 1403, 1998, pp. 475–488.

[63] Fon-Der-Flaass D. G. A bound on correlation immunity. Siberian electronic mathematical reports. — 2007. — Vol. 4. — pp. 133–135.

[64] Friedman J. On the bit extraction problem, Proc. 33rd IEEE Symposium on Foundations of Computer Science, 1992, pp. 314–319.

[65] Fu S., Sun B., Li C., Qu L. Construction of odd-variable resilient Boolean functions with optimal degree, Journal of information science and engineering, Vol. 27, 2011, pp. 1931–1942.

[66] Gao S., Ma W., Zhao Y., Zhuo Z. Walsh spectrum of cryptographically concatenating functions and its applications in constructing resilient Boolean functions. Journal of Computational Information Systems Vol. 7, №4, 2011, pp. 1074–1081.

[67] Gilbert E. N. Lattice theoretic properties of frontal switching functions, Journal of Math. Phys., 1954, V. 33, N 1, pp. 57–67. [Русский перевод: Гильберт Э. Н. Теоретико-структурные свойства замыкающих переключательных функций, Кибернетический сборник. Вып. 1, М. ИЛ., 1960, с. ??–??.]

[68] Guo-Zhen X., Massey J. A spectral characterization of correlation-immune combining functions, IEEE Transactions on Information Theory, V. 34, No 3, May 1988, pp. 569–571.

[69] Hedayat A. S., Sloane N. J. A., Stufken J. Orthogonal Arrays: Theory and Applications, Springer-Verlag, New York, 1999.

[70] Heden O. A survey of the different types of vector space partitions, Discrete Math. Algorithms Appl. 2012. Vol. 4, No. 1. pp. 1–14.

[71] Heden O., Solov'eva F. Partitions of $\mathbf{F}^n$ into non-parallel Hamming codes, Advances in Math. of Communications. 2009. Vol. 3, No. 4. pp. 385–397.

[72] Kasami T., Tokura N., Azumi S. On the weight enumeration of weights less than $2.5d$ of Reed–Muller codes, Information and Control, Vol. 30 (4), April 1976, pp. 380–395.

[73] Kavut S., Yusel M., Maitra S., Construction of resilient functions by the concatenation of Boolean functions having nonintersecting Walsh spectra. Third International Workshop of Boolean functions, BFCA 07, May 2–3, 2007, Paris, France.

[74] Khalyavin A. Constructing Boolean functions with extremal properties. Proceedings of the NATO advanced study institute on Boolean functions in cryptology and information security, Amsterdam: IOS Press, 2008. P. 289-295. (NATO science for peace and security Series D: Information and communication security, Vol. 18).

[75] Krotov D. A partition of the hypercube into maximally nonparallel Hamming codes, J. Comb. Des. 2014. Vol. 22, No. 4. pp. 179–187.

[76] La Poutré J. A. A theorem on associative block designs, Discrete Math. 1986. Vol. 58, pp. 205–208.

[77] Levenshtein V. Split orthogonal arrays and maximum independent resilient systems of functions, Designs, Codes and Cryptography, V. 12, 1997, pp. 131–160.

[78] MacWilliams F. J. A theorem on the distribution of weights in a systematic code, Bell Syst. Tech. J., V. 42, 1963, pp. 79–94.

[79] MacWilliams F. J., Sloane N. J. A. The theory of error-correcting codes, North–Holland, Amsterdam, 1977. [Русский перевод: Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки, М., Связь, 1979.]

[80] Maitra S. Highly Nonlinear balanced Boolean functions with very good autocorrelation property, Cryptology ePrint archive (http://eprint.iacr.org/), Report 2000/047, September 2000, 11 pp.

[81] Maitra S. Correlation immunity goes against autocorrelation, Preprint, 2000, 11 pp.

[82] Maitra S. Autocorrelation properties of correlation immune Boolean functions, Progress in Cryptology — Indocrypt 2001, Chennai, India, December 16–20, 2001, Proceedings, Lecture Notes in Computer Science, V. 2247, pp. 242–253, Springer-Verlag, 2001.

[83] Maitra S., Sarkar P. Highly nonlinear resilient functions optimizing Siegenthaler's Inequality, Crypto '99, Lecture Notes in Computer Science, Vol. 1666, 1999, pp. 198–215.

[84] Mesnager S. Bent functions. Fundamentals and results. Cham: Springer, 2016.

[85] Minc H. Nonnegative matrices, New York: John Wiley and Sons, 1988.

[86] Mykkeltveit J. The covering radius of the $[128, 8]$ Reed–Muller code is 56, IEEE Transactions on Information Theory, V. 26, No 3, pp. 358–362, May 1980.

[87] Nešetřil J. Some nonstandard Ramsey-like applications, Theoret. Comput. Sci., V. 34, № 1–2, 1984, pp. 3–15.

[88] Nisan N., Szegedy M. On the degree of Boolean functions as real polynomials, Comput Complexity, Vol. 4, 1994, pp. 301–313.

[89] O'Donnell, R. Analysis of Boolean Functions, Cambridge: Cambridge University Press, 2014.

[90] Pasalic E., Johansson T. Further results on the relation between nonlinearity and resiliency for Boolean functions, IMA Conference on Cryptography and Coding, Lecture Notes in Computer Science, Vol. 1746, 1999, pp. 35–44.

[91] Pasalic E., Maitra S., Johansson T., Sarkar P. New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity, WCC2001 International Workshop on Coding and Cryptography, Paris, January 8–12, 2001, Electronic Notes in Discrete Mathematics, Volume 6, Elsevier Science, 2001.

[92] Patterson N. J., Wiedemann D. H. The covering radius of the $\left[2^{15}, 16\right]$ Reed–Muller code is at least 16276, IEEE Transactions on Information Theory, V. 29, No. 3, pp. 354–356, May 1983.

[93] Patterson N. J., Wiedemann D. H. Correction to [92], IEEE Transactions on Information Theory, V. 36, No. 2, p. 443, March 1990.

[94] Pei D., Qin W. The correlation of a Boolean function with its variables, Progress in cryptology — Indocrypt 2000, Lecture Notes in Computer Science, V. 1977, Springer-Verlag, 2000, pp. 1–8.

[95] Potapov V. N. DP-colorings of unifirm hypergraphs and splittings of Boolean hypercube into faces. Electron. J. Comb. V. 29, No 3, ID P3.37, 7 p. (2022).

[96] Ramsey F. P. On a problem of formal logic, Proc. London Math. Soc., Ser. 2, V. 30, 1930, pp. 264–286.

[97] Rao C. R. Factorial experiments derivable from combinatorial arrangements of array, Jour. Royal Statist. Soc., V. 9, 1947, p. 128–139.

[98] Riordan J. An introduction to combinatorial analysis, New York and etc., John Wiley & Sons, 1958. [Русский перевод: Риордан Дж. Введение в комбинаторный анализ. М.: Изд-во иностранной литературы, 1963.]

[99] Riordan J. Combinatorial identities, New York and etc., John Wiley & Sons, 1968. [Русский перевод: Риордан Дж. Комбинаторные тождества. М.: Наука, 1982.]

[100] Rivest R. L. On hash-coding algorithms for partial-match retrieval, Proceedings of the 15th Annual Symposium on Switching and Automata Theory, October 1974. 1974. pp. 95–103.

[101] Rosaz L. Unavoidable sets of words, Thèse de doctorat, Université Paris 7, 1993.

[102] Rothaus O. S. On bent functions, Journal of Combinatorial Theory, Series A, V. 20, 1976, pp. 300–305.

[103] Roy B. A brief outline of research on correlation immune functions, In Information security and privacy: 7th Australasian conference, ACISP 2002, Melbourne, Australia, July 3–5, 2002, Proceedings, Lecture Notes in Computer Science, V. 2384, 2002, pp. 379–394.

[104] Saber Z., Faisal Uddin M., Youssef A. On the existence of $(9, 3, 5, 240)$ resilient functions. IEEE Transactions on Information Theory, Vol. 52, №5, May, 2006, pp. 2269–2270, .

[105] Sanyal S. Near-optimal upper bound on Fourier dimension of Boolean functions in terms of Fourier sparsity, Automata, Languages, and Programming. 42nd Int. Colloquium, ICALP 2015, Kyoto, Japan, July 6–10, 2015. Proceedings. Part I. Springer, Berlin, 2015, pp. 1035–1045.

[106] Sanyal S. Fourier Sparsity and Dimension. Theory of Computing, Vol. 15, No 11, 2019, pp. 1–13.

[107] Sarkar P. Spectral domain analysis of correlation immune and resilient Boolean functions, Cryptology ePrint archive (http://eprint.iacr.org/), Report 2000/049, September 2000, 14 pp.

[108] Sarkar P., Maitra S. Construction of nonlinear Boolean functions with important cryptographic properties, In Advanced in Cryptology: Eurocrypt 2000, Lecture Notes in Computer Science, V. 1807, 2000, pp. 485–506.

[109] Sarkar P., Maitra S. Nonlinearity bounds and constructions of resilient Boolean functions, In Advanced in Cryptology: Crypto 2000, Proceedings, Lecture Notes in Computer Science, V. 1880, 2000, pp. 515–532.

[110] Schneider M. A Note on the Construction and Upper Bounds of Correlation-Immune Functions, 6th IMA International Conference, Cirencester, UK, Dec. 1997, Proceedings, Lecture Notes in Computer Science, V. 1355, 1997, pp. 295–306.

[111] Seberry J., Zhang X., Zheng Y. On Constructions and Nonlinearity of Correlation Immune Functions, Advances in Cryptology, Eurocrypt '93, Proceedings, Lecture Notes in Computer Science, V. 765, 1993, pp. 181–199.

[112] Shapiro G. S., Slotnik D. L. On the mathematical theory of error correcting codes, IBM J. Res. and Devel, V. 3, N 1, 1959, pp. 25–34. [Русский перевод: Шапиро Г. С., Злотник Д. Л. К математической теории кодов с исправлением ошибок, Кибернетический сборник, М., Изд-во иностр. лит., 1962, Вып. 5, с. 7–32.]

[113] Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications, IEEE Transactions on Information theory, V. IT-30, No 5, 1984, p. 776–780.

[114] Siegenthaler T. Decrypting a Class of Stream Ciphers Using Ciphertext Only, IEEE Transactions on Computer, V. C-34, No 1, Jan. 1985, pp. 81–85.

[115] Simon H.-U. A tight $\Omega(\log\log n)$-bound on the time for parallel RAM's to compute nondegenerated boolean functions, FCT'83, Lecture Notes in Computer Science, V. 158, 1984, p. 439–444.

[116] Singh D. Construction of highly nonlinear plateaued resilient functions with disjoint spectra. Mathematical Modelling and Scientific Computation. Communications in Computer and Information Science, Vol. 283, 2012, pp. 522–529.

[117] Van der Waerden B. L. Algebra, I, Springer-Verlag, Berlin etc., 1971 [Русский перевод: Ван дер Варден Б. Л. Алгебра. 2-е изд. М.: Наука, 1979].

[118] van Lint J. H. $\{0, 1, *\}$-distance problems in combinatorics, Surveys in combinatorics: invited papers for the tenth British Combinatorial Conference, Glasgow, UK, July 22-26, 1985, Ed. I. Anderson). 1985. Cambridge: Cambridge University Press, pp. 113–135.

[119] van Lint J. H., Wilson R. M. A Course in Combinatorics, Second Edition. Cambridge: Cambridge University Press, 2001. 602 c.

[120] Wang T., Liu M., Lin D. Construction of resilient and nonlinear Boolean functions with almost perfect immunity to algebraic and fast algebraic attacks. Information Security and Cryptology, Lecture Notes in Computer Science, Vol. 7763, 2013, pp. 276–293.

[121] Wegener I. The complexity of Boolean functions, Stutgart: B. G. Teubner, Chichester, John Wiley & Sons, 1987.

[122] Wellens J. Relationships between the number of inputs and other complexity measures of Boolean functions. Ithaca, NY: Cornell Univ., 2020. (Cornell Univ. Libr. e-Print Archive; arXiv:2005.00566).

[123] Zhang F., Carlet C., Hu Y., Zhang W., Secondary constructions of bent functions and highly nonlinear resilient functions. Ithaca, NY: Cornell Univ., 2012. (Cornell Univ. Libr. e-Print Archive; arXiv:1211.4191).

[124] Zhang X.-M., Zheng Y., GAC — the criterion for global avalanche characteristics of cryptographic functions, Journal of Universal Computer Science, V. 1, N 5, 1995, pp. 316–333. (http://www.jucs.org/)

[125] Zheng Y., Zhang X.-M. Plateaued functions, Proceedings of ICICS 1999, Lecture Notes in Computer Science, V. 1726, Springer-Verlag, 1999, pp. 284–300.

[126] Zheng Y., Zhang X. M. Improved upper bound on the nonlinearity of high order correlation immune functions, Selected Areas in Cryptography, 7th Annual International Workshop, SAC2000, Lecture Notes in Computer Science, V. 2012, pp. 264–274, Springer-Verlag, 2001.

[127] Zheng Y., Zhang X. M. New results on correlation immune functions, The 3nd International Conference on Information Security and Cryptology (ICISC 2000), Seoul, Korea, Lecture Notes in Computer Science, V. 2015, pp. 49–63, Springer-Verlag, 2001.

Работы автора по теме диссертации

Публикации в рецензируемых научных изданиях, индексируемых в базах данных Web of Science (WoS), Scopus, RSCI

[128] Тарannиков Ю. В. О числе единичных значений l-уравновешенных булевых функций, Дискретный анализ и исследование операций. 1995. Т. 2, N 1. с. 80–81.

[129] Тарannиков Ю. В. О некоторых оценках для веса l-уравновешенных булевых функций, Дискретный анализ и исследование операций. 1995. Т. 2, N 4. с. 80–96. [Перевод на английский язык: Tarannikov Yu. V. On certain bounds for the weight of l-balanced Boolean functions. Mathematics and Its Applications, V. 391, Korshunov A. D. (ed.), Operation Research and Discrete Analysis, 1997, 285–299.]

[130] Тарannиков Ю. В. О классе булевых функций, равномерно распределенных по шарам со степенью 1, М., — Издательство Московского университета, Вестник Московского университета, Серия 1, Математика, Механика, 1997, N 5, с. 17–21. [Перевод на английский язык: Tarannikov Yu. A class of Boolean functions homogeneously distributed over balls with degree 1. Moscow University Mathematics Bulletin. — 1997. — Vol. 52, №. 5. — pp. 18–22.]

[131] Carlet C., Tarannikov Yu. Covering sequences of Boolean functions and their

cryptographic significance, Designs, Codes and Cryptography, V. 25, 2002, pp. 263–279.

[132] Fedorova M., Tarannikov Yu. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices, Progress in Cryptology — Indocrypt 2001, Chennai, India, December 16–20, 2001, Proceedings, Lecture Notes in Computer Science, V. 2247, pp. 254–266, Springer-Verlag, 2001.

[133] Tarannikov Yu. On the structure and numbers of higher order correlation-immune functions, Proceedings of 2000 IEEE International Symposium on Information Theory ISIT2000, Sorrento, Italy, June 25–30, 2000, p. 185.

[134] Tarannikov Yu. On resilient Boolean functions with maximal possible nonlinearity, Proceedings of Indocrypt 2000, Lecture Notes in Computer Science, V. 1977, pp. 19–30, Springer-Verlag, 2000.

[135] Tarannikov Yu., Kirienko D. Spectral analysis of high order correlation immune functions, Proceedings of 2001 IEEE International Symposium on Information Theory ISIT2001, Washington, DC, USA, June 2001, p. 69.

[136] Tarannikov Yu., Korolev P., Botev A. Autocorrelation coefficients and correlation immunity of Boolean functions, Proceedings of Asiacrypt 2001, Gold Coast, Australia, December 9–13, 2001, Lecture Notes in Computer Science, V. 2248, pp. 460–479, Springer-Verlag, 2001.

[137] Tarannikov Y. New constructions of resilient Boolean functions with maximal nonlinearity, Fast Software Encryption, 8th International Workshop, FSE 2001, Yokohama, Japan, April 2–4, 2001. Revised Papers. Lecture Notes in Computer Science. Vol. 2355, pp. 66–77, Springer-Verlag, 2002.

[138] Fedorova M., Tarannikov Yu. On impossibility of uniform distribution of codewords over spheres in some cases, Proceedings of 2002 IEEE International Symposium on Information Theory ISIT2002, Lausanne, Switzerland, June 30 – July 05, 2002. — 2002. — p. 344–344.

[139] Таранников Ю. В. О значениях аффинного ранга носителя спектра платовидной функции. Дискретная математика. — 2006. — Т. 18, №3. — с. 120–137. [Перевод на английский язык: Tarannikov Yu. V. On values of the affine rank of the support of spectrum of a plateaued function. Discrete Mathematics and Applications. — 2006. — Vol. 16, №. 4. — pp. 401–421.]

[140] Tarannikov Yu. Generalized proper matrices and constructing of m-resilient Boolean functions with maximal nonlinearity for expanded range of parameters. Siberian electronic mathematical reports. — 2014. — Vol. 11. — pp. 229–245.

[141] Таранников Ю. В. О рангах подмножеств пространства двоичных векторов, допускающих встраивание системы Штейнера $S(2, 4, v)$. Прикладная дискретная математика. — 2014. — №1 (23). — с. 73–76.

[142] Sauskan A. V., Tarannikov Y. V. On packings of (n, k)-products. Siberian electronic mathematical reports. — 2016. — Vol. 13. — pp. 888–896.

[143] Khalyavin A. V., Lobanov M. S., Tarannikov Yu. V. On plateaued Boolean functions with the same spectrum support. Siberian electronic mathematical reports. —2016. — Vol. 13. — pp. 1346–1368.

[144] Баксова И. П., Таранников Ю. В. Оценки числа разбиений пространства $\mathbf{F}_2^m$ на аффинные подпространства размерности k. Вестник Московского университета. Серия 1: Математика. Механика. — 2022. — №3. — с. 21–25.

[Перевод на английский язык: Baksova I. P., Tarannikov Yu. V. The bounds on the number of partitions of the space $\mathbf{F}_2^{\boldsymbol{m}}$ into $\boldsymbol{k}$-dimensional affine subspaces. Moscow University Mathematics Bulletin. — 2022. — Vol. 77, №. 3. — pp. 131–135.]

[145] Таранников Ю. В. О существовании разбиений, примитивных по Агиевичу. Дискретный анализ и исследование операций. — 2022. — Т. 29, №4. — с. 104–123. [Перевод на английский язык: Tarannikov Y. V. On the existence of Agievich-primitive partitions. Journal of Applied and Industrial Mathematics. — 2022. — Vol. 16, №. 4.]

Публикации в рецензируемых научных изданиях, входивших в перечень ВАК Минобрнауки России

[146] Тарannиков Ю. В. О критериях бесконечности инвариантных классов дискретных функций, Математические вопросы кибернетики, Вып. 9, М., Физматлит, 2000, с. 59–78.

[147] Тарannиков Ю. В. О корреляционно-иммунных и устойчивых булевых функциях, Математические вопросы кибернетики / Под ред. О. Б. Лупанов. — Т. 11 из Математические вопросы кибернетики. — М.: Физматлит, 2002. — С. 91–148.

Другие публикации

[148] Тарannиков Ю. В. Класс 1-РРШ функций и сложность его реализации, Материалы XI Международной конференции «Проблемы теоретической кибернетики» 10–14 июня 1996 г., М., Рос. гос. гуманит. ун-т, 1996, с. 189–190.

[149] Тарannиков Ю. В. О весах l-уравновешенных булевых функций. В сб. Материалы VII межгосударственной школы-семинара «Синтез и сложность управляющих систем», Минск, 13–16/XI 1995. М: изд-во механико-математич. ф-та МГУ, 1996, с. 28.

[150] Тарannиков Ю. В. О классах булевых функций, единичные значения которых равномерно распределены по однотипным подмножествам. Второй Сибирский Конгресс по Прикладной и Индустриальной Математике, тезисы докладов, Новосибирск, Институт математики СО РАН, 1996, с. 126.

[151] Kasim-Zadeh O. M., Tarannikov Yu. V., Zykov K. A. Complexity and combinatorial aspects of informatics systems. In: Applied mathematics and computer science. Proceedings of the Conference on Applied Mathematics and Computer Science, 28–29 October 1996, Moscow, Russia. M: изд-во механико-математич. ф-та МГУ, 1997, p. 82–90.

[152] Тарапников Ю. В. Однородные булевы наборы и функции. Материалы Международных научных чтений по аналитической теории чисел и ее приложениям, состоявшихся на механико-математическом факультете МГУ им. М. В. Ломоносова 3–6 февраля 1997 года. М: изд-во механико-математич. ф-та МГУ, 1997, с. 31–33.

[153] Tarannikov Yu. Limit values for the density of l-balanced k-valued functions defined over the Boolean cube, International Symposium on Combinatorial Optimization, Bruxelles, 15–17 April 1998, p. 191.

[154] Тарапников Ю. В. О предельных значениях плотности l-уравновешенных k-значных функций, заданных на булевом кубе, Международная Сибирская конференция по исследованию операций, Новосибирск, 22–27 июня 1998 г., с. 140.

[155] Тарапников Ю. В. О корреляционно-иммунных булевых функциях наивысших порядков, Проблемы теоретической кибернетики. Тезисы докладов XII Международной конференции. (Нижний Новгород, 17–22 мая 1999 г.), Москва, Изд-во механико-математического факультета МГУ, 1999, с. 223.

[156] Тарапников Ю. В. О структуре и числе корреляционно-иммунных функций наивысших порядков, Материалы IX Межгосударственной школы-семинара «Синтез и сложность управляющих систем» (Нижний Новгород, 16–19 декабря 1998 г.), Москва, Изд-во механико-математического факультета МГУ, 1999, с. 81–92.

[157] Tarannikov Yu. Ramsey-like theorems on the structure and numbers of higher order correlation-immune functions, Moscow State University, French-Russian Institute of Applied Mathematics and Informatics, Preprint No 5, Moscow, October 1999, 20 pp.

[158] Tarannikov Yu. On a method for the constructing of cryptographically strong Boolean functions, Moscow State University, French-Russian Institute of

Applied Mathematics and Informatics. Preprint No 6, Moscow, October 1999, 24 pp.

[159] Tarannikov Yu. On resilient Boolean functions with maximal possible nonlinearity, Cryptology ePrint archive (http://eprint.iacr.org/), Report 2000/005, March 2000, 18 pp.

[160] Tarannikov Yu. On some connections between codes and cryptographic properties of Boolean functions, Proceedings of Seventh International Workshop on Algebraic and Combinatorial Coding Theory, Bansko, Bulgaria, June 18–24, 2000, pp. 299–304.

[161] Tarannikov Yu., Kirienko D. Spectral analysis of high order correlation immune functions, Cryptology ePrint archive (http://eprint.iacr.org/), Report 2000/050, October 2000, 8 pp.

[162] Tarannikov Yu. New constructions of resilient Boolean functions with maximal nonlinearity, Cryptology ePrint archive (http://eprint.iacr.org/), Report 2000/069, December 2000, 11 pp.

[163] Таранников Ю. В. Одно естественное обобщение теоремы о максимальном паросочетании в двух соседних слоях булева куба является неверным, Материалы XI Межгосударственной школы-семинара «Синтез и сложность управляющих систем», Нижний Новгород, 20–25 ноября 2000 г., М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 2, с. 173–176.

[164] Таранников Ю. В., Кириенко Д. П. Спектральный анализ корреляционно-иммунных функций высокого порядка, Материалы XI Межгосударственной школы-семинара «Синтез и сложность управляющих систем», Нижний Новгород, 20–25 ноября 2000 г., М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 2, с. 177–189.

[165] Таранников Ю. В. Числовые характеристики булевых функций, Дискретная математика и ее приложения. Сборник лекций молодежных научных

школ по дискретной математике и ее приложениям, М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 1, с. 129–144.

[166] Тарасников Ю. В. Об автокорреляционных свойствах корреляционно-иммунных функций, Материалы VII международного семинара «Дискретная математика и ее приложения» (29 января — 2 февраля 2001 г.), М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 3, с. 331–333.

[167] Тарасников Ю. В. Несуществование неуравновешенных неконстантных корреляционно-иммунных порядка m булевых функций от n переменных при $m > 0.75n - 1.25$, Материалы XII Международной школы-семинара «Синтез и сложность управляющих систем», Пенза, 15–21 октября 2001 г, М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 2, с. 212–218.

[168] Fedorova M., Tarannikov Yu. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices, Cryptology ePrint archive (http://eprint.iacr.org/), Report 2001/083, October 2001, 16 pp.

[169] Тарасников Ю. В. Теорема типа теоремы Симона–Вегенера для регулярных булевых функций. Проблемы теоретической кибернетики. Тезисы докладов XIII Международной конференции (Казань, 27–31 мая 2002 г.). — Проблемы теоретической кибернетики. — М.: Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2002. — с. 175.

[170] Тарасников Ю. В. О построении корреляционно-иммунных и устойчивых булевых функций. Труды V Международной конференции «Дискретные модели в теории управляющих систем» (26–29 мая 2003 г.). — М.: МАКС Пресс Москва, 2003. — с. 84–85.

[171] Тарасников Ю. В. Об аффинном ранге платовидных функций. Труды VI Международной конференции «Дискретные модели в теории управляющих систем» (7–11 декабря 2004 г.). — М.: МАКС Пресс, 2004. – с. 259–262.

[172] Тарannиков Ю. В. О платовидных устойчивых булевых функциях. Материалы VIII Международного семинара «Дискретная математика и ее приложения», 2–6 февраля 2004 г., Москва, —М.: МГУ, 2004. — с. 431–435.

[173] Тарannиков Ю. В. О новых конструкциях нелинейных фильтров для поточных шифраторов и их устойчивости против стандартных и новых криптографических атак. Математика и безопасность информационных технологий. Материалы конференции в МГУ 23–24 октября 2003 г. — М.: МЦНМО, 2004. — с. 160–164.

[174] Тарannиков Ю. В. О значениях аффинного ранга носителя спектра платовидных функций. Математика и безопасность информационных технологий. Материалы конференции в МГУ 28–29 октября 2004 г. — М.: МЦНМО, 2005. — с. 226–231.

[175] Tarannikov Yu. On affine rank of spectrum support for plateaued function. Cryptology ePrint archive (http://eprint.iacr.org/), Report 2005/399, November 2005, 22 pp.

[176] Тарannиков Ю. В. Алгебраические атаки на потоковые шифры и алгебраическая иммунность булевых функций. Материалы международной научной конференции по проблемам безопасности и противодействия терроризму. — М.: МНЦМО, 2006. — с. 132–140.

[177] Tarannikov Yu. On correlation immune Boolean functions. Proceedings of the NATO advanced study institute on Boolean functions in cryptology and information security, Amsterdam: IOS Press, 2008. P. 219–231. (NATO science for peace and security Series D: Information and communication security, Vol. 18).

[178] Тарannиков Ю. В. Описание одного класса рекурсивных конструкций булевых функций. Современные проблемы математики, механики и их приложений. Материалы международной конференции, посвященной 70-летию ректора МГУ академика В. А. Садовничего. — М.: Университетская книга, 2009. — с. 401.

[179] Тарannиков Ю. В. Корреляционная иммунность и другие криптологические свойства булевых функций. Современные проблемы математики и механики. Т. III. Математика. Вып. 3. Дискретная математика. — М.: Изд-во Московского университета, 2009. — с. 95–142.

[180] Тарannиков Ю. В. О верхней оценке аффинного ранга носителя спектра платовидной функции. Материалы X Международного семинара «Дискретная математика и ее приложения» (Москва, 1–6 февраля 2010 г.). — М.: Изд-во механико-математического факультета МГУ, 2010. — с. 529–531.

[181] Тарannиков Ю. В. Комбинаторные свойства дискретных структур и приложения к криптологии. — М.: МЦНМО, 2011. — 152 с.

[182] Тарannиков Ю. В. О булевых функциях из пересечения нескольких специальных классов. 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 мех.-мат. ф-та МГУ, 2012. — с. 433–436.

[183] Tarannikov Yu. Generalized proper matrices and constructing of m-resilient Boolean functions with maximal nonlinearity for expanded range of parameters. Cryptology ePrint archive (http://eprint.iacr.org/), Report 2014/164, March 2014, 19 pp.

[184] Тарannиков Ю. В. Несократимые разложения однородных произведений двучленов для построения m-устойчивых функций с максимально возможной нелинейностью. Проблемы теоретической кибернетики. Материалы XVII Международной конференции (Казань, 16–20 июня 2014 г.). — Проблемы теоретической кибернетики. — Казань: Отечество, 2014. — с. 271–272.

[185] Тарannиков Ю. В. О возможности построения m-устойчивых функций с оптимальной нелинейностью в рамках одного метода. Материалы XII Международного семинара «Дискретная математика и ее приложения»

имени академика О. Б. Лупанова (Москва, МГУ, 20–25 июня 2016 г.). — М.: Изд-во механико-математического факультета МГУ Москва, 2016. — с. 394–397.

[186] Тарannиков Ю. В. On plateaued Boolean functions with the same spectrum support. Graphs and Groups, Spectra and Symmetries, 2016: Abstracts of the International Conference and PhD-Master Summer School on Graphs and Groups, Spectra and Symmetries. Novosibirsk: Sobolev Institute of Mathematics, 2016. — p. 38.

[187] Баксова И. П., Тарannиков Ю. В. Об одной конструкции бент-функций. Обозрение прикладной и промышленной математики. — 2020. — Т. 27, №1. — с. 64–66.

[188] Potapov V. N., Taranenko A. A., Tarannikov Yu. V. Asymptotic bounds on numbers of bent functions and partitions of the Boolean hypercube into linear and affine subspaces. Ithaca, NY: Cornell Univ., 2021. (Cornell Univ. Libr. e-Print Archive; arXiv:2108.00232).

[189] Тарannиков Ю. В. О существовании A-примитивных разбиений. Материалы XIV Международного семинара «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (Москва, МГУ, 20–25 июня 2022 г.). — М., 2022. — с. 285–288.