МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

На правах рукописи

Царегородцев Кирилл Денисович

Правильные семейства функций и порождаемые ими квазигруппы: комбинаторные и алгебраические свойства

Специальность 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научные руководители:
кандидат физико-математических наук
Панкратьев Антон Евгеньевич
кандидат физико-математических наук
Галатенко Алексей Владимирович

Москва — 2025

Оглавление

Стр.

Стр.

Введение

Диссертация посвящена вопросам, лежащим на стыке дискретной математики (теория дискретных функций), алгебры (теория квазигрупп) и криптографии. Основным объектом изучения является особый класс дискретных функций, введенных В. А. Носовым [1; 2] (т.н. «правильные семейства» функций), которые могут быть использованы для построения параметрических классов квазигрупп. Квазигруппы — одна из базовых структур в алгебре. Таблицы умножения квазигрупп, более известные под названием «латинские квадраты», с древнейших времен и по настоящее время используются в различных областях математики (см., например, монографию Й. Денеша и Э.Д. Кидвелла [3]): при планировании статистических экспериментов, в играх и головоломках, а также в теории кодирования и криптографии, которые рассматриваются более подробно в настоящей работе. Из общих обзоров криптографических приложений квазигрупп можно отметить следующие источники:

- статья М.М. Глухова [4], в которой приводятся примеры кодов аутентификации, шифров и однонаправленных функций на основе квазигрупповых преобразований, а также недавний обзор индийских авторов [5], затрагивающий тематику построения симметричных криптопримитивов на основе квазигрупповых операций;
- монография В. Щербакова [6], в которой довольно подробно освещена тематика использования квазигрупп в криптографии; в частности, в работе рассматриваются следующие темы: поточные шифры и их криптоанализ, хэш-функции и односторонние функции, схемы разделения секрета; а также смежная тематика теории кодирования (в частности, рекурсивные МДР-коды);
- монография Й. Денеша и Э.Д. Кидвелла [3] и статья М.Э. Тужилина [7], посвященные общим обзорам тематики латинских квадратов, их использованию в докомпьютерный этап развития криптографии и современным приложениям.

В качестве непосредственного приложения квазигрупп в области симметричной криптографии можно привести следующие механизмы, основанные на квазигрупповых операциях, предлагаемые к рассмотрению в статьях македонских авторов С. Марковски, Д. Глигороски, В. Димитровой, А. Милевой и т.д.:

– поточные шифры и хэш-функции, основанные на квазигрупповом умножении [8—11],
– кандидат на стандартизацию в качестве поточного шифра **Edon80** [12],
– кандидаты на стандартизацию в качестве хэш-функции **Edon-R** [13; 14] и **NaSHA** [15; 16],
– кандидаты на стандартизацию в качестве низкоресурсной хэш-функции и алгоритма шифрования с ассоциированными (присоединенными) данными (AEAD-алгоритм) **GAGE** и **InGAGE** [17; 18],
– предложения Г. Теселеану [19—21] и И.В. Чередника [22—24] по использованию квазигрупповых операций в рамках (обобщенных) сетей Фейстеля.

Однако недостаточная изученность задач, лежащих в основании подобных предложений, иногда приводит к возможности довольно простого криптоанализа полученных решений (см. работы М. Войводы и И. Сламинковой [25—27], М. Хелла и Т. Йохансона [28], И. Николича и Д. Ховратовича [29], Ж. Ли и соавторов [30]).

Квазигруппы (а также более сложные алгебраические структуры, в основе которых лежат квазигруппы) и их приложения в теории кодирования исследовались в ряде работ за авторством С. Гонсалеса, Е. Коусело, В.Т. Маркова, А.А. Нечаева, А.В. Михалёва, А.В. Грибова и других. Так, в статье [31] исследуются k-рекурсивные коды (т.е. коды, для которых позиции в кодовых словах с номерами $i + k$ однозначно определяются по позициям $i, i + 1, \ldots, i + k - 1$ для $i = k + 1, \ldots, n - k$, иначе говоря, $u_{i+k} = f(u_i, \ldots, u_{i+k-1})$), лежащие на границе Синглтона (МДР-коды). Подход, основанный на применении ортогональных латинских квадратов, позволяет получить в данном случае оценки на максимальную длину кодовых слов. В серии работ [32—35] используются так называемые луповые кольца (формальные суммы квазигрупповых элементов) для построения различных оптимальных в разных смыслах кодов.

Луповые кольца и другие алгебраические структуры, основанные на квазигруппах, могут быть использованы для построения множества асимметричных криптографических примитивов. Такие конструкции исследовались С.Ю. Катышевым, В.Т. Марковым, А.А. Нечаевым, А.В. Михалёвым, А.В. Барышниковым, А.В. Грибовым, А.В. Зязиным, Е.С. Кислициным и другими авторами. В качестве примера можно привести следующие криптографические схемы и протоколы:

– протоколы формирования общего ключа — аналоги протокола Диффи-Хеллмана [36—39];
– схемы асимметричного шифрования [34; 40; 41];
– схемы гомоморфного шифрования [41—44].

Отдельно можно выделить ряд работ, в которых изучаются схемы асимметричного шифрования и цифровой подписи, основанные на сложности решений систем уравнений в конечных полях (см. работы Д. Глигороски, С. Марковски, С. Кнапского, Й. Ченя и других [45—48]).

При этом применяемые в области защиты информации квазигруппы часто имеют довольно большие размеры (см., например, требования к квазигруппе в работах Д. Глигороски и соавторов [13; 14; 47]), что делает затруднительным поэлементное хранение в памяти компьютера всей таблицы умножения. Так, например, для построения хэш-функции Edon-$\mathcal{R}'$ необходимо задать квазигруппу порядка 2^{256}. В связи с этим обстоятельством в большинстве предлагаемых криптосистем большая квазигруппа строится, как правило, согласно одному из следующих подходов:

– случайная генерация квазигруппы (случайных поиск подходящей квазигруппы совместно с процедурой отсева неподходящих) из некоторого узкого класса (Д. Глигороски и соавторы [45; 47]);
– итеративное построение большой квазигруппы из квазигрупп меньшего размера (Д. Глигороски и соавторы [14], А.В. Грибов [41]) с помощью конструкций произведений;
– изотопы некоторых «хорошо изученных» групп: например, изотоп группы точек эллиптической кривой (В.Т. Марков, А.В. Михалёв, А.А. Нечаев [37]), модульное вычитание (В. Снашель и соавторы [11]);
– функциональное задание квазигруппы, рассматриваемое в настоящей работе более подробно.

В работах В.А. Носова [1; 2] был предложен метод задания латинского квадрата при помощи семейства булевых функций, которое определяет элемент квадрата по его координатам (номеру строки и столбца). Такие семейства функций, задающие целые параметрические классы латинских квадратов, были названы правильными. Понятие правильного семейства функций было сначала обобщено на случай абелевых групп (см. работы В.А. Носова, А.Е. Панкратьева, А.А. Козлова [49—53]), а затем и на более общие алгебраические структуры

(см. работы И.А. Плаксиной [54] и А.В. Галатенко, В.А. Носова, А.Е. Панкратьева[55]). Ряд работ посвящен изучению свойств введенных булевых отображений:

– В.А. Носовым [1] было (среди прочего) показано, что проверка свойства правильности является coNP-полной задачей (т.е. в общем случае задача проверки правильности является сложной),
– в работах В.А. Носова, А.Е. Панкратьева, А.А. Козлова [51—53] рассматривались свойства т.н. графа существенной зависимости правильных семейств (граф на n вершинах, ребро $i \to j$ присутствует в графе тогда и только тогда, когда j-я функция семейства зависит существенно от x_i) и были выделены широкие классы семейств, для которых свойство правильности эквивалентно свойству отсутствия циклов в графе существенной зависимости,
– в работах Д.О. Рыкова [56; 57] показано, как задача проверки свойства правильности может быть упрощена, если дополнительно известна структура графа существенной зависимости семейства,
– работы И.А. Плаксиной [54] и А.В. Галатенко, В.А. Носова, А.Е. Панкратьева [55] посвящены, в том числе, различным способам задания (d-)квазигрупп с помощью правильных семейств над различными алгебраическими структурами,
– работы А.В. Галатенко, В.А. Носова, А.Е. Панкратьева, В.М. Староверова [58; 59] посвящены вопросам построения новых правильных семейств функций из старых.

При этом не всякая квазигруппа подходит для реализации на ее основе криптографических примитивов. Критически важными являются алгебраические свойства используемой квазигруппы, такие как свойства полиномиальной полноты (И. Хагеманн, К. Херрман [60]; Т. Нипков [61]; Г. Хорвац и соавторы [62]; В.А. Артамонов и соавторы [63]), количество ассоциативных троек (Т. Кепка [64]; А. Котзиг, К. Райшер [65]; Ж. Жезек, Т. Кепка [66]), наличие подквазигрупп (см., например, работу П.И. Собянина [67] и А.В. Галатенко, А.Е. Панкратьева, В.М. Староверова [68]). В ряде работ изучаются свойства квазигрупп, порождаемых правильными семействами булевых функций:

– Н.А. Пивнем [69] исследуются алгебраические свойства квазигрупп размера 4, порождаемых правильными семействами булевых функций размера $n = 2$, вводится понятие «перестановочной конструкции» (способ получения новых квазигрупп из уже имеющихся),

– в работе Н.А. Пивня [70] рассмотрена избыточность «перестановочной конструкции» (различные значения параметров могут давать одну и ту же квазигруппу) и способы сокращения избыточности,
– в работе А.В. Галатенко, В.А. Носова, А.Е. Панкратьева [71] предложен способ построения квадратичных квазигрупп, которые являются оптимальными с точки зрения криптографических приложений (обладают наиболее компактным представлением, при этом задача решения систем уравнений над подобными квазигруппами является в общем случае сложной),
– в дипломной работе А.С. Шварёва [72], среди прочего, рассмотрены «криптографические» свойств квазигрупп, порождаемых правильными семействами (линейная, дифференциальная характеристики) и способы их «усиления».

В контексте проведенных исследований остаются актуальными ряд нерешенных задач, исследованию которых и посвящена настоящая работа:

– изучение правильных семейств и их свойств как одного из возможных способов функционального задания квазигрупповой операции,
– изучение свойств квазигрупп, порождаемых правильными семействами.

Целью исследования является изучение свойств правильных семейств функций, а также алгебраических свойств квазигрупп, заданных правильными семействами функций. Тема, объект и предмет диссертационной работы соответствуют следующим пунктам паспорта специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика: теория алгебраических структур (полугрупп, групп, колец, полей, модулей и т.д.), теория дискретных функций и автоматов, теория графов и комбинаторика.

Для достижения поставленной цели автору необходимо было решить следующие **задачи**:

1. Получение новых критериев правильности семейств функций, а также установление естественного соответствия между правильными семействами функций и другими комбинаторно-алгебраическими структурами.
2. Исследование общих свойств правильных семейств функций, включая структуру множества неподвижных точек, а также стабилизатор относительно определенных классов преобразований.

3. Нахождение новых классов правильных семейств и изучение их свойств, включая мощность класса и мощность образа представителей.
4. Разработка нового способа построения квазигрупп на основе правильных семейств функций, создание шифра, сохраняющего формат, на основе этой конструкции, и анализ характеристик полученного шифра.

Научная новизна: результаты диссертации являются новыми и получены автором самостоятельно. Все результаты, выносимые автором на защиту, получены им лично. Результаты других авторов, используемые в диссертации, отмечены соответствующими ссылками. Основные результаты диссертации состоят в следующем.

1. Установлено естественное соответствие между булевыми правильными семействами и одностоковыми ориентациями графов булевых кубов (USO-ориентации), а также между булевыми правильными семействами и булевыми сетями с наследственно единственной неподвижной точкой (HUFP-сети); установлено естественное соответствие между правильными семействами в логике произвольной значности и кликами в обобщенных графах Келлера.
2. Доказано, что стабилизатором множества правильных семейств функций являются изометрии пространства Хэмминга (согласованные перенумерации и перекодировки); показано, что отображения, задаваемые с помощью правильных семейств булевых функций, всегда имеют четное число неподвижных точек; получена оценка на число правильных семейств булевых функций, предложены оценки доли треугольных семейств среди всех правильных семейств булевых функций.
3. Построены новые классы правильных семейств функций (рекурсивно треугольные, локально треугольные, сильно квадратичное семейство); получены оценки на число рекурсивно треугольных семейств; для некоторых правильных семейств булевых функций получены точные значения мощности образа отображений, задаваемых этими правильными семействами.
4. Предложен новый способ порождения квазигрупп на основе правильных семейств функций; доказан ряд утверждений о числе ассоциативных троек в порождаемых квазигруппах; предложен новый алгоритм шифрования, сохраняющего формат (FPE-схема), основанный на квазигрупповых операциях.

Методология и методы исследования. В работе используются методы алгебры, дискретной математики, криптографии, теории графов, теории сложности.

Основные положения, выносимые на защиту:

1. Между булевыми правильными семействами и одностоковыми ориентациями графов булевых кубов (USO-ориентациями), а также между булевыми правильными семействами и булевыми сетями с наследственно единственной неподвижной точкой (HUFP-сетями) существует естественное соответствие. Между правильными семействами в логике произвольной значности и кликами в обобщенных графах Келлера также существует естественное соответствие.
2. Стабилизатор множества правильных семейств функций представляет собой множество пар согласованных изометрий пространства Хэмминга (согласованных перенумераций и перекодировок).
3. Отображения, задаваемые правильными семействами булевых функций, всегда имеют четное число неподвижных точек.
4. Мощность множества правильных семейств булевых функций размера n $T(n)$ удовлетворяет отношению $\log_2(T(n)) = \Theta\left(2^n \cdot \log_2(n)\right)$. Треугольные семейства составляют бесконечно малую долю среди всех правильных семейств булевых функций.
5. Локально треугольные, рекурсивно треугольные и сильно квадратичное семейства являются правильными. Мощность образов рассмотренных в работе квадратичных булевых правильных семейств близка к максимально возможной.
6. Предложенная в работе конструкция позволяет порождать квазигруппы с помощью правильных семейств функций. Алгоритм шифрования, построенный на основе этой конструкции, сохраняет формат исходных сообщений (является FPE-схемой). Ряд утверждений о числе ассоциативных троек в квазигруппах, построенных на основе предложенной конструкции, позволяет свести вопрос об изучении индексов ассоциативности от всех пар правильных семейств к классам эквивалентности пар правильных семейств.

Достоверность полученных результатов обеспечивается строгими математическими доказательствами. Результаты работы докладывались на научных конференциях, опубликованы в рецензируемых научных журналах и находятся в соответствии с результатами, полученными другими авторами. Результаты дру-

гих авторов, используемые в диссертации, отмечены соответствующими ссылками.

Апробация работы. Основные результаты работы докладывались на следующих международных и всероссийских конференциях:

1. XXVI Международная конференция студентов, аспирантов и молодых учёных «Ломоносов», Москва, Россия, с 8 по 12 апреля 2019 г.;
2. X симпозиум «Современные тенденции в криптографии» (CTCrypt 2021), Дорохово, Россия, с 1 по 4 июня 2021 г.;
3. XI симпозиум «Современные тенденции в криптографии» (CTCrypt 2022), Новосибирск, Россия, с 6 по 9 июня 2022 г.;
4. Четырнадцатый международный семинар «Дискретная математика и ее приложения» имени академика О.Б. Лупанова под руководством В. В. Кочергина, Э. Э. Гасанова, С. А. Ложкина, А. В. Чашкина, с 20 по 25 июня 2022 г.;
5. 11-я Международная конференция «Дискретные модели в теории управляющих систем», Красновидово, Россия, с 26 по 29 мая 2023 г.;
6. Третья Международная конференция “MATHEMATICS IN ARMENIA: ADVANCES AND PERSPECTIVES”, Ереван, Армения, со 2 по 8 июля 2023 г.;
7. 22-я Международная конференция «Сибирская научная школа-семинар “Компьютерная безопасность и криптография” имени Геннадия Петровича Агибалова», Барнаул, Россия, с 4 по 9 сентября 2023 г.;
8. Международная конференция «Математика в созвездии наук», Москва, Россия, с 1 по 2 апреля 2024 г.;
9. Международная конференция «Алгебра и математическая логика: теория и приложения», Казань, Россия, с 27 июня по 1 июля 2024 г.;
10. XX Международная научная конференция «Проблемы теоретической кибернетики», Москва, Россия, с 5 по 8 декабря 2024 г.

Результаты работы докладывались и обсуждались на заседаниях следующих научных семинаров:

1. научно-исследовательский семинар по алгебре механико-математического факультета МГУ под руководством Д. О. Орлова, М. В. Зайцева, 2023 г.;
2. научно-исследовательский семинар «Математические вопросы кибернетики» кафедр дискретной математики и математической теории интеллектуальных систем механико-математического факультета и ма-

тематической кибернетики факультета вычислительной математики и кибернетики МГУ под руководством Э. Э. Гасанова, В. В. Кочергина, С. А. Ложкина, 2023 г.;

3. семинар «Компьютерная алгебра» факультета ВМК МГУ и ВЦ РАН под руководством профессора С. А. Абрамова, 2023 г.;
4. семинар «Теория автоматов» механико-математического факультета МГУ под руководством профессора Э. Э. Гасанова, 2023 г.;
5. семинар «Современные проблемы криптографии» под руководством ведущего научного сотрудника В. А. Носова и доцента А. Е. Панкратьева, механико-математический факультет МГУ, неоднократно;
6. семинар «Компьютерная безопасность» под руководством старшего научного сотрудника А.В. Галатенко, механико-математический факультет МГУ, неоднократно.

Публикации. Основные результаты по теме диссертации изложены в 9 печатных изданиях [73—81], 8 из которых ([73—80]) опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика, из них 6 — в рецензируемых научных изданиях, входящих в ядро РИНЦ и международные базы цитирования (Web of Science / Scopus), RSCI ([73—78]), 2 — в рецензируемых научных изданиях из дополнительного списка МГУ, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика и входящих в список ВАК ([79; 80]).

Объем и структура работы. Диссертация состоит из введения, 4 глав и заключения. Полный объём диссертации составляет 143 страницы, включая 5 рисунков и 9 таблиц. Список литературы содержит 171 наименование.

Глава 1. Основные определения и обозначения

В настоящей главе мы приведем основные определения, необходимые для дальнейшего рассмотрения. В разделе 1.1 приведены основные обозначения, используемые на протяжении всей работы. Раздел 1.2 посвящен введению базовых понятий (d-)квазигруппы и семейства отображений. В разделе 1.3 вводится основной объект исследования — правильные семейства функций. В разделе 1.4 кратко рассматриваются основные характеристики квазигрупп, важные в контексте криптографических приложений (индекс ассоциативности, полиномиальная полнота, наличие подквазигрупп).

Отдельно рассмотрен один выделенный класс семейств (1.5):

– показано, что этот класс семейств является правильным (теорема 2);

– доказана теорема о сильной квадратичности семейства (теорема 3).

Введена конструкция, позволяющая строить квазигруппы на основе пары правильных семейств (теорема 1), доказан ряд утверждений о количестве ассоциативных троек в квазигруппах, получаемых с помощью указанной конструкции (раздел 1.4.1).

Результаты главы были опубликованы в [74; 76; 77; 80].

1.1 Основные обозначения

Введем основные обозначения, используемые на протяжении всей работы.

– $Q_1 \times \ldots \times Q_n$ — прямое (декартово) произведение множеств $Q_1, \ldots, Q_n$; если на Q_i заданы некоторые операции $\circ_i$, то они переносятся покоординатно на прямое произведение.

– G — некоторая группа с операцией «$\cdot$».

– $d(\mathbf{x}, \mathbf{y})$ — метрика Хэмминга; метрическое пространство, снабженное метрикой Хэмминга, будем называть пространством Хэмминга.

– $Func(A, B)$ — множество функций $\{f \mid f\colon A \to B\}$.

– $\mathcal{S}_Q$ — группа подстановок (биекций с операцией композиции) на множестве Q, $\mathcal{S}_n$ — группа подстановок на множестве $Q = \{1, \ldots, n\}$.

– $\mathbb{E}_k$ — множество $\{0, 1, \ldots, k-1\}$.

– $\mathcal{F}_n$, $\mathcal{G}_n$ — семейства функций на $Q_1 \times \ldots \times Q_n$.
– id — тождественное отображение, $\mathsf{id}(x) = x$.
– inv — отображение «переворота», ставящее для любого n в соответствие набору $\mathbf{x} \in Q^n$ набор $\mathbf{y} \in Q^n$ следующим образом: $y_i = x_{n-i+1}$, $1 \leqslant i \leqslant n$.
– $Aut(X)$ — группа автоморфизмов объекта X.
– $Mult(Q)$ — группа умножений квазигруппы Q.
– $\mathbb{N}$ — множество натуральных чисел.
– $x \leftarrow^{\mathcal{U}} A$ — выбор случайного элемента x в соответствии с распределением, задаваемым вероятностным алгоритмом A.

Набор элементов будет обозначаться либо жирным шрифтом: $\mathbf{x}, \mathbf{y}, \mathbf{v}$ и так далее, либо греческими символами α, β. Также вместо набора будем иногда использовать в качестве синонимов слова «точка» или «вектор». Если $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_m)$, то под записью

$$\begin{bmatrix} \mathbf{x} \\ \mathbf{y} \end{bmatrix}$$

мы подразумеваем вектор-столбец $(x_1, \ldots, x_n, y_1, \ldots, y_m)^T$. Если $b \in \{0, 1\}$, то b^n — вектор-столбец

$$b^n = \left(\underbrace{b, \ldots, b}_{n \text{ раз}} \right)^T.$$

Если $n, m \in \mathbb{N}$, то $m \mid n$ означает, что m делит число n.

Пусть $f, g \colon \mathbb{N} \to \mathbb{N}$. Будем писать

– $f = \mathcal{O}(g)$, если

$$\exists M\ \exists N\ \forall n > N \colon f(n) < M \cdot g(n);$$

– $f = \Theta(g)$, если

$$\exists m > 0\ \exists M\ \exists N\ \forall n > N \colon m \cdot g(n) < f(n) < M \cdot g(n);$$

– $f = o(g)$, если

$$\forall \varepsilon > 0\ \exists N\ \forall n > N \colon f(n) < \varepsilon \cdot g(n);$$

– $f \sim g$, если

$$\forall \varepsilon > 0\ \exists N\ \forall n > N \colon \left| \frac{f(n)}{g(n)} - 1 \right| < \varepsilon;$$

– $f \lesssim g$, если существует h такое, что выполнены условия

$$f \leqslant h,\ h \sim g.$$

Все остальные обозначения будут вводиться в основном тексте работы.

1.2 Основные определения

В настоящем разделе мы введем основные определения, связанные с группами, квазигруппами, дискретными функциями и семействами функций на множествах, которые необходимы для дальнейшего изложения.

1.2.1 Квазигруппы

Приведем стандартные определения из теории квазигрупп (более подробно см., например, [3; 82; 83]).

Определение 1. Квазигруппой называется множество Q с заданной на нем бинарной операцией $\circ\colon Q \times Q \to Q$, удовлетворяющей следующему условию: для любых $a, b \in Q$ найдутся единственные элементы $x, y \in Q$ — решения уравнений

$$a \circ x = b, \quad y \circ a = b.$$

Далее мы будем рассматривать конечные квазигруппы $|Q| < \infty$, для краткости слово «конечный» будем опускать.

Замечание 1. Пусть Q — квазигруппа, тогда мы можем задать операции левого L_a и правого R_a сдвига на элемент $a \in Q$:

$$L_a\colon Q \to Q, L_a(x) = a \circ x,$$
$$R_a\colon Q \to Q, R_a(y) = y \circ a.$$

Операции L_a и R_a задают биективные отображения на множестве Q: $L_a, R_a \in \mathcal{S}_Q$.

Определение 2. Латинский квадрат размера k — это квадратная таблица $k \times k$, заполненная элементами k различных типов таким образом, что в каждой строке и в каждом столбце элемент каждого типа встречается ровно один раз.

Определение 3. Пусть $Q = \{q_1, \ldots, q_k\}$ — квазигруппа, тогда мы можем рассмотреть ее таблицу умножения: квадратную таблицу $k \times k$, заполненную элементами $q \in Q$ таким образом, что на пересечении i-й строки и j-го столбца записывается произведение $(q_i \circ q_j) \in Q$.

Замечание 2. Латинские квадраты являются таблицами умножения квазигрупп. Это следует из того факта, что левые и правые сдвиги являются биекциями.

Далее мы будем отождествлять квазигруппу с латинским квадратом, задающим ее таблицу умножения.

Понятие квазигруппы может быть обобщено на операции большей арности.

Определение 4. Множество Q с заданной на нем d-арной операцией $h\colon Q^d \to Q$, удовлетворяющей следующему условию: при любой фиксации d переменных из набора $a_1, \ldots, a_d, a_{d+1} \in Q$ уравнение

$$h(a_1, \ldots, a_d) = a_{d+1} \tag{1.1}$$

однозначно разрешимо (относительно свободной переменной), называется d-квазигруппой.

Замечание 3. Квазигруппа является d-квазигруппой с $d = 2$.

Замечание 4. Многомерная «таблица» умножения d-квазигруппы Q является латинским (гипер)кубом. На пересечении «строк» таблицы с номерами $i_1, \ldots, i_d$ будем писать значение $h(q_{i_1}, \ldots, q_{i_d})$. В таком случае по свойству однозначной разрешимости уравнений (1.1) при фиксации любых $d - 1$ номеров строк полученной таблицы оставшиеся элементы будут пробегать все множество Q.

Пример 1 (пример d-квазигруппы)**.** Для группы $(G, \cdot)$ и элемента $g \in G$ мы можем определить d-квазигрупповую операцию следующим способом:

$$h(x_1, \ldots, x_d) = x_1 \cdot \ldots \cdot x_d \cdot g.$$

Определение 5. Пусть Q — квазигруппа с операцией $\circ$. Ее изотопом называется квазигруппа $Q_{\alpha\beta\gamma}$ с операцией $*$, заданной на том же множестве по следующему правилу:

$$a * b = \gamma^{-1}(\alpha(a) \circ \beta(b)),$$

где $\alpha, \beta, \gamma \in \mathcal{S}_Q$ — подстановки на множестве Q.

Определение 6. Главным изотопом $Q_{\alpha\beta}$ называется изотоп квазигруппы Q с дополнительным условием $\gamma = \mathsf{id}$, где id — тождественное отображение на Q.

Определение 7. Биекция $\theta \in \mathcal{S}_Q$ называется полным отображением (complete mapping) квазигруппы Q, если отображение

$$\sigma\colon Q \to Q, \quad \sigma(x) = x \circ \theta(x)$$

также является биекцией $\sigma \in \mathcal{S}_Q$. Если θ — полное отображение, то ассоциированное с ним отображение σ называется ортоморфизмом.

Определение 8. Трансверсалью в латинском квадрате L размера $k \times k$ называется множество троек (i, j, q) мощности k, таких что $L[i, j] = q$, и для каждой пары (i, j, q) и (i', j', q') выполнены неравенства:

$$i \neq i',\ j \neq j',\ q \neq q'.$$

Замечание 5. Существование полного отображения в квазигруппе эквивалентно существованию трансверсали в ее таблице умножения [3, теорема 1.5.1].

Определение 9. Идемпотентом в квазигруппе Q называется элемент $x \in Q$ со свойством $x \circ x = x$.

Фактически, идемпотент x является подквазигруппой размера 1 (см. раздел 1.4.3).

1.2.2 Действия групп

Определение 10. Разбиением множества Q назовем набор $A_1, \ldots, A_t$ непересекающихся подмножеств Q со свойством

$$A_1 \sqcup \ldots \sqcup A_t = Q.$$

Разбиение называется нетривиальным, если $t > 1$, все A_i непусты и существует A_i с условием $|A_i| > 1$.

Определение 11. Пусть G — некоторая группа. Говорят, что группа G действует (слева) на множестве M, если задан гомоморфизм

$$\Psi\colon G \to S_M,$$

то есть каждому элементу группы $g \in G$ ставится в соответствие биекция на множестве M. Гомоморфизм Ψ называется действием группы G на множестве M.

Для краткости операцию $\Psi(g)(x)$ будем обозначать через $g \cdot x$, где $g \in G$, $x \in M$.

Определение 12. Действие Ψ группы G на множестве M называется транзитивным, если

$$\forall x \in M\ \forall y \in M\ \exists g \in G\colon g \cdot x = y.$$

Аналогично, действие называется t-транзитивным, если для любых подмножеств $\{x_1, \ldots, x_t\} \subseteq M$, $\{y_1, \ldots, y_t\} \subseteq M$ мощности t найдется элемент $g \in G$, что $g \cdot x_i = y_i$, $1 \leqslant i \leqslant t$.

Определение 13. Действие группы G на множестве Q называется примитивным, если оно транзитивно и не сохраняет никаких нетривиальных разбиений.

1.2.3 Дискретные функции

Напомним некоторые понятия из теории булевых функций (см., например, [84]).

Мы будем использовать стандартные обозначения $\bar{x}$, $\oplus$, $\cdot$, $\vee$ для логического отрицания, сложения по модулю 2, умножения по модулю 2 (логического «И») и логического «ИЛИ» соответственно.

Замечание 6 (полином Жегалкина)**.** Каждая булева функция $f\colon \mathbb{E}_2^n \to \mathbb{E}_2$ единственным образом представима в виде полинома, называемого полиномом Жегалкина [84, часть I, глава 5]:

$$\bigoplus_{\alpha \in \mathbb{E}_2^n} a_\alpha x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n},$$

где $a_\alpha \in \mathbb{E}_2$, $x^0 := 1$, $x^1 := x$, суммирование ведется по модулю 2.

Произведение вида $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ называется мономом, а число $\alpha_1 + \ldots + \alpha_n$ — степенью монома.

Определение 14. Под степенью булевой функции будем понимать максимальную степень монома в полиноме Жегалкина для этой функции.

В силу единственности представления булевой функции полиномом Жегалкина понятие степени булевой функции определено корректно.

Определение 15. Пусть $\mathbf{x}, \mathbf{y} \in \mathbb{E}_2^n$, тогда расстояние Хэмминга $d(\mathbf{x}, \mathbf{y})$ между наборами $\mathbf{x}$ и $\mathbf{y}$ определяется как число несовпадающих координат векторов:

$$d(\mathbf{x}, \mathbf{y}) = |\{1 \leqslant i \leqslant n \mid \mathbf{x}[i] \neq \mathbf{y}[i]\}|.$$

Определение 16. Пусть $p(X) \in \mathbb{F}_q[X]$ — многочлен над конечным полем. Многочлен p называется перестановочным, если отображение $x \to p(x)$, $x \in \mathbb{F}_q$, биективно.

1.2.4 Семейства функций и их преобразования

В этом разделе мы введем понятие семейства функций, а также определим некоторые преобразования, которые можно осуществлять над семействами.

Семейство функций

Определение 17. Пусть $Q_1, \ldots, Q_n$ — набор непустых конечных множеств. Под семейством функций $\mathcal{F}_n$ на $Q_1 \times \ldots \times Q_n$ будем понимать отображение вида

$$\mathcal{F}_n \colon Q_1 \times \ldots \times Q_n \to Q_1 \times \ldots \times Q_n,$$
$$\mathcal{F}_n \colon \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \to \begin{bmatrix} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_n(x_1, \ldots, x_n) \end{bmatrix},$$

где $f_i(x_1, \ldots, x_n)\colon Q_1 \times \ldots \times Q_n \to Q_i$. Число n будем называть размером семейства. Иногда мы будем опускать размер семейства n из обозначения $\mathcal{F}_n$, если он понятен из контекста.

Замечание 7. Часто в качестве множеств Q_i у нас будут выступать конечные квазигруппы $(Q_i, \circ_i)$ или конечные группы $(G_i, +_i)$. В таком случае мы будем предполагать, что на прямом произведении Q_i задана операция покоординатного умножения: для $\mathbf{x}, \mathbf{y} \in Q_1 \times \ldots \times Q_n$ определим $\mathbf{x} \circ \mathbf{y}$ равенством

$$\mathbf{x} \circ \mathbf{y} = (x_1 \circ_1 y_1, \ldots, x_n \circ_n y_n)\,.$$

Заметим также, что в большинстве случаев мы рассматриваем произведение из n одинаковых экземпляров (квази)группы, т.е.

$$Q_1 = \ldots = Q_n = Q, \quad \circ_1 = \ldots = \circ_n = \circ.$$

Определение 18. Функция f существенно зависит от переменной x_i, если найдутся два набора значений

$$\alpha = (\alpha_1, \ldots, \alpha_{i-1}, a, \alpha_{i+1}, \ldots, \alpha_n) \quad \beta = (\alpha_1, \ldots, \alpha_{i-1}, b, \alpha_{i+1}, \ldots, \alpha_n)\,,$$

такие что $f(\alpha) \neq f(\beta)$.

Определение 18 напрямую обобщается на семейства функций.

Определение 19. Будем говорить, что семейство $\mathcal{F}_n$ существенно зависит от переменной x_i, если найдутся два набора значений

$$\alpha = (\alpha_1, \ldots, \alpha_{i-1}, a, \alpha_{i+1}, \ldots, \alpha_n) \quad \beta = (\alpha_1, \ldots, \alpha_{i-1}, b, \alpha_{i+1}, \ldots, \alpha_n)\,,$$

такие что $\mathcal{F}_n(\alpha) \neq \mathcal{F}_n(\beta)$.

В работе [52] было введено следующее определение.

Определение 20. Графом существенной зависимости семейства функций $\mathcal{F}_n$ будем называть ориентированный граф $G_{\mathcal{F}} = (V, E)$, множество вершин которого равно $V = \{1, \ldots, n\}$, а вершины i и j соединены ориентированным ребром $i \to j$ в том и только в том случае, когда функция f_j существенно зависит от x_i (см. определение 18).

Замечание 8 (петли в $G_{\mathcal{F}}$)**.** В терминах графа $G_{\mathcal{F}}$ свойство существенной зависимости f_i от x_i эквивалентно наличию петли $i \to i$ в графе $G_{\mathcal{F}}$.

В работе [85] была введена следующая характеристика, которая показывает «степень нелинейности» булева отображения (строгий тип нелинейности).

Определение 21. Семейство булевых функций $\mathcal{F}_n = (f_1, \ldots, f_n)$ называется квадратичным строгого типа $Quad_v^s Lin_{n-v}^s$, $1 \leqslant v \leqslant n$, если

- каждая функция семейства не более чем квадратична;
- имеется v функций, все нетривиальные линейные комбинации которых квадратичны;
- если $v < n$, то для любых $v+1$ функции найдется нетривиальная линейная комбинация, степень которой меньше двух.

Если $v = n$, то семейство $\mathcal{F}_n$ называется сильно квадратичным.

Преобразования семейств функций

Рассмотрим преобразования внешнего и внутреннего сдвига семейства.

Определение 22. Пусть $(Q_1, \circ_1), \ldots, (Q_n, \circ_n)$ — квазигруппы,

$$\mathbf{s} = (s_1, \ldots, s_n) \in Q_1 \times \ldots \times Q_n.$$

Под **внешним сдвигом** семейства $\mathcal{F}_n$ на $\mathbf{s}$ будем понимать семейство $\mathcal{G}_n$ вида

$$\mathcal{G}_n(\mathbf{x}) = \mathcal{F}_n(\mathbf{x}) \circ \mathbf{s} = \begin{bmatrix} f_1(x_1, \ldots, x_n) \circ_1 s_1 \\ \vdots \\ f_n(x_1, \ldots, x_n) \circ_n s_n \end{bmatrix}.$$

Под **внутренним сдвигом** семейства $\mathcal{F}_n$ на $\mathbf{s}$ будем понимать семейство $\mathcal{G}_n$ вида

$$\mathcal{G}_n(\mathbf{x}) = \mathcal{F}_n(\mathbf{x} \circ \mathbf{s}) = \mathcal{F}_n(x_1 \circ_1 s_1, \ldots, x_n \circ_n s_n).$$

Введем также действие группы подстановок $\mathcal{S}_n$ на множестве векторов фиксированного размера n.

Определение 23. Для подстановки $\sigma \in \mathcal{S}_n$ и вектора $\mathbf{x} \in Q^n$ мы можем рассмотреть преобразование

$$\mathbf{x} \to \sigma(\mathbf{x}) = \left(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}\right),$$

которое переводит компоненту x_i вектора $\mathbf{x}$ на место компоненты $x_{\sigma(i)}$.

Определение 24. Для пары подстановок $\sigma, \tau \in \mathcal{S}_n$ и семейства $\mathcal{F}_n \colon Q^n \to Q^n$ размера n рассмотрим семейство $(\sigma, \tau)(\mathcal{F}_n)$, которое получено из $\mathcal{F}_n$ с помощью перестановки индексов переменных и индексов входящих в семейство функций:

$$(\sigma, \tau)(\mathcal{F}_n) = \begin{bmatrix} f_{\sigma^{-1}(1)}\left(x_{\tau^{-1}(1)}, \ldots, x_{\tau^{-1}(n)}\right) \\ \vdots \\ f_{\sigma^{-1}(n)}\left(x_{\tau^{-1}(1)}, \ldots, x_{\tau^{-1}(n)}\right) \end{bmatrix},$$

т.е. функция (переменная) с номером i переходит на место функции (переменной) с номером $\sigma(i)$ ($\tau(i)$). Введем также преобразование $\sigma(\mathcal{F}_n)$ следующим образом:

$$\sigma(\mathcal{F}_n) = (\sigma, \sigma)(\mathcal{F}_n).$$

Другими словами, $\sigma(\mathcal{F}_n)$ — семейство, полученное применением подстановки σ как к индексам функций, так и индексам координат. Таким образом введенное преобразование будем называть **согласованной перестановкой семейства.**

Введем понятие проекции и сужения семейства.

Определение 25. Пусть $\mathcal{F}_n$ — семейство размера n на $Q_1 \times \ldots \times Q_n$. Под проекцией семейства $\Pi_i^q(\mathcal{F}_n)$, где $q \in Q_i$, будем понимать семейство $\mathcal{G}_{n-1}$, полученное из $\mathcal{F}_n$ подстановкой вместо x_i константы q и вычеркиванием функции f_i:

$$\mathcal{G}_{n-1}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = \Pi_i^q(\mathcal{F}_n) = \\ = \begin{bmatrix} f_1(x_1, \ldots, x_{i-1}, q, x_{i+1}, \ldots, x_n) \\ \vdots \\ f_{i-1}(x_1, \ldots, x_{i-1}, q, x_{i+1}, \ldots, x_n) \\ f_{i+1}(x_1, \ldots, x_{i-1}, q, x_{i+1}, \ldots, x_n) \\ \vdots \\ f_n(x_1, \ldots, x_{i-1}, q, x_{i+1}, \ldots, x_n) \end{bmatrix}.$$

Аналогичным образом вводится кратная проекция семейства:

$$\Pi_{i_1, \ldots, i_k}^{q_1, \ldots, q_k}(\mathcal{F}_n) = \Pi_{i_1}^{q_1}\left(\ldots\left(\Pi_{i_k}^{q_k}(\mathcal{F}_n)\right)\ldots\right).$$

Замечание 9. Далее мы будем предполагать, что исходное семейство также является своей проекцией, т.е. тождественное преобразование также является (тривиальной) проекцией.

Определение 26. Пусть $\mathcal{F}_n$ — семейство на $Q_1 \times \ldots \times Q_n$, $q \in Q_i$. Тогда сужением семейства $\mathcal{F}_n$ будем называть набор функций $\mathcal{G}$ от $n-1$ переменной, где каждая функция задана на подмножестве $Q_1 \times \ldots \times Q_n$ с i-й фиксированной координатой $x_i := q$:

$$\mathcal{G}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = \mathcal{F}_n(x_1, \ldots, x_{i-1}, q, x_{i+1}, \ldots, x_n).$$

Аналогичным образом вводится сужение на несколько координат.

1.3 Правильные семейства функций

В этом разделе мы введем определение для основного объекта исследования — правильного семейства функций. Мы рассмотрим как булев, так и общий случай. Заметим, что с точки зрения практических приложений булев случай является одним из наиболее интересных.

1.3.1 Правильные семейства булевых функций

Понятие правильного семейства булевых функций было введено и исследовалось в работах [1; 2].

Определение 27. Семейство булевых функций

$$\mathcal{F}_n \colon \mathbb{E}_2^n \to \mathbb{E}_2^n, \quad \mathcal{F}_n(\mathbf{x}) = \begin{bmatrix} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_n(x_1, \ldots, x_n) \end{bmatrix},$$

называется правильным, если для любых двух неравных двоичных наборов

$$\alpha = (\alpha_1, \ldots, \alpha_n), \quad \beta = (\beta_1, \ldots, \beta_n), \quad \alpha \neq \beta,$$

выполняется следующее условие:

$$\exists i : \ \alpha_i \neq \beta_i, \quad f_i(\alpha) = f_i(\beta).$$

Правильные семейства булевых функций могут использоваться для построения больших параметрических семейств латинских квадратов (см. определение 2) или, что эквивалентно, для задания структуры квазигруппы (см. определение 1); а именно, верно утверждение.

Утверждение 1 ([2, утверждение 2])**.** *Рассмотрим следующую конструкцию. Пусть* $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n$, $\mathcal{F}_n$ *— семейство функций размера* n *на* $\mathbb{Z}_2^n$, $\pi_i \colon \mathbb{Z}_2^2 \to \mathbb{Z}_2$ *— произвольные булевы функции,* $1 \leqslant i \leqslant n$*. Рассмотрим операцию* $\circ$ *на множестве* $\mathbb{E}_2^n$*, задаваемую равенством*

$$\mathbf{x} \circ \mathbf{y} = \mathbf{x} \oplus \mathbf{y} \oplus \mathcal{F}(\pi(\mathbf{x}, \mathbf{y})), \tag{1.2}$$

где через $\mathcal{F}(\pi(\mathbf{x}, \mathbf{y}))$ *обозначена конструкция*

$$\mathcal{F}(\pi(\mathbf{x}, \mathbf{y})) = \begin{bmatrix} f_1(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)) \\ \vdots \\ f_n(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)) \end{bmatrix}.$$

Операция $\circ \colon \mathbb{E}_2^n \times \mathbb{E}_2^n \to \mathbb{E}_2^n$ *задает структуру квазигруппы на* $\mathbb{E}_2^n$ *для любых функций* π_i *тогда и только тогда, когда* $\mathcal{F}_n$ *— правильное семейство.*

Функции π_i, $1 \leqslant i \leqslant n$, из условия утверждения 1 будем называть параметрическими функциями. Таким образом, варьируя параметрические функции π_i, можно получать (потенциально различные) квазигрупповые операции из одного заданного правильного семейства $\mathcal{F}_n$. В работе [77, теорема 4] оценивается снизу количество различных порождаемых квазигрупп (при варьировании параметрических функций с заданным фиксированным правильным семейством). При этом оценивается только число попарно различных квазигрупп (с различными таблицами умножения): оценка не учитывает тот факт, что различные полученные квазигруппы могут оказаться изотопными.

Утверждение 2 ([77, теорема 4])**.** *Пусть мощность образа отображения, индуцируемого семейством* $\mathcal{F}$*, равна* M*:*

$$\mathcal{F} \colon \mathbf{x} \to \mathcal{F}(\mathbf{x}), \quad |\mathsf{Im}(\mathcal{F})| = M.$$

Тогда операция (1.2) порождает не менее M^{2^n} *попарно различных квазигрупп.*

Таким образом, мощность образа $\mathsf{Im}(\mathcal{F})$ является важной характеристикой правильного семейства $\mathcal{F}$.

Правильные семейства булевых функций могут быть определены различными эквивалентными способами. Далее приведем два из них.

Определение 28. Пусть $I = \{i_1, \ldots, i_s\} \subseteq \{1, \ldots, n\}$ — некоторое подмножество индексов. Назовем набор переменных $\mathbf{x}_I = (x_{i_1}, \ldots, x_{i_s})$ существенным для булевой функции $f(x_1, \ldots, x_n)$, если выполнено равенство

$$\sum_{(\alpha_1,\ldots,\alpha_s)\in\mathbb{E}_2^s} f(x_1, \ldots, x_{i_1-1}, \alpha_1, x_{i_1+1}, \ldots, x_{i_s-1}, \alpha_s, x_{i_s+1}, \ldots, x_n) \not\equiv 0 \bmod 2.$$

Замечание 10. Для одноэлементного множества $I = \{i\}$ мы получаем определение существенной зависимости булевой функции f от x_i (см. определение 18), для множества $I = \{1, \ldots, n\}$ — требование нечетности веса булевой функции f.

Утверждение 3 ([1, теорема 1])**.** *Семейство булевых функций $\mathcal{F}_n$ является правильным тогда и только тогда, когда для любого подмножества $I \subseteq \{1, \ldots, n\}$ набор переменных $\mathbf{x}_I$* ***не является*** *существенным для функции $f = \prod_{i\in I} f_i$.*

Можно также привести следующий критерий правильности, основанный на регулярности преобразования, задаваемого с помощью семейства функций.

Утверждение 4 ([50, теорема 2])**.** *Семейство булевых функций $\mathcal{F}_n(\mathbf{x})$ является правильным тогда и только тогда, когда для любого набора отображений*

$$\Psi = (\psi_1, \ldots, \psi_n), \quad \psi_i \colon \mathbb{E}_2 \to \mathbb{E}_2,$$

отображение

$$\mathbf{x} \to \mathbf{x} \oplus \Psi(\mathcal{F}_n(\mathbf{x})) = \begin{bmatrix} x_1 \oplus \psi_1(f_1(x_1, \ldots, x_n)) \\ \vdots \\ x_n \oplus \psi_n(f_n(x_1, \ldots, x_n)) \end{bmatrix}$$

является биекцией $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$.

Замечание 11. С помощью утверждения 4 можно предложить альтернативный способ задания семейств латинских квадратов. Введем операции $*$: для $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n$ и наборов отображений

$$\Phi = (\varphi_1, \ldots, \varphi_n), \quad \varphi_i \colon \mathbb{Z}_2 \to \mathbb{Z}_2,$$
$$\Psi = (\psi_1, \ldots, \psi_n), \quad \psi_i \colon \mathbb{Z}_2 \to \mathbb{Z}_2,$$

зададим $\mathbf{x} * \mathbf{y}$ равенством

$$\mathbf{x} * \mathbf{y} = \mathbf{x} \oplus \Phi(\mathcal{F}_n(\mathbf{x})) \oplus \mathbf{y} \oplus \Psi(\mathcal{G}_n(\mathbf{y})),$$

где $\mathcal{F}_n$, $\mathcal{G}_n$ — два правильных семейства булевых функций размера n.

Построенная таким образом квазигруппа является главным изотопом группы $\mathbb{Z}_2^n$ (см. определение 6).

1.3.2 Обобщение понятия правильного семейства

Понятие правильности семейства может быть перенесено со случая булевых функций на произвольные абелевы группы [49—52], поля [52], квазигруппы и d-квазигруппы [55] практически без изменений формулировок. Приведем общее определение правильного семейства.

Определение 29. Семейство функций $\mathcal{F}_n$ на $Q_1 \times \ldots \times Q_n$ называется правильным, если для любых двух неравных наборов

$$\alpha = (\alpha_1, \ldots, \alpha_n), \quad \beta = (\beta_1, \ldots, \beta_n), \quad \alpha \neq \beta,$$

выполняется следующее условие:

$$\exists i \colon \alpha_i \neq \beta_i,\ f_i(\alpha) = f_i(\beta).$$

В наиболее общей форме теорему о правильных семействах, аналогичную утверждению 1, можно сформулировать для прямого произведения $(d+1)$-квазигрупп.

Утверждение 5 ([55, теорема 5], [76, теорема 4])**.** *Рассмотрим следующую конструкцию. Пусть* $(Q, h_1), \ldots, (Q, h_n)$ *—* $(d+1)$*-квазигруппы,*

$$\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_d \in Q^n,$$

$\mathcal{F}_n$ *— семейство функций на* Q^n*,* $\pi_i \colon Q^d \to Q$*,* $1 \leqslant i \leqslant n$ *— произвольные параметрические функции. Зададим операцию* H *на множестве* $(Q, h_1) \times \ldots \times (Q, h_n)$*:*

$$\mathbf{v} = H(\mathbf{x}_1, \ldots, \mathbf{x}_d),$$

$$v_i \;=\; h_i\Big(x_1[i], x_2[i], \ldots, x_d[i], \\ f_i\left(\pi_1(x_1[1], \ldots, x_d[1]),\; \ldots\; , \pi_n(x_1[n], \ldots, x_d[n])\right)\Big).$$

Операция $H : Q^n \times \ldots \times Q^n \to Q^n$ задает структуру d-квазигруппы на множестве Q^n для любых параметрических функций π_i тогда и только тогда, когда $\mathcal{F}_n$ — правильное семейство на Q^n.

Замечание 12. Частными случаями рассмотренной конструкции являются конструкции, предложенные в работах [49—52] (в качестве 3-квазигрупповой операции h_i в них рассматривается операция 3-сложения в абелевой группе $h(x, y, z) = x + y + z$), а также конструкция, предложенная в работе [54], в которой рассматривается конкретная $(d+1)$-квазигрупповая операция $h(x_1, \ldots, x_{d+1}) = x_1 + \ldots + x_{d+1}$ над абелевой группой.

Замечание 13 (о существенной (не)зависимости)**.** Из утверждения 3 и замечания 10 следует, что для правильного булева семейства $\mathcal{F}_n$ i-я функция f_i не может существенно зависеть от x_i. На самом деле, это свойство легко следует из общего определения правильного семейства и выполняется для любых (не только булевых) правильных семейств. Если бы в семействе $\mathcal{F}_n$, заданном на $Q_1 \times \ldots \times Q_n$, f_i зависела бы существенно от x_i, то по определению существенной зависимости (см. определение 18) нашлось бы два набора, различающихся только в i-й компоненте, на которых f_i принимала бы различные значения:

$$\exists \alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n : \\ f_i(\alpha_1, \ldots, \alpha_{i-1}, a, \alpha_{i+1}, \ldots, \alpha_n) \neq f_i(\alpha_1, \ldots, \alpha_{i-1}, b, \alpha_{i+1}, \ldots, \alpha_n),$$

что противоречит условию правильности: два указанных набора различаются лишь в i-й компоненте, но при этом функция f_i на этих двух наборах также принимает различные значения.

Замечание 14. Правильное семейство $\mathcal{F}_n : \mathbb{E}_k^n \to \mathbb{E}_k^n$ не может принимать «противоположные» значения (т.е. значения $\alpha, \beta \in \mathbb{E}_k^n$ с тем свойством, что $\alpha_i \neq \beta_i$, $1 \leqslant i \leqslant n$). В противном случае на соответствующих этим значениям прообразах нарушается свойство правильности.

Аналог утверждения 4 был получен и для абелевых групп [50, теорема 2]. Докажем дальнейшее обобщение критерия регулярности на случай произвольных квазигрупп.

Теорема 1. *Семейство $\mathcal{F}_n$ на $Q_1 \times \ldots \times Q_n$ является правильным тогда и только тогда, когда для любого набора отображений*

$$\psi_i \colon Q_i \to Q_i,\ 1 \leqslant i \leqslant n,$$

следующее отображение из $Q_1 \times \ldots \times Q_n$ в себя биективно:

$$\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \to \mathbf{x} \circ \Psi(\mathcal{F}_n(\mathbf{x})) = \begin{bmatrix} x_1 \circ_1 \psi_1(f_1(x_1, \ldots, x_n)) \\ \vdots \\ x_n \circ_n \psi_n(f_n(x_1, \ldots, x_n)) \end{bmatrix},\ x_i \in Q_i.$$

Доказательство. Пусть $\mathcal{F}$ — правильное семейство на $Q_1 \times \ldots \times Q_n$. Покажем, что отображение $\mathbf{x} \to \mathbf{x} \circ \Psi(\mathcal{F}_n(\mathbf{x}))$ инъективно. Пусть $\mathbf{x} \neq \mathbf{y}$, $\mathbf{x}, \mathbf{y} \in Q_1 \times \ldots \times Q_n$, тогда по условию правильности найдется такой индекс i, что $x_i \neq y_i$, но $f_i(\mathbf{x}) = f_i(\mathbf{y})$, а значит,

$$x_i \circ_i \psi_i(f_i(\mathbf{x})) \neq y_i \circ_i \psi_i(f(\mathbf{y})).$$

Из конечности $Q_1 \times \ldots \times Q_n$ и инъективности отображения следует его биективность.

Пусть $\mathcal{F}$ не является правильным. Построим отображение Ψ таким образом, чтобы $\mathbf{x} \to \mathbf{x} \circ \Psi(\mathcal{F}_n(\mathbf{x}))$ не было биекцией. Поскольку $\mathcal{F}$ не является правильным, то найдутся две точки $\mathbf{x} \neq \mathbf{y}$, для которых для всех индексов i со свойством $x_i \neq y_i$ следует $f_i(\mathbf{x}) \neq f_i(\mathbf{y})$. Рассмотрим все индексы, в которых наборы $\mathbf{x}$ и $\mathbf{y}$ различаются. Для каждого подобного индекса зададим ψ_i таким образом, чтобы $x_i \circ_i \psi_i(f_i(\mathbf{x})) = \mathbf{y}_i \circ_i \psi_i(f_i(\mathbf{y}))$; это можно сделать, зафиксировав $\psi_i(f_i(\mathbf{x}))$ произвольным образом и доопределив $\psi_i(f_i(\mathbf{y}))$ из уравнения (из условия на «плохие» индексы мы имеем $f_i(\mathbf{x}) \neq f_i(\mathbf{y})$, а значит, определение ψ_i корректно). В тех индексах, где $x_i = y_i$, зададим ψ_i как правый нейтральный элемент для x_i для любого значения аргумента.

Если мы зададим ψ_i обозначенным выше образом, то получим равенство

$$\mathbf{x} \neq \mathbf{y}, \quad \mathbf{x} \circ \Psi(\mathcal{F}_n(\mathbf{x})) = \mathbf{y} \circ \Psi(\mathcal{F}_n(\mathbf{y})),$$

а значит, отображение не может быть биективным. □

В случае $Q_i = \mathbb{Z}_p = \mathbb{F}_p$, где p — простое, теорема 1 может быть усилена следующим образом.

Утверждение 6 ([49, теорема 3])**.** *Семейство $\mathcal{F}_n$ на $\mathbb{F}_p^n$, где $\mathbb{F}_p$ — простое поле, является правильным тогда и только тогда, когда для любого набора элементов $a_i \in \mathbb{F}_p$ следующее отображение $\mathbb{F}_p^n \to \mathbb{F}_p^n$ биективно:*

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \to \begin{bmatrix} x_1 + a_1 \cdot f_1(x_1, \ldots, x_n) \\ \vdots \\ x_n + a_n \cdot f_n(x_1, \ldots, x_n) \end{bmatrix}.$$

1.3.3 Примеры правильных семейств

В настоящем разделе мы приведем некоторые примеры правильных семейств.

Константные и треугольные семейства

Пример 2 (константные функции)**.** Набор константных функций

$$f_1 \equiv q_1, \ \ldots \ , f_n \equiv q_n, \quad q_i \in Q_i, 1 \leqslant i \leqslant n,$$

является правильным семейством.

В статье [50] приводится пример так называемых треугольных правильных семейств. Немного обобщая определение из [50], дадим следующее определение.

Пример 3 (треугольное семейство)**.** Треугольное семейство $\mathcal{F}_n$ на Q^n — это семейство функций, которое после переупорядочивания номеров переменных и функций может быть записано в виде:

$$\begin{bmatrix} f_{\sigma(1)}(\cdot) \\ f_{\sigma(2)}(x_{\sigma(1)}) \\ f_{\sigma(3)}(x_{\sigma(1)}, x_{\sigma(2)}) \\ \vdots \\ f_{\sigma(n)}(x_{\sigma(1)}, \ldots, x_{\sigma(n-1)}) \end{bmatrix},$$

другими словами, есть такое упорядочивание $\sigma \in \mathcal{S}_n$ входящих в семейство функций, что каждая последующая функция в семействе может существенно зависеть только от переменных с номерами предыдущих функций.

Замечание 15 (о правильности треугольных семейств)**.** Нетрудно убедиться, что треугольные семейства являются правильными: если даны два различных набора $\alpha = (\alpha_1, \ldots, \alpha_n)$ и $\beta = (\beta_1, \ldots, \beta_n)$, и при этом верно:

$$\alpha_{\sigma(1)} = \beta_{\sigma(1)}, \ldots, \alpha_{\sigma(k)} = \beta_{\sigma(k)}, \alpha_{\sigma(k+1)} \neq \beta_{\sigma(k+1)},$$

то достаточно взять функцию с номером $\sigma(k+1)$, которая на наборах α и β будет давать одинаковый результат:

$$f_{\sigma(k+1)}(\alpha) = f_{\sigma(k+1)}(\beta).$$

Можно также обобщить понятие треугольного семейства следующим образом [49, теорема 4].

Пример 4 (треугольное расширение)**.** Пусть $F^0 = (g_{1,0}, \ldots, g_{n,0})$ — семейство функций, зависящих от переменных $(x_{1,0}, \ldots, x_{n,0})$. Пусть $s_1, \ldots, s_n \in \mathbb{N} \cup \{0\}$ — некоторый набор чисел длины n. Определим функции $f_{i,j}$ следующим образом:

$$\begin{gathered} f_{i,1} = F_{i,1}(g_{i,0}), \\ f_{i,2} = F_{i,2}(g_{i,0}, x_{i,1}), \\ \vdots \\ f_{i,s_i} = F_{i,s_i}(g_{i,0}, x_{i,1}, \ldots, x_{i,s_i-1}), \\ f_{i,0} = F_{i,0}(g_{i,0}, x_{i,1}, \ldots, x_{i,s_i}), \end{gathered}$$

где $F_{i,j}$ — произвольные функции подходящей арности (если $s_i = 0$, то остается только первая строка). Если семейство F^0 правильное, то семейство

$$F = (f_{i,j})_{i=1,\ldots,n, j=0,\ldots,s_i}$$

также является правильным.

Линейные семейства и g-семейства

Существует еще одно возможное обобщение свойства, указанного в замечании 13.

Определение 30. Определим линейное семейство $\mathcal{F}_n$ на абелевой группе G^n следующим образом:

$$f_1(x_1, \ldots, x_n) = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n + c_1,$$
$$\vdots$$
$$f_n(x_1, \ldots, x_n) = a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n + c_n,$$

где $a_{ij} \in \mathbb{Z}$, $c_i \in G$.

Для линейных семейств правильность эквивалентна отсутствию циклов в графе существенной зависимости.

Утверждение 7 ([50, теорема 3])**.** *Линейное семейство $\mathcal{F}_n$ задает правильное семейство на абелевой группе G^n тогда и только тогда, когда граф существенной зависимости $G_{\mathcal{F}}$ не содержит циклов (в том числе петель).*

Семейство функций, для которых правильность равносильна отсутствию циклов в графе существенной зависимости, можно расширить, введя понятие g-семейства [52].

Определение 31. Для фиксированного элемента $g \in G$ будем говорить, что функция $f(x_1, \ldots, x_n)\colon G^n \to G$ является g-функцией, если для любой переменной x_i, от которой она зависит существенным образом, выполнено условие

$$f(g, \ldots, g, x_i, g, \ldots, g) \not\equiv const.$$

В качестве конкретных примеров g-функций можно привести следующие:
– $x_1 \vee \ldots \vee x_n$ является 0-функцией;
– $x_1 \wedge \ldots \wedge x_n$ является 1-функцией;
– $x_1 \oplus \ldots \oplus x_n$ является 0-функцией и 1-функцией.

Утверждение 8 ([52, теорема 10])**.** *Семейство g-функций $\mathcal{F}_n$ является правильным тогда и только тогда, когда граф существенной зависимости $G_{\mathcal{F}}$ не содержит циклов.*

Дальнейшее изучение графов существенной зависимости и их матриц инцидентности проводилось в работе [53]. Графы существенной зависимости могут упрощать проверку свойства правильности семейства функций [56; 57]: так, возможно свести задачу проверки правильности исходного семейства $\mathcal{F}$ со всего множества $\left(\mathbb{E}_k^n\right)^2$ на проверку правильности на компонентах сильной связности графа существенной зависимости семейства $\mathcal{F}$ (подробнее см. [57]).

Ортогональные семейства

Определение 32. Две функции $f, g\colon \mathbb{E}_k^n \to \mathbb{E}_k$ будем называть ортогональными, если для любого $\mathbf{x} \in \mathbb{E}_k^n$ выполняется условие:

$$f(\mathbf{x}) = 0 \text{ или } g(\mathbf{x}) = 0.$$

Следующий пример правильных семейств приводится в работах [49; 52].

Пример 5 (семейство ортогональных функций)**.** Пусть $\mathcal{F}_n$ — семейство попарно ортогональных функций, причем каждая функция f_i не зависит существенно от x_i, $1 \leqslant i \leqslant n$. Тогда $\mathcal{F}_n$ является правильным. В частности, семейство

$$\begin{aligned} f_1 &= \bar{x}_2 x_3 \cdots x_{n-1} x_n, \\ f_2 &= \bar{x}_3 x_4 \cdots x_n x_1, \\ &\vdots \\ f_n &= \bar{x}_1 x_2 \cdots x_{n-2} x_{n-1} \end{aligned} \tag{1.3}$$

состоит из попарно ортогональных булевых функций, каждая из которых не зависит от одноименной переменной. Следовательно, оно является правильным.

Замечание 16. Требование ортогональности можно обобщить следующим образом: существует $q \in Q$, что для любых $i \neq j$ и любого $\mathbf{x} \in Q^n$ хотя бы одно из значений $f_i(x)$, $f_j(x)$ равно q. В частности, при $Q = \mathbb{E}_k$ и $q = 0$ это свойство означает, что векторы значений функций, составляющих ортогональное семейства, попарно ортогональны (как векторы из $\mathbb{Z}^{k^n}$).

Семейства на основе перестановочного многочлена

В работе [49, теорема 5] приводится следующий пример правильного семейства, заданного для простого поля $\mathbb{F}_p$.

Пример 6 (семейство на основе перестановочного многочлена)**.** Пусть $\mathbb{F}_p$ — простое поле, φ — перестановочный многочлен. Тогда семейство $\mathcal{F}_n$ размера $n \geqslant 3$

на $\mathbb{F}_p^n$

$$\begin{bmatrix} f_1(x_1,\ldots,x_n) \\ f_2(x_1,\ldots,x_n) \\ \vdots \\ f_n(x_1,\ldots,x_n) \end{bmatrix} = \begin{bmatrix} \varphi(x_2+1)\cdot\ldots\cdot\varphi(x_2+p-1)\cdot\varphi(x_3) \\ \varphi(x_3+1)\cdot\ldots\cdot\varphi(x_3+p-1)\cdot\varphi(x_4) \\ \vdots \\ \varphi(x_1+1)\cdot\ldots\cdot\varphi(x_1+p-1)\cdot\varphi(x_2) \end{bmatrix}$$

является правильным тогда и только тогда, когда n нечетно.

Замечание 17. Для булева случая можно рассмотреть частный случай конструкции из примера 6, приведенный в работе [71]:

$$\mathcal{F}(\mathbf{x}) = \begin{bmatrix} f_1(x_1,\ldots,x_n) \\ f_2(x_1,\ldots,x_n) \\ \vdots \\ f_n(x_1,\ldots,x_n) \end{bmatrix} = \begin{bmatrix} \overline{x}_2\cdot x_3 \\ \overline{x}_3\cdot x_4 \\ \vdots \\ \overline{x}_1\cdot x_2 \end{bmatrix}. \tag{1.4}$$

Указанное семейство является сильно квадратичным булевым правильным семейством (см. определение 21) при нечетных $n \geqslant 3$ [71, теорема 4].

Один выделенный класс булевых правильных семейств

Рассмотрим следующее семейство булевых функций [74].

$$\begin{bmatrix} 0 \\ x_1 \\ x_1\oplus x_2 \\ \vdots \\ x_1\oplus x_2\oplus\ldots\oplus x_{n-1} \end{bmatrix} \bigoplus \begin{bmatrix} \bigoplus_{i<j,\, i,j\neq 1}^{n} x_ix_j \\ \bigoplus_{i<j,\, i,j\neq 2}^{n} x_ix_j \\ \bigoplus_{i<j,\, i,j\neq 3}^{n} x_ix_j \\ \vdots \\ \bigoplus_{i<j,\, i,j\neq n}^{n} x_ix_j \end{bmatrix}, \tag{1.5}$$

в правой части суммируются все попарные произведения, в которые не входит одноименная с функцией переменная (т.к. в правильном семействе функция f_i заведомо не может зависеть от x_i, см. замечание 13).

Так, при $n=1$, $n=2$, $n=3$ имеем следующие семейства:

$$\begin{bmatrix} 0 \end{bmatrix}, \begin{bmatrix} 0 \\ x_1 \end{bmatrix}, \begin{bmatrix} x_2x_3 \\ x_1\overline{x}_3 \\ x_1\vee x_2 \end{bmatrix}.$$

Нетрудно убедиться, что первые три семейства этой последовательности являются правильными. Докажем следующее утверждение.

Теорема 2. *Булевы семейства, задаваемые формулой (1.5), являются правильными для любого* $n \geqslant 1$.

Доказательство. Через $\mathcal{F}_n(x_1, \ldots, x_n)$ обозначим исследуемое семейство размера n. Будем доказывать утверждение индукцией по размеру семейства.

База индукции: для $n = 1, 2, 3$ утверждение верно (прямая проверка по определению).

Индуктивный переход: пусть семейства $\mathcal{F}_k$ являются правильными для всех $k < n$. Рассмотрим семейство $\mathcal{F}_n$ размера n.

Заметим, что на наборах с последней координатой 0 первые $n-1$ функций семейства задают семейство того же вида размера на 1 меньше:

$$\mathcal{F}_n(x_1, \ldots, x_{n-1}, 0) = \begin{bmatrix} \mathcal{F}_{n-1}(x_1, \ldots, x_{n-1}) \\ f_n(x_1, \ldots, x_{n-1}) \end{bmatrix},$$

поскольку все попарные произведения $x_i x_n$ в квадратичной части обнуляются, линейная часть остается неизменной.

На наборах с последней координатой $x_n = 1$ аналогичным образом мы получаем, что первые $n-1$ функций семейства задают семейство того же вида размера на 1 меньше, но с инвертированным порядком функций и переменных. Используя обозначение, введенное в определении 24, мы можем записать данный факт в следующем виде:

$$\mathcal{F}_n(x_1, \ldots, x_{n-1}, 1) = \begin{bmatrix} \mathsf{inv}(\mathcal{F}_{n-1})(x_1, \ldots, x_{n-1}) \\ f_n(x_1, \ldots, x_{n-1}) \end{bmatrix},$$

где подстановка inv — отображение «переворота», ставящее для любого n в соответствие набору $\mathbf{x} \in Q^n$ набор $\mathbf{y} \in Q^n$ следующим образом: $y_i = x_{n-i+1}$, $1 \leqslant i \leqslant n$. Это верно, поскольку к линейной части каждой функции из семейства добавляется сумма $x_1 \oplus x_2 \oplus \ldots \oplus x_{n-1}$.

Покажем, что для семейства $\mathcal{F}_n$ выполняется свойство правильности, то есть для любых неравных наборов $\alpha \neq \beta$ найдется координата i, для которой $\alpha_i \neq \beta_i$, но $f_i(\alpha) = f_i(\beta)$. Для этого рассмотрим следующие возможные случаи.

1. Последние координаты наборов α, β совпадают.
2. Наборы α, β различаются только в последней координате.

3. Наборы α, β различаются не менее чем в трех координатах.
4. Наборы α, β различаются ровно в двух координатах.

В случаях 1 и 3 мы воспользуемся индуктивным предположением и сведем задачу к одинаковым семействам меньшего размера $k < n$. Случаи 2 и 4 требуют отдельного рассмотрения.

Если наборы α, β таковы, что их последние координаты совпадают (то есть $\alpha_n = \beta_n$), то по индуктивному предположению и в силу строения семейств $\mathcal{F}_n$ условие правильности должно выполниться среди первых $n-1$ функций (координат).

Если n — единственная позиция, в которой наборы различаются, то $f_n(\alpha) = f_n(\beta)$, поскольку f_n не зависит существенно от x_n (а значит, условие правильности выполняется для индекса n).

Пусть теперь среди первых $n-1$ координаты также есть различия. Рассмотрим в таком случае **предпоследнюю** различающуюся координату:

$$\alpha_k \neq \beta_k, \quad \alpha_{k+1} = \beta_{k+1}, \ \ldots, \ \alpha_{n-1} = \beta_{n-1}.$$

В таком случае мы имеем равенство:

$$\alpha_k \oplus \ldots \oplus \alpha_n = \beta_k \oplus \ldots \oplus \beta_n = t$$

После подстановки в семейство $\mathcal{F}_n$ последних $(n-k)$ координат наборов получим равенства:

$$\mathcal{F}_n(x_1, \ldots, x_{k-1}, \alpha_k, \ldots, \alpha_n) = \begin{bmatrix} \mathsf{inv}^t(\mathcal{F}_{k-1})(x_1, \ldots, x_{k-1}) \\ \mathbf{y} \end{bmatrix},$$
$$\mathcal{F}_n(x_1, \ldots, x_{k-1}, \beta_k, \ldots, \beta_n) = \begin{bmatrix} \mathsf{inv}^t(\mathcal{F}_{k-1})(x_1, \ldots, x_{k-1}) \\ \mathbf{v} \end{bmatrix},$$

где $\mathbf{y}, \mathbf{v}$ — некоторые вектора булевых функций длины $n-k+1$.

Таким образом, первые $(k-1)$ функций, полученных после подстановки наборов $\alpha_k, \ldots, \alpha_n$ и $\beta_k, \ldots, \beta_n$ соответственно, опять образуют правильное семейство булевых функций рассматриваемого вида («прямое» или «инвертированное»). Следовательно, если среди оставшихся $k-1$ координат наборов есть различающиеся, то свойство правильности будет выполняться для какой-либо из первых $k-1$ координат по индуктивному предположению.

Единственный оставшийся нерассмотренный случай состоит в том, что мы имеем два набора с ровно двумя различными координатами:

$$\alpha_k \neq \beta_k, \alpha_n \neq \beta_n, \quad \alpha_i = \beta_i \ \ \forall i \neq k, n,$$

и в этом случае необходимо показать, что выполнено хотя бы одно из равенств: $f_k(\alpha) = f_k(\beta)$ или $f_n(\alpha) = f_n(\beta)$.

Положим $S = \alpha_1 \oplus \ldots \oplus \alpha_n = \beta_1 \oplus \ldots \oplus \beta_n$. Тогда мы имеем:

$$f_k(\alpha) = \alpha_1 \oplus \ldots \oplus \alpha_{k-1} \oplus \bigoplus_{i<j,\ i,j\neq k,n}^{n} \alpha_i\alpha_j \oplus \alpha_n\Big(S \oplus \alpha_k \oplus \alpha_n\Big),$$

$$f_k(\beta) = \beta_1 \oplus \ldots \oplus \beta_{k-1} \oplus \bigoplus_{i<j,\ i,j\neq k,n}^{n} \beta_i\beta_j \oplus \beta_n\Big(S \oplus \beta_k \oplus \beta_n\Big).$$

Линейные части обоих выражений, а также квадратичная часть, не содержащая членов α_n и β_n (выделена в отдельную сумму), совпадают. С учетом того, что $\alpha_n \oplus \beta_n = 1$, а также $\alpha_k \oplus \alpha_n = \beta_k \oplus \beta_n$, мы имеем:

$$f_k(\alpha) \oplus f_k(\beta) = \alpha_n(S \oplus \alpha_k \oplus \alpha_n) \oplus \beta_n(S \oplus \beta_k \oplus \beta_n) = S \oplus \alpha_k \oplus \alpha_n.$$

Аналогично можно прийти к соотношению для f_n:

$$f_n(\alpha) = S \oplus \alpha_n \oplus \bigoplus_{i<j,\ i,j\neq k,n}^{n} \alpha_i\alpha_j \oplus \alpha_k(S \oplus \alpha_k \oplus \alpha_n),$$

$$f_n(\beta) = S \oplus \beta_n \oplus \bigoplus_{i<j,\ i,j\neq k,n}^{n} \beta_i\beta_j \oplus \beta_k(S \oplus \beta_k \oplus \beta_n),$$

$$f_n(\alpha) \oplus f_n(\beta) = \alpha_n \oplus \beta_n \oplus (\alpha_k \oplus \beta_k)(S \oplus \alpha_k \oplus \alpha_n) = S \oplus \alpha_k \oplus \alpha_n \oplus 1.$$

Таким образом, либо $f_k(\alpha) = f_k(\beta)$, либо $f_n(\alpha) = f_n(\beta)$, из чего следует выполнение свойства правильности и в этом случае. □

Сделаем несколько наблюдений касательно приведенного класса правильных семейств.

1. Все семейства класса при $n \geqslant 3$ не являются треугольным: каждая функция в семействе существенно зависит от всех неодноименных переменных.
2. Каждое из семейств класса при $n \geqslant 3$ имеет полный граф существенной зависимости.

3. Полином Жегалкина каждого из семейств класса при $n \geqslant 3$ имеет степень 2, что может быть использовано при построении квадратичных квазигрупп [71].

Уточним последнее замечание.

Теорема 3. *Для $n \geqslant 3$ семейство (1.5) является квадратичным строгого типа $Quad^s_{n-1}Lin^s_1$ (см. определение 21) при четных n и квадратичным строгого типа $Quad^s_nLin^s_0$ (сильно квадратичным) при нечетных n.*

Доказательство. Рассмотрим линейную комбинацию $h = \alpha_1 f_1 \oplus \ldots \oplus \alpha_n f_n$. При мономе $x_i x_j$ в h стоит коэффициент $A \oplus \alpha_i \oplus \alpha_j$, где $A = \alpha_1 \oplus \ldots \oplus \alpha_n$. Рассмотрим условия на коэффициенты $\alpha_1, \ldots, \alpha_n$, при которых квадратичная часть h обращается в нуль. Для этого необходимо потребовать, чтобы $A \oplus \alpha_i \oplus \alpha_j = 0$ для всех $1 \leqslant i < j \leqslant n$. Из этих условий следует, что все α_i должны быть равны:

$$A \oplus \alpha_1 \oplus \alpha_2 = A \oplus \alpha_2 \oplus \alpha_l, \quad l = 3, \ldots, n,$$

а значит, $\alpha_1 = \alpha_l$, $l = 3, \ldots, n$, а также

$$A \oplus \alpha_1 \oplus \alpha_2 = A \oplus \alpha_1 \oplus \alpha_3,$$

а значит, $\alpha_2 = \alpha_3$. При четных n у этой системы уравнений есть нетривиальное решение $\alpha_1 = \ldots = \alpha_n = 1$, любая отличная от данной нетривиальная линейная комбинация не обнуляет квадратичную часть, а значит, для четных $n \geqslant 3$ семейство $\mathcal{F}_n$ является квадратичным строгого типа $Quad^s_{n-1}Lin^s_1$. Для нечетных n у системы уравнений нет нетривиальных решений, и следовательно, для нечетных n семейство $\mathcal{F}_n$ является квадратичным строгого типа $Quad^s_nLin^s_0$. □

1.3.4 Элементарные свойства правильных семейств

В настоящем разделе сформулируем некоторые базовые свойства правильных семейств. Ранее (см. раздел 1.2.4) мы ввели преобразования сдвига (определение 22), перестановки (определение 24) и проекции (определение 25). Известно, что эти преобразования сохраняют свойство семейства быть правильным.

Утверждение 9 ([50, замечание 1]). *Пусть $\mathcal{F}_n$ — правильное семейство на $Q_1 \times \ldots \times Q_n$, $\mathbf{s} \in Q_1 \times \ldots \times Q_n$. Тогда семейство $\mathcal{G}_n(\mathbf{x}) = \mathcal{F}_n(\mathbf{x}) \circ \mathbf{s}$ также является правильным.*

Теорема 4. *Пусть $\mathcal{F}_n$ — правильное семейство на $Q_1 \times \ldots \times Q_n$, $\mathbf{s} \in Q_1 \times \ldots \times Q_n$. Тогда семейство $\mathcal{G}_n(\mathbf{x}) = \mathcal{F}_n(\mathbf{x} \circ \mathbf{s})$ также является правильным.*

Доказательство. Пусть $\mathbf{x}, \mathbf{y} \in Q_1 \times \ldots \times Q_n$ — два неравных набора, рассмотрим наборы $\mathbf{u} = \mathbf{x} \circ \mathbf{s}$, $\mathbf{v} = \mathbf{y} \circ \mathbf{s}$. Заметим, что $x_i \neq y_i$ эквивалентно утверждению $u_i \neq v_i$ (следует из свойства сокращения в квазигруппе Q_i). По свойству правильности семейства $\mathcal{F}_n$ найдется индекс i, что $u_i \neq v_i$, но $f_i(\mathbf{u}) = f_i(\mathbf{v})$. Таким образом, найдется индекс i, что $x_i \neq y_i$, но $g_i(\mathbf{x}) = g_i(\mathbf{y})$. □

Утверждение 10 ([50, замечание 3]). *Пусть $\mathcal{F}_n$ — правильное семейство на Q^n. Тогда семейство $\mathcal{G}_n(\mathbf{x}) = \sigma(\mathcal{F}_n)(\mathbf{x})$ также является правильным.*

Утверждение 11 ([55, лемма 1]). *Пусть $\mathcal{F}_n$ — правильное семейство на $Q_1 \times \ldots \times Q_n$, $i \in \{1, \ldots, n\}$, $q \in Q_i$. Тогда $\Pi_i^q(\mathcal{F}_n)$ также является правильным семейством на $Q_1 \times \ldots \times Q_{i-1} \times Q_{i+1} \times \ldots \times Q_n$.*

Указанные преобразования могут быть использованы для получения новых правильных семейств из уже заданных. Также некоторые свойства квазигрупп, задаваемых правильными семействами, сохраняются при переходе к эквивалентному (в смысле действия некоторой группы) семейству, что иногда позволяет сократить перебор.

В работах [58; 59] предложен алгоритм генерации равномерного распределения на множестве правильных семейств с помощью MCMC-алгоритма: предложен способ перехода от некоторого фиксированного правильного семейства $\mathcal{F}$ к новому правильному семейству $\mathcal{F}'$ с помощью итеративного применения процедуры

$$\mathsf{Switch}(\mathcal{F}, i, \alpha),\ 1 \leqslant i \leqslant n,\ \alpha \in \mathbb{E}_k^*,$$

которая задается следующим образом:

- рассмотреть все возможные проекции $\mathcal{F}^q := \Pi_i^q(\mathcal{F}_n)$, $q \in \mathbb{E}_k$;
- рассмотреть граф с множеством вершин $V = \mathbb{E}_k^{n-1}$, в котором проводится неориентированное ребро от вершины $\mathbf{u} = (u_1, \ldots, u_{n-1})$ к вершине $\mathbf{v} = (v_1, \ldots, v_{n-1})$ тогда и только тогда, когда найдется пара индексов $1 \leqslant i, j \leqslant n-1$, $i \neq j$ таких, что $\mathcal{F}^i(\mathbf{u})$ и $\mathcal{F}^j(\mathbf{v})$ отличаются во всех позициях, в которых отличаются $\mathbf{u}$ и $\mathbf{v}$;

– найти компоненты связности полученного графа и перенумеровать их;
– задать значение функции f_i: на j-й компоненте связности полученного графа зададим $f_i \coloneqq \alpha[j]$.

Для порождения равномерного распределения на множестве всех правильных семейств заданного размера предлагается MCMC-процедура: алгоритм стартует с тождественно равного нулю правильного семейства, на каждом шаге случайно выбирается номер i для проекции и набор α (значения функции f_i на полученных компонентах связности).

1.4 Свойства квазигрупп

В этом разделе мы кратко рассмотрим основные алгебраические свойства квазигрупп, релевантные с точки зрения криптографических приложений: количество ассоциативных троек, полиномиальную полноту, наличие подквазигрупп. Приводится обзор существующих результатов по каждому из направлений.

Упомянутые свойства, а также некоторые другие (в частности, отсутствие левой и правой единицы в квазигруппе), указаны среди основных требований к используемой квазигруппе в работе [13], где рассматриваются т.н. «бесформенные» (shapeless) квазигруппы. Заметим также, что существуют также «геометрические» (т.н. «нефрактальность», см. работы [86; 87]) и «статистические» (см. работы [88—91]) подходы к оценке криптографического качества квазигруппы.

1.4.1 Количество ассоциативных троек

Для того, чтобы некоторые криптографические примитивы, основанные на квазигрупповом умножении (см. также раздел 4.1), были стойкими к криптоанализу, необходимо, чтобы в квазигруппе было как можно меньше ассоциативных троек, то есть, чтобы квазигрупповая операция была как можно менее ассоциативна. Так, например, большое количество ассоциативных троек может быть использовано при нахождении коллизий и вторых прообразов для некоторых

хэш-функций, построенных на основе квазигруппового умножения [92]. Следовательно, с практической точки зрения интересны следующие вопросы:

- каково минимально возможное (и достижимое) число ассоциативных троек для квазигрупп заданного размера;
- можно ли построить классы квазигрупп с заданным малым числом ассоциативных троек;
- можно ли найти квазигруппы с малым числом ассоциативных троек и компактным описанием (в частности, для которых не нужно было бы хранить всю таблицу умножения в компьютере, а вычислять результат квазигрупповой операции более эффективно)?

Указанные вопросы, а также тесно связанные с ними (например, каково *минимально возможное* число неассоциативных троек в неассоциативной квазигруппе заданного порядка?) изучались с 1980-х годов и в отрыве от практических приложений (см. работы [64; 65; 93—95], а также [3, задача 1.1]). Таким образом, сформулированные вопросы интересны как с точки зрения практики, так и чисто теоретически. В этом разделе мы рассматриваем большинство полученных на данный момент результатов по количеству ассоциативных троек в квазигруппах, а также приводим результаты исследований, описывающих количество ассоциативных троек в квазигруппах, задаваемых правильными семействами булевых функций малых размеров. Результаты, полученные в настоящем разделе, были описаны в работе [80].

Предварительные сведения

Определение 33. Ассоциативной тройкой называется тройка элементов квазигруппы $a, b, c \in Q$ таких, что выполнено равенство:

$$(a \circ b) \circ c = a \circ (b \circ c).$$

Если указанное равенство не выполняется, то тройка называется неассоциативной.

Определение 34 ([65])**.** Индексом ассоциативности $a(Q)$ квазигруппы Q называется число ассоциативных троек в ней.

Индекс ассоциативности, как было отмечено выше (см. раздел 1.4.1), является важной характеристикой квазигруппы, которая, в частности, показывает, насколько квазигрупповая операция близка к групповой. В дальнейшем изложении нам понадобятся следующие обозначения.

- $a(Q)$: индекс ассоциативности квазигруппы Q;
- $b(Q)$: число неассоциативных троек в квазигруппе Q;
- $a(n)$: минимальное число ассоциативных троек среди всех квазигрупп порядка n;
- $a(n, C)$: минимальное число ассоциативных троек среди всех квазигрупп из класса C порядка n;
- $b(n)$: минимальное число неассоциативных троек среди всех неассоциативных квазигрупп порядка n;
- $b(n, C)$: минимальное число неассоциативных троек среди всех квазигрупп из класса C порядка n.

Оценки на число ассоциативных троек

Очевидно, что число ассоциативных троек в квазигруппе не может превышать $|Q|^3$ — общего числа всех троек элементов в квазигруппе. Данная оценка достижима при условии что Q — группа. Можно легко получить следующую универсальную для всех квазигрупп оценку.

Утверждение 12 ([66]). *Выполняется следующее двойное неравенство:*

$$n \leqslant a(n) \leqslant n^3.$$

Утверждение следует из того факта, что в любой квазигруппе для каждого элемента $x \in Q$ существует левая и правая единицы $le(x), re(x) \in Q$ со свойством $le(x) \circ x = x = x \circ re(x)$. Тогда для каждого $x \in Q$ тройка $(le(x), x, re(x))$ является ассоциативной:

$$(le(x) \circ x) \circ re(x) = x = le(x) \circ (x \circ re(x)).$$

Одной из первых работ, в которых изучалось число ассоциативных троек в алгебраических структурах, является работа [93], автор которой исследовал коммутативные группоиды. В работе [93] было показано, что для коммутативного

неассоциативного группоида Q порядка n верны оценки:

$$n^2 \leqslant a(Q) \leqslant n^3 - 2,$$

причем каждая из границ достижима в классе коммутативных группоидов (при $n \geqslant 3$). Также в указанной работе были рассмотрены классы коммутативных квазигрупп, изотопных группам, коммутативных медиальных [82, глава 2, определение 7] квазигрупп и несколько других классов, для каждого из которых получены похожие оценки ($\Theta(n^2)$ для нижней границы и $\Theta(n^3)$ для верхней).

Работа [64] также посвящена группоидам (а именно, классу группоидов с сокращением, частными случаями которых являются квазигруппы). Следствием результатов из работы [64] является неравенство $b(n) \geqslant n$ (т.е. число неассоциативных троек в группоидах Q с сокращениями не может быть меньше, чем $|Q|$)

В работе [94] был рассмотрен класс квазигрупп, изотопных группам, и на него были расширены некоторые результаты из работы [93]. Общим результатом этих работ является следующее наблюдение.

Утверждение 13 ([94, теорема 5.1])**.** *Пусть C — класс всех неассоциативных квазигрупп Q, изотопных группам. Тогда:*

$$b(n, C) \geqslant \begin{cases} 4n^2 - 6n, \ n \geqslant 3, \ n \textit{ нечетно;} \\ 4n^2 - 8n, \ n \textit{ четно.} \end{cases}$$

Работа [95] посвящена смежному вопросу: каково минимальное число неассоциативных троек в неассоциативной квазигруппе? В [95] для исследования величины $b(Q)$ вводится следующая характеристика квазигрупповой операции.

Определение 35. Для квазигруппы $(Q, \circ)$ определим расстояние до группы $\mathsf{gdist}(Q)$ как минимум среди чисел $\mathsf{dist}(Q, G)$, где $(G, \cdot)$ — группа, заданная на том же множестве, что и квазигруппа Q, а функция dist определена следующим образом:

$$\mathsf{dist}(Q, G) = |\{(x, y) \in Q^2 \mid x \circ y \neq x \cdot y\}|.$$

Утверждение 14 ([95, утверждение 4.1])**.** *Пусть Q — квазигруппа порядка n, $t = \mathsf{gdist}(Q)$. Тогда выполнены следующие неравенства:*

1. $4tn - 2t^2 - 24t \leqslant b(Q) \leqslant 4tn$.
2. *если* $t \geqslant 24$, *то* $b(Q) \geqslant 4tn - 2t^2 - 16t$.

Также в [95] показано, что для всех $n \geqslant 6$ выполняется неравенство

$$b(n) \leqslant 16n - 64.$$

Обозначим через $i(Q) = |\{x \in Q \mid x \circ x = x\}|$ количество идемпотентов (см. определение 9) в квазигруппе Q. Основным результатом работы [96] является связь чисел $i(Q)$ и $a(Q)$.

Утверждение 15 ([96, теорема 1.1])**.** *Для квазигруппы Q выполняется следующее неравенство:*

$$a(Q) \geqslant 2n - i(Q).$$

В частности, из этого результата следует, что если в квазигруппе Q порядка n число ассоциативных троек $a(Q)$ также равно n (т.е. достигается нижняя граница на число ассоциативных троек для квазигруппы порядка n), то каждый элемент квазигруппы является идемпотентом: $i(Q) = n$. Заметим, что с криптографической точки зрения это требование входит в противоречие с требованием отсутствия подквазигрупп [13; 97] (в частности, подквазигрупп размера 1).

Дальнейшие продвижения были получены в работе [98]. Обозначим через $\delta_L(Q)$ число элементов $a \in Q$, таких что подстановка L_a (см. замечание 1) не имеет неподвижных точек, через $\delta_R(Q)$ — число элементов $a \in Q$, таких что подстановка R_a не имеет неподвижных точек.

Утверждение 16 ([98, теорема 2.5])**.** *Выполнено следующее неравенство:*

$$a(Q) \geqslant 2n - i(Q) + \delta_L(Q) + \delta_R(Q).$$

Таким образом, если для квазигруппы Q порядка n достигается минимально возможное число ассоциативных троек $a(Q) = n$, то в Q каждый элемент является идемпотентом (т.е., $i(Q) = n$), и у отображений L_a, R_a нет неподвижных точек.

Примеры квазигрупп с заданным числом ассоциативных троек

В работах [65; 66] приведены несколько примеров классов квазигрупп с малым числом ассоциативных троек, что позволяет получить верхние оценки на минимальное число ассоциативных троек $a(n)$.

Так, для случая $n \neq 2 \bmod 4$ строится квазигруппа Q на основе коммутативной квазигруппы $(G, +)$ и автоморфизма $\varphi \in Aut(G)$ со свойством

$$\varphi(x) \neq x \qquad \forall x \in G \backslash \{0\}.$$

Операция $x \circ y$ задается следующим образом:

$$x \circ y = \varphi(x + y).$$

Для полученной квазигруппы Q верно равенство $a(Q) = n^2$, а следовательно,

$$a(n) \leqslant n^2, \quad n \neq 2 \bmod 4.$$

Для случая $n = 2 \bmod 4$ можно построить квазигруппу Q с индексом ассоциативности $a(Q) = 2n^2$, а следовательно,

$$a(n) \leqslant 2n^2, \quad n = 2 \bmod 4.$$

В работе [65] приведен пример класса квазигрупп размера n, где $n \geqslant 6$, $n = 0, 2 \bmod 6$, с количеством ассоциативных троек $a(Q) = n^2 - 3n + 3$. Таким образом, в случае $n \geqslant 6$, $n = 0, 2 \bmod 6$ мы получаем оценку

$$a(n) \leqslant n^2 - 3n + 3.$$

В ряде статей [99—101] были получены примеры классов **максимально неассоциативных** квазигрупп, т.е. квазигрупп, для которых $a(Q) = |Q|$. В статье [99] была дана конструкция на основе т.н. почтиполей (см., например, [102]), из которой следует, что $a(n) = n$ для $n = 2^{6k} \cdot r^2$, где $k \geqslant 0$, r нечетное. В частности, $a(p^2) = p^2$ для всех нечетных простых чисел p.

Указанный результат был расширен в статьях [100] и [101]. Обозначим через $\nu_p(n)$ такое число e, что $p^e \mid n$, но $p^{e+1} \nmid n$. В статье [101] показано, что для n, удовлетворяющих условиям:

$$\nu_p(n) \neq 1,\ p \in \{3, 5, 7, 11\}, \quad \nu_2(n) \neq 2, 4 \text{ и четно},$$

существует максимально неассоциативная квазигруппа порядка n.

В статье [100] показано, что максимально неассоциативная квазигруппа существует для всех достаточно больших порядков n, которые **не имеют** вид $n = 2p_1$ или $n = 2p_1p_2$, где p_1, p_2 — нечетные простые, $p_1 \leqslant p_2 < 2p_1$. В частности, существует максимально неассоциативная квазигруппа для простых порядков $p \geqslant 13$.

Выводы

Таким образом, из ряда вышеприведенных работ следует, что:

1. $a(n) \geqslant 2n - i(Q) + \delta_L(Q) + \delta_R(Q)$.
2. $a(n) \leqslant n^2, \quad n \geqslant 3, \quad n \neq 4k+2$.
3. $a(n) \leqslant 2n^2, \quad n \geqslant 3$.
4. $a(n) \leqslant n^2 - 3n + 3, \quad n \geqslant 6, n \equiv 0, 2 \bmod 6$.
5. Доказано существование максимально неассоциативных квазигрупп размера n (т.е. $a(n) = n$) для большого класса чисел n (см. конструкции на основе полей и почтиполей).

Оценка среднего числа ассоциативных троек

В работах [92; 103] предложен еще один подход к подсчету числа ассоциативных троек в квазигруппах. Как известно (см., например, [104]), ассоциативные тройки можно рассматривать как неподвижные точки коммутатора отображений $[L_a, R_b]$, где $[x, y] = x^{-1}y^{-1}xy$: если (a, x, b) — ассоциативная тройка, то выполняется условие

$$(a \circ x) \circ b = R_b(L_a(x)) = a \circ (x \circ b) = L_a(R_b(x)),$$

то есть x является неподвижной точкой коммутатора: $[L_a, R_b](x) = x$.

В работах [92; 103] предложено оценивать среднее число ассоциативных троек в квазигруппе, где усреднение берется по всем главным изотопам. Обозначим через $Q_{\alpha\beta}$ главный изотоп Q, заданный операцией

$$a * b = \alpha(a) \circ \beta(b)$$

Утверждение 17 ([103, утверждение 2.1])**.** *Выполнено следующее равенство:*

$$\frac{1}{(n!)^2} \sum_{\alpha,\beta \in \mathcal{S}_Q} a(Q_{\alpha\beta}) = \frac{n^3}{n-1}.$$

Идея доказательства состоит в подсчете числа неподвижных точек всех коммутаторов $[L_a, R_b]$ для всех главных изотопов, что, в свою очередь, сводится к

задаче подсчета суммы

$$\sum_{\varphi,\psi\in\mathcal{S}_Q} |Fix([\varphi,\psi])|,$$

где $Fix(\pi) = \{x \in Q \mid \pi(x) = x\}$ — множество неподвижных точек подстановки $\pi \in \mathcal{S}_Q$.

Следующее утверждение следует из предыдущего.

Утверждение 18 ([92, следствие 3.5])**.** *Выполнено следующее равенство:*

$$\frac{1}{(n!)^3} \sum_{\alpha,\beta,\gamma\in\mathcal{S}_Q} a(Q_{\alpha\beta\gamma}) = \frac{n^3}{n-1}.$$

Таким образом, для каждой квазигруппы среднее число ассоциативных троек (при усреднении по всем изотопам квазигруппы) примерно равно n^2.

Утверждение 19 ([103, утверждение 2.3])**.** *Выполнено неравенство:*

$$\frac{1}{n!} \sum_{\beta} a(Q_{\alpha\beta}) \geqslant n^2,$$

и равенство достигается тогда и только тогда, когда α^{-1} — ортоморфизм квазигруппы Q.

Минимальное число ассоциативных троек в квазигруппах малого порядка

В ряде работ [66; 92; 96] путем перебора были получены точные значения минимального числа ассоциативных троек $a(n)$ для квазигрупп порядка $n \leqslant 7$ (см. таб. 1). Для квазигрупп порядка $n = 8, 9$ число $a(n)$ уже не может быть получено путем полного перебора, поэтому в работах [98; 105; 106] был предложен способ сократить перебор. С помощью ограниченного перебора были получены точные значения чисел $a(8)$, $a(9)$ и получена оценка снизу для $a(10)$ (а именно, было показано, что не существует квазигрупп порядка 10 с индексом ассоциативности 10). Полученные результаты отображены в Таб. 1. Заметим, что полученные значения меньше существующих теоретических оценок, приведенных в разделе 1.4.1.

Таблица 1 — Минимальное число ассоциативных троек для квазигрупп порядка $n \leqslant 10$

n	$a(n)$	Работа
1	1	[66]
2	8	[66]
3	9	[66]
4	16	[66]
5	15	[66]
6	16	[66]
7	17	[92]
8	16	[98]
9	9	[105]
10	> 10	[106]

Некоторые результаты о виде ассоциативных троек в квазигруппах, заданных правильными семействами

Обобщим конструкцию, обозначенную в замечании 11. Пусть $\mathcal{F}$, $\mathcal{G}$ — два правильных семейства функций размера n над группой $(G^n, +)$. Для $\mathbf{x}, \mathbf{y} \in G^n$ зададим операцию $\circ$ следующим образом:

$$\mathbf{x} \circ \mathbf{y} = \mathbf{x} + \mathcal{F}(\mathbf{x}) + \mathbf{y} + \mathcal{G}(\mathbf{y}).$$

Поскольку отображение $\mathbf{x} \to \pi_{\mathcal{F}}(\mathbf{x}) = \mathbf{x} + \mathcal{F}(\mathbf{x})$, где $\mathcal{F}$ — правильное, является биекцией, то операция $\circ$ задает главный изотоп группы G^n (а значит, задает квазигрупповую операцию).

Потребуем дополнительно, чтобы группа G^n была коммутативной, и рассмотрим условие на ассоциативность тройки $(\mathbf{x},\mathbf{y},\mathbf{z})$ в квазигруппе Q, построенной по паре правильных семейств $(\mathcal{F}, \mathcal{G})$:

$$(\mathbf{x} \circ \mathbf{y}) \circ \mathbf{z} = (\mathbf{x} + \mathcal{F}(\mathbf{x})) + (\mathbf{y} + \mathcal{G}(\mathbf{y})) + \\ + (\mathbf{z} + \mathcal{G}(\mathbf{z})) + \mathcal{F}(\mathbf{x} + \mathcal{F}(\mathbf{x}) + \mathbf{y} + \mathcal{G}(\mathbf{y})),$$

$$\mathbf{x} \circ (\mathbf{y} \circ \mathbf{z}) = (\mathbf{x} + \mathcal{F}(\mathbf{x})) + (\mathbf{y} + \mathcal{F}(\mathbf{y})) + \\ + (\mathbf{z} + \mathcal{G}(\mathbf{z})) + \mathcal{G}(\mathbf{y} + \mathcal{F}(\mathbf{y}) + \mathbf{z} + \mathcal{G}(\mathbf{z})),$$

и из условия $(\mathbf{x} \circ \mathbf{y}) \circ \mathbf{z} = \mathbf{x} \circ (\mathbf{y} \circ \mathbf{z})$ получаем, что:

$$\mathcal{F}(\mathbf{y}) - \mathcal{G}(\mathbf{y}) = \mathcal{F}(\mathbf{x} + \mathcal{F}(\mathbf{x}) + \mathbf{y} + \mathcal{G}(\mathbf{y})) - \mathcal{G}(\mathbf{y} + \mathcal{F}(\mathbf{y}) + \mathbf{z} + \mathcal{G}(\mathbf{z})). \qquad (1.6)$$

Из подобного эквивалентного представления относительно легко следуют два наблюдения, которые могут быть доказаны прямой проверкой.

Теорема 5. *Тройка $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ является ассоциативной в квазигруппе $(G^n, \circ)$, построенной по паре семейств $(\mathcal{F}, \mathcal{G})$, тогда и только тогда, когда тройка $(\mathbf{z}, \mathbf{y}, \mathbf{x})$ является ассоциативной в квазигруппе, построенной по паре семейств $(\mathcal{G},\mathcal{F})$.*

В частности, индексы ассоциативности квазигрупп, построенных по парам семейств $(\mathcal{F}, \mathcal{G})$ и по парам семейств $(\mathcal{G}, \mathcal{F})$, совпадают.

Теорема 6. *Пусть $\mathcal{A}$ — такое обратимое линейное отображение (т.е. $\mathcal{A}(\mathbf{x}+\mathbf{y}) = \mathcal{A}(\mathbf{x}) + \mathcal{A}(\mathbf{y})$), что семейства*

$$\mathcal{F}'(\mathbf{x}) = \mathcal{A}^{-1}(\mathcal{F}(\mathcal{A}(\mathbf{x}))), \quad \mathcal{G}'(\mathbf{y}) = \mathcal{A}^{-1}(\mathcal{G}(\mathcal{A}(\mathbf{y})))$$

также являются правильными (так, в качестве $\mathcal{A}$ можно рассмотреть преобразование обратимой линейной перекодировки, см. раздел 3.1.1). В таком случае $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ является ассоциативной тройкой для квазигруппы, построенной по паре правильных семейств $(\mathcal{F}, \mathcal{G})$, тогда и только тогда, когда тройка $(\mathcal{A}^{-1}(\mathbf{x}), \mathcal{A}^{-1}(\mathbf{y}), \mathcal{A}^{-1}(\mathbf{z}))$ является ассоциативной для квазигруппы, построенной по паре правильных семейств $(\mathcal{F}', \mathcal{G}')$.

В частности, индексы ассоциативности квазигрупп, построенных по парам семейств $(\mathcal{F}, \mathcal{G})$ и $(\mathcal{F}', \mathcal{G}')$, совпадают.

В случае $G^n = \mathbb{Z}_2^n$ выполняется несколько дополнительных свойств.

Теорема 7. *Тройка $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ является ассоциативной для квазигруппы, построенной по паре правильных семейств $(\mathcal{F}, \mathcal{G})$, тогда и только тогда, когда она является ассоциативной для квазигруппы, построенной по паре правильных семейств $(\mathcal{F} \oplus \alpha, \mathcal{G} \oplus \alpha)$, где $\alpha \in \mathbb{Z}_2^n$.*

Утверждение следует из равенства (1.6) путем прямой подстановки значений.

Теорема 8. *Количество ассоциативных троек в квазигруппе, построенной по паре правильных булевых семейств $(\mathcal{F}, \mathcal{G})$, четно.*

Доказательство. Зафиксируем значения $\mathbf{x}$, $\mathbf{y}$ и найдем все значения $\mathbf{z}$, которые удовлетворяют требованию ассоциативности (1.6):

$$\mathcal{F}(\mathbf{y}) \oplus \mathcal{G}(\mathbf{y}) = \mathcal{F}(\mathbf{x} \oplus \mathcal{F}(\mathbf{x}) \oplus \mathbf{y} \oplus \mathcal{G}(\mathbf{y})) \oplus \mathcal{G}(\mathbf{y} \oplus \mathcal{F}(\mathbf{y}) \oplus \mathbf{z} \oplus \mathcal{G}(\mathbf{z})).$$

После фиксации $\mathbf{x}$, $\mathbf{y}$, мы получим уравнение на $\mathbf{z}$ вида

$$\mathcal{G}(\mathbf{z} \oplus \mathcal{G}(\mathbf{z}) \oplus \alpha) = \beta, \quad \alpha, \beta \in \mathbb{Z}_2^n. \tag{1.7}$$

Как показано в теореме 20 (см. раздел 3.2.1), уравнение вида $\mathcal{G}(t) = \beta$ всегда имеет четное число решений для булевых правильных семейств. Поскольку отображение $\mathbf{z} \to \mathbf{z} \oplus \mathcal{G}(\mathbf{z}) \oplus \alpha$ является биекцией, для каждой фиксации переменных $\mathbf{x}$, $\mathbf{y}$ уравнение (1.7) будет иметь четное число решений $\mathbf{z}$. Тем самым мы получим четное число ассоциативных троек. □

Указанные свойства могут быть использованы при исследовании индексов ассоциативности квазигрупп, построенных по различным парам правильных семейств.

Алгоритмы проверки ассоциативности

В книге [107, раздел 1.2] приводится алгоритм проверки ассоциативности для произвольного группоида, который работает со сложностью порядка $\mathcal{O}(k^2 \log k)$ операций вычисления умножения в группоиде (тест Лайта с добавлением процедуры вычисления множества порождающих квазигруппы [108] размера $\sim \log k$ с временной сложностью $\mathcal{O}(k^2)$ операций).

В работе [109] был предложен вероятностный алгоритм проверки ассоциативности операции «$\circ$»:

– если $\circ$ ассоциативна, то алгоритм всегда выдает верный ответ (операция ассоциативна);

– если $\circ$ неассоциативна, то алгоритм может ошибаться с вероятностью ε.

Было показано, что время работы алгоритма оценивается величиной $\mathcal{O}(k^2 \cdot \log \frac{1}{\varepsilon})$. В той же работе было показано, что не может быть существенно более быстрого вероятностного (классического) алгоритма, а именно, была получена нижняя

оценка времени работы алгоритма в общем случае вида $\mathcal{O}(k^2)$ (для квантовых алгоритмов существуют как стандартные методы ускорения алгоритма, наподобие алгоритма Гровера, так и более быстрые специфические процедуры [110]).

Наконец, в работе [111] был предложен алгоритм со сложностью $\Theta(k^2)$ в модели вычислений RAM (равнодоступная адресная машина, см., например, [112, раздел 2.2]).

Для задачи нахождения числа ассоциативных троек существует «наивный» алгоритм со сложностью порядка $\mathcal{O}(k^3)$. При поиске примеров квазигрупп с минимальным числом ассоциативных троек может быть использован алгоритм, работающий для частично построенных таблиц умножения [105].

1.4.2 Полиномиальная полнота

Помимо малого количества ассоциативных троек одним из важных условий в контексте криптографических приложений является полиномиальная полнота алгебраической структуры, над которой мы строим криптографический механизм. Как было показано в работах [61] и [62], задача проверки разрешимости уравнения (и системы уравнений) над полиномиально (функционально) полной алгеброй является NP-полной задачей (об NP-полных задачах см., например, [112, глава 34]): сертификатом для неё является запись конкретного решения уравнения или системы, полнота следует из представимости задачи 3SAT в виде уравнения над полиномиально полной алгеброй. Свойство полиномиальной полноты дает дополнительные гарантии сложности разрешимости задач, используемых как базовые в криптографических приложениях.

Обозначим через $\mathcal{O}^m(Q)$ множество всех m-арных операций на множестве Q:

$$\mathcal{O}^m(Q) = \{f \mid f\colon Q^m \to Q\}.$$

Также введем обозначение $\mathcal{O}(Q) = \cup_{m=0}^{\infty}\mathcal{O}^m(Q)$. Пусть $(Q, \circ)$ — некоторая конечная квазигруппа, $Q = \{q_1, \ldots, q_k\}$, через $[X]$ обозначим операцию замыкания множества функций X (см., например, [84, часть I, параграф 5]).

Определение 36. Квазигруппа Q называется полиномиально полной (как алгебра с одной операцией), если замыкание операции $\circ$ и всех нуль-арных функций

(констант) порождает все множество функций на Q:

$$[\{\circ\} \cup \mathcal{O}^0(Q)] = \mathcal{O}(Q).$$

Другими словами, квазигруппа полиномиально полна, когда любую m-арную функцию $Q^m \to Q$, $m \in \mathbb{N}_0$, можно выразить через операцию умножения $\circ$ в квазигруппе и подстановку констант.

Замечание 18. Также мы можем рассматривать полиномиальную полноту квазигруппы как алгебры с тремя операциями: «$\circ$», «$\backslash$», «$/$», где последние две операции задаются равенствами [82]:

$$a \circ x = b \Leftrightarrow x = a\backslash b,$$
$$x \circ a = b \Leftrightarrow x = a/b.$$

В работе [60] было показано, что для конечных алгебр полиномиальная полнота эквивалентна существованию т.н. «мальцевского оператора» в множестве всех операций над Q совместно с требованием простоты и неаффинности алгебры. В [113] отмечено, что квазигруппы как алгебры с тремя операциями (см. замечание 18) имеют как минимум два мальцеских оператора; несложно показать, что в этом случае вопрос изучения полиномиальной полноты по сути сводится к вопросу о простоте и неаффинности квазигруппы. Аналогичный результат верен и для (d-)квазигрупп как алгебр с одной операцией [114]. Далее в разделе мы формально введем все упомянутые понятия и рассмотрим существующие результаты.

Из результатов работ [115; 116] следует, что почти все квазигруппы полиномиально полны (т.е. доля полиномиально полных квазигрупп среди всех квазигрупп порядка k при $k \to \infty$ стремится к 1). В работе [117] указанный результат усилен: почти все квазигруппы сильно полиномиально полны (т.е. не изотопны квазигруппам, не являющимся полиномиально полными).

Критерии и достаточные условия полиномиальной полноты

Как было отмечено выше, для квазигрупп полиномиальная полнота эквивалентна простоте и неаффинности.

Определение 37. Пусть задано некоторое разбиение $A_1, \ldots, A_t$ множества Q (см. раздел 1.2.2). Введем отношение эквивалентности: $a \sim b$, если $a, b \in A_i$, то есть принадлежат одному и тому же блоку разбиения. Квазигруппа $(Q, \circ)$ сохраняет разбиение $A_1 \sqcup \ldots \sqcup A_t$, если для любой пары наборов (a_1, a_2), (b_1, b_2) из выполнения равенств $a_1 \sim b_1$ и $a_2 \sim b_2$ следует $a_1 \circ a_2 \sim b_1 \circ b_2$.

Определение 38. Квазигруппа $(Q, \circ)$ называется простой, если она не сохраняет никакое нетривиальное разбиение.

Определение 39. Квазигруппа $(Q, \circ)$ называется аффинной (или T-квазигруппой), если на множестве Q можно так ввести структуру абелевой группы $(Q, +)$, что квазигрупповая операция выражается через введенную групповую следующим образом:

$$x \circ y = \varphi(x) + \psi(y) + c,$$

где $\varphi, \psi \in Aut(Q, +)$, $c \in Q$.

Можно дать несколько альтернативных характеризаций указанных выше свойств квазигруппы, связанных с полиномиальной полнотой.

Определение 40. Обозначим через $Mult(Q)$ группу всех подстановок, порождаемых левыми и правыми сдвигами:

$$Mult(Q) = \langle L_{q_1}, \ldots, L_{q_k}, R_{q_1}, \ldots, R_{q_k} \rangle.$$

Определение 41. Обозначим через $G(Q)$ подгруппу в группе $Mult(Q)$, порождаемую следующими подстановками:

$$G(Q) = \langle L_{q_i} \circ L_{q_j}^{-1},\ R_{q_i} \circ R_{q_j}^{-1}, 1 \leqslant i, j \leqslant k \rangle.$$

Можно получить несколько достаточных условий полиномиальной полноты в терминах групп $Mult(Q)$ и $G(Q)$.

Утверждение 20 ([97])**.** *Квазигруппа Q проста тогда и только тогда, когда $Mult(Q)$ действует примитивно на Q.*

Утверждение 21 ([97; 104])**.** *Если $Mult(Q)$ содержит подгруппу, изоморфную A_m, где $m \geqslant \max(\frac{k}{2} + 1, 5)$, A_m — знакопеременная группа степени m, то Q полиномиально полна.*

В частности, отсюда следует, что если $Mult(Q) = \mathcal{S}_Q$ и $|Q| \geqslant 5$, то Q является полиномиально полной.

Утверждение 22 ([97; 118])**.** *Если $G(Q)$ действует 2-транзитивно на Q, $|Q| \geqslant 3$, то Q полиномиально полна.*

Замечание 19 ([104])**.** Для квазигрупп, размер которых не представим в виде p^α, где p — простое число, полиномиальная полнота эквивалентна простоте квазигруппы.

В работе [119] приводится критерий полиномиальной полноты в терминах предполных классов функций k-значной логики. Указанный результат был расширен в работе [114] на случай d-квазигрупп.

Проверка полиномиальной полноты для квазигрупп малых порядков

В работах [63; 113] приведены критерии полиномиальной полноты и классификация квазигрупп порядка 4. В работе [120] было замечено, что классификация из [63] немного некорректна, и была предложена полная исправленная классификация квазигрупп порядка 4: всего имеется 384 полиномиально полных квазигрупп порядка 4, 104 простых и аффинных квазигрупп, 88 непростых и аффинных квазигрупп.

В работе [69] изучаются латинские квадраты размера 4×4, порожденные правильными семействами размера 2 на предмет полиномиальной полноты. В работе используется критерий, полученный в работе [113] для квазигрупп размера 4. Установлено, что квазигруппы, получаемые с помощью операции

$$(x, y) \to x \oplus y \oplus \mathcal{F}(\pi(x, y))$$

не являются полиномиально полными ни для какого правильного семейства $\mathcal{F}$ размера 2 и ни для каких наборов параметрических функций $\pi = (\pi_1, \pi_2)$. Класс порождаемых правильными семействами квазигрупп можно расширить за счет т.н. перестановочной конструкции, подробно рассматриваемой в [70]. Перестановочная конструкция является частным случаем изотопии латинского квадрата. При этом получаемые квазигруппы могут оказаться полиномиально полными.

Проверка полиномиальной полноты квазигруппы

Работа [121] посвящена изучению полиномиальной полноты для квазигрупп простого порядка $k = p$. Для таких квазигрупп достаточно проверить, что квазигрупповая операция не является линейной ни для какой биекции $Q \to \mathbb{Z}_p$, что может быть выполнено за время, полиномиальное от размера квазигруппы (а точнее, за $O(k^3)$ вычислений квазигрупповой операции). В работе [122] приведено обобщение алгоритма с квазигрупп простого порядка на d-квазигруппы (латинские гиперкубы) простого порядка со сложностью $O(k^{d+1})$. В работе [123] описан алгоритм проверки простоты квазигруппы, основанный на определении простоты. Для проверки простоты строятся все возможные транзитивные замыкания отношения эквивалентности $a_1 \sim a_i$ для $i = 2, \ldots, k$, где $|Q| = k$. Сложность алгоритма составляет $\mathcal{O}(k^4)$ квазигрупповых операций, то есть полиномиальна по размеру квазигруппы. В той же статье [123] описан алгоритм проверки аффинности со сложностью $\mathcal{O}(k^3)$.

В статье [124] рассматривается дальнейшая оптимизация алгоритма проверки с помощью параллельных вычислений и дополнительных оптимизаций исходного алгоритма, за счет чего удалось понизить сложность с $\mathcal{O}(k^4)$ до $\mathcal{O}(k^3)$ операций в квазигруппе. Статьи [125; 126] посвящены рассмотрению алгоритма проверки полиномиальной полноты для d-квазигрупп, являющегося прямым обобщением алгоритма, предложенного в [123].

Комбинируя все упомянутые выше результаты, можно получить следующий алгоритм проверки полиномиальной полноты квазигруппы.

1. Если порядок квазигруппы является простым числом, $k = p$, то необходимо проверить только неаффинность, что может быть выполнено за $\mathcal{O}(k^3)$ шагов.
2. Если порядок квазигруппы является степенью простого числа, $k = p^\alpha$, где $\alpha \geqslant 2$, то необходимо проверить и простоту, и неаффинность, что может быть сделано за $\mathcal{O}(k^3)$ шагов.
3. Во всех остальных случаях достаточно проверять только простоту, что может быть сделано за $\mathcal{O}(k^3)$ шагов.

Отметим также, что проверка неаффинности может быть ускорена за счет более быстрого алгоритма проверки неассоциативности (см. [109; 111]).

1.4.3 Наличие подквазигрупп

Третьим важным криптографическим свойством является отсутствие нетривиальных подквазигрупп в рассматриваемой квазигруппе. Здесь также может быть применен «наивный» алгоритм построения замыкания одноэлементного множества до подквазигруппы (см. [67; 127]). Предложенный алгоритм имеет временную сложность $\mathcal{O}(k^3)$ квазигрупповых операций. Также было показано [128], что алгоритм может быть расширен на случай задачи проверки существования подквазигруппы размера $\geqslant t$, при этом временная сложность алгоритма будет равна $\mathcal{O}(k^{2+t})$.

Дальнейшее улучшение было получено в [68]. Модифицированный алгоритм учитывает возможность того, что в квазигруппе каждый элемент может образовывать подквазигруппу (каждый элемент является идемпотентом $x \circ x = x$). В таком случае алгоритм из работ [67; 127] либо закончит работу, не перейдя к 2-элементным множествам, либо будет вынужден перебирать все возможные пары стартовых элементов, что даст временную сложность проверки порядка $\mathcal{O}(k^4)$. Алгоритмы, приводимые в [68] имеют следующую временную сложность:

- $\mathcal{O}(k^{7/3} \cdot (\log k)^{2/3})$ для алгоритма проверки существования любой собственной подквазигруппы;
- $\mathcal{O}(k^3 \log k)$ для алгоритма проверки существования собственной подквазигруппы размера не менее 2.

Улучшение достигается за счет использования свойства «монотонности» замыкания, что позволяет рассматривать лишь экстремальные случаи. Алгоритм напрямую обобщается на случай d-квазигрупп [129].

С помощью аппарата теории графов описанные выше алгоритмы были ещё несколько улучшены в работе [130]. Так, в частности, были получены следующие результаты:

- проверка наличия собственной подквазигруппы размера $\geqslant 1$ имеет временную сложность $\mathcal{O}(k^{7/3})$, пространственную сложность $\mathcal{O}(k^2)$;
- проверка наличия нетривиальной собственной подквазигруппы (т.е. размера $\geqslant 2$) имеет временную сложность $\mathcal{O}(k^3)$, пространственную сложность $\mathcal{O}(k^3)$;

– проверка наличия собственной d-подквазигруппы размера $\geqslant 1$ имеет временную сложность
$$\mathcal{O}\left(k^{\frac{d^2+d+1}{d+1}}\right)$$
и пространственную сложность $\mathcal{O}(k^d)$;
– проверка наличия нетривиальной собственной d-подквазигруппы (т.е. размера $\geqslant 2$) имеет временную сложность
$$\mathcal{O}\left(k^{\frac{d^2+2d+4}{d+2}}\right)$$
и пространственную сложность $\mathcal{O}\left(\max\left(k^d, k^{16/5}\right)\right)$.

1.4.4 Заключение

Квазигруппа, являющаяся полиномиально полной, имеющая малое число ассоциативных троек и не имеющая подквазигрупп, может рассматриваться в качестве базисной для построения криптографических примитивов. Все указанные свойства могут быть проверены за время, полиномиальное от размера исследуемой квазигруппы. Аналогичные результаты могут быть получены и для d-квазигрупп.

Выводы

В настоящей главе были введены основные понятия квазигруппы, правильных семейств функций, графа существенной зависимости семейства, рассмотрены преобразования, сохраняющие квазигрупповую структуру и свойство правильности. Выделены основные свойства квазигрупп, релевантные с точки зрения криптографических приложений: малое число ассоциативных троек, полиномиальная полнота, отсутствие подквазигрупп; рассмотрены алгоритмы проверки указанных свойств.

Отдельно рассмотрен один выделенный класс семейств, для семейств из этого класса доказана их правильность, а также доказана теорема о сильной квадратичности семейств. Введена конструкция, позволяющая строить квазигруппы

на основе пары правильных семейств, доказан ряд утверждений о количестве ассоциативных троек в квазигруппах, получаемых с помощью указанной конструкции.

Глава 2. Эквивалентные условия правильности семейств

> Математика — это искусство называть разные вещи одним и тем же именем.
>
> Жюль Анри Пуанкаре

В настоящей главе рассматриваются несколько альтернативных способов описания правильного семейства булевых функций:

– характеризация в терминах одностоковой ориентации: USO-ориентации булева куба (раздел 2.1);
– характеризация в терминах булевой сети с наследственно неподвижной точкой: HUFP-сети (раздел 2.2);
– характеризация в терминах булева отображения, каждая проекция которого не является самодвойственной (раздел 2.2.2).

Также рассматривается характеризация правильных семейств k-значной логики, где $k \geqslant 2$, в терминах клик обобщенных графов Келлера (раздел 2.3). Наконец, в разделе 2.4 приводится одно возможное обобщение свойства правильности, доказывается эквивалентность введенного определения и определения в терминах неортогональности аффинных пространств. Полученные альтернативные описания правильных семейств позволяют частично перенести (иногда с обобщением) результаты из одной области исследований в другие.

Результаты главы ранее были опубликованы в [73; 74; 79].

2.1 Одностоковые ориентации булевых кубов

В данном разделе мы приведем характеризацию правильных семейств булевых функций в геометрических терминах, а именно, в терминах ориентации, индуцируемой булевым правильным семейством на графе булева куба.

2.1.1 Определение одностоковых ориентаций

Для начала дадим необходимые предварительные определения.

Определение 42. Графом булева куба $G(\mathbb{E}_2^n)$ размерности n будем называть граф на 2^n вершинах с метками $(\alpha_1, \ldots, \alpha_n)$, $\alpha_i \in \{0, 1\}$, где ребра проведены между вершинами, расстояние Хэмминга (см. раздел 1.2.3) между которыми равно 1.

Определение 43. Подкубом булева куба размерности $(n - m)$ будем называть подграф графа $G(\mathbb{E}_2^n)$, порожденный вершинами с фиксированными значениями некоторых координат $i_1, \ldots, i_m \in \{1, \ldots, n\}$. В частности, подкубами размерности 1 являются ребра графа булева куба $G(\mathbb{E}_2^n)$, подкубами размерности 2 — всевозможные двумерные грани куба $G(\mathbb{E}_2^n)$ и так далее.

Определение 44. Стоком в ориентированном графе будем называть вершину, в которую входят ребра и из которой не исходят ребра.

Следующее определение было введено в работе [131] в контексте изучения задач оптимизации.

Определение 45. Реберной ориентацией с единственным стоком на графе булева куба $G(\mathbb{E}_2^n)$ называется ориентация всех ребер графа $G(\mathbb{E}_2^n)$ с таким свойством, что в каждом подкубе размерностей $m = 1, 2, \ldots, n$ существует ровно 1 сток.

Для краткости будем в дальнейшем называть такие ориентации одностоковыми (или USO-ориентациями, от англ. **U**nique **S**ink **O**rientation). Примеры одностоковых ориентаций кубов приведены на рисунках 2.1 и 2.2.

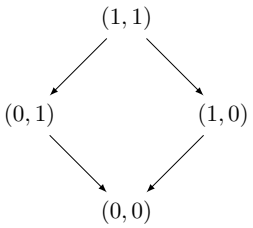

Рисунок 2.1 — Одностоковая ориентация двумерного куба $G(\mathbb{E}_2^2)$

Определение 46. Пусть задано семейство булевых функций $\mathcal{F}_n$ размера n, в котором функция f_i не зависит существенно от x_i, $1 \leqslant i \leqslant n$. Тогда семейство $\mathcal{F}_n$ индуцирует на $G(\mathbb{E}_2^n)$ ориентацию ребер следующим образом. Пусть $(\mathbf{u}, \mathbf{v})$ —

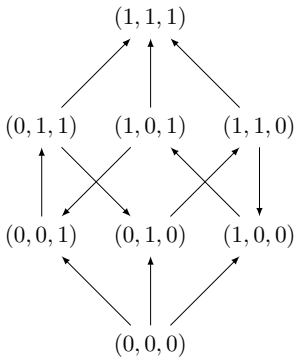

Рисунок 2.2 — Одностоковая ориентация трехмерного куба $G(\mathbb{E}_2^3)$

смежные вершины в $G(\mathbb{E}_2^n)$, различающиеся в i-м бите. Рассмотрим значение i-й функции семейства $\mathcal{F}_n$ на этих двух наборах. Поскольку f_i не зависит существенно от одноименной переменной x_i, то $f_i(\mathbf{u}) = f_i(\mathbf{v})$. Если $f_i(\mathbf{u}) = u_i$, то ребро ориентируется от $\mathbf{v}$ к $\mathbf{u}$, в противном случае ($f_i(\mathbf{u}) = v_i$) ребро ориентируется от $\mathbf{u}$ к $\mathbf{v}$.

Определение 47. Полученный выше ориентированный граф (граф $G(\mathbb{E}_2^n)$ с дополнительно индуцированной семейством $\mathcal{F}_n$ ориентацией ребер) называется асинхронным графом семейства (или асинхронной булевой сетью) $\mathcal{F}_n$ и обозначается $\Gamma_{\mathcal{F}_n}$.

Замечание 20. Нетрудно заметить, что вершина $\mathbf{y}$ является стоком в графе $\Gamma_{\mathcal{F}_n}$ тогда и только тогда, когда $\mathbf{y}$ — неподвижная точка отображения $\mathcal{F}_n\colon \mathbb{E}_2^n \to \mathbb{E}_2^n$. Действительно, $\mathcal{F}(\mathbf{y}) = \mathbf{y}$ тогда и только тогда, когда $f_i(\mathbf{y}) = y_i$ для каждого $i = 1, \ldots, n$, что, в свою очередь, равносильно тому, что $\mathbf{y}$ является стоком в описанном графе.

Замечание 21. Соответствие между семействами $\mathcal{F} = (f_1, \ldots, f_n)$ булевых функций (где f_i не зависит существенно от x_i) и асинхронными графами семейств $\Gamma_{\mathcal{F}}$ является взаимно-однозначным.

1. По семейству однозначно задается (указанным выше способом) ориентация на графе булева куба $G(\mathbb{E}_2^n)$.
2. По ориентированному графу булева куба $\Gamma_{\mathcal{F}}$ можно восстановить значение всех функций семейства на любом $\mathbf{x} \in \mathbb{E}_2^n$: рассмотрим вершину с меткой $\mathbf{x}$ и все смежные с ней ребра. Если i-е ребро (ребро, ведущее из вершины $\mathbf{x}$ в вершину, отличную от $\mathbf{x}$ в i-й координате) выходит из

x, то $f_i(\mathrm{x}) = \overline{x_i}$, иначе $f_i(\mathrm{x}) = x_i$. В полученном семействе f_i не зависит существенно от x_i, поскольку ни одно ребро не ориентировано в две стороны.

2.1.2 Неподвижные точки правильных семейств

Лемма 1. *У правильного семейства булевых функций всегда существует единственная неподвижная точка.*

Доказательство. Будем вести доказательство индукцией по размеру правильного семейства. Булевы семейства размера $n = 1$ — это константы $a \in \mathbb{E}_2^n$, для них утверждение тривиально выполнено.

Рассмотрим семейство $\mathcal{F}_n$ размера $n \geqslant 2$. Рассмотрим его проекции $\Pi_n^0(\mathcal{F}_n)$ и $\Pi_n^1(\mathcal{F}_n)$, которые также являются правильными семействами (утверждение 11). По предположению индукции для указанных проекций в каждом подкубе существует единственная неподвижная точка:

$$\alpha = (\alpha_1, \ldots \alpha_{n-1}),\ \beta = (\beta_1, \ldots \beta_{n-1}),$$

причем точка α соответствует точке $(\alpha, 0)$, лежащей в подкубе с последней координатой $x_n = 0$, а точка β — точке $(\beta, 1)$, лежащей в подкубе с последней координатой $x_n = 1$. По определению неподвижных точек выполнены равенства:

$$f_1(\alpha, 0) = \alpha_1, \ldots, f_{n-1}(\alpha, 0) = \alpha_{n-1},$$
$$f_1(\beta, 1) = \beta_1, \ldots, f_{n-1}(\beta, 1) = \beta_{n-1}.$$

Рассмотрим значения $f_n(\alpha, 0)$ и $f_n(\beta, 1)$. Так как семейство $\mathcal{F}_n = (f_1, \ldots, f_n)$ — правильное, то найдется либо индекс $j \in \{1, \ldots n-1\}$, такой что $\alpha_j \neq \beta_j$, $f_j(\alpha) = f_j(\beta)$, либо $j = n$, и $f_n(\alpha, 0) = f_n(\beta, 1)$. Из приведенных выше рассуждений видно, что случай $j < n$ не может выполняться. Следовательно, если $f_j(\alpha) = 0$, то единственной неподвижной точкой всего семейства является $(\alpha, 0)$, иначе такой точкой является точка $(\beta, 1)$. □

Следующая теорема устанавливает взаимно-однозначное соответствие между правильными семействами булевых функций размера n и USO-ориентациями булевых кубов размерности n.

Теорема 9. *Граф семейства $\Gamma_{\mathcal{F}}$ является одностоковой ориентацией булева куба $\mathbb{E}_n$ тогда и только тогда, когда $\mathcal{F}$ — правильное семейство.*

Доказательство. Как было отмечено выше, стоки в графе $\Gamma_{\mathcal{F}}$ соответствуют неподвижным точкам ограничения отображения $\mathcal{F}$ на соответствующий подкуб куба $\mathbb{E}_n$.

Пусть $\mathcal{F}_n$ — правильное булево семейство. Тогда по утверждению 11 любая проекция семейства $\mathcal{F}$ на любой подкуб $\mathbb{E}_n$ также является правильным семейством. По лемме 1 такое ограничение имеет единственную неподвижную точку в данном подкубе, т.е. данный подкуб имеет единственный сток. Следовательно, граф $\Gamma_{\mathcal{F}}$ для правильного семейства $\mathcal{F}$ является одностоковой ориентацией.

Докажем утверждение в обратную сторону. Пусть $\Gamma_{\mathcal{F}}$ — одностоковая ориентация. Покажем по индукции, что в этом случае F является правильным семейством.

База индукции: при $n = 1$ нетрудно убедиться, что существует ровно две одностоковые ориентации на двух вершинах, соответствующие константным (а значит, правильным) семействам размера 1:

$$\mathcal{F}^0 = \left[0\right], \quad \mathcal{F}^1 = \left[1\right].$$

Индуктивный переход: пусть $\alpha \neq \beta$, где $\alpha, \beta \in \mathbb{E}_2^n$. По определению правильного семейства мы должны показать, что тогда существует индекс i, такой что $\alpha_i \neq \beta_i$, но $f_i(\alpha) = f_i(\beta)$. Если найдется индекс k, такой что $\alpha_k = \beta_k$, то задача может быть сведена к задаче меньшей размерности: рассмотрим проекцию на подкуб $x_k = \alpha_k$ и используем индуктивное предположение.

Следовательно, можем считать, что $\alpha_k \neq \beta_k$, $1 \leqslant k \leqslant n$. Дополнительно мы можем считать, что α — сток, то есть $f_k(\alpha) = \alpha_k$, $1 \leqslant k \leqslant n$. Если это не так, то мы можем перейти к новому семейству $g_k(\mathbf{x}) = f_k(\mathbf{x}) \oplus 1$, таким образом изменив направление всех ребер между подкубами $x_k = 0$ и $x_k = 1$. Данная смена направлений ребер не разрушает свойство ориентации быть одностоковой. В силу теоремы 9 указанное преобразование не нарушает правильность семейства. Таким образом, можно без ограничения общности считать, что вершина α является стоком.

Но в таком случае если $f_k(\alpha) \neq f_k(\beta)$, $1 \leqslant k \leqslant n$, то мы имеем $f_k(\beta) = \beta_k$, $1 \leqslant k \leqslant n$, то есть вершина β также является стоком, что противоречит одностоковости. Следовательно, должен найтись какой-либо индекс k, для которого $f_k(\alpha) = f_k(\beta)$, что и требовалось доказать. □

Таким образом, учитывая то, что стокам в USO-ориентациях соответствуют неподвижные точки семейства (см. замечание 20), был получен следующий критерий правильности семейства (см. также раздел 2.2).

Следствие 1. *Семейство булевых функций $\mathcal{F}_n$ правильно тогда и только тогда, когда каждое подсемейство семейства $\mathcal{F}_n$ (в том числе и само исходное семейство) имеет единственную неподвижную точку.*

В работе [78] (см. теорему 2) было показано, что данный критерий нельзя напрямую распространить с булева случая на случай k-значной логики, где $k \geqslant 3$. Более точно, было показано, что если семейство $\mathcal{F}_n$ в k-значной логике является правильным, то у него и всех его проекций существует единственная неподвижная точка, однако обратное утверждение неверно: так, например, для семейства

$$\begin{bmatrix} f_1(x_1, x_2) \\ f_2(x_1, x_2) \end{bmatrix} = \begin{bmatrix} 2x_2 \\ x_1 \end{bmatrix}$$

выполняется свойство единственности неподвижной точки для всех возможных подсемейств, однако семейство не является правильным (см. [132]). Обобщение критерия может быть сформулировано в терминах перекодировок исходного семейства (см. раздел 3.1.1 и утверждение 25).

2.1.3 Оценки на число правильных булевых семейств

Полученное выше соответствие между USO-ориентациями и правильными семействами булевых функций позволяет получить оценку на число правильных семейств булевых функций размера n. Обозначим через $T_k(n)$ количество правильных семейств в k-значной логике размера n (если $k = 2$, то индекс k будем опускать).

Следствие 2 ([133, лемма 6.10])**.** *Выполнение следующее неравенство*

$$T(n) \geqslant 4\left(T(n-1)\right)^2.$$

Отметим, что более слабая оценка вида $T(n) \geqslant 2\left(T(n-1)\right)^2$, или, более общо,

$$T_k(n) \geqslant k \cdot \left(T_k(n-1)\right)^k$$

для случая k-значной логики может быть получена за счет явных конструкций построения новых правильных семейств из старых (см., например, [134, теорема 2]).

Утверждение 23 ([135, теорема 1])**.** *Существуют константы $B \geqslant A > 0$, такие что для $n \geqslant 2$ выполняются неравенства:*

$$n^{A \cdot 2^n} \leqslant T(n) \leqslant n^{B \cdot 2^n}.$$

В частности, из этого результата следует, что доля булевых правильных семейств даже среди булевых семейств, для которых f_i не зависит существенно от x_i (необходимое условие правильности, см. замечание 13), является экспоненциально малой.

Также, используя полученную выше оценку, можно показать, что число треугольных семейств среди правильных есть $o(1)$ при стремлении размера семейства $n \to \infty$, а именно, что доля треугольных семейств среди правильных убывает со скоростью $n^{-D \cdot 2^n}$, где $D > 0$ (т.е. экспоненциально мала).

Теорема 10. *Обозначим через $\Delta(n)$ количество булевых треугольных семейств размера n. Тогда:*

$$\frac{\Delta(n)}{T(n)} = o\left(\frac{1}{n^{D \cdot 2^n}}\right) \text{ при } n \to \infty$$

для некоторого $D > 0$.

Докажем несколько вспомогательных утверждения (верхнюю и нижнюю оценки на число $\Delta(n)$, а также техническую лемму, необходимую для оценки).

Лемма 2. *Выполнено неравенство:*

$$\sum_{k=2}^{\infty} \frac{k}{2^{2^{k-1}}} < 0.705.$$

Доказательство. С помощью компьютерных вычислений можно убедиться, что:

$$\sum_{k=2}^{10} \frac{k}{2^{2^{k-1}}} < 0.704.$$

Остаток ряда можно оценить следующим образом:

$$\sum_{k=11}^{\infty} \frac{k}{2^{2^{k-1}}} < \sum_{k=11}^{\infty} \frac{1}{2^k} < 0.001,$$

поскольку для каждого члена ряда выполнено неравенство (при $k > 4$):

$$\frac{k}{2^{2^{k-1}}} < \frac{1}{2^k} \Leftrightarrow k \cdot 2^k < 2^{2^{k-1}}.$$

□

Лемма 3. *Выполнено следующее неравенство:*

$$\Delta(n) \leqslant n! \cdot 2^{2^n-1}.$$

Доказательство. Зафиксируем подстановку $\sigma \in \mathcal{S}_n$ и оценим сверху число булевых функций, которые могут стоять на позиции $\sigma(m)$ значением $2^{2^{m-1}}$, поскольку функция с номером $\sigma(m)$ зависит существенно не более чем от $m-1$ переменной. В таком случае общее число треугольных семейств не превышает:

$$\Delta(n) \leqslant n! \cdot 2^{2^0} \cdot 2^{2^1} \cdot \ldots \cdot 2^{2^{n-1}} = n! \cdot 2^{2^n-1}.$$

□

Заметим, что некоторые семейства при такой оценке могли быть подсчитаны более одного раза. Тем не менее, оценка является достаточно точной, а именно, выполняется следующее утверждение.

Лемма 4. *Выполнено следующее неравенство:*

$$\Delta(n) \geqslant 0.145 \cdot n! \cdot 2^{2^n-1}.$$

Доказательство. Через $e(n)$ обозначим число n-местных булевых функций, существенно зависящих от всех n переменных. Тогда количество треугольных семейств может быть оценено снизу значением

$$\Delta(n) \geqslant n! \cdot e(0) \cdot e(1) \cdot \ldots \cdot e(n-1),$$

поскольку в данном случае мы подсчитываем число треугольных семейств, в которых после упорядочивания первая функция существенно зависит ровно от 0 переменных, вторая функция зависит существенно ровно от одной переменной $x_{\sigma(1)}$, и так далее. При этом при различных σ мы получаем заведомо различные семейства. Необходимо оценить снизу полученное произведение.

Можно оценить число $e(n)$ снизу согласно неравенству Бонферрони (см. [136, раздел 1.3]):

$$e(n) \geqslant 2^{2^n} - n \cdot 2^{2^{n-1}}.$$

Данная оценка получается из следующих соображений: из множества всех булевых функций от n переменных $x_1, \ldots, x_n$ вычтем все функции, которые зависят только от $n-1$ выбранной переменной (имеется n способов зафиксировать одну переменную, от которой не будет зависеть функция).

При этом данная оценка является оценкой снизу, поскольку некоторые функции учитываются более одного раза в вычитаемом (например, функции, не зависящие одновременно от двух переменных).

Таким образом,

$$\begin{aligned}\frac{\Delta(n)}{n! \cdot 2^{2^0} \cdot 2^{2^1} \cdot \ldots \cdot 2^{2^{n-1}}} &\geqslant \frac{e(0)}{2^{2^0}} \times \ldots \times \frac{e(n-1)}{2^{2^{n-1}}} \geqslant \\ &\geqslant 1 \cdot \left(1 - \frac{1}{2^{2^0}}\right) \cdot \left(1 - \frac{2}{2^{2^1}}\right) \times \ldots \times \left(1 - \frac{n-1}{2^{2^{n-2}}}\right) \geqslant \\ &\geqslant \frac{1}{2} \cdot \left(1 - \left(\frac{2}{2^{2^1}} + \ldots + \frac{n-1}{2^{2^{n-2}}}\right)\right) \geqslant \\ &\geqslant \frac{1}{2}\left(1 - \sum_{k=2}^{\infty} \frac{k}{2^{2^{k-1}}}\right).\end{aligned}$$

Для завершения доказательства леммы 4 остается воспользоваться оценкой сверху для ряда $\sum_{k=2}^{\infty} \frac{k}{2^{2^{k-1}}}$. Используя лемму 2, получим:

$$\frac{1}{2}\left(1 - \sum_{k=2}^{\infty} \frac{k}{2^{2^{k-1}}}\right) \geqslant \frac{1}{2}(1 - 0.705) = 0.1475,$$

откуда следует утверждение леммы 4. □

Таким образом, можно утверждать, что при $n \to \infty$ имеется оценка:

$$\Delta(n) = \Theta\left(n! \cdot 2^{2^n - 1}\right).$$

Перейдем к доказательству теоремы 10.

Доказательство. Используя нижнюю оценку из утверждения 23 и формулу Стирлинга (см., например, [84, часть II, параграф 4]), можно оценить долю треугольных семейств среди правильных:

$$\frac{\Delta(n)}{T(n)} \leqslant \frac{n! \cdot 2^{2^n-1}}{n^{A\cdot 2^n}} \sim \frac{n^n \cdot 2^{2^n-1} \cdot \sqrt{2\pi n}}{e^n \cdot n^{A\cdot 2^n}} =$$

$$= \Theta\left(\frac{2^{(n+\frac{1}{2})\log n} \cdot 2^{2^n}}{2^{n\log e} \cdot 2^{A\cdot 2^n \log n}}\right) =$$

$$= \Theta\left(2^{2^n(1-A\log n)} \cdot 2^{n\cdot(\log n - \log e + \frac{\log n}{2n})}\right) =$$

$$= o\left(2^{-(A-\varepsilon)\cdot 2^n \log n}\right) \text{ при } n \to \infty$$

для любого $\varepsilon > 0$. Для того, чтобы удостовериться в этом, заметим, что

$$\frac{2^{2^n(1-A\log n)} \cdot 2^{n\cdot(\log n - \log e + \frac{\log n}{2n})}}{2^{-(A-\varepsilon)\cdot 2^n \log n}} = 2^{-\varepsilon\cdot 2^n \log n\cdot(1+o(1))},$$

и при $n \to \infty$ показатель стремится к $-\infty$.

Отсюда следует утверждение теоремы 10 для $D = A - \varepsilon$ для любого фиксированного $0 < \varepsilon < A$. □

Из доказанной теоремы следует, что булевы треугольные семейства размера n образуют лишь экспоненциально малую часть от всех правильных семейств булевых функций размера n.

2.1.4 Рекурсивно треугольные семейства

Еще одним примером «переноса» результатов с геометрического языка USO-ориентаций на алгебраический язык правильных семейств является понятие рекурсивно треугольного семейства. В работе [137] вводится понятие рекурсивной ориентации булева куба. Рекурсивная ориентация булева n-мерного куба $G(\mathbb{E}_2^n)$ задается следующим характеристическим свойством: найдется такая координата x_i, вдоль которой все ребра ориентированы в одном направлении, и ориентация на каждом из подкубов $x_i = 0$ и $x_i = 1$ размерности $(n-1)$ также является рекурсивной. Мы можем обобщить указанную конструкцию, перенеся ее на алгебраический язык правильных семейств следующим образом.

Определение 48. Назовем семейство $\mathcal{F}_n$, заданное на Q^n, рекурсивно треугольным, если существует координата i, такая что $f_i = q \in Q$ (константа), и каждое из

семейств вида $\Pi_i^a(\mathcal{F}_n)$, где a пробегают все множество Q, также является рекурсивно треугольным.

Замечание 22. Треугольные семейства являются частным случаем рекурсивно треугольных: треугольные семейства являются такими рекурсивно треугольными, что каждая из проекций $\Pi_i^a(f_n)$ постоянна вдоль одного и того же направления j.

Класс рекурсивно треугольных семейств вкладывается в класс локально треугольных семейств (см. определение 51). Как будет показано далее, локально треугольные семейства являются правильными, а следовательно, и рекурсивно треугольные семейства также являются правильными.

Введем обозначение $\Delta_k^{\mathsf{rec}}(n)$ для числа рекурсивно треугольных семейств k-значной логики размера n.

Лемма 5. *Для числа рекурсивно треугольных семейств справедлива формула:*

$$\Delta_k^{\mathsf{rec}}(n) = \sum_{j=1}^{n} (-1)^{j+1} \cdot k^j \cdot \binom{n}{j} \left(\Delta_k^{\mathsf{rec}}(n-j)\right)^{k^j},$$

где $\Delta_k^{\mathsf{rec}}(0) = 1$, $k = |Q|$.

Доказательство. Утверждение следует напрямую из формулы включений-исключений (см., например, [84, часть II, параграф 3]). Существует $\binom{n}{j}$ способов выбрать j «фиктивных направлений», для которых $f_\ell = const$, и k^j способов зафиксировать значения j фиктивных функций. Каждая из проекций должна образовывать рекурсивно треугольное семейство размера $n - j$, и различные рекурсивно треугольные семейства в проекциях могут выбираться независимо друг от друга, что дает итоговый вклад $\left(\Delta_k^{\mathsf{rec}}(n-j)\right)^{k^j}$. □

Замечание 23. Для $k = 2$ число рекурсивно треугольных семейств размера n совпадает с числом рекурсивных ориентаций куба $G(\mathbb{E}_2^n)$ [138, A141770].

Теорема 11. *Доля булевых рекурсивно треугольных семейств размера n в классе всех булевых правильных семейств размера n стремится к 0 при $n \to \infty$.*

Доказательство. Для числа рекурсивно треугольных семейств справедливо неравенство:

$$\Delta_k^{\mathsf{rec}}(n) \leqslant n \cdot k \cdot \left(\Delta^{\mathsf{rec}}(n-1)\right)^k.$$

Применяя неравенство рекурсивно и используя равенство $\Delta_k^{\mathsf{rec}}(0) = 1$, можно получить оценку:

$$\Delta_k^{\mathsf{rec}}(n) \leqslant \left(n^{k^0} \cdot (n-1)^{k^1} \cdot (n-2)^{k^2} \times \ldots \times (n-(n-1))^{k^{n-1}}\right) \cdot k^{\frac{k^n-1}{k-1}}.$$

Обозначим через $S(n,k)$ число вида:

$$S(n,k) = \prod_{i=0}^{n-1} (n-i)^{k^i},$$

тогда согласно полученному неравенству имеем

$$\Delta_k^{\mathsf{rec}}(n) \leqslant S(n,k) \cdot k^{\frac{k^n-1}{k-1}}.$$

Для $S(n,2)$ верна следующая асимптотика при $n \to \infty$ [139, раздел 6.10]:

$$S(n,2) \sim \frac{s^{2^n}}{n},$$
$$s = \sqrt{1 \cdot \sqrt{2 \cdot \sqrt{3 \cdot \ldots}}} \approx 1.661688.$$

Таким образом, для величины $\Delta_2^{\mathsf{rec}}(n)$ справедливо асимптотическое неравенство:

$$\Delta_2^{\mathsf{rec}}(n) \lesssim \frac{(2s)^{2^n}}{2n},$$

а для доли рекурсивно треугольных с учетом неравенства на число правильных булевых семейств размера n (см. утверждение 23) выполняется

$$\frac{\Delta_2^{\mathsf{rec}}(n)}{T(n)} \lesssim \frac{1}{2n} \cdot \left(\frac{2s}{n}\right)^{2^n}.$$

Полученная величина стремится к 0 при $n \to \infty$. □

Замечание 24. В общем случае для чисел $S(n,k)$ верна асимптотика [140]:

$$S(n,k) \sim \frac{(A_k)^{k^n}}{n^{\frac{1}{1-k}}},$$

где A_k — некоторая константа, зависящая только от k.

2.2 Булевы сети с наследственно единственной неподвижной точкой

Введенное ранее понятие асинхронного графа семейства $\Gamma_{\mathcal{F}}$ (асинхронной булевой сети) имеет и другую сферу приложения. А именно, подобные сети рассматриваются в контексте математической биологии [141—143] как аппарат для изучения экспрессии генов [144]. В указанном контексте особо интересны неподвижные точки асинхронной булевой сети [145—147], которые соответствуют устойчивым паттернам экспрессии генов [145].

Оказывается, что правильные семейства булевых функций задают такие асинхронные булевы сети, что в каждой порожденной подсети (которые соответствуют рассмотрению проекции подсемейства) существует единственная неподвижная точка (такой объект обычно называется «асинхронной булевой сетью с наследственно единственной неподвижной точкой», или сокращенно HUFP-сетью, от англ. hereditarily unique fixed point network). Несложно видеть, что в HUFP-семействе каждая функция f_i не может зависеть существенно от одноименной переменной x_i (в противном случае соотвествующая проекция имела бы 0 или 2 неподвижные точки).

Для исходного правильного семейства неподвижная точка существует и единственна по лемме 1, и при этом каждая проекция правильного семейства также является правильным семейством (см. утверждение 11), и, в свою очередь, также имеет единственную неподвижную точку. Таким образом, верна следующая теорема.

Теорема 12. *Булевы правильные семейства находятся во взаимно-однозначном соответствии с* HUFP-*сетями.*

С помощью полученного естественного соответствия мы можем переносить результаты из области HUFP-сетей на «язык» правильных семейств (и наоборот). В этом разделе мы рассмотрим некоторые из подобных результатов.

2.2.1 Локальные графы взаимодействий и локально треугольные семейства

Пусть $f\colon Q^n \to Q$ — функция на Q^n.

Определение 49. Введем частную производную $\partial_i f(\mathbf{x}) \in \{0, 1\}$ в точке $\mathbf{x}$:

$$\partial_i \mathcal{F}(\mathbf{x}) = \begin{cases} 1, & \text{если существует } q\text{, т.ч.} \\ & \mathcal{F}_n(x_1, \ldots, x_{i-1}, q, x_{i+1}, \ldots, x_n) \neq \mathcal{F}(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n), \\ 0, & \text{в противном случае.} \end{cases}$$

В работе [148] было введено понятие локального графа взаимодействия для семейства $\mathcal{F}$ в точке $\mathbf{x}$. По сути, это понятие определяет «локализованный» в точке $\mathbf{x}$ граф существенной зависимости семейства $\mathcal{F}$, а именно, он показывает, как локальные изменения аргумента в точке $\mathbf{x}$ влияют на поведение семейства.

Определение 50. Определим локальный граф взаимодействий $G_{\mathcal{F}}(\mathbf{x})$ семейства $\mathcal{F}$ в точке $\mathbf{x}$ как ориентированный граф на множестве вершин $V = 1, 2, \ldots, n$, вершины с номерами j и i соединяются ориентированным ребром $j \to i$ тогда и только тогда, когда $\partial_i f_j(x) \neq 0$.

Замечание 25. Можно также определить глобальный граф взаимодействий $G_{\mathcal{F}}$ семейства $\mathcal{F}$ как ориентированный граф на множестве вершин $V = 1, 2, \ldots, n$, вершины с номерами j и i соединяются ориентированным ребром $j \to i$ тогда и только тогда, когда существует точка $\mathbf{x}$, для которой $\partial_i f_j(\mathbf{x}) \neq 0$.

Иными словами, в глобальном графе взаимодействий присутствует ребро $j \to i$ тогда и только тогда, когда f_j существенно зависит от x_i. Следовательно, глобальный граф взаимодействий совпадает с (уже введенным) графом существенной зависимости семейства $G_{\mathcal{F}}$ (см. определение 20). Заметим также, что глобальный граф взаимодействий $G_{\mathcal{F}}$ представляет собой объединение локальных графов взаимодействий $G_{\mathcal{F}}(\mathbf{x})$ по всем точкам $\mathbf{x}$.

В работе [149] было показано, что если глобальный граф взаимодействия $G_{\mathcal{F}}$ булева семейства $\mathcal{F}$ является ациклическим, то семейство $\mathcal{F}$ задает HUFP-сеть. По сути, было показано, что треугольные семейства являются правильными. Обобщение указанного результата приведено в работе [148], где было показано, что если локальный граф взаимодействия булева семейства $\mathcal{F}$ для каждой точки $\mathbf{x}$ является ациклическим, то семейство задает HUFP-сеть. Мы можем обобщить указанное наблюдение на любые (не только булевы) семейства $\mathcal{F}$ (см. теорему 13). Дадим предварительные определения.

Определение 51. Назовем семейство $\mathcal{F}$, заданное на Q^n, локально треугольным в точке $\mathbf{x}$, если существует такая согласованная перестановка семейства σ, что после ее применения мы получим семейство $\mathcal{G}$ со свойством

$$\partial_i g_j(\mathbf{x}) = 0, \quad 1 \leqslant j \leqslant i \leqslant n.$$

Назовем семейство $\mathcal{F}$ локально треугольным, если оно является локально треугольным в каждой точке $\mathbf{x} \in Q^n$.

Лемма 6. *Семейство $\mathcal{F}$ локально треугольно в точке $\mathbf{x}$ тогда и только тогда, когда $G_{\mathcal{F}}(\mathbf{x})$ задает направленный ациклический граф.*

Доказательство. Перейдем к согласованной перестановке семейства $\mathcal{F}$ — семейству $\mathcal{G}$. Для переставленного семейства $\mathcal{G}$ первая функция g_1 локально постоянна по любому из направлений, функция g_2 локально постоянна по направлениям $x_2, \ldots, x_n$, и так далее. Это значит, что из вершины с номером i в графе $G_{\mathcal{G}}(\mathbf{x})$ могут выходить ребра только к вершинам с номерами $j < i$. Если в графе $G_{\mathcal{G}}(\mathbf{x})$ существует цикл $i_1 \to i_2 \to i_k \to i_1$, то указанное свойство нарушается: достаточно рассмотреть вершину с наибольшим номером в цикле. По указанному выше свойству ребра к этой вершине могут идти только от вершин с большими номерами, но все оставшиеся номера в цикле меньше, чем у рассматриваемой вершины. Мы пришли к противоречию, которое доказывает, что в графе $G_{\mathcal{G}}(\mathbf{x})$ не может быть направленных циклов. Поскольку согласованная перестановка семейства только меняет метки у вершин графа $G_{\mathcal{F}}(\mathbf{x})$, то и в исходном графе не может быть циклов.

Докажем в обратную сторону: пусть в $G_{\mathcal{F}}(\mathbf{x})$ нет циклов. Тогда существует топологическая сортировка графа $G_{\mathcal{F}}(\mathbf{x})$ (см., например, [112, раздел 22.4]), т.е. такая перенумерация вершин σ, что после нее в графе остаются только такие ребра $(i, j) \in E$, для которых $i > j$. Если применить σ к семейству $\mathcal{F}$ как согласованную перенумерацию, то функция f_1 не будет зависеть существенно в точке $\mathbf{x}$ ни от какой из переменных, функция f_2 может зависеть только от x_1 и так далее. Поскольку это верно для каждой точки $\mathbf{x}$, то по определению $\mathcal{F}$ является локально треугольным семейством. □

Лемма 7. *Пусть $\mathcal{F}$ — локально треугольное семейство, $\mathcal{G}$ — некоторая его проекция. Тогда $\mathcal{G}$ также является локально треугольным семейством.*

Доказательство. Без ограничения общности рассмотрим однократную проекцию вида $\mathcal{G} = \Pi_i^a(\mathcal{F})$. Тогда граф $G_{\mathcal{G}}(\mathbf{x})$ для точки $\mathbf{x} = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \in Q^{n-1}$ совпадает с графом $G_{\mathcal{F}}((x_1, \ldots, x_{i-1}, a, x_{i+1}, \ldots, x_n))$ с удаленной i-й вершиной (и всеми инцидентными ей ребрами). При удалении вершины новых циклов появиться не может, а значит, графы $G_{\mathcal{G}}(\mathbf{x})$ остаются ациклическими для каждой точки $\mathbf{x}$. Следовательно, $\mathcal{G}$ локально треугольно. □

Лемма 8. *Пусть $v_1 \neq y_1, \ldots, v_n \neq y_n$, $\mathcal{F}_n$ локально треугольное. Тогда найдется такой индекс i, что $f_i(\mathbf{v}) = f_i(\mathbf{y})$.*

Доказательство. Проведем доказательство индукцией по размеру семейства n. **База индукции:** при $n = 1$ локально треугольными семействами размера 1 будут только константы $\mathcal{F} = \left[a\right]$, $a \in \mathbb{E}_k$.

Индуктивный переход: рассмотрим $n \geqslant 2$. Так как $\mathcal{F}_n$ локально треугольно в точке $\mathbf{v}$, то найдется такая координата (без ограничения общности можем предполагать, что x_n), что при ее варьировании при остальных фиксированных координатах никакая из функций не поменяется.

Рассмотрим проекцию вида $\mathcal{G} = \Pi_n^{y_n}(\mathcal{F}_n)$. В таком случае мы переходим к локально треугольному (см. лемму 7) семейству $\mathcal{G}$ размера $n-1$, по предположению индукции найдется индекс $j < n$, такой что

$$f_j(v_1, \ldots, v_{n-1}, y_n) = g_j(v_1, \ldots, v_{n-1}) = g_j(y_1, \ldots, y_{n-1}) = f_j(y_1, \ldots, y_{n-1}, y_n).$$

Но поскольку исходное семейство $\mathcal{F}_n$ локально постоянно вдоль направления x_n в точке $\mathbf{v}$, то

$$f_j(v_1, \ldots, v_{n-1}, v_n) = f_j(v_1, \ldots, v_{n-1}, y_n) = f_j(y_1, \ldots, y_{n-1}, y_n),$$

что и требовалось доказать. □

Теорема 13. *Пусть $\mathcal{F}$ — заданное на Q^n локально треугольное семейство. Тогда $\mathcal{F}$ является правильным.*

Доказательство. Для любых двух неравных наборов $\mathbf{x} \neq \mathbf{y}$, $\mathbf{x}, \mathbf{y} \in Q^n$ рассмотрим проекцию $\mathcal{G}$ исходного семейства $\mathcal{F}$ на общие координаты. Проекция $\mathcal{G}$ будет локально треугольным семейством по лемме 7. К семейству $\mathcal{G}$ можно применить лемму 8 и получить индекс i, для которого значения функций g_i в рассматриваемой точке совпадут, а значит, для исходного семейства $\mathcal{F}$ выполняется характеристическое свойство правильности. □

Замечание 26. Множество булевых локально треугольных семейств шире множества треугольных семейств (см. раздел 1.3.3). Так, например, булевы семейства

$$\begin{bmatrix} 0 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_1x_2 \end{bmatrix}, \begin{bmatrix} x_2x_3x_4 \\ x_1 \oplus x_1x_3 \\ x_2 \oplus x_1x_2 \oplus x_2x_4 \oplus x_1x_2x_4 \\ x_1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_2x_3 \end{bmatrix} \tag{2.1}$$

являются локально треугольными, но не треугольными.

Покажем, что рекурсивно треугольные семейства (см. определение 48) являются локально треугольными (а следовательно, правильными).

Лемма 9. *Пусть $\mathcal{F}_n$ — рекурсивно треугольное семейство на Q^n. Тогда $\mathcal{F}_n$ является локально треугольным семейством.*

Доказательство. Покажем, что для каждой точки $\mathbf{v}$ граф $G_{\mathcal{F}}(\mathbf{v})$ является ациклическим. Для рекурсивно треугольных семейств размера $n = 1$ и $n = 2$ утверждение проверяется напрямую.

Пусть $\mathcal{F}_n$ — рекурсивно треугольное семейство размера n. По свойству рекурсивной треугольности найдется такой индекс i, что $f_i \equiv const$, а следовательно, вершина с номером i в графе $G_{\mathcal{F}}(\mathbf{v})$ является истоком (в нее не входит ребер), т.к. f_i не зависит ни от одного x_j существенным образом. Следовательно, вершина i не может входить ни в какой из циклов.

Рассмотрим какую-либо проекцию $\mathcal{G} = \Pi_i^a(\mathcal{F})$ и ее локальный граф взаимодействий в точке $\widetilde{\mathbf{v}} = (v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$. Граф $G_{\mathcal{G}}(\widetilde{\mathbf{v}})$ является подграфом графа $G_{\mathcal{F}}(\mathbf{v})$. При этом если в графе $G_{\mathcal{F}}(\mathbf{v})$ был цикл, то он останется хотя бы в одном из $G_{\mathcal{G}}(\widetilde{\mathbf{v}})$. Но каждое из семейств $\mathcal{G}$ также является рекурсивно треугольным (меньшего размера), а значит, по предположению индукции, в графах $G_{\mathcal{G}}(\widetilde{\mathbf{v}})$ нет циклов.

Таким образом, исходный граф $G_{\mathcal{F}}(\mathbf{v})$ является ациклическим для любой точки $\mathbf{v}$. □

Замечание 27. Свойство рекурсивной треугольности, вообще говоря, слабее свойства локальной треугольности (см., например, семейство размера 4 из замечания 26: в нём нет константы).

Фактически, из рекурсивной треугольности следует, что *для всех* графов $G_{\mathcal{F}}(\mathbf{v})$ найдется одна и та же вершина i, являющаяся истоком. Для $n = 1, 2, 3$

множества локально треугольных и рекурсивно треугольных семейств совпадают. Для $n = 4$ количество локально треугольных семейств $\Delta^{\mathsf{loc}}(4) = 3349488$ превышает число рекурсивно треугольных семейств $\Delta^{\mathsf{rec}}(4) = 3209712$ (см. таблицу 4).

Таким образом, множество локально треугольных семейств шире, чем множество рекурсивно треугольных семейств (и включает его в себя целиком), множество рекурсивно треугольных семейств шире, чем множество треугольных семейств (и включает его в себя целиком).

2.2.2 Несамодвойственные проекции

В настоящем разделе мы сформулируем еще один критерий правильности семейства функций, сформулированного в работе [145, раздел 4] для HUFP-сетей. Для начала дадим предварительные определения.

Пусть $\mathcal{F}_n$ — семейство булевых функций.

Определение 52. Будем называть отображение $\mathcal{F}\colon \mathbb{E}_2^n \to \mathbb{E}_2^k$ самодвойственным, если для любого набора $\mathbf{x} \in \mathbb{E}_2^n$ выполняется свойство $\mathcal{F}(\overline{\mathbf{x}}) = \overline{\mathcal{F}(\mathbf{x})}$.

Замечание 28. Для $k = 1$ введенное выше определение совпадает со стандартным определением самодвойственной функции (см., например, [84, Часть I, глава 1]).

Замечание 29. Свойство самодвойственности сохраняется при всевозможных сдвигах семейства (как внутренних, так и внешних) и при согласованных перестановках.

Теорема 14. *Семейство $\mathcal{F}_n$ булевых функций правильно тогда и только тогда, когда каждая из его проекций $\Pi_{i_1,\ldots,i_k}^{a_1,\ldots,a_k}(\mathcal{F})$ не является самодвойственной булевой функцией.*

Утверждение следует из следствия 2 работы [145].

2.3 Кликовое представление правильных семейств

В работах [150; 151] изучались «кубические замощения» пространства (англ.: cube tilings), а также подсчитывалось количество подобных неэквивалентных замощений (число классов изоморфизма) для разных размерностей замощаемого пространства (см. таблицу 2).

Таблица 2 — Число неэквивалентных замощений пространства размерности n.

Размер n	Число замощений
$n = 1$	2
$n = 2$	12
$n = 3$	744
$n = 4$	5541744
$n = 5$	638560878292512

Для $n = 1,2,3,4$ количество замощений пространства размерности n совпадает с числом правильных булевых семейств размера n. Это совпадение неслучайно: в работе [152] было показано, что одностоковые ориентации булевых кубов находятся в биективном соответствии с замощениями пространства гиперкубами, а именно, было показано, что каждой одностоковой ориентации можно однозначно сопоставить клику в некотором графе специального вида (т.н. графы Келлера, см. [153]). Обобщим этот результат на случай k-значный случай: покажем, что правильные семейства функций k-значной логики находятся в биективном соответствии с кликами графов, построенных аналогично графам Келлера (и совпадающих с этими графами при $k = 2$).

Определение 53. Пусть $G = (V, E)$ — некоторый граф. Клика на m вершинах в графе G — это подмножество вершин $V' \subseteq V$ размера m, такое что каждые две вершины $v, w \in V'$ соединены ребром в G: $\{v, w\} \in E$.

Рассмотрим следующее обобщение графов Келлера на k-значный случай.

Определение 54. Зададим обобщенный граф Келлера $G(k, n)$ следующим образом:

– множество вершин графа V — наборы чисел от 0 до k^2-1 длины n:

$$V = \mathbb{E}_{k^2}^n;$$

– пара $\{v, w\}$ принадлежит множеству ребер E тогда и только тогда, когда найдется координата i, $1 \leqslant i \leqslant n$, что выполнены два условия:

$$v_i \equiv w_i \bmod k,\ v_i \neq w_i.$$

Будем рассматривать правильные семейства $\mathcal{F}_n$ размера n на $\mathbb{E}_k^n$. Покажем, что они находятся во взаимно-однозначном соответствии с **кликами** в графе $G(k,n)$ размера k^n (по правильному семейству строится клика в графе $G(k,n)$, и наоборот, по каждой клике размера k^n в $G(k,n)$ задается правильное семейство на $\mathbb{E}_k^n$).

Теорема 15. *Каждой клике на k^n вершинах в графе $G(k,n)$ можно поставить в биективное соответствие некоторое правильное семейство $\mathcal{F}_n$ размера n на $\mathbb{E}_k^n$.*

Доказательство. Доказательство будет состоять из двух частей. Сначала рассмотрим вложение множества правильных семейств в множество клик графа $G(k,n)$, а затем покажем обратное: по каждой клике графа $G(k,n)$ построим некоторое правильное семейство $\mathcal{F}_n$ размера n на $\mathbb{E}_k^n$.

Рассмотрим некоторое правильное семейство $\mathcal{F} = (f_1, \ldots, f_n)$ на $\mathbb{E}_k^n$. Каждому набору $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{E}_k^n$ поставим в соответствие набор из $\mathbb{E}_{k^2}^n$ следующим образом. Для $a, b \in \mathbb{E}_k$ определим число $\varphi(a,b) = k \cdot a + b \in \mathbb{E}_{k^2}$, тогда набору $\mathbf{x}$ поставим в соответствие набор

$$\mathbf{x} \to \Phi_{\mathcal{F}}(\mathbf{x}) = (\varphi(x_1, f_1(\mathbf{x})), \ldots, \varphi(x_n, f_n(\mathbf{x}))) \in \mathbb{E}_{k^2}^n.$$

Повторим указанный процесс для каждого $\mathbf{x} \in \mathbb{E}_k^n$ и получим набор вершин в графе $G(k,n)$, построенный по семейству $\mathcal{F}$.

Полученное отображение $\Phi_{\mathcal{F}}$ в множество вершин V инъективно для каждого фиксированного правильного семейства $\mathcal{F}$: если $\mathbf{x} \neq \mathbf{y}$, то $\Phi_{\mathcal{F}}(\mathbf{x}) \neq \Phi_{\mathcal{F}}(\mathbf{y})$. Это следует из свойства правильности: найдется индекс $1 \leqslant i \leqslant n$, что $x_i \neq y_i$, но $f_i(\mathbf{x}) = f_i(\mathbf{y})$, а значит, $\varphi(x_i, f_i(\mathbf{x})) = k \cdot x_i + f_i(\mathbf{x}) \neq k \cdot y_i + f_i(\mathbf{y}) = \varphi(y_i, f_i(\mathbf{y}))$. Заметим также, что для полученных элементов выполняется условие

$$\varphi(x_i, f_i(\mathbf{x})) \neq \varphi(y_i, f_i(\mathbf{y})), \quad \varphi(x_i, f_i(\mathbf{x})) \equiv \varphi(y_i, f_i(\mathbf{y})) \bmod k,$$

а значит, полученные вершины графа соединены ребром в $G(k,n)$. Таким образом, отображение $\Phi_{\mathcal{F}}$ задает по правильному семейству $\mathcal{F}$ некоторый подграф графа $G(k,n)$ на k^n вершинах, причем любые две вершины в подграфе соединены ребром, а значит, составляют клику.

Отображение $\mathcal{F} \to \Phi_{\mathcal{F}}$ также является инъективным (определяет различные клики при разных правильных семействах): если $\mathcal{F} \neq \mathcal{G}$, то существует $\mathbf{x} \in \mathbb{E}_k^n$, такой что $\mathcal{F}(\mathbf{x}) \neq \mathcal{G}(\mathbf{x})$, но тогда $\Phi_{\mathcal{F}}(\mathbf{x}) \neq \Phi_{\mathcal{G}}(\mathbf{x})$, и ни для какой точки $\mathbf{y} \in \mathbb{E}_k^n$ не может выполняться равенство $\Phi_{\mathcal{F}}(\mathbf{x}) = \Phi_{\mathcal{G}}(\mathbf{y})$, а значит, точки $\Phi_{\mathcal{F}}(\mathbf{x})$ нет в клике, задаваемой отображением $\Phi_{\mathcal{G}}$.

Рассмотрим теперь обратное отображение: каждому элементу $a \in \mathbb{E}_{k^2}$ поставим в соответствие пару $(x,y) \in \mathbb{E}_k^2$ вида

$$a \to \psi(a) = (a \text{ div } k,\ a \bmod k),$$

а каждому элементу $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{E}_{k^2}^n$ — пару векторов

$$(\mathbf{x}, \mathbf{y}) = \Psi(\mathbf{v}) \in (\mathbb{E}_k^n)^2,$$
$$(x_i, y_i) = \psi(v_i),\ 1 \leqslant i \leqslant n.$$

Покажем, что при этом отображении клики перейдут в правильные семейства.

Во-первых, такое отображение на кликах инъективно: если $\mathbf{v} \neq \mathbf{w}$, $\Psi(\mathbf{v}) = (\mathbf{x}, \alpha)$, $\Psi(\mathbf{w}) = (\mathbf{y}, \beta)$, $\mathbf{v}$ и $\mathbf{w}$ соединены ребром в графе $G(k,n)$, то найдется индекс i, для которого $v_i \neq w_i$, но $v_i \equiv w_i \bmod k$, а значит, $x_i \neq y_i$. В силу того, что в каждой рассматриваемой клике k^n вершин, указанное отображение ставит ей в соответствие множество пар $\{(\mathbf{x}, \alpha) \in (\mathbb{E}_k^n)^2 \mid \mathbf{x} \in \mathbb{E}_k^n\}$, где первые элементы пар $\mathbf{x}$ пробегают все множество $\mathbb{E}_k^n$.

Во-вторых, если мы интерпретируем второй элемент пары α как значение некоторого отображения $\mathcal{F} \in P_k^n$ на элементе первой пары $\mathbf{x}$ (т.е. $(\mathbf{x}, \alpha) = (\mathbf{x}, \mathcal{F}(\mathbf{x}))$), то семейство $\mathcal{F}$ будет правильным, покажем это. Рассмотрим два неравных набора $\mathbf{x} \neq \mathbf{y} \in \mathbb{E}_k^n$, а также их прообразы при отображении Ψ: $\mathbf{v} = \Psi^{-1}(\mathbf{x}, \alpha)$, $\mathbf{w} = \Psi^{-1}(\mathbf{y}, \beta)$. Для векторов $\mathbf{v}$ и $\mathbf{w}$ найдется индекс $1 \leqslant i \leqslant n$, для которого $v_i \neq w_i$, но $v_i \equiv w_i \bmod k$ (поскольку $\mathbf{v}$ и $\mathbf{w}$ соединены ребром в $G(k,n)$), а значит, $x_i \neq y_i$, но при этом $\alpha_i = \beta_i$, т.е. выполнено условие правильности. $\square$

2.4 Неортогональность аффинных подпространств

Рассмотрим одно обобщение результата [146, теорема 6], касающегося ортогональности подпространств булева куба. Указанный результат также был сформулирован для HUFP-сетей. На язык правильных семейств он «переводится» в более общей формулировке, но за счет некоторого ослабления понятия правильности в случае k-значных логик при $k \geqslant 3$ (см. определение 57).

Определение 55. Пусть $\mathbf{x}, \mathbf{y} \in Q^n$ — два набора из n элементов, обозначим через $[\mathbf{x}, \mathbf{y}]$ множество таких элементов $\mathbf{v} \in Q^n$, что $\mathbf{v}$ совпадает с $\mathbf{x}$ в тех номерах координат, где $x_i = y_i$:

$$[\mathbf{x}, \mathbf{y}] = \{\mathbf{v} \in Q^n \mid v_i = x_i = y_i \text{ для всех } i, \text{ где } x_i = y_i\}.$$

Будем называть $[\mathbf{x}, \mathbf{y}]$ подпространством в Q^n.

Замечание 30. В случае $Q = \mathbb{Z}_k$ нетрудно видеть, что $[\mathbf{x}, \mathbf{y}]$ — это аффинное подпространство в $\mathbb{Z}_k^n$.

Определение 56. Пусть $[\mathbf{x}, \mathbf{y}]$ и $[\mathbf{w}, \mathbf{v}]$ — два подпространства. Обозначим через $I = \{i_1, \ldots, i_s\}$ все позиции, для которых $x_{i_j} \neq y_{i_j}$; обозначим через $L = \{\ell_1, \ldots, \ell_t\}$ все позиции, для которых $w_{\ell_j} \neq v_{\ell_j}$. Будем говорить, что $[\mathbf{x}, \mathbf{y}]$ и $[\mathbf{w}, \mathbf{v}]$ ортогональны (и писать $[\mathbf{x}, \mathbf{y}] \perp [\mathbf{w}, \mathbf{v}]$), если выполнено следующее условие: $I \cap J = \varnothing$.

Пример 7 (Ортогональность в случае $Q = \mathbb{Z}_k$)**.** Рассмотрим случай $Q = \mathbb{Z}_k$. Тогда $[\mathbf{x}, \mathbf{y}]$ и $[\mathbf{w}, \mathbf{v}]$ являются аффинными подпространствами $\mathbb{Z}_k^n$. Пусть $[\mathbf{x}, \mathbf{y}] = \alpha + \mathcal{L}_1$, $[\mathbf{w}, \mathbf{v}] = \beta + \mathcal{L}_2$, тогда $[\mathbf{x}, \mathbf{y}] \perp [\mathbf{w}, \mathbf{v}]$ тогда и только тогда, когда $\mathcal{L}_1$ и $\mathcal{L}_2$ перпендикулярны (как векторные подпространства) относительно билинейной формы $\langle \mathbf{x} \mid \mathbf{y} \rangle = \sum_{i=1}^{n} x_i \cdot y_i$, то есть для любых $\mathbf{x} \in \mathcal{L}_1$ и $\mathbf{y} \in \mathcal{L}_2$ выполняется $\langle \mathbf{x} \mid \mathbf{y} \rangle = 0$.

Теперь сформулируем необходимое условие правильности семейства в терминах ортогональных подпространств.

Теорема 16. *Если семейство $\mathcal{F}_n \colon Q^n \to Q^n$ правильно, то для любых неравных $\mathbf{x}, \mathbf{y} \in Q^n$ выполнено условие не-ортогональности:*

$$[\mathbf{x}, \mathbf{y}] \not\perp [\mathbf{x} \circ \mathcal{F}_n(\mathbf{x}), \mathbf{y} \circ \mathcal{F}_n(\mathbf{y})].$$

Доказательство. Пусть $\mathcal{F}$ — правильное. Тогда по определению найдется такой индекс i, что $x_i \neq y_i$, но $f_i(x) = f_i(y)$. Но отсюда следует, что $x_i \circ f_i(x) \neq y_i \circ f_i(y)$. Следовательно, нашлась общая для $[\mathbf{x}, \mathbf{y}]$ и $[\mathbf{x} \circ \mathcal{F}(\mathbf{x}), \mathbf{y} \circ \mathcal{F}(\mathbf{y})]$ координата i такая, что $x_i \neq y_i$ и $x_i \circ f_i(x) \neq y_i \circ f_i(y)$. Это по определению влечет не-ортогональность соответствующих пространств. □

Обратное утверждение не всегда верно.

Пример 8. Рассмотрим случай $k = 3$, $n = 1$, $\mathcal{F}(x) = x$, $\circ = +$. В таком случае:

– семейство $\mathcal{F}$ не является правильным, так как зависит существенно от x;
– для семейства $\mathcal{F}$ выполнено условие не-ортогональности: для любых неравных $x \neq y$ имеем

$$[x, y] = \mathbb{E}_3,\ x + f(x) = 2x \neq y + f(y) = 2y,$$
$$[x + f(x), y + f(y)] = \mathbb{E}_3.$$

Однако мы можем ввести понятие «обобщенного правильного семейства», для которого условие «обобщенной правильности» будет эквивалентно условию отсутствия ортогональных аффинных подпространств указанного выше вида.

Определение 57. Пусть $(Q, \circ)$ — квазигруппа. Будем называть семейство $\mathcal{F}_n \colon Q^n \to Q^n$ обобщенно правильным, если для любых двух неравных наборов $\mathbf{x}, \mathbf{y} \in Q^n$ найдется индекс i, такой что выполнены условия:

$$x_i \neq y_i, \quad x_i \circ f_i(\mathbf{x}) \neq y_i \circ f_i(\mathbf{y}).$$

Замечание 31. Отметим два факта:

– правильные семейства являются обобщенно правильными: для правильных семейств найдется индекс i, что $x_i \neq y_i$, но $f_i(\mathbf{x}) = f_i(\mathbf{y})$, откуда следует $x_i \circ f_i(x) \neq y_i \circ f_i(y)$;
– для булева случая понятия правильности и обобщенной правильности эквивалентны: фактически, сформулированное выше характеристическое свойства эквивалентно свойству отсутствия т.н. «зеркальных пар» у семейства булевых функций (см. [147, раздел 3]).

Теорема 17. *Семейство $\mathcal{F}_n \colon Q^n \to Q^n$ является обобщенно правильным тогда и только тогда, когда выполнено условие не-ортогональности аффинных подпространств: для любых двух неравных наборов $\mathbf{x}, \mathbf{y} \in Q^n$ выполняется*

$$[\mathbf{x}, \mathbf{y}] \not\perp [\mathbf{x} \circ \mathcal{F}(\mathbf{x}), \mathbf{y} \circ \mathcal{F}(\mathbf{y})]$$

Доказательство. В прямую сторону утверждение доказывается аналогично утверждению 16. В обратную сторону утверждение также является простым следствием определения ортогональности. □

Теорема 18. *Пусть семейство $\mathcal{F}\colon Q^n \to Q^n$ обобщенно правильное. Тогда отображение $\sigma_{\mathcal{F}}\colon Q^n \to Q^n$, переводящее $\mathbf{x} \in Q^n$ в $\mathbf{x} \circ \mathcal{F}(\mathbf{x})$, является биективным.*

Доказательство. Докажем инъективность отображения $\sigma_{\mathcal{F}}$: по определению обобщенной правильности для любых $\mathbf{x} \neq \mathbf{y}$ найдется индекс i такой, что

$$x_i \circ f_i(\mathbf{x}) = \sigma_{\mathcal{F}}(\mathbf{x})[i] \neq \sigma_{\mathcal{F}}(\mathbf{y})[i] = y_i \circ f_i(\mathbf{y}).$$

Биективность следует из конечности Q^n. □

Выводы

В этой главе мы рассмотрели несколько альтернативных способов описания булева правильного семейства:

- характеризация в терминах одностоковой ориентации (т.н. USO-ориентации булева куба);
- характеризация в терминах булевой сети с наследственно неподвижной точкой (т.н. HUFP-сети);
- характеризация в терминах булева отображения, каждая проекция которого не является самодвойственной,
- характеризация в терминах клик обобщенных графов Келлера.

Также было введено понятие обобщенно правильного семейства и его альтернативная характеризация в терминах ортогональности подпространств (в случае $k = 2$ понятие обобщенно правильного семейства совпадает с понятием правильного семейства).

Таким образом, один и тот же объект (правильные семейства) может быть рассмотрен сразу с нескольких точек зрения, а результаты, полученные в рамках одного «языка», могут быть перенесены на другой «язык» (часто даже в более общем виде). При этом геометрическая интуиция позволяет ввести некоторые новые классы семейств, такие как рекурсивно и локально треугольные семейства, а также доказать некоторые свойства правильных семейств (например, coNP-полноту

задачи распознавания правильности по схеме из функциональных элементов [58; 154] или оценку на число булевых правильных семейств).

Глава 3. Свойства правильных семейств

В настоящей главе мы рассмотрим некоторые свойства правильных семейств.

1. В разделе 3.1 мы рассмотрим задачу поиска стабилизатора множества правильных семейств относительно действий биекциями

$$(\Phi, \Psi) \curvearrowright \mathcal{F} \colon x \to \Phi(\mathcal{F}(\Psi(x))).$$

2. В разделе 3.2 рассмотрены вопросы оценки мощности образов и прообразов при действии отображения

$$\mathbf{x} \to \mathcal{F}(\mathbf{x}), \mathbf{x} \in \mathbb{E}_2^n, \mathcal{F} \text{ — правильное.}$$

3. Раздел 3.3 посвящен изучению свойств подстановок $\pi_{\mathcal{F}}$, порождаемых правильными семействами.

На протяжении всей главы рассматриваемые объекты предполагаются конечными.

Результаты главы ранее были опубликованы в [73; 74; 77; 79].

3.1 Преобразования, сохраняющие правильность

В разделе 1.3.4 было показано, что сдвиги (внутренние и внешние), а также согласованные перестановки семейства сохраняют свойство семейства «быть правильным». В настоящем разделе мы рассмотрим обратную задачу.

Пусть Φ, Ψ — биекции на множестве $\mathbb{E}_k^n$: $\Phi, \Psi \in \mathcal{S}_{\mathbb{E}_k^n}$. При каких условиях на Φ, Ψ семейство, задающее отображение

$$\mathbf{x} \to \Phi(\mathcal{F}(\Psi(\mathbf{x})))$$

также будет являться правильным для всех правильных семейств $\mathcal{F}$? Другими словами, рассматривается вопрос о поиске стабилизатора для множества всех правильных семейств $\mathcal{F}_n$ размера n при действии группы $\mathcal{S}_{E_k^n} \times \mathcal{S}_{E_k^n}$ на множестве всех семейств размера n, при котором (Φ, Ψ) переводит семейство $\mathcal{F}$ в семейство $\mathcal{F}'$,

заданное соотношением

$$\mathcal{F}' \colon \mathbf{x} \to \Phi(\mathcal{F}(\Psi(\mathbf{x}))).$$

Далее мы покажем, что такими Φ и Ψ могут быть только композиции согласованных перестановок и перекодировок семейства (см. определения 24 и 59).

3.1.1 Перекодировки и изометрии пространства $\mathbb{E}_k^n$

Дадим несколько предварительных определений.

Определение 58. Перекодировкой вектора $\mathbf{x} \in Q^n$ будем называть вектор $\mathbf{y}$ вида $\mathbf{y} = (\varphi_1(x_1), \ldots, \varphi_n(x_n))$, где $\varphi_i \in \mathcal{S}_Q$.

Определение 59. Перекодировкой семейства $\mathcal{F}_n$, заданного на Q^n, будем называть семейство $\mathcal{G}$ вида:

$$\mathcal{G}(\mathbf{x}) = \begin{bmatrix} \varphi_1(f_1(\psi_1(x_1), \ldots, \psi_n(x_n))) \\ \vdots \\ \varphi_n(f_n(\psi_1(x_1), \ldots, \psi_n(x_n))) \end{bmatrix},$$

где $\varphi_i, \psi_i \in \mathcal{S}_Q$.

Замечание 32. Перекодировка семейства является композицией перекодировки аргумента функции (как вектора) и перекодировки полученного вектора значений функции.

Как было отмечено ранее (см. утверждение 10), согласованные перестановки сохраняют свойство правильности. Аналогичное свойство выполняется и для перекодировок (при этом перекодировки не обязаны быть согласованными).

Утверждение 24 ([132, Лемма 2])**.** *Если $\mathcal{F}_n$ — правильное семейство, то любая перекодировка $\mathcal{G}_n$ семейства $\mathcal{F}_n$ также является правильным семейством.*

Там же доказан следующий критерий правильности семейства в терминах перекодировок, являющийся обобщением критерия из раздела 2.1.2.

Утверждение 25 ([132, Теорема 1])**.** *Семейство $\mathcal{F}_n$ на Q^n является правильным тогда и только тогда, когда любая перекодировка любой проекции $\mathcal{F}_n$ (в том числе и тривиальная проекция) имеет единственную неподвижную точку.*

Заметим, что перекодировки и перестановки вектора (см. определение 23) сохраняют (не)равенство координат пары векторов. Другими словами, если $d(\mathbf{x}, \mathbf{y})$ — метрика Хэмминга на пространстве $\mathbb{E}_k^n$, то для перекодировок и перестановок вектора Φ выполняется равенство

$$d(\mathbf{x}, \mathbf{y}) = d(\Phi(\mathbf{x}), \Phi(\mathbf{y})).$$

Это наблюдение побуждает поставить следующий вопрос: верно ли, что преобразования, сохраняющие правильность, обязаны быть изометриями пространства $\mathbb{E}_k^n$ с метрикой Хэмминга? Далее мы утвердительно ответим на этот вопрос. Введем несколько предварительных определений.

Определение 60. Пусть (M, d) — метрическое пространство с метрикой d, тогда группой изометрий $Iso(M, d)$ пространства (M, d) будем называть множество подстановок на множестве M

$$Iso(M, d) = \{\Phi \in \mathcal{S}_M \mid d(\Phi(\mathbf{x}), \Phi(\mathbf{y})) = d(\mathbf{x}, \mathbf{y})\ \forall \mathbf{x}, \mathbf{y} \in M\}$$

с операцией композиции отображений.

Нам также понадобится понятие слабой изометрии как отображения, которое сохраняет расстояние между точками, находящимися на строго определенном фиксированном расстоянии.

Определение 61. Будем называть p-изометрией (слабой изометрией) биективное отображение $\Phi\colon M \to M$ такое, что оно сохраняет расстояние между точками, которые находятся на расстоянии p. Введем в рассмотрение множество всех p-изометрий:

$$Iso_p(M, d) = \{\Phi \in \mathcal{S}_M \mid d(\Phi(\mathbf{x}), \Phi(\mathbf{y})) = d(\mathbf{x}, \mathbf{y})\ \forall \mathbf{x}, \mathbf{y} \in M,\ d(\mathbf{x}, \mathbf{y}) = p\}.$$

Замечание 33. Легко увидеть, что множество p-изометрий $Iso_p(M, d)$ для конечных пространств M образует группу относительно операции композиции отображений (в частности, обратное к p-изометрии преобразование также является p-изометрией).

Замечание 34. Если метрика d понятна из контекста, то обозначение d можно опустить. Далее будет рассматриваться только метрика Хэмминга.

Приведем два результата, связывающих множество слабых изометрий и изометрий пространств с метрикой Хэмминга d.

Утверждение 26 ([155, Теорема 1], [156, Лемма 1])**.** *Если* Φ *является 1-изометрией пространства* $(\mathbb{E}_2^n, d)$*, то* Φ *является изометрией* $(\mathbb{E}_2^n, d)$.

Утверждение 27 ([157, Теорема 4.1])**.** *Если* Φ *является 1-изометрией* $(\mathbb{E}_k^n, d)$*,* $k > 2$*,* $n > 2$*, то* Φ *является изометрией* $(\mathbb{E}_k^n, d)$.

Замечание 35. Из формулировки утверждений 26 и 27 видно, что существуют особые случаи, не покрываемые приведенными выше утверждениями. Рассмотрим каждый из них более подробно.

Случай $k > 2$, $n = 1$ тривиален: любая биекция в указанном вырожденном случае является изометрией.

Случай $k > 2$, $n = 2$: пусть Φ является 1-изометрией и биекцией. Покажем, что Φ также сохраняет расстояние 2. Пусть $\alpha, \beta \in \mathbb{E}_k^2$, $d(\alpha, \beta) = 2$. В силу биективности $d(\Phi(\alpha), \Phi(\beta)) > 0$. Предположим, что $d(\Phi(\alpha), \Phi(\beta)) = 1$. В таком случае, поскольку Φ^{-1} также является 1-изометрией (см. замечание 33), мы имеем противоречие:

$$1 = d\left(\Phi(\alpha), \Phi(\beta)\right) = d\left(\Phi^{-1}(\Phi(\alpha)), \Phi^{-1}(\Phi(\beta))\right) = d\left(\alpha, \beta\right) = 2.$$

Других значений расстояния в случае $n = 2$ не бывает.

Таким образом, мы доказали следующее вспомогательное утверждение.

Лемма 10. *Группа 1-изометрий пространства* $\mathbb{E}_k^n$ *с метрикой Хэмминга совпадает с группой всех изометрий пространства* $\mathbb{E}_k^n$*:*

$$Iso_1(\mathbb{E}_k^n) = Iso(\mathbb{E}_k^n).$$

Также для пространств Хэмминга верно следующее утверждение, устанавливающее связь между изометриями $\mathbb{E}_k^n$ и ранее введенными преобразованиями векторов (см. определения 58 и 23).

Утверждение 28 ([158])**.** *Группа изометрий* $Iso(\mathbb{E}_k^n)$ *состоит из композиций перестановок и перекодировок векторов.*

3.1.2 Биекции, сохраняющие правильность

Нашей задачей является доказательство того факта, что если Φ и Ψ — биекции, и $\Phi(\mathcal{F}_n(\Psi(x)))$ — правильное семейство для любого правильного семейства $\mathcal{F}_n\colon \mathbb{E}_k^n \to \mathbb{E}_k^n$, то Φ, Ψ являются изометриями пространства $Iso(\mathbb{E}_k^n)$. Для этого мы сначала докажем, что Φ и Ψ должны быть 1-изометриями (леммы 12 и 13). Тогда из леммы 10 будет следовать, что Φ и Ψ являются изометриями $\mathbb{E}_k^n$. Наконец, мы применим утверждение 28 совместно с некоторыми дополнительными соображениями и покажем, что биективные преобразования, сохраняющие правильность семейств, исчерпываются перекодировками и согласованными перестановками семейства (теорема 19).

Замечание 36. Мы рассматриваем только пары биекций. Так, например, в указанные классы преобразований не входят отображения вида $f_n(x_1, \ldots, x_n) \to a$, $a \in \mathbb{E}_k$, $f_i(x_1, \ldots, x_n) \to f_i(x_1, \ldots, x_{n-1}, b)$, $1 \leqslant i \leqslant n-1$ (комбинация проекции семейства с дополнением константой), которые сохраняют правильность, а также преобразования, описанные в работе [59].

Как уже было отмечено ранее (см. замечание 14), правильное семейство не может принимать противоположные значения. Однако верно следующее утверждение.

Лемма 11. *Пусть α, $\beta \in Q^n$ — два не-противоположных набора (т.е. $d(\alpha, \beta) < n$). Тогда существует правильное семейство $\mathcal{F}_n$ и наборы $\mathbf{x}$, $\mathbf{y}$, такие что $\mathcal{F}(\mathbf{x}) = \alpha$, $\mathcal{F}(\mathbf{y}) = \beta$.*

Доказательство. Достаточно рассмотреть правильным образом подобранное треугольное семейство. Без ограничения общности будем предполагать, что первые ℓ координат наборов совпадают:

$$\alpha_1 = \beta_1, \ldots, \alpha_\ell = \beta_\ell, \ell \geqslant 1.$$

В таком случае зададим первые ℓ функций треугольного семейства как константы

$$f_i \equiv \alpha_i,\ 1 \leqslant i \leqslant \ell,$$

оставшиеся $(n-\ell)$ функций зададим так, чтобы на некотором фиксированном $\mathbf{x}_0$ они принимали значения $\alpha_{\ell+1}, \ldots, \alpha_n$, на некотором фиксированном $\mathbf{y}_0$ (отличном от $\mathbf{x}_0$ в первых ℓ координатах) — значения $\beta_{\ell+1}, \ldots, \beta_n$. Тогда мы получим

семейство вида

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_\ell \\ \mathcal{F}_{n-\ell}(x_1, \ldots, x_\ell) \end{bmatrix},$$

которое является треугольным и обладает требуемым свойством. □

Лемма 12. *Пусть семейства $\mathcal{G}(\mathbf{x})$ вида $\mathcal{G}(\mathbf{x}) = \Phi(\mathcal{F}(\Psi(\mathbf{x})))$ являются правильными для всех правильных семейств $\mathcal{F}$, заданных на $\mathbb{E}_k^n$, Φ и Ψ — биекции множества $\mathbb{E}_k^n$. Тогда Ψ является 1-изометрией пространства Хэмминга $\mathbb{E}_k^n$.*

Доказательство. Докажем от противного. Предположим, что Ψ не является 1-изометрией, Φ и Ψ биективны, и покажем, что существует такое правильное семейство $\mathcal{F}$ на $\mathbb{E}_k^n$, что $\mathcal{G}(\mathbf{x}) = \Phi(\mathcal{F}(\Psi(\mathbf{x})))$ не является правильным.

Так как Ψ — не 1-изометрия, то найдутся наборы $\mathbf{x}_1$, $\mathbf{x}_2$, что $d(\mathbf{x}_1, \mathbf{x}_2) = 1$, но $d(\Psi(\mathbf{x}_1), \Psi(\mathbf{x}_2)) > 1$ (заметим, что указанное расстояние не может быть равно 0, т.к. Ψ биективно). Пусть для определенности $\mathbf{x}_1$ и $\mathbf{x}_2$ различны только в i-й координате, и найдутся такие индексы j_1, j_2, что $\Psi(\mathbf{x}_1)$ и $\Psi(\mathbf{x}_2)$ различны в позициях j_1 и j_2. Подберем такое семейство $\mathcal{F}_n$, что выполнено неравенство

$$\mathcal{G}_i(\mathbf{x}_1) = \Phi(\mathcal{F}(\Psi(\mathbf{x}_1)))[i] \neq \Phi(\mathcal{F}(\Psi(\mathbf{x}_2)))[i] = \mathcal{G}_i(\mathbf{x}_2).$$

Рассмотрим множество пар точек $(\mathbf{w}_1, \mathbf{w}_2)$, $\mathbf{w}_1, \mathbf{w}_2 \in \mathbb{E}_k^n$, таких что $\mathbf{w}_1[i] \neq \mathbf{w}_2[i]$. Число таких пар точек равно $k^{2n-1}(k-1)$, поскольку есть k^n способов зафиксировать $\mathbf{w}_1$ и $k^{n-1}(k-1)$ способов зафиксировать $\mathbf{w}_2$. Теперь рассмотрим множество пар точек

$$(\mathbf{y}_1, \mathbf{y}_2) = (\Phi^{-1}(\mathbf{w}_1), \Phi^{-1}(\mathbf{w}_2)).$$

Среди таких пар найдется пара со свойством $\mathbf{y}_1[j_1] = \mathbf{y}_2[j_1]$ или $\mathbf{y}_1[j_2] = \mathbf{y}_2[j_2]$, поскольку число пар, не удовлетворяющих этому свойству, равно $k^{2n-2} \cdot (k-1)^2$, что меньше числа $k^{2n-1} \cdot (k-1)$.

Таким образом, найдутся два набора $\mathbf{y}_1$, $\mathbf{y}_2$ со свойствами:

– $\Phi(\mathbf{y}_1)[i] \neq \Phi(\mathbf{y}_2)[i]$;

– $\mathbf{y}_1[j] = \mathbf{y}_2[j]$, где $j \in \{j_1, j_2\}$.

Построим по этим наборам семейство $\mathcal{F}$ так, чтобы выполнялись равенства

$$\mathcal{F}(\Psi(\mathbf{x}_1)) = \mathbf{y}_1, \ \mathcal{F}(\Psi(\mathbf{x}_2)) = \mathbf{y}_2.$$

Для этого рассмотрим треугольное семейство $\mathcal{F}$, такое что $f_j(\cdot) \equiv \mathbf{y}_1[j]$, а остальные функции зависят от j-й переменной таким образом, что если она равна $\Psi(\mathbf{x}_1)[j]$, то все семейство принимает значение $\mathbf{y}_1$, а если она равна $\Psi(\mathbf{x}_2)[j]$, то все семейство принимает значение $\mathbf{y}_2$.

Построенное семейство $\mathcal{F}$ будет правильным (в силу треугольности). При этом будет выполняться условие:

$$\Phi(\mathcal{F}(\Psi(\mathbf{x}_1)))[i] = \Phi(\mathbf{y}_1)[i] \neq \Phi(\mathbf{y}_2)[i] = \Phi(\mathcal{F}(\Psi(\mathbf{x}_2)))[i],$$

а значит, семейство $\mathcal{G}$ не является правильным (нарушено условие правильности на паре наборов $\mathbf{x}_1$, $\mathbf{x}_2$). □

Замечание 37. Из доказанного утверждения и леммы 10 следует, что Ψ является изометрией пространства $\mathbb{E}_k^n$ с метрикой Хэмминга.

Лемма 13. *Пусть семейства $\mathcal{G}(\mathbf{x})$ вида $\mathcal{G}(\mathbf{x}) = \Phi(\mathcal{F}(\Psi(\mathbf{x})))$ являются правильными для всех правильных семейств $\mathcal{F}$, заданных на $\mathbb{E}_k^n$, Φ и Ψ — биекции множества $\mathbb{E}_k^n$. Тогда Φ является 1-изометрией пространства Хэмминга $\mathbb{E}_k^n$.*

Доказательство. Случай биективного отображения Ψ, не являющегося изометрией, был разобран ранее, поэтому мы можем предполагать, что Ψ — изометрия.

Предположим, что Φ — не 1-изометрия. Это означает, что найдутся наборы $\mathbf{y}_1, \mathbf{y}_2 \in \mathbb{E}_k^n$ такие, что

$$d(\mathbf{y}_1, \mathbf{y}_2) = 1, d(\Phi(\mathbf{y}_1), \Phi(\mathbf{y}_2)) = t > 1;$$

указанное расстояние не может быть равно 0, т.к. Φ — биекция. Для определенности обозначим через j индекс, в котором $\mathbf{y}_1$ и $\mathbf{y}_2$ различаются: $\mathbf{y}_1[j] \neq \mathbf{y}_2[j]$.

Если мы предположим, что $t = n$, то по лемме 11 найдется правильное семейство $\mathcal{F}_n$, которое принимает оба значения $\mathbf{y}_1$ и $\mathbf{y}_2$ на некоторых $\mathbf{x}_1$, $\mathbf{x}_2$. Но тогда $\Phi(\mathcal{F}_n(\Psi(\mathbf{x})))$ не может быть правильным, так как принимает противоположные значения (см. замечание 14).

Следовательно, мы имеем $1 < t < n$ (что возможно только при $n \geqslant 3$). Будем считать без ограничения общности, что $\Phi(\mathbf{y}_1)$ и $\Phi(\mathbf{y}_2)$ различаются в первых t индексах:

$$\Phi(\mathbf{y}_1)[i] \neq \Phi(\mathbf{y}_2)[i],\ 1 \leqslant i \leqslant t.$$

Построим два набора $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{E}_k^n$ и правильное семейство $\mathcal{F}_n$ так, чтобы выполнялись условия:

$$\mathcal{F}_n(\Psi(\mathbf{x}_1)) = \mathbf{y}_1,\ \mathcal{F}_n(\Psi(\mathbf{x}_2)) = \mathbf{y}_2,$$

при этом потребуем, чтобы

– $\mathbf{x}_1[i] \neq \mathbf{x}_2[i]$ при $1 \leqslant i \leqslant t$;
– $\mathbf{x}_1[i] = \mathbf{x}_2[i]$ при $t+1 \leqslant i \leqslant n$.

Поскольку Ψ по предположению является изометрией, то

$$d(\Psi(\mathbf{x}_1), \Psi(\mathbf{x}_2)) = t > 1,$$

следовательно, найдется $j' \neq j$, такой что $\Psi(\mathbf{x}_1)[j'] \neq \Psi(\mathbf{x}_2)[j']$. Зададим j-ю функцию семейства $\mathcal{F}_n$ следующим образом:

– $\mathbf{y}_1[j]$, если j'-я переменная принимает значения $\Psi(x_1)[j']$;
– $\mathbf{y}_2[j]$, если j'-я переменная принимает значения $\Psi(x_2)[j']$.

Остальные функции f_i положим тождественно равными $\mathbf{y}_1[i]$, где $1 \leqslant i \leqslant n, i \neq j$. Полученное семейство является треугольным, а следовательно, правильным. Для семейства $\mathcal{G}(\mathbf{x}) = \Phi(\mathcal{F}(\Psi(\mathbf{x})))$ условие правильности нарушается на наборах $\mathbf{x}_1$ и $\mathbf{x}_2$. Мы предположили, что Φ не является 1-изометрией, и пришли к противоречию, из которого следует утверждение. □

Замечание 38. Из доказанного утверждения и леммы 10 следует, что Φ является изометрией $\mathbb{E}_k^n$.

Теорема 19. *Пусть семейства $\mathcal{G}(\mathbf{x})$ вида $\mathcal{G}(\mathbf{x}) = \Phi(\mathcal{F}(\Psi(\mathbf{x})))$ являются правильными для всех правильных семейств $\mathcal{F}$, заданных на $\mathbb{E}_k^n$, Φ и Ψ — биекции множества $\mathbb{E}_k^n$. Тогда Φ и Ψ имеют вид*

$$\Phi = \sigma \circ A, \Psi = \sigma \circ B,$$

где использованы следующие обозначения:

– $\sigma \in \mathcal{S}_n$ *(перенумерация координат вектора);*
– $A, B \in (\mathcal{S}_{\mathbb{E}_k})^n$ *(перекодировки вектора).*

Доказательство. Мы уже показали (см. замечания 37 и 38), что Φ и Ψ обязаны быть изометриями пространства $\mathbb{E}_k^n$. Из утверждения 28 следует, что $\Phi = (\sigma_1 \circ A)$, $\Psi = (\sigma_2 \circ B)$, где $\sigma_1, \sigma_2 \in \mathcal{S}_n$, $A, B \in (\mathcal{S}_{\mathbb{E}_k})^n$. Покажем, что в таком случае $\sigma_1 = \sigma_2$ (т.е. перестановка семейства должна быть согласованной).

Применение покомпонентных преобразований A и B не меняет свойства правильности, поэтому можно ограничиться случаем рассмотрения $\Phi = (\sigma_1 \circ \mathrm{id})$, $\Psi = (\sigma_2 \circ \mathrm{id})$, где id — тождественное преобразование $\mathbb{E}_k^n \to \mathbb{E}_k^n$. Пусть $\sigma_1 \neq \sigma_2$.

Тогда существуют i и j со свойством $\sigma_1(i) = \sigma_2(j) = s$, при этом $i \neq j$. В таком случае достаточно рассмотреть треугольное семейство

$$f_i(x_j) = x_j,\ f_\ell \equiv const,\ \ell \neq i.$$

Под действием $(\Phi, \Psi) \curvearrowright \mathcal{F}$ семейство $\mathcal{F}$ перейдет в семейство, включающее в себя функцию $f_{\sigma_1(i)}(x_{\sigma_2(j)}) = f_s(x_s) = x_s$, что противоречит правильности. □

Замечание 39. Заметим, что в булевом случае $k = 2$ перекодировки семейства исчерпываются сдвигами. Для одностоковых ориентаций булева куба (см. раздел 2.1) внешние и внутренние сдвиги, равно как и согласованная перенумерация сохраняют свойство ориентации быть одностоковой (подробнее см. [133, Лемма 4.4]). Таким образом, в булевом случае имеется взаимно-однозначное соответствие между «алгебраическим» и «геометрическим» описанием семейства. В случае k-значной логики класс преобразований, сохраняющих правильность, является более широким, чем класс преобразований, сохраняющих «одностоковость», и указанное соответствие разрушается.

3.2 Образы и прообразы при действии правильного семейства

В этом разделе мы будем рассматривать булево семейство $\mathcal{F}_n$ как отображение $\mathbb{E}_2^n \to \mathbb{E}_2^n$:

$$\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \to \mathcal{F}_n(\mathbf{x}) = \begin{bmatrix} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_n(x_1, \ldots, x_n) \end{bmatrix}.$$

Как было показано в работе [77], мощность образа правильного семейства является важной характеристикой, которая, в частности, определяет, какое количество различных d-квазигрупп может быть порождено с помощью конструкции, описанной в утверждении 5.

Для правильных семейств выполняется следующее ограничение на мощность образа.

Утверждение 29 ([77, Теорема 5])**.** *Число значений, принимаемых правильным семейством размера n в k-значной логике, не превосходит k^{n-1}.*

3.2.1 Мощность прообраза при действии правильного семейства

Зададимся следующим вопросом. Пусть дана точка $\alpha \in \mathbb{E}_2^n$. Что в таком случае можно сказать о мощности множества прообразов точки α при действии отображения $\mathcal{F}_n$:

$$\mathcal{F}_n^{-1}(\alpha) = \{\mathbf{x} \in \mathbb{E}_2^n \mid \mathcal{F}_n(\mathbf{x}) = \alpha\}.$$

Оказывается, что для правильных семейств булевых функций верна следующая теорема.

Теорема 20. *Пусть $\mathcal{F}_n$ — правильное семейство булевых функций. Тогда для любого $\alpha \in \mathbb{E}_2^n$ число решений уравнения $\mathcal{F}_n(\mathbf{x}) = \alpha$ четно.*

Замечание 40. Случай уравнения $\mathcal{F}_n(\mathbf{x}) = \alpha$ можно свести к рассмотрению уравнения $\mathcal{F}_n(\mathbf{x}) = 0^n$. По утверждению 9 если $\mathcal{F}_n(\mathbf{x})$ — правильное семейство, то и $\mathcal{G}(\mathbf{x}) = \mathcal{F}(\mathbf{x}) \oplus \alpha$ также является правильным. При этом $\mathbf{x}^*$ является решением уравнения $\mathcal{F}(\mathbf{x}) = \alpha$ тогда и только тогда, когда $\mathbf{x}^*$ является решением уравнения $\mathcal{G}(\mathbf{x}) = 0^n$.

Перейдем к доказательству теоремы 20.

Доказательство. Используя замечание 40, достаточно доказать, что уравнение $\mathcal{F}_n(\mathbf{x}) = 0^n$ всегда имеет четное число решений, где $\mathcal{F}_n$ — правильное семейство булевых функций размера n. Будем вести доказательство индукцией по размеру правильного семейства.

База индукции $(n = 1)$**:** семейства размера 1 — это константные функции

$$0(x_1) \equiv 0, \quad 1(x_1) \equiv 1.$$

Очевидно, что для этих двух семейств уравнение $\mathcal{F}_1(x_1) = 0$ имеет 2 или 0 решений соответственно.

Предположение индукции: допустим, что уравнение $\mathcal{G}_k(\mathbf{x}) = 0^k$ имеет четное число решений для любого правильного семейства $\mathcal{G}$ размера $k \leqslant n$. Пусть теперь нам дано правильное булево семейство $\mathcal{F}_{n+1}$ размера $n+1$. Введем обозначение $\mathbf{x} = (x_1, \ldots, x_n)$. По свойству правильности мы можем утверждать, что f_{n+1} не зависит существенно от переменной x_{n+1} (см. замечание 13). С учетом этого

замечания мы можем считать, что f_{n+1} зависит только от первых n переменных, то есть от $\mathbf{x}$. Тогда верно следующее разложение:

$$\mathcal{F}_{n+1}(x_1, \ldots, x_{n+1}) = \begin{bmatrix} x_{n+1} \cdot \mathcal{F}^1(\mathbf{x}) \oplus \overline{x_{n+1}} \cdot \mathcal{F}^0(\mathbf{x}) \\ f_{n+1}(\mathbf{x}) \end{bmatrix},$$

где через $\mathcal{F}^b(x)$, $b \in \{0, 1\}$, обозначены семейства-проекции

$$\mathcal{F}^b(\mathbf{x}) = \Pi^b_{n+1}(\mathcal{F}_{n+1}) = \begin{bmatrix} f_1(x_1, \ldots, x_n, b) \\ \vdots \\ f_n(x_1, \ldots, x_n, b) \end{bmatrix}.$$

Заметим, что оба семейства $\mathcal{F}^b$, $b \in \{0, 1\}$, также являются правильными семействами размера n (согласно утверждению 11), а значит, к ним применимо предположение индукции.

Рассмотрим множество M решений уравнения $f_{n+1}(\mathbf{x}) = 0$:

$$M = \{\mathbf{x}^* \mid f_{n+1}(\mathbf{x}^*, 0) = f_{n+1}(\mathbf{x}^*, 1) = 0\} \subseteq \mathbb{E}_2^n.$$

Если $M = \varnothing$, то нет ни одного решения уравнения $\mathcal{F}_{n+1}(x_1, \ldots, x_{n+1}) = 0^{n+1}$, и утверждение теоремы верно для $\mathcal{F}_{n+1}$.

Если набор $\mathbf{x}^* \in M$ таков, что $\mathcal{F}^0(\mathbf{x}^*) = \mathcal{F}^1(\mathbf{x}^*) = 0^n$, то мы можем продолжить набор $\mathbf{x}^*$ любым значением $x_{n+1} \in \{0, 1\}$ и получить два набора $(\mathbf{x}^*, 0)$, $(\mathbf{x}^*, 1)$, каждый из которых является решением исходного уравнения.

Если набор $\mathbf{x}^* \in M$ таков, что $\mathcal{F}^0(\mathbf{x}^*) \neq 0^n$, $\mathcal{F}^1(\mathbf{x}^*) \neq 0^n$, то для любого продолжения x_{n+1} получим $\mathcal{F}_{n+1}(\mathbf{x}^*, x_{n+1}) \neq 0^{n+1}$, то есть такой набор $\mathbf{x}^*$ не продолжается до решения исходного уравнения.

Если набор $\mathbf{x}^* \in M$ таков, что $\mathcal{F}^0(\mathbf{x}^*) \neq 0^n$, $\mathcal{F}^1(\mathbf{x}^*) = 0^n$ (или наоборот, $\mathcal{F}^0(\mathbf{x}^*) = 0^n$, $\mathcal{F}^1(\mathbf{x}^*) \neq 0^n$), то продолжение x_{n+1} возможно единственным способом ($x_{n+1} = 1$ в первом случае и $x_{n+1} = 0$ во втором случае). Следовательно, необходимо показать, что может существовать только четное число наборов $\mathbf{x}^*$ таких, что ровно одно из подсемейств $\mathcal{F}^0(\mathbf{x}^*)$ или $\mathcal{F}^1(\mathbf{x}^*)$ равно нулю на нем.

Схематично все наборы из множества M можно разбить на 4 категории (см. таблицу 3): $M = A \sqcup B \sqcup C \sqcup D$, где

- A — множество наборов $\mathbf{x}^* \in M$, для которых $\mathcal{F}^0(\mathbf{x}^*) = \mathcal{F}^1(\mathbf{x}^*) = 0$;
- B — множество наборов $\mathbf{x}^* \in M$, для которых $\mathcal{F}^0(\mathbf{x}^*) \neq 0$, $\mathcal{F}^1(\mathbf{x}^*) = 0$;
- C — множество наборов $\mathbf{x}^* \in M$, для которых $\mathcal{F}^0(\mathbf{x}^*) = 0$, $\mathcal{F}^1(\mathbf{x}^*) \neq 0$;
- D — множество наборов $\mathbf{x}^* \in M$, для которых $\mathcal{F}^0(\mathbf{x}^*) \neq 0$, $\mathcal{F}^1(\mathbf{x}^*) \neq 0$.

Таблица 3 — Разбиение множества M

	$\mathcal{F}^0(\mathbf{x}^*) = 0^n$	$\mathcal{F}^0(\mathbf{x}^*) \neq 0^n$
$\mathcal{F}^1(\mathbf{x}^*) = 0^n$	A	B
$\mathcal{F}^1(\mathbf{x}^*) \neq 0^n$	C	D

Нам достаточно доказать, что $|B|+|C|$ четно. По предположению индукции мы знаем, что число решений уравнений $\mathcal{F}^0(\mathbf{x}) = 0^n$ и $\mathcal{F}^1(\mathbf{x}) = 0^n$ четно, то есть $|A| + |B|$ и $|A| + |C|$ — четные числа. Но тогда четно и число

$$(|A| + |B|) + (|A| + |C|) = 2|A| + (|B| + |C|),$$

а следовательно, $|B| + |C|$ также четно.

Таким образом, мы получили четное число продолжений набора $\mathbf{x}^* \in M$ до полного решения исходной системы $\mathcal{F}_{n+1}(x_1, \ldots, x_{n+1}) = 0^{n+1}$, что и требовалось доказать. □

3.2.2 Мощность образов некоторых семейств

В настоящем разделе изучаются некоторые из приведенных в разделе 1.3.3 примеров правильных семейств булевых функций с точки зрения мощности образа.

Рассмотрим семейство (1.5) из раздела 1.3.3, обозначим его через $\mathcal{F}_n$. Введем несколько дополнительных обозначений:

– обозначение для суммы:

$$S = S(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n;$$

– обозначение для веса Хэмминга двоичного вектора $\mathbf{x}$:

$$wt(x) = \big|\{i \mid x_i = 1\}\big|;$$

– обозначение для подстановки inv, которая переставляет в обратном порядке элементы на входе:

$$\mathsf{inv}((x_1, \ldots, x_\ell)) = (x_\ell, \ldots, x_1).$$

Покажем, что семейство $\mathcal{F}_n$ из раздела 1.3.3 имеет максимально возможную (для правильного булева семейства) мощность образа, а именно, $|\mathsf{Im}(\mathcal{F}_n)| = 2^{n-1}$.

Доказательству предпошлем несколько технических лемм.

Лемма 14. *Пусть через $\mathcal{F}_n$ обозначено семейство (1.5). Проекция семейства $\mathcal{F}_n$ на любую из его координат не меняет вида семейства. Более точно, результат операции взятия проекции на уровнях 0 и 1 устроен следующим образом:*

$$\Pi_i^0(\mathcal{F}_n) = \mathcal{F}_{n-1}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n),$$
$$\Pi_i^1(\mathcal{F}_n) = \mathsf{inv}(\mathcal{F}_{n-1})(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \oplus (\underbrace{0, \ldots, 0}_{i-1}, \underbrace{1, \ldots, 1}_{n-i}).$$

Доказательство. Доказательство осуществляется прямой подстановкой $x_i \leftarrow 0$ и $x_i \leftarrow 1$ в каждую из функций семейства $\mathcal{F}_n$ и последующим сокращением совпадающих членов. Так, подстановка $x_i \leftarrow 0$ не меняет вида семейства: все члены вида $x_i x_j$, $j \in \{1, \ldots, n\}$, $j \neq i$, обнуляются, из линейной части убирается член x_i. При подстановке $x_i \leftarrow 1$ для функций $\mathcal{F}_n[j]$ с $j > i$ в линейной части добавляется член $\oplus 1$. Кроме того, некоторые квадратичные слагаемые вырождаются в линейные, что приводит к следующему изменению линейной части:

$$x_1 \oplus \ldots \oplus x_{j-1} \to$$
$$\to x_1 \oplus \ldots \oplus x_{j-1} \oplus x_1 \oplus \ldots \oplus x_{j-1} \oplus x_{j+1} \oplus \ldots \oplus x_n,$$

что соответствует рассмотрению семейства $\mathsf{inv}(\mathcal{F}_{n-1}(\mathsf{inv}(\mathbf{x})))$. □

Лемма 15. *Пусть через $\mathcal{F}_n$ обозначено семейство (1.5). Справедливо равенство*

$$\mathcal{F}_n(x_1, \ldots, x_{i-1}, x_i \oplus 1, x_{i+1}, \ldots, x_n) =$$
$$= \mathcal{F}_n(x_1, \ldots, x_n) \oplus \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \oplus \begin{bmatrix} S \oplus x_1 \oplus x_i \\ \vdots \\ S \oplus x_{i-1} \oplus x_i \\ 0 \\ S \oplus x_{i+1} \oplus x_i \\ \vdots \\ S \oplus x_n \oplus x_i \end{bmatrix}.$$

Доказательство. Доказывается прямой проверкой: при замене $x_i \to x_i \oplus 1$ для $\mathcal{F}_n[j]$, $j > i$ в линейной части появляется дополнительное слагаемое $\oplus 1$, в квадратичной части каждой функции (кроме $\mathcal{F}_n[i]$) изменяется произведение вида:

$$x_i \cdot (S \oplus x_i \oplus x_j) \to (x_i \oplus 1) \cdot (S \oplus 1 \oplus x_i \oplus 1 \oplus x_j) =$$

$$= x_i \cdot (S \oplus x_i \oplus x_j) \oplus S \oplus x_i \oplus x_j.$$

Функция $\mathcal{F}_n[i]$ не изменяется, так как $\mathcal{F}_n[i]$ зависит от x_i фиктивно. □

Лемма 16. *Пусть через $\mathcal{F}_n$ обозначено семейство (1.5). Справедливо равенство*

$$\mathcal{F}_n(x_1 \oplus 1, \ldots, x_n \oplus 1) = \mathcal{F}_n(x_1, \ldots, x_n) \oplus \\ \oplus \begin{bmatrix} \left(n + \frac{n(n+1)}{2}\right) \bmod 2 \\ \left(n - 1 + \frac{n(n+1)}{2}\right) \bmod 2 \\ \left(n - 2 + \frac{n(n+1)}{2}\right) \bmod 2 \\ \vdots \\ \left(1 + \frac{n(n+1)}{2}\right) \bmod 2 \end{bmatrix} \oplus (n \bmod 2) \cdot \begin{bmatrix} S \oplus x_1 \\ S \oplus x_2 \\ S \oplus x_3 \\ \vdots \\ S \oplus x_n \end{bmatrix}.$$

Доказательство. Доказываем путем последовательного применения леммы 15. На первом шаге имеем:

$$\mathcal{F}_n(x_1 \oplus 1, \ldots, x_n \oplus 1) = \mathcal{F}_n(x_1, x_2 \oplus 1, \ldots, x_n \oplus 1) \oplus \\ \oplus \begin{bmatrix} 0 \\ S(x_1, x_2 \oplus 1, \ldots, x_n \oplus 1) \oplus x_2 \oplus 1 \\ S(x_1, x_2 \oplus 1, \ldots, x_n \oplus 1) \oplus x_3 \oplus 1 \\ \vdots \\ S(x_1, x_2 \oplus 1, \ldots, x_n \oplus 1) \oplus x_n \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ x_1 \\ x_1 \\ \vdots \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} =$$

$$= \mathcal{F}_n(x_1, x_2 \oplus 1, \ldots, x_n \oplus 1) \oplus \begin{bmatrix} 0 \\ S \oplus x_2 \\ S \oplus x_3 \\ \vdots \\ S \oplus x_n \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ n+1 \\ n+1 \\ \vdots \\ n+1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ x_1 \\ x_1 \\ \vdots \\ x_1 \end{bmatrix} =$$

$$= \mathcal{F}_n(x_1, x_2 \oplus 1, \ldots, x_n \oplus 1) \oplus \begin{bmatrix} 0 \\ S \oplus x_2 \\ S \oplus x_3 \\ \vdots \\ S \oplus x_n \end{bmatrix} \oplus \begin{bmatrix} 0 \\ n \\ n \\ \vdots \\ n \end{bmatrix} \oplus \begin{bmatrix} 0 \\ x_1 \\ x_1 \\ \vdots \\ x_1 \end{bmatrix}.$$

Аналогично, при ℓ-м применении леммы 15, имеем:

$$\mathcal{F}_n(x_1, x_2, \ldots, x_{\ell-1}, x_\ell \oplus 1, \ldots, x_n \oplus 1) = \\ = \mathcal{F}_n(x_1, x_2, \ldots, x_\ell, x_{\ell+1} \oplus 1, \ldots, x_n \oplus 1) \oplus$$

$$\oplus \begin{bmatrix} S(x_1, \ldots, x_\ell, x_{\ell+1} \oplus 1, \ldots, x_n \oplus 1) \oplus x_1 \\ \vdots \\ S(x_1, \ldots, x_\ell, x_{\ell+1} \oplus 1, \ldots, x_n \oplus 1) \oplus x_{\ell-1} \\ 0 \\ S(x_1, \ldots, x_\ell, x_{\ell+1} \oplus 1, \ldots, x_n \oplus 1) \oplus x_{\ell+1} \oplus 1 \\ \vdots \\ S(x_1, \ldots, x_\ell, x_{\ell+1} \oplus 1, \ldots, x_n \oplus 1) \oplus x_n \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \oplus \begin{bmatrix} x_\ell \\ \vdots \\ x_\ell \\ 0 \\ x_\ell \\ \vdots \\ x_\ell \end{bmatrix} =$$

$$= \mathcal{F}_n(x_1, x_2, \ldots, x_\ell, x_{\ell+1} \oplus 1, \ldots, x_n \oplus 1) \oplus \begin{bmatrix} S \oplus x_1 \\ \vdots \\ S \oplus x_{\ell-1} \\ 0 \\ S \oplus x_{\ell+1} \\ \vdots \\ S \oplus x_n \end{bmatrix} \oplus \begin{bmatrix} n-\ell+1 \\ \vdots \\ n-\ell+1 \\ 0 \\ n-\ell+1 \\ \vdots \\ n-\ell+1 \end{bmatrix} \oplus \begin{bmatrix} x_\ell \\ \vdots \\ x_\ell \\ 0 \\ x_\ell \\ \vdots \\ x_\ell \end{bmatrix}.$$

Учитывая все полученные равенства, приходим к утверждению леммы. □

Лемма 17. *Пусть через $\mathcal{F}_n$ обозначено семейство (1.5). Пусть $\mathbf{x} \neq \mathbf{y}$, $\mathbf{x}, \mathbf{y} \in \mathbb{E}_2^n$, $\mathcal{F}_n(\mathbf{x}) = \mathcal{F}_n(\mathbf{y})$, тогда*

$$|wt(\mathbf{x}) - wt(\mathbf{y})| = 1.$$

Доказательство. Допустим, что среди координат $\mathbf{x}$ и $\mathbf{y}$ есть ровно $(n-m)$ попарно совпадающих:

$$x_{i_1} = y_{i_1} = a_1, \ldots, x_{i_{n-m}} = y_{i_{n-m}} = a_{n-m}.$$

Тогда подставим все такие координаты и перейдем к семейству:

$$\mathcal{G}_m = \Pi_{i_1}^{a_1}\big(\ldots (\Pi_{i_{n-m}}^{a_{n-m}}(\mathcal{F}_n)) \ldots \big).$$

По лемме 14, семейство $\mathcal{G}_m$ имеет тот же вид, что и исходное семейство $\mathcal{F}_n$, а именно, путем перестановки координат можно свести уравнение

$$\mathcal{G}_m(t_1, \ldots, t_m) = \alpha$$

к уравнению

$$\mathcal{F}_m(s_1, \ldots, s_m) = \alpha'.$$

Поскольку мы на первом шаге подставили все совпадающие координаты, все оставшиеся координаты являются попарно несовпадающими, и мы получаем уравнение вида:

$$\mathcal{F}_m(s_1, \ldots, s_m) = \mathcal{F}_m(s_1 \oplus 1, \ldots, s_m \oplus 1) = \alpha'.$$

Применим лемму 16 к значению $\mathcal{F}_m(s_1 \oplus 1, \ldots, s_m \oplus 1)$ и рассмотрим возможные значения числа m по модулю 2 и модулю 4.

$$\mathcal{F}_m(s_1 \oplus 1, \ldots, s_m \oplus 1) =$$
$$= \mathcal{F}_m(s_1, \ldots, s_m) \oplus \begin{bmatrix} \left(m + \frac{m(m+1)}{2}\right) \bmod 2 \\ \left(m - 1 + \frac{m(m+1)}{2}\right) \bmod 2 \\ \vdots \\ \left(1 + \frac{m(m+1)}{2}\right) \bmod 2 \end{bmatrix} \oplus (m \bmod 2) \cdot \begin{bmatrix} S \oplus s_1 \\ S \oplus s_2 \\ \vdots \\ S \oplus s_m \end{bmatrix}.$$

Рассмотрим следующие случаи.

1. Случай $m \equiv 0 \bmod 4$: в таком случае мы получаем тождество вида

   $$(0, 0, \ldots, 0, 0) = (0, 1, \ldots, 0, 1),$$

   которое может выполняться только при $m = 1$, что противоречит условию.
2. Случай $m \equiv 1 \bmod 4$: в таком случае мы получаем систему уравнений

   $$S \oplus s_i = i \bmod 2,\ 1 \leqslant i \leqslant m,$$

   решениями которой являются наборы

   $$\mathbf{v} = (0, 1, \ldots, 0, 1, 0),\ \mathbf{w} = (1, 0, \ldots, 1, 0, 1),$$

   вес которых различается на 1.
3. Случай $m \equiv 2 \bmod 4$: в таком случае мы получаем тождество вида

   $$(0, 0, \ldots, 0, 0) = (1, 0, \ldots, 1, 0),$$

   которое не может выполняться ни при каких значениях m.

4. Случай $m \equiv 3 \bmod 4$: в таком случае мы получаем систему уравнений

$$S \oplus s_i = (i+1) \bmod 2,\ 1 \leqslant i \leqslant m,$$

решениями которой являются наборы

$$\mathbf{v} = (0,1,\ldots,0,1,0),\ \mathbf{w} = (1,0,\ldots,1,0,1),$$

вес которых различается на 1.

Таким образом, мы показали, что если существуют наборы $\mathbf{x}$, $\mathbf{y}$, для которых выполнено равенство $\mathcal{F}_n(\mathbf{x}) = \mathcal{F}_n(\mathbf{y})$, то их вес различается ровно на 1. □

Докажем теперь следующую теорему.

Теорема 21. *Пусть через $\mathcal{F}_n$ обозначено семейство (1.5). Справедливо следующее равенство:*

$$|\mathsf{Im}(\mathcal{F}_n)| = 2^{n-1}.$$

Доказательство. Из леммы 17 следует, что для каждого набора $\mathbf{y} \in \mathbb{E}_2^n$ может быть не более двух прообразов при отображении $\mathbf{x} \to \mathcal{F}_n(\mathbf{x})$. Если мы предположим, что найдутся хотя бы три набора $\mathbf{x}, \mathbf{y}, \mathbf{v} \in \mathbb{E}_2^n$ такие, что попарные разности их весов различаются ровно на 1, то придем к противоречию: пусть без ограничения общности $wt(\mathbf{x}) > wt(\mathbf{y})$, тогда $wt(\mathbf{y}) = wt(\mathbf{x}) - 1$, но при этом должны выполняться два равенства:

$$|wt(\mathbf{x}) - wt(\mathbf{v})| = 1, \quad |wt(\mathbf{y}) - wt(\mathbf{v})| = |wt(\mathbf{x}) - wt(\mathbf{v}) - 1| = 1,$$

что невозможно. Отсюда и из принципа Дирихле следует, что

$$|\mathsf{Im}(\mathcal{F}_n)| \geqslant 2^{n-1}.$$

С другой стороны, для каждого булева правильного семейства из утверждения 29 следует, что

$$|\mathsf{Im}(\mathcal{F}_n)| \leqslant 2^{n-1}.$$

Следовательно, $|\mathsf{Im}(\mathcal{F}_n)| = 2^{n-1}$. □

Рассмотрим теперь семейство (1.4) из замечания 17, обозначим его через $\mathcal{F}_n$. Напомним, что числами Люка Lucas_n (см., например, [159, Глава 1]) называется рекуррентная последовательность, заданная соотношением:

$$\mathsf{Lucas}_n = \mathsf{Lucas}_{n-1} + \mathsf{Lucas}_{n-2}, \quad \mathsf{Lucas}_0 = 2, \mathsf{Lucas}_1 = 1.$$

Нам понадобится следующее свойство чисел Люка ([159, Глава 3]):

$$\mathsf{Lucas}_n = \mathsf{Fib}_{n-1} + \mathsf{Fib}_{n+1},$$

где Fib_n — число Фибоначчи с индексом n.

Теорема 22. *Справедливо следующее равенство:*

$$|\mathsf{Im}(\mathcal{F}_n)| = \mathsf{Lucas}_n,$$

где через $\mathcal{F}_n$ обозначено семейство (1.4).

Доказательство. Рассмотрим множество A_n всех двоичных строк длины n со следующим ограничением: никакие два соседних бита строки $\alpha \in A_n$ или какого-либо ее циклического сдвига не равны одновременно 1. Доказательство утверждения состоит в проверке двух условий:

– уравнение $\mathcal{F}_n(\mathbf{x}) = \alpha$ имеет решение тогда и только тогда, когда $\alpha \in A_n$;
– множество строк A_n имеет мощность Lucas_n.

Рассмотрим подробнее первое условие. Мы рассматриваем систему уравнений

$$x_{i+1} \cdot \bar{x}_{i+2} = \alpha_i,$$

индексы «зациклены» (после индекса n идет индекс 1). Для всех таких индексов i, что $\alpha_i = 1$, положим $x_{i+1} := 1$, $x_{i+2} := 0$. Оставшиеся x_j также положим равными нулю. В таком случае мы получим $\mathcal{F}_n(\mathbf{x}) = \alpha$. Условие на биты строки α используется для того, чтобы получить согласованное присваивание значений битам (исключается ситуация, когда некоторое x_j должно быть равно 1 и 0 одновременно). Заметим также, что других решений нет: если в наборе α есть два соседних бита $\alpha_i = \alpha_{i+1} = 1$, то α не лежит в $\mathsf{Im}(\mathcal{F}_n)$, поскольку для «соседних» функций из семейства $\mathcal{F}_n$ выполняется условие $f_i(\mathbf{x}) \cdot f_{i+1}(\mathbf{x}) \equiv 0$.

Рассмотрим второе условие. Возьмем некоторую строку $\alpha \in A_n$. Если $\alpha_1 = 0$, то необходимым и достаточным условием для $\alpha \in A_n$ будет отсутствие подстроки «11» в строке $(\alpha_2, \ldots, \alpha_n)$. Если $\alpha_1 = 1$, то $\alpha_2 = \alpha_n = 0$, и необходимым и достаточным условием будет отсутствие подстроки «11» в строке $(\alpha_3, \ldots, \alpha_{n-1})$. Таким образом, $|A_n| = |B_{n-1}| + |B_{n-3}|$, где B_n — множество двоичных строк длины n, не содержащих подстроку «11». Хорошо известно (см., например, [136, Раздел 1.5]), что число элементов $|B_n| = \mathsf{Fib}_{n+2}$. В таком случае

$$|A_n| = \mathsf{Fib}_{n+1} + \mathsf{Fib}_{n-1} = \mathsf{Lucas}_n,$$

что и требовалось доказать. □

Следствие 3. *Для* $|\mathsf{Im}(\mathcal{F}_n)|$ *верна формула:*

$$|\mathsf{Im}(\mathcal{F}_n)| = \lfloor \varphi^n \rceil,$$

где $\mathcal{F}_n$ *— семейство (1.4),* $\varphi = \frac{1+\sqrt{5}}{2}$ *— пропорция золотого сечения, а* $\lfloor \cdot \rceil$ *— операция взятия ближайшего целого числа.*

3.3 О группе подстановок, порождаемых правильными семействами

В настоящем разделе мы будем рассматривать свойства множества подстановок $\mathcal{S}^{\mathsf{prop}}$, порожденных правильными семействами функций $\mathcal{F}$.

Определение 62. Пусть $\mathcal{F}_n$ — правильное семейство размера n на Q^n, где $(Q, \circ)$ — квазигруппа. Рассмотрим отображение:

$$\sigma_{\mathcal{F}}(\mathbf{x})\colon \mathbf{x} \to \mathbf{x} \circ \mathcal{F}(\mathbf{x}), \quad \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \to \begin{bmatrix} x_1 \circ f_1(\mathbf{x}) \\ \vdots \\ x_n \circ f_n(\mathbf{x}) \end{bmatrix}.$$

Это отображение является подстановкой на множестве Q^n (см. теорему 18): $\sigma_{\mathcal{F}} \in \mathcal{S}_{Q^n}$. Будем через $\mathcal{S}^{\mathsf{prop}}$ обозначать множество таких подстановок $\sigma \in \mathcal{S}_{Q^n}$, что отображение $\mathcal{F}_n$ вида

$$\mathcal{F}_n(\mathbf{x}) = L_{\mathbf{x}}^{-1}\left(\sigma(\mathbf{x})\right) = \begin{bmatrix} L_{x_1}^{-1}(\sigma_1(\mathbf{x})) \\ \vdots \\ L_{x_n}^{-1}(\sigma_n(\mathbf{x})) \end{bmatrix},$$

где $L_x(y) = x \circ y$, является правильным на Q^n.

3.3.1 Замкнутость относительно инверсии подстановки

Пусть $\sigma \in \mathcal{S}^{\mathsf{prop}}$ — подстановка, порожденная некоторым правильным семейством $\mathcal{F}$ на Q^n. Покажем, что если Q является группой, то $\sigma \in \mathcal{S}^{\mathsf{prop}}$ тогда и только тогда, когда $\sigma^{-1} \in \mathcal{S}^{\mathsf{prop}}$. Другими словами, $\mathcal{S}^{\mathsf{prop}}$ замкнуто относительно взятия обратного элемента (в случае, когда $Q = G$ — группа).

Теорема 23. *Пусть $\mathcal{F}$ — правильное семейство на G^n, $(G, \cdot)$ — группа. Рассмотрим дуальное к семейству $\mathcal{F}$ семейство $\mathcal{G}$, соответствующее подстановке σ^{-1}:*

$$\mathcal{G}\colon Q^n \to Q^n, \quad \mathcal{G}(\mathbf{x}) = \mathbf{x} \cdot \sigma^{-1}(\mathbf{x}).$$

Тогда $\mathcal{G}(\mathbf{x})$ также является правильным на Q^n.

Доказательство. Необходимо доказать, что для любых наборов $\mathbf{x} \neq \mathbf{y}$, $\mathbf{x}, \mathbf{y} \in G^n$ существует такой индекс i, что $x_i \neq y_i$, но $\mathcal{G}(\mathbf{x})[i] = \mathcal{G}(\mathbf{y})[i]$. Возьмем два набора $\mathbf{x}, \mathbf{y} \in Q^n$, $\mathbf{x} \neq \mathbf{y}$. Поскольку $\sigma_{\mathcal{F}}$ является подстановкой, то найдутся $\mathbf{v}, \mathbf{w} \in G^n$ такие, что

$$\mathbf{x} = \sigma_{\mathcal{F}}(\mathbf{v}) = \mathbf{v} \cdot \mathcal{F}(\mathbf{v}), \mathbf{y} = \sigma_{\mathcal{F}}(\mathbf{w}) = \mathbf{w} \cdot \mathcal{F}(\mathbf{w}).$$

Из условия $\mathbf{x} \neq \mathbf{y}$ следует неравенство $\mathbf{v} \neq \mathbf{w}$, а значит, по свойству правильности семейства $\mathcal{F}$ найдется такой индекс i, что $v_i \neq w_i$, но $\mathcal{F}(\mathbf{v})[i] = \mathcal{F}(\mathbf{w})[i]$. В таком случае

$$x_i = v_i \cdot f_i(\mathbf{v}) \neq y_i = w_i \cdot f_i(\mathbf{w}).$$

Поскольку $\sigma_{\mathcal{F}}(\mathbf{u}) = \mathbf{u} \cdot \mathcal{F}(\mathbf{u})$, то по определению семейства $\mathcal{G}$, имеем:

$$\mathbf{u} = \sigma_{\mathcal{F}}^{-1}(\mathbf{u} \cdot \mathcal{F}(\mathbf{u})) = (\mathbf{u} \cdot \mathcal{F}(\mathbf{u})) \cdot \mathcal{G}(\mathbf{u} \cdot \mathcal{F}(uu)),$$

откуда следует уравнение на $\mathcal{G}$:

$$\mathcal{G}(\mathbf{u} \cdot \mathcal{F}(\mathbf{u})) = \mathcal{F}(\mathbf{u})^{-1},$$

где через $\mathcal{F}(t)^{-1}$ обозначен обратный элемент к $\mathcal{F}(t)$ в группе G^n. Подставим вместо $\mathbf{u}$ значения $\mathbf{v}$ и $\mathbf{w}$ и рассмотрим i-ю координату полученного вектора:

$$g_i(\mathbf{x}) = g_i(\mathbf{v} \cdot \mathcal{F}(\mathbf{v})) = f_i(\mathbf{v})^{-1} = f_i(\mathbf{w})^{-1} = g_i(\mathbf{w} \cdot \mathcal{F}(\mathbf{w})) = g_i(\mathbf{y}),$$

что и требовалось доказать. □

Замечание 41. При доказательстве утверждения мы пользовались ассоциативностью операции $(\cdot)$ на множестве $Q^n = G^n$; в общем случае из уравнения

$$\mathbf{u} = (\mathbf{u} \circ \mathcal{F}(\mathbf{u})) \circ \mathcal{G}(\mathbf{u} \circ \mathcal{F}(\mathbf{u}))$$

не следует, что $G(\mathbf{u} \circ \mathcal{F}(\mathbf{u})) = inv(\mathcal{F}(\mathbf{u}))$, где через $inv(\mathcal{F}(\mathbf{u}))$ обозначен *левый обратный* к элементу $\mathcal{F}(\mathbf{u})$, через $\circ$ — некоторая бинарная операция.

3.3.2 Неподвижные точки

Покажем, что подстановки $\pi_{\mathcal{F}} \in \mathcal{S}^{\mathsf{prop}}$ для булевых правильных семейств $\mathcal{F}$ всегда имеют четкое число неподвижных точек. Для этого докажем более общее утверждение относительно преобразований вида $\mathbf{x} \to x \oplus \Phi(\mathcal{F}(\mathbf{x}))$.

Теорема 24. *Пусть $\mathcal{F}_n$ — правильное семейство на $\mathbb{Z}_2^n$. Отображение на множестве $\mathbb{Z}_2^n$, задаваемое формулой*

$$\mathbf{x} \to \mathbf{x} \oplus \Phi(\mathcal{F}_n(\mathbf{x})),$$
$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \to \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \oplus \Phi \left(\begin{bmatrix} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_n(x_1, \ldots, x_n) \end{bmatrix} \right),$$

где Φ — произвольное отображение вида $\Phi\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, имеет четное число неподвижных точек.

Доказательство. Неподвижные точки указанного отображения удовлетворяют уравнению

$$\mathbf{x} = \mathbf{x} \oplus \Phi(\mathcal{F}_n(\mathbf{x})),$$

следовательно $\mathbf{x}$ — неподвижная точка тогда и только тогда, когда $\mathcal{F}(\mathbf{x}) \in \Phi^{-1}(0^n)$. Для каждой точки α, попавшей в указанный прообраз, по теореме 20 имеется четное число решений уравнения $\mathcal{F}(\mathbf{x}) = \alpha$. □

Замечание 42. Теорема 24 выполняется не только для $\mathbb{Z}_2^n$, но и для любой лупы Q^n, где $|Q| = 2$.

3.3.3 Транзитивность

Покажем, что замыкание множества $\mathcal{S}^{\mathsf{prop}}$ действует транзитивно на множестве Q^n, т.е. для любых $\alpha, \beta \in Q^n$ существует такой набор правильных семейств $\mathcal{F}_1, \ldots, \mathcal{F}_n$, что

$$\beta = \pi_{\mathcal{F}_n} \left(\ldots \pi_{\mathcal{F}_1} (\alpha) \ldots \right).$$

Теорема 25. *Пусть Q — квазигруппа. Рассмотрим множество подстановок $\mathcal{S}^{\mathsf{prop}}$, порождаемых правильными семействами функций на Q^n. Тогда замыкание множества подстановок $\langle \mathcal{S}^{\mathsf{prop}} \rangle$ действует транзитивно на Q^n.*

Доказательство. Пусть α, β — элементы Q^n на расстоянии Хэмминга 1 друг от друга (т.е. $\exists i \colon \alpha_i \neq \beta_i$, и $\alpha_j = \beta_j$, $j \neq i$). Покажем, что элемент α может быть переведен некоторой подстановкой $\sigma_{\mathcal{F}} \in \mathcal{S}^{\mathsf{prop}}$ в элемент β. Рассмотрим такой элемент c, что $\alpha_i \circ c = \beta_i$, а также элементы e_j, $j \neq i$, такие что $\alpha_j \circ e_j = \alpha_j$. Зададим следующее треугольное семейство $\mathcal{F}_n$:

$$\mathcal{F}_n = \begin{bmatrix} e_1 \\ \vdots \\ e_{i-1} \\ f(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \\ e_{i+1} \\ \vdots \\ e_n \end{bmatrix},$$

где $f(\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n) = c$, для всех остальных наборов f задана произвольным образом. В таком случае мы имеем:

$$\sigma_{\mathcal{F}}(\alpha) = \alpha \circ \mathcal{F}(\alpha) = \begin{bmatrix} \alpha_1 \circ e_1 \\ \vdots \\ \alpha_{i-1} \circ e_{i-1} \\ \alpha_i \circ c \\ \alpha_{i+1} \circ e_{i+1} \\ \vdots \\ \alpha_n \circ e_n \end{bmatrix} = \beta,$$

следовательно, $\sigma_{\mathcal{F}}(\alpha) = \beta$. Перевод элемента α в β, находящие на расстоянии Хэмминга более 1, проводится последовательными сдвигами. □

Замечание 43. Для $Q^n = \mathbb{E}_2^n$ выполнено равенство $\langle \mathcal{S}^{\mathsf{prop}} \rangle = \mathcal{S}_{\mathbb{E}_2^n}$.

Выводы

В настоящей главе были рассмотрены некоторые свойства правильных семейств.

1. Доказано, что пары отображений, сохраняющие множество правильных семейств, являются согласованными изометриями соответствующего пространства Хэмминга.
2. Доказано, что для булевых правильных семейств прообраз любой точки имеет четную мощность.
3. Подсчитаны мощности образов отображений, задаваемых некоторыми правильными булевыми семействами.
4. Показано, что множество «правильных подстановок» замкнуто относительно операции обращения подстановки (для семейств над прямыми произведениями групп), замыкание множества «правильных подстановок» действует транзитивно на множестве Q^n, в случае $Q = \mathbb{E}_2$ было показано, что «правильные подстановки» имеют четное число неподвижных точек.

Глава 4. Алгоритмические и вычислительные аспекты

В настоящей главе рассматриваются некоторые прикладные вопросы, связанные с правильными семействами:

– в разделе 4.1 предлагается к рассмотрению один алгоритм шифрования, сохраняющего формат, основанный на сдвиговых преобразованиях в квазигруппах, порожденных правильными семействами булевых функций;
– раздел 4.2 посвящен рассмотрению одного улучшения «наивного» алгоритма распознавания правильности;
– в разделе 4.3 приведены результаты численных экспериментов (количество булевых правильных семейств в некоторых классах, число ассоциативных троек).

Результаты главы ранее были опубликованы в [75; 80; 81].

4.1 Шифрование, сохраняющее формат

Шифрование, сохраняющее формат (FPE, Format preserving encryption [160], далее FPE-схема) — алгоритм, позволяющий зашифровывать сообщения из произвольного конечного множества $\mathbf{Dom}$ таким образом, что результат зашифрования также лежит в множестве $\mathbf{Dom}$. Такой тип алгоритмов довольно востребован на практике, о чем свидетельствует большое количество статей и предложений, рассматривающих стойкость таких криптомеханизмов (см., например, [160—162]). При этом подобные алгоритмы часто подвергаются специфическим атакам, связанным, в том числе, и с возможным относительно малым размером области определения (см., например, [163; 164]). Известны «доказуемо стойкие» (о теоретико-сложностных сведениях/«доказуемой стойкости» см., например, [165]) алгоритмы как для очень малых ($|\mathbf{Dom}| \approx 2^{10}$), так и для очень больших областей определения (размер которых приближается к размеру области определения стандартных блочных шифров, либо превышает их, см. т.н. wide-block encryption), в то время как для «средних» областей определения всё ещё не существует одного предпочтительного подхода. В этом разделе мы

рассмотрим один возможный подход к построению FPE-схем, основанный на квазигрупповых операциях.

4.1.1 Общее описание FPE-схем

FPE-схемы позволяют зашифровывать тексты с заданным форматом (например, 6 десятичных цифр, номер кредитной карты, СНИЛС и так далее) таким образом, чтобы зашифрованное сообщение имело бы тот же формат, что и исходное. Указанное свойство желательно, например, при шифровании баз данных, где поля записей имеют строго предписанный формат. Формализация данного требования выглядит следующим образом.

Определение 63. FPE-схема — это тройка (вероятностных) алгоритмов $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$:

- (вероятностный) алгоритм генерации ключа Gen: на вход принимает пустую строку и возвращает ключ $K \in \mathbf{Keys}$;
- (детерминированный) алгоритм зашифрования Enc: на вход принимает ключ K, параметр-настройку $t \in \mathbf{Twk}$ и сообщение $m \in \mathbf{Dom}$ и возвращает шифртекст $ct \in \mathbf{Dom}$:

$$\mathsf{Enc} : \mathbf{Keys} \times \mathbf{Twk} \times \mathbf{Dom} \to \mathbf{Dom};$$

- (детерминированный) алгоритм расшифрования Dec: на вход принимает ключ K, параметр-настройку $t \in \mathbf{Twk}$ и шифртекст $ct \in \mathbf{Dom}$ и возвращает открытый текст-сообщение $m \in \mathbf{Dom}$:

$$\mathsf{Dec} : \mathbf{Keys} \times \mathbf{Twk} \times \mathbf{Dom} \to \mathbf{Dom}.$$

Для указанной тройки алгоритмов должно выполняться требование корректности расшифрования: для любого ключа K, порождаемого алгоритмом Gen и любых $t \in \mathbf{Twk}$, $m \in \mathbf{Dom}$ выполнено равенство

$$\mathsf{Dec}_K^t(\mathsf{Enc}_K^t(m)) = m.$$

Замечание 44. Чаще всего алгоритм Gen порождает равномерное распределение на множестве всех двоичных наборов длины $klen$. Далее мы будем опускать обозначение Gen и предполагать, что ключ выбирается случайно равновероятно из множества $\{0,1\}^{klen}$: $K \xleftarrow{\mathcal{U}} \{0,1\}^{klen}$.

Замечание 45. Введение дополнительного параметра-настройки $t \in \mathbf{Twk}$ обусловлено тем, что область определения $\mathbf{Dom}$ может быть слишком маленькой, что приведет к возможности атаки по словарю/кодовой книге, в ходе которой противник получает шифртексты для всех возможных сообщений $m \in \mathbf{Dom}$ и может далее осуществлять бесключевое чтение.

Замечание 46. Множество $\mathbf{Dom}$ может быть устроено нестандартно. К примеру, если необходимо шифровать номера банковских карточек, то на множество $\mathbf{Dom}$ налагаются следующие ограничения:

- формат номера — 16 десятичных цифр;
- первые 6 цифр кодируют ID банка, выдавшего карточку (для многих приложений они должны храниться в открытом виде);
- последняя цифра является контрольной суммой и не должна зашифровываться.

Таким образом, необходимо зашифровывать 9 средних цифр в номере карточки, в этом случае мы имеем:

$$\mathbf{Dom} = \{0, \ldots 9\}^9, \quad |\mathbf{Dom}| \approx 2^{30}.$$

«Обычный» блочный шифр действует на множестве двоичных строк фиксированной длины (например, $\mathbf{Dom} = \{0,1\}^{128}$ для алгоритма «Кузнечик», см. [166]), и результат шифрования элемента $m \in \mathbf{Dom}$ может оказаться вне требуемого множества: $\mathsf{Enc}_K^t(m) \notin \mathbf{Dom}$. В связи с этим актуальна задача разработки алгоритма, который по ключу K и параметру t порождал бы некоторую подстановку $\mathsf{Enc}_K^t \in \mathcal{S}_{\mathbf{Dom}}$ со следующими желательными свойствами:

- операции Enc_K^t, Dec_K^t быстро вычислимы;
- при случайном выборе ключа $K \xleftarrow{\mathcal{U}} \mathsf{Gen}$ получаемое отображение $\mathsf{Enc}_K^t(\cdot)$ вычислительно неотличимо (более подробно о понятии вычислительной неотличимости см. [165]) от случайной подстановки $\pi \xleftarrow{\mathcal{U}} \mathcal{S}_{\mathbf{Dom}}$;
- вероятность успешной атаки схемы мала даже для малых ($|\mathbf{Dom}| \approx 2^{20}$ и менее) областей определения.

4.1.2 Подход на основе квазигрупп

В работе [75] был предложен подход на основе квазигрупповых операций сдвига. В качестве базовой сложной задачи предлагается рассматривать задачу различения случайной подстановки от структурированной: пусть дана некоторая квазигруппа Q, и мы хотим измерить, насколько композиция квазигрупповых операций (например, серия умножений слева на случайные элементы квазигруппы) похожа на случайную подстановку на множестве Q.

Базовая задача

Задачи изучения неотличимости случайной подстановки от структурированной в несколько неформальном модельном описании может быть представлена следующим образом (больше о теоретико-сложностных сведениях в контексте изучения криптографических механизмов и протоколов можно посмотреть, например, в [165]).

1. Противник $\mathcal{A}$ (вероятностный алгоритм) взаимодействует с оракулом $\mathcal{O}$, реализующим некоторую функцию f. Перед началом взаимодействия оракул «подбрасывает монетку» (выбирает случайно равновероятно бит $b \leftarrow^{\mathcal{U}} \{0,1\}$).
   - если бит $b = 0$, оракул выбирает случайную подстановку $\pi \leftarrow^{\mathcal{U}} \mathcal{S}_Q$ на множестве Q, и при дальнейших запросах к нему от противника $\mathcal{A}$ вычисляет функцию f по правилу $f(x) = \pi(x)$;
   - если бит $b = 1$, оракул выбирает λ случайных элементов $q_i \leftarrow^{\mathcal{U}} Q$, $i = 1, \ldots, \lambda$ и при дальнейших запросах к нему от противника $\mathcal{A}$ вычисляет функцию f по правилу

$$f(x) = L_{q_1}\left(L_{q_2}\left(\ldots L_{q_\lambda}(x)\ldots\right)\right). \tag{4.1}$$

2. На запросы x противника $\mathcal{A}$ оракул $\mathcal{O}$ возвращает ответ $f(x)$.
3. Изучая ответы оракула, противник должен понять, какой бит был выбран оракулом до начала взаимодействия, то есть по какому правилу оракул вычисляет функцию f.

Параметрами рассматриваемой модели, от которых зависит успешность угадывания противником секретного значения b являются «количество запросов к оракулу» и «время работы противника» (количество тактов вычислений). Если противник может с высокой вероятностью и низкой затратой рассматриваемых ресурсов правильно угадывать значение бита b, то он способен отличать истинно случайную подстановку $\pi \in \mathcal{S}_Q$ от «структурированной»

$$f(x) = L_{q_1}\left(L_{q_2}\left(\ldots L_{q_\lambda}(x)\ldots\right)\right).$$

Вероятность успеха противника зависит от структуры используемой квазигруппы. Так, например, если рассмотреть в качестве базовой квазигруппу $(Q, \circ) = (\mathbb{Z}_{2^n}, +)$, то полученная структурированная подстановка будет тривиально отличима от случайной, поскольку в таком случае «левым умножением» является сложение поданного на вход элемента со случайными элементами $L_q(x) = q + x$, и полученное преобразование будет аффинным; в частности, с вероятностью 1 будет выполнено равенство:

$$f(x + y) - f(x) = y,$$

что позволит легко отличить его от случайной подстановки.

В контексте рассматриваемой FPE-схемы можно выделить следующие важные свойства квазигруппы, которые могут потенциально усложнять криптоанализ, а значит, делать схему более стойкой (отметим также, что выделенные свойства упоминаются, например, в [13] как необходимые при использовании квазигрупп в криптографических механизмах).

1. Малый индекс ассоциативности квазигруппы Q (см. раздел 1.4.1): если в квазигруппе Q большое количество ассоциативных троек, то в операции (4.1) реальное количество элементов, на которых умножается m, может быть сильно меньше, чем λ.
2. Полиномиальная полнота квазигруппы Q (см. раздел 1.4.2): свидетельством в пользу того, что рассматриваемая задача может быть сложной, является NP-полнота задачи проверки разрешимости уравнений над полиномиально полной квазигруппой общего вида. Тем не менее, такое наблюдение может давать теоретические гарантии лишь в «худшем» случае, ничего не говоря о «генерической» сложности задачи [167].
3. Отсутствие подквазигрупп в квазигруппе Q (см. раздел 1.4.3): если в Q имеются достаточно большие подквазигруппы, и исходный элемент

m принадлежал такой подквазигруппе, то операция (4.1) может сохранять принадлежность элемента m подквазигруппе, что дает критерий на отличимость случайной подстановки от структурированной и может рассматриваться как потенциальная слабость алгоритма.

Отметим также, что L-сдвиги (и им родственные преобразования) рассматривались, в частности, в работах [10; 97; 168]. Так, в работе [168] среди прочего показано, что для любой квазигрупповой операции $\circ$ при случайном независимом выборе элементов $q_i \in \mathbf{Dom}$ (при условии, что носитель распределения q_i достаточно большой) распределение элемента ct экспоненциально быстро (при увеличении параметра λ) сходится к равновероятному распределению на множестве $\mathbf{Dom}$. При этом результаты работы [168], вообще говоря, не применимы к ситуации, в которой противник может получать образы различных адаптивно выбираемых m (см. постановку задачи выше), но могут свидетельствовать в пользу сложности рассматриваемой задачи для некоторых квазигрупп.

Предлагаемая FPE-схема

Для того, чтобы получить FPE-схему на основе описанной выше задачи, необходимо задать пару алгоритмов $(\mathsf{Enc}, \mathsf{Dec})$ — отображений из $\mathbf{Keys} \times \mathbf{Twk} \times \mathbf{Dom}$ в $\mathbf{Dom}$. В работе [75] был предложен следующий подход. Для зашифрования элемента m на ключе K и параметре t выполним следующие шаги.

1. По ключу $K \in \mathbf{Keys}$ и параметру $t \in \mathbf{Twk}$ построим с помощью псевдослучайной функции (см., например, функцию PRF из работы [169]) последовательность псевдослучайных элементов $q_1, \ldots, q_\lambda \in Q$.
2. Переведем с помощью левых квазигрупповых сдвигов заданный элемент $m \in \mathbf{Dom}$ в элемент

$$ct = L_{q_1}\left(L_{q_2}\left(\ldots L_{q_\lambda}(m)\ldots\right)\right).$$

Для расшифрования сообщения ct сначала получим согласно п. 1 элементы $q_1, \ldots, q_\lambda \in Q$, а затем последовательно решим уравнения вида $q_i \circ x = y_i$ (λ штук) и получим решение m.

Сложность нахождения решения m по заданным (t, ct) и неизвестному K в предложенной схеме обуславливается двумя факторами (см. более подробное доказательство в [75]).

1. По известному t и неизвестному K трудно восстановить элементы $q_1, \ldots, q_\lambda \in Q$, полученные в п. 1 с помощью псевдослучайной функции (и даже отличить их от истинно случайных).
2. При неизвестных $q_1, \ldots, q_\lambda$ трудно отличить результат применения структурированной подстановки

$$x \to L_{q_1} \circ (L_{q_2} \circ \ldots \circ (L_{q_\lambda} \circ x) \ldots)$$

от результата применения случайной подстановки

$$x \to \pi(x).$$

Рассмотрим ограниченный класс квазигрупп, порожденных правильными семействами функций. Пусть $\mathcal{F}$, $\mathcal{G}$ — два правильных семейства размера n на прямом произведении H^n групп $(H, +)$ (не обязательно абелевых). Как было отмечено выше (см. раздел 1.4.1), операция умножения $\circ\colon H^n \times H^n \to H^n$, определяемая равенством

$$\mathbf{x} \circ \mathbf{y} = \sigma_{\mathcal{F}}(\mathbf{x}) + \sigma_{\mathcal{G}}(\mathbf{y}), \tag{4.2}$$

где $\sigma_{\mathcal{F}}(\mathbf{x}) = \mathbf{x} + \mathcal{F}(\mathbf{x})$ (см. определение 62), а сложение $+$ понимается как покомпонентное сложение в группе H^n, задает структуру квазигруппы.

Определенное таким образом умножение в H^n может быть эффективно обращено используя следующее соображение. Рассмотрим подстановку $\sigma_{\mathcal{F}}^{-1}$. Как было отмечено в разделе 3.3.1, подстановка $\sigma_{\mathcal{F}}^{-1}$ также порождается некоторым правильным семейством $\widetilde{\mathcal{F}}$ (которое было названо дуальным). Семейства $\mathcal{F}$ и $\widetilde{\mathcal{F}}$ связаны соотношением:

$$\widetilde{\mathcal{F}}(\mathbf{x}) = (-\mathbf{x}) + \sigma_{\mathcal{F}}^{-1}(\mathbf{x}), \quad \sigma_{\mathcal{F}}(\mathbf{x}) = \mathbf{x} + \mathcal{F}(\mathbf{x}), \quad x \in H^n. \tag{4.3}$$

Таким образом, если $\mathcal{F}$ и $\widetilde{\mathcal{F}}$ — пара правильных семейств, связанных соотношением (4.3), и операция $\circ$ задается формулой (4.2), то операция $x \circ y$ обращается справа следующим образом:

$$\mathbf{x} = \sigma_{\widetilde{\mathcal{F}}}\left((\mathbf{x} \circ \mathbf{y}) - \sigma_{\mathcal{G}}(\mathbf{y})\right).$$

Аналогичным образом операция $\mathrm{x} \circ \mathrm{y}$ может быть обращена слева, используя «дуальное» к $\mathcal{G}$ семейство $\widetilde{\mathcal{G}}$.

Из этих соображений вытекает, что как L-преобразование, так и обратное к нему L^{-1} могут быть заданы с помощью правильных семейств функций, что позволяет перейти от табличного задания квазигруппы к функциональному.

4.2 Алгоритм проверки правильности булевых семейств

В настоящем разделе мы рассмотрим один алгоритм проверки правильности булева семейства $\mathcal{F}_n$, время работы которого существенно лучше «наивного» алгоритма.

4.2.1 О сложности проверки правильности

Полученное в разделе 2.1 взаимно-однозначное соответствие между правильными семействами булевых функций и USO-ориентациями позволяет перенести часть результатов из теории, развитой в работах [133; 135; 154], на правильные семейства. В частности, верны следующие утверждения.

Следствие 4 ([154, теорема 5])**.** *Пусть семейство булевых функций $\mathcal{F}_n$ задано в виде схемы из функциональных элементов в некотором функционально полном конечном базисе. Тогда задача распознавания правильности семейства по его схеме из функциональных элементов является* coNP*-полной.*

Заметим, что указанное выше утверждение для случая задания функций в виде КНФ было известно и ранее (см. работу [1]). При этом в определенных случаях задача проверки правильности может быть упрощена, в частности, за счет вида графа существенной зависимости [56; 57].

Таким образом, нахождение быстрого (полиномиального по размеру семейства n) алгоритма проверки правильности семейства представляется маловероятным. Заметим, что «наивный» алгоритм проверки правильности требует 4^n операций вычисления значения семейства $\mathcal{F}_n$ на наборе $\mathbf{x} \in \mathbb{E}_2^n$.

4.2.2 Описание алгоритма

Рассмотрим алгоритм проверки правильности со сложностью $2 \cdot 3^n$ операций вычисления семейства $\mathcal{F}_n$ на наборе x, который является следствием теоремы 14. На вход алгоритму подаётся семейство булевых функций $\mathcal{F}_n$ (например, в виде схем из функциональных элементов в некотором базисе). Алгоритм перебирает все проекции исходного семейства $\mathcal{F}_n$, проверяя выполнение свойства несамодвойственности на какой-либо **единственной паре** антиподальных наборов из области определения проекции.

Если на выбранной паре антиподов свойство самодвойственности выполнено, то исходное семейство не может быть правильным: нашлась такая проекция, для которой принимаются противоположные значения, а значит, эта проекция (и исходное семейство) не является правильным семейством (см. замечание 14).

Если на выбранной паре антиподов свойство самодвойственности не выполнено, то рассматриваемая проекция заведомо не является самодвойственным отображением. Поскольку в ходе работы алгоритма перебираются все возможные проекции семейства, то из теоремы 14 следует, что если семейство проходит проверки на несамодвойственность на всех проекциях, то оно является правильным.

Таким образом, мы доказали корректность следующего алгоритма.

Алгоритм 1. *Цикл по всем возможным наборам* $\mathbf{x} \in \mathbb{E}_3^n$*:*

1. *Построить два набора* $\mathbf{y}, \in \mathbb{E}_2^n$ *по правилу:*
   - *если* $x_i \in \{0, 1\}$*, то положить* $y_i \leftarrow x_i$*,* $z_i \leftarrow x_i$*;*
   - *в противном случае положить* $y_i \leftarrow 0$*,* $z_i \leftarrow 1$*.*
2. *Если существует номер* j*, что* $y_j \neq z_j$*, и* $f_j(y) \neq f_j(z)$*, вернуть ответ: «*$\mathcal{F}_n$ *не является правильным».*

Если все проверки пройдены успешно, то вернуть: «$\mathcal{F}_n$ *является правильным».*

Рассмотренный алгоритм позволяет снизить количество вычислений значения отображения $\mathcal{F}_n$ в точке с 4^n до $2 \cdot 3^n$. Вопрос о возможном обобщении алгоритма со случая $k = 2$ на логики большей значности пока что остаётся открытым.

4.3 Некоторые результаты численных экспериментов

В разделе 4.1 был описан один подход к построению алгоритма шифрования, сохраняющего формат сообщений, предложена к рассмотрению одна конкретная конструкция на основе правильных семейств функций, а также выделены три основных свойства, которые можно предъявлять к квазигруппам, которые потенциально могут быть использованы в рассмотренном алгоритме: малое число ассоциативных троек, полиномиальная полнота, отсутствие (больших) подквазигрупп.

В настоящем разделе мы приведем некоторые результаты численных экспериментов:

– в разделе 4.3.1 приводятся точные значения числа булевых правильных семейств малых размеров;
– раздел 4.3.2 посвящен вычислению индексов ассоциативности для квазигрупп, порожденных парами правильных семейств булевых функций;
– в разделе 4.3.3 рассматриваются результаты изучения свойств простоты и аффинности в квазигруппах, порожденных парами правильных семейств булевых функций.

4.3.1 Число различных булевых правильных семейств

В разделе 4.2 был предложен алгоритм, который позволяет ускорить проверку правильности семейства. С использованием указанного алгоритма оказывается возможным вычисление точного значения числа правильных семейств в различных классах. Введем следующие обозначения.

– $\Delta(n)$: число булевых треугольных семейств размера n;
– $\Delta^{\mathsf{loc}}(n)$: число булевых локально-треугольных семейств размера n;
– $\Delta^{\mathsf{rec}}(n)$: число булевых рекурсивно-треугольных семейств размера n;
– $T(n)$: число булевых правильных семейств размера n.

Соберем известные результаты для числа правильных булевых семейств различных классов и размеров (см. таблицу 4). Число треугольных семейства размера $n = 5$ получено в работе [170] (число CP-сетей размера $n = 5$). Число

правильных семейств размера $n = 5$ получено в работе [151] (для числа классов эквивалентности замощений пространства), а также в работах [133; 171] (для числа одностоковых ориентаций). Число $\Delta^{\mathsf{loc}}(5)$ на настоящий момент неизвестно.

Таблица 4 — Число треугольных, рекурсивно треугольных, локально треугольных и правильных булевых семейств размера n.

Размер n	$\Delta(n)$	$\Delta^{\mathsf{rec}}(n)$	$\Delta^{\mathsf{loc}}(n)$	$T(n)$
$n = 1$	2	2	2	2
$n = 2$	12	12	12	12
$n = 3$	488	680	680	744
$n = 4$	481776	3209712	3349488	5541744
$n = 5$	157549032992	94504354122272	—	638560878292512

Как было показано в разделе 3.1, преобразования согласованной перестановки, а также внутренние и внешние сдвиги являются стабилизаторами множества всех правильных семейств. Указанные преобразования можно рассматривать как группу $S_n \times \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ с операцией композиции преобразований, которая действует на правильные семейства следующим образом:

$$(\sigma, A, B) \circ \mathcal{F} = \mathcal{G}, \quad \mathcal{G}(\mathbf{x}) = \sigma(\mathcal{F})(\mathbf{x} \oplus A) \oplus B.$$

В таком случае для каждого правильного семейства определяется его класс эквивалентности относительно действия всей группы или некоторой ее подгруппы. Заметим, что внешние сдвиги не оставляют никакое семейство на месте, в то время как внутренние сдвиги и согласованные перестановки могут не изменять семейства. Будем рассматривать два отношения эквивалентности:

– классы 1: классы отношения эквивалентности, заданного согласованными подстановками совместно с внешними сдвигами;
– классы 2: классы отношения эквивалентности, заданного согласованными подстановками совместно с внутренними и внешними сдвигами;

Были проведены численные эксперименты по подсчету различных классов эквивалентности для булевых правильных семейств размера n. Полученные результаты приведены в таблице 5.

Таблица 5 — Число классов эквивалентности правильных булевых семейств размера n

Размер n	Число классов 1	Число классов 2
$n = 1$	1	1
$n = 2$	2	2
$n = 3$	19	10
$n = 4$	14614	1291

4.3.2 Индексы ассоциативности для квазигрупп, построенных по правильным булевым семействам малых размеров

Приведем результаты численных экспериментов для количества ассоциативных троек (см. раздел 1.4.1) в квазигруппах, порожденных правильными семействами булевых функций.

Для $n = 2$ имеется 12 правильных булевых семейств, с помощью которых можно задать $12^2 = 144$ квазигруппы (используя конструкцию, описанную в разделе 4.1.2). Для $n = 3$ имеется 744 правильных булевых семейства, с помощью которых можно задать $744^2 = 553536$ квазигрупп. Все порождаемые квазигруппы будут попарно различны: если $\mathcal{F} \neq \mathcal{G}$, то для некоторого $\mathbf{x}$ имеем

$$\pi_{\mathcal{F}}(\mathbf{x}) = \mathbf{x} \oplus \mathcal{F}(\mathbf{x}) \neq \mathbf{x} \oplus \mathcal{G}(\mathbf{x}) = \pi_{\mathcal{G}}(\mathbf{x}).$$

Результаты численных экспериментов для $n = 2$ приведены в таблице 6, для $n = 3$ — приведены в таблице 7 и на рис. 4.1. Заметим также, что индекс ассоциативности для всех полученных квазигрупп является четным (см. теорему 8).

Таблица 6 — Число квазигрупп с заданным $a(Q)$ для квазигрупп, построенных по правильным булевым семействам размера $n = 2$

$a(Q)$	Кол-во Q
16	32
32	96
64	16

Таблица 7 — Число квазигрупп с заданным $a(Q)$ для квазигрупп, построенных по правильным булевым семействам размера $n = 3$

$a(Q)$	Кол-во Q
64	27648
80	103424
88	18432
96	82944
104	33792
112	21504
120	21504
128	116352

$a(Q)$	Кол-во Q
144	3072
160	84480
176	6144
192	18432
208	3072
256	10368
320	2304
512	64

Для $n = 4$ был проведен статистический эксперимент. Случайно равновероятно (среди всех возможных пар) выбирались $N = 10^5$ пар правильных семейств, по каждой паре строилась квазигруппа, подсчитывался индекс ассоциативности полученной квазигруппы. Была построена ядерная оценка плотности полученной случайной величины (с нормальной ядерной функцией, ширина полосы пропускания выбиралась в соответствии с эмпирическим правилом Сильвермана), результат приведен на рис. 4.2.

Заметим, что при $n = 2$ достигается минимально возможное значение индекса ассоциативности для квазигрупп порядка 4 (а именно 16). При $n \geqslant 3$ все полученные индексы ассоциативности существенно превышают минимальные теоретически возможные для квазигрупп заданного порядка. Отметим также, что во всех исследованных случаях $n = 2, 3, 4$ минимально достижимый индекс ассоциативности у построенных квазигрупп оказался равным квадрату порядка квазигруппы, в связи с чем можно выдвинуть гипотезу, что у квазигрупп, построенным по парам правильных булевых семейств размера n, число ассоциативных троек не может быть меньше, чем 2^{2n}.

Для $n = 3$ также был проведен следующий эксперимент. Все 744 правильных семейства были разбиты на 10 классов эквивалентности относительно изометрий пространства Хэмминга (см. таблицу 5). Затем для каждой пары классов эквивалентности (F, G) перебирались все пары представителей $\mathcal{F} \in F$, $\mathcal{G} \in G$ и вычислялся индекс ассоциативности квазигруппы, порождаемой парой

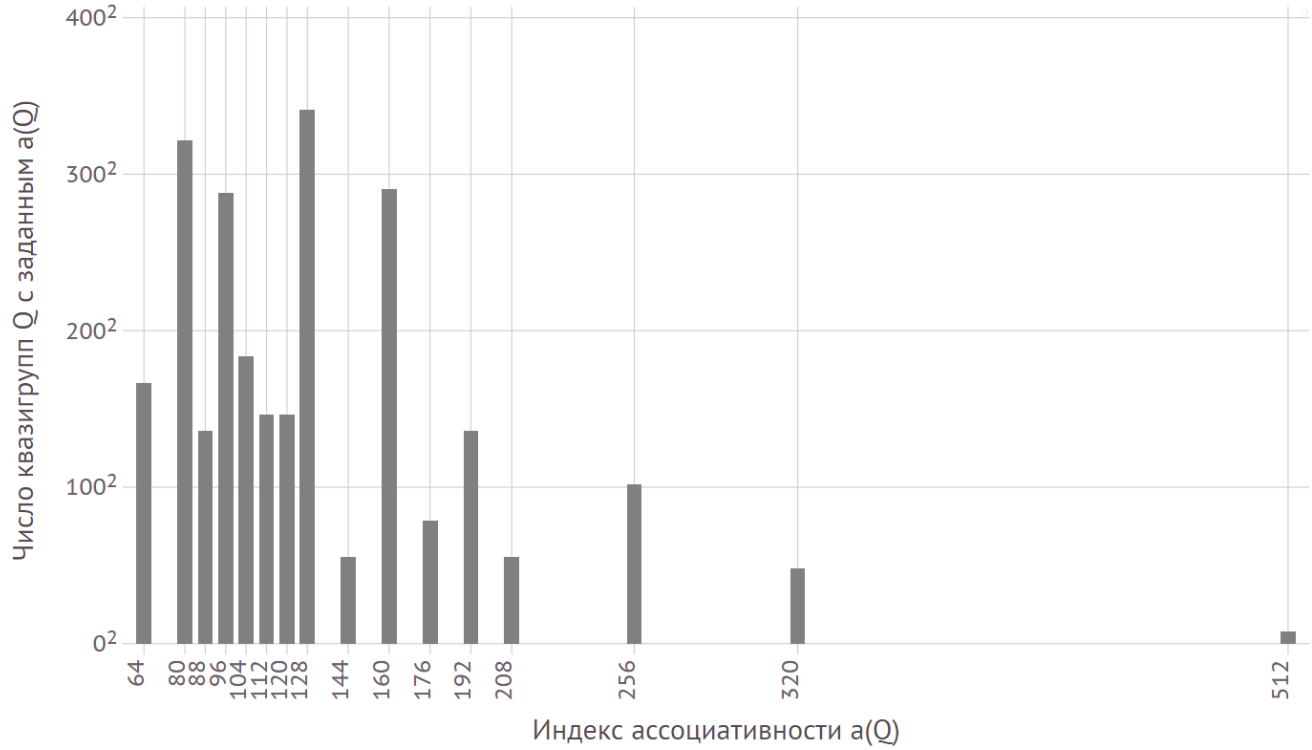

Рисунок 4.1 — Распределение числа квазигрупп с заданным $a(Q)$ для $n = 3$

правильных булевых семейств $(\mathcal{F}, \mathcal{G})$, после чего вычислялся «средний индекс ассоциативности» для пары классов эквивалентности (F, G). Результаты эксперимента отображены на рис. 4.3. Из приведенной тепловой карты видно, что наиболее неассоциативные квазигруппы порождаются при использовании 6-го класса эквивалентности, представителем которого является, например, семейство

$$\left(x_2x_3,\ x_1 \oplus x_1x_3,\ x_1 \oplus x_2 \oplus x_1x_2\right).$$

Отметим, что представители указанного класса изучались в разделе 1.3.3: было показано, что представители класса имеют полный граф существенной зависимости и являются квадратичным строгого типа $Quad^s_{n-1}Lin^s_1$ (см. определение 21) при четных n и квадратичным строгого типа $Quad^s_nLin^s_0$ (сильно квадратичным) при нечетных n (см. теорему 3).

4.3.3 Экспериментальное изучение простоты и аффинности

Приведем результаты вычислительных экспериментов для квазигрупп, порожденных операцией (4.2):

$$\mathbf{x} \circ \mathbf{y} = \mathbf{x} + \mathcal{F}(\mathbf{x}) + \mathbf{y} + \mathcal{G}(\mathbf{y}), \tag{4.4}$$

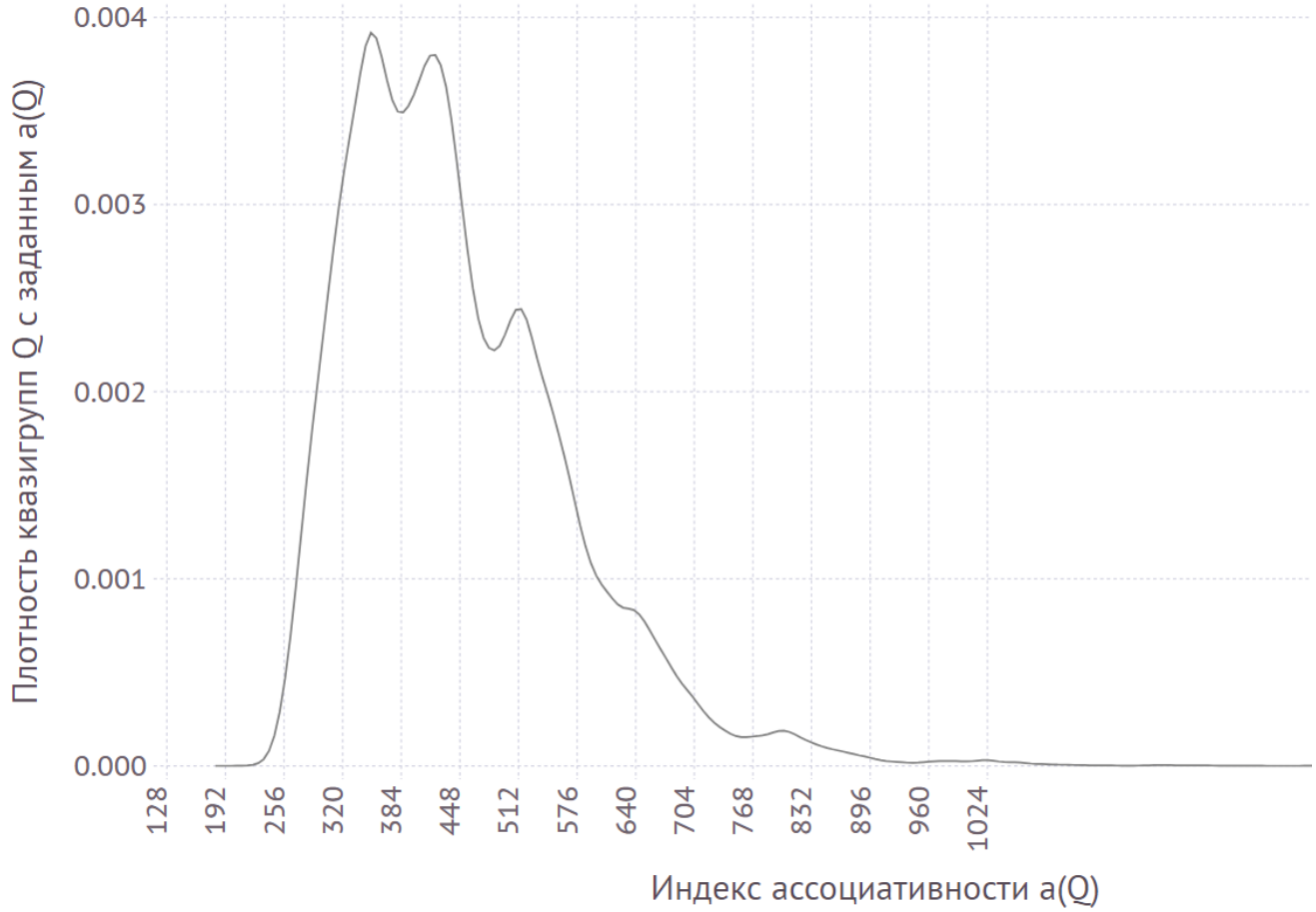

Рисунок 4.2 — Оценка плотности распределения квазигрупп, построенных по парам правильных булевых семейств, с заданным $a(Q)$ для $n = 4$

где в качестве базовой рассматривается группа $\mathbb{Z}_2^n$, $\mathcal{F}$, $\mathcal{G}$ — семейства размера n на $\mathbb{Z}_2^n$.

Для $n = 2$ существует 12 правильных семейств (см. таблицу 4). При этом все 144 квазигруппы, порожденные с помощью конструкции (4.2) оказываются аффинными, 32 — простыми. Таким образом, полиномиально полные квазигруппы среди квазигрупп, порожденных конструкцией (4.2), для $n = 2$ отсутствуют. Результаты отображены в таблице 8.

Для $n = 3$ существует 744 правильных семейства и, соответственно, 553536 возможных квазигрупп. Среди этих квазигрупп 40000 являются аффинными, 290816 — простыми, 281600 — полиномиально полными. Результаты отображены в таблице 9.

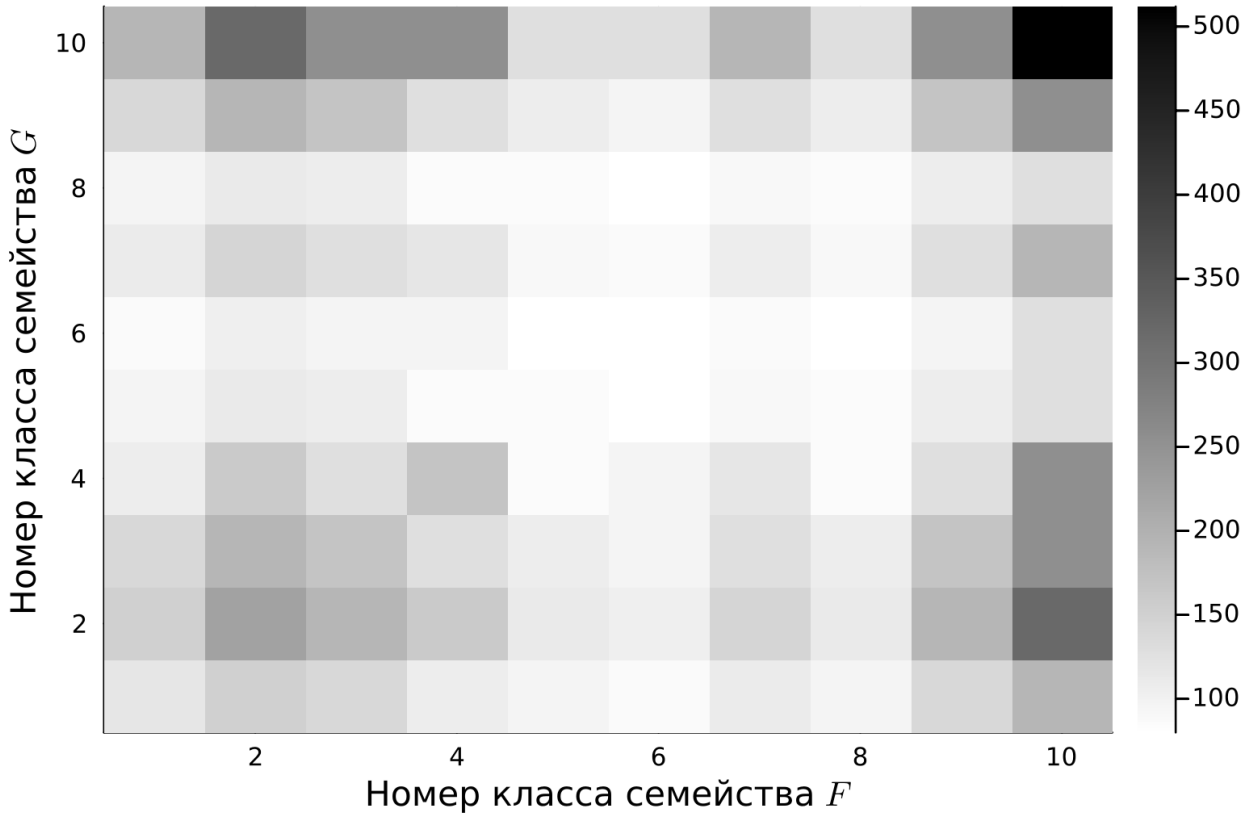

Рисунок 4.3 — Тепловая карта для среднего индекса ассоциативности, усреднение берется по представителям классов эквивалентности, $n = 3$

Таблица 8 — Число квазигрупп, построенных с помощью конструкции (4.2) с заданными свойствами для $n = 2$

Свойства	Афинная	Неаффинная
Не простая	112	0
Простая	32	0

Выводы

В настоящей главе были рассмотрены два алгоритма:

– алгоритм шифрования, сохраняющего формат сообщений (FPE-схема), основанный на квазигрупповых сдвигах;
– ускоренный алгоритм для задачи распознавания правильности семейства булевых функций.

Были выделены основные требования к квазигруппам, которые могут использоваться в качестве базовых в предложенной FPE-схеме. Также были приведены

Таблица 9 — Число квазигрупп, построенных с помощью конструкции (4.2) с заданными свойствами для $n = 3$

Свойства	Афинная	Неаффинная
Не простая	30784	231936
Простая	9216	281600

результаты некоторых статистических и численных экспериментов, в которых изучалось число правильных семейств в различных классах и свойства квазигрупп, порожденных парами правильных семейств булевых функций: индексы ассоциативности, простота и аффинность.

Заключение

В начале диссертационного исследования были поставлены следующие задачи.

1. Получение новых критериев правильности семейств функций, а также установление естественного соответствия между правильными семействами функций и другими комбинаторно-алгебраическими структурами.
2. Исследование общих свойств правильных семейств функций, включая структуру множества неподвижных точек, а также стабилизатор относительно определенных классов преобразований.
3. Нахождение новых классов правильных семейств и изучение их свойств, включая мощность класса и мощность образа представителей.
4. Разработка нового способа построения квазигрупп на основе правильных семейств функций, создание шифра, сохраняющего формат, на основе этой конструкции, и анализ характеристик полученного шифра.

Основные результаты работы заключаются в следующем.

1. Установлено естественное соответствие между булевыми правильными семействами и одностоковыми ориентациями графов булевых кубов (USO-ориентации).
2. Установлено естественное соответствие между булевыми правильными семействами и булевыми сетями с наследственно единственной неподвижной точкой (HUFP-сети).
3. Установлено естественное соответствие между правильными семействами в логике произвольной значности и кликами в обобщенных графах Келлера.
4. Доказано, что стабилизатором множества правильных семейств функций являются изометрии пространства Хэмминга (согласованные перенумерации и перекодировки).
5. Показано, что отображения, задаваемые с помощью правильных семейств булевых функций, всегда имеют четное число неподвижных точек.

6. Получена оценка на число правильных семейств булевых функций, предложены оценки доли треугольных семейств среди всех правильных семейств булевых функций.
7. Обнаружены и исследованы новые классы правильных семейств функций (рекурсивно треугольные, локально треугольные, сильно квадратичное семейство).
8. Получены оценки на число рекурсивно треугольных семейств.
9. Для некоторых правильных семейств булевых функций получены точные значения мощности образа отображений, задаваемых этими правильными семействами.
10. Предложен новый способ порождения квазигрупп на основе правильных семейств функций.
11. Доказан ряд утверждений о числе ассоциативных троек в порождаемых квазигруппах.
12. Предложен новый алгоритм шифрования, сохраняющего формат (FPE-схема), основанный на квазигрупповых операциях.

Результаты диссертационной работы могут представлять интерес для специалистов, работающих в области теории дискретных и булевых функций, теории квазигрупп, криптографии.

В качестве тем для дальнейших исследований можно отметить следующие направления.

1. Предложить способ построения достаточно широких классов правильных семейств с хорошими алгебраическими и комбинаторными свойствами, в том числе и для логик большей значности $k > 2$.
2. Предложить способ быстрого построения множества представителей всех правильных семейств размера $n + 1$ с помощью представителей размера n и менее (с точностью до согласованных перенумераций и перекодировок).
3. Предложить альтернативные геометрические описания правильных семейств в k-значной логике, где $k > 2$, которые были бы инвариантны относительно согласованных перенумераций и перекодировок.
4. Предложить алгоритм, полиномиальный по длине входа, на вход принимающий правильное семейство (например, в виде КНФ или полиномов Жегалкина) и параметрические подстановки и выдающий количество ассоциативных троек (или нижние и верхние границы на число троек),

проверяющий полиномиальную полноту порождаемой квазигруппы, наличие или отсутствие подквазигрупп.

5. Оценить генерическую сложность задачи решения системы уравнений над квазигруппами, заданными правильными семействами.

Автор выражает глубокую благодарность своим научным руководителям А. В. Галатенко и А. Е. Панкратьеву за оказанную помощь при написании настоящей работы, постановку задачи, обсуждение результатов и постоянное внимание к работе.

Список литературы

1. *Носов В. А.* Критерий регулярности булевского неавтономного автомата с разделенным входом // Интеллектуальные системы. Теория и приложения. — 1998. — Т. 3, № 3/4. — С. 269—280.
2. *Носов В. А.* Построение классов латинских квадратов в булевой базе данных // Интеллектуальные системы. Теория и приложения. — М., 1999. — Т. 4, № 3/4. — С. 307—320.
3. *Denes J., Keedwell A.* Latin squares and their applications (2nd edition). — Elsevier, 2015. — 428 p.
4. *Глухов М. М.* О применениях квазигрупп в криптографии // Прикладная дискретная математика. — 2008. — 2 (2). — С. 28—32.
5. *Chauhan D., Gupta I., Verma R.* Quasigroups and their applications in cryptography // Cryptologia. — 2021. — Vol. 45, no. 3. — P. 227—265.
6. *Shcherbacov V.* Elements of Quasigroup Theory and Applications. — Chapman, Hall/CRC, 2017.
7. *Тужилин М. Э.* Латинские квадраты и их применение в криптографии // Прикладная дискретная математика. — 2012. — Т. 17, № 3. — С. 47—52.
8. *Markovski S., Gligoroski D., Bakeva V.* Quasigroup String Processing: Part 1 // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tect. Sci. XX. — 1999. — P. 157—162.
9. *Markovski S.* Quasigroup string processing and applications in cryptography // Proc. 1-st Inter. Conf. Mathematics and Informatics for industry. Vol. 1002. — 2003. — P. 14—16.
10. *Markovski S., Bakeva V.* Quasigroup string processing: Part 4 // Contributions, Section of Natural, Mathematical and Biotechnical Sciences. — 2017. — Vol. 27, no. 1/2.
11. Hash functions based on large quasigroups / V. Snášel, A. Abraham, J. Dvorskỳ, P. Krömer, J. Platoš // Computational Science–ICCS 2009: 9th International Conference Baton Rouge, LA, USA, May 25-27, 2009 Proceedings, Part I 9. — Springer. 2009. — P. 521—529.

12. *Gligoroski D., Markovski S., Knapskog S. J.* The stream cipher Edon80 // New stream cipher designs. — Springer, 2008. — P. 152—169.

13. *Gligoroski D., Markovski S., Kocarev L.* Edon-R, An Infinite Family of Cryptographic Hash Functions // International Journal of Security and Networks. — 2009. — Vol. 8, no. 3. — P. 293—300.

14. Cryptographic hash function Edon-R’ / D. Gligoroski, R. S. Ødegård, M. Mihova, S. J. Knapskog, A. Drápal, V. Klima, J. Amundse, M. El-Hadedy // 2009 Proceedings of the 1st International Workshop on Security and Communication Networks. — IEEE. 2009. — P. 1—9.

15. NaSHA Cryptographic Hash Function / S. Markovski, A. Mileva, S. Samardziska, B. Jakimovski. — Algorithm Specifications and Supporting Documentations.

16. *Mileva A., Markovski S.* Quasigroup String Transformations and Hash Function Design: A Case Study: The NaSHA Hash Function // International Conference on ICT Innovations. — Springer. 2009. — P. 367—376.

17. GAGE and InGAGE / D. Gligoroski, M. El-Hadedy, H. Mihajloska, D. Otte // A Submission to the NIST Lightweight Cryptography Standardization Process. — 2019.

18. *Gligoroski D.* On the S-box in GAGE and InGAGE. — 2019. — http : / / gageingage.org/upload/LWC2019NISTWorkshop.pdf.

19. *Teşeleanu G.* Quasigroups and substitution permutation networks: a failed experiment // Cryptologia. — 2021. — Vol. 45, no. 3. — P. 266—281.

20. *Teşeleanu G.* The Security of Quasigroups Based Substitution Permutation Networks // International Conference on Information Technology and Communications Security. — Springer. 2022. — P. 306—319.

21. *Teşeleanu G.* Cryptographic symmetric structures based on quasigroups // Cryptologia. — 2023. — Vol. 47, no. 4. — P. 365—392.

22. *Чередник И. В.* Один подход к построению транзитивного множества блочных преобразований // Прикладная дискретная математика. — 2017. — Т. 38. — С. 5—34.

23. *Чередник И. В.* Об использовании бинарных операций при построении транзитивного множества блочных преобразований // Дискретная математика. — 2019. — Т. 31, № 3. — С. 93—113.

24. *Чередник И. В.* Об использовании бинарных операций при построении кратно транзитивного множества блочных преобразований // Дискретная математика. — 2020. — Т. 32, № 2. — С. 85—111.

25. *Vojvoda M.* Cryptanalysis of one hash function based on quasigroup // Tatra Mt. Math. Publ. — 2004. — Vol. 29, no. 3. — P. 173—181.

26. *Vojvoda M., Sỳs M., Jókay M.* A note on algebraic properties of quasigroups in edon80 // Workshop Record of SASC. — 2007.

27. *Slaminková I., Vojvoda M.* Cryptanalysis of a hash function based on isotopy of quasigroups // Tatra Mountains Mathematical Publications. — 2010. — Vol. 45, no. 1. — P. 137—149.

28. *Hell M., Johansson T.* A key recovery attack on Edon80 // International Conference on the Theory and Application of Cryptology and Information Security. — Springer. 2007. — P. 568—581.

29. *Nikolic I., Khovratovich D.* Free-start attacks on NaSHA. — https://ehash.isec.tugraz.at/uploads/3/33/Free-start_attacks_on_Nasha.pdf.

30. *Li Z., Jiang H., Li C.* Collision attack on NaSHA-384/512 // 2010 International Conference on Networking and Information Technology. — IEEE. 2010. — P. 243—246.

31. Рекурсивные МДР-коды и рекурсивно дифференцируемые квазигруппы / С. Гонсалес, Е. Коусело, В. Т. Марков, А. А. Нечаев // Дискретная математика. — 1998. — Т. 10, № 2. — С. 3—29.

32. Групповые коды и их неассоциативные обобщения / С. Гонсалес, Е. Коусело, В. Т. Марков, А. А. Нечаев // Дискретная математика. — 2004. — Т. 16, № 1. — С. 146—156.

33. Loop codes / E. Couselo, S. González, V. T. Markov, A. A. Nechaev // Discrete Mathematics and Applications. — 2004. — Vol. 14, no. 2. — P. 163—172.

34. Квазигруппы и кольца в кодировании и построении криптосхем / В. Т. Марков, А. В. Михалёв, А. В. Грибов, П. А. Золотых, С. С. Скаженик // Прикладная дискретная математика. — 2012. — Т. 4.

35. *Markov V. T.*, *Mikhalev A. V.*, *Nechaev A. A.* Nonassociative Algebraic Structures in Cryptography and Coding // Journal of Mathematical Sciences. — 2020. — Vol. 245, no. 2.

36. *Катышев С. Ю.*, *Марков В. Т.*, *Нечаев А. А.* Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей // Дискретная математика. — 2014. — Т. 26, № 3. — С. 45—64.

37. *Марков В. Т.*, *Михалёв А. В.*, *Нечаев А. А.* Неассоциативные алгебраические структуры в криптографии и кодировании // Фундаментальная и прикладная математика. — 2016. — Т. 21, № 4. — С. 99—124.

38. *Baryshnikov A. V.*, *Katyshev S. Y.* Key agreement schemes based on linear groupoids // Математические вопросы криптографии. — 2017. — Т. 8, № 1. — С. 7—12.

39. *Барышников А. В.*, *Катышев С. Ю.* Использование неассоциативных структур для построения алгоритмов открытого распределения ключей // Математические вопросы криптографии. — 2018. — Т. 9, № 4. — С. 5—30.

40. *Грибов А. В.*, *Золотых П. А.*, *Михалёв А. В.* Построение алгебраической криптосистемы над квазигрупповым кольцом // Математические вопросы криптографии. — 2010. — Т. 1, № 4. — С. 23—32.

41. *Грибов А. В.* Алгебраические неассоциативные структуры и их приложения в криптографии : дис. … канд. / Грибов А. В. — Московский государственный университет им. М. В. Ломоносова, 2015.

42. *Грибов А. В.* Гомоморфность некоторых криптографических систем на основе неассоциативных структур // Фундаментальная и прикладная математика. — 2015. — Т. 20, № 1. — С. 135—143.

43. *Katyshev S. Y.*, *Zyazin A. V.*, *Baryshnikov A. V.* Application of non-associative structures for construction of homomorphic cryptosystems // Математические вопросы криптографии. — 2020. — Т. 11, № 3. — С. 31—39.

44. *Марков В. Т.*, *Михалёв А. В.*, *Кислицын Е. С.* Неассоциативные структуры в гомоморфной криптографии // Фундаментальная и прикладная математика. — 2020. — Т. 23, № 2. — С. 209—215.

45. *Gligoroski D.*, *Markovski S.*, *Knapskog S. J.* A public key block cipher based on multivariate quadratic quasigroups // arXiv preprint arXiv:0808.0247. — 2008.

46. *Gligoroski D., Markovski S., Knapskog S. J.* Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups // Proceedings of the American Conference on Applied Mathematics. — 2008. — P. 44—49.

47. *Chen Y., Knapskog S. J., Gligoroski D.* Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity // Submitted to ISIT. — 2010. — Vol. 2010. — P. 14.

48. MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme / D. Gligoroski, R. S. Ødegård, R. E. Jensen, L. Perret, J.-C. Faugere, S. J. Knapskog, S. Markovski // International Conference on Trusted Systems. — Springer. 2011. — P. 184—203.

49. *Носов В. А.* Построение параметрического семейства латинских квадратов в векторной базе данных // Интеллектуальные системы. Теория и приложения. — М., 2006. — Т. 8, № 1—4. — С. 517—529.

50. *Носов В. А., Панкратьев А. Е.* Латинские квадраты над абелевыми группами // Фундаментальная и прикладная математика. — 2006. — Т. 12, № 3. — С. 65—71.

51. *Носов В. А., Панкратьев А. Е.* О семействах функций, задающих латинские квадраты над абелевыми группами // Лесной вестник Forestry bulletin. — 2007. — № 2.

52. *Носов В. А., Панкратьев А. Е.* О функциональном задании латинских квадратов // Интеллектуальные системы. Теория и приложения. — М., 2008. — Т. 12, № 1—4. — С. 317—332.

53. *Козлов А. А., Носов В. А., Панкратьев А. Е.* Матрицы и графы существенной зависимости правильных семейств функций // Фундаментальная и прикладная математика. — 2008. — Т. 14, № 4. — С. 137—149.

54. *Плаксина И. А.* Построение параметрического семейства многомерных латинских квадратов // Интеллектуальные системы. Теория и приложения. — 2014. — Т. 18, № 2. — С. 323—330.

55. *Galatenko A. V., Nosov V. A., Pankratiev A. E.* Latin squares over quasigroups // Lobachevskii Journal of Mathematics. — 2020. — Vol. 41, no. 2. — P. 194—203.

56. *Рыков Д. О.* Об алгоритмах проверки правильности семейств функций // Интеллектуальные системы. Теория и приложения. — 2010. — Т. 14, № 1—4. — С. 261—276.

57. *Рыков Д. О.* О правильных семействах функций, используемых для задания латинских квадратов // Интеллектуальные системы. Теория и приложения. — 2014. — Т. 18, № 1. — С. 141—152.

58. Порождение правильных семейств функций / А. В. Галатенко, В. А. Носов, А. Е. Панкратьев, В. М. Староверов // Интеллектуальные системы. Теория и приложения. — 2021. — Т. 25, № 4. — С. 100—103.

59. *Galatenko A. V., Pankratiev A. E., Staroverov V. M.* Generation of Proper Families of Functions // Lobachevskii Journal of Mathematics. — 2022. — Vol. 43, no. 3. — P. 571—581.

60. *Hagemann J., Herrmann C.* Arithmetical locally equational classes and representation of partial functions // Universal algebra. — 1982. — P. 345—360. — Proceedings of the Colloquium on Universal Algebra.

61. *Nipkow T.* Unification in primal algebras, their powers and their varieties // Journal of the ACM (JACM). — 1990. — Vol. 37, no. 4. — P. 742—776.

62. *Horváth G., Nehaniv C. L., Szabó C.* An assertion concerning functionally complete algebras and NP-completeness // Theoretical computer science. — 2008. — Vol. 407, no. 1—3. — P. 591—595.

63. *Artamonov V., Chakrabarti S., Pal S. k.* Characterization of polynomially complete quasigroups based on Latin squares for cryptographic transformations // Discrete Applied Mathematics. — 2016. — Vol. 200. — P. 5—17.

64. *Kepka T.* A note on associative triples of elements in cancellation groupoids // Commentationes Mathematicae Universitatis Carolinae. — 1980. — Vol. 21, no. 3. — P. 479—487.

65. *Kotzig A., Reischer C.* Associativity index of finite quasigroups // Glasnik Matematicki Series III. — 1983. — Vol. 18, no. 38. — P. 243—253.

66. *Ježek J., Kepka T.* Notes on the number of associative triples // Acta Universitatis Carolinae. Mathematica et Physica. — 1990. — Vol. 31, no. 1. — P. 15—19.

67. *Собянин П. И.* Об алгоритме проверки наличия подквазигруппы в квазигруппе // Интеллектуальные системы. Теория и приложения. — 2019. — Т. 23, № 2. — С. 79—84.

68. *Галатенко А. В., Панкратьев А. Е., Староверов В. М.* Об одном алгоритме проверки существования подквазигрупп // Чебышевский сборник. — 2021. — Т. 22, 2 (78). — С. 76—89.

69. *Пивень Н. А.* Исследование квазигрупп, получаемых с помощью правильных семейств булевых функций порядка 2 // Интеллектуальные системы. Теория и приложения. — 2018. — Т. 22, № 1. — С. 21—35.

70. *Пивень Н. А.* Некоторые свойства перестановочной конструкции для параметрического задания квазигрупп // Интеллектуальные системы. Теория и приложения. — 2019. — Т. 23, № 2. — С. 71—78.

71. *Галатенко А. В., Носов В. А., Панкратьев А. Е.* Порождение квадратичных квазигрупп с помощью правильных семейств булевых функций // Фундаментальная и прикладная математика. — 2020. — Т. 23, № 2. — С. 57—73.

72. *Шварёв А. С.* Криптоанализ и совершенствование квазигрупповых алгоритмов шифрования : дис. … маг. / Шварёв А. С. — МГУ имени М.В. Ломоносова, Казахстанский филиал, 2024. — выпускная квалификационная (бакалаврская) работа.

73. *Царегородцев К. Д.* О взаимно однозначном соответствии между правильными семействами булевых функций и рёберными ориентациями булевых кубов // Прикладная дискретная математика. — 2020. — Т. 48. — С. 16—21.

74. *Царегородцев К.* О свойствах правильных семейств булевых функций // Дискретная математика. — 2021. — Т. 33, № 1. — С. 91—102.

75. *Tsaregorodtsev K.* Format-preserving encryption: a survey // Математические вопросы криптографии. — 2022. — Т. 13, № 2. — С. 133—153.

76. Proper families of functions and their applications / A. V. Galatenko, V. A. Nosov, A. E. Pankratiev, K. D. Tsaregorodtsev // Математические вопросы криптографии. — 2023. — Т. 14, № 2. — С. 43—58.

77. О порождении n-квазигрупп с помощью правильных семейств функций / А. Галатенко, В. Носов, А. Панкратьев, К. Царегородцев // Дискретная математика. — 2023. — Т. 35, № 1. — С. 35—53.

78. *Galatenko A., Pankratiev A., Tsaregorodtsev K.* A Criterion of Properness for a Family of Functions // Journal of Mathematical Sciences. — 2024. — Vol. 284, no. 4. — P. 451—459.

79. *Царегородцев К.* О соответствии между правильными семействами и реберными ориентациями булевых кубов // Интеллектуальные системы. Теория и приложения. — 2020. — Т. 24, № 1. — С. 97—100.

80. *Царегородцев К.* Об индексе ассоциативности конечных квазигрупп // Интеллектуальные системы. Теория и приложения. — 2024. — Т. 28, № 3. — С. 80—101.

81. *Царегородцев К.* Об одном квазигрупповом алгоритме шифрования, сохраняющего формат // Прикладная дискретная математика. Приложение. — 2023. — Т. 16. — С. 102—104.

82. *Белоусов В. Д.* Основы теории квазигрупп и луп. — М. : Наука, 1967.

83. *Галкин В. М.* Квазигруппы // Итоги науки и техники. Серия «Алгебра. Топология. Геометрия». — 1988. — Т. 26, № 0. — С. 3—44.

84. *Яблонский С. В.* Введение в дискретную математику. — М. : Наука, 1986. — 2-е изд., перераб. и доп.

85. *Chen Y., Gligoroski D., Knapskog S. J.* On a special class of multivariate quadratic quasigroups (MQQs) // Journal of Mathematical Cryptology. — 2013. — Vol. 7, no. 2. — P. 111—141.

86. *Dimitrova V., Markovski S.* Classification of quasigroups by image patterns // Proceedings of the Fifth International Conference for Informatics and Information Technology, Bitola, Macedonia. — Institute of Informatics, Faculty of Natural Sciences, Mathematics, Ss. Cyril, Methodius University in Skopje. 2007. — P. 470—483.

87. *Falcón R. M., Álvarez V., Gudiel F.* A computational algebraic geometry approach to analyze pseudo-random sequences based on Latin squares // Advances in Computational Mathematics. — 2019. — Vol. 45. — P. 1769—1792.

88. *Markovski S., Gligoroski D., Markovski J.* Classification of quasigroups by random walk on torus // Journal of applied mathematics and computing. — 2005. — Vol. 19, no. 1. — P. 57—75.

89. *Bakeva V., Dimitrova V.* Some probabilistic properties of quasigroup processed strings useful for cryptanalysis // ICT Innovations 2010: Second International Conference, ICT Innovations 2010, Ohrid Macedonia, September 12-15, 2010. Revised Selected Papers 2. — Springer. 2011. — P. 61—70.

90. Testing the properties of large quasigroups / E. Ochodkova, J. Dvorskỳ, V. Snášel, A. Abraham // 2009 International Conference on Ultra Modern Telecommunications & Workshops. — IEEE. 2009. — P. 1—7.

91. Large quasigroups in cryptography and their properties testing / J. Dvorskỳ, E. Ochodková, V. Snášel, A. Abraham // 2009 World Congress on Nature & Biologically Inspired Computing (NaBIC). — IEEE. 2009. — P. 965—971.

92. *Valent V.* Quasigroups with few associative triples : Master's thesis / Valent V. — Univerzita Karlova, Matematicko-fyzikálnı fakulta, 2016. — Bachelor thesis.

93. *Kepka T.* Notes on associative triples of elements in commutative groupoids // Acta Universitatis Carolinae. Mathematica et Physica. — 1981. — Vol. 22, no. 2. — P. 39—47.

94. *Drápal A., Kepka T.* A note on the number of associative triples in quasigroups isotopic to groups // Commentationes Mathematicae Universitatis Carolinae. — 1981. — Vol. 22, no. 4. — P. 735—743.

95. *Drápal A.* On quasigroups rich in associative triples // Discrete Mathematics. — 1983. — Vol. 44, no. 3. — P. 251—265.

96. *Grošek O., Horák P.* On quasigroups with few associative triples // Designs, Codes and Cryptography. — 2012. — Vol. 64, no. 1/2. — P. 221—227.

97. *Артамонов В. А.* Квазигруппы и их приложения // Чебышевский сборник. — 2018. — Т. 19, 2 (66). — С. 111—122.

98. *Drápal A., Valent V.* High nonassociativity in order 8 and an associative index estimate // Journal of Combinatorial Designs. — 2019. — Vol. 27, no. 4. — P. 205—228.

99. *Drápal A., Lisoněk P.* Maximal nonassociativity via nearfields // Finite Fields and Their Applications. — 2020. — Vol. 62.

100. *Drápal A., Wanless I.* Maximally nonassociative quasigroups via quadratic orthomorphisms // Algebraic Combinatorics. — 2021. — Vol. 4, no. 3. — P. 501—515.

101. *Lisoněk P.* Maximal nonassociativity via fields // Designs, Codes and Cryptography. — 2020. — Vol. 88, no. 12. — P. 2521—2530.

102. *Ионин Ю.* Конечные проективные плоскости // Математическое просвещение. — 2009. — Т. 13. — С. 50—79.

103. *Drápal A., Valent V.* Few associative triples, isotopisms and groups // Designs, Codes and Cryptography. — 2018. — Vol. 86, no. 3. — P. 555—568.

104. *Artamonov V., Chakrabarti S., Pal S. K.* Characterizations of highly non-associative quasigroups and associative triples // Quasigroups and Related Systems. — 2017. — Vol. 25, no. 1. — P. 1—19.

105. *Valent V.* Small order quasigroups with minimum number of associative triples : Master's thesis / Valent V. — Univerzita Karlova, Matematicko-fyzikální fakulta, 2018.

106. *Drápal A., Valent V.* Extreme nonassociativity in order nine and beyond // Journal of Combinatorial Designs. — 2020. — Vol. 28, no. 1. — P. 33—48.

107. *Clifford A. H., Preston G. B.* The Algebraic Theory of Semigroups. Vol. 7. — American Mathematical Soc., 1961. — https://www.ams.org/books/surv/007.1/.

108. *Miller G. L.* On the $n^{\log n}$ isomorphism technique (a preliminary report) // Proceedings of the tenth annual ACM symposium on theory of computing. — 1978. — C. 51—58.

109. *Rajagopalan S., Schulman L. J.* Verification of identities // SIAM Journal on Computing. — 2000. — Vol. 29, no. 4. — P. 1155—1163.

110. *Childs A. M., Van Dam W.* Quantum algorithms for algebraic problems // Reviews of Modern Physics. — 2010. — Vol. 82, no. 1. — P. 1—52.

111. Verifying Groups in Linear Time / S. Evra, S. Gadot, O. Klein, I. Komargodski // 2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS). — IEEE. 2024. — P. 2131—2147.

112. Алгоритмы. Построение и анализ:[пер. с англ.] / Т. Кормен, Ч. Лейзерсон, Р. Ривест, К. Штайн. — Издательский дом Вильямс, 2009.

113. On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts / V. Artamonov, S. Chakrabarti, S. Gangopadhyay, S. K. Pal // Quasigroups and related systems. — 2013. — Vol. 21, no. 2. — P. 117—130.

114. *Chaplygina S., Galatenko A.* Polynomial completeness and completeness of finite n-quasigroups // Quasigroups and related systems. — 2024. — Vol. 32, no. 2. — P. 207—223.

115. *Salomaa A.* Some completeness criteria for sets of functions over a finite domain // II. Annales Universitatis Turkuensis, Series A I. — 1963.

116. *Cameron P. J.* Almost all quasigroups have rank 2 // Discrete Mathematics. — 1992. — Vol. 106/107. — P. 111—115. — URL: https://www.sciencedirect.com/science/article/pii/0012365X9290537P.

117. *Галатенко А. В., Галатенко В. В., Панкратьев А. Е.* О сильной полиномиальной полноте почти всех квазигрупп // Математические заметки. — 2022. — Т. 111, № 1. — С. 8—14.

118. Constructions of polynomially complete quasigroups of arbitrary order / V. A. Artamonov, S. Chakrabarti, V. T. Markov, S. K. Pal // Journal of Algebra and Its Applications. — 2021. — Vol. 20, no. 12. — P. 2150236.

119. *Югай В. Л.* Об одном критерии полиномиальной полноты квазигрупп // Интеллектуальные системы. Теория и приложения. — 2017. — Т. 21, № 3. — С. 131—135.

120. *Халитова Р. Б.* О некоторых свойствах квазигрупп в криптографических приложениях : дис. … маг. / Халитова Р. Б. — МГУ имени М.В. Ломоносова, 2024. — выпускная квалификационная (дипломная) работа.

121. *Галатенко А. В., Панкратьев А. Е., Родин С. Б.* О полиномиально полных квазигруппах простого порядка // Интеллектуальные системы. Теория и приложения. — 2016. — Т. 20, № 3. — С. 194—198.

122. *Галатенко А. В., Панкратьев А. Е., Родин С. Б.* О полиномиально полных квазигруппах простого порядка // Алгебра и логика. — 2018. — Т. 57, № 5. — С. 509—521.

123. *Галатенко А. В., Панкратьев А. Е.* О сложности проверки полиномиальной полноты конечных квазигрупп // Дискретная математика. — 2018. — Т. 30, № 4. — С. 3—11.

124. *Galatenko A. V., Pankratiev A. E., Staroverov V. M.* Efficient verification of polynomial completeness of quasigroups // Lobachevskii Journal of Mathematics. — 2020. — Vol. 41, no. 8. — P. 1444—1453.

125. *Галатенко А. В., Панкратьев А. Е., Староверов В. М.* Проверка полиномиальной полноты n-квазигрупп // Алгебра, теория чисел и дискретная геометрия: современные проблемы, приложения и проблемы истории. — Тульский государственный педагогический университет им. Л.Н. Толстого. 2020. — Материалы XVIII Международной конференции, посвященной

столетию со дня рождения профессоров Б. М. Бредихина, В. И. Нечаева и С. Б. Стечкина.

126. *Галатенко А. В., Панкратьев А. Е., Староверов В. М.* Эффективность проверки полиномиальной полноты n-квазигрупп // Алгебра, теория чисел, дискретная геометрия и многомасштабное моделирование: современные проблемы, приложения и проблемы истории. — Тульский государственный педагогический университет им. Л.Н. Толстого. 2021. — Материалы XIX Международной конференции, посвященной двухсотлетию со дня рождения академика П. Л. Чебышёва.

127. *Торопов Н. А.* Алгоритм проверки наличия подквазигрупп в квазигруппе : дис. … маг. / Торопов Н. А. — МГУ имени М.В. Ломоносова, 2018. — выпускная квалификационная (бакалаврская) работа.

128. *Galatenko A. V., Pankratiev A. E., Staroverov V. M.* Algorithms for Checking Some Properties of n-Quasigroups // Programming and Computer Software. — 2022. — Vol. 48, no. 1. — P. 36—48.

129. *Галатенко А. В., Панкратьев А. Е., Староверов В. М.* Эффективность проверки существования n-подквазигрупп // Интеллектуальные системы. Теория и приложения. — 2021. — Т. 25, № 4. — С. 104—107.

130. *Мазурин А. Д.* Алгоритмы проверки существования подквазигрупп в конечных квазигруппах : дис. … маг. / Мазурин А. Д. — МГУ имени М.В. Ломоносова, 2023. — выпускная квалификационная (бакалаврская) работа.

131. *Szabó T., Welzl E.* Unique sink orientations of cubes // Proceedings 42nd IEEE Symposium on Foundations of Computer Science. — IEEE. 2001. — P. 547—555.

132. *Галатенко А. В., Носов В. А., Панкратьев А. Е.* Об одном критерии правильности семейства функций // Алгебра, теория чисел, дискретная геометрия и многомасштабное моделирование: современные проблемы, приложения и проблемы истории. — Тульский государственный педагогический университет им. Л.Н. Толстого. 2021. — Материалы XIX Международной конференции, посвященной двухсотлетию со дня рождения академика П. Л. Чебышёва.

133. *Schurr I.* Unique sink orientations of cubes : PhD thesis / Schurr I. — ETH Zurich, 2004.

134. *Галатенко А. В., Носов В. А., Панкратьев А. Е.* Об одном алгоритме построения правильных семейств функций // Алгебра, теория чисел и дискретная геометрия: современные проблемы, приложения и проблемы истории. — Тульский государственный педагогический университет им. Л.Н. Толстого. 2020. — Материалы XVIII Международной конференции, посвященной столетию со дня рождения профессоров Б. М. Бредихина, В. И. Нечаева и С. Б. Стечкина.

135. *Matousek J.* The Number Of Unique-Sink Orientations of the Hypercube // Combinatorica. — 2006. — Feb. — Vol. 26. — P. 91—99.

136. *Зуев Ю. А.* По океану дискретной математики. Том 1. — УРСС, 2012.

137. *Gao Y., Gartner B., Lamperski J.* A new combinatorial property of geometric unique sink orientations // arXiv preprint arXiv:2008.08992. — 2020.

138. *OEIS Foundation Inc.* The On-Line Encyclopedia of Integer Sequences. — 2008. — Published electronically at http://oeis.org.

139. *Finch S. R.* Mathematical constants. — Cambridge university press, 2003.

140. *Xu A.* Asymptotic expansion related to the generalized Somos recurrence constant // International Journal of Number Theory. — 2019. — Vol. 15, no. 10. — P. 2043—2055.

141. *Kauffman S. A.* Metabolic stability and epigenesis in randomly constructed genetic nets // Journal of Theoretical Biology. — 1969. — Vol. 22, no. 3. — P. 437—467. — URL: https://www.sciencedirect.com/science/article/pii/0022519369900150.

142. *Thomas R.* Boolean formalization of genetic control circuits // Journal of Theoretical Biology. — 1973. — Vol. 42, no. 3. — P. 563—585. — URL: https://www.sciencedirect.com/science/article/pii/0022519373902476.

143. *De Jong H.* Modeling and simulation of genetic regulatory systems: a literature review // Journal of computational biology. — 2002. — Vol. 9, no. 1. — P. 67—103.

144. *Thomas R.* Regulatory networks seen as asynchronous automata: a logical description // Journal of theoretical biology. — 1991. — Vol. 153, no. 1. — P. 1—23.

145. *Richard A.* Fixed point theorems for Boolean networks expressed in terms of forbidden subnetworks // Theoretical Computer Science. — 2015. — Vol. 583. — P. 1—26.

146. *Ruet P.* Asynchronous Boolean networks and hereditarily bijective maps // Natural Computing. — 2015. — Vol. 14. — P. 545—553.

147. *Ruet P.* Local cycles and dynamical properties of Boolean networks // Mathematical Structures in Computer Science. — 2016. — Vol. 26, no. 4. — P. 702—718.

148. *Shih M.-H., Dong J.-L.* A combinatorial analogue of the Jacobian problem in automata networks // Advances in Applied Mathematics. — 2005. — Vol. 34, no. 1. — P. 30—46.

149. *Robert F.* Iterations sur des ensembles finis et automates cellulaires contractants // Linear Algebra and its applications. — 1980. — T. 29. — P. 393-412.

150. *Sikirić M. D., Itoh Y., Poyarkov A.* Cube packings, second moment and holes // European Journal of Combinatorics. — 2007. — Vol. 28, no. 3. — P. 715—725.

151. *Mathew K. A., Östergård P., Popa A.* Enumerating cube tilings // Discrete & Computational Geometry. — 2013. — Vol. 50, no. 4. — P. 1112—1122.

152. *Borzechowski M., Doolittle J., Weber S.* A Universal Construction for Unique Sink Orientations // arXiv preprint arXiv:2211.06072. — 2022.

153. *Corrádi K., Szabó S.* A combinatorial approach for Keller's conjecture // Periodica Mathematica Hungarica. — 1990. — Vol. 21. — P. 95—100.

154. *Gartner B., Antonis T.* The Complexity of Recognizing Unique Sink Orientations // Leibniz International Proceedings in Informatics, LIPIcs. — 2015. — Mar. — Vol. 30.

155. *Красин В. Ю.* О слабых изометриях булева куба // Дискретный анализ и исследование операций. — 2006. — Т. 13, № 4. — С. 26—32.

156. *De Winter S., Korb M.* Weak isometries of the Boolean cube // Discrete Mathematics. — 2016. — Vol. 339, no. 2. — P. 877—885.

157. *Bruner R., De Winter S.* Weak isometries of Hamming spaces // Journal of Algebra Combinatorics Discrete Structures and Applications. — 2014. — Vol. 3, no. 3. — P. 209—216.

158. *Chirivi R.* The isometry group for the Hamming distance. — 2015. — http://annualreport.dmf.unisalento.it/2015/maths/algebra/chirivi1.pdf.

159. *Vajda S.* Fibonacci and Lucas numbers, and the golden section: theory and applications. — Courier Corporation, 2008.

160. Format-preserving encryption / M. Bellare, T. Ristenpart, P. Rogaway, T. Stegers // Selected Areas in Cryptography: 16th Annual International Workshop, SAC 2009, Calgary, Alberta, Canada. — Springer. 2009. — P. 295—312.

161. Format-preserving encryption algorithms using families of tweakable blockciphers / J.-K. Lee, B. Koo, D. Roh, W.-H. Kim, D. Kwon // Information Security and Cryptology-ICISC 2014: 17th International Conference, Seoul, South Korea. — Springer. 2015. — P. 132—159.

162. *Dworkin M.* Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption. — 2016. — NIST Special Publication 800-38G.

163. *Hoang V. T., Tessaro S., Trieu N.* The curse of small domains: new attacks on format-preserving encryption // Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA. — Springer. 2018. — P. 221—251.

164. Three third generation attacks on the format preserving encryption scheme FF3 / O. Amon, O. Dunkelman, N. Keller, E. Ronen, A. Shamir // Annual International Conference on the Theory and Applications of Cryptographic Techniques. — Springer. 2021. — P. 127—154.

165. *Katz J., Lindell Y.* Introduction to modern cryptography. — CRC press, 2020.

166. Межгосударственный стандарт ГОСТ 34.12-2018 Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры. — 2018.

167. Generic-case complexity, decision problems in group theory, and random walks / I. Kapovich, A. Myasnikov, P. Schupp, V. Shpilrain // Journal of Algebra. — 2003. — Vol. 264, no. 2. — P. 665—694.

168. *Яшунский А. Д.* О скорости сходимости квазигрупповых сверток вероятностных распределений // Дискретная математика. — 2022. — Т. 34, № 3. — С. 160—171.

169. О криптографических свойствах алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 / Е. К. Алексеев, И. Б. Ошкин, В. О. Попов, С. В. Смышляев // Математические вопросы криптографии. — 2016. — Т. 7, № 1. — С. 5—38.

170. *Allen T. E.*, *Goldsmith J.*, *Mattei N.* Counting, ranking, and randomly generating CP-nets // Workshops at the Twenty-Eighth AAAI Conference on Artificial Intelligence. — 2014.

171. *Bosshard V.*, *Gärtner B.* Pseudo unique sink orientations // arXiv preprint arXiv:1704.08481. — 2017.

Список рисунков

Список таблиц