Федеральное государственное бюджетное учреждение науки

Институт математики им. С. Л. Соболева
Сибирского отделения Российской академии наук

на правах рукописи

Потапов Владимир Николаевич

Дискретные функции и структуры в q-ичных гиперкубах

Специальность 01.01.09 — Дискретная математика и математическая кибернетика

Диссертация на соискание учёной степени
доктора физико-математических наук

Новосибирск — 2016

Содержание

Введение

§ 0.1. Основные определения и обозначения

В диссертации рассматриваются комбинаторные структуры в q-ичных гиперкубах с метрикой Хэмминга. Под комбинаторной структурой мы понимаем такое подмножество гиперкуба или дискретную функцию, на которой достигается максимум некоторой характеристики, такой как, например, мощность подмножества при сохранении метрической однородности. Хорошим примером такой структуры служат 1-совершенные коды, которые достигают границы Хэмминга плотной упаковки шаров и вследствие этого метрически однородно заполняют гиперкуб. Программа исследований комбинаторных объектов как правило состоит из следующих этапов: определение множества параметров, при которых возможно существование конкретной комбинаторной структуры; оценка количества различных структур при фиксированных параметрах; нахождение свойств, всегда присущих комбинаторным объектам этого типа; построение комбинаторных конфигураций с некоторыми дополнительными свойствами; конструктивное описание множества структур при некоторых параметрах. Перейдём к определению основных объектов исследования.

Пусть Q_q — конечное множество из q элементов. Без ограничения общности будем полагать, что $Q_q = \{0, 1, \ldots, q-1\}$. Множество Q_q^n, состоящее из наборов длины

n, называется *q-ичным n-мерным гиперкубом.* Множество позиций в наборах или номеров *координат* в гиперкубе будем обозначать через $[n] = \{1, \ldots, n\}$.

Расстоянием Хэмминга $d(x, y)$ между наборами $x, y \in Q_q^n$ называется число позиций, в которых наборы x и y различаются.

Графом минимальных расстояний дискретного метрического пространства (X, d) называется граф ΓX, вершинами которого являются точки множества X и каждая пара точек на минимальном ненулевом расстоянии соединена ребром. В частности, в графе ΓQ_k^n ребром соединены вершины, находящиеся на расстоянии Хэмминга равном 1. Граф ΓQ_k^n нередко называют *графом Хэмминга.* Через ΓB будем обозначать подграф порождённый множеством $B \subseteq Q_q^n$. Множество $B \subseteq Q_q^n$ будем называть двудольным, связным или гамильтоновым, если таков граф ΓB.

Шаром радиуса ρ с центром в вершине $x \in Q_q^n$ называется множество $B_\rho(x) = \{y \in Q_q^n \mid d(x, y) \leq \rho\}$.

Кодом называется произвольное подмножество $C \subseteq Q_q^n$, *кодовым расстоянием* минимальное расстояние между двумя различными вершинами кода.

t-Совершенным (исправляющим t ошибок) кодом в гиперкубе Q_q^n называется такое множество $C \subset Q_q^n$, что для любого $x \in Q_q^n$ найдётся ровно один $y \in C$ такой, что $d(x, y) \leq t$, т.е. шары радиуса t центрами в кодовых вершинах образуют разбиение гиперкуба Q_q^n. Очевидно кодовое расстояние t-совершенного кода равняется $2t + 1$.

Гранью размерности m называется подмножество гиперкуба Q_q^n, состоящее из вершин с одинаковыми фиксированными значениями в некоторых $n-m$ координатах. Например, множество

$$\{(x_1, \ldots, x_{i_1-1}, a_1, x_{i_1+1}, \ldots, a_{n-m}, x_{i_m+1}, \ldots, x_n) \mid x_1, \ldots, x_n \in Q_q\},$$

где значения $a_1, \ldots, a_{n-m} \in Q_q$ фиксированы, является гранью размерности m. Пусть $Q_{q*} = Q_q \cup \{*\}$. Множество граней гиперкуба Q_q^n взаимно однозначно соответствует словам из Q_{q*}^n. А именно, каждой m-мерной грани соответствует слово, содержащее m символов $*$ на тех позициях, которые не зафиксированы у наборов, лежащих в этой грани. Одномерные грани гиперкуба будем называть *линиями* , а $(n-1)$-мерные *слоями.*

Паросочетанием в графе называется набор непересекающихся по вершинам рёбер графа. Рёбрам графа ΓQ_2^n соответствуют (*линии*) в Q_2^n, т. е. паросочетанием в булевом (двоичном) гиперкубе является набором непересекающихся линий. Линии в q-ичном гиперкубе оказываются максимальными кликами в графе ΓQ_q^n, поэтому набор непересекающихся линий в q-ичном гиперкубе называется *кликосочетанием*. Паросочетание или кликосочетание называются *совершенными*, если покрывают все вершины гиперкуба.

Гамильтоновым циклом в графе называется путь, однократно проходящий через все вершины графа.

Ретрактом (сечением) множества $M \subset Q_q^n$ называется множество $M(a_1, \ldots, a_m, i_1, \ldots, i_m)$, полученное фиксацией одной или нескольких координат

$$M(a_1, \ldots, a_m, i_1, \ldots, i_m) = \{(x_1, \ldots, x_{n-m}) \mid (x_1, \ldots, x_{i_1-1}, a_1, x_{i_1}, \ldots, a_m, x_{i_m}, \ldots, x_{n-m}) \in M\}.$$

Проекцией множества $M \subset Q_q^n$ называется множество $M'(i_1, \ldots, i_m)$ наборов, полученных вычёркиванием координат из наборов, принадлежащих множеству M

$$M'(i_1, \ldots, i_m) = \{(x_1, \ldots, x_{n-m}) \mid \exists(a_1, \ldots, a_m), \quad (x_1, \ldots, x_{i_1-1}, a_1, x_{i_1}, \ldots, a_m, x_{i_m}, \ldots, x_{n-m}) \in M\}.$$

Множество $C \subset Q_q^n$ называется МДР-*кодом с (кодовым) расстоянием* ρ, если $|C \cap \Gamma| = 1$ для каждой грани Γ размерности $\rho - 1$.

Подмножество $M \subseteq Q_q^n$ называется t-*кратным* МДР-кодом с расстоянием ρ, если оно пересекается с каждой гранью гиперкуба размерности $\rho - 1$ ровно по t элементам ($|M \cap \Gamma| = t$). Двукратные МДР-коды с расстоянием 2 будем называть 2-МДР-*кодами*.

Функция $f : Q_q^n \to \{0, \ldots, k-1\}$ называется *корреляционно-иммунной порядка* $n - m$, если для любого $a \in \{0, \ldots, k-1\}$ величина $|f^{-1}(a) \cap \Gamma|$ не зависит от выбора m-мерной грани Γ. Обозначим через $\mathrm{cor}(f)$ максимальный порядок иммунности функции f. Если C есть МДР-код (возможно кратный) с расстоянием ρ, то $\mathrm{cor}(\chi^C) = n - \rho + 1$, где χ^C — характеристическая функция множества C.

Функция $f : Q_q^n \to Q_q$ называется n-*арной квазигруппой порядка* q *(мультиарной квазигруппой)*, если она обратима по каждой своей переменной, т. е. отображение, полученное из f произвольной фиксацией всех переменных кроме одной (одномер-

ный ретракт) является биекцией. Для мультиарных квазигрупп конечного порядка условие обратимости эквивалентно следующему: для любых $x, y \in Q_q^n$ из $d(x, y) = 1$ следует, что $f(x) \neq f(y)$.

Таблица значений n-арной квазигруппы называется *латинским n-кубом (гипер-кубом)*, при $n = 2$ — *латинским квадратом*. Например,

0	1	2	3
1	0	3	2
2	3	1	0
3	2	0	1

Нетрудно видеть, что функция $f : Q_q^n \to Q_q$ является n-арной квазигруппой тогда и только тогда, когда её график $\mathcal{M}\langle f\rangle = \{(x, f(x)) \mid x \in Q_q^n\}$ является МДР-кодом с расстоянием 2.

Ретрактом функции $f : Q_q^n \to Q_q$ называется функция $f' : Q_q^m \to Q_q$, полученная из f фиксацией нескольких переменных[1].

Совершенной раскраской гиперкуба Q_q^n в k цветов называется отображение $Col : Q_q^n \to \{0, 1, \ldots, k-1\}$, удовлетворяющее следующему условию: мощность пересечения $|Col^{-1}(i) \cap B_1(x)|$ зависит только от цветов i и $Col(x)$, но не от вершины $x \in Q_q^n$.

Каждой совершенной раскраске соответствует матрица параметров $P = \{p_{ij}\}$, где p_{ij} — число вершин цвета j в сфере радиуса 1 с центром в вершине цвета i.

В дальнейшем рассматриваются только раскраски в два цвета (2-раскраски). В двуцветном $\{0, 1\}$ случае функция Col является булевозначной и $Col = \chi^C$, где C — множество вершин цвета 1.

В частности, характеристические функции 1-совершенного кода и МДР-кода с расстоянием 2 в гиперкубе Q_q^n являются совершенными раскрасками с матрицами параметров $P_1 = \begin{pmatrix} 0 & (q-1)n \\ 1 & (q-1)n-1 \end{pmatrix}$ и $P_2 = \begin{pmatrix} 0 & (q-1)n \\ n & (q-2)n \end{pmatrix}$ соответственно.

Изотопией гиперкуба называется преобразование $\overline{x} \mapsto \overline{\tau x}$, где $\overline{x} = (x_1, \ldots, x_n) \in Q_q^n$, $\overline{\tau x} = (\tau_1 x_1, \ldots, \tau_n x_n)$, $\tau_i \in S_q$ — перестановки на множестве Q_q, $i \in [n]$. *Парастрофией* гиперкуба называется преобразование $\overline{x} \mapsto \overline{x}_\varepsilon$, где $\overline{x}_\varepsilon = (x_{\varepsilon 1}, \ldots, x_{\varepsilon n})$, $\varepsilon \in S_n$ —

[1] Ретрактом n-арной квазигруппы f принято называть мультиарные квазигруппы, графики которых являются ретрактами множества $\mathcal{M}\langle f\rangle$.

перестановка координат. Введём обозначения $A_\varepsilon = \{\overline{x}_\varepsilon \mid \overline{x} \in A\}$, $\overline{\tau}A = \{\overline{\tau x} \mid \overline{x} \in A\}$. Определим группу автотопий $\mathrm{Ist}(A) = \{\overline{\tau} \mid \overline{\tau}A = A\}$ и группу парастрофий $\mathrm{Prs}(A) = \{\varepsilon \mid A_\varepsilon = A\}$, переводящих множество $A \subseteq Q_q^n$ в себя. Известно (см. [41]), что группа изометрий гиперкуба Q_q^n представима в виде полупрямого произведения $\mathrm{Ist}(Q_q^n) \leftthreetimes \mathrm{Prs}(Q_q^n)$. Подгруппу группы изометрий гиперкуба, переводящую множество $A \subseteq Q_q^n$ в себя обозначим $\mathrm{Aut}(A)$.

Множества $A, B \subseteq Q_q^n$ называются *изотопными*, если они переводятся друг в друга изотопией, и *эквивалентными*, если они переводятся друг в друга изометрией гиперкуба Q_q^n. Мультиарные квазигруппы называются изотопными (эквивалентными), если изотопны (эквивалентны) их графики.

Множество $A \subseteq Q_q^n$ называется *транзитивным*, если группа изометрий $\mathrm{Aut}(A)$ действует транзитивно на A, т. е. для любых двух вершин $\overline{x}, \overline{y}$ из A найдутся парастрофия $\varepsilon \in \mathrm{Prs}(Q_q^n)$ и изотопия $\overline{\tau} \in \mathrm{Ist}(Q_q^n)$ такие, что $\overline{\tau y} = \overline{x}_\varepsilon$ и $\overline{\tau}A = A_\varepsilon$. Множество $A \subseteq Q_q^n$ называется *изотопно транзитивным*, если группа $\mathrm{Ist}(A)$ действует транзитивно на A.

§ 0.2. Цели исследования

Основной целью исследований, в рамках которых подготовлена диссертация, является конструктивное описание известных комбинаторных объектов: латинских гиперкубов, совершенных кодов, корреляционно-иммунных функций, гамильтоновых циклов в булевом кубе.

Конструктивная классификация должна обеспечивать не только перечисление объектов классифицируемого типа, но и возможность проверки наличия естественным образом определённых свойств для конкретной комбинаторной конфигурации. Исследования по классификации перечисленых выше комбинаторных объектов далеки от завершения, но на основе уже полученных результатов (конструктивное описание n-арных квазигрупп порядка 4) удалось доказать некоторые свойства латинских гиперкубов и совершенных кодов, а также построить серии этих объектов с дополнительными свойствами, в частности, транзитивных.

Обнаружение комбинаторных объектов с трудносочетаемыми свойствами всегда являлось одной из приоритетных задач комбинаторики. Построение комбинаторных объектов новых типов, как правило удовлетворяющих некоторому набору экстремальных свойств, которые ранее не удавалось совместить, также может рассматриваться как цель данной диссертации. Полученные здесь результаты ограничиваются конструкциями блок-схем (дизайнов) с новыми параметрами и нерасщепляемых МДР-кодов.

§ 0.3. Исторический обзор

С точки зрения теории дискретных функций n-арные квазигруппы конечного порядка представляют собой замкнутый (относительно операций суперпозиции и взятия ретракта) класс дискретных функций, с точки зрения алгебры — класс алгебраических систем с n-арной операцией, содержащий при $n = 2$ конечные группы. В комбинаторике начало изучению эквивалентных n-арным квазигруппам объектов — латинских квадратов и гиперкубов было положено Л.Эйлером. Дифференцируемые n-арные квазигруппы (n-ткани) над полями вещественных и комплексных чисел рассматриваются в непрерывной математике как класс отображений, состоящий из функций n переменных, обратимых по каждой переменной (см., например, [17]). Важность специального изучения такого естественного комбинаторно-алгебраического объекта как n-арные квазигруппы подчёркивалась А.Г.Курошем в сборнике лекций по общей алгебре [37]. Значительный вклад в изучение n-арных квазигрупп в 70–80 годах прошлого столетия внесла научная школа В.Д.Белоусова [4].

В настоящее время возрождению интереса к n-арным квазигруппам способствует их связь с помехоустойчивыми кодами и корреляционно-имунными функциями, что обеспечивает возможность приложения результатов исследований в теории кодирования [171], [31], [26], [127] и криптографии [14], [15], [66], [177].

В настоящей работе n-арные квазигруппы конечного порядка рассматриваются преимущественно с комбинаторной точки зрения. Это означает, что преимуществен-

но рассматриваются те свойства n-арных квазигрупп, которые инвариантны относительно естественных преобразований изотопии (перестановка в области задания аргумента функции) и парастрофии (перестановки аргументов). Эти преобразования сохраняют комбинаторные свойства функций, но могут изменить алгебраические (например, ассоциативность).

Мультиарные квазигруппы, представимые в виде бесповторной суперпозиции мультиарных квазигрупп от меньшего числа аргументов, называются разделимыми (приводимыми). Вопрос о представимости функции суперпозицией функций от меньшего числа переменных имеет важное значение как в непрерывной (13-я проблема Гильберта), так и в дискретной (классы Поста) математике. Естественный вопрос о существовании неразделимых n-арных квазигрупп известен как одна из проблем В.Д. Белоусова [4]. Частичное решение (для некоторых порядков или для более узкого определения понятия суперпозиции) этой проблемы содержится в работах В.Д.Белоусова и М.Д.Сандика [5], Б.Р.Френкина [70], В.В.Борисенко [6], М.М.Глухова [12], [13], М.А.Акивиса и В.В.Гольдберга [78]. В [148] проблема Белоусова была решена полностью, а именно, были построены неразделимые n-арные квазигруппы для любого порядка $q > 3$ и $n > 2$.

Другим важным направлением в изучении мультиарных квазигрупп является обнаружение связей между разделимостью n-арной квазигруппы и её ретрактов. Подробное исследование этого вопроса имеется в статьях [36], [145], [147], [154]. Исследование связей между приводимостью (представимостью в виде суперпозиции с учётом порядка переменных) n-арных квазигрупп и их ретрактов опубликовал Т.Заславски [192], [191]. В целом, при рассмотрении представимости n-арных квазигрупп в виде бесповторной суперпозиции крайне полезным фактом является каноническое разложения мультиарной квазигруппы в суперпозицию. Существование и единственность (в определенном смысле, см. § 1.2) такого представления было доказано А.В.Черёмушкиным [73]. Стоит отметить, что подобные представления возможны для значительно более широкого класса функций, чем n-арные квазигруппы (см. [184], [74]).

Представимость функций из некоторого класса в виде суперпозиции функций

от меньшего числа переменных позволяет рекуррентно описывать этот класс функций, на каждом шаге увеличивая на единицу число переменных. Как указано выше, начиная с порядка 4, такое описание класса мультиарных квазигрупп невозможно. Имеется множество исследований по классификации n-арных квазигрупп порядка q (латинских гиперкубов) для малых n и q с помощью компьютера [165], [133], [27], [29] [131], [183], [161], [162], [130]. В частности, в работе Б.Мак-Кэя и Я.Уонлеса [163] найдено число латинских n-мерных кубов порядка 5 до $n = 4$ и порядка 6 до $n = 3$, причем подсчитано также число классов эквивалентности латинских гиперкубов при тех же параметрах. Продвинуться в существенно большие размерности при помощи переборных алгоритмов не представляется возможным, так как число объектов растет дважды экспоненциально по n. При фиксированной размерности и растущем порядке верхняя асимптотическая оценка числа мультиарных квазигрупп получена Л.Линиалом и З.Лурией [160]. При фиксированном порядке и растущей размерности верхняя и нижняя асимптотические оценки числа мультиарных квазигрупп имеются в [55]. Наиболее важным результатом в области теоретического описания мультиарных квазигрупп является конструктивная классификация n-арных квазигрупп порядка 4 [150] и нахождение рекурретной формулы для их числа [55].

Из классической теоремы Кёнига — Холла [72], [141], [121] следует, что любой латинский прямоугольник $n \times m$ можно продолжить до латинского квадрата $n \times n$. Однако были обнаружены латинские параллелепипеды, которые невозможно продолжить до латинских кубов [115], [129], [138]. К настоящему времени построены примеры непродолжаемых латинских параллелепипедов всех порядков, начиная с порядка 5. Наиболее широкое множество параметров непродолжаемых латинских параллелепипедов найдено в работах Д.Брайанта с соавторами [93] и М.Кохола [140]. С другой стороны, доказано, что латинские параллелепипеды вида $4 \times \cdots \times 4 \times m$ всегда продолжаемы до латинского гиперкуба порядка 4 (см. [51]).

Как было указано выше, график мультиарной квазигруппы является МДР-кодом с кодовым расстоянием 2. Теория разделимых кодов с максимальным расстоянием (МДР-коды) в классической монографии Ф.Дж.Мак-Вильямс и Н.Дж.А.Слоэна «Теория кодов, исправляющих ошибки» [40] названа "одним из самых удивительных

разделов во всей теории кодирования". Линейные МДР-коды, в частности, класс циклических МДР-кодов, известных как коды Рида — Соломона, широко применяются для передачи сообщений по каналам связи с помехами. Центральной математической задачей при исследовании классов кодов является определение возможных параметров: длины кода, мощности кода и кодового расстояния. С.Болом [84], [85] доказано, что за исключением расстояний 2 и n линейный q-ичный МДР-код не может иметь длину, большую чем $q+1$ (или $q+2$, если q - степень двойки). Линейные МДР-коды, достигающие этой границы, были известны ранее (см. [40]). Построение нелинейных МДР-кодов представляет значительный интерес, например, в связи с возможными приложениями в криптографии. Здесь следует отметить работы по рекурсивным МДР-кодам А.А.Нечаева с соавторами [18], [19], в которых предлагается оригинальный подход к построению нелинейных МДР-кодов с большими расстояниями, и обзор М.М.Глухова [15], в котором описаны методы построения МДР-кодов на основе теории групп.

Нелинейные МДР-коды с любыми кодовыми расстояниями могут бы представлены системой ортогональных мультиарных квазигрупп (ортогональных латинских гиперкубов). Впервые ортогональные латинские квадраты (греко-латинские квадраты) были рассмотрены Л.Эйлером. Проблема существования систем ортогональных латинских квадратов (порядков, не равных степени простого числа) является одной из центральных в комбинаторике (см. монографии [105], [126]). В [108] представлен обзор результатов по ортогональным системам функций. Связи теории систем ортогональных квадратов с такими комбинаторными объектами как ортогональные массивы и конечные геометрии рассмотрены, например, в учебнике Ю.В.Таранникова [64]. Системы ортогональных латинских кубов применяются в теории оптимизации, например, при рассмотрении многоиндексной задачи выбора (см. [23]).

Другим направлением применения n-арных квазигрупп в теории кодирования являются совершенные раскраски гиперкубов и, в частности, 1-совершенные коды. Понятие совершенной раскраски графа неоднократно возникало в комбинаторике под разными названиями. Эквивалентные совершенной раскраске понятия (partition design, equitable partition, дистрибутивная раскраска) определяются в работах клас-

сиков комбинаторики: П.Дельсарта с соавторами [99], С.Д.Годсила [117], В.Г.Визинга [10]. В [63] совершенные 2-раскраски в булевом гиперкубе называются (c_0, c_1)-регулярными функциями. Наиболее полное описание множеств параметров, при которых существуют или не существуют раскраски булева гиперкуба в два цвета, получено Д.Г.Фон-Дер-Флаассом ([68], [69], [113]). Известным частным случаем совершенных раскрасок в несколько цветов являются полностью регулярные коды, определённые П.Дельсартом [104], серия работ на эту тему опубликована В.А.Зиновьевым с соавторами (см., например, [28]). В свою очередь частным случаем полностью регулярных кодов являются совершенные коды. Характеристическая функция совершенного кода, исправляющего одну ошибку (1-совершенного кода или совершенного кода с расстоянием 3), является совершенной 2-раскраской q-ичного гиперкуба. Известны конструкции В.А.Зиновьева [25], К.Т.Фелпса [171], О.Хедена и Д.С.Кротова [127], позволяющие строить 1-совершенные коды из МДР-кодов с расстоянием 2 (графиков мультиарных квазигрупп). В [50] конструкция Зиновьева — Фелпса обобщена для построения совершенных раскрасок в булевом кубе с другими параметрами. Число совершенных раскрасок булева гиперкуба в два цвета оценивается в [11] и [50].

В 1973 году В.А.Зиновьев, В.К.Леонтьев [24] и А.Тиетвайнен [188] полностью описали все возможные параметры совершенных кодов в q-ичных гиперкубах, если $q = p^s$ — степень простого. Оказалось, что за исключением кодов Голея[2] [118] d-совершенные коды в Q_q^n $(0 < d < n)$ существуют только при $d = 1$ и все эти коды имеют параметры линейных кодов Хэмминга. В 1962 году Ю.Л.Васильев [8] предложил плодовитую конструкцию нелинейных 1-совершенных кодов. Возникла проблема классификации таких кодов. В последние годы получено несколько важных результатов в направлении описания 1-совершенных кодов. В частности, перечислены все совершенные коды длины 15 ([167], [168]), что обеспечивает достаточную базу для контрпримеров к старым гипотезам и формулировки новых предположений о 1-совершенных кодах произвольной длины. Д.С.Кротов ([151], [155], [153]) продолжил эти исследования и, используя методы развитые для описания совершенных раскра-

[2] Коды Голея являются линейными кодами с параметрами $q = 3$, $d = 2$, $n = 11$; $q = 2$, $d = 2$, $n = 23$.

сок, получил перечисление оптимальных кодов (с расстоянием 3) длины меньшей чем 15. Наилучшие на сегодня асимптотические нижние оценки числа 1-совершенных двоичных и q-ичных кодов получены в работах С.В.Августиновича и Д.С.Кротова ([149]) и, соответственно, О.Хедена и Д.С.Кротова [127]. Обе оценки получены конструктивно, причём во втором случае конструкция явным образом основывается на МДР-кодах и нижних оценках числа МДР-кодов из [55]. Имеющиеся нижние оценки числа совершенных кодов весьма далеки от верхних (см. [1], [59]), что свидетельствует о том, что описание всех 1-совершенных кодов ещё далеко до завершения. В связи с этим представляется весьма актуальным описание некоторых классов совершенных кодов, в частности, в работе С.В.Августиновича, О.Хедена и Ф.И.Соловьёвой [80], предложено описание совершенных кодов малого (не более чем на 2 превышающего ранг линейного 1-совершенного кода той же длины) ранга посредством 4-ичных МДР-кодов. Этот результат в объединении с конструктивным описанием 4-ичных МДР-кодов [150] позволяет получить характеризацию таких 1-совершенных кодов. Что в свою очередь позволяет решить вопросы о принадлежности этих кодов свитчинговому классу кода Хэмминга ([35]) и о транзитивности кодов из этого класса ([48]).

Транзитивные коды так же как и линейные коды обладают свойством алгебраической однородности, что позволяет строить эффективные алгоритмы их кодирования и декодирования. При исследовании симметрий (групп автоморфизмов) мультиарных квазигрупп удобнее рассматривать представление мультиарной квазигруппы в виде её графика — МДР-кода, как более симметричное (без выделенной координаты — значения функции). Среди транзитивных кодов наиболее известны Z_4-линейные. Особенно интересна возможность построения транзитивных кодов с параметрами, для которых не существует линейных кодов. Интерес к Z_4-линейным кодам был вызван пионерскими работами [124], [43] и сохраняется до настоящего времени. Полное описание всех Z_4-линейных кодов Адамара ([144]) и 1-совершенных кодов ([32]) было сделано Д.С.Кротовым. Транзитивные коды, на множестве вершин которых возможно задание групповой операции, являющейся изометрией гиперкуба, называются *предлинейными (properlinear)*. Транзитивные и предлинейные 1-совершенные

коды исследованы в цикле работ Ф.И.Соловьёвой с соавторами ([61], [88], [89], [120]). Коды, на которых транзитивно действует группа автотопий, называются *изотопно транзитивными*. При $q = 2$ понятие изотопной тразитивности совпадает с понятием аффинности множества. Для луп изотопная транзитивность эквивалентна свойству быть G-лупой (см. [156]). В [189] показано, что при простом порядке q любая G-лупа является группой (циклической), в [158] аналогичный результат был получен для $q = 3p$, где $p > 3$ — простое. С другой стороны в [119] показано, что для любого непростого порядка q, за возможным исключением случая, когда в разложении числа q на простые отсутствует 2 и кратные сомножители, имеются G-лупы порядка q, не эквивалентные группам. Семейство изотопно транзитивных МДР-кодов порядка 4 почти экспоненциальной мощности (при растущей длине кода) построено в [48]. В [156] изотопно транзитивные МДР-коды порядка 4 конструктивно описаны и построены семейства изотопно транзитивных МДР-кодов сверхэкспоненциальной мощности для порядков, делящихся на квадрат простого числа. В [?] утверждается, что МДР-коды порядка 4 любой размерности имеют нетривиальную группу автотопий, в то время как латинские квадраты порядка q (МДР-коды размерности 3) почти все имеют тривиальную группу автоморфизмов при $q \to \infty$.

Равномерность распределения по граням (корреляционная иммунность) — одна из важнейших характеристик булевозначной функции в криптографии. Максимальной корреляционной иммунностью среди не постоянных функций обладают характеристические функции МДР-кодов (возможно кратных) с расстоянием 2, однако в булевом и троичном гиперкубах имеется всего лишь один с точностью до эквивалентности МДР-код с расстоянием 2. Таким образом, построение достаточно больших семейств булевых функций с высокой корреляционной иммунностью является отдельной задачей. Для этого требуются как плодовитые конструкции, так и точные верхние оценки возможного значения иммунности. Сводка результатов по этой тематике имеется в обзоре Ю.В.Таранникова [63]. Оценку корреляционной иммунности булевой функции через её плотность (долю единиц) даёт неравенство Бирбрауэра — Фридмана ([87], [114]). В работе [53] данное неравенство удалось усилить. Оценка числа корреляционно-иммунных функций с высокой иммунностью имеется в упомя-

нутой выше работе Ю.В.Таранникова, асимптотические оценки числа булевых функций с малой и средней иммунностью имеются в работах О.В.Денисова [20], К.Карле [95] и Б.Маккея с соавторами [94]. Важнейший результат в области корреляционно-иммунных функций был получен Д.Г.Фон-Дер-Флаассом [113]. Он доказал, что порядок корреляционной иммунности неуравновешенных (с плотностью единиц менее $1/2$) неконстантных булевых функций в n-мерном булевом кубе не превышает $\frac{2n}{3} - 1$ (ранее функции достигающие этой границы были построены Ю.В.Таранниковым [63]). Кроме того, им доказано, что неуравновешенная функция, достигающая максимальной корреляционной иммунности, является совершенной 2-раскраской. В работах [50], [53] удалось получить аналогичный результат для функций, достигающих границы Бирбрауэра — Фридмана. Аналогичный результат для совершенных кодов имеется в [168]. Для раскраски гиперкуба в два цвета 0 и 1 совершенность означает, что единицы функции раскраски регулярным образом распределены по шарам (в метрике Хэмминга). Таким образом, в случае максимальной корреляционной иммунности для данной плотности из равномерной распределённости единиц функции по граням n-мерного куба следует регулярная распределённость единиц функции по шарам. Обратное: из регулярной распределённости единиц булевозначной функции по шарам следует равномерная распределённость по граням, тоже верно и было известно ранее (см. [63]).

Одним из основных методов исследований экстремальных комбинаторных объектов в q-ичных гиперкубах является метод *свитчинга компонент*. Этот метод состоит в многократном применении таких локальных преобразований, которые не выводят комбинаторный объект из рассматриваемого класса. Решающий вклад в разработку метода свитчинга компонент принадлежит новосибирским математикам Ю.Л.Васильеву, С.В.Августиновичу, Ф.И.Соловьёвой, С.А.Малюгину и Д.С.Кротову. В настоящее время метод свитчинга получил широкое признание, свидетельством которому является обзорная статья П.Остергарда [166]. Компонентой дискретной функции (в частности характеристической функции кода) называется множество вершин, на котором функция отличается от другой функции с теми же параметрами. Нередко рассматриваются специальные типы компонент, например, i-компоненты со-

вершенных кодов и $\{a, b\}$-компоненты мультиарных квазигрупп. Коды или функции, получаемые друг из друга многократным свитчингом (заменой) компонент специального вида, называют свитчингово связными. Компонента связности множества, на котором n-арная квазигруппа принимает два различных значения $a, b \in Q_k$, называется $\{a, b\}$-компонентой n-арной квазигруппы. Ясно, что перемена мест двух значений в некоторой компоненте приводит к новой n-арной квазигруппе. Нетрудно видеть, что компоненте n-арной квазигруппы соответствует подмножество гиперкуба, мощность пересечения которого с любой линией гиперкуба равна двум или нулю. Это свойство было взято за определение унитрейда (см. [56]). В трёхмерном кубе двудольным унитрейдам соответствуют латинские битрейды. Обзор результатов, полученных при изучении латинских битрейдов, имеется в [98]. Все возможные унитрейды мощности не более 2^{n+1} в n-мерном гиперкубе произвольного порядка перечислены в [56].

Нетрудно видеть, что компоненты корреляционно-иммунных функций в гиперкубе должны содержать чётное число точек в любых гранях фиксированной (определённой порядком иммунности) размерности. В булевом гиперкубе это свойство прямо соответствует алгебраической степени характеристической функции компоненты (см., например, [38]). Как известно, вектора значений булевых функций ограниченной алгебраической степени в n-мерном булевом кубе являются точками кода Рида — Маллера в 2^n-мерном кубе. Таким образом, вопрос о существовании компонент заданной мощности оказывается тесно связан с исследованием весовых спектров кодов Рида — Маллера. Наибольшие продвижения в этом вопросе были достигнуты в работах Т.Касами и Н.Токуры [134], [135].

Мощность минимальной компоненты функции является минимальным расстоянием от неё до другой функции с теми же параметрами. Следовательно, изучение компонент дискретных функций некоторого типа тесно связано с вопросом о числе таких функции и об их конструктивном перечислении. Исследование вопроса о мощностях пересечений 1-совершенных кодов (или о мощностях компонент кодов) начато Т.Этционом и А.Варди [110] и продолжено в работах С.В.Августиновича и Ф.И.Соловьёвой с соавторами ([9], [62], [81], [82], [79], [128]). Известны миниманль-

ные мощности компонент 1-совершенного кода, бент-функции (см. [30]), совершенной 2-раскраски (см. [50]). В [51], основываясь на результатах Т. Касами и Н. Токуры, показано, что мощности компонент совершенных кодов и раскрасок, корреляционно-иммунных и бент-функций в промежутке между 2^k и 2^{k+1} может принимать только значения вида $2^{k+1}-2^p$, где $p \in \{0,\dots,k\}$ и 2^k — минимальная мощность компоненты для комбинаторного объекта с теми же параметрами. Для бент-функций доказано существование компонент любой мощности из данного спектра. Для совершенных раскрасок с некоторыми параметрами и корреляционно-иммунных функций найдены компоненты некоторых из указанных выше мощностей.

Комбинаторные H-схемы (H-дизайны) были предложены Х.Ханани в [125] как обобщение систем Штейнера. Определение H-схемы сформулированное ниже было дано У.Милсом в [164]. Путь X множество точек и $C = \{C_1,\dots,C_n\}$ есть разбиение множества X на n не пересекающихся множеств мощности q. *Трансверсалью* разбиения C называется подмножество в X, пересекающиеся с каждым из множеств C_i не более чем по одному элементу. Множество w-элементных трансверсалей C называется *блок-схемой (дизайном) типа* $H(n,q,w,t)$ (кратко, H-схемой), если каждая t-элементная трансверсаль в C содержится точно в одной трансверсали H-схемы. Другим обобщением систем Штейнера являются A-схемы (A-дизайны), идея специального рассмотрения этих комбинаторных объектов принадлежит С.В.Августиновичу. Множество t-элементных трансверсалей разбиения C называется *блок-схемой (дизайном) типа* $A(n,q,w,t)$ (кратко, A-схемой) если каждая w-элементная трансверсаль разбиения C содержит точно одну трансверсаль из A-схемы. Здесь и далее подразумевается, что $n \geq w \geq t \geq 1$,то $q \geq 1$ и все эти числа целые.

Напомним, что $Q_q = \{0,1,\dots,q-1\}$ и $Q_{q*} = Q_q \cup \{*\}$. Ясно, что каждая w-трансверсаль разбиения C соответствует *слову* $u = (a_1,\dots,*,\dots,a_i,\dots,*,\dots,a_n) \in Q^n_{q*}$, где a_i — номер элемента множества C_i, который принадлежит w-трансверсали. На позиции j в слове u находится символ $*$ тогда и только тогда, когда w-трансверсаль не пересекается с C_j. Определим *вес* слова u из Q^n_{q*} как n минус число символов $*$ в слове u. Тогда множество H, состоящее из слов $x \in Q^n_{q*}$ веса w, является комбинаторной схемой типа $H(n,q,w,t)$, если каждое слово $y \in Q^n_{q*}$ веса t покрывается точно

одним словом $x \in H$. Аналогично множество A, состоящее из слов $y \in Q^n_{q*}$ веса t, является комбинаторной схемой типа $A(n, q, w, t)$ если каждое слово $x \in Q^n_{q*}$ веса w покрывает точно одно слово $y \in A$. Поскольку каждой k-мерной грани гиперкуба Q^n_q соответствует слово, содержащее k символов $*$, схема типа $H(n, q, w, t)$ является однократным протыканием всех $(n-t)$-мерных граней Q^n_q гиперкуба $(n-w)$-мерными гранями, соответствующими словам из H-схеме. Аналогичным образом схема типа $A(n, q, w, t)$ является покрытием $(n-t)$-мерными гранями всех $(n-w)$-мерных граней гиперкуба Q^n_q.

Если $q = 1$, то комбинаторная схема типа $H(n, 1, w, t)$ является в точности системой Штейнера $S(t, w, n)$ (где символы $*$ заменены на 0 и 0 заменены на 1). В то же время схемы типа $A(n, 1, w, t)$ является системой Штейнера $S(n-w, n-t, n)$ (где символы $*$ заменены на 1). В [28] H-схемы названы q-арными системами Штейнера. Множество T, состоящее из слов $y \in Q^n_{1*}$ веса t называется (n, w, t)-системой Турана, если каждое слово $x \in Q^n_{1*}$ веса w покрывает как минимум один из элементов $y \in T$. Следовательно схема типа $A(n, 1, w, t)$ является частным случаем (n, w, t)-системы Турана.

В случае $w = n$ комбинаторные схемы типа $H(n, q, w, t)$ являются в точности МДР-кодами в гиперкубе Q^n_q с кодовым расстоянием $d = n - t + 1$. Если $w = n$ и $t = n - 1$, то схема типа $A(n, q, w, t)$ является замощением гиперкуба одномерными гранями. Если, кроме того $q = 2$, то замощение оказывается совершенным паросочетанием[3] в Q^n_2. Если $q > 2$, то схема типа $A(n, q, n, n-1)$ называется *совершенным кликосочетанием*, поскольку 1-мерные грани гиперкуба, соответствуют максимальным кликам в гиперкубе, снабжённым метрикой Хэмминга.

Нетрудно видеть, что схемы типа $H(n, q, n, n-1)$ и $A(n, q, n, t)$ существуют для любых $q \geq 2$ and $n \geq 2$. У.Миллс в [164] показал, что при $n > 3$ $(n \neq 5)$ схемы типа $H(n, q, 4, 3)$ существуют тогда и только тогда, когда число nq чётно и число $q(n-1)(n-2)$ делится на 3. Л.Джи в [132] доказал, что схема типа $H(5, q, 4, 3)$ существуют, если число q чётно, причём $q \neq 2$ и $q \not\equiv 10, 26 (\mathrm{mod} 48)$. Множество линий называется *точным кликосочетанием*, если оно одновременно является схемой типа

[3] Предполагается, что гиперкуб снабжён метрикой Хэмминга.

$H(n, q, n-1, n-2)$ и типа $A(n, q, n, n-1)$. Точные кликосочетания (и разбиения на точные кликосочетания) при $n = 2^{t+1}$ и $q = 2^t$ построены в [52].

Рассмотрим схемы типа $H(n, q, w, t)$ как код постоянного веса. Расстояние Хэмминга[4] между двумя словами H-схемы всегда больше чем $w - t$, с другой стороны кодовое расстояние схемы типа $H(n, q, w, t)$ не превышает $2(w-t+1)$. Дизайны типа $H(n, q, w, t)$, являющиеся кодами с расстоянием $2(w - t + 1)$ называются обобщёнными системами Штейнера (см. [109]). Отметим, что система Штейнера (схема типа $H(n, 1, w, t)$) всегда является кодом с расстоянием равным $2(w - t + 1)$.

Т.Этцион в [109] построил ряд конструкций обобщённых систем Штейнера, которые являются комбинаторными схемами типов $H(n, q, 3, 2)$ и $H(n, 2, 4, 3)$. Он доказал, что обобщённые системы Штейнера типа $H(n, 2, 3, 2)$ существуют тогда и только тогда, когда $n \equiv 0$ или $1 (\mathrm{mod}\, 3)$, $n \geq 4$, $n \neq 6$.

Подобным образом можно рассмотреть схемы типа $A(n, q, w, t)$ с максимальным кодовым расстоянием. Кодовое расстояние A-схемы не превосходит $1+2(w-t)$ (однако может равняться 1). Комбинаторные схемы типа $A(n, 2, n, n-1)$ с расстоянием 2 были впервые построены в [122] для любого $n \geq 4$. Д.С.Кротов [33] и М.А.Сванстрём [186] доказали (в терминологии совершенных паросочетаний и кодов постоянного веса), что схемы типа $A(n, 2, n, n-1)$ с кодовым расстоянием 3 существуют тогда и только тогда, когда $n = 2^t$. Это прямо следует из того, что каждая схема типа $A(n, 2, n, t)$ с кодовым расстоянием $1 + 2(n - t)$ является совершенных тернарным кодом постоянного веса.

Известно, что число совершенных паросочетаний в двудольном графе равняется перманенту матрицы смежности графа и отлично от нуля для любого регулярного графа (теорема Кёнига). Л. М. Брэгман [7] доказал верхнюю оценку для перманента квадратной $(0, 1)$-матрицы, из которой непосредственно следует верхняя оценка $(n!)^{\frac{N}{n}}$ для числа различных совершенных паросочетаний в n-регулярном (n-однородном) двудольном графе с $2N$-вершинами.

Квадратная матрица, состоящая из неотрицательных элементов, называется *дважды стохастической*, если суммы элементов в каждой строке и в каждом столбце

[4] Элементы схемы рассматриваются как слова в алфавите $\{*, 0, \ldots, q-1\}$.

этой матрицы равны 1. В 1980 году Г.П.Егорычев [22] и Д.И.Фаликман [67] доказали гипотезу Ван дер Вардена о том, что перманент произвольной дважды стохастической матрицы порядка N, содержащей хотя бы два различных элемента, больше перманента дважды стохастической матрицы порядка N с одинаковыми элементами. Отсюда получается следующая нижняя оценка $(N!)\left(\frac{n}{N}\right)^N$ для числа различных совершенных паросочетаний в n-регулярном двудольном графе с $2N$-вершинами. В [179] А.Шривер доказал, что если граф является n-регулярным двудольным графом с $2N$ вершинами, $N \geq n$, то в нём имеется не менее $\left(\frac{(n-1)^{n-1}}{n^{n-2}}\right)^N$ различных совершенных паросочетаний. В случае булева n-мерного куба ($N = 2^{n-1}$) последняя оценка сильнее полученной из гипотезы Ван дер Вардена.

С.В.Августинович [3] предложил выражать число комбинаторных объектов, подобных совершенным паросочетаниям или замощениям, через многомерные перманенты. В частности, он доказал, что число совершенных кодов может быть представлено как многомерный перманент некоторого массива. В [52] показано, что число совершенных кликосочетаний в q-ичном n-мерном кубе выражается как q-мерный перманент массива смежности некоторого гиперграфа и получены асимптотические оценки для числа совершенных кликосочетаний в q-ичном n-мерном кубе. А именно, вычислен порядок логарифма числа совершенных кликосочетаний в q-ичном n-мерном кубе при любом натуральном q и $n \to \infty$.

Произвольная совокупность простых попарно не пересекающихся циклов в графе, покрывающая все вершины графа, называется 2-*фактором*. Ясно, что два не пересекающихся совершенных паросочетания в графе порождают 2-фактор. *Гамильтоновым циклом* в графе называется 2-фактор, состоящий из одного цикла. Спектром гамильтонова цикла (кода Грея) в булевом n-мерном кубе называется набор $(a_1, \ldots, a_n)$, где a_i — число рёбер i-го направления в цикле.

В 4-м томе "Искусства программирования" [137] в разделе где рассмотрены коды Грея (гамильтоновы циклы в булевом n-мерном кубе) Д.Кнут указал на три нерешённые на момент издания книги задачи. Первая из них состоит в оценке числа различных кодов Грея в булевом n-кубе. Исследование этого вопроса имеет длительную историю (см. [77], [106], [107], [116]). Порядок логарифма числа гамильтоновых

циклов был найден в [44] и асимптотика логарифма этого числа (при $n \to \infty$) была определена Т.Федером и К.Суби [111]. Во второй задаче было предложено ответить на вопрос ранее поставленный Г.Креверасом в [142]: каждое ли совершенное паросочетание в булевом гиперкубе можно дополнить до гамильтонова цикла? Положительный ответ на этот вопрос получен И.Финком в [112]. В случае, когда паросочетание содержит рёбра малого числа направлений дополняемость совершенного паросочетания до гамильтонова цикла была ранее доказана в [44]. В третьей задаче требовалось выяснить являются ли необходимые условия существования кода Грея со спектром $a = (a_1, \ldots, a_n)$: числа a_i чётные и для любого $k = 1, \ldots, n$ сумма k произвольных компонент набора a не меньше чем 2^k; достаточными для существования кода Грея с таким спектром? В [53] предложено асимптотическое решение последней задачи. А именно, если необходимые условия являются достаточными в булевом n-мерном кубе для некоторого достаточно большого n, то они являются достаточными для любого n. Отметим, что известно несколько способов построения кодов Грея с различными свойствами, в частности, в [86] и [187] были построены гамильтоновы циклы с максимально равномерным (для фиксированной размерности) спектром.

§ 0.4. Основные результаты

В диссертации предпринята попытка связного изложения тех разделов комбинаторики и теории кодирования, к которым относятся результаты автора. Для создания полной картины современного состояния этих областей математики в работе формулируются не только результаты выносимые на защиту, но и теоремы других исследователей работающих в данных областях. Особенно часто в диссертации цитируются результаты С.В.Августиновича и Д.С.Кротова. Совместные с ними исследования и обсуждения привели к написанию этой диссертационной работы. Все упоминаемые в диссертации утверждения, за исключением простых общеизвестных фактов и имеющих лишь техническое или методическое значение предложений автора, снабжены ссылками на источник. Утверждения, содержащие выносимые на защиту результаты автора, подчёркнуты. Диссертация состоит из введения, трёх глав и списка литера-

туры.

В первой главе изложены результаты относящиеся к теории мультиарных квазигрупп, латинских гиперкубов и МДР-кодов. Основные результаты автора в этой области состоят в следующем.

- Перечислены все возможные n-мерные унитрейды мощности, не более чем вдвое превышающей минимальную.

- Для троичного n-мерного куба определено число различных унитрейдов и получена экспоненциальная нижняя оценка числа неэвивалентных латинских битрейдов.

- Доказано, что при любых натуральных $k > 3$ и $n > 2$ имеются неразделимые n-арные квазигруппы порядка k.

- Доказано, что множество n-арных квазигрупп порядка 4 является свитчингово связным для любого n.

- Получена рекуррентная формула и асимптотика для числа n-арных квазигрупп порядка 4

- Усилены асимптотические оценки для числа n-арных квазигрупп порядка $k > 4$.

- Доказано, что любой латинский параллелепипед размера $4 \times 4 \times \cdots \times 4 \times k$, где $k = 1, 2, 3$, дополняется до латинского гиперкуба.

- Построены кратные МДР-коды чётного порядка $q > 2$ длины $n > 2$, которые не содержат однократных подкодов.

- Получены слабо экспоненциальные относительно длины кода нижние оценки числа транзитивных МДР-кодов чётного порядка $q > 2$.

- Доказано, что все бесконечномерные квазигруппы порядка 4 полулинейны или разделимы.

В второй главе изложены результаты относящиеся к теории совершенных раскрасок, совершенных кодов и корреляционно-иммунных функций. Основные результаты автора в этой области состоят в следующем.

- Построены кратные двоичные 1-совершенные коды длины $n = 2^t - 1 \geq 31$, которые не содержат однократных подкодов.

- Получены слабо экспоненциальные относительно длины кода нижние оценки числа транзитивных 1-совершенных кодов.

- Доказано, что множество 1-совершенных двоичных кодов ранга, не более чем на два превосходящего ранг линейного кода той же длины, является свитчингово связным.

- Усилено неравенство Бирбрауэра — Фридмана, оценивающее корреляционую иммунность булевозначных функций через их плотность.

- Доказано, что достижение равенства в усиленном неравенстве является критерием совершенности раскраски n-мерного куба в два цвета.

- Получены верхние и нижние асимптотические оценки числа совершенных 2-раскрасок булева n-мерного куба для некоторого семейства параметров раскрасок.

- Определён спектр возможных мощностей компонент 1-совершенных кодов и 2-раскрасок, корреляционно-иммунных и бент-функций в промежутке между мощностью минимальной компоненты и удвоенной мощностью минимальной компоненты.

- Показано, что существуют бент-функции с компонентами всех мощностей из данного спектра. Для корреляционно-иммунных функций и совершенных 2-раскрасок доказана реализация части спектра.

В третьей главе изложены результаты относящиеся к теории блок-схем, совершенных кликосочетаний и гамильтоновых циклов в булевом кубе. Основные результаты автора в этой области состоят в следующем.

- Найдена асимптотика логарифма числа совершенных кликосочетаний в q-ичном n-мерном кубе при любом натуральном q и растущем n.

- Построены точные кликосочетания в q-ичных n-мерных кубах при $n = 2q = 2^t$ и блок-схемы с неизвестными ранее параметрами.

- Доказано, что если известное необходимое условие существования гамильтонова цикла в булевом n-мерном кубе с заданным спектром является достаточным условием при n, меньших некоторого N, то это условие является достаточным для любых натуральных n.

Глава 1

Латинские гиперкубы, МДР-коды и n-арные квазигруппы

§ 1.1. Латинские битрейды и двукратные МДР-коды

§ 1.1.1. Унитрейды

Как было сказано во введении, множество $B \subset Q_k^n$ называется унитрейдом[1], если мощности его пересечений с линиями гиперкуба принимают только два значения 0 и 2. Унитрейд $B \subset Q_k^n$ называется двудольным (расщепляемым), если подграф ΓB графа ΓQ_k^n, порождённый множеством вершин B, является двудольным. Унитрейд называется *простым*, если не содержит унитрейдов в качестве собственного подмножества.

Латинским битрейдом называют пару частичных латинских квадратов (см.[98]), объединение графиков которых является двудольным унитрейдом. Мы распространяем название "латинский битрейд" на многомерный случай. Кроме того, в тех случаях, когда двудольный унитрейд однозначно разделяется на доли (состоит из одной компоненты связности) будем называть латинским битрейдом не только пару долей, но и сам унитрейд.

Непосредственно из определений вытекают следующие свойства унитрейдов и

[1] В [146] использовался термин 2-код.

МДР-кодов.

Предложение 1.

(a) *Симметрическая разность двух* МДР-*кодов есть двудольный унитрейд.*

(b) *Симметрическая разность (объединение) двух не пересекающихся* МДР-*кодов есть двудольный* 2-МДР-*код.*

(c) 2-МДР-*код — двудольный тогда и только тогда, когда он расщепляемый, т. е. является объединением двух не пересекающихся* МДР-*кодов.*

Предложение 2.

Любой ретракт унитрейда (двудольного унитрейда, 2-МДР-*кода) является унитрейдом (двудольным унитрейдом,* 2-МДР-*кодом) в гиперкубе меньшей размерности.*

Следующее предложение дает естественную характеризацию подмножеств унитрейда, которые в свою очередь являются унитрейдами.

Предложение 3. *Пусть S есть унитрейд и S_0 — его произвольное подмножество. Тогда*

(a) *S_0 является унитрейдом если и только если ΓS_0 есть объединение некоторых компонент связности графа ΓS;*

(b) *S_0 является простым унитрейдом если и только если ΓS_0 есть компонента связности графа ΓS.*

Поскольку любой граф разделяется на компоненты связности имеем

Следствие 1. *Любой унитрейд однозначно представляется в виде объединения набора попарно не пересекающихся простых унитрейдов.*

Следствие 2. *Если простые унитрейды C и C' содержатся в одном и том же унитрейде, то они либо совпадают, либо не пересекаются.*

Из следствия 2 нетрудно получить следующее простое утверждение, которое будет использовано при доказательстве леммы 7.

Предложение 4 ([146]). *Пусть S есть* 2-МДР-код *и γ есть число простых унитрейдов, лежащих в S. Тогда*

(a) *если* 2-МДР-код *S — двудольный, то S содержит ровно 2^γ различных* МДР-*кодов;*

(b) *в противном случае S не содержит ни одного* МДР-*кода.*

Граф унитрейда в Q_k^2 разбивается на простые циклы чётной длины, поэтому справедливо

Предложение 5. *Любой унитрейд $B \subset Q_k^2$ является двудольным.*

Следующее предложение нетрудно доказать по индукции.

Предложение 6. *Любой унитрейд $B \subset Q_3^n$ является простым.*

Замечание 1. *При $k \geq 4$, $n \geq 2$ в гиперкубе Q_k^n имеются непростые унитрейды (см. рис. 1.1).*

Унитрейд B называется *пополняемым*, если найдётся такой 2-МДР-код M, что $B \subseteq M$.

Замечание 2. *При $k \geq 3$, $n \geq 2$ в гиперкубе Q_k^n имеются непополняемые унитрейды (см. рис. 1.1).*

Унитрейд B будем называть *полученным* из МДР-кода M_1 (возможно кратного), если найдётся такой МДР-код M_2 (той же кратности), что $B = M_1 \triangle M_2$. В этом случае множество $B \cap M_1$ будем называть *свитчинговой компонентой* МДР-кода M_1 в соответствии с общим представлением о свитчинговой компоненте кода как о подможестве кода, замена которого на равномощное сохраняет кодовое расстояние. Свитчинговым компонентам МДР-кодов M_1 и M_2 соответствуют доли компонент связности графа ΓB, они же — компоненты латинского битрейда, соответствующего унитрейду B.

Пример 1. На рисунке показаны все унитрейды в Q_4^2, с точностью до перестановок строк и столбцов.

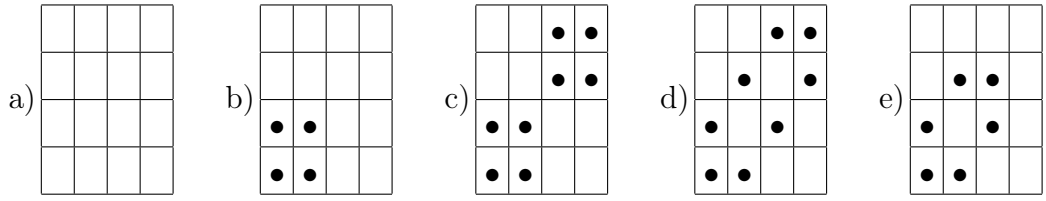


Рис. 1.1: • — элементы унитрейдов в Q_4^2.

Унитрейды a)-d) пополняемые, e) — непополняемый. Унитрейды c) и d) являются

2-МДР-кодами. Унитрейды b), d) и e) простые.

§ 1.1.2. Мощности унитрейдов

Предложение 7.

(a) *Декартово произведение двух унитрейдов является унитрейдом.*

(b) *Декартово произведение двух двудольных унитрейдов является двудольным унитрейдом.*

Доказательство пункта (a) непосредственно вытекает из определений, при доказательстве пункта (b) пользуемся тем, что декартово произведение двудольных графов является двудольным графом.

Следующие два утверждения доказаны в [146].

Предложение 8. *Пусть $B \subset Q_k^n$ — непустой унитрейд, тогда $|B| \geq 2^n$.*

Предложение 9. *Пусть $B \subset Q_k^n$ — унитрейд. Следующие условия эквивалентны:*

(a) $|B| = 2^n$,

(b) *для любой m-мерной грани мощность её пересечения с B равняется* 0 *или* 2^m,

(c) *унитрейд B пересекается только с двумя гипергранями каждого направления,*

(d) *граф ΓB изоморфен булеву кубу ΓQ_2^n.*

Из предложения 8 непосредственно вытекает, что в Q_2^n существует единственный унитрейд, совпадающий со всем множеством Q_2^n.

Рассмотрим вопрос о спектре мощностей унитрейдов.

Предложение 10 ([57]). *Пусть $B \subset Q_k^n$ — унитрейд и $2^{n+1} > |B| \geq 2^n$. Тогда $|B| = 2^{n+1} - 2^{s+1}$, где $s \in \{0, \ldots, n-1\}$.*

Доказательство. Будем доказывать утверждение методом индукции по n. При $n = 1$ утверждение очевидно, предположим оно верно при $n-1$. Если унитрейд $B \subset Q_k^n$ содержится в объединении двух гиперграней каждого направления, то $|B| = 2^n$ по предложению 9.

Если унитрейд B пересекается с четырьмя гипергранями одного направления, то по предложению 9 его мощность больше или равна 2^{n+1}. Пусть унитрейд B пе-

ресекается с тремя гипергранями одного направления. Если пересечение хотя бы с одной из них имеет мощность большую либо равную 2^n, то по предложению 8 имеем $|B| \geq 2^{n+1}$. В противном случае по предположению индукции имеем $|B| = 3 \cdot 2^n - 2^{s_1} - 2^{s_2} - 2^{s_3}$. Поскольку неравенство $2^{s_1} + 2^{s_2} + 2^{s_3} > 2^n$ выполнено только когда как минимум два из трёх s_i равняются $n-1$, имеем $|B| = 2^{n+1} - 2^s$. ▲

Как видно из доказательства предложения 10 унитрейд $B \subset Q_k^n$ мощности меньшей чем 2^{n+1} пересекается не более чем с тремя гипергранями любого направления, следовательно, может быть вложен в троичный гиперкуб.

Предложение 11.

(a) *Симметрическая разность двух унитрейдов в гиперкубе Q_3^n является унитрейдом.*

(b) *Если симметрическая разность двух двудольных унитрейдов в гиперкубе Q_k^n является унитрейдом, а их пересечение порождает связный подграф в Q_k^n, то симметрическая разность является латинским битрейдом.*

Доказательство пункта (a) непосредственно вытекает из определений, при доказательстве пункта (b) пользуемся тем, что связный двудольный граф однозначно разделяется на доли.

Предложение 12 ([57]). *Для любого $s \in \{0, \ldots, n-1\}$ существует единственный (с точностью до эквивалентности) унитрейд $B_s \subset Q_3^n$ мощности $|B_s| = 2^{n+1} - 2^{s+1}$. Унитрейды B_s являются латинскими битрейдами.*

Доказательство. Из предложения 11 следует, что множество $B_s = (\{0,1\}^{n-s} \triangle \{1,2\}^{n-s}) \times \{0,1\}^s$ является латинским битрейдом. Очевидно $|B| = 2^s(2^{n-s} + 2^{n-s} - 2)$.

Перейдём к доказательству единственности. Рассмотрим унитрейд $B \subset Q_3^n$, $|B| < 2^{n+1}$. Аналогично доказательству предложения 10 получаем, что пересечения множества B с гипергранями некоторого направления имеют мощности 2^{n-1}, 2^{n-1}, $2^n - 2^s$. По предположению 9 два пересечения эквивалентны булевым кубам, тогда из определения унитрейда следует, что третье пересечение является симметрической разностью двух булевых кубов. ▲

§ 1.1.3. Компоненты n-арных квазигрупп

Исследования унитрейдов и латинских битрейдов в значительной степени инициированы связью этих объектов с латинскими гиперкубами и n-арными квазигруппами. В частности, они используются при исследовании свитчинговой связности n-арных квазигрупп (определение дано ниже) и дополняемости частичных n-арных квазигрупп.

Для n-арных квазигрупп определим понятия свитчинговых компонент и свитчинговой эквивалентности. $\{a,b\}$-*Компонентой* n-арной квазигруппы f будем называть такое непустое подмножество $S \subset Q_k^n$, что $f(S) = \{a,b\}$ $(a \neq b)$ и для любых $\overline{x}$ из S и $i \in [n]$ найдётся ровно один набор $\overline{y}$ из S, отличающийся от $\overline{x}$ только в i-й координате. Тривиальным примером $\{a,b\}$-компоненты является весь прообраз $f^{-1}(\{a,b\})$, который будем обозначать через $\mathcal{S}_{a,b}(f)$; иногда его можно разбить на более мелкие $\{a,b\}$-компоненты.

Предложение 13. *Любая $\{a,b\}$-компонента n-арной квазигруппы является двудольным унитрейдом.*

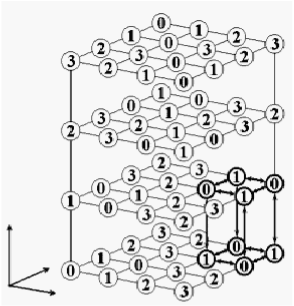


Рис. 1.2: Свитчинг $\{0,1\}$-компоненты.

Будем говорить, что функция g получается из n-арной квазигруппы f *свитчингом* $\{a,b\}$-компоненты S, если

$$g(\overline{x}) = \begin{cases} f(\overline{x}) & \text{при } \overline{x} \notin S; \\ a & \text{при } \overline{x} \in S, f(\overline{x}) = b; \\ b & \text{при } \overline{x} \in S, f(\overline{x}) = a. \end{cases}$$

Из определения $\{a,b\}$-компоненты следует, что функция g является n-арной квази-

группой.

Очевидно, что свитчинг непересекающихся компонент можно производить независимо.

Предложение 14. *Пусть S и S' — непересекающиеся $\{a,b\}$- и $\{c,d\}$- (соответственно) компоненты n-арной квазигруппы f и n-арная квазигруппа g получена из f свитчингом компоненты S. Тогда S' также является $\{c,d\}$-компонентой квазигруппы g.*

Следующее предложение нетрудно получить из определения $\{a,b\}$-компоненты, аналогичное утверждение имеется в [148].

Предложение 15 ([35]). *Пусть множество $C = \{c_1,d_1\} \times \{c_2,d_2\}$ является $\{a,b\}$-компонентой 2-квазигруппы g. Пусть множество C_i является $\{c_i,d_i\}$-компонентой n_i-арной квазигруппы q_i при $i = 1,2$. Тогда множество $C_1 \times C_2$ является $\{a,b\}$-компонентой (n_1+n_2)-арной квазигруппы f, где $f(\bar{x}_1,\bar{x}_2) \equiv g(q_1(\bar{x}_1),q_2(\bar{x}_2))$.*

n-Арные квазигруппы f и g называют *свитчингово эквивалентными* (для краткости, *с.-эквивалентными*), если одна получается из другой конечным числом последовательных свитчингов $\{a,b\}$-компонент, где пары элементов $a,b \in Q_k$ могут быть различными для разных свитчингов.

Перейдём к подробному рассмотрению латинских битрейдов в Q_k^n при $k = 3,4$.

§ 1.1.4. Число унитрейдов в Q_3^n

Предложение 16.

a) *В гиперкубе Q_3^n имеется только один (с точностью до эквивалентности)* МДР-*код, который может быть задан равенством* $= \{x \in Q_3^n \mid x_1 + \cdots + x_n = 0 \mod 3\}$.

b) *В гиперкубе Q_3^n имеется только один (с точностью до эквивалентности)* 2-МДР-*код B, который может быть задан равенством* $B = \{x \in Q_3^n \mid x_1 + \cdots + x_n \neq 0 \mod 3\}$.

Утверждение пункта (a) хорошо известно (см., например, [159], Exercise 13.15), (b) следует из (a).

Рассмотрим множество функций $g : Q_3^n \to \{0,1\}$ как векторное пространство $\mathbb{V}(n)$ над полем $GF(2)$. Характеристические функции унитрейдов образуют в $\mathbb{V}(n)$

линейное подпространство $\mathcal{B}(n)$, в котором в качестве базиса можно выбрать характеристические функции χ^B гиперкубов вида $B = \{\alpha_1, 2\} \times \cdots \times \{\alpha_n, 2\}$, где $\alpha_i \in \{0, 1\}$. Набор коэффициентов в разложении функции g по базису $\{\chi^B\}$ является булевой функцией от набора $(\alpha_1, \ldots, \alpha_n)$. Далее в явной форме определим преобразование, которое каждой булевой функции ставит в соответствие элемент из $\mathcal{B}(n)$.

Определим частичный порядок на Q_3: $0 < 2$, $1 < 2$, а символы 0 и 1 несравнимы. Пусть $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in Q_3^n$. Будем писать $(x_1, \ldots, x_n) \leq (y_1, \ldots, y_n)$, если для любого $i \in \{1, \ldots, n\}$ верно, что $x_i < y_i$ или $x_i = y_i$. Отметим, что множество $\{x \in \{0,1\}^n \mid x \leq y\}$ является гранью булева n-мерного гиперкуба размерности $wt(y)$ равной числу символов 2 в наборе y. Более того, множество граней находится во взаимно однозначном соответствии с множеством наборов $y \in Q_3^n$.

Пусть f — некоторая булева функция. Определим функцию $U[f] : Q_3^n \to \{0, 1\}$ равенством $U[f](y) = \bigoplus\limits_{x \leq y} f(x)$. Заметим, что булева функция $U[f]|_{\{0,2\}^n}$ является преобразованием Мёбиуса от функции f.

Предложение 17. (a) *Пусть $A \subseteq \{0,1\}^n$, тогда $U[\chi^A] \in \mathcal{B}(n)$.*

(b) *Пусть $g \in \mathcal{B}(n)$, тогда $U[g|_{\{0,1\}^n}] = g$.*

Доказательство. (a) Пусть $f = \chi^A$. Из определения преобразования U имеем равенство

$$U[f](a_1, \ldots, a_{i-1}, 2, a_{i+1}, \ldots, a_n) =$$

$$= U[f](a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) \oplus U[f](a_1, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n)$$

для любых $a_j \in Q_3$. Следовательно функция $U[f]$ имеет чётное число единиц в каждой одномерной грани гиперкуба Q_3^n и $U[f] \in \mathcal{B}(n)$.

(b) Равенство $U[g|_{\{0,1\}^n}](y) = g(y)$ для любого $y \in Q_3^n$ нетрудно показать методом индукции по числу символов 2 в наборе y. ▲

Из предложения 17 вытекает, что подпространство $\mathcal{B}(n)$ имеет размерность 2^n. Следовательно, справедливо следующее

Предложение 18 ([57]). *В гиперкубе Q_3^n имеется ровно 2^{2^n} различных унитрейдов.*

Рассмотрим множество функций $g : Q_3^n \to R$ как векторное пространство $\mathbb{V}_R(n)$ над полем R вещественных чисел. Рассмотрим линейное подпространство $\mathcal{B}_R(n)$, со-

стоящее из функций, сумма значений которых по любой одномерной грани равняется 0. Пусть $B \subset Q_3^n$ — двудольный унитрейд. Определим функцию $h_B : Q_3^n \to \{-1, 0, 1\}$, которая принимает значение 1 на первой доле унитрейда, -1 — на второй и 0 — в остальных вершинах гиперкуба. Ясно, что $h_B \in \mathcal{B}_R(n)$. Определим оператор U_R для вещественнозначных функций аналогично оператору U. Пусть $f : Q_2^n \to R$, тогда

$$U_R[f](y) = (-1)^{wt(y)} \sum_{x \le y} f(x). \tag{1.1}$$

Следующее предложение аналогично предложению 17.

Предложение 19. (a) *Для любой функции $f : Q_2^n \to R$ имеем $U_R[f] \in \mathcal{B}_R(n)$.*

(b) *Пусть $g \in \mathcal{B}_R(n)$, тогда $U_R[g|_{\{0,1\}^n}] = g$.*

Пусть множество $\mathcal{F}(n)$ состоит из функций $f : Q_2^n \to \{-1, 0, 1\}$, сумма значений которых в любой грани равна одному из трёх чисел $-1, 0, 1$. *Счётчиком чётности* называется булева функция $\delta(x_1, x_2, \ldots, x_n) = \bigoplus_{i=1}^n x_i$. Нетрудно видеть, что $(-1)^{\delta(x)} \in \mathcal{F}(n)$.

Справедливо следующее

Предложение 20. (a) *Пусть B — двудольный унитрейд, тогда $h_B|_{\{0,1\}^n} \in \mathcal{F}(n)$.*

(b) *Если $f \in \mathcal{F}(n)$, то $U_R[f] = h_B$ для некоторого двудольного унитрейда $B \subset Q_3^n$.*

Доказательство.

(a) По предложению 19 (b) имеем $U_R[|h_B|_{\{0,1\}^n}] = h_B$. Тогда для любой грани $\{x \in \{0,1\}^n | x \le y\}$ имеем $\sum\limits_{x \le y} h_B|_{\{0,1\}^n}(x) = (-1)^{wt(y)} h_B(y) \in \{-1, 0, 1\}$.

(b) По предложению 19 (a) имеем $U_R[f] \in \mathcal{B}_R(n)$. Из условия $f \in \mathcal{F}(n)$ и определения оператора U_R следует, что $U_R[f](Q_3^n) \subseteq \{-1, 0, 1\}$. Тогда в каждой одномерной грани функция $U_R[f]$ либо трижды принимает значение 0, либо по одному разу принимает значения $-1, 0, 1$. ▲

Рассмотрим некоторые конструкции функций из $\mathcal{F}(n)$.

Предложение 21. (a) *Пусть $f \in \mathcal{F}(n)$, тогда $f \cdot \chi^\gamma \in \mathcal{F}(n)$ для любой грани γ.*

(b) *Пусть γ_1, γ_2 — грани в Q_2^n и $\gamma_1 \cap \gamma_2 \neq \varnothing$. Определим функцию f равенством*

$$f(x_1, \ldots, x_n, x_{n+1}) = \begin{cases} \chi^{\gamma_1}(-1)^{\delta(x_1,\ldots,x_n)} & \text{при } x_{n+1} = 0 \\ \chi^{\gamma_2}(-1)^{\delta(x_1,\ldots,x_n)\oplus 1} & \text{при } x_{n+1} = 1. \end{cases}$$

Тогда $f \in \mathcal{F}(n+1)$.

Предложение 22. *Пусть* $f \in \mathcal{F}(n)$, $g \in \mathcal{F}(m)$ *и* $F(x,y) = f(x)g(y)$. *Тогда* $F \in \mathcal{F}(n+m)$.

Доказательства предложений 21 и 22 нетрудно получить непосредственной проверкой.

Заметим, что все унитрейды в Q_3^n состоят из одной компоненты связности, поэтому двудольные унитрейды являются латинскими битрейдами.

Далее получим нижнюю оценку числа неэквивалентных латинских битрейдов. Две определённые на гиперкубе функции называются эквивалентными, если они переходят друг в друга посредством изометрий гиперкуба. Рассмотрим гиперкуб Q_2^n как векторное пространство над полем $GF(2)$. Будем называть *носителем* вектора $x \in Q_2^n$ множество позиций, на которых в векторе x находятся единицы. Рассмотрим набор векторов $z^1, \ldots, z^k$ с попарно непересекающимися носителями. Пусть $V \subset Q_2^n$ — подпространство натянутое на вектора $z^1, \ldots, z^k$, $V = \{\bigoplus \alpha_i z^i \ | \alpha \in Q_2^k\}$. Пусть $f : Q_2^k \to \{-1, 0, 1\}$. Определим функцию $G_V[f] : Q_2^n \to \{-1, 0, 1\}$ равенствами

$$G_V[f](x) = \begin{cases} f(\alpha) & \text{при } \ x = \bigoplus \alpha_i z^i \\ 0 & \text{при } \ x \notin V. \end{cases}$$

Теорема 1 ([57]).

(a) *Множество* $\mathcal{F}(n)$ *содержит не менее* $e^{\Omega(\sqrt{n})}$ *неэквивалентных функций*[2].

(b) *В гиперкубе* Q_3^n *имеется не менее* $e^{\Omega(\sqrt{n})}$ *неэквивалентных латинских битрейдов.*

Доказательство.

Если $f \in \mathcal{F}(k)$, то $G_V[f] \in \mathcal{F}(n)$. Действительно, поскольку носители векторов $z^1, \ldots, z^k$ попарно не пересекаются, сумма значений функции $G_V[f]$ по грани гиперкуба Q_2^n совпадает с суммой значений функции f по некоторой грани гиперкуба Q_2^k. Тогда $G_V[f](Q_3^n) \subseteq \{-1, 0, 1\}$.

(a) Известно (см., например, [76]), что имеется $e^{\Omega(\sqrt{n})}$ различных разбиений числа

[2] Равенство $f(n) = \Omega(g(n))$ означает, что $f(n) \geq cg(n)$ для некоторого $c > 0$ при $n \to \infty$.

n на целые неотрицательные слагаемые. Каждое такое разбиение порождает некоторый набор векторов $z^1, \ldots, z^k$ с попарно не пересекающимися носителями и соответствующее набору подпространство V. Функции $G_V[\delta]$ неэквивалентны для различных разбиений, поскольку расстояния Хэмминга между базисными векторами не меняются при изометриях гиперкуба.

(b) По предложению 20 (b) каждая функция $U_R[G_V[\delta]]$ порождает латинский битрейд B. Рассмотрим случай, когда все носители векторов $z^1, \ldots, z^k$ имеют мощность не менее трёх и сумма этих мощностей равна n. Покажем, что пересечения битрейда B с гипергранями вида $\gamma = \{x \in Q_3^n | x_i = 2\}$ обладают некоторым инвариантным относительно изометрии свойством (*), которым не обладают пересечения битрейда B с гипергранями вида $\{x \in Q_3^n | x_i = 0\}$ и $\{x \in Q_3^n | x_i = 1\}$. Тогда для любой изометрии φ по битрейду $\varphi(B)$ можно определить множество $\varphi(B \cap \{0,1\}^n)$. Следовательно, неэквивалентность битрейдов $U_R[G_V[\delta]]$ при различных V является следствием пункта (a).

(*) Пусть $\gamma = \{x \in Q_3^n | x_i = a\}$. Неравенство $a \neq 2$ справедливо тогда и только тогда, когда найдётся такая гиперграни $\gamma' = \{x \in Q_3^n | x_j = b\}$, $b \in Q_3$, $j \neq i$, что пересечение $\gamma \cap \gamma' \cap B$ пусто.

Без ограничения общности полагаем, что $i = 1$ и носитель вектора z^1 содержит 1 и 2. Тогда

$$\{x \in Q_3^n | x_1 = 0\} \cap \{x \in Q_3^n | x_2 = 1\} \cap B = \varnothing,$$

$$\{x \in Q_3^n | x_1 = 1\} \cap \{x \in Q_3^n | x_2 = 0\} \cap B = \varnothing.$$

В то время как из формулы (2.1) имеем

$$y = (2, 0, \ldots, 0) \in \{x \in Q_3^n | x_1 = 2\} \cap \{x \in Q_3^n | x_j = 0\} \cap B,$$

$$y' = (2, 0, \ldots, 0, 2, 0 \ldots) \in \{x \in Q_3^n | x_1 = 2\} \cap \{x \in Q_3^n | x_j = 2\} \cap B,$$

поскольку $\{\overline{0}\} = \{x \in \{0,1\}^n | x \leq y\} \cap \{x \in \{0,1\}^n | G_V[\delta](x) \neq 0\} =$
$\{x \in \{0,1\}^n | x \leq y'\} \cap \{x \in \{0,1\}^n | G_V[\delta](x) \neq 0\}$.

Кроме того,

$$y'' = (2, 0, \dots, 0, 1, \dots, 1, 0 \dots) \in \{x \in Q_3^n | x_1 = 2\} \cap \{x \in Q_3^n | x_j = 1\} \cap B,$$

поскольку

$\{x \in \{0,1\}^n \mid x \leq y''\} \cap \{x \in \{0,1\}^n \mid G_V[\delta](x) \neq 0\} = \{(0, \dots, 0, 1, \dots, 1, 0 \dots)\} = \{z^k\}$, где носитель вектора z^k содержит позицию j. ▲

Отметим, что латинский битрейд B_s (см. предложение 12) можно задать также функцией $h_{B_s} = U_R[G_V[\delta]]$, где базис подпространства V состоит из одного вектора z с носителем мощности $n - s$.

§ 1.1.5. Получение унитрейдов из МДР-кодов и n-арных квазигрупп

Функция $g : B \to Q_k$, $B \subseteq Q_k^n$, называется *частичной* n-арной квазигруппой, если $g(x) \neq g(y)$ при любых $x, y \in B$, $d(x, y) = 1$. Таблица значений частичной квазигруппы называется *частичным* латинским n-кубом, если $B = Q_k^{n-1} \times Q_{k'}$, $1 < k' < k$, — латинским гиперкубоидом. Из определений непосредственно следует

Предложение 23. (a) *Сужение n-арной квазигруппы на любое подмножество гиперкуба является частичной квазигруппой.*

(b) *При $B = Q_k^n$ частичная n-арная квазигруппа является n-арной квазигруппой.*

Если частичная квазигруппа является сужением всюду определённой n-арной квазигруппы, то она называется *дополняемой*.

Для произвольной функции $f : Q_k^n \to Q_k$ определим множества $\mathcal{M}\langle f \rangle \stackrel{def}{=} \{(\bar{x}, f(\bar{x})) : \bar{x} \in Q_k^n\}$ — график функции и $\mathcal{M}_a\langle f \rangle \stackrel{def}{=} \{\bar{x} \in Q_k^n \ : f(\bar{x}) = a\}$, $a \in Q_k$ — поверхность уровня a. Пусть $M \subset Q_k^{n+1}$ — МДР-код с расстоянием 2. Определим функцию $F_i\langle M \rangle$ равенством $F_i\langle M \rangle(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{n+1}) = x_i$, если и только если $(x_1, \dots, x_{n+1}) \in M$. Из определений вытекает

Предложение 24. (a) *Отображение $\mathcal{M}\langle \cdot \rangle$ есть взаимно однозначное соответствие между множеством n-арных квазигрупп и множеством* МДР-*кодов длины $n + 1$.*

(b) *Для любого* $a \in Q_k$ *отображение* $\mathcal{M}_a\langle\cdot\rangle$ *отображает* n*-арные квазигруппы в множество* МДР*-кодов длины* n *для любого* $i, 1 \le i \le n$.

(c) *Отображение* $F_i\langle\cdot\rangle$ *есть взаимно однозначное соответствие между множеством* МДР*-кодов длины* $n+1$ *и множеством* n*-арных квазигрупп.*

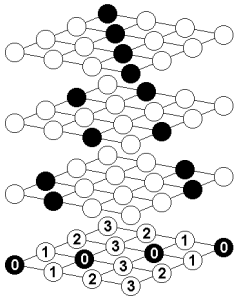


Рис. 1.3: Отображение $\mathcal{M}\langle\cdot\rangle$.

В [101] доказано, что любая частичная n-арная квазигруппа конечного порядка есть сужение n-арной квазигруппы некоторого большего порядка. Отсюда следует

Предложение 25. *Любой латинский битрейд* $B \subset Q_k^n$ *может быть получен из некоторого* МДР*-кода* $M \subset Q_m^n$*, где* $m \ge k$.

Предложение 26. *Латинский битрейд* $B \subset Q_k^n$ *такой, что* $2^{n+1} > |B| > 2^n$*, не может быть получен из* МДР*-кода* $M \subset Q_k^n$ *при* $k \in \{3, 4\}$.

Доказательство. Поскольку все МДР-коды в Q_3^n эквивалентны при любом n (см. предложение 16), достаточно рассмотреть произвольный МДР-код в Q_3^n, например, $M = \{x \in Q_3^n \mid x_1 + \cdots + x_n = 0 \bmod 3\}$. Нетрудно видеть, что любой полученный из M унитрейд содержит весь МДР-код M и имеет мощность $2 \cdot 3^{n-1}$.

Пусть $k = 4$. Если латинский битрейд получен из МДР-кода $M \subset Q_4^n$, то по определению он является подмножеством 2-МДР-кода $M \cup M'$. Тогда по следствию 3 (см. ниже) его мощность делится на 2^n. ▲

Рассмотрим возможность получения латинских битрейдов малой мощности из двукратных МДР-кодов.

Предложение 27 ([57]). *Любой* n*-мерный латинский битрейд мощности меньше* 2^{n+1} *может быть получен из двукратных* МДР*-кодов в* Q_4^n.

Доказательство. Вначале покажем, что битрейд $B_0^k = \{0,1\}^k \triangle \{1,2\}^k$ может быть получен из некоторого двукратного МДР-кода в Q_4^k. Пусть функция $g : Q_k^n \to \{0,1\}$ определена равенством $g(a_1,\ldots,a_k) = \sum\limits_{i=1}^{k} a_i \bmod 2$. Нетрудно видеть, что функции g, $g_1 = g \oplus \chi^{\{1,2\}^k}$ и $g_2 = g \oplus \chi^{\{0,1\}^k}$ являются характеристическими функциями некоторых двукратных МДР-кодов M_0, M_1 и M_2. Поскольку $g_1 \oplus g_2 = \chi^{\{1,2\}^k} \oplus \chi^{\{0,1\}^k}$, имеем $B_0^k = M_1 \triangle M_2$.

Рассмотрим булевозначные функции

$$f_1(a_1,\ldots,a_k,y) = \begin{cases} g_1(a_1,\ldots,a_k) & \text{при } \ y=0, \\ g_2(a_1,\ldots,a_k) & \text{при } \ y=1, \\ g_1(a_1,\ldots,a_k)\oplus 1 & \text{при } \ y=2, \\ g_2(a_1,\ldots,a_k)\oplus 1 & \text{при } \ y=3; \end{cases} \tag{1.2}$$

и

$$f_2(a_1,\ldots,a_k,y) = \begin{cases} g_2(a_1,\ldots,a_k) & \text{при } \ y=0, \\ g_1(a_1,\ldots,a_k) & \text{при } \ y=1, \\ g_1(a_1,\ldots,a_k)\oplus 1 & \text{при } \ y=2, \\ g_2(a_1,\ldots,a_k)\oplus 1 & \text{при } \ y=3. \end{cases} \tag{1.3}$$

Легко видеть, что f_1 и f_2 являются характеристическими функциями двукратных МДР-кодов, причём $f_1 \oplus f_2 = \chi^{B_0^k \times \{0,1\}}$.

Подставляя в формулы (1.2–1.3) функции f_1 и f_2 вместо g_1 и g_2, обнаружим, что латинский битрейд $B_0^k \times \{0,1\}^2$ также может быть получен из некоторого двукратного МДР-кода в Q_4^{k+2} и т. д. Для окончания доказательства остаётся сослаться на предложения 10 и 12. ▲

Приведём таблицы функций g, g_1, g_2 при $n = 2$:

$$\begin{pmatrix} 0&1&0&1 \\ 1&0&1&0 \\ 0&1&0&1 \\ 1&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&1 \\ 1&1&0&0 \\ 0&0&1&1 \\ 1&0&1&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&1 \\ 0&1&1&0 \\ 0&1&0&1 \\ 1&0&1&0 \end{pmatrix}.$$

Можно показать, что построенные в предложении 27 двукратные МДР-коды не двудольные при $n \geq 3$ (см.также § 1.6.2).

§ 1.1.6. 2-МДР коды в Q_4^n

В этом разделе рассмотрена некоторая характеризация 2-МДР кодов в Q_4^n. Ниже показано, что не простые 2-МДР могут быть представлены через простые 2-МДР-коды меньшей размерности.

Предложение 28. *Множество $S \subset Q_4^n$ является* 2-МДР-*кодом тогда и только тогда, когда множество $Q_4^n \setminus S$ является* 2-МДР-*кодом.*

Сформулированное в предложении 28 свойство является специфическим для 4-ичного гиперкуба. Это объясняет гораздо более богатую теорию 2-МДР-кодов в Q_4^n по сравнению с другими размерностями.

Предложение 29 ([146]). *Пусть*

- $\chi_j : Q_4^{n_j} \to \{0,1\}$ — *характеристическая функция* 2-МДР-*кода* $S_j \subset Q_4^{n_j}$, $j \in [m]$,
- $\tilde{x}_1, \ldots, \tilde{x}_m$ — *непересекающиеся наборы переменных из* $\bar{x}$, $\tilde{x}_j \stackrel{def}{=} (x_{i_{j,1}}, \ldots, x_{i_{j,n_j}})$,
- $\delta \in \{0,1\}$.

Тогда множество S, заданное характеристической функцией

$$\chi_S(\bar{x}) = \bigoplus_{j=1}^{m} \chi_{S_j}(\tilde{x}_j) \oplus \delta, \tag{1.4}$$

является 2-МДР-*кодом.*

Теорема 2 ([146]). *Характеристическая функция χ_S* 2-МДР-*кода S имеет единственное представление в виде* (1.4)*, где для каждого $j \in [m]$ множество $S_j \subset Q_4^{n_j}$ есть простой* 2-МДР-*код и $\bar{0} \in S_j$. При этом*
(a) *S и ${Q_4}^n \setminus S$ — объединения 2^{m-1} равномощных простых унитрейдов,*
(b) *если $m \geq 2$ и* 2-МДР-*код S двудольный, то для любого $j \in [m]$* 2-МДР-*коды S_j и $(Q_4^{n_j} \setminus S_j)$ также двудольные.*

Следствие 3. *Если простой унитрейд содержится в* 2-МДР-*коде, лежащем в гиперкубе* Q_4^n, *то его мощность равна* 2^t, *для некоторого натурального* t, $t \geq n$.

Замечание 3. *Теорема 2 обобщается на* t-*кратные МДР-коды в гиперкубе* Q_{2t}^n.

Предложение 30. ([146]) *Пусть* $S, S', S'' \subset {Q_4}^n$ *есть 2-*МДР-*коды и* S_0 *есть унитрейд. Тогда*

(a) *если* $S_0 \subseteq S \cap S'$, *то* $S = S'$;

(b) *если* $S_0 \subseteq S \backslash S''$, *то* $S = {Q_4}^n \backslash S''$.

Таким образом, 2-МДР-код в гиперкубе Q_4^n однозначно определяется любым содержащимся в нём непустым унитрейдом. Для гиперкубов большего порядка это неверно.

Для характеризации n-арных квазигрупп порядка 4 и исследования вопроса о дополняемости частичных n-арных квазигрупп порядка 4 были использованы следующие утверждения о 2-МДР-кодах в 4-ичном гиперкубе.

Предложение 31. (теорема 4.1(c) [146]). *Пусть* 2-МДР-*код* $S \subset Q_4^n$ *удовлетворяет равенству* $\chi_S = \chi_{S_1} \oplus \chi_{S_2}$, *где* S_1 *и* S_2 — 2-МДР-*коды меньших размерностей. Тогда* 2-МДР-*код* S *двудольный, если и только если каждый из* 2-МДР-*кодов* S_1 *и* S_2 *двудольный.*

Предложение 32 ([51]). *Пусть* 2-МДР-*код* $S \subset Q_4^n$ *двудольный и справедливо равенство* $\chi_S = \chi_{S_1} \oplus \chi_{S_2}$, *где* S_1 *и* S_2 — 2-МДР-*коды меньших размерностей. Тогда* 2-МДР-*код* $S' = Q_4^n \setminus S$ *двудольный.*

Пусть $S \subseteq Q_4^n$, $k \in [n]$ и $y \in Q_4$. Введём обозначение

$$\mathcal{L}_{k;y} S \stackrel{def}{=} \{(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n) \mid (x_1, \ldots, x_{k-1}, y, x_{k+1}, \ldots, x_n) \in S\}$$

для ретрактов размерности $n-1$, для краткости будем называть такой ретракт *слоем* множества S по k-му направлению.

Из определения следуют простые свойства

Предложение 33 ([49]). *Пусть* $S, S' \subseteq Q_4^n$ – *некоторые множества,* $k \in [n]$ *и* $\{a, b, c, d\} = Q_4$.

(a) *Если* S *есть унитрейд (двудольный унитрейд,* 2-МДР-*код), то* $\mathcal{L}_{k;a} S$ *также явля-*

ется унитрейдом (двудольным унитрейдом, 2-МДР-*кодом) в* Q_4^{n-1}.

(b) *Если* $k < k' \in [n]$, *то* $\mathcal{L}_{k;b}(\mathcal{L}_{k';a}S) = \mathcal{L}_{k'-1;a}(\mathcal{L}_{k;b}S)$.

(c) $\mathcal{L}_{k;a}(S \cap S') = \mathcal{L}_{k;a}S \cap \mathcal{L}_{k;a}S'$.

(d) *Если* S *и* S' *есть унитрейды и* $\mathcal{L}_{k;a}S = \mathcal{L}_{k;a}S'$, $\mathcal{L}_{k;b}S = \mathcal{L}_{k;b}S'$, $\mathcal{L}_{k;c}S = \mathcal{L}_{k;c}S'$, *то* $\mathcal{L}_{k;d}S = \mathcal{L}_{k;d}S'$.

(e) *Если* S *есть* 2-МДР-*код и* $\mathcal{L}_{k;a}S = \mathcal{L}_{k;b}S$, *то* $\mathcal{L}_{k;c}S = \mathcal{L}_{k;d}S = Q_4^{n-1} \backslash \mathcal{L}_{k;a}S$.

§ 1.1.7. Линейные 2-МДР коды

Если в равенстве (1.4) имеем $n_j = 1$ для любого $j \in [m]$, то 2-МДР-код S называется *линейным*, т. е. справедливо равенство

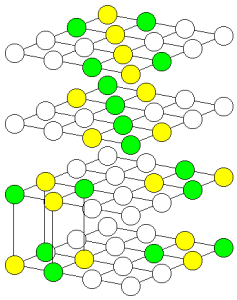


Рис. 1.4: Линейный 2-МДР-код.

$$\chi_S(x_1, \ldots, x_n) \equiv \chi_{S_1}(x_1) \oplus \chi_{S_2}(x_2) \oplus \cdots \oplus \chi_{S_n}(x_n), \tag{1.5}$$

где S_i ($i \in [n]$) есть двухэлементные подмножества в Q_4. Линейный 2-МДР-код в Q_4^2 изображён на рис.1c, линейный 2-МДР-код в Q_4^3 на рис. 1.4.

В следующих двух предложениях сформулированы элементарные свойства линейных 2-МДР-кодов.

Предложение 34. ([49])

(a) *Линейные* 2-МДР-*коды образуют класс эквивалентности.*

(b) *Линейный* 2-МДР-*код является расщепляемым* 2-МДР-*кодом.*

(c) *Дополнение линейного* 2-МДР-*кода есть линейный* 2-МДР-*код.*

(d) 2-МДР-*код* S *является линейным если и только если найдётся простой* 2-МДР-

код $S_0 \subset S$ мощности 2^n.

(e) *Линейный* 2-МДР-*код однозначно определяется подмножеством всех своих наборов, содержащих не более одного ненулевого элемента.*

(f) *Число линейных* 2-МДР-*кодов в Q_4^n равно $2 \cdot 3^n$.*

Доказательство. (a), (b) и (c) следуют непосредственно из определений.

(d) Необходимость. Согласно п. (a), без потери общности можно считать, что $\chi_S(x_1, \ldots, x_n) \equiv \bigoplus_{i=1}^n \chi_{\{2,3\}}(x_i)$. В этом случае $S_0 \stackrel{def}{=} \{2,3\} \times \{0,1\}^{n-1}$ есть подмножество S.

Достаточность. По предложению 9, не теряя общности, положим $S_0 = \{2,3\} \times \{0,1\}^{n-1}$. Тогда S_0 есть подмножество линейного 2-МДР-кода S', где $\chi_{S'}(x_1, ..., x_n) \equiv \bigoplus_{i=1}^n \chi_{\{2,3\}}(x_i)$. По предложению 30(a) имеем $S = S'$.

(e) Действительно, пусть 2-МДР-код S представим в виде (1.5). Обозначив $\chi^0 \stackrel{def}{=} \chi_S(\bar{0})$ и $\chi^i(y) \stackrel{def}{=} \chi_S(0, \ldots, 0, y, 0 \ldots, 0)$, $i \in [n]$, имеем

$$\chi_S(x_1, \ldots, x_n) \equiv \chi^0 \oplus \bigoplus_{i=1}^n (\chi^i(x_i) \oplus \chi^0), \tag{1.6}$$

что легко проверить, расписав χ_S по формуле (1.5).

(f) следует из представления (1.6). Действительно, χ^0 можно выбрать двумя способами, после чего каждую из функций χ^i, $i \in [n]$ – тремя способами, учитывая что она есть характеристическая функция 2-МДР-кода в Q_4 и $\chi^i(\bar{0}) = \chi^0$.▲

Из представления (1.5) нетрудно видеть, что справедливо

Предложение 35.

(a) *Если $S \subset Q_4^n$ – линейный* 2-МДР-*код, то $\mathcal{L}_{k;y}S$ – линейный* 2-МДР-*код.*

(b) *Пусть $S \subset Q_4^n$ есть* 2-МДР-*код. Если по какому-либо направлению два слоя S линейны и совпадают, то S — линейный* 2-МДР-*код.*

Основным результатом данного раздела является следующая лемма, которая представляет собой частичное обращение п. (a) и частичное усиление п. (b) предложения 35. В лемме показано, что наличие линейного слоя в расщепляемом 2-МДР-коде влечёт наличие по тому же направлению слоя, который является дополнением к первому, “антислоя”.

Лемма 1. (лемма об антислое [49]) *Пусть $S \subset Q_4^n$ — двудольный* 2-МДР-*код и $L = \mathcal{L}_{k;a}S$ – линейный* 2-МДР-*код для некоторых $k \in [n]$ и $a \in Q_4$. Тогда*

(a) *найдётся такое $b \in Q_4$, что $\mathcal{L}_{k;b}S = Q_4^{n-1}\backslash L$;*

(b) *$Q_4^n\backslash S$ — двудольный* 2-МДР-*код.*

Перед тем, как приступить к доказательству леммы 1, введём обозначение $\neg(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\alpha_1 \oplus 1, \alpha_2 \oplus 1, \ldots, \alpha_n \oplus 1)$, где $\alpha_i \in \{0, 1\}$ и докажем два вспомогательных предложения.

Предложение 36. *Пусть $\{P_1, P_2, P_3\}$ – разбиение булевого n-мерного куба, $n \geq 4$, на три непустых множества: $P_1 \cup P_2 \cup P_3 = \{0, 1\}^n$. Причём выполнено условие*

(*) *для каждого $k \in [n]$ и каждого $b \in \{0, 1\}$ хотя бы одно множество (слой) из $\mathcal{L}_{k;b}P_1$, $\mathcal{L}_{k;b}P_2$, $\mathcal{L}_{k;b}P_3$ пустое.*

Тогда $\{P_1, P_2, P_3\} = \{\{\bar{\alpha}\}, \{\neg\bar{\alpha}\}, \{0, 1\}^n\backslash\{\bar{\alpha}, \neg\bar{\alpha}\}\}$, где $\bar{\alpha} \in \{0, 1\}^n$.

Доказательство. Обозначим через $N_i \subseteq [n]$ множество координат k, значения которых не фиксированы в P_i, то есть $\mathcal{L}_{k;0}P_i \neq \varnothing$ и $\mathcal{L}_{k;1}P_i \neq \varnothing$. Легко видеть, что, множества N_1, N_2, N_3 попарно не пересекаются (если, к примеру, $k \in N_1 \cap N_2$, то из условия (*) следует $\mathcal{L}_{k;0}P_3 = \varnothing$ и $\mathcal{L}_{k;1}P_3 = \varnothing$, что противоречит непустоте P_3). Тогда из очевидного соотношения $2^n = \sum_i |P_i| \leq \sum_i 2^{|N_i|}$ вытекает, что $\{N_1, N_2, N_3\} = \{\varnothing, \varnothing, [n]\}$ и $\{P_1, P_2, P_3\} = \{\{\bar{\alpha}\}, \{\bar{\beta}\}, \{0, 1\}^n\backslash\{\bar{\alpha}, \bar{\beta}\}\}$. Из (*) прямо следует, что $\bar{\beta} = \neg\bar{\alpha}$. ▲

Предложение 37. *Пусть S есть 2-МДР-код в Q_4^n, где $n \geq 3$, и $k \in [n]$. Пусть P_0, P_1, P_2, P_3 – пересечения четырёх слоёв множества S по k-му направлению с булевым $(n-1)$-кубом, то есть $P_i \stackrel{def}{=} \mathcal{L}_{k;i}S \cap \{0, 1\}^{n-1}$. Предположим, что верно одно из двух утверждений:*

(a) *$n = 3$, $P_i = \{0, 1\}^2$ для некоторого i и $P_i \neq \varnothing$ для всех $i \in \{0, 1, 2, 3\}$;*

(b) *$\{P_0, P_1, P_2, P_3\} = \{\{0, 1\}^{n-1}, \{\bar{\alpha}\}, \{\bar{\beta}\}, \{0, 1\}^{n-1}\backslash\{\bar{\alpha}, \bar{\beta}\}\}$, где $\bar{\alpha} \in \{0, 1\}^{n-1}$ и $\bar{\beta} = \neg\bar{\alpha}$.*

Тогда 2-МДР-коды S и $Q_4^n\backslash S$ недвудольные.

Доказательство. (a) Имеется два неэквивалентных случая выбора множеств P_i. Нетрудно убедиться, что в каждом из случаев любая попытка восстановить

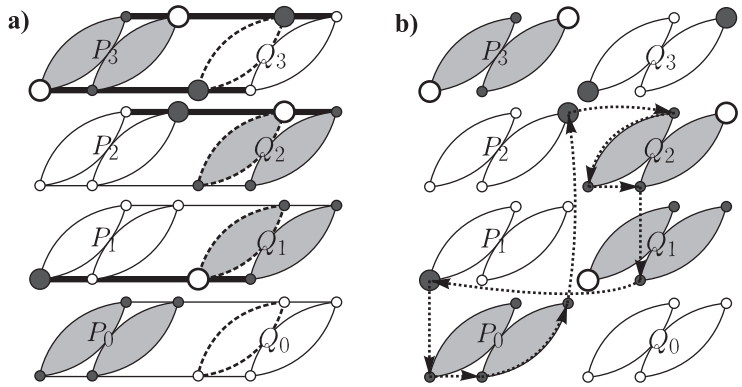


Рис. 1.5: Иллюстрация к предложению 37

2-МДР-код S приводит к недвудольному 2-МДР-коду с недвудольным дополнением.

(b) Без потери общности можно считать, что $k = n$, $\bar{\alpha} = 0^{n-1}$, $\bar{\beta} = 1^{n-1}$,

$$P_0 = \{0,1\}^{n-1}, \quad P_1 = \{\bar{\alpha}\}, \quad P_2 = \{\bar{\beta}\} \text{ и } P_3 = \{0,1\}^{n-1} \backslash \{\bar{\alpha}, \bar{\beta}\}$$

(в противном случае, подобрав подходящие перестановку координат и изотопию, можно рассмотреть эквивалентный 2-МДР-код, удовлетворяющий этим условиям). Рассуждения будем проводить индукцией по n. База индукции – случай $n = 3$ – рассмотрен в п. (a). Предположим, что предложение верно при $n = m-1$. Покажем, что оно выполняется и при $n = m$. Рассмотрим пересечения слоёв $\mathcal{L}_{k;0}S$, $\mathcal{L}_{k;1}S$, $\mathcal{L}_{k;2}S$, $\mathcal{L}_{k;3}S$ с "соседним" булевому $(n-1)$-мерному кубу $\{0,1\}^{n-1}$ и эквивалентным ему множеством $E \stackrel{def}{=} \{2,3\} \times \{0,1\}^{n-2}$:

$$R_i \stackrel{def}{=} \{2,3\} \times \{0,1\}^{n-2} \cap \mathcal{L}_{1;i}S.$$

Иллюстрации приведены на рис. 1.5.

(*) *Мы утверждаем, что множества R_0, R_1, R_2, R_3 определены с точностью до четырёх элементов. Точнее,*

$$R_0 = \varnothing, \quad R_1 = E \backslash \{\bar{\alpha}'\}, \quad R_2 = E \backslash \{\bar{\beta}'\} \text{ и } R_3 = \{\bar{\alpha}'', \bar{\beta}''\}, \tag{1.7}$$

где $\bar{\alpha}', \bar{\alpha}'' \in \{(2,0,...,0),(3,0,...,0)\}$ и $\bar{\beta}', \bar{\beta}'' \in \{(2,1,...,1),(3,1,...,1)\}$. Действительно, множество $\{0,1\}^{n-1} \cup E$ разбивается на линии направления 1, проходящие через вершины $\bar{x} \in \{0\} \times \{0,1\}^{n-2}$. Из того, что S есть 2-МДР-код, следует, что каждое такая

линия содержит две вершины из $P_i \cup R_i$ для любого $i \in \{0,1,2,3\}$. В частности,

- если такая линия содержит две вершины из P_i, то она не содержит вершин из R_i;
- если она не содержит вершин из P_i, то содержит две вершины из R_i.

В согласии с (1.7) эти два правила определяют все вершины множеств R_i, $i = 0,1,2,3$, за исключением четырёх случаев (рис. 1.5a, жирные горизонтальные линии):

- линия, проходящая через $(0,0,...,0)$, содержит ровно одну вершину $(0,0,...,0)$ из P_1,
- линия, проходящая через $(0,0,...,0)$, — ровно одну вершину $(1,0,...,0)$ из P_3,
- линия, проходящая через $(0,1,...,1)$ — ровно одну вершину $(1,1,...,1)$ из P_2,
- линия, проходящая через $(0,1,...,1)$ – ровно одну вершину $(0,1,...,1)$ из P_3.

В каждом из этих случаев есть возможность выбора вершины из R_i для соответствующего i. Этому выбору соответствует выбор вершин $\alpha', \alpha'', \beta', \beta''$. Утверждение (*) доказано.

Так как S есть 2-МДР-код, то каждая вершина из E принадлежит ровно двум множествам R_i. Таким образом, из (1.7) сразу следует, что $\bar{\alpha}' = \bar{\alpha}''$ и $\bar{\beta}' = \bar{\beta}''$. Без потери общности можно считать, что $\bar{\alpha}' = \bar{\alpha}'' = (2,0,...,0)$. Таким образом, достаточно рассмотреть два случая: $\bar{\beta}' = \bar{\beta}'' = (2,1,...,1)$ (рис. 1.5a) и $\bar{\beta}' = \bar{\beta}'' = (3,1,...,1)$ (рис. 1.5b).

1) Случай $\bar{\beta}' = \bar{\beta}'' = (2,1,...,1)$ (рис. 1.5a). В этом случае мы можем использовать предположение индукции. Действительно, рассмотрим множество $Q_4^{n-1} \backslash \mathcal{L}_{1;2} S$. Слои этого множества по последнему направлению в пересечении с булевым $(n-2)$-мерным кубом совпадают с $\{0,1\}^{n-2}$, $\{(0,...,0)\}$, $\{(1,...,1)\}$ и $\{0,1\}^{n-1} \backslash \{(0,...,0),(1,...,1)\}$ (см. рис. 1.5a, пунктир). По предположению индукции 2-МДР-коды $Q_4^{n-1} \backslash \mathcal{L}_{1;2} S$ и $\mathcal{L}_{1;2} S$ недвудольные. Следовательно, $Q_4^n \backslash S$ и S также недвудольные.

2) Случай $\bar{\beta}' = \bar{\beta}'' = (3,1,...,1)$ (рис. 1.5b). В этом случае в графе $\Gamma(S)$ можно указать цикл нечётной длины $2n+3$:

$$(0000...00,\ \underbrace{1000...00,\ 1100...00,\ 1110...00,\ \cdots, 1111...10}_{n-1},\ 1111...12,$$
$$\underbrace{2111...12,\ 2011...12,\ 2001...12,\ \cdots,\ 2000...02}_{n-1},\ 3000...02,\ 3000...01,\ 0000...01)$$

(рис. 1.5b, пунктир), – откуда следует, что этот граф не является двудольным и

2-МДР-код S недвудольный по определению. Аналогично, нечётный цикл

$$(2000...00,\ \underbrace{3000...00,\ 3100...00,\ 3110...00,\ \cdots, 3111...10}_{n-1},\ 3111...12,$$
$$\underbrace{0111...12,\ 0011...12,\ 0001...12,\ \cdots,\ 0000...02}_{n-1},\ 1000...02,\ 1000...01,\ 2000...01)$$

в графе $\Gamma(Q_4^n \backslash S)$ доказывает недвудольность 2-МДР-кода $Q_4^n \backslash S$. ▲

Доказательство леммы 1. (a) Покажем утверждение по индукции. Базис индукции – случай $n = 2$ – тривиален. Пусть утверждение леммы верно для $n = m - 1$. Покажем, что оно выполняется при $n = m \geq 3$.

Учитывая сохранение свойств расщепляемости и линейности 2-МДР-кода при изотопии и перестановке переменных, а также предложение 34(d), без потери общности можно считать, что $k = n$, $a = 0$ и линейный 2-МДР-код L содержит $\{0,1\}^{n-1}$. Пусть множества P_0, P_1, P_2 и P_3 определяются как в предложении 37: $P_i \stackrel{def}{=} \{0,1\}^{n-1} \cap \mathcal{L}_{n;i}S$.

Нам достаточно показать, что хотя бы одно из множеств P_1, P_2, P_3 пустое, тогда по предложению 30(b) соответствующий слой 2-МДР-кода S будет дополнением L.

(*) *Предположим противное, что ни одно из множеств P_1, P_2 и P_3 непустое.*

(**) *Мы утверждаем, что тогда множества P_1, P_2 и P_3 удовлетворяют условиям предложения* 36. Поскольку S есть 2-МДР-код, его слои по данному направлению составляют двукратное покрытие множества Q_4^{n-1}, а множества P_0, P_1, P_2 и P_3 – двукратное покрытие множества $\{0,1\}^{n-1}$. Поскольку $P_0 = \{0,1\}^{n-1}$, получаем, что P_1, P_2 и P_3 попарно не пересекаются и $P_1 \cup P_2 \cup P_3 = \{0,1\}^{n-1}$. Осталось показать, что для любых $r \in [n-1]$ и $b \in \{0,1\}$ хотя бы одно множество из $\mathcal{L}_{r;b}P_1$, $\mathcal{L}_{r;b}P_2$, $\mathcal{L}_{r;b}P_3$ пустое. Это следует из индукционного предположения. Действительно, 2-МДР-код $\mathcal{L}_{r;b}S$ удовлетворяет всем условиям леммы и по предположению индукции найдётся его слой $\mathcal{L}_{n-1;i}\mathcal{L}_{r;b}S$, $i \in \{1,2,3\}$, являющийся дополнением "линейного" слоя $\mathcal{L}_{n-1;0}\mathcal{L}_{r;b}S$. Используя предложение 33(b,d) и $\mathcal{L}_{n-1;0}\mathcal{L}_{r;b}S \supset \{0,1\}^{n-2}$, получаем

$$\mathcal{L}_{r;b}P_i = \mathcal{L}_{r;b}(\{0,1\}^{n-1} \cap \mathcal{L}_{n;i}S) = \{0,1\}^{n-2} \cap \mathcal{L}_{r;b}\mathcal{L}_{n;i}S = \{0,1\}^{n-2} \cap \mathcal{L}_{n-1;i}\mathcal{L}_{r;b}S = \varnothing.$$

Утверждение (**) доказано.

По предложению 36 множество S удовлетворяет условиям предложения 37. Из последнего следует, что 2-МДР-код S не двудольный, что противоречит условиям леммы. Таким образом, предположение (*) неверно и одно из множеств P_1, P_2 и P_3 пустое.

Пусть $P_j = \varnothing$. Тогда $b = j$, $\{0,1\}^{n-1} \subset L \backslash \mathcal{L}_{n;b}S$, откуда $\mathcal{L}_{n;b}S = Q_4^{n-1} \backslash L$ по предложению 30(b). Утверждение (a) леммы доказано.

(b) Как было показано в п. (a), по направлению k два слоя 2-МДР-кода S являются дополнениями друг друга (до Q_4^{n-1}). Из определения 2-МДР-кода следует, что оставшиеся два слоя также есть дополнения друг друга. Таким образом, соответствующая перестановка слоёв переводит S в его дополнение $Q_4^n \backslash S$, и из двудольности первого следует двудольность второго. ▲

Примеры показывают, что условие линейности слоя в лемме 1 является существенным для наличия в двудольном 2-МДР-коде слоя, дополнительного к данному.

§ 1.2. Разделимость n-арных квазигрупп

Напомним, что n-арной (мультиарной) квазигруппой порядка k называется взаимно однозначно обратимая по каждой своей переменной n-арная функция $f : Q_k^n \to Q_k$.

Обращением n-арной квазигруппы f называется отображение $f^{\langle i \rangle} : Q_k^n \to Q_k$, определяемое тождеством $f^{\langle i \rangle}(x_1, \ldots, x_{i-1}, f(x), x_{i+1}, \ldots, x_n) \equiv x_i$. Из определения следует, что обращение n-арной квазигруппы является n-арной квазигруппой того же порядка.

Напомним, что ретрактом размерности m множества $B \subseteq Q_k^n$ называется сечение $B' \subseteq Q_k^m$ множества B, полученное некоторой фиксацией $n - m$ координат, где $1 \leq m \leq n - 1$.

Рассмотрим произвольную n-арную квазигруппу f. Пусть M' — ретракт размерности m, $m \leq n$, МДР-кода $\mathcal{M}\langle f \rangle \subset Q_k^{n+1}$. Тогда $(m-1)$-квазигруппы $F_i\langle M' \rangle$ называются *ретрактами* n-арной квазигруппы f. Из определений вытекает

Предложение 38. *Функция является мультиарной квазигруппой тогда и только тогда, когда все её ретракты являются мультиарными квазигруппами.*

n-Арные квазигруппы f и g называются эквивалентными (изотопными), если эквивалентны (изотопны) МДР-коды $\mathcal{M}\langle f\rangle$ и $\mathcal{M}\langle g\rangle$. В частности, n-арная квазигруппа и все её обращения эквивалентны. n-Арные квазигруппы f и g называются *главно изотопными*, если существует такая изотопия $\overline{\tau}$, что $f(\overline{x}) = g(\overline{\tau x})$.

n-Арная квазигруппа f называется *разделимой*, если имеются целое число m, $2 \leq m < n$, $(n-m+1)$-арная квазигруппа h, m-арная квазигруппа g и перестановка $\sigma \in S_n$ такие, что

$$f(x_1, \ldots, x_n) \equiv h(g(x_{\sigma(1)}, \ldots, x_{\sigma(m)}), x_{\sigma(m+1)}, \ldots, x_{\sigma(n)}).$$

Такие представления мультиарных квазигрупп в виде суперпозиции будем называть нетривиальными. Если h и g можно выбрать так, чтобы $\sigma(i) \equiv i + t \mod n$, $t \leq n - m$, то f называется *приводимой*.

При $n = 1, 2$ все n-арные квазигруппы считаются неразделимыми.

Следующие утверждения непосредственно вытекают из определения разделимой n-арной квазигруппы.

Предложение 39. *Мультиарная квазигруппа f представляется в виде суперпозиции $f(x, y) = g(h(x), y)$ тогда и только тогда, когда для любых наборов аргументов y, x, x' из равенства $f(x, \overline{0}) = f(x', \overline{0})$ следует равенство $f(x, y) = f(x', y)$.*

Доказательство. Необходимость очевидна. Докажем достаточность. Выделим из набора x первую переменную x_1 и определим $h(x) = x_1$, если $f(x, \overline{0}) = f(x_1, \overline{0}, \overline{0})$. Функция h является мультиарной квазигруппой по определению. Пусть $g(x_1, y) \stackrel{def}{=} f(x_1, \overline{0}, y)$. Имеем

$$f(x, y) = f(x_1, \overline{0}, y) = g(x_1, y) = g(h(x), y).$$

▲

Предложение 40. (геометрический критерий разделимости). *Если n-арная квазигруппа порядка k $(n \geq 3)$ при произвольной фиксации некоторого набора из m переменных, $2 \leq m \leq n-1$, имеет только k различающихся ретрактов, то она является разделимой.*

Предложение 41. (a) *Изотопные n-арные квазигруппы разделимы или неразделимы одновременно.* (b) *Если n-арная квазигруппа f разделима, то и её обращения $f^{\langle i \rangle}$, $i \in [n]$, разделимы.*

Таким образом, разделимый МДР-код можно корректно определить как график разделимой n-арной квазигруппы.

Предложение 42. МДР-*код разделим тогда и только тогда, когда его можно представить в виде $M = \{(x, y) \mid f(x) = g(y)\}$, где f и g — мультиарные квазигруппы, имеющие больше одного аргумента.*

Теорема 3 ([73]). *n-Арную квазигруппу f ($n \geq 2$) можно представить в виде суперпозиции ровно одним из двух способов: либо*

$$f(\overline{x}) \equiv q_0(q_1(\tilde{x}_1), ..., q_m(\tilde{x}_m)), \tag{1.8}$$

где q_j суть n_j-арные квазигруппы при любом $j, 1 \leq j \leq m$, $m \geq 2$, q_0 есть неразделимая m-арная квазигруппа, не эквивалентная группе, $\tilde{x}_j$ — некоторые наборы переменных x_i, $i \in I_j$, где $\{I_j\}_{j=1,...,m}$ — разбиение множества $[n]$ на наборы мощности $n_1, \ldots, n_m$; либо

$$f(\tilde{x}_1, \ldots, \tilde{x}_m) \equiv q_1(\tilde{x}_1) * ... * q_m(\tilde{x}_m), \tag{1.9}$$

где $*$ есть ассоциативная квазигрупповая операция, q_j суть n_j-арные квазигруппы, $1 \leq j \leq k$, не представимые в виде $q_j(\tilde{x}_j) = q'(\tilde{x}'_j) * q''(\tilde{x}''_j)$, $\tilde{x}_j$ — некоторые наборы переменных x_i, $i \in I_j$, где $\{I_j\}_{j=1,...,m}$ — разбиение множества $[n]$ на наборы мощности $n_1, \ldots, n_m$, $m \geq 2$.

Причём в представлениях (1.8) *и* (1.9) *разбиение $\{I_j\}_{j=1,...,m}$ единственно, m-арная квазигруппа q_0 и квазигрупповая операция $*$ определяются единственным образом с точностью до эквивалентности и набор мультиарных квазигрупп $q_1, \ldots, q_m$ единственный с точностью до эквивалентности и перестановки элементов.*

Равенство $n = m$ в представлении (1.8) означает, n-арная квазегруппа f неразделима. Содержание теоремы 3 состоит в единственности представления. Доказательство теоремы можно проводить от противного, исходя из того, что при различных представлениях вида (1.8) различные ретракты оказываются неразделимыми.

Представление (1.8) (или (1.9)) называется *каноническим разложением* n-арной квазигруппы f. Разделимые мультиарные квазигруппы из набора $q_1, \ldots, q_m$ также могут быть представлены в виде суперпозиции мультиарных квазигрупп от меньшего числа аргументов и т. д.

Иногда бывает полезно рассматривать представление мультиарной квазигруппы в виде суперпозиции, в которой неразделимой является внутренняя мультиарная квазигруппа. Очевидно справедливо следующее

Предложение 43. *Любая разделимая n-арная квазигруппа f представима в виде $f(\overline{x}, \overline{y}) \equiv f'(\overline{x}, f''(\overline{y}))$, где f' — n_1-арная квазигруппа, f'' — неразделимая n_2-арная квазигруппа, $n_1 + n_2 = n + 1$, $1 < n_2 < n$.*

Найдём число различных разбиений множества из n элементов. Простой комбинаторный подсчёт показывает, что число $F_{\overline{j},\overline{m}}$ различных разбиений множества $[n]$ на m подмножеств, из которых m_i подмножеств имеет мощность j_i, $1 \leq i \leq t$, $0 < j_1 < \cdots < j_t$, удовлетворяет равенству

$$F_{\overline{j},\overline{m}} = \frac{n!}{(j_1!)^{m_1} \ldots (j_t!)^{m_t}} \frac{1}{m_1! \ldots m_t!}, \tag{1.10}$$

где $m_1 + m_2 + \cdots + m_t = m$, $m_1 j_1 + m_2 j_2 + \cdots + m_t j_t = n$.

Разделимая n-арная квазигруппа f называется *полностью разделимой*, если все её ретракты от 3-х и большего числа переменных разделимы.

Корневой операцией n-арной квазигруппы f будем называть m-арную квазигруппу q_0, если имеет место представление (1.8), и бинарную операцию $*$, если имеет место представление (1.9).

Будем говорить, что две n-арные квазигруппы f и g разделимы *синхронно*, если они имеют представления вида $f(\widetilde{x}, \widetilde{y}) = f_1(\widetilde{x}, f_2(\widetilde{y}))$ и $g(\widetilde{x}, \widetilde{y}) = g_1(\widetilde{x}, g_2(\widetilde{y}))$, где набор переменных $\widetilde{y}$ состоит не менее чем из двух переменных.

Ясно, что арность (число аргументов) неразделимого ретракта n-арной квазигруппы f не может быть больше всех арностей неразделимых мультиарных квазигрупп, входящих в представление f в виде многократной суперпозиции. Тогда из теоремы 3 имеем

Следствие 4. *Если разделимая n-арная квазигруппа f имеет неразделимый ретракт арности $m \geq 2$, который не содержится в неразделимых ретрактах большей арности, то* МДР-*код $\mathcal{M}\langle f\rangle$ можно представить в виде*

$$\mathcal{M}\langle f\rangle = \{\overline{x} \in Q_k^{n+1} : q_{m+1}(x_{n+1}, \tilde{x}_{m+1}) = q_0(q_1(\tilde{x}_1), ..., q_m(\tilde{x}_m))\}, \qquad (1.11)$$

где q_j суть n_j-арные квазигруппы при $j, 1 \leq j \leq m+1$, q_0 есть неразделимая m-арная квазигруппа, $\tilde{x}_j$ — некоторые наборы переменных x_i, $i \in I_j$, где $\{I_j\}_{j=1,\ldots,m+1}$ — разбиение множества $[n]$ на наборы мощности $n_1, \ldots, n_{m+1}$.

Если представление (1.11) выбрано так, что $m+1$ есть максимальная размерность неразделимого ретракта МДР-кода $\mathcal{M}\langle f\rangle$, и среди таких представлений мощность множества I_{m+1} выбрана минимально возможной, то представление (1.11) единственно (в смысле, аналогичном сформулированному в теореме 3). Такое представление будем называть *каноническим представлением* МДР-кода $\mathcal{M}\langle f\rangle$.

Разделимой n-арной квазигруппе f, имеющей представление (1.8) или (1.9), поставим в соответствие корневое дерево $T(f)$, внутренние вершины которого помечены операциями, а листья — переменными. Построим дерево рекуррентно. Предположим, что T_j — дерево, соответствующее функции q_j $(1 \leq j \leq m)$. Тогда дерево n-арной квазигруппы f определяется как корень, помеченный операцией q_0 (или $*$), с выходящими из него m рёбрами, причём к j-му ребру присоединено дерево T_j. Пример дерева некоторой 9-арной квазигруппы приведён на рис. 1.6.

n-Арная квазигруппа f называется *приведённой* или *n-арной лупой* (при $n = 2$ просто лупой), если найдётся такой элемент $o \in Q_k$, что для всех $i \in [n]$ и $a \in Q_k$ имеет место равенство $f(o, \ldots, o, a, o, \ldots, o) = a$. Такой элемент $o \in Q_k$ называется нейтральным элементом n-арной лупы. Ассоциативная бинарная лупа является группой.

Для удобства дальнейшего изложения будем считать, что нейтральным элементом рассматриваемых n-арных луп является $0 \in Q_k$. Перестановку (1-арную квазигруппу) $\tau : Q_k \to Q_k$ будем называть *приведённой*, если $\tau(0) = 0$.

Предложение 44 ([49]). *Пусть $h : Q_k^n \to Q_k$ есть n-арная квазигруппа; тогда найдётся единственная изотопия $(\tau_0, \tau_1, \ldots, \tau_n)$, где $\tau_0 = (0, a)$, $a \in Q_k$, и перестановки*

Рис. 1.6: Дерево $T(f)$, где $f(x_1,\dots,x_9) \equiv (\psi(x_1,x_2,(x_3\star x_4))\diamond((x_5 * x_6)\star(x_7*(x_8\star x_9)))$.

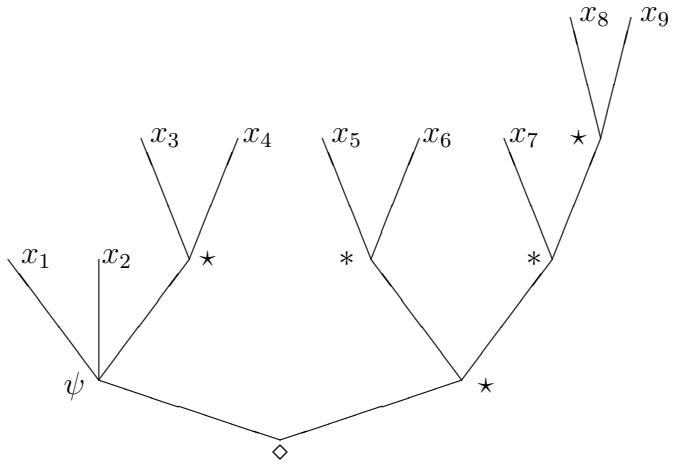
$\tau_1,\dots,\tau_n : Q_k \to Q_k$ приведённые такая, что

$$h(\bar{x}) \equiv \tau_0 g(\tau_1 x_1, \tau_2 x_2, \dots, \tau_n x_n), \tag{1.12}$$

где g – приведённая n-арная квазигруппа, $\bar{x} = (x_1, x_2, \dots, x_n)$

Используя предложение 44, нетрудно показать, что если n-арная квазигруппа f является приведённой, то n_j-арные квазигруппы q_j в канонических представлениях (1.8) и (1.9) можно выбрать приведёнными. В этом случае n_j-арные квазигруппы q_j в канонических представлениях (1.8) и (1.9) определяются единственным образом с точностью до перестановки переменных внутри разбиений I_j.

Далее будет доказано, что исходя из некоторой информации о разделимости ретрактов n-арной квазигруппы, можно сделать вывод о разделимости самой квазигруппы.



В следующем предложении приведено представление разделимой квазигруппы через её ретракты.

Предложение 45 ([148]). *Пусть h и g — $(n-m+1)$-арная и m-арная квазигруппы,*

$\bar{o} \in Q_k^{m-1}$, $\bar{\theta} \in Q_k^{n-m}$ *и*

$$f(x, \bar{y}, \bar{z}) \equiv h(g(x, \bar{y}), \bar{z}),$$
$$h_0(x, \bar{z}) \stackrel{def}{=} f(x, \bar{o}, \bar{z}), \qquad g_0(x, \bar{y}) \stackrel{def}{=} f(x, \bar{y}, \bar{\theta}), \qquad \delta(x) \stackrel{def}{=} f(x, \bar{o}, \bar{\theta}), \tag{1.13}$$

где $x \in Q_k$, $\bar{y} \in Q_k^{m-1}$, $\bar{z} \in Q_k^{n-m}$. *Тогда*

$$f(x, \bar{y}, \bar{z}) \equiv h_0(\delta^{-1}(g_0(x, \bar{y})), \bar{z}). \tag{1.14}$$

Доказательство. Из равенств (1.13) имеем

$$h_0(\cdot, \bar{z}) \equiv h(g(\cdot, \bar{o}), \bar{z}), \quad g_0(x, \bar{y}) \equiv h(g(x, \bar{y}), \bar{\theta}), \quad \delta^{-1}(\cdot) \equiv g^{-1}(h^{-1}(\cdot, \bar{\theta}), \bar{o}).$$

Подставляя эти представления для функций h_0, g_0 и δ^{-1} в (1.14), получаем требуемое. ▲

Пусть множество $A_k^n(s) \subset Q_k^n$ состоит из всех наборов, в которых не более s элементов не равны 0.

Лемма 2 ([148]). *Пусть* $q, f : Q_k^n \to Q_k$ *— разделимые* n*-арные квазигруппы,* $n \geq 4$. *Предположим, что для всех* $\bar{a} \in A_k^n(n-1)$ *справедливо равенство*

$$q(\bar{a}) = f(\bar{a}). \tag{1.15}$$

Тогда $q(\bar{x}) = f(\bar{x})$ *для всех* $\bar{x} \in Q_k^n$.

Доказательство. Применим метод индукции по n. При $n = 4$ достаточно перебрать все возможные представления q и f в виде суперпозиций и, применяя предложение 45, убедиться в справедливости утверждения леммы.

Пусть $n > 4$ и для $(n-1)$-арных квазигрупп утверждение доказано. Нетрудно видеть, что возможно выбрать аргумент так, чтобы при любой его фиксации полученные ретракты функций q и f были разделимы. Поскольку эти ретракты удовлетворяют предположению индуции при $n-1$, они равны. Тогда n-арные квазигруппы q и f совпадают. ▲

Следствие 5. *Если* n*-арная квазигруппа* $f : Q_k^n \to Q_k$ *не содержит неразделимых ретрактов арности большей чем* m, $n > m > 2$, *то она однозначно восстанавливается по своим значениям на* $A_k^n(m)$.

Замечание 4. *По своим значениям на множестве $A_k^n(2)$ полностью неразделимая n-арная квазигруппа, вообще говоря, не восстанавливается. Например, разделимые 3-квазигруппы $q(x_1, x_2, x_3) \equiv (x_1 * x_2) * x_3$ и $f(x_1, x_2, x_3) \equiv x_1 * (x_2 * x_3)$, где $*$ есть бинарная операция с нейтральным элементом 0 (т. е. лупа) совпадают при $x_1 = 0$, $x_2 = 0$ или $x_3 = 0$; однако не равны в случае, когда операция $*$ не ассоциативна.*

С другой стороны частичную n-арную квазигруппу с полностью разделимыми опорными ретрактами можно дополнить до всюду определённой полностью разделимой n-арной квазигруппы. А именно, справедлива

Лемма 3 ([154]). *Предположим, что все главные 3- и 4-арные ретракты n-арной квазигруппы f являются разделимыми. Тогда найдётся полностью разделимая n-арная квазигруппа ϕ_f, которая совпадает с f на множестве $A_k^n(3)$.*

Доказательство леммы 3 основано на построении дерева разложения полностью разделимой n-арной квазигруппы по известным деревьям разложения 3-арных ретрактов.

Из лемм 2 и 3 непосредственно следует

Следствие 6 ([154]). *Пусть все главные 3- и 4-арные ретракты разделимой n-арной квазигруппы f ($n \geq 5$) разделимы. Тогда n-арная квазигруппа f полностью разделима.*

Доказательство леммы 3 было опубликовано в работе [150] как часть доказательства характеризационной теоремы 7 для n-арных квазигрупп порядка 4. Затем утверждение удалось обобщить на случай произвольного порядка (см. [154]). При обобщении на произвольный порядок доказательства леммы 3 пришлось отказаться от удобного изложения в терминах графов. Случай порядка 4 оказывается проще, поскольку все 2-квазигруппы являются изотопами коммутативных групп, таким образом, нет необходимости рассматривать неассоциативные 2-квазигруппы и некоммутативные группы.

Пусть $f : Q_k^n \to Q_k$ — n-арная квазигруппа. Если найдётся подмножество $\Omega \subset Q_k$, для которого $f|_{\Omega^n} \subseteq \Omega$, то функция $g = f|_{\Omega^n}$ является n-арной квазигруппой порядка $|\Omega|$. Функцию g будем называть подквазигруппой n-арной квазигруппы f. Функцию

g можно также рассматривать как дополняемую частичную n-арную квазигруппу порядка k.

Замечание 5. *Из разделимости n-арной квазигруппы следует разделимость её подквазигруппы.*

Предложение 46 ([148]). *Для любого $n \geq 3$, k и $k' \leq \lfloor k/2 \rfloor$ найдётся разделимая n-арная квазигруппа порядка k, имеющая подквазигруппу порядка k'.*

Доказательство. При $n = 2$ из теоремы 17 (Райзера) о латинских квадратах сразу следует утверждение: для любого k и $k' \leq \lfloor k/2 \rfloor$ и любой 2-квазигруппы φ порядка k' найдётся 2-квазигруппа ψ порядка k, имеющая подквазигруппу φ.

Рассмотрим n-арные квазигруппы $f(x_1, \ldots, x_n) = \psi(x_1, \psi(x_2, \ldots \psi(x_{n-1}, x_n) \ldots)$ и $g(x_1, \ldots, x_n) = \varphi(x_1, \varphi(x_2, \ldots \varphi(x_{n-1}, x_n) \ldots)$. Нетрудно видеть, что g есть подквазигруппа n-арной квазигруппы f. ▲

Непосредственно из определений следует

Предложение 47 ([148]). *Пусть n-арная квазигруппа $q : Q_k^n \to Q_k$ имеет подквазигруппу $g : \Omega^n \to \Omega$, $g = q|_{\Omega^n}$, $\Omega \subset Q_k^n$. Пусть $h : \Omega^n \to \Omega$ — n-арная квазигруппа. Тогда функция f, заданная равенствами*

$$f(\bar{x}) \stackrel{def}{=} \begin{cases} h(\bar{x}), & \text{если } \bar{x} \in \Omega^n \\ q(\bar{x}), & \text{если } \bar{x} \notin \Omega^n, \end{cases} \tag{1.16}$$

является n-арной квазигруппой порядка k.

Говорят, что n-арная квазигруппа f получена из n-арной квазигруппы q *свитчингом* подквазигруппы g.

Очевидно, что для любого n имеется две n-арные квазигруппы порядка 2 (счётчик чётности). По предложению 16 n-арные квазигруппы порядка 3 составляют единственный класс эквивалентности, включающий соответствующую итерированную группу. При $n = 1, 2$ все n-арные квазигруппы неразделимы по определению. Покажем, что в остальных случаях имеются неразделимые n-арные квазигруппы.

Теорема 4 ([148]). *При любых $n \geq 3$ и $k \geq 4$ существует неразделимая n-арная квазигруппа порядка k.*

Доказательство. По предложению 46 можно построить разделимую n-арную квазигруппу $q : Q_k^n \to Q_k$ порядка k с подквазигруппой $g : \{0,1\}^n \to \{0,1\}$ порядка 2. Пусть $h = g \oplus 1$ — n-арная квазигруппа порядка 2 и n-арная квазигруппа f получена из q свитчингом по формуле (1.16). При $n \geq 4$ n-арная квазигруппа f неразделима по лемме 2. При $n = 3$ n-арная квазигруппа f неразделима по предложению 40. ▲

Из замечания 5 следует справедливость предыдущего утверждения и для n-арных квазигрупп бесконечного порядка.

Сформулируем критерий разделимости n-арной квазигруппы в терминах разделимости её ретрактов.

Теорема 5 ([154]). *Пусть f — неразделимая n-арная квазигруппа, $n \geq 4$. Тогда f имеет неразделимый $(n-1)$-арный или $(n-2)$-арный ретракт. Более того, если порядок n-арной квазигруппы f конечный и простой, то f имеет неразделимый $(n-1)$-арный ретракт.*

Другими словами, если все $(n-1)$- и $(n-2)$-арные ретракты n-арные квазигруппы разделимы, то сама n-арная квазигруппа также разделима. Для разделимости n-арной квазигруппы простого конечного порядка достаточно разделимости всех ее $(n-1)$-арных ретрактов.

Обозначим через $\kappa(f)$ максимальную арность неразделимого ретракта n-арной квазигруппы f. Доказательство теоремы 5 в соответствии со значением параметра $\kappa(f)$ разделяется на три случая, которые можно сформулировать в виде лемм.

Случай $\kappa = 2$ рассмотрен в следствии 6 даже с более слабой посылкой: достаточно разделимости только 3- и 4-арных ретрактов.

Лемма 4 (случай $3 \leq \kappa \leq n-3$, [147]). *Если $\kappa(f) \in \{3, \ldots, n-3\}$, то n-арная квазигруппа f разделима.*

Доказательство леммы состоит из трёх частей. На первом этапе нужно показать, что ретракты, полученные любой фиксацией некоторых $n - \kappa$ переменных, эквивалентны. На втором этапе нужно показать, что ретракты большей арности разделимы синхронно, поскольку в противном случае найдётся неразделимый ретракт арности,

большей чем κ. На последнем этапе достаточно показать, что n-арная квазигруппа, составленная из синхронно разделимых ретрактов малой арности, является разделимой, когда все ретракты размерности на 1 и на 2 большей чем κ, разделимы.

Наконец, последняя лемма расширяет диапазон достаточных для разделимости значений κ для простых порядков.

Лемма 5 (случай $\kappa = n - 2$, [154]). *Пусть $n \geq 4$. Если n-арная квазигруппа f конечного простого порядка имеет неразделимый $(n-2)$-арный ретракт, а все ее $(n-1)$-арные ретракты разделимы, то f — разделимая.*

Существенная разница (в данном контексте) случая простого порядка k от непростого состоит в справедливости следующего утверждения.

Предложение 48 ([154]). *Пусть f — 2-квазигруппа простого порядка k. Если найдутся нетождественные перестановки $\nu, \mu : Q_k \to Q_k$ такие, что либо $f(\mu(x), \nu(y)) \equiv f(x, y)$, либо $f(\mu(x), y) \equiv \nu(f(x, y))$, либо $f(x, \nu(y)) \equiv \mu(f(x, y))$, то*

(a) *μ и ν являются циклами на k элементах;*

(b) *2-квазигруппа f изотопна циклической группе Z_k.*

Доказательство леммы 5 в целом аналогично доказательству леммы 4 за исключением того, что для обоснования синхронной разделимости ретрактов размерности $n - 1$ применяется предложение 48. Случай $n = 4$ в лемме 5 приходится рассматривать отдельно из-за тривиальности ретрактов размерности $n - 3$.

Как следует из статьи Д.С.Кротова [145] для любой четной арности $n \geq 4$ и любого порядка $q = 4k$ существует неразделимая n-арная квазигруппа, все $(n - 1)$-арные ретракты которой разделимы. Таким образом, последнее утверждение теоремы 5 не может быть расширено на все порядки. Однако, в случае нечётного n или составного порядка $q \not\equiv 0 \bmod 4$ вопрос о том, следует ли из разделимости всех $(n - 1)$-арных ретрактов разделимость самой n-арной квазигруппы, остается нерешенным.

Сформулированные выше признаки разделимости использованы для характеризации интересного подкласса класса n-арных квазигрупп порядков 5 и 7. Будем говорить, что n-арная квазигруппа порядка k *сублинейная*, если все ее бинарные ретракты изотопны циклической группе Z_k.

Теорема 6 ([154]). *Все сублинейные n-арные квазигруппы порядка* 5 *разделимы при $n \geq 4$. Все сублинейные n-арные квазигруппы порядка* 7 *разделимы при $n \geq 3$.*

Замечание 6. *Существует пример неразделимой сублинейной* 3*-квазигруппы порядка* 5*.*

Кроме того, теорема 5 применяется для конструктивной характеризации n-арных квазигрупп порядка 4.

§ 1.3. n-Арные квазигруппы порядка 4

Известно (см., например, [4]), что все 2-квазигруппы порядка 4 изотопны либо группе $Z_2 \times Z_2$, либо группе Z_4. Всюду далее будем полагать, что нейтральный элемент $0 \in Q_4$ зафиксирован. Все 2-квазигруппы, изотопные $Z_2 \times Z_2$, можно перевести главной изотопией в группу $Z_2 \times Z_2$ (с $0 \in Q_4$ в качестве нейтрального элемента). 2-Квазигруппы, изотопные группе Z_4, образуют относительно главной изотопии три класса эквивалентности (класс определяется тем, какой элемент группы 1, 2 или 3 имеет порядок два). В дальнейшем под групповой операцией на множестве Q_4 будем подразумевать одну из четырёх перечисленных.

Напомним, что 2-МДР-код $S \subset Q_4^n$ называется линейным, если

$$\chi_S(x_1, \ldots, x_n) \equiv \chi_{S_1}(x_1) \oplus \chi_{S_2}(x_2) \oplus \cdots \oplus \chi_{S_n}(x_n), \tag{1.17}$$

где $\oplus$ есть сложение по модулю 2 и S_i, $i \in [n]$, являются двухэлементными подмножествами в Q_4.

В выражении (1.17) любая из функций $\chi_{S_j}(x_j)$ может быть заменена на $\chi_{Q_4 \setminus S_j}(x_j) \oplus 1$. Для определённости из двух множеств S_j и $Q_4 \setminus S_j$ будем выбирать то, которое содержит 0. Таким образом, каждый линейный 2-МДР-код $S \subset Q_4^n$, $\chi_S(\bar{x}) \equiv \delta \oplus \bigoplus_{j=1}^{n} \chi_{\{0,\alpha_j\}}(x_j)$, определяется чётностью $\delta \in \{0, 1\}$ и упорядоченным набором $(\alpha_1, \ldots, \alpha_n) \in Q_4^n$, который будем называть *характеристикой* 2-МДР-кода S.

МДР-код $\mathcal{M}\langle f \rangle$ будем называть: *полулинейным*, если он содержится в линейном 2-МДР-коде; *a-полулинейным*, если он содержится в линейном 2-МДР-коде с характеристикой $(a, \ldots, a)$ и $\delta = 1$, т. е. $\mathcal{M}\langle f \rangle \subset S$, где $\chi_S(\bar{x}) = 1 \oplus \bigoplus_{i=1}^{n} \chi_{\{0,a\}}(x_i)$;

анти-a-полулинейным, если $\mathcal{M}\langle f\rangle \subset S$, где $\chi_S(\bar{x}) = \bigoplus_{i=1}^{n} \chi_{\{0,a\}}(x_i)$. МДР-код $\mathcal{M}\langle f\rangle$ будем называть *линейным*, если имеется более одного линейного 2-МДР-кода, содержащего $\mathcal{M}\langle f\rangle$. В перечисленных случаях n-арная квазигруппа f также называется *полулинейной*, *a-полулинейной*, *анти-a-полулинейной* и *линейной* соответственно. Полулинейная 3-квазигруппа, изображена на рис.1.2.

Две полулинейные n-арные квазигруппы f и g будем называть *противоположными*, если $\chi_{\mathcal{S}_{a,b}\langle f\rangle} = \chi_{\mathcal{S}_{a,b}\langle g\rangle} \oplus 1$ для некоторых $a, b \in Q_4$, где $\mathcal{S}_{a,b}\langle f\rangle = \mathcal{M}_a\langle f\rangle \cup \mathcal{M}_b\langle f\rangle$ — линейный 2-МДР-код. В частности, a-полулинейная и анти-a-полулинейная n-арные квазигруппы являются противоположными.

Следующие утверждения, являющиеся непосредственным следствием определений, имеются в [49] и [150].

Предложение 49. *Из четырёх бинарных луп порядка* 4 *одна (изоморфная группе* $Z_2 \times Z_2$*) является линейной, а три остальных* 1-, 2- *и* 3- *полулинейными соответственно.*

Предложение 50 ([49]).

(a) *Ретракты полулинейной n-арной квазигруппы являются полулинейными.*

(b) *Ретракты a-полулинейной n-арной квазигруппы являются a-полулинейными или анти-a-полулинейными.*

(c) *Обращения полулинейной* (*линейной*) *n-арной квазигруппы относительно любой переменной полулинейны* (*линейны*).

(d) *Любая полулинейная n-арная квазигруппа главно изотопна a-полулинейной n-арной лупе для некоторого $a \in Q_4$.*

Предложение 51 ([49]).

(a) *n-Арная квазигруппа f является полулинейной тогда и только тогда, когда найдутся такие $a, b \in Q_4$, что* 2-МДР-*код $\mathcal{S}_{a,b}\langle f\rangle$ — линейный.*

(b) 2-МДР-*коды $\mathcal{S}_{a,b}\langle f\rangle$ линейны для всех $a, b \in Q_4$, $a \neq b$, если найдутся различные $a, b, c \in Q_4$ такие, что* 2-МДР-*коды $\mathcal{S}_{a,b}\langle f\rangle$ и $\mathcal{S}_{a,c}\langle f\rangle$ являются линейными.*

(c) *n-Арная квазигруппа f является линейной тогда и только тогда, когда для всех $a, b \in Q_4$, $a \neq b$, 2-*МДР-*код $\mathcal{S}_{a,b}\langle f\rangle$ — линейный.*

(d) *Любая линейная n-арная квазигруппа f представима в виде*

$$f(x_1,\dots,x_n) \equiv \pi_1(x_1) + \cdots + \pi_n(x_n), \tag{1.18}$$

т. е. изотопна n-арной квазигруппе $\ell_0(\overline{x}) \stackrel{def}{=} x_1 + x_2 + \cdots + x_n$, где $+$ — групповая операция в $Z_2 \times Z_2$ и π_i — перестановки Q_4.

(e) *Пусть q — полулинейная m-арная квазигруппа $2 \le m$. Тогда композиция $\ell_0(\overline{x}, q(\overline{y}))$ является полулинейной квазигруппой.*

Из предложения 44 следует, что справедливо

Предложение 52. *Пусть f — разделимая a-полулинейная n-арная лупа, тогда f можно представить как суперпозицию вида* (1.8) *или* (1.9) *a-полулинейных луп.*

Элементы группы $(Q_4, +)$ удобно представлять в виде двумерных двоичных векторов $\overline{(\mu^1,\mu^2)}$, $\mu^i \in \{0,1\}$ с естественным отождествлением $0 = \overline{(0,0)}, 1 = \overline{(1,0)}, 2 = \overline{(0,1)}, 3 = \overline{(1,1)}$, причём $\overline{(\mu^1,\mu^2)} + \overline{(\nu^1,\nu^2)} = \overline{(\mu^1 \oplus \nu^1, \mu^2 \oplus \nu^2)}$. Пусть $S \subset Q_4^n$ — линейный 2-МДР-код с характеристикой $(1,\dots,1)$. Тогда

$$S = \{(\overline{(\mu_1^1,\mu_1^2)},\dots,\overline{(\mu_n^1,\mu_n^2)}) : \bigoplus_{i=1}^{n} \mu_i^2 = \delta\},$$

где $\delta \in \{0,1\}$. Из определения 1-полулинейности ясно, что любой 1-полулинейный МДР-код $M \subset S$ можно представить в виде

$$M = \{(\overline{(\mu_1^1,\mu_1^2)},\dots,\overline{(\mu_n^1,\mu_n^2)}) : \bigoplus_{i=1}^{n} \mu_i^2 = \delta, \bigoplus_{i=1}^{n} \mu_i^1 = \lambda_M(\mu_1^2,\dots,\mu_n^2)\}, \tag{1.19}$$

где λ_M — некоторая булева функция, определённая на множестве $E_\delta^n = \{(\mu_1^2,\dots,\mu_n^2) : \bigoplus_{i=1}^{n} \mu_i^2 = \delta\}$ булевых векторов чётности δ. И наоборот, множество, удовлетворяющее равенству (1.19), является 1-полулинейным МДР-кодом.

Из перечисленных выше свойств видно, что каждая полулинейная n-арная квазигруппа однозначно задаётся булевой функцией и изотопией, переводящей её в 1-полулинейную.

Имеется следующий критерий разделимости полулинейных n-арных квазигрупп.

Предложение 53. (лемма 1, [145]). *Пусть* МДР-*код M удовлетворяет равенству* (1.19). *Тогда* МДР-*код M разделим, если и только если функция λ_M представима в виде $\lambda_M(\overline{\mu}', \overline{\mu}'') \equiv \lambda'(\overline{\mu}') \oplus \lambda''(\overline{\mu}'')$ и наборы $\overline{\mu}'$ и $\overline{\mu}''$ содержат более одной переменной.*

Главное утверждение в теории n-арных квазигрупп порядка 4 заключается в следующем.

Теорема 7 ([150]). *Каждая n-арная квазигруппа порядка 4 является разделимой или полулинейной.*

Теорема 7 обеспечивает конструктивную характеризацию множества n-арных квазигрупп порядка 4. Действительно, каждой n-арной квазигруппе по теореме 3 соответствует единственное дерево разложения с приписанными к каждой вершине дерева неразделимыми, а значит, по теореме 7, полулинейными n-арными квазигруппами. Для неразделимой n-арной квазигруппы дерево будет состоять только из корня. Отметим, что как видно из предложения 53, полулинейная n-арная квазигруппа может быть разделимой.

Доказательство теоремы 7 так же, как и доказательство теоремы 5, разделяется на случаи в зависимости от величины $\kappa(f)$ — максимальной размерности неразделимого ретракта рассматриваемой n-арной квазигруппы f.

При $2 \leq \kappa(f) \leq n-3$ утверждение теоремы 7 следует из теоремы 5.

При $n-2 \leq \kappa(f) \leq n-1$ в доказательстве теоремы 7 используется математическая индукция: предполагается, что неразделимые m-арные квазигруппы являются полулинейными при $m < n$. Требуемое следует из двух лемм 6 и 7.

Лемма 6 (случай $\kappa = n-2$, [150]). *Пусть $n \geq 5$. Если n-арная квазигруппа f порядка 4 имеет полулинейный неразделимый $(n-2)$-арный ретракт и все ее $(n-1)$-арные ретракты разделимые, то f является разделимой или полулинейной.*

Доказательство леммы 6 подобно доказательству леммы 5, причём в качестве признака неразделимости полулинейной n-арной квазигруппы используется предложение 39, а роль предложения 48 играет

Предложение 54. *Пусть s и t есть 2-квазигруппы. Положим $s_i(x) \stackrel{def}{=} s(x,i)$ и $t_i(x) \stackrel{def}{=} t(x,i)$. Пусть $s_0 = t_0 = id$ и пусть для каждого i либо $t_i s_i^{-1} = id$, либо $t_i s_i^{-1} = \pi = (0,1)(2,3)$. Тогда либо $s \equiv t$, либо для некоторой перестановки ϕ 2-квазигруппа $s(x, \phi y)$ является 1-полулинейной.*

Главной частью доказательства теоремы 7 является рассмотрение случая $\kappa(f) =$

$n-1$. Именно трудность рассмотрения случая $\kappa(f) = n-1$ не позволяет получить характеризацию n-арных квазигрупп порядков, больших 4.

Лемма 7 (случай $\kappa = n-1$, [49, лемма 4]). *Если n-арная квазигруппа f порядка 4 имеет полулинейный $(n-1)$-арный ретракт, то она является разделимой или полулинейной.*

Доказательство леммы 7 основано на лемме 1 об антислое и лемме 8 о связи между разложимостью 2-МДР-кода и разделимостью МДР-кода, содержащегося в этом 2-МДР-коде. Лемму 1 о линейном антислое можно переформулировать следующим образом:

Пусть f — n-арная квазигруппа порядка 4, $f' = f|_{x_i=c}$ — некоторый полулинейный $(n-1)$-арный ретракт f и $S = \mathcal{S}_{0,1}\langle f'\rangle$ — линейное множество. Тогда имеется такой $d \in Q_4$, что ретракт $f'' = f|_{x_i=d}$ противоположен ретракту f', т. е. $\mathcal{S}_{0,1}\langle f''\rangle = Q_4^n \setminus \mathcal{S}_{0,1}\langle f'\rangle$.

Лемма 8 ([146]). *Пусть* МДР-*код C полностью лежит в некотором* 2-МДР-*коде $S \subset Q_4^n$. Тогда C может быть представлен следующим образом:*

$$C = \{(x_1,\dots,x_n) \mid (g_1(\tilde{x}_1),\dots,g_m(\tilde{x}_m)) \in B_C\}, \tag{1.20}$$

$$C = \{(x_1,\dots,x_n) \mid (\tilde{x}_j, y_j) \in C_j,\ j=1,\dots,m;\ (y_1,\dots,y_m) \in B_C\}, \tag{1.21}$$

где

- $\tilde{x}_j = (x_{i_{j,1}},\dots,x_{i_{j,n_j}})$,
- $B_C \subset Q_4^m$ — *полулинейный* МДР-*код*,
- $C_j \subset Q_4^{n_j+1}$ — *некоторый* МДР-*код*,
- *отображение* $g_j : {Q_4}^{n_j} \to Q_4$ *является* n_j-*арной квазигруппой*, $j \in [m]$,
- *числа* m, n_j, $i_{j,s}$ *для* МДР-*кода* S *определяются теоремой 2.*

Доказательство. Легко видеть, что равенства (1.20) и (1.21) эквивалентны, если $C_j = \{(\tilde{z}, g_j(\tilde{z})) \mid \tilde{z} \in Q_4^{n_j}\}$.

Докажем равенство (1.20). Если $m = 1$, то утверждение тривиально. Предположим, что $m > 1$. По теореме 2(c), графы ΓS_j и $\Gamma(Q_4^{n_j} \backslash S_j)$ двудольные (множества S_j определены в теореме 2(a)). Для каждого $j \in [m]$ можно легко определить n_j-арную квазигруппу g_j такую, что множество ее нулей и единиц совпадает с S_j. Точнее, определим множество нулей g_j как долю графа ΓS_j, множество единиц как другую долю ΓS_j; множество двоек как долю графа $\Gamma(Q_4^{n_j} \backslash S_j)$, и множество троек как другую долю $\Gamma(Q_4^{n_j} \backslash S_j)$, т. е.

$$\chi_{S_j}(\tilde{x}_j) \equiv \chi_{\{0,1\}}(g_j(\tilde{x}_j)). \tag{1.22}$$

Определим линейный 2-МДР-код $D \subset Q_4^m$ равенством

$$\chi_D(y_1, \ldots, y_k) \stackrel{def}{=} \chi_{\{0,1\}}(y_1) \oplus \ldots \oplus \chi_{\{0,1\}}(y_m) \oplus \delta. \tag{1.23}$$

Пользуясь (1.22) и (1.23), мы можем переписать равенство (1.4) следующим образом:

$$S = \{(x_1, \ldots, x_n) \,|\, (g_1(\tilde{x}_1), \ldots, g_m(\tilde{x}_m)) \in D\}.$$

Если $B \subset D$ является МДР-кодом, то множество

$$\{(x_1, \ldots, x_n) \,|\, (g_1(\tilde{x}_1), \ldots, g_m(\tilde{x}_m)) \in B\} \subset S$$

также является МДР-кодом. 2-МДР код D имеет $2^{2^{m-1}}$ подмножеств — МДР-кодов (все они полулинейны). Получаем, что $2^{2^{m-1}}$ различных МДР-кодов — подмножеств множества S представимы в виде (1.20).

С другой стороны, по теореме 2(b) множество S является объединением 2^{m-1} простых унитрейдов. По предложению 4(a) имеется ровно $2^{2^{m-1}}$ подмножеств S, которые являются МДР-кодами. Следовательно, все эти МДР-коды имеют представление (1.20), и код C — один из них (где $B = B_C$). ▲

Если МДР-код C в гиперкубе произвольного порядка представим в виде (1.20), то при $2 < m < n$ или при наличии двух наборов переменных $\tilde{x}_j$ мощности, большей двух, он разделим по предложению 42. В случае $m = n$ МДР-код C полулинеен. Отметим, что представление вида (1.20) при $m = 2$ имеется для любого МДР-кода. Из леммы 8 следует, что если 2-МДР-код S содержит более четырёх МДР-кодов (а значит, не менее восьми), то все эти МДР-коды разделимы.

Предложение 55 ([49]). *Пусть q есть n-арная квазигруппа и частичная n-арная квазигруппа $g \stackrel{def}{=} q|_{Q_4^{n-1}\times\{0,1\}}$ имеет более двух продолжений до всюду определённой n-арной квазигруппы. Тогда n-арная квазигруппа q разделима или полулинейна.*

Доказательство. Действительно, рассмотрим 2-МДР-код S, определённый равенством $S \stackrel{def}{=} \mathcal{M}\langle q^{\langle n\rangle}\rangle \cup \mathcal{M}\langle \pi q^{\langle n\rangle}\rangle$, где перестановка π определена в предложении 54. Для любого продолжения f частичной n-арной квазигруппы g имеем $(f^{\langle n\rangle})^{-1}\{0,1\} = (q^{\langle n\rangle})^{-1}\{0,1\}$ и $(f^{\langle n\rangle})^{-1}\{2,3\} = (q^{\langle n\rangle})^{-1}\{2,3\}$. Тогда $\mathcal{M}\langle f^{\langle n\rangle}\rangle \subset S$. Следовательно, S содержит более 4-х МДР-кодов и все они разделимы или полулинейны по лемме 8.▲

Доказательство леммы 7. Пусть q есть n-арная квазигруппа и найдётся $\alpha \in Q_4$, такое что ретракт $q_\alpha = q|_{x_n=\alpha}$ полулинеен. Тогда 2-МДР-код $\mathcal{S}_{a,b}(q_\alpha)$ – линейный при некоторых $a, b \in Q_4$. Рассмотрим $\mathcal{S}_{a,b}(q)$. По лемме 1 найдётся $\beta \in Q_4$, $\beta \neq \alpha$ такое, что $\mathcal{S}_{a,b}(q_\beta) = Q_4^{n-1}\backslash\mathcal{S}_{a,b}(q_\alpha)$, т. е. $(n-1)$-арная квазигруппа q_β является полулинейной. Без ограничения общности можно положить $\{a,b\} = \{\alpha,\beta\} = \{0,1\}$.

Функции f и f', определенные следующими равенствами:

$$f(x_1,\dots,x_{n-1},0) \stackrel{def}{=} q(x_1,\dots,x_{n-1},0), \qquad f(x_1,\dots,x_{n-1},1) \stackrel{def}{=} q(x_1,\dots,x_{n-1},1),$$
$$f(x_1,\dots,x_{n-1},2) \stackrel{def}{=} \pi q(x_1,\dots,x_{n-1},0), \qquad f(x_1,\dots,x_{n-1},3) \stackrel{def}{=} \pi q(x_1,\dots,x_{n-1},1),$$
$$f'(x_1,\dots,x_{n-1},0) \stackrel{def}{=} q(x_1,\dots,x_{n-1},0), \qquad f'(x_1,\dots,x_{n-1},1) \stackrel{def}{=} q(x_1,\dots,x_{n-1},1),$$
$$f'(x_1,\dots,x_{n-1},2) \stackrel{def}{=} \pi q(x_1,\dots,x_{n-1},1), \qquad f'(x_1,\dots,x_{n-1},3) \stackrel{def}{=} \pi q(x_1,\dots,x_{n-1},0),$$

являются полулинейными продолжениями частичной n-арной квазигруппы g.

В заключении заметим, что q либо совпадает с f или f', и тогда q полулинейна, либо g имеет более двух продолжений (q, f, f'), и тогда q полулинейна или разделима по предложению 55. ▲

Одним из следствий характеризационной теоремы 7 является свитчинговая эквивалентность n-арных квазигрупп порядка 4.

Теорема 8 ([35]). *Для любого $n \in \mathbb{N}$ все n-арные квазигруппы порядка 4 с.-эквивалентны.*

Для доказательства теоремы нам понадобятся следующие простые утверждения.

Предложение 56 ([35]). *Пусть q есть m-арная квазигруппа, h и ℓ — с.-эквивалентные n-арные квазигруппы. Тогда квазигруппы $h(\overline{x}, q(\overline{y}))$ и $\ell(\overline{x}, q(\overline{y}))$ с.-эквивалентны.*

Доказательство. Пусть квазигруппа ℓ получается из квазигруппы h свитчингом $\{a, b\}$-компоненты S. Нетрудно видеть, что $S = \{\overline{x} \in Q_4^n \mid h(\overline{x}) \neq \ell(\overline{x})\}$. Тогда множество $S' = \{(\overline{x}, \overline{y}) \in Q_4^{n+m-1} \mid h(\overline{x}, q(\overline{y})) \neq \ell(\overline{x}, q(\overline{y}))\}$ является $\{a, b\}$-компонентой квазигруппы $h(\overline{x}, q(\overline{y}))$, и квазигруппа $\ell(\overline{x}, q(\overline{y}))$ получается из $h(\overline{x}, q(\overline{y}))$ свитчингом S'. Из определения с.-эквивалентности получаем требуемое. ▲

Предложение 57 ([35]). *Для любого $n \in \mathbb{N}$ все линейные n-арные квазигруппы с.-эквивалентны.*

Доказательство. Покажем, что если n-арная квазигруппа g представима в виде (1.18), то квазигруппа f, полученная заменой любой перестановки π_i на тождественную, с.-эквивалентна g. Поскольку операция $+$ сложения в $Z_2 \times Z_2$ коммутативна и ассоциативна, мы без потери общности можем считать, что $i = 1$. Имеем $g(x_1, \overline{y}) = \ell_{\pi_1}(x_1, q(\overline{y}))$ и $f(x_1, \overline{y}) = \ell(x_1, q(\overline{y}))$, где $\ell(x, z) = x + z$, $\ell_{\pi_1}(x, z) = \pi_1(x) + z$ и $q(x_2, \ldots, x_n) \equiv \pi_2(x_2) + \cdots + \pi_n(x_n)$. Поскольку бинарные квазигруппы ℓ и ℓ_{π_1} с.-эквивалентны (что проверяется непосредственно для любой перестановки π_1), из предложения 56 получаем с.-эквивалентность g и f.

Таким образом, оставаясь в рамках класса с.-эквивалентности, мы можем, начиная с любой линейной n-арной квазигруппы вида (1.18), заменить одну за другой все перестановки π_i, $i = 1, \ldots, n$, на тождественные. ▲

Предложение 58 ([35]). *Для любого $n \in \mathbb{N}$ каждая полулинейная n-арная квазигруппа с.-эквивалентна некоторой линейной.*

Доказательство. Сначала рассмотрим две n-арные квазигруппы f и g такие, что множества $S_{a,b}(f)$ и $S_{a,b}(g)$ совпадают. Покажем, что f и g получаются одна из другой свитчингами $\{a, b\}$- и $\{c, d\}$-компонент, где $\{c, d\} = Q_4 \setminus \{a, b\}$.

Рассмотрим функцию $h : Q_4^n \to Q_4$, совпадающую с f на множестве $S_{a,b}(f)$ и с g на множестве $S_{c,d}(f)$. Очевидно, что h является квазигруппой. Множество $D_{c,d} = \{\overline{x} \in Q_4 \mid |f(\overline{x}) \neq h(\overline{x})\}$ обязано быть $\{c, d\}$-компонентой, откуда следует с.-экви-

валентность f и h. Аналогично, g получается из h свитчингом $\{a,b\}$-компоненты. Таким образом, с.-эквивалентность f и g доказана.

Осталось заметить, что для любого множества $S_{a,b}(f)$, удовлетворяющего (1.17), можно подобрать такие перестановки π_1, ..., π_n, что линейная квазигруппа g, задаваемая тождеством (1.18), будет удовлетворять равенству $S_{a,b}(g) = S_{a,b}(f)$. Это означает, что каждая полулинейная квазигруппа с.-эквивалентна некоторой линейной. ▲

Доказательство теоремы 8. Докажем индукцией по n, что любая n-арная квазигруппа с.-эквивалентна некоторой линейной. При $n = 1, 2$ утверждение проверяется непосредственно. Предположим, что утверждение доказано для n-арных квазигрупп при всех $n < r$, и докажем его для $n = r$. Рассмотрим произвольную n-арную квазигруппу f. Из теоремы 7 следует, что квазигруппа f либо полулинейна и тогда по предложению 58 с.-эквивалентна линейной квазигруппе, либо разделима и тогда может быть представлена в виде

$$f(x_1, \ldots, x_n) \equiv h(q(x_{\sigma(1)}, \ldots, x_{\sigma(m)}), x_{\sigma(m+1)}, \ldots, x_{\sigma(n)}),$$

где квазигруппа q неразделима и, следовательно, полулинейна. По предположению индукции мультиарная квазигруппа h с.-эквивалентна линейной квазигруппе ℓ. Тогда по предложению 56 квазигруппа f с.-эквивалентна g, где

$$g(x_1, \ldots, x_n) \equiv \ell(q(x_{\sigma(1)}, \ldots, x_{\sigma(m)}), x_{\sigma(m+1)}, \ldots, x_{\sigma(n)}).$$

По предложению 51(e) квазигруппа g полулинейна, и по предложению 58 она с.-эквивалентна линейной квазигруппе, что завершает индуктивный шаг доказательства.

Теперь с.-эквивалентность всех n-арных квазигрупп порядка 4 следует из предложения 57.▲

Более того, в [35] доказано

Замечание 7. *Любые две n-арные квазигруппы порядка 4 можно преобразовать друг в друга последовательными свитчингами $\{0,1\}$-, $\{0,2\}$- и $\{2,3\}$-компонент.*

§ 1.4. Число n-арных квазигрупп

Напомним, что n-арная квазигруппа f называется приведённой или n-арной лупой, если для всех $i \in [n]$ и $a \in Q_k$ имеет место равенство $f(0,\dots,0,\underset{i}{a},0,\dots,0) = a$. Пусть $N_{mds}(n,k)$ — число n-арных квазигрупп порядка k и $N'(n,k)$ — число n-арных луп порядка k. Имеем следующий простой и хорошо известный факт:

Предложение 59. $N_{mds}(n,k) = k \cdot ((k-1)!)^n N'(n,k)$.

Из предложения 16 имеем

Предложение 60 (см.[163]). $N'(n,2) = N'(n,3) = 1$.

Перейдём к рассмотрению вопроса о числе n-арных квазигрупп порядка 4. Обозначим через ℓ_n^a мощность множества a-полулинейных n-арных луп и через ℓ_n мощность множества полулинейных n-арных луп.

Мощность множества полулинейных n-арных луп легко вычисляется из представления (1.19). Имеем

Предложение 61 ([49]). $\ell_n = 3 \cdot 2^{2^n-n-1} - 2$, $\ell_n^a = 2^{2^n-n-1}$ *при* $a \in \{1,2,3\}$.

Вывод рекуррентной формулы для числа n-арных луп (и квазигрупп) порядка 4 основывается на теореме 7.

Введём следующие обозначения:

v_n — число n-арных луп (порядка 4);

r_n^* — число n-арных луп с бинарной корневой операцией $*$;

r_n^0 — число разделимых n-арных луп с корневой операцией арности, большей либо равной 3;

r_n^{a*} — число a-полулинейных n-арных луп с a-полулинейной бинарной корневой операцией $*$;

r_n^{a0} — число разделимых a-полулинейных n-арных луп с корневой операцией арности, большей либо равной 3;

p_n^a — число неразделимых a-полулинейных n-арных луп, $n > 2$;

p_n — число неразделимых n-арных луп, $n > 2$.

Из равенства (1.10), теоремы 3 и предложения 52 вытекают следующие соотно-

шения:

$$r_n^{a*} = \sum_{i=2}^{n} \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (\ell_{j_1}^a - r_{j_1}^{a*})^{k_1} \cdots (\ell_{j_t}^a - r_{j_t}^{a*})^{k_t},$$

$$r_n^* = \sum_{i=2}^{n} \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (v_{j_1} - r_{j_1}^*)^{k_1} \cdots (v_{j_t} - r_{j_t}^*)^{k_t},$$

$$r_n^{a0} = \sum_{i=3}^{n-1} p_i^a \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (\ell_{j_1}^a)^{k_1} \cdots (\ell_{j_t}^a)^{k_t},$$

$$r_n^0 = \sum_{i=3}^{n-1} p_i \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (v_{j_1})^{k_1} \cdots (v_{j_t})^{k_t},$$

где вторая сумма берётся по наборам $\bar{k} = (k_1, \ldots, k_t)$ и $\bar{j} = (j_1, \ldots, j_t)$ положительных целых чисел, удовлетворяющих равенствам $k_1 + \cdots + k_t = i$, $k_1 j_1 + k_2 j_2 + \cdots + k_t j_t = n$ и неравенствам $j_1 < \cdots < j_t$. Из теоремы 7 и предложения 51(c,d) вытекают соотношения $v_n = p_n + r_n^0 + 4r_n^*$, $p_n^a = \ell_n^a - r_n^{a0} - 2r_n^{a*}$, $p_n = 3p_n^a$. Из предложения 61 имеем $\ell_n^a = 2^{2^n - n - 1}$ при $a \in \{1, 2, 3\}$.

Из предложения 49 имеем начальные значения для перечисленных выше величин: $p_2 = 0$, $r_1^{a*} = r_1^* = r_1^{a0} = r_1^0 = 0$. Нетрудно видеть, что приведённые выше равенства и предложение 59 обеспечивают рекуррентный способ вычисления числа n-арных квазигрупп порядка 4.

Наконец, выпишем первые восемь значений величины $N'(n, 4)$:

1,

4,

64,

7132,

201538000,

432345572694417712,

39876839873547476429227735 3963277968,

67846927287489958255998624028528071036486706348977951042703872222975027 6832.

Из приведённых выше формул нетрудно по индукции доказать, что мощность множества всех n-арных луп асимптотически совпадает с мощностью множества полулинейных n-арных луп, причём справедливо

Предложение 62 ([49]). $3^{n+1} \cdot 2^{2^n+1} \leq N_{mds}(n,4) \leq (3^{n+1}+1) \cdot 2^{2^n+1}$ *при* $n \geq 5$.

Эта неравенство было получено "косвенными" методами в статье [49] до доказательства теоремы 7 и вывода реккурентной формулы.

Перебор, осуществлённый с помощью компьютера, дают следующие результаты для числа луп (приведённых латинских квадратов) [130], [162]:

k	$N'(2,k)$
1	1,
2	1,
3	1,
4	4,
5	56,
6	9408,
7	16942080,
8	535281401856,
9	377597570964258816,
10	7580721483160132811489280,
11	536393777327737129811967354077184 0;

и для числа приведённых латинских кубов [163]:

k	$N'(3,k)$
1	1,
2	1,
3	1,
4	64,
5	40246,
6	95909896152

Кроме того, известно число 4- и 5-арных луп порядка 5 [163]: $N'(5,4) = 201538000$, $N'(5,5) = 50490811256$.

Следствием гипотезы Ван дер Вардена о перманентах (см. теорему 50) и теоремы 49 [7] является асимптотическая при $k \to \infty$ оценка числа латинских квадратов $N_{mds}(2,k) = ((1+o(1))k/e^2)^{k^2}$. Недавно получено обобщение этой теоремы при $n > 2$.

Теорема 9 ([160]). *Для любого $n \geq 2$ справедливо асимптотическое неравенство $N_{mds}(n,k) \leq ((1+o(1))k/e^n)^{k^n}$ при $k \to \infty$.*

Перейдём к асимптотическим не по порядку, а по размерности (при $n \to \infty$) оценкам числа n-арных квазигрупп, порядков больших чем 4.

Предложение 63. *Пусть $B = Q_k \setminus \{a,b\}$, $k \geq 3$, $a,b \in Q_k$. Тогда частичная n-арная квазигруппа $g : Q_k^{n-1} \times B \to Q_k$ имеет не более чем $2^{(k/2)^{n-1}}$ различных продолжений.*

Для доказательства предложения 63 достаточно заметить, что множество $M = Q_k^n \setminus \{(x, g(x,y)) : x \in Q_k^{n-1}, y \in B\}$ является унитрейдом и по предложению 8 имеет не более $|M|/2^n$ компонент связности.

Теорема 10 ([55]). *Если $k \geq 5$ и $n \geq 2$, то $N_{mds}(n,k) \leq 2^{c_k(k-2)^n}$, где $c_k = \frac{\log_2 k!}{k-2} + \frac{k}{k-4}$.*

Доказательство. Число частичных n-арных квазигрупп $g : Q_k^n \times B \to Q_k$, $B = Q_k \setminus \{a,b\}$ не превосходит $N_{mds}(n,k)^{k-2}$. Из предложения 63 следует неравенство

$$N_{mds}(n+1,k) \leq N_{mds}(n,k)^{k-2} 2^{(k/2)^n}. \tag{1.24}$$

Введём обозначение $\alpha_n = \log_2 N_{mds}(n,k)/(k-2)^n$. Тогда из неравенства (1.24) имеем

$$\alpha_{n+1} \leq \alpha_n + \left(\frac{k}{2(k-2)}\right)^n.$$

Поскольку $\alpha_1 = \frac{\log_2 k!}{k-2}$ и $\sum\limits_{n=1}^{\infty} \left(\frac{k}{2(k-2)}\right)^n = \frac{k}{k-4}$, имеем $\alpha_n \leq \frac{\log_2 k!}{k-2} + \frac{k}{k-4}$. ▲

2-Квазигруппа $\varphi : Q_k \to Q_k$ называется *идемпотентной*, если $\varphi(x,x) = x$ для любого $x \in Q_k$. Известно, что верно

Предложение 64 (см. [4]). *Для любого $m \geq 3$ имеется идемпотентная 2-квазигруппа порядка m.*

В следующем предложении приведена конструкция 2-квазигрупп, которая будет использована при доказательстве нижней оценки числа n-арных квазигрупп нечётного порядка.

Предложение 65 ([55]). *Для любого $m \geq 3$ найдётся 2-квазигруппа ψ порядка $2m+1$, имеющая m $\{2i, 2i+1\}$-компонент для каждого $i \in \{0, \ldots, m-1\}$, причём все кроме одной $\{2i, 2i+1\}$-компоненты имеют вид $\{2j, 2j+1\} \times \{2l, 2l+1\}$.*

Доказательство. По предложению 64 найдётся идемпотентная 2-квазигруппа φ_m порядка m. Для любых $a, b \in \{0, \ldots, m-1\}$, $a \neq b$, и $\delta, \sigma \in \{0, 1\}$ определим

$\psi(2a+\delta, 2b+\sigma) = 2\varphi_m(a,b) + (\delta + \sigma \bmod 2)$;

$\psi(2a+\delta, 2a+\delta) = 2a+1-\delta$;

$\psi(2a+\delta, 2a+1-\delta) = k-1$;

$\psi(k-1, 2a+\delta) = \psi(2a+\delta, k-1) = 2a+\delta$;

$\psi(k-1, k-1) = k-1$.

Непосредственная проверка показывает, что ψ есть 2-квазигруппа, обладающая требуемыми свойствами. ▲

Ниже приведён пример таблиц значений 2-квазигруппы φ_4 и соответствующей ψ:

1	8	4	5	6	7	2	3	0
8	0	5	4	7	6	3	2	1
6	7	3	8	0	1	4	5	2
7	6	8	2	1	0	5	4	3
2	3	6	7	5	8	0	1	4
3	2	7	6	8	4	1	0	5
4	5	0	1	2	3	7	8	6
5	4	1	0	3	2	8	6	7
0	1	2	3	4	5	6	7	8

φ_4 :

0	2	3	1
3	1	0	2
1	3	2	0
2	0	1	3

Из предложения 8 нетрудно заключить, что 2-квазигруппа нечётного порядка k, построенная в предложении 65, имеет максимальное число непересекающихся компонент среди всех 2-квазигрупп порядка k.

Теорема 11 ([55]). *Если $k \geq 7$ — нечётное и $n \geq 2$, то*

$$N_{mds}(n,k) \geq 2^{\left(\frac{k-3}{2}\right)^{\left\lfloor \frac{n-1}{2} \right\rfloor} \left(\frac{k-1}{2}\right)^{\left\lceil \frac{n+1}{2} \right\rceil}} > 2^{\left(\frac{k-3}{2}\right)^{n/2} \left(\frac{k-1}{2}\right)^{n/2}}.$$

Доказательство. Пусть ψ – 2-квазигруппа порядка k, построенная в предложении 65. Определим рекуррентно n-арную квазигруппу Ψ^n равенствами:

$\Psi^2 \stackrel{def}{=} \psi$;

$\Psi^{2m+1}(\overline{x}, y) \stackrel{def}{=} \psi(\Psi^{2m}(\overline{x}), y)$;

$\Psi^{2m+2}(\overline{x}, y, z) \stackrel{def}{=} \psi(\Psi^{2m}(\overline{x}), \psi(y, z))$.

Обозначим через α_n — число $\{2i, 2i+1\}$-компонент n-арной квазигруппы Ψ^n, где $i \in \{0, \ldots, \frac{k-3}{2}\}$. Из предложений 15 и 65 имеем соотношения $\alpha_2 = \frac{k-1}{2}$, $\alpha_{2m+1} \geq \alpha_{2m}\frac{k-3}{2}$, $\alpha_{2m+2} \geq \alpha_{2m}\frac{k-3}{2}\frac{k-1}{2}$. Тогда $\alpha_{2m} \geq \left(\frac{k-3}{2}\right)^{m-1}\left(\frac{k-1}{2}\right)^m$ и $\alpha_{2m+1} \geq \left(\frac{k-3}{2}\right)^m\left(\frac{k-1}{2}\right)^m$.

Поскольку $\{2i, 2i+1\}$-компоненты при различных i не пересекаются, всего непересекающихся компонент не меньше, чем $\frac{k-1}{2}\alpha_n$. Из предложения 14 следует, что из n-арной квазигруппы Ψ^n свитчингами непересекающихся компонент можно получить требуемое число различных n-арных квазигрупп порядка k. ▲

§ 1.5. Транзитивные МДР-коды

Напомним несколько определений. Группа изотопий (*автотопий*) множества $A \subseteq Q_q^n$ определяется равенством $\mathrm{Ist}(A) = \{\overline{\tau} \mid \overline{\tau}A = A\}$, а группа парастрофий — равенством $\mathrm{Prs}(A) = \{\varepsilon \mid A_\varepsilon = A\}$. Подгруппа группы изометрий гиперкуба, переводящая множество $A \subseteq Q_q^n$ в себя обозначается через $\mathrm{Aut}(A)$. Множество $A \subseteq Q_q^n$ называется *транзитивным*, если для любых двух вершин $\overline{x}, \overline{y}$ из A найдутся парастрофия $\varepsilon \in \mathrm{Prs}(Q_q^n)$ и изотопия $\overline{\tau} \in \mathrm{Ist}(Q_q^n)$ такие, что $\overline{\tau y} = \overline{x}_\varepsilon$ и $\overline{\tau}A = A_\varepsilon$, т. е. группа изометрий $\mathrm{Aut}(A)$ действует транзитивно на A. Множество $A \subseteq Q_q^n$ называется *изотопно транзитивным* (см. [48]), если группа $\mathrm{Ist}(A)$ действует транзитивно на A. Ясно, что одну из вершин в определении транзитивности (изотопной транзитивности) можно зафиксировать. В дальнейшем будем полагать, что вершина $\overline{0}$ содержится в транзитивном множестве и именно её будем фиксировать ($\overline{x} = \overline{0}$).

Замечание 8. *При $q = 2$ понятие изотопной транзитивности совпадает с понятием аффинности множества.*

Множество $A \subseteq Q_q^n$ называется *предлинейным (propelinear)*, если $\mathrm{Aut}(A)$ содержит регулярную подгруппу, т. е. подгруппу группы $\mathrm{Aut}(A)$ мощности $|A|$, действу-

ющую транзитивно на A. Множество $A \subseteq Q_q^n$ назовём *тополинейным*, если $\mathrm{Ist}(A)$ содержит регулярную подгруппу G_A.

Непосредственно из определений имеем

Предложение 66. *Множество $A \subset Q_q^n$, $\overline{0} \in A$, — предлинейно с регулярной подгруппой $G_A < \mathrm{Aut}(A)$ тогда и только тогда, когда*

1) для любого $a \in A$ найдётся единственный $\varphi_a \in G_A$ такой, что $\varphi_a(\overline{0}) = a$;

2) для любых $a, b \in A$ композиция $\varphi_a \cdot \varphi_b$ содержится в G_A.

Предлинейность множества эквивалентна возможности введения на множестве групповой операции, согласованной с метрикой:

$$a * b = c \qquad \Leftrightarrow \qquad \varphi_a \cdot \varphi_b = \varphi_c.$$

А именно, справедливо

Предложение 67. *Множество $A \subset Q_q^n$, $\overline{0} \in A$, предлинейно тогда и только тогда, когда на множестве A можно определить бинарную операцию $* : A^2 \to A$ со следующими свойствами:*

1) пусть $\varphi'_a(x) = a * x$, тогда φ'_a можно продолжить до изометрии $\varphi_a \in \mathrm{Aut}(Q_q^n)$;

2) $a * \overline{0} = a$;

3) операция $*$ ассоциативна.

Доказательство. ($\Rightarrow$) В соответствии с предложением 66 имеется группа G_A. Определим $a * b = c$, если $\varphi_a \cdot \varphi_b = \varphi_c$. Проверим свойства 1)-3).

1) $\varphi'_a(x) = (\varphi_a \cdot \varphi_x)(\overline{0}) = \varphi_a(x)$.

2) $a * \overline{0} = c \Rightarrow \varphi_a \cdot \varphi_{\overline{0}} = \varphi_c \Rightarrow a = c$.

3) следует из ассоциативности композиции.

($\Leftarrow$) Достаточно проверить, что множество изометрий φ_a замкнуто относительно композиции. Пусть $x \in A$, имеем $\varphi_a(\varphi_b(x)) = \varphi'_a(b*x) = a*(b*x) = (a*b)*x = \varphi'_{a*b}(x)$. Тогда φ'_{a*b} продолжается до $\varphi_a \cdot \varphi_b = \varphi_{a*b}$. ▲

Аналогичная характеризация (с заменой $\mathrm{Aut}(Q_q^n)$ на $\mathrm{Ist}(Q_q^n)$) справедлива для тополинейных множеств.

Нетрудно видеть, что справедливо

Предложение 68.

1) Ретракты изотопно транзитивного множества являются изотопно транзитивными.

2) Ретракты тополинейного множества являются тополинейными.

Доказательство. 1) Пусть $A \subseteq Q_q^n$ — изотопно транзитивное множество. Без ограничения общности можно полагать, что
$R = \{(x_1, \ldots, x_{n-m}, 0, \ldots, 0) \mid (x_1, \ldots, x_{n-m}, 0, \ldots, 0) \in A\}$. Пусть $\tau \in \mathrm{Ist}(A)$, $x \in R$ и $\tau x = \overline{0}$. Тогда $\tau_{n-m+1}(0) = \cdots = \tau_n(0) = 0$, следовательно, $\tau \in \mathrm{Ist}(R)$.

2) Аналогично п. 1). ▲

Замечание 9. *Ретракты транзитивных (предлинейных) множеств не обязательно являются транзитивными (предлинейными).*

Ясно, что декартово произведение транзитивных (предлинейных) множеств является транзитивным (предлинейным) множеством. Рассмотрим естественное отождествление $Q_q^n \times Q_p^n$ и Q_{pq}^n. При этом отождествлении метрика не сохраняется, но справедливо следующее

Предложение 69. *Пусть $A \subseteq Q_q^n$ и $B \subseteq Q_p^n$ — изотопно транзитивные (тополинейные) множества. Тогда множество $A \times B \subseteq Q_{pq}^n$ является изотопно транзитивным (тополинейным).*

Тополинейность изотопно транзитивного МДР-кода можно проверять покоординатно, а именно, справедливо

Предложение 70. *Пусть $M \subseteq Q_q^n$ — изотопно транзитивный* МДР-*код. Пусть $G < \mathrm{Ist}(M)$ — группа изотопий, транзитивно действующая на M и удовлетворяющая следующему условию: для любых $\overline{\tau}, \overline{\pi} \in G$ из равенства $\overline{\tau}(\overline{0}) = \overline{\pi}(\overline{0})$ следует, что $\pi_1 = \tau_1$. Тогда множество M является тополинейным с регулярной группой G.*

Доказательство. Рассмотрим $\overline{\sigma} = \overline{\tau}(\overline{\pi})^{-1} \in G$. По условию, $\sigma_1 = \mathrm{id}$ и $\sigma(\overline{0}) = \overline{0}$. Покажем, что $\sigma_i = \mathrm{id}$. Для любого $b_i \in Q_q^n$ найдётся такое $b_1 \in Q_q^n$, что $b = (b_1, 0, \ldots, 0, b_i, 0 \ldots, 0) \in M$. Тогда $\sigma(b) = (b_1, 0, \ldots, 0, \sigma_i(b_i), 0 \ldots, 0) \in M$. По определению МДР-кода, имеем $\sigma_i(b_i) = b_i$. Следовательно, $\overline{\tau} = \overline{\pi}$, т. е. подгруппа G является регулярной. ▲

n-Арную квазигруппу будем называть *транзитивной* (*тополинейной, изотопно транзитивной, предлинейной*), если её график (МДР-код) является транзитивным (тополинейным, изотопно транзитивным, предлинейным). Ясно, что две эквивалентные n-арные квазигруппы обладают или не обладают перечисленными свойствами одновременно.

Нетрудно видеть, что любая группа является тополинейной 2-квазигруппой.

Если $\circ$ — групповая операция на Q_q, то n-арная квазигруппа $f(x_1, \ldots, x_n) = x_1 \circ \cdots \circ x_n$ называется *итерированной* группой. Вследствие ассоциативности результат итерирования не зависит от порядка.

Из предложения 70 следует

Предложение 71. *Итерированная группа является тополинейной мультиарной квазигруппой.*

Кроме того, нам понадобится следующее

Предложение 72. *Пусть m-арная квазигруппа h является итерированной группой. Тогда для любого $\overline{b} \in Q_q^n$, $h(\overline{b}) = 0$, найдётся такая изотопия $\overline{\theta}$, что $\overline{\theta b} = \overline{0}$ и $h(\overline{\theta z}) \equiv h(\overline{z})$.*

Мультиарные квазигруппы f и g *изоморфны*, если справедливо равенство $\overline{\tau}\mathcal{M}\langle f\rangle = \mathcal{M}\langle g\rangle$, где $\overline{\tau} = (\sigma, \ldots, \sigma)$ для некоторой перестановки σ.

Теорема 12 (теорема Алберта, см. [37]). *Если 2-лупа изотопна группе, то она изоморфна группе.*

2-Лупа называется *G-лупой*, если любая изотопная ей лупа оказывается ей изоморфной.

Предложение 73 ([156]). *2-Лупа изотопно транзитивна тогда и только тогда, когда она является G-лупой.*

Из предложений 73 и 48 (см. также [189]) следует

Предложение 74 ([189]). *При простом q любая G-лупа является группой (циклической).*

В [158] аналогичный результат был получен для $q = 3p$, где $p > 3$ — простое. С

другой стороны, в [119] доказана

Теорема 13 ([119]). *Для любого непростого порядка $q > 5$ имеются G-лупы порядка q, не эквивалентные группам, за возможным исключением случая, когда в разложение числа $q = p_1 p_2 \dots p_s$ на простые множители удовлетворяет условиям: $2 < p_1 < \dots < p_s$ и $p_j \not\equiv 1 \mod p_i$ при $i < j$.*

В [48] имеется конструкция изотопно транзитивных n-арных квазигрупп порядка 4. Эта конструкция обобщается на большие чётные порядки. Следующая лемма является обобщением утверждения из [48].

Лемма 9 ([156]). *Пусть* (a) *m_i-арные квазигруппы h_i, $i \in [n]$, являются итерированными группами,* (b) *n-арная квазигруппа f изотопно транзитивна с транзитивно действующей группой автотопий G_f, c) для любого $i \in [n]$ и $\overline{\sigma} \in G_f$ существует изотопия $\overline{\tau}_i \in S_{n_i}$ такая, что $h_i(\overline{\tau}_i \overline{z_i}) = \sigma_i h(\overline{z_i})$, где $\overline{z_i}$ — наборы из n_i переменных. Тогда m-арная квазигруппа $f(h_1(\overline{z_1}), \dots, h_n(\overline{z_n}))$, где $m = m_1 + \dots + m_n$, является изотопно транзитивной.*

Доказательство. Рассмотрим произвольный набор $b_0, \overline{b}_1, \dots, \overline{b}_n$, для которого $f(h_1(\overline{b}_1), \dots, h_n(\overline{b}_n)) = b_0$. Найдётся такая изотопия $\sigma \in G_f$, что $\sigma_0 b_0 = 0$ и $\sigma_i h_i(\overline{b}_i) = 0$ для любого $i \in [n]$. Имеем равенства

$$\sigma_0 f(h_1(\overline{\tau}_1 \overline{z_1}), \dots, h_n(\overline{\tau}_n \overline{z_n})) \equiv \sigma_0 f(\sigma_1 h_1(\overline{z_1}), \dots, \sigma_n h_n(\overline{z_n})) \equiv f(h_1(\overline{z_1}), \dots, h_n(\overline{z_n})).$$

Таким образом, построена изотопия переводящая набор $b_0, \overline{b}_1, \dots, \overline{b}_n$ в набор $0, \overline{\tau}_1 \overline{b}_1, \dots, \overline{\tau}_n \overline{b}_n$.

Применяя предложение 72 для n_i-арных квазигрупп h_i получаем, что для любого $i \in [n]$ найдётся такая изотопия $\overline{\theta_i}$, что $\overline{\theta_i} \overline{\tau}_i \overline{b}_i = \overline{0}$ и $h_i(\overline{\theta_i} \overline{z_i}) \equiv h_i(\overline{z_i})$. Таким образом, построена изотопия переводящая набор $0, \overline{\tau}_1 \overline{b}_1, \dots, \overline{\tau}_n \overline{b}_n$ в набор $\overline{0}$. ▲

n-Арная квазигруппа f, полученная итерированием группы $Z_p \times Z_2$, $p > 2$, (см. [156]), и мультиарные квазигруппы h_i, полученные итерированием диэдральной группы D_p подходят под условие леммы 9. При $p = 2$ роль f может играть итерированная группа Z_4, а в качестве h_i можно использовать итерированные группы Z_2^2. Нетрудно показать, что различные разбиения числа m, применённые в конструкции леммы 9, порождают неэквивалентные m-арные квазигруппы. Известно (см., например, [72]),

что количество различных разбиений числа m на натуральные слагаемые асимптотически равно $\frac{1}{4m\sqrt{3}}e^{\pi\sqrt{2m/3}}(1+o(1))$.

Тогда из леммы 9 получаем

Теорема 14 ([48]). *При $q=2p$ число попарно не эквивалентных изотопно транзитивных n-арных квазигрупп порядка q растёт как $e^{\Omega(\sqrt{n})}$ при $n\to\infty$.*

Теперь рассмотрим конструкцию тополинейных мультиарных квазигрупп порядка $q=p^k$, где p — простое. Далее будем считать, что множество Q_q наделено структурой поля $GF(p^k)$. Пусть $r(x)=\sum_{i,j}\alpha_{ij}x_ix_j+\sum_{i=1}^n\beta_i(x_i)$, где $\beta_i:Q_q\to Q_q$ — произвольные функции.

Теорема 15 ([156]). *Пусть множество $M\subset(Q_q\times Q_q)^n$ определено следующей системой уравнений*

$$((x_1,y_1),\dots,(x_n,y_n))\in M\Leftrightarrow\begin{cases}\sum_{i=1}^n x_i=0;\\ \sum_{i=1}^n y_i+r(x)=0.\end{cases}$$

Тогда множество M является тополинейным МДР*-кодом.*

Доказательство. Без ограничения общности полагаем, что $\overline{0}\in M$ и $\beta_i(0)=0$ для любого $i\in[n]$. Изотопная транзитивность МДР-кода M вытекает из следующих равенств:

Пусть $((a_1,b_1),\dots,(a_n,b_n))\in M$, $a_i,b_i\in Q_q^n$. Тогда изотопия $(\overline{\sigma},\overline{\tau})$, где $\sigma_i(x_i)=x_i-a_i$,

$\tau_i(y_i)=y_i+x_i\sum_{j=1}^n\alpha_{ij}a_j+x_i\sum_{j=1}^n\alpha_{ji}a_j-\beta_i(x_i-a_i)+\beta_i(x_i)-\sum_{j=1}^n\alpha_{ij}a_ja_i$,

содержится в группе $\mathrm{Ist}(M)$ и переводит вершину $((a_1,b_1),\dots,(a_n,b_n))\in M$ в вершину $((0,\tau_1b_1),\dots,(0,\tau_nb_n))\in M$. Изотопия $(\overline{\sigma}',\overline{\tau}')$, где $\sigma_i'(x_i)=x_i$, $\tau_i'(y_i)=y_i-c_i$ содержится в группе $\mathrm{Ist}(M)$ и переводит вершину $((0,c_1),\dots,(0,c_n))\in M$ в $\overline{0}$.

Из предложения 70 получаем тополинейность МДР-кода M. ▲

Нетрудно видеть, что неэквивалентные квадратичные формы $\sum_{i,j}\alpha_{ij}x_ix_j$ порождают неизометричные МДР-коды.

Пусть $M\subset Q_{q^2}^n$ — МДР-код, построенный в теореме 15. Из предложения 71 следует, что в гиперкубе Q_s^n при произвольных n имеется тополинейный МДР-код S, порождённый некоторой группой порядка s. Из предложения 69 следует, что множе-

ство $M \times S \subset Q^n_{q^2} \times Q^n_s \simeq Q^n_{sq^2}$ является тополинейным МДР-кодом. Тогда из теоремы 15 получаем следующую оценку числа тополинейных МДР-кодов.

Следствие 7 ([156]). *Пусть $q = p^k$, где p — простое, $s \geq 1$. В гиперкубе $Q^n_{q^2 s}$, имеется не менее $q^{\binom{n}{2}(1+o(1))}$ (при $n \to \infty$) попарно не изометричных тополинейных* МДР-*кодов.*

В случае порядка 4 применение характеризационной теоремы 7 позволяет получить полную характеризацию тополинейных МДР-кодов.

Теорема 16 ([156]). МДР-*код $M \subset Q^n_4$ является изотопно транзитивным тогда и только тогда, когда он является полулинейным с квадратичной*[3] *функцией λ.*

Доказательство. $\Leftarrow$ Достаточно рассмотреть 1-полулинейные МДР-коды. Из равенства (1.19) следует, что 1-полулинейный МДР-код можно задать системой уравнений

$$(*) \qquad \begin{cases} \sum_{i=1}^n x_i = 0; \\ \sum_{i=1}^n y_i + \lambda(x) = 0, \end{cases}$$

Требуемое следует из теоремы 15.

$\Rightarrow$ Из классификационной теоремы 7 следует, что

1) не полулинейный МДР-код имеет ретракт размерности 4 изотопный МДР-коду $H = \{(x_1, x_2, x_3, x_4) \mid x_1 \bullet_1 x_2 = x_3 \bullet_2 x_4\}$, где $\bullet_1, \bullet_2$ — групповые операции эквивалентные операции Z_4 с одинаковым нейтральным элементом, но разными элементами порядка 2;

2) имеется 4 различных класса изотопий полулинейных МДР-кодов размерности 4 с булевыми функцями $r_1(x) \equiv 0$, $r_2(x) = x_1x_2 \oplus x_3x_4$, $r_3(x) = x_1x_2$ и $r_4(x) = x_1x_2x_3$ соответственно, где r_i получены подставлением в функцию λ равенства $x_1 + x_2 + x_3 + x_4 = 0$.

Непосредственной проверкой можно доказать, что неполулинейный код H и полулинейный код S_4 с функцией r_4 не являются изотопно транзитивными. Любой неполулинейный МДР-код имеет ретракт изотопный коду H, а любой полулинейный

[3] Поскольку функция λ задана только на вершинах булева куба чётного веса, её алгебраическое задание определяется не однозначно. Мы имеем ввиду минимально возможную степень функции λ.

МДР-код с функцией λ степени строго больше 2 имеет ретракт изотопный коду S_4. Такие коды не являются изотопно транзитивными по предложению 68. ▲

§ 1.6. Дополняемость латинских параллелепипедов

§ 1.6.1. Дополняемость и продолжаемость латинских параллелепипедов и расщепляемость МДР-кодов

Набор n-арных квазигрупп $f_0, \dots, f_{m-1}$ будем называть *совместимым*, если $f_i(\overline{x}) \neq f_j(\overline{x})$ для любых $i \neq j$ и $\overline{x} \in Q_k^n$. Ясно, что набор n-арных квазигрупп $f_0, \dots, f_{m-1}$ совместим тогда и только тогда, когда $\mathcal{M}\langle f_i\rangle \cap \mathcal{M}\langle f_j\rangle = \varnothing$ при $i \neq j$. Набор совместимых n-арных квазигрупп $f_0, \dots, f_{m-1}$ можно рассматривать как частичную $(n+1)$-арную квазигруппу $f : Q_k^n \times \{0, \dots, m-1\} \to Q_k$, $f|_{x_{n+1}=i} = f_i$. Набор n-арных квазигрупп $f_0, \dots, f_{m-1}$ будем называть *продолжаемым*, если найдётся такая n-арная квазигруппа f_m, что набор $f_0, \dots, f_m$ совместим. Набор различных n-арных квазигрупп $f_0, \dots, f_{m-1}$ будем называть *дополняемым*, если найдётся такая $(n+1)$-арная квазигруппа f', что $f'|_{x_{n+1}=i} = f_i$ при $i \in Q_k$, т. е. когда дополняема частичная $(n+1)$-арная квазигруппа f. Таблица значений частичной $(n+1)$-арной квазигруппы f является $(n+1)$-мерным латинским параллелепипедом (гиперкубоидом). Таким образом, можно говорить о дополняемости и продолжаемости латинского параллелепипеда. Очевидно из дополняемости набора $f_0, \dots, f_{m-1}$ следует продолжаемость, а из продолжаемости совместимость.

t-Кратный МДР-код называется *расщепляемым*, если он является объединением t однократных МДР-кодов и *вполне нерасщепляемым*, если он не содержит ни одного однократного МДР-кода. Очевидно 2-МДР-код расщепляем, если и только если он является двудольным. Вопрос о дополняемости наборов совместимых n-арных квазигрупп сводится к вопросу о расщепляемости кратных МДР-кодов. В частности, из определений видно, что справедливо

Предложение 75. (а) *Набор совместимых n-арных квазигрупп $f_1, \dots, f_m$ дополняем тогда и только тогда, когда $(k-m)$-кратный* МДР-*код $M = Q_k^{n+1} \setminus (\bigcup \mathcal{M}\langle f_i\rangle)$*

расщепляем.

(b) *Набор совместимых n-арных квазигрупп $f_1, \ldots, f_m$ непродолжаем тогда и только тогда, когда $(k-m)$-кратный* МДР*-код $M = Q_k^{n+1} \setminus (\bigcup \mathcal{M}\langle f_i \rangle)$ вполне нерасщепляем.*

Случай, когда $k - m = 2$, и, следовательно, M является унитрейдом, наиболее изучен. Классическая теорема Кёнига [141] утверждает, что любая квадратная матрица, содержащая равное (ненулевое) число единиц в каждом столбце и каждой строке, содержит диагональ из одних единиц. Из теоремы Кёнига сразу следует, что любой кратный МДР-код в Q_k^2 расщепляем и по предложению 75 каждый латинский прямоугольник $k \times m$ продолжаем до латинского квадрата $k \times k$ (этот факт указан, например, в [121]). Известно обобщение этого утверждения на произвольные латинские прямоугольники.

Теорема 17 (теорема Райзера, [175]). *Пусть $f : Q_r \times Q_s \to Q_k$ — частичная 2-квазигруппа и $|f^{-1}(a)| \geq r+s-k$ для любого $a \in Q_k$. Тогда частичная* 2*-квазигруппа f дополняема.*

Перейдём к многомерному случаю. Имеется существенное различие между дополняемостью до мультиарной квазигруппы с увеличением порядка и с сохранением порядка. В первом случае дополнение всегда возможно, а именно, справедлива

Теорема 18 ([101]). *Любая частичная n-арная квазигруппа конечного порядка дополняема до n-арной квазигруппы некоторого большего порядка.*

Во-втором случае, как будет показано ниже, не всегда дополняются даже трёхмерные латинские параллелепипеды. Однако, справедливо следующее

Предложение 76 (см., например, [139]).

(a) *Любой набор из $k-1$ попарно совместимых n-арных квазигрупп порядка k дополняем.*

(b) *Любой набор, состоящий из одной n-арной квазигруппы, дополняем.*

Пункт (a) нетрудно доказать по индукции, используя то, что продолжение однозначно определяется уже по одномерной грани. Для доказательства пункта (b) всегда можно выбрать линейное продолжение $F(x_1, \ldots, x_{n+1}) = f(x_1, \ldots, x_n) + x_{n+1} \mod k$.

Из предложения 76 следует, что при $k \leq 3$ любой набор совместимых n-арных квазигрупп порядка k является дополняемым. В случае порядка 4 справедливо аналогичное утверждение.

Теорема 19 ([51]). *Любой набор совместимых n-арных квазигрупп порядка 4 является дополняемым.*

Доказательство теоремы 19 основано на характеризационной теореме 7.

По предложению 76 достаточно рассмотреть случай пары совместимых n-арных квазигрупп.

Доказательство проводится по индукции (при $n = 4$ утверждение теоремы проверено с помощью компьютера) и состоит из рассмотрения нескольких случаев:

(a) когда n-арные квазигруппы f_1 и f_2 неразделимы;

(b) когда хотя бы одна из n-арных квазигрупп f_1 и f_2 разделима, причём разделимость не синхронна;

(c) когда n-арные квазигруппы f_1 и f_2 не полностью синхронно разделимы;

(d) когда одна из n-арных квазигрупп f_1 и f_2 разделима полностью, а другая нет;

(e) когда n-арные квазигруппы f_1 и f_2 полностью разделимы.

В связи со значительным объёмом формальное доказательство вынесено в отдельный раздел.

§ 1.6.2. Непродолжаемые латинские параллелепипеды

При $k \geq 5$ аналогичное теореме 19 утверждение неверно: доказано, что существуют недополняемые латинские параллелепипеды размера $k \times k \times (k-2)$ (при $k = 2^s$, $s \geq 3$ в [129]; при $k \geq 12$ и $k = 6$ в [115]; при $k \geq 5$ в [138]).

Для построения недополняемых латинских параллелепипедов большего порядка из недополняемых латинских параллелепипедов меньшего порядка полезно следующее

Предложение 77 ([140]). *Пусть имеется непродолжаемый латинский параллелепипед размера $k \times k \times (k-m)$, тогда найдётся непродолжаемый латинский параллелепипед размера $k' \times k' \times (k'-m)$ при $k' \geq 2k$.*

Доказательство. Из предложения 46 следует, что найдётся 3-квазигруппа f порядка k' с подквазигруппой q порядка k. Аналогично предложению 47, проведём свитчинг подквазигруппы q порядка k, заменив её на частичную подквазигруппу q', таблица которой есть непродолжаемый латинский параллелепипед размера $k \times k \times (k-m)$. Полученная частичная 3-квазигруппа соответствует непродолжаемому латинскому параллелепипеду. ▲

По предложению 76 (a) для латинских параллелепипедов размера $k \times k \times (k-2)$ продолжаемость и дополняемость совпадают. По предложению 77 для доказательства существования недополняемых латинских параллелепипедов размера $k \times k \times (k-2)$ достаточно построить их при $k = 5, 6, 7, 8, 9$. Рассмотрим пример непродолжаемого латинского параллелепипеда из [138]. Пусть следующие латинские квадраты

3	0	4	2	1		0	4	3	1	2		4	1	2	0	3	
0	4	3	1	2		4	0	1	2	3		3	2	0	4	1	
4	2	1	0	3		2	1	0	3	4		1	3	4	2	0	являются таблицами
1	3	2	4	0		3	2	4	0	1		2	0	1	3	4	
2	1	0	3	4		1	3	2	4	0		0	4	3	1	2	

2-квазигрупп f_0, f_1, f_2 и 2-квазигруппы f_3, f_4 дополняют этот набор. Тогда $\{f_3(0,0), f_4(0,0)\} = \{1,2\}$, $\{f_3(0,1), f_4(0,1)\} = \{1,2\}$, $\{f_3(1,0), f_4(1,0)\} = \{3,2\}$, $\{f_3(1,1), f_4(1,1)\} = \{1,3\}$. Нетрудно видеть, что таких 2-квазигрупп f_3 и f_4 не существует.

Справедливы следующие теоремы.

Теорема 20 ([139]). *Для любого $k > 5$ и $m, k/2 < m \leq k-2$ существуют недополняемые латинские параллелепипеды размера $k \times k \times m$.*

Теорема 21 ([93]). (a) *Для любого $m \geq 4$ существуют недополняемые латинские параллелепипеды размера $2m \times 2m \times m$.*

(b) *Для любого $m \geq 3$ существуют непродолжаемые латинские параллелепипеды размера $(2m-1) \times (2m-1) \times m$.*

Кроме того, в [163] построено несколько примеров недополняемых наборов из l попарно совместимых 2-квазигрупп порядка k при $k = 5, 6, 7, 8$ и $l = 2, 2, 3, 4$ соответственно.

Из теоремы 21 следует, что найдётся расщепляемый m-кратный МДР-код M в Q^3_{2m}, дополнение которого $Q^3_{2m} \setminus M$ нерасщепляемо и расщепляемый m-кратный МДР-код M в Q^3_{2m-1}, дополнение которого $Q^3_{2m-1} \setminus M$ вполне нерасщепляемо. Кроме того, справедлива

Теорема 22 ([34]). *Для любого чётного m существует вполне нерасщепляемый m-кратный* МДР-*код M в Q^3_{2m}.*

Доказательство. Пусть $m = 2p$. Вначале докажем, что линейный МДР-код $G_{2p} = \{(x, y, z) \in Q^3_{2p} : x + y + z = 0 \bmod 2p\}$ не содержит диагонали[4]. Пусть, от противного, имеется диагональ $H \subset G_{2p}$. Для любого (x, y, z) из G_{2p} выполнено $x + y + z = 0 \bmod 2p$, поэтому

$$0 \overset{\bmod 2p}{=} \sum_{(x,y,z)\in H} (x + y + z) = \sum_{(x,y,z)\in H} x + \sum_{(x,y,z)\in H} y + \sum_{(x,y,z)\in H} z =$$

$$\sum_{x=0}^{2p-1} x + \sum_{y=0}^{2p-1} y + \sum_{z=0}^{2p-1} z = p(2p-1) + p(2p-1) + p(2p-1) \overset{\bmod 2p}{=} p.$$

Получили противоречие.

Для $C \subset Q^3_m$ введём обозначения: $\widehat{C} = Q^3_m \setminus C$,

$$C + (a, b, c) \overset{def}{=} \{(x + a, y + b, z + c) : (x, y, z) \in C\}.$$

Определим множества $C_1, C_2, C_3, G_m \subset Q^3_m$ равенствами

$$C_1 \overset{def}{=} \{(x, y, y) : \ x, y \in Q_m\}, C_2 \overset{def}{=} \{(y, x, y) : \ x, y \in Q_m\}, C_3 \overset{def}{=} \{(y, y, x) : \ x, y \in Q_m\},$$

$$G_m \overset{def}{=} \{(x, y, z) \in Q^3_m \ : \ x + y + z = 0 \bmod m\}.$$

Пусть

$$M = G_m \cup (\widehat{C}_3 + (m, 0, 0)) \cup (\widehat{C}_1 + (0, m, 0)) \cup (\widehat{C}_2 + (0, 0, m))$$

$$\cup (C_3 + (m, 0, m)) \cup (C_1 + (m, m, 0)) \cup (C_2 + (0, m, m)) \cup (\widehat{G}_m + (m, m, m)).$$

Пример множества M ($p = 2$) показан на рис.1.7 (заметим, что это не минимальный пример: p может быть равным 1). Нетрудно проверить, что M является m-кратным

[4] Подробнее диагонали многомерных массивов рассматриваются в главе 3.

МДР-кодом. Докажем от противного, что M вполне нерасщепляем. Пусть найдётся однократный МДР-код $D \subset M$.

Пусть $a \in Q_m$. Рассмотрим слой $D_1(a) = \mathcal{L}_{1;a}D \subset \mathcal{L}_{1;a}M$ (см. рис.1.7). Через $\mathcal{E}_i(y)$ будем обозначать линию направления i, содержащую вершину y. По построению пересечение кода M с линией $\mathcal{E}_2(a, 0, a+m)$ содержится в $Q_m^3 + (0, m, m)$. Следовательно, единственный элемент множества D (а также множества $D_1(a)$), принадлежащий этой линии, лежит в $Q_m^3 + (0, m, m)$. Аналогично, пересечение каждой из $m+1$ линий $\mathcal{E}_2(a, 0, b+m)$, $b \in Q_m$, $b \neq a$, с кодом M содержится в множестве $Q_m^3 + (0, 0, m)$. Следовательно, $m-1$ элементов множества D (и $D_1(a)$), принадлежащих этим линиям, лежат в $Q_m^3 + (0, 0, m)$. Таким образом, $D_1(a)$ пересекается с $Q_m^3 + (0, m, m)$ в одном элементе и с $Q_m^3 + (0, 0, m)$ в $m-1$ элементе. Множество $\mathcal{L}_{1;a}(Q_m \times Q_m \times Q_{2m}) = \mathcal{L}_{1;a}Q_m^3 \cup \mathcal{L}_{1;a}(Q_m^3 + (0, 0, m))$ пересекается с D в m элементах (т. к. разбивается на m линий). Из них, как уже показано, $m-1$ элементов содержатся в $Q_m^3 + (0, 0, m)$. Следовательно, $|D_1(a) \cap Q_m^3| = 1$.

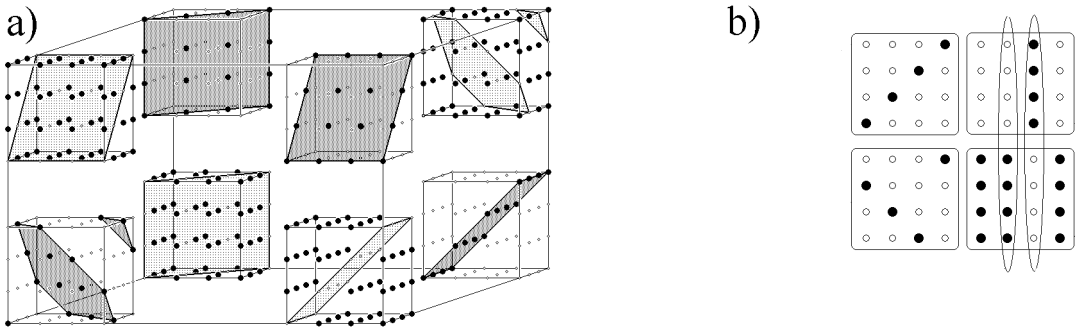


Рис. 1.7: a) Вполне нерасщепляемый 4-х кратный 8-ичный код; b) множество $\mathcal{L}_{1;a}M$, $m = 4$, $a = 2$.

Аналогично показывается, что $|D_i(a) \cap Q_m^3| = 1$ для любых $i \in \{1, 2, 3\}$ и $a \in Q_m$. Таким образом, множество D имеет по одному элементу в каждой грани из Q_m^3. Следовательно, множество $D \cap Q_m^3$ есть диагональ по определению. Это противоречит отсутствию диагонали в G_m, поскольку $D \cap Q_m^3 \subset G_m$. ▲

Тем не менее справедлива следующая

Теорема 23 ([102]). *Для любого m, начиная с достаточно большого s, все латинские*

параллелепипеды размера $2ms \times 2ms \times m$ *продолжаемы.*

Нетрудно видеть, что 3-х мерные примеры непродолжаемых или недополняемых латинских параллелепипедов переносятся на многомерный случай.

Предложение 78. *Если имеется непродолжаемый (недополняемый) набор из* s n*-арных квазигрупп порядка* k*, то найдётся непродолжаемый (недополняемый) набор из* s $(n+1)$*-арных квазигрупп порядка* k*.*

Доказательство. Пусть $f_1, \ldots, f_s$ непродолжаемый (недополняемый) набор. Тогда набор $(n+1)$-арных квазигрупп $f'_i(x_1, \ldots, x_n, x_{n+1}) = f_i(x_1, \ldots, x_n) + x_{n+1} \mod k$ при $i \in [s]$ также непродолжаемый (недополняемый).▲

Из теорем 20, 21 и предложений 77 и 78 имеем

Следствие 8. (a) *Для любого* $n \geq 2$, $k \geq 5$ *и* m, $k - 2 \geq m \geq k/2$, *найдётся недополняемый набор из* m n*-арных квазигрупп порядка* k*.*

(b) *Для любого* $n \geq 2$, $k \geq 10$ *и* m, $k - 2 \geq m \geq (3k+2)/4$, *найдётся непродолжаемый набор из* m n*-арных квазигрупп порядка* k*.*

§ 1.6.3. Доказательство теоремы 19

Доказательство теоремы будем проводить методом математической индукции по арности квазигрупп со следующим индукционным предположением (ИП):
для любого натурального m, $m \leq n-1$, *каждая пара совместимых* m*-арных квазигрупп порядка* 4 *является дополняемой.*

По предложению 75 ИП эквивалентно следующему :
для любого натурального m, $m \leq n$, *дополнение расщепляемого* 2-МДР*-кода в* Q_4^m *является расщепляемым* 2*-МДР кодом.*

Сформулируем и докажем несколько вспомогательных предложений и лемм. Всюду в этом разделе подразумевается, что мультиарные квазигруппы имеют порядок 4.

Из предложений 50, 55, теоремы 7 и определения полулинейности следует

Предложение 79. *Пусть* f *— неразделимая* n*-арная квазигруппа. Тогда*

(a) *ретракты* $f|_{x_1=a}$, $a \in Q_4$, *полулинейные;*

(b) *для каждого* $a \in Q_4$ *среди ретрактов* $f|_{x_1=b}$, $b \in Q_4 \setminus \{a\}$, *имеется два противоположных ретракту* $f|_{x_1=a}$, *и один изотопный вида* $\tau f|_{x_1=a}$, *где* τ — *некоторая перестановка.*

(c) *два ретракта* $f|_{x_1=a}$ *и* $f|_{x_1=b}$ *дополняются только до неразделимой* n*-арной квазигруппы, изотопной* n*-арной квазигруппе* f *тогда и только тогда, когда они противоположны.*

Предложение 80. *Если два полулинейных* МДР*-кода* $\mathcal{M}\langle f\rangle$ *и* $\mathcal{M}\langle g\rangle$ *не пересекаются и характеристики содержащих их линейных* 2-МДР*-кодов различаются во всех позициях, то один из* МДР*-кодов* $\mathcal{M}\langle f\rangle$ *или* $\mathcal{M}\langle g\rangle$ *линейный.*

Доказательство. Условие предложения эквивалентно следующему: найдутся $a, b \in Q_4 \setminus \{0\}, a \neq b$, что множества $\mathcal{S}_{0,a}\langle f\rangle$ и $\mathcal{S}_{0,b}\langle g\rangle$ являются линейными и все составляющие их простые унитрейды попарно пересекаются. Без ограничения общности можно положить, что характеристика линейного 2-МДР-кода, содержащего МДР-код $\mathcal{M}\langle f\rangle$, равна $(1, 1, \ldots, 1)$. Тогда $a = 1$ и множество $\mathcal{S}_{0,1}\langle f\rangle$ состоит из непересекающихся простых кодов вида $S_\sigma = \bigotimes_{i=1}^{n} \{0,1\}^{\sigma_i}$, где $\sigma_i \in \{0,1\}$, $\{0,1\}^1 = \{0,1\}$ и $\{0,1\}^0 = \{2,3\}$.

Пусть $b = 2$ (случай $b = 3$ аналогичен). Если $f(\mathcal{S}_{0,1}\langle f\rangle \cap \mathcal{S}_{0,2}\langle g\rangle) = \{1\}$, то n-арная квазигруппа f — линейная. Пусть f — нелинейная n-арная квазигруппа и $f(\{0,1\}^n \cap \mathcal{S}_{0,2}\langle g\rangle) \neq \{1\}$. По условию (характеристики линейных 2-МДР-кодов различаются во всех позициях) множество $P = \{0,1\}^n \cap \mathcal{S}_{0,2}\langle g\rangle$ состоит из всех чётных или всех нечётных булевых векторов. Поэтому функция f постоянна на P. Таким образом, $f(P) = \{0\}$ и $g(P) = \{2\}$. Кроме того, $f(\{0,1\}^n \setminus P) = \{1\}$, следовательно, $g(\{0,1\}^n \setminus P) = \{3\}$. Тогда множество $\mathcal{S}_{0,3}\langle g\rangle$ является линейным 2-МДР-кодом и n-арная квазигруппа g линейна по предложению 51 (b, c). ▲

Предложение 81. *Пусть полулинейный* МДР*-код* $M \subset Q_4^n$ *удовлетворяет равенству* (1.19), *т. е. содержится в линейном* 2-МДР*-коде с характеристикой* $\overline{1}$, *полулинейный* МДР*-код* $M' \subset Q_4^n$ *содержится в линейном* 2-МДР*-коде с характеристикой* $(\alpha_1, \ldots, \alpha_n)$, *где* $\alpha_1 = 1$, $\alpha_{n-1} \neq 1$, $\alpha_n \neq 1$ *и* $M \cap M' = \varnothing$. *Тогда функция* $\lambda_M(\overline{\mu})$ *не зависит существенно от переменных* μ_{n-1} *и* μ_n.

Доказательство. При $n = 3$ данное утверждение можно проверить простым перебором. Пусть $n > 3$. Фиксируя произвольным образом переменные μ_i при $i \neq 1, n-1, n$, сводим вопрос к рассмотренному выше трёхмерному случаю. ▲

Из предложений 80, 81 и 53 непосредственно следует

Предложение 82. *Если два нелинейных* МДР*-кода, среди которых по крайней мере один неразделим, не пересекаются, то характеристики содержащих их линейных* 2-МДР*-кодов могут различаться не более чем в одной позиции.*

Предложение 83. *Пусть f и g совместимые n-арные квазигруппы и выполнено одно из условий* (a) $\mathcal{S}_{a,b}\langle f\rangle = Q_4^n \setminus \mathcal{S}_{a,b}\langle g\rangle$ *или* (b) $\mathcal{S}_{a,b}\langle f\rangle = \mathcal{S}_{a,c}\langle g\rangle$ *для некоторых попарно различных $a, b, c \in Q_4$. Тогда пара n-арных квазигрупп f и g дополняема, причём в случае* (b) $g = \sigma f$ *для некоторой перестановки σ.*

Доказательство. Пусть $\{c, d\} = Q_4 \setminus \{a, b\}$. (a) Определим перестановку τ на множестве Q_4 равенством $\tau = (a, b)(c, d)$. Тогда n-арные квазигруппы f и g дополняются до $(n+1)$-арной квазигруппы n-арными квазигруппами τf и τg. (b) Нетрудно видеть, что $g = \sigma f$, $\sigma = (acdb)$. По теореме Кёнига [141] тождественная перестановка Id и перестановка σ дополняются до латинского квадрата некоторыми перестановками, например, $\sigma' = (abdc)$ и $\sigma'' = (ad)(bc)$. Тогда n-арные квазигруппы $\sigma' f$ и $\sigma'' f$ дополняют n-арные квазигруппы f и g.▲

Предложение 84. *Пусть $M_1, M_2 \subset Q_4^{n+1}$ — 1-полулинейные (но не линейные)* МДР*-коды такие, что $M_1 \cap (\theta_1, \theta_2, \mathrm{Id}, \ldots, \mathrm{Id})M_2 = \varnothing$ и $M_1 \cap (\theta_1, \mathrm{Id}, \ldots, \mathrm{Id})M_2 = \varnothing$, где $\theta_1 \notin \Omega = \{\mathrm{Id}, (0,1), (2,3), (0,1)(2,3), (0,2)(1,3), (0,3)(1,2)\}$, $\theta_2 \neq \mathrm{Id}$. Тогда* МДР*-коды M_1 и M_2 изотопны и разделимы.*

Доказательство. Пусть S — линейный 2-МДР-код, содержащий МДР-код M_2. По условию характеристика S равна $(1, \ldots, 1)$. Нетрудно видеть, что для произвольной изотопии $\bar{\xi}$ линейный 2-МДР-код $\bar{\xi}S$ имеет характеристику $(1, \ldots, 1)$ тогда и только тогда, когда $\xi_i \in \Omega$ при любом $i = 1, \ldots, n+1$. Тогда из условия и предложения 82 следует, что $\theta_2 \in \Omega$.

Рассмотрим n-арные квазигруппы $f = F_1\langle M_1\rangle$ и $g_1 = F_1\langle(\theta_1, \theta_2, \mathrm{Id}, \ldots, \mathrm{Id})M_2\rangle$ и $g_2 = F_1\langle(\theta_1, \mathrm{Id}, \ldots, \mathrm{Id})M_2\rangle$. Из 1-полулинейности кодов M_1, M_2 следует выполнение

условия предложения 83(b). Следовательно, $g_1 = \sigma_1 f$ и $g_2 = \sigma_2 f$ для некоторых перестановок σ_1 и σ_2, $\sigma_1 \neq \sigma_2$. Тогда имеем равенство

$$\chi_{M_1}(\sigma_2^{-1}\sigma_1 x_1, x_2, x_3, \ldots, x_{n+1}) \equiv \chi_{M_1}(x_1, x_2, x_3, \ldots x_{n+1}). \tag{1.25}$$

Поскольку МДР-код M_1 содержится в единственном линейном 2-МДР-коде с характеристикой $(1, \ldots, 1)$, имеем $\sigma_2^{-1}\sigma_1 \in \Omega$. Рассмотрим функцию λ_{M_1}. Из равенства (1.25) следует, что

$$\lambda_{M_1}(x_1 \oplus 1, x_2, \ldots, x_{n+1}) \equiv \lambda_{M_1}(x_1, x_2, x_3, \ldots x_{n+1}).$$

Тогда заданная на булевых векторах одной чётности функция λ_{M_1} существенно зависит только от $n-1$ переменной. По предложению 53 МДР-код M_1 разделим. ▲

Предложение 85. *Пусть* 2-МДР-*код* $S \subset Q_4^{n+1}$ *расщепляем и справедливо равенство* $\chi_S = \chi_{S_1} \oplus \chi_{S_2}$, *где* S_1 *и* S_2 — 2-МДР-*коды меньших размерностей. Тогда* 2-МДР-*код* $S' = Q_4^{n+1} \setminus S$ *расщепляем.*

Доказательство. Пусть $S_1 \subset Q_4^m$, $S_2 \subset Q_4^{n-m+1}$, $1 \leq m \leq n$. Введём обозначения $S_1' = Q_4^m \setminus S_1$ и $S_2' = Q_4^{n-m+1} \setminus S_2$. Тогда $\chi_S = \chi_{S_1} \oplus \chi_{S_2} = \chi_{S_1'} \oplus \chi_{S_2'}$. Из предложения 31 следует, что 2-МДР-коды S_1, S_2, S_1' и S_2' являются расщепляемыми. Очевидно, $\chi_{S'} = \chi_{S_1} \oplus \chi_{S_2'}$. Тогда из предложения 31 получаем, что 2-МДР-код S' также является расщепляемым. ▲

Предложение 86.

Пусть $\Omega = \{\mathrm{Id}, (0,1), (2,3), (0,1)(2,3), (0,2)(1,3), (0,3)(1,2)\}$ — *множество перестановок,* g *и* f — n-*арные квазигруппы и для любого набора* $\overline{u} \in Q_4^{n-1}$ *и любого* $i \in [n]$ *перестановка* $\xi_{i,\overline{u}}$, *определяемая равенством одномерных ретрактов* $g(z\overline{u}) = \xi_{i,\overline{u}} f(z\overline{u})$, *где переменная* z *подставлена в* i-*ю позицию, содержится в множестве* Ω. *Тогда* $\mathcal{S}_{0,1}\langle f\rangle = \mathcal{S}_{0,1}\langle g\rangle$ *или* $\mathcal{S}_{0,1}\langle f\rangle = \mathcal{S}_{2,3}\langle g\rangle$.

Доказательство. Докажем по индукции, что если $\mathcal{S}_{0,1}\langle f\rangle \cap \mathcal{S}_{0,1}\langle g\rangle \neq \varnothing$, то $\mathcal{S}_{0,1}\langle f\rangle = \mathcal{S}_{0,1}\langle g\rangle$. При $n = 1, 2$ это предположение легко проверить простым перебором. Индукционный шаг следует из рассмотрения гиперграней множества Q_4^n, поскольку множество $\mathcal{S}_{0,1}\langle f\rangle$ как 2-МДР-код пересекается с любой гранью размерности $n-2$ при $n \geq 3$. ▲

Предложение 87. *Пусть не пересекающиеся* МДР-*коды* $M_1, M_2 \subset Q_4^n$ *определяются уравнениями* $f_1(\widetilde{x}_1) = g_1(\widetilde{x}_2)$ *и* $f_2(\widetilde{x}_1) = g_2(\widetilde{x}_2)$ *соответственно, где* $\widetilde{x}_1$, $\widetilde{x}_2$ — *непересекающиеся наборы переменных, кроме того* f_1 *и* f_2 — *пара, состоящая из* 1-*полулинейной и анти*-1-*полулинейной* n_1-*арных квазигрупп,* $n_1 \geq 2$. *Тогда при выполнении ИП множество* $Q_4^{n+1} \setminus (M_1 \cup M_2)$ — *расщепляемый* 2-МДР-*код.*

Доказательство. Из условия имеем $\mathcal{M}_0\langle f_1\rangle \cup \mathcal{M}_1\langle f_1\rangle = \mathcal{M}_2\langle f_2\rangle \cup \mathcal{M}_3\langle f_2\rangle$. Если для любого $a \in Q_4$ найдётся такое $\tau(a) \in Q_4$, что $\mathcal{M}_a\langle f_1\rangle = \mathcal{M}_{\tau(a)}\langle f_2\rangle$, то $\tau f_1 = f_2$. Тогда требуемое следует из ИП для мультиарных квазигрупп g_1 и τg_2.

В противном случае $\mathcal{M}_0\langle f_1\rangle \cap \mathcal{M}_2\langle f_2\rangle \neq \varnothing$ и одновременно $\mathcal{M}_0\langle f_1\rangle \cap \mathcal{M}_3\langle f_2\rangle \neq \varnothing$ или, симметрично, $\mathcal{M}_2\langle f_1\rangle \cap \mathcal{M}_0\langle f_2\rangle \neq \varnothing$ и $\mathcal{M}_2\langle f_1\rangle \cap \mathcal{M}_1\langle f_2\rangle \neq \varnothing$. Пусть выполнено первое. Тогда из условия имеем $\mathcal{M}_1\langle f_1\rangle \cap \mathcal{M}_2\langle f_2\rangle \neq \varnothing$ и $\mathcal{M}_1\langle f_1\rangle \cap \mathcal{M}_3\langle f_2\rangle \neq \varnothing$. Поскольку $M_1 \cap M_2 = \varnothing$, получаем

$\mathcal{M}_0\langle f_1\rangle \cap \mathcal{M}_2\langle f_2\rangle \neq \varnothing \Rightarrow \mathcal{M}_0\langle g_1\rangle \cap \mathcal{M}_2\langle g_2\rangle = \varnothing$,$\mathcal{M}_0\langle f_1\rangle \cap \mathcal{M}_3\langle f_2\rangle \neq \varnothing \Rightarrow$
$\mathcal{M}_0\langle g_1\rangle \cap \mathcal{M}_3\langle g_2\rangle = \varnothing$,
$\mathcal{M}_1\langle f_1\rangle \cap \mathcal{M}_2\langle f_2\rangle \neq \varnothing \Rightarrow \mathcal{M}_1\langle g_1\rangle \cap \mathcal{M}_2\langle g_2\rangle = \varnothing$,$\mathcal{M}_1\langle f_1\rangle \cap \mathcal{M}_3\langle f_2\rangle \neq \varnothing \Rightarrow$
$\mathcal{M}_1\langle g_1\rangle \cap \mathcal{M}_3\langle g_2\rangle = \varnothing$.

Следовательно, $\mathcal{S}_{0,1}\langle g_1\rangle = \mathcal{S}_{0,1}\langle g_2\rangle$. Тогда МДР-код $\{(\widetilde{x}_1, \widetilde{x}_2) : f_1(\widetilde{x}_1) = \tau g_1(\widetilde{x}_2)\}$, где $\tau = (0,1)(2,3)$, не пересекается с МДР-кодами M_1 и M_2. ▲

Предложение 88. *Любая пара совместимых неразделимых* n-*арных квазигрупп* f *и* g *дополняема.*

Доказательство. Из теоремы 7 и предложения 82 следует, что n-арные квазигруппы f и g полулинейны, причём характеристики 2-МДР-кодов, содержащих МДР-коды $\mathcal{M}\langle f\rangle$ и $\mathcal{M}\langle g\rangle$, отличаются не более чем в одной координате. Тогда в случае, когда характеристики не отличаются, требуемое утверждение вытекает из предложения 83 (a), а в случае, когда характеристики отличаются в одной координате, — из предложения 83 (b).▲

Предложение 89. *Пусть* n-*арная квазигруппа* f *не является анти*-1-*полулинейной. Тогда существует не более одной* 1-*полулинейной* n-*арной квазигруппы* g, *совместимой с* f.

Доказательство. Пусть g — 1-полулинейная n-арная квазигруппа. Пусть найдётся унитрейд $S' \subset \mathcal{S}_{01}\langle g\rangle \setminus \mathcal{S}_{01}\langle f\rangle$. Тогда из утверждения 30 следует, что $\mathcal{S}_{01}\langle f\rangle = Q_4^n \setminus \mathcal{S}_{01}\langle g\rangle$, т. е. n-арная квазигруппа f является анти-1-полулинейной, что противоречит условию. Таким образом, любой простой унитрейд $S' \subset \mathcal{S}_{01}\langle g\rangle$ имеет непустое пересечение с множеством $\mathcal{S}_{01}\langle f\rangle$. Нетрудно видеть, что в этом случае для совместимой с f n-арной квазигруппы g значения на множестве S' определены однозначно. Поскольку множество $\mathcal{S}_{01}\langle g\rangle$ однозначно разбивается на простые унитрейды (см. следствие 6), на нём значения n-арной квазигруппы g определены однозначно. Аналогично однозначно определяются значения n-арной квазигруппы g на множестве $\mathcal{S}_{23}\langle g\rangle$. ▲

Лемма 10 ([51]). *Пусть разделимая n-арная квазигруппа f совместима с полулинейной n-арной квазигруппой g ($n \geq 3$). Тогда n-арная квазигруппа g разделима или n-арная квазигруппа f полулинейна и противоположна g.*

Доказательство. Можно считать (см. предложение 43), что n-арная квазигруппа f представима в виде $f(\overline{x}, \overline{y}) \equiv f'(\overline{x}, f''(\overline{y}))$, где f' — n_1-арная квазигруппа, f'' — неразделимая n_2-арная квазигруппа, $n_1 + n_2 = n + 1$, $1 < n_2 < n$. n_2-Арную квазигруппу f'' всегда можно выбрать такой, что $f''(0\overline{0}) = 0$ и $f''(1\overline{0}) = 1$. Для упрощения рассуждений без потери общности полагаем, что n-арная квазигруппа g является 1-полулинейной. Рассмотрим ретракты $f'_a = f'|_{x_{n_1}=a}$, $a \in Q_4$. Из леммы 1 (лемма о линейном антислое) следует, что возможны три случая:

1) все четыре ретракта не являются 1-полулинейными и не являются анти-1-полулинейными;

2) имеется ровно один 1-полулинейный и один анти-1-полулинейный ретракты;

3) имеется два 1-полулинейных и два анти-1-полулинейных ретракта.

Рассмотрим случаи 1) – 3) по отдельности.

1) Предположим имеется более четырёх различных ретрактов $g|_{\overline{y}=\overline{v}}$ при $\overline{v} \in Q_4^{n_2}$. По предложению 50(b) все ретракты $g|_{\overline{y}=\overline{v}}$ при $\overline{v} \in Q_4^{n_2}$ 1-полулинейные или анти-1-полулинейные. Тогда можно считать, что имеется не менее трёх различных 1-полулинейных ретракта $g|_{\overline{y}=\overline{v}}$, поскольку случай, когда имеется три анти-1-полулинейных

ретракта, симметричен рассматриваему. Из 1-полулинейности g следует, что для каждого 1-полулинейного ретракта $g|_{\overline{y}=\overline{v}}$ найдётся парный к нему 1-полулинейный ретракт $g|_{\overline{y}=\overline{u}}$ такой, что $g|_{\overline{y}=\overline{v}} = \tau g|_{\overline{y}=\overline{u}}$, где $\tau = (0,1)(2,3)$. Это равенство верно для любых двух 1-полулинейных ретрактов $g|_{\overline{y}=\overline{v}}$ и $g|_{\overline{y}=\overline{u}}$, если наборы $\overline{v}$ и $\overline{u}$ отличаются ровно в одной позиции. Следовательно, число различных 1-полулинейных ретрактов $g|_{\overline{y}=\overline{v}}$ должно быть чётным. По предложению 89 каждая из 4-х (n_1-1)-арных квазигрупп f'_a, $a \in Q_4$, совместима не более чем с одним 1-полулинейным ретрактом. Тогда имеется ровно 4 различных 1-полулинейных ретрактов $g|_{\overline{y}=\overline{v}}$ и они находятся во взаимно однозначном соответствии с ретрактами f'_a, $a \in Q_4$. В любой 1-полулинейной n-арной квазигруппе g имеется только два различных ретракта $g|_{\overline{y}=\overline{v}}$ при $\overline{v} \in \{0,1\}^{n_2}$, которые получаются один из другого умножением на перестановку τ. Тогда имеется только два различных ретракта $f|_{\overline{y}=\overline{v}}$ при $\overline{v} \in \{0,1\}^{n_2}$, т. е. n_2-арная квазигруппа f'' принимает только два значения на множестве $\overline{v} \in \{0,1\}^{n_2}$. Теперь из предложения 30 можно заключить, что n_2-арная квазигруппа f'' является 1-полулинейной (здесь используем, что $f''(0\overline{0}) = 0$ и $f''(1\overline{0}) = 1$). Получается, что $f''(\overline{v}) \in \{0,1\}$ тогда и только тогда, когда ретракт $g|_{\overline{y}=\overline{v}}$ является 1-полулинейным. Следовательно, любой 1-полулинейный ретракт $g|_{\overline{y}=\overline{v}}$ при $\overline{v} \in Q_4^{n_2}$ совместим с f'_0 или с f'_1. Тогда по предложению 89 имеется ровно два различных 1-полулинейных ретракта $g|_{\overline{y}=\overline{v}}$. Пришли к противоречию. Значит, имеется всего 4 различных ретракта $g|_{\overline{y}=\overline{v}}$ при $\overline{v} \in Q_4^{n_2}$ (1-полулинейных и анти-1-полулинейных) и из предложения 40 получаем требуемое утверждение.

2) Предположим, что ретракт f'_0 является 1-полулинейным и ретракт f'_2 является анти-1-полулинейным (остальные случаи можно рассмотреть аналогичным образом). Рассмотрим 4 ретракта $g'_a = g|_{\overline{y}=a\overline{0}}$, $a \in Q_4$. По предложению 50(b) ретракты g'_0 и g'_1 — 1-полулинейные, а ретракты g'_2 и g'_3 — анти-1-полулинейные. Ретракт f'_1 совместим с двумя 1-полулинейными (n_1-1)-арными квазигруппами g'_1 и f'_0. Из предложения 89 следует, что $g'_1 = f'_0$. Тем же способом получаем равенство $g'_3 = f'_2$. Поскольку n-арная квазигруппа g является 1-полулинейной, имеем $g'_0 = \tau g'_1 = \tau f'_0$ и $g'_2 = \tau g'_3 = \tau f'_2$. Заметим, что аналогичные рассуждения справедливы для любого набора $\overline{u} \in Q_4^{n_2-1}$ и ретрактов $g|_{\overline{y}=a\overline{u}}$, $a \in Q_4$. Таким образом, имеется всего 4 различных ретракта $g|_{\overline{y}=a\overline{u}}$,

каждый из которых совпадает с одной из (n_1-1)-арных квазигрупп f'_0, f'_2, $\tau f'_0$, $\tau f'_2$. Тогда из предложения 40 следует разделимость n-арной квазигруппы g.

3) Если для каждого 1-полулинейного ретракта $g|_{\overline{y}=\overline{v}}$ при $\overline{v} \in Q_4^{n_2}$ ретракт $f|_{\overline{y}=\overline{v}}$ является анти-1-полулинейным, то n-арная квазигруппа f противоположна g и, следовательно, полулинейна. В противном случае найдётся такое $\overline{v} \in Q_4^{n_2}$, что ретракты $g|_{\overline{y}=\overline{v}}$ и $f|_{\overline{y}=\overline{v}}$ являются 1-полулинейными. Без ограничения общности предположим, что $\overline{v} = 0\overline{0}$. Тогда $\tau g|_{\overline{y}=1\overline{0}} = g|_{\overline{y}=0\overline{0}} = \tau f|_{\overline{y}=0\overline{0}}$, т. е. $g|_{\overline{y}=1\overline{0}} = f|_{\overline{y}=0\overline{0}} = f'_0$. Далее заключаем, что наборы ретрактов g'_0, g'_1, g'_2, g'_3 и f'_0, f'_1, f'_2, f'_3 состоят из одинаковых (n_1-1)-арных квазигрупп, взятых в разном порядке. Из предложения 30 следует, что множество $\mathcal{S}_{0,1}\langle f|_{\overline{x}=\overline{0}}\rangle$ имеет непустое пересечение со всеми простыми унитрейдами — компонентами 2-МДР-кода $\mathcal{S}_{0,1}\langle g|_{\overline{x}=\overline{0}}\rangle$ (случай, когда $\mathcal{S}_{0,1}\langle f|_{\overline{x}=\overline{0}}\rangle = Q_4^n \setminus \mathcal{S}_{0,1}\langle g|_{\overline{x}=\overline{0}}\rangle$, рассмотрен в начале п. 3)). Аналогичным образом получаем, что в любом простом унитрейде, содержащимся в $\mathcal{S}_{0,1}\langle g|_{\overline{x}=\overline{0}}\rangle$, найдётся такой $\overline{v} \in Q_4^{n_2}$, что ретракт $g|_{\overline{y}=\overline{v}}$ совпадает с одной из 4-х (n_1-1)-арных квазигрупп f'_0, f'_1, f'_2, f'_3. Тогда это верно для любого $\overline{v} \in Q_4^{n_2}$, так как для всех $\overline{v} \in Q_4^{n_2}$, лежащих в простом унитрейде из множества $\mathcal{S}_{0,1}\langle g|_{\overline{x}=\overline{0}}\rangle$, ретракты $g|_{\overline{y}=\overline{v}}$ бывают только двух видов, переходящих друг в друга под действием перестановки τ. Из предложения 40 следует разделимость n-арной квазигруппы g. ▲

Предложение 90. *Пусть f и g — разделимые совместимые n-арные квазигруппы и*

$$f(\overline{x}) \equiv f_0(q_1(\tilde{x}_1), ..., q_m(\tilde{x}_m)),$$

$$g(\overline{x}) \equiv g_0(q'_1(\tilde{x}'_1), ..., q'_{m'}(\tilde{x}'_{m'})),$$

где f_0 и g_0 — неразделимые мультиарные квазигруппы ($m \geq 3$, $m \geq m'$), $\{I_j\}_{j=1,...,m}$ и $\{I'_j\}_{j=1,...,m'}$ — несовпадающие разбиения множества $[n]$. Пусть f_0 — 1-полулинейная m-арная квазигруппа, $\tau = (01)(23)$. Тогда $g(\overline{x}) \neq \tau f(\overline{x})$ для любого $\overline{x} \in Q_4^n$, т. е. пара n-арных квазигрупп f и g дополняема.

Доказательство. Из множества $[n]$ выберем m таких чисел i_j, чтобы для каждого $j \in [m]$ нашёлся номер $i_j \in I_j$ и в то время некоторые из множеств I'_j содержали более одного элемента. Без ограничения общности можно считать, что $[m]$ — требуемый набор чисел. Набор переменных $x_1, \ldots, x_m$ будем обозначать через $\overline{y}$, а

набор переменных $x_{m+1}, \dots, x_n$ — через $\overline{z}$. По построению ретракт $f|_{\overline{z}=\overline{u}}$ неразделим, а ретракт $g|_{\overline{z}=\overline{u}}$ разделим при любом $\overline{u} \in Q_4^{n-m}$. Из предложения 50(b) следует, что $\mathcal{S}_{0,1}\langle f|_{\overline{z}=\overline{u}}\rangle$ — линейный 2-МДР-код. Тогда из леммы 10 имеем $\mathcal{S}_{0,1}\langle f|_{\overline{z}=\overline{u}}\rangle = Q_4^m \setminus \mathcal{S}_{0,1}\langle g|_{\overline{z}=\overline{u}}\rangle$ при любом $u \in Q_4^{n-m}$. Таким образом, $\mathcal{S}_{0,1}\langle \tau f\rangle = \mathcal{S}_{0,1}\langle f\rangle = Q_4^n \setminus \mathcal{S}_{0,1}\langle g\rangle$. Из предложения 76(a) получаем, что пара n-арных квазигрупп f и g дополняема. ▲

Предложение 91. *Пусть непересекающиеся* МДР*-коды* $M_1 = \mathcal{M}\langle f\rangle$ *и* $M_2 = \mathcal{M}\langle g\rangle$ *определяются каноническими представлениями*

$$q_{m+1}(x_{n+1}, \tilde{x}_{m+1}) = q_0(q_1(\tilde{x}_1), ..., q_m(\tilde{x}_m)) \quad и$$

$$q'_{m'+1}(x_{n+1}, \tilde{x}'_{m'+1}) = q'_0(q'_1(\tilde{x}'_1), ..., q'_{m'}(\tilde{x}'_{m'})),$$

где $m \geq m' \geq 3$*, и соответствующие этим представлениям разбиения* $\{I_j\}_{j=1,\dots,m+1}$ *и* $\{I'_j\}_{j=1,\dots,m'+1}$ *множества* $[n]$ *не совпадают. Тогда при выполнении ИП пара* n*-арных квазигрупп* f *и* g *дополняема.*

Доказательство. По теореме 7 неразделимая m-арная квазигруппа является полулинейной и, следовательно, эквивалентной некоторой 1-полулинейной. Без ограничения общности m-арную квазигруппу q_0 можно считать 1-полулинейной.

Определим МДР-код $N \subset Q_4^{n+1}$ как множество решений уравнения

$$q_{m+1}(x_{n+1}, \tilde{x}_{m+1}) = \tau q_0(q_1(\tilde{x}_1), ..., q_m(\tilde{x}_m)), \tag{1.26}$$

где τ — перестановка (01)(23).

Зафиксируем произвольным образом все переменные набора $\tilde{x}_{m+1}$, т. е. возьмём $\tilde{x}_{m+1} = \widetilde{u}$. Из определения канонического представления имеем, что группы переменных $\tilde{x}_{m+1}$ и $\tilde{x'}_{m'+1}$ минимально возможные по мощности. Таким образом, ретракты $F_{n+1}\langle M_1\rangle|_{\tilde{x}_{m+1}=\widetilde{u}}$ и $F_{n+1}\langle M_2\rangle|_{\tilde{x}_{m+1}=\widetilde{u}}$ удовлетворяют условию предложения 90. Тогда МДР-коды $M_1|_{\tilde{x}_{m+1}=\widetilde{u}}$, $M_2|_{\tilde{x}_{m+1}=\widetilde{u}}$, $N|_{\tilde{x}_{m+1}=\widetilde{u}}$ попарно не пересекаются. Из произвольности выбора набора значений $\widetilde{u}$ и предложения 76(a) получаем требуемое. ▲

Совершенно аналогично предложению 91 можно доказать

Предложение 92. *Пусть* n*-арная квазигруппа* f *не полностью разделима, а* n*-арная квазигруппа* g *полностью разделима. Тогда при выполнении ИП из совместимости пары* n*-арных квазигрупп* f *и* g *следует их дополняемость.*

Предложение 93. *Пусть f и g — разделимые совместимые n-арные квазигруппы и их канонические представления ($m \geq 4$) имеют одинаковые разбиения множества переменных, т. е.*

$$\mathcal{M}\langle f\rangle = \{\overline{x} \in Q_4^{n+1} : q_1(\tilde{x}_1) = f_0(q_2(\tilde{x}_2), ..., q_m(\tilde{x}_m))\}, \tag{1.27}$$

$$\mathcal{M}\langle g\rangle = \{\overline{x} \in Q_4^{n+1} : q'_1(\tilde{x}_1) = g_0(q'_2(\tilde{x}_2), ..., q'_m(\tilde{x}_m))\}.$$

Тогда при выполнении ИП пара n-арных квазигрупп f и g дополняема.

Доказательство. Если все наборы переменных $\tilde{x}_i$, $i = 1, \ldots, m$, состоят ровно из одной переменной, то требуемое вытекает из предложения 88.

Изменяя квазигруппы q_i в выражении (1.27), $(m-1)$-арную квазигруппу f_0 можно преобразовать в любую изотопную ей $(m-1)$-арную квазигруппу без изменения множества $\mathcal{M}\langle f\rangle$. Поэтому можно считать, что m-арные квазигруппы f_0 и g_0 — 1-полулинейные, т. е. $\mathcal{M}\langle f_0\rangle, \mathcal{M}\langle g_0\rangle \subset S$, где $\chi_S(\overline{y}) = 1 \oplus \bigoplus\limits_{i=1}^{m} \chi_{\{0,1\}}(y_i)$. Без ограничения общности положим[5], что переменная x_i содержится в группе переменных $\tilde{x}_i$ при любом $i = 1, \ldots, m$.

Теперь рассмотрим фиксацию переменных $x_{m+1}, \ldots, x_{n+1}$ произвольными константами. Предположим найдутся номер $i \in [m]$ и набор $\overline{u} \in Q_4^{n_i-1}$ такие, что $q_i(z\overline{u}) = \xi q'_i(z\overline{u})$, где перестановка $\xi \notin \Omega = \{\mathrm{Id}, (0,1), (2,3), (0,1)(2,3), (0,2)(1,3), (0,3)(1,2)\}$ (предполагается, что переменная z может быть подставлена на любую позицию). Из предложения 84 вытекает, что если квазигруппы q_j и q'_j при некотором $j \in [m]\setminus\{i\}$ не совпадают с точностью до перестановки значений (т. е. $q_j \neq \sigma q'_j$ для некоторой перестановки σ), то m-арные квазигруппы f_0 и g_0 разделимы, что противоречит условию.

Если арности квазигрупп q_j равны 1 при любом $j \in [m]$, $j \neq i$, то требуемое следует из предложения 87. Пусть $q_j = \sigma q'_j$ и квазигруппа q_j зависит не менее чем от двух переменных. Тогда после замены на новую переменную одинаковых функций q_j в канонических представлениях (1.27) к полученным в результате МДР-кодам меньшей размерности можно применить ИП, а затем, произведя обратную замену, получить требуемое.

[5] Для упрощения рассуждений в предложении 93 роль выделенной переменной x_{n+1} в каноническом представлении играет переменная x_1.

Ясно, что $\mathcal{M}\langle f\rangle \subset \widetilde{S}$, где 2-МДР-код $\widetilde{S}$ определяется формулой

$$\chi_{\widetilde{S}}(\overline{x}) = 1 \oplus \bigoplus_{j=1}^{m} \chi_{\{0,1\}}(q_j(\tilde{x}_j)).$$

В случае, если для любого номера $i \in [m]$ и набора $\overline{u} \in Q_4^{n_i-1}$ перестановка ξ, определяемая равенством $q_i(z\overline{u}) = \xi q_i'(z\overline{u})$, содержится в множестве Ω, по предложению 86 получаем, что $\chi_{\{0,1\}}(q_j(\tilde{x}_j)) = \chi_{\{0,1\}}(q_j'(\tilde{x}_j))$ или $\chi_{\{0,1\}}(q_j(\tilde{x}_j)) = 1 \oplus \chi_{\{0,1\}}(q_j'(\tilde{x}_j))$. Тогда МДР-код $\mathcal{M}\langle g\rangle$ содержится либо в 2-МДР-коде $\widetilde{S}$, либо в его дополнении. По предложению 85 и ИП 2-МДР-коды $\widetilde{S}$ и $Q_4^{n+1} \setminus \widetilde{S}$ являются двудольными (расщепляемыми) и из предложения 75 получаем требуемое. ▲

Предложение 94. *Пусть непересекающиеся* МДР*-коды $M_1, M_2 \subset Q_4^n$ определяются уравнениями $\varphi_1(x_1, x_2) = f_1(x_3, \ldots, x_{n+1})$ и $\varphi_2(x_1, x_2) = f_2(x_3, \ldots, x_{n+1})$ соответственно, $n \geq 4$. Тогда из ИП вытекает, что $Q_4^{n+1} \setminus (M_1 \cup M_2)$ — расщепляемый* 2*-*МДР*-код.*

Доказательство. Из перебора всевозможных пар 2-квазигрупп φ_1 и φ_2 видно, что возможны следующие случаи.

0) МДР-коды $C_a^1 = \mathcal{M}_a\langle\varphi_1\rangle$ и $C_b^2 = \mathcal{M}_b\langle\varphi_2\rangle$ пересекаются для любой пары $(a, b) \in Q_4^2$.

1) Существует такая перестановка π, что МДР-коды C_a^1 и C_b^2 не пересекаются тогда и только тогда, когда $b = \pi(a)$.

2) Существует такая перестановка π, что МДР-коды C_a^1 и C_b^2 пересекаются тогда и только тогда, когда $b = \pi(a)$.

3) Квазигруппы φ_1 и φ_2 противоположные, но неэквивалентные.

Рассмотрим случаи 0) — 3) по отдельности.

0) Противоречит условию непересекаемости МДР-кодов M_1 и M_2.

1) Из непересекаемости МДР-кодов M_1 и M_2 следует, что $f_2 = \pi f_1$. Перенесём перестановку π в левую часть уравнения, задающего МДР-код M_2. Получаем, что МДР-код M_2 задаётся равенством $\pi\varphi_2(x_1, x_2) = f_1(x_3, \ldots, x_{n+1})$ и утверждение сводится к дополняемости пар совместимых 2-квазигрупп.

2) Имеем $\varphi_1 = \tau\varphi_2$ для некоторой перестановки τ и утверждение сводится к дополняемости пар совместимых $(n-1)$-арных квазигрупп.

3) Требуемое следует из предложения 87. ▲

Пару переменных $\langle x_i, x_j\rangle$ будем называть *внутренней* относительно n-арной квазигруппы f, если $f(\overline{x}) \equiv g(\varphi(x_i, x_j), \widetilde{x})$, где g — некоторая $(n-1)$-арная квазигруппа, φ — некоторая 2-квазигруппа и $\widetilde{x}$ — набор переменных с индексами из множества $[n] \setminus \{i, j\}$. Например, пары переменных $\langle x_1, x_2\rangle$ и $\langle x_3, x_4\rangle$ являются внутренними для 9-квазигруппы f, изображённой на рис. 1.6. Нетрудно видеть, что если пара переменных $\langle x_i, x_j\rangle$ является внутренней относительно n-арной квазигруппы f, то она является внутренней и относительно любого ретракта n-арной квазигруппы f, который содержит переменные x_i и x_j. Тогда, используя теорему 3, индукцией по числу переменных нетрудно доказать

Предложение 95. *Пусть* $\{(\overline{x}, \overline{y}) : f(\overline{x}) = g(\overline{y})\} = \{(\widetilde{x}, \widetilde{y}) : f'(\widetilde{x}) = g'(\widetilde{y})\}$, *где* f, g, f', g' *— разделимые квазигруппы (от многих переменных),* $\overline{x}$, $\overline{y}$ *и* $\widetilde{x}$, $\widetilde{y}$ *— два разбиения множества переменных. Если внутренняя относительно* f *пара переменных содержится в наборе* $\widetilde{x}$, *то эта пара переменных является внутренней относительно* f'.

Пусть МДР-код определяется уравнением $f(\overline{x}) = g(\overline{y})$, т. е.
$M = \{(\overline{x}, \overline{y}) : f(\overline{x}) = g(\overline{y})\}$, где квазигруппа f полностью разделима, либо зависит от двух переменных. Пару переменных $\{x_i, x_j\}$ будем называть *внутренней* относительно МДР-кода M, если пара переменных $\{x_i, x_j\}$ — *внутренняя* относительно f или g. Обозначим через $I(M)$ множество пар внутренних переменных МДР-кода M, через $\widetilde{I}(M) = \cup I(M)$ обозначим множество внутренних переменных МДР-кода M.

Непосредственно из определения пары внутренних переменных МДР-кода вытекают следующие предложения.

Предложение 96. *Полностью разделимый* МДР-*код* $M \subset Q_4^n$ *имеет не менее двух непересекающихся пар внутренних переменных при* $n \geq 4$.

Предложение 97. *Пара переменных* $\{x_i, x_j\}$ *является внутренней относительно разделимого* МДР-*кода* $M \subset Q_4^n$ *тогда и только тогда, когда* $M = \{\varphi(x_i, x_j) = q(\widetilde{x})\}$, *где* q *— некоторая* $(n-1)$-*арная квазигруппа,* φ *— некоторая* 2-*квазигруппа и* $\widetilde{x}$ *— набор переменных с индексами из множества* $[n] \setminus \{i, j\}$.

Предложение 98. *Если пара переменных* $\{x_i, x_j\}$ *— внутренняя относительно пол-*

ностью разделимого МДР-*кода* $M \subset Q_4^n$, *то эта пара переменных является внутренней относительно ретракта* $M|_{x_k=a}$ *при любых* $a \in Q_4$ *и* $k \in [n] \setminus \{i, j\}$.

Напомним, что для любого полностью разделимого МДР-кода
$M = \{(\overline{x}, \overline{y}) : f(\overline{x}) = g(\overline{y})\}$ определено дерево $T = T(M)$.

Пусть $W \subset V(T)$ — некоторое множество вершин дерева T. Будем говорить, что вершина $w \in W$ *крайняя* в W, если в дереве T она не лежит на пути, соединяющим две другие вершины из W. Пусть $M \subset Q_4^{n+1}$ — полностью разделимый МДР-код и $S \subset [n+1]$ — некоторое подмножество переменных. Обозначим через $w(s)$ вершину дерева T, смежную с вершиной, помеченной переменной с номером s. Переменную x_t будем называть *крайней* в множестве переменных с индексами из S, $t \in S$, если вершина $w(t)$ крайняя в множестве $\{w(s) \mid s \in S\}$. Переменные x_t и x_s будем называть *соседними*, если вершины $w(s)$ и $w(t)$ являются смежными. Например, на рис. 1.6 переменные x_7 и x_8 соседние.

Пусть $M \subset Q_4^{n+1}$ — полностью разделимый МДР-код. Рассмотрение поддеревьев дерева $T(M)$ показывает, что справедливы следующие предложения.

Предложение 99.

(a) *Если вершина* $w(s)$ *имеет степень более трёх в дереве* $T(M)$, *то* $I(M|_{x_s=a}) \subset I(M)$ *при любом* $a \in Q_4$.

(b) *Если* $x_s \notin \widetilde{I}(M)$ *и* $\{x_p, x_q\} \in I(M|_{x_s=a}) \setminus I(M)$, *то переменные* x_p *и* x_s, *как и* x_q, x_s — *соседние, а* x_p, x_q — *нет.*

(c) *Если* $x_s \notin \widetilde{I}(M)$ *и* x_s — *крайняя переменная в* S, *то*
$\{\{x_p, x_q\} \mid p, q \in S\} \cap (I(M|_{x_s=a}) \setminus I(M)) = \varnothing$ *для любого* $a \in Q_4$.

Предложение 100. *Пусть* $M \subset Q_4^{n+1}$ $(n \geq 5)$ *полностью разделимый* МДР-*код,*
$x_s \in \widetilde{I}(M)$, $a \in Q_4$ *и* $M' = M|_{x_s=a}$. *Пара переменных* $\{x_p, x_q\}$ *содержится в*
$I(M') \setminus I(M)$ *тогда и только тогда, когда* МДР-*код* M *с точностью до изотопии можно представить в виде*

$$M = \{\overline{x} : x_p *_1 (x_s *_2 x_q) = f(\widetilde{x})\}, \tag{1.28}$$

где $\widetilde{x}$ — *набор переменных с индексами из множества* $[n+1] \setminus \{s, p, q\}$, f — $(n-2)$-*арная квазигруппа и групповые операции* $*_1$ *и* $*_2$ *не совпадают, причём если* $x_p \notin \widetilde{I}(M)$, *то*

$I(M') \setminus I(M) = \{x_p, x_q\}$.

Предложение 101.

(a) *Пусть* МДР-*код* $M \subset Q_4^{n+1}$ *полностью разделим. Тогда для любого* $i \in [n+1]$ *ретракты* $M|_{x_i=a}$, $a \in Q_4$, *имеют одинаковую пару внутренних переменных.*

(b) *Пусть* МДР-*код* $M \subset Q_4^{n+1}$ *разделим не полностью и для некоторого* $i \in [n+1]$ *его ретракты* $M|_{x_i=a}$, $M|_{x_i=b}$, $a, b \in Q_4$, *полностью разделимы. Тогда ретракты* $M|_{x_i=a}$ *и* $M|_{x_i=b}$, *имеют одинаковую пару внутренних переменных.*

Доказательство.

(a) Предложение 96 утверждает, что любой полностью разделимый МДР-код размерности не менее 4 имеет по крайней мере две пары внутренних переменных. По предложению 98 любая не содержащая переменную x_i пара внутренних переменных относительно M будет внутренней для ретракта $M|_{x_i=a}$, $a \in Q_4$.

(b) По следствию 4 имеем, что МДР-код M может быть представлен как множество решений уравнения

$$q_1(\tilde{x}_1) = q_0(q_2(\tilde{x}_2), ..., q_m(\tilde{x}_m)),$$

где $(m-1)$-арная квазигруппа q_0 неразделима и $m \geq 4$. Не ограничивая общности, будем полагать, что группа $\tilde{x}_1$ содержит не менее 2-х переменных. Из условия полной разделимости ретракта следует, что переменная x_i не содержится в группе $\tilde{x}_1$, кроме того квазигруппа q_1 полностью разделима или имеет арность 2. Тогда ретракты по любой переменной из группы $\tilde{x}_1$ не являются полностью разделимыми, а ретракты по любой другой переменной сохраняют пару внутренних переменных относительно q_1. ▲

Предложение 102. *Пусть полностью разделимые* МДР-*коды* $M_1, M_2 \subset Q_4^{n+1}$ *не пересекаются* ($n \geq 5$), *причём* $M_1 = \{(\widetilde{x}_1, \widetilde{x}_2) \mid f_1(\widetilde{x}_1) = g_1(\widetilde{x}_2)\}$, $M_2 = \{(\widetilde{x}_1, \widetilde{x}_2) \mid f_2(\widetilde{x}_1) = g_2(\widetilde{x}_2)\}$, *где* $\widetilde{x}_1$, $\widetilde{x}_2$ — *наборы переменных, в каждом из которых содержится не менее* 2-*х переменных. Тогда из ИП вытекает, что* $Q_4^{n+1} \setminus (M_1 \cup M_2)$ — *расщепляемый* 2-МДР-*код.*

Доказательство. Если квазигруппы f_1 и f_2 (g_1 и g_2) имеют одинаковую пару внутренних переменных, то требуемое следует из предложения 94. В против-

ном случае наборы $\widetilde{x}_1$ и $\widetilde{x}_2$ состоят не менее чем из 3-х переменных каждый. Не ограничивая общности, можно положить, что $g_1(\overline{0}x_{n+1}) = g_2(\overline{0}x_{n+1}) = x_{n+1}$. Рассмотрим МДР-коды $M_1' = \{(\widetilde{x}_1, y) \mid f_1(\widetilde{x}_1) = y\}$, $M_2' = \{(\widetilde{x}_1, y) \mid f_2(\widetilde{x}_1) = y\}$. Имеем $M_1' \cap M_2' = \varnothing$ и в рассматриваемом случае МДР-коды M_1' и M_2' не содержат одинаковой пары внутренних переменных вида $\{x_i, x_j\}$. Без ограничения общности можно полагать, что набор $\widetilde{x}_1$ выбран миниальным по мощности, поэтому общая пара $\{x_i, y\}$ также отсутствует. По ИП пара квазигрупп f_1 и f_2 дополняется, причём по предложению 101 только до неразделимой квазигруппы. Тогда, применяя предложения 79 и 87, нетрудно получить требуемое. ▲

Предложение 103. *Пусть полностью разделимые n-арные квазигруппы f и g совместимы и для любого $a \in Q_4$ пары ретрактов $f|_{x_1=a}$ и $g|_{x_1=a}$ дополняемы только до неразделимых n-арных квазигрупп. Тогда при выполнении ИП пара n-арных квазигрупп f и g дополняема.*

Доказательство. По лемме 1 о линейном антислое и предложению 79 пары ретрактов $f|_{x_1=a}$ и $g|_{x_1=a}$ являются полулинейными противоположными при любом $a \in Q_4$, причём по крайней мере один из каждой пары ретрактов $f|_{x_1=a}$ и $g|_{x_1=a}$ нелинеен, иначе по предложению 94 пара ретрактов $f|_{x_1=a}$ и $g|_{x_1=a}$ дополнялась бы и до разделимой n-арной квазигруппы.

Нетрудно видеть, что если некоторый ретракт $f|_{x_1=b}$ полностью разделимой n-арной квазигруппы f является линейным, то для любого $a \in Q_4$ ретракт $f|_{x_1=a}$ линейный. Таким образом, без ограничения общности можно полагать, что ретракты $f|_{x_1=a}$, $a \in Q_4$, полулинейны, но нелинейны.

Рассмотрим характеристики линейных 2-МДР-кодов, содержащих ретракты $\mathcal{M}\langle f|_{x_1=a}\rangle$, $a \in Q_4$. Пары противоположных ретрактов (см. лемму 1 о линейном антислое), содержатся в линейных 2-МДР-кодах с одинаковой характеристикой. Пары непротивоположных ретрактов имеют характеристики, совпадающие в некоторой позиции, иначе по предложению 80 один из них был бы линейным. Без ограничения общности можно полагать, что совпадают $(n+1)$-позиции характеристик, т. е. множества $\mathcal{S}_{0,1}\langle f|_{x_1=a}\rangle$ являются линейными. Тогда из нелинейности ретрактов $\mathcal{M}\langle f|_{x_1=a}\rangle$

следует, что множества $\mathcal{S}_{0,b}\langle f|_{x_1=a}\rangle$ при $b=2,3$ и любом $a \in Q_4$ нелинейные (см. предложение 51). Тогда из предложения 79 и условия дополняемости только до неразделимых n-арных квазигрупп следует, что $\mathcal{S}_{0,1}\langle f\rangle = Q_4^n \setminus \mathcal{S}_{0,1}\langle g\rangle$, и требуемое вытекает из предложения 83 (а). ▲

Лемма 11 ([51]). *Пусть полностью разделимые* МДР-*коды* $M_1, M_2 \subset Q_4^{n+1}$ *не пересекаются* ($n \geq 5$) *и* $I(M_1) \cap I(M_2) = \varnothing$. *Тогда из ИП вытекает, что* $Q_4^{n+1} \setminus (M_1 \cup M_2)$ — *двудольный* 2-МДР-*код.*

Доказательство. Если $I(M_1|_{x_i=a}) \cap I(M_2|_{x_i=a}) = \varnothing$ для некоторого $i \in [n+1]$ и всех $a \in Q_4$, то по предложению 101 ретракты $M_1|_{x_i=a}$ и $M_2|_{x_i=a}$ не могут быть ретрактами (по одной переменной) разделимого МДР-кода. Тогда требуемое следует из ИП и предложения 103. Предположим противное (*). Рассмотрим два случая:

1) $x_t \in \widetilde{I}(M_1) \cap \widetilde{I}(M_2)$;

2) $\widetilde{I}(M_1) \cap \widetilde{I}(M_2) = \varnothing$.

Рассмотрим случай 1). Пусть $M_i' = M_i|_{x_t=a}$ и $\{x_p, x_q\} \in I(M_1') \cap I(M_2')$. Если $\{x_p, x_q\} \in (I(M_1') \setminus I(M_1)) \cap (I(M_2') \setminus I(M_2))$, т. е. пара $\{x_p, x_q\}$ не является внутренней ни для M_1, ни для M_2, то по предложению 100 МДР-коды M_1, и M_2 определяются уравнениями вида $g_1(x_p, x_q, x_t) = f_1(\overline{y})$ и $g_2(x_p, x_q, x_t) = f_2(\overline{y})$ соответственно. Тогда требуемое следует из предложения 102.

Если $\{x_p, x_q\} \notin (I(M_1') \setminus I(M_1)) \cap (I(M_2') \setminus I(M_2))$, то $\{x_p, x_q\} \in I(M_1) \cap (I(M_2') \setminus I(M_2))$ (или наоборот). По предложению 100 имеем $\{x_t, x_q\} \in I(M_2)$ или $\{x_t, x_p\} \in I(M_2)$. Без ограничения общности полагаем, что $\{x_t, x_q\} \in I(M_2)$.

Если $x_p \in \widetilde{I}(M_2)$, то по предложению 99(а) имеем $I(M_2|_{x_p=c}) \subset I(M_2)$. В то же время из предложения 100 следует, что все пары из $I(M_1|_{x_p=c}) \setminus I(M_1)$ содержат переменную x_q. Здесь и далее элемент $c \in Q_4$ произвольный. По предположению (*) ретракты $M_2|_{x_p=b}$ и $M_1|_{x_p=b}$ при некотором $b \in Q_4$ имеют общую пару внутренних переменных и из сказанного выше следует, что этой парой может быть только $\{x_t, x_q\}$ (см. рис. 1.8). Следовательно, по предложению 100 МДР-коды M_1, и M_2 определяются уравнениями вида $g_1(x_p, x_q, x_t) = f_1(\overline{y})$ и $g_2(x_p, x_q, x_t) = f_2(\overline{y})$ соответственно.

Тогда требуемое следует из предложения 102.

Если $x_p \notin \widetilde{I}(M_2)$, то $I(M_2|_{x_q=c}) \setminus I(M_2) = \{\{x_p, x_t\}\}$ из предложения 100. Тогда аналогично разобранному выше заключаем, что общей внутренней парой ретрактов $M_2|_{x_q=c}$ и $M_1|_{x_q=c}$ может быть только пара $\{x_p, x_t\}$ и требуемое следует из предложений 100 и 102.

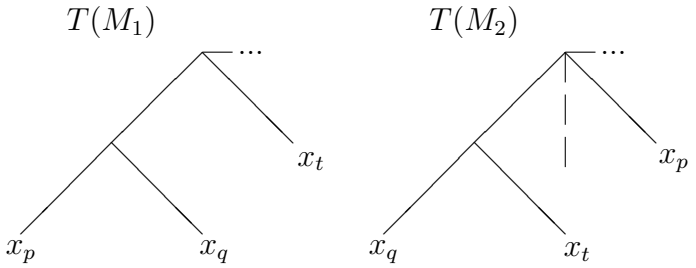


Рис. 1.8

Рассмотрим случай 2). В множестве $S = \widetilde{I}(M_1)$ выберем крайнюю переменную x_s относительно дерева $T(M_2)$. Пусть $M_i'' = M_i|_{x_s=b}$, $b \in Q_4$ и $\{x_p, x_q\} \in I(M_1'') \cap I(M_2'')$. Поскольку x_s — крайняя переменная в S, из предложения 99(c) следует, что $\{x_p, x_q\} \notin I(M_1)$. По предложению 100 имеем $\{x_p, x_s\} \in I(M_1)$ (или $\{x_q, x_s\} \in I(M_1)$). Заметим, что $x_q \notin \widetilde{I}(M_1)$, поскольку иначе $x_p, x_q \in S$, что противоречит крайнему положению переменной x_s. Рассмотрим ретракты $M_i''' = M_i|_{x_p=c}$. Из предложения 100 получаем, что единственной парой в $I(M_1''')$, содержащей переменную x_s, является пара $\{x_q, x_s\}$ (см. рис. 1.9). Из предложения 99(b) следует, что $\{x_q, x_s\} \notin I(M_2''') \setminus I(M_2)$, но переменная $x_s \notin \widetilde{I}(M_2)$ содержится в любой паре из $I(M_2''') \setminus I(M_2)$. Поэтому $I(M_2''') \cap I(M_1''') = \varnothing$. Поскольку $c \in Q_4$ произвольно, пришли к противоречию с предположением (*). ▲

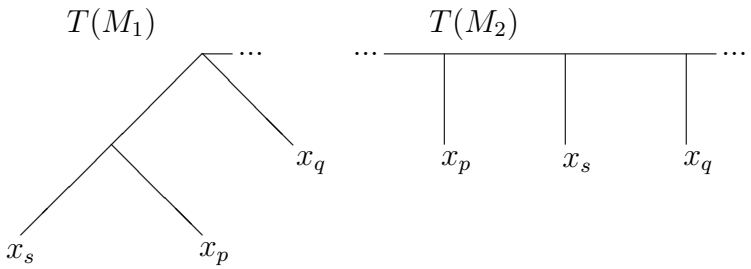


Рис. 1.9

Доказательство теоремы 19. Доказательство будем проводить по индукции. Для $n = 1, 2, 3$ утверждение теоремы легко проверить простым перебором (см. [143]), при $n = 4$ утверждение теоремы проверено с помощью компьютера. Пусть утверждение теоремы верно для любого натурального m, $m < n$ и $n \geq 5$.

1) Пусть хотя бы одна из совместимых n-арных квазигрупп f и g имеет неразделимый ретракт арности, большей или равной 3.

1a) Если n-арные квазигруппы f и g неразделимы, то для вывода требуемого утверждения достаточно применить предложение 88.

Если n-арная квазигруппа f имеет неразделимый ретракт арности m, $n > m > 2$, то по следствию 4 МДР-код $\mathcal{M}(f)$ задаётся каноническим уравнением

$$q_{m+1}(x_{n+1}, \tilde{x}_{m+1}) = q_0(q_1(\tilde{x}_1), ..., q_m(\tilde{x}_m))$$

с разбиением переменных $\{I_j\}_{j=1,...,m+1}$.

Пусть МДР-код $\mathcal{M}\langle g\rangle$ определяется каноническим уравнением

$$q'_{m'+1}(x_{n+1}, \tilde{x}'_{m'+1}) = q'_0(q'_1(\tilde{x}'_1), ..., q'_{m'}(\tilde{x}'_{m'}))$$

с разбиением переменных $\{I'_j\}_{j=1,...,m'+1}$, где $n > m' > 2$.

1b) Если разбиения $\{I_j\}_{j=1,...,m+1}$ и $\{I'_j\}_{j=1,...,m'+1}$ множества $[n]$ не совпадают, то применяем предложение 91.

1c) Если разбиения $\{I_j\}_{j=1,...,m+1}$ и $\{I'_j\}_{j=1,...,m'+1}$ множества $[n]$ совпадают, то применяем предложение 93.

1d) Если n-арная квазигруппа g полностью разделима, то применяем предложение 92.

2) Пусть МДР-коды $\mathcal{M}\langle f\rangle$ и $\mathcal{M}\langle g\rangle$ полностью разделимы. Если $I(\mathcal{M}\langle f\rangle) \cap I(\mathcal{M}\langle g\rangle) = \varnothing$, то требуемое следует из леммы 11. В противном случае требуемое вытекает из предложения 94. Все возможные случаи рассмотрены. ▲

§ 1.7. Бесконечномерные квазигруппы конечных порядков

§ 1.7.1. Бесконечномерные квазигруппы и неизмеримые множества

Пусть $\mathbb{A}$ — некоторое конечное или бесконечное множество, элементами которого нумеруются аргументы функций, действующих из $Q_k^{\mathbb{A}}$ в Q_k. Определим функцию $d : Q_k^{\mathbb{A}} \times Q_k^{\mathbb{A}} \to [0, \infty]$ так, что $d(\overline{y}, \overline{z})$ — число различающихся координат в $\overline{y}, \overline{z} \in Q_k^{\mathbb{A}}$. Функция $f : Q_k^{\mathbb{A}} \to Q_k$ называется $\mathbb{A}$-*квазигруппой* (мультиарной квазигруппой), когда $f(\overline{y}) \neq f(\overline{z})$ при $d(\overline{y}, \overline{z}) = 1$.

Случай конечного множества $\mathbb{A}$ был рассмотрен выше. В этом разделе рассматривается случай мультиарных квазигрупп от бесконечного числа аргументов. Пусть $\mathbb{N}$ — множество натуральных чисел. Элементы множества $Q_k^{\mathbb{N}}$ можно рассматривать как k-ичные представления вещественных чисел $\delta \in [0, 1]$. Отождествим вещественные числа и их k-ичные представления[6].

Предложение 104. *Для любой мультиарной квазигруппы $f : Q_k^{\mathbb{N}} \to Q_k$ конечного порядка k и элемента $a \in Q_k$ множество $\{\delta \in [0, 1] \mid f(\delta) = a\}$ неизмеримо по Лебегу.*

Доказательство. Предположим, что множество $B = \{\delta \in [0, 1] \mid f(\delta) = a\}$ измеримо. Пусть $\tau \in [0, 1]$ — некоторое k-ично рациональное число, в k-ичной записи которого не более начальных m символов отличны от нуля. Рассмотрим полуинтервал $[\tau, \tau + 1/k^{m+1})$. Из определения мультиарной квазигруппы следует, что $(B \cap [\tau, \tau + 1/k^{m+1}) + i/k^{m+1}) \cap B = \varnothing$ для любого $i = 1, \ldots, k-1$. Тогда, используя инвариантность меры Лебега относительно сдвига множества, получаем неравенство $\mu(B \cap [\tau, \tau + 2/k^{m+1})) \leq \mu([\tau, \tau + 2/k^{m+1}))/2$. Поскольку в сколь угодно малой окрестности любой точки $\upsilon \in (0, 1)$ найдутся k-ично рациональные точки, имеем

$$\varlimsup_{\varepsilon \to 0} \frac{\mu((\upsilon - \varepsilon, \upsilon + \varepsilon) \cap B)}{\mu((\upsilon - \varepsilon, \upsilon + \varepsilon))} \leq \frac{1}{2}.$$

[6] Для дальнейшего изложения не существенно нарушение взаимной однозначности на счётном множестве.

По теореме Лебега о плотности для произвольного измеримого множества A этот предел равен 1 для почти всех точек $\upsilon \in A$. Тогда $\mu(B) = 0$. Кроме того, из определения мультиарной квазигруппы имеем $[0,1] \subset \bigcup\limits_{i=1-k}^{1+k} (B + i/k)$. Тогда $\mu([0,1]) = 0$. Пришли к противоречию. ▲

Определим $\operatorname{supp} \overline{y} = \{i \in \mathbb{A} \mid y_i \neq 0\}$. Обозначим через $\mathcal{I}$ совокупность конечных подмножеств множества $\mathbb{A}$. Пусть множество $\mathbb{A}$ бесконечно. Рассмотрим
$\mathcal{F} = \{\overline{y} \in Q_k^{\mathbb{A}} \mid \operatorname{supp} \overline{y} \in \mathcal{I}\}$. Ясно, что множество $Q_k^{\mathbb{A}}$ представимо в виде дизъюнктного объединения подмножеств вида $\mathcal{F}_{\overline{a}} = \overline{a} + \mathcal{F}$. Причём если $\mathcal{F}_{\overline{a}} \neq \mathcal{F}_{\overline{b}}$, то $d(\overline{y}, \overline{z}) = \infty$ для любых $\overline{y} \in \mathcal{F}_{\overline{a}}$ и $\overline{z} \in \mathcal{F}_{\overline{b}}$. Поэтому мультиарная квазигруппа f может быть независимо определена на каждом $\mathcal{F}_{\overline{a}}$. В дальнейшем будем подразумевать, что $f : \mathcal{F} \to Q_k$. Как будет показано ниже, мультиарные квазигруппы на $\mathcal{F}$ допускают конструктивное определение, в то время как для определения мультиарных квазигрупп на $Q_k^{\mathbb{A}}$ необходимо выбирать по представителю из каждого класса $\mathcal{F}_{\overline{a}}$.

Символом x всюду будем обозначать набор аргументов (переменных) мультиарной квазигруппы, через x_L будем обозначать выборку аргументов с индексами из множества L, $L \subseteq \mathbb{A}$. Понятия ретракта, изотопии, разделимой, полулинейной и приведённой мультиарной квазигруппы переносятся на случай бесконечного числа аргументов с учётом того, что количество ненулевых аргументов должно оставаться конечным при всех рассматриваемых преобразованиях. В частности, ретрактом бесконечномерной квазигруппы f называется подфункция, полученная из f подстановкой констант в некоторые аргументы, причём только конечное число констант может быть отлично от нуля. Через f_L будем обозначать ретракт мультиарной квазигруппы $f : \mathcal{F} \to Q_k$, в котором фиксированы нулём все аргументы, кроме имеющих индексы из множества L. Через $f(y_{\{i\}}, x_L)$ будем обозначать мультиарную квазигруппу, полученную подстановкой функции, переменной или константы y на место аргумента x_i, $i \notin L$. Символами I и J будем обозначать только конечные подмножества в $\mathbb{A}$. Ясно, что ретракт f_J можно рассматривать как $|J|$-арную квазигруппу.

Обозначим через S_0 группу перестановок на Q_k, сохраняюших нуль. В этом разделе будем рассматривать только изотопии, сохраняющие нуль, т. е. элементы множества $S_0 \times S_0^{\mathbb{A}}$. Напомним, что мультиарная квазигруппа f называется приведённой

или мультиарной лупой, если при подстановке любого $a \in Q_k$ в любой аргумент x_i, $i \in \mathbb{A}$, и нулей в остальные аргументы получаем a, т. е. справедливо равенство $f(a_{\{i\}}, \overline{0}_{\mathbb{A}\setminus\{i\}}) = a$.

Целью данного раздела является классификация мультиарных квазигрупп порядка 4; как и для n-арных квазигрупп будет доказано, что все бесконечномерные квазигруппы порядка 4 полулинейны или разделимы. Полулинейные квазигруппы допускают описание посредством булевых функций. Разделимые мультиарные квазигруппы могут быть представлены через собственные ретракты. Однако, в отличие от аналогичного описания квазигрупп конечной размерности (см. теорему 7), этот результат не обеспечивает конструктивной классификации бесконечномерных мультиарных квазигрупп, ибо дерево разложения мультиарной квазигруппы в суперпозиции может оказаться бесконечным.

§ 1.7.2. Разделимость

Напомним, что мультиарная квазигруппа f называется разделимой, если она может быть представлена в виде суперпозиции, т. е. $f(x_{L_1}, x_{L_2}) = g(h(x_{L_1})_{\{j\}}, x_{L_2})$, где h и g — L_1 и $(\{j\} \cap L_2)$- квазигруппы, $L_1 \cap L_2 = \varnothing$, $|L_1| \geq 2$, $|L_2| \geq 1$, $j \notin L_2$[7].

Из предложения 44 следует, что любая мультиарная квазигруппа изотопна приведённой квазигруппе и приведённая разделимая мультиарная квазигруппа может быть представлена как суперпозиция приведённых мультиарных квазигрупп. В качестве основного признака разделимости мультиарных квазигрупп в этом разделе используется следующее утверждение, обобщающее предложение 39 на бесконечномерный случай.

Предложение 105. *Мультиарная квазигруппа f представляется в виде суперпозиции*
$f(x_{L_1}, x_{L_2}) = g(h(x_{L_1})_{\{j\}}, x_{L_2})$ *тогда и только тогда, когда для любых наборов аргументов $y_{L_2}, y_{L_1}, y'_{L_1}$ из равенства $f(y_{L_1}, \overline{0}_{L_2}) = f(y'_{L_1}, \overline{0}_{L_2})$ следует равенство $f(y_{L_1}, y_{L_2}) = f(y'_{L_1}, y_{L_2})$.*

[7] Для определённости будем полагать, что $j \in L_1$.

Доказательство. Без ограничения общности считаем мультиарную квазигруппу f приведённой и $1 = j \in L_1$. Необходимость очевидна, докажем достаточность. Определим $h = f_{L_1}$ и $g = f_{\{1\} \cup L_2}$.

Пусть $f(y_{L_1}, \overline{0}_{L_2}) = h(y_{L_1}) = a = f(a_{\{1\}}, \overline{0}_{L_1 \setminus \{1\}}, \overline{0}_{L_2})$ для некоторого $a \in Q_k$. Тогда

$$f(y_{L_1}, y_{L_2}) = f(a_{\{1\}}, \overline{0}_{L_1 \setminus \{1\}}, y_{L_2}) = g(a_{\{1\}}, y_{L_2}) = g(h(y_{L_1})_{\{1\}}, y_{L_2}).$$

▲

Зафиксируем некоторую мультиарную квазигруппу $f : \mathcal{F} \to Q_k$. Будем говорить, что множество $M \subseteq \mathbb{A}$ *неразделимое* (относительно f), если $|M| \geq 3$ и для любого конечного набора $J \subseteq M$ найдётся такой конечный набор J', $J \subseteq J' \subseteq M$, что мультиарная квазигруппа $f_{J'}$ неразделимая.

Система множеств, в которой для каждой пары множеств L_1, L_2 имеется такое множество L, что $L_1 \cup L_2 \subset L$ называется *направлением*. Будем говорить, что направление $S \subseteq \mathcal{I}$ сходится к множеству $M \subseteq \mathbb{A}$, если для каждого конечного подмножества в M найдётся включающий его элемент направления S. По определению неразделимого множества M найдётся сходящееся к M направление S, состоящее из неразделимых конечных наборов.

Предложение 106. *Если направление $S \subseteq \mathcal{I}$ сходится к множеству $M \subseteq \mathbb{A}$ и $S = \bigcup_{i=1}^{m} S_i$, то найдётся такое $i \in \{1, \ldots, m\}$, что множество S_i есть направление, сходящееся к M.*

Доказательство. Пусть S_i не есть направление, сходящееся к M. Тогда имеется $J_i \in \mathcal{I}$, которое не мажорируется элементами S_i. Рассмотрим $J = \bigcup_{i=1}^{m} J_i$. Найдётся такое $I \in S$, что $J \subseteq I$. По условию $I \in S_i$ для некоторого $i \in \{1, \ldots, m\}$. Пришли к противоречию. ▲

Предложение 107. *Если множество M неразделимое, то мультиарная квазигруппа f_M неразделимая.*

Доказательство. Предположим противное, т. е. имеется представление мультиарной квазигруппы f_M в виде суперпозиции

$$f_M(x_{L_1}, x_{L_2}) = g(h(x_{L_1})_{\{i_0\}}, x_{L_2}), \tag{1.29}$$

где $M = L_1 \cup L_2$, $|L_1| \geq 2, |L_2| \geq 1$. Пусть $i_0, i_1 \in L_1$, $i_2 \in L_2$. По определению неразделимого множества найдётся такой конечный набор J, $\{i_0, i_1, i_2\} \subset J \subseteq M$, что мультиарная квазигруппа f_J неразделимая. Однако, это противоречит равенству (1.29). ▲

Обращение этого утверждения, разбитое на два подслучая (Леммы 12 и 13) является основным результатом этого и следующего подразделов: если мультиарная квазигруппа $f_{\mathbb{A}}$ неразделима, то множество $\mathbb{A}$ является неразделимым.

Обозначим через $\mathcal{N}(f)$ совокупность неразделимых подмножеств множества $\mathbb{A}$. Отметим, что если $\mathcal{N}(f) \neq \varnothing$, то множество $\mathcal{N}(f)$ содержит конечные элементы.

Предложение 108. *Пусть $\mathcal{N}(f) \neq \varnothing$. Для любого неразделимого L найдётся максимальный элемент M в $\mathcal{N}(f)$, содержащий L.*

Доказательство. Рассмотрим произвольную конечную или бесконечную цепь (по включению) неразделимых множеств $\{L_\beta\}$. Покажем, что множество $K = \cup L_\beta$ неразделимо. Пусть $I \subset K$ — некоторый конечный набор. Тогда найдётся такое β, что $I \subset L_\beta$ и, следовательно, имеется конечный неразделимый набор J', $I \subseteq J' \subseteq L_\beta \subseteq K$. Требуемое следует из леммы Цорна. ▲

Предполагая, что множество $\mathcal{N}(f)$ непусто, зафиксируем некоторый максимальный по включению элемент M_f в $\mathcal{N}(f)$.

Сформулируем в новых обозначениях следствие 4 теоремы 3 о каноническом представлении разделимых n-арных квазигрупп.

Следствие 9. *Если разделимая n-арная квазигруппа f имеет неразделимый ретракт размерности $m > 2$, который не содержится в неразделимых ретрактах большей размерности, то*

$$\{x \mid x_0 = f_J(x_J)\} = \{x \mid q_0(x_{J_0}) = F(q_1(x_{J_1}), ..., q_m(x_{J_m}))\}, \tag{1.30}$$

где q_j суть n_j-арные квазигруппы при $j \in \{0, \ldots, m\}$, F есть неразделимая m-арная квазигруппа, $\{J_i\}$ — разбиение множества $J \cup \{0\}$ на наборы мощности $n_0, \ldots, n_m$[8].

[8] Здесь и далее подразумеваем, что x_0 не является аргументом мультиарной квазигруппы f.

Предложение 109. *Пусть $J \in \mathcal{N}(f)$, $J' \in \mathcal{I}$ и $J \subset J'$. Тогда имеется представление*

$$\{x \mid x_0 = f_{J'}(x_{J'})\} = \{x \mid q_0(x_{J_0}) = F(q_1(x_{J_1}), ..., q_m(x_{J_m}))\}, \tag{1.31}$$

где q_i суть n_i-арные квазигруппы при $i \in \{0, \ldots, m\}$, F есть неразделимая m-арная квазигруппа, $\{J_i\}$ — разбиение множества $J' \cup \{0\} \in \mathcal{I}$ на наборы мощности $n_0, \ldots, n_m$. Причём $|(J \cup \{0\}) \cap J_i| \leq 1$ для любого i, $i \in \{0, \ldots, m\}$.

Доказательство. Если J есть максимальное неразделимое подмножество в J', то требуемое получаем из следствия 9. В противном случае нужно применить следствие 9 к максимальному неразделимому множеству J'', $J \subset J'' \subseteq J'$. ▲

Заметим, что $m \geq |J|$ в формуле (1.31), но не утверждается, что неравенство $m \geq |J|$ верно для всех представлений множества $\{x \mid x_0 = f_{J'}(x_{J'})\}$. Будем писать $[i, j]_{f, J' \supset J}$, если в представлении (1.31) для $f_{J'}$ имеем $i, j \in J_l$ для некоторого l, $0 \leq l \leq m$.

Предложение 110. *Для любого $i \notin M_f$ найдётся набор $J(i) \in \mathcal{I}$, $J(i) \subseteq M_f$ и единственное $\alpha(i) \in M_f \cup \{0\}$ такие, что для любого $J \in \mathcal{I}$, $i \in J$, $J(i) \subset J \subseteq M_f \cup \{0, i\}$ имеем $[i, \alpha(i)]_{f, J \supset J(i)}$.*

Доказательство. Поскольку $i \notin M_f$, то для конечных наборов $J' \subset M_f$ больших некоторого $J(i) \subseteq M_f$ мультиарная квазигруппа $f_{J' \cup \{i\}}$ разделима. Очевидно, что набор индексов $J(i)$ можно выбрать неразделимым. Для определённости выбора будем считать множество индексов упорядоченным, а набор $J(i)$ лексикографически минимальным из возможных. По предложению 109 имеется представление (1.31). Если номер $\alpha(i)$ принимает различные значения $i_1, i_2 \in J(i)$ для различных конечных наборов $J', J'' \subseteq M_f$, то, подставляя нуль во все аргументы кроме аргументов с индексами из $\{0, i\} \cup J(i)$ в представлениях вида (1.31) для мультиарных квазигрупп $f_{J'}$ и $f_{J''}$ приходим в противоречие с единственностью представления мультиарной квазигруппы, обеспеченной теоремой 3. ▲

Предложение 111. *Для любых наборов $J', J'' \in \mathcal{I}$, $i \in J''$, $J' \subset M_f$, $J(i) \subset J' \subset J''$ имеем $[i, \alpha(i)]_{f, J'' \supset J'}$.*

Доказательство. Из предложения 110 имеем $[i, \alpha(i)]_{f, J' \cup \{i\} \supset J(i)}$. Рассмот-

рим представление (1.31) для мультиарной квазигруппы $f_{J''}$. Для того, чтобы убедиться в выполнении $[i,\alpha(i)]_{f,J''\supset J'}$ достаточно подставить нуль во все аргументы кроме аргументов с индексами из $J'\cup\{0,i\}$ и применить следствие 9. ▲

Следствие 10. *Для любого конечного набора $J\subset\mathbb{A}\setminus M_f$ найдётся такой набор $J'\in\mathcal{I}$, $J'\subset M_f$, что для любого набора $J''\in\mathcal{I}$, $J'\cup J\subset J''$ и любого $i\in J$ имеем $[i,\alpha(i)]_{f,J''\supset J'}$.*

Доказательство. Рассмотрим конечный набор $J'\subset M_f$ такой, что $f_{J'}$ — неразделимая мультиарная квазигруппа и $J(i)\subset J'$ для любого $i\in J$. Требуемое следует из предложения 111. ▲

Лемма 12 ([56]). *Если множество $\mathbb{A}$ разделимо и $\mathcal{N}_f\neq\varnothing$, то мультиарная квазигруппа $f:\mathcal{F}\to Q_k$ разделима.*

Доказательство. Рассмотрим некоторое множество M_f, по условию $M_f\neq\mathbb{A}$. Для любого $m\in M_f$ определим множество индексов $A_m=\{i\notin M_f\mid\alpha(i)=m\}\cup\{m\}$. Без ограничения общности можно считать, что $1\in M_f$ и $|A_1|\geq 2$. Пусть $B=\mathbb{A}\setminus A_1$. Покажем, что для любых наборов аргументов y_B, y_{A_1}, y'_{A_1} из равенства $f(y_{A_1},\overline{0}_B)=f(y'_{A_1},\overline{0}_B)$ следует равенство $f(y_{A_1},y_B)=f(y'_{A_1},y_B)$. Рассмотрим произвольные $y,y'\in\mathcal{F}$ и конечный набор $J=\operatorname{supp}y_B\cup\operatorname{supp}y_{A_1}\cup\operatorname{supp}y'_{A_1}$. По следствию 10 найдётся такой набор $J'\subseteq M_f$, $J\cap M_f\subset J'$, что для любого конечного набора J'', $J'\cup J\subset J''$ и любого $i\in J\setminus M_f$ имеем $[i,\alpha(i)]_{f,J''\supset J'}$. Тогда $f_{J''}(x_{A_1\cap J''},x_{B\cap J''})=g(h(x_{A_1\cap J''})_{\{1\}},x_{B\cap J''})$.

Пусть $f(y_{A_1},\overline{0}_B)=f(y'_{A_1},\overline{0}_B)$. Тогда $h(y_{A_1\cap J''})=h(y'_{A_1\cap J''})$ и

$$f(y_{A_1},y_B)=f_{J''}(y_{A_1\cap J''},y_{B\cap J''})=f_{J''}(y'_{A_1\cap J''},y_{B\cap J''})=f(y'_{A_1},y_B).$$

Из предложения 105 получаем требуемое. ▲

Методы, подобные использованным выше, применялись в [147] для исследования свойств разделимых n-арных квазигрупп.

§ 1.7.3. Полная разделимость

Все 2-квазигруппы в соответствии с определением являются неразделимыми. Разделимая n-арная квазигруппа f называется *полностью коммутативно разделимой*, если все её ретракты размерности большей 2-х разделимы и все ретракты размерности 2 изотопны коммутативным группам.

Далее в этом параграфе речь пойдёт только об мультиарных квазигруппах порядка 4. Как было сказано выше, все 2-квазигруппы порядка 4 изотопны либо группе $Z_2 \times Z_2$, либо группе Z_4. Поэтому разделимые n-арные квазигруппы порядка 4, не содержащие неразделимых ретрактов размерности большей 2-х, являются полностью коммутативно разделимыми. Следующее утверждение является прямым следствием теоремы 3 о каноническом представлении разделимых n-арных квазигрупп.

Следствие 11. *Полностью коммутативно разделимую n-арную квазигруппу $f : Q_4^n \to Q_4$ можно представить в виде*

$$f(x_{J_1}, \ldots, x_{J_k}) = q_1(x_{J_1}) * \ldots * q_k(x_{J_k}), \tag{1.32}$$

где $*$ есть коммутативная групповая операция, q_j суть n_j-арные квазигруппы при $j \in [k]$, не представимые в виде $q_j(x_{J'_j}, x_{J''_j}) = q'(x_{J'_j}) * q''(x_{J''_j})$. Причём в данном представлении конечные наборы $\{J_j\}$ и операция $*$ определяются единственным (при фиксированном нейтральном элементе группы) образом.

Полностью коммутативно разделимой n-арной квазигруппе f, имеющей представление (1.32), как и в общем случае (см. § 1.2) поставим в соответствие корневое дерево $T(f)$, внутренние вершины которого помечены операциями, а листья аргументами функции.

Пусть мультиарная квазигруппа $f : \mathcal{F} \to Q_4$ такова, что множество $\mathcal{N}(f)$ пусто. Будем обозначать $T(f_J)$ через T_J, где $J \in \mathcal{I}$. Рассмотрим в T_J минимальное поддерево, содержащее пару аргументов с индексами $i_1, i_2 \in J$ и обозначим через $C(J, i_1, i_2) \in \mathcal{I}$ множество индексов, соответствующих висячим вершинам этого поддерева. Корректность определения дерева $T(f)$ и множества $C(J, i_1, i_2)$ получается из следствия 11. Множество $C(J, i_1, i_2) \in \mathcal{I}$ можно эквивалентно определить через

существование следующего представления

$$f_J(x_J) = g((h_1(x_{C_1}) * h_2(x_{C_2}))_{\{i_1\}}, x_{J\setminus(C_1\cup C_2)}),$$

где $C_1 \cup C_2 = C(J, i_1, i_2)$, $i_1 \in C_1$, $i_2 \in C_2$, и мультиарная квазигруппа $(h_1(x_{C_1}) * h_2(x_{C_2}))$ соответствует минимальному поддереву, содержащему пару аргументов с индексами $i_1, i_2 \in J$.

Предложение 112. *Пусть $J \subset J' \in \mathcal{I}$, $i_1, i_2 \in J$. Тогда справедливо равенство $C(J, i_1, i_2) = C(J', i_1, i_2) \cap J$.*

Доказательство. Имеем $f_{J'}(x_{J'}) = g((h_1(x_{C_1}) * h_2(x_{C_2}))_{\{i_1\}}, x_{J'\setminus(C_1\cup C_2)})$, где $C_1 \cup C_2 = C(J', i_1, i_2)$, $i_1 \in C_1$, $i_2 \in C_2$. Подставляя нуль во все аргументы из $J' \setminus J$, получаем требуемое представление для мультиарной квазигруппы f_J. ▲

Лемма 13 ([56]). *Пусть мультиарная квазигруппа $f : \mathcal{F} \to Q_4$ такова, что $\mathcal{N}(f) = \varnothing$. Тогда f разделима.*

Доказательство. Без ограничения общности будем считать, что f приведённая. Если мультиарная квазигруппа f линейна (изотопна итерированной группе $Z_2 \times Z_2$) или f изотопна итерированной группе Z_4, то f разделима. Иначе найдётся набор $J = \{i_1, i_2, i_3\}$, что $f_J(x_J) = (x_{i_1} *_1 x_{i_2}) *_2 x_{i_3}$, где $*_1$ и $*_2$ — различные групповые операции. Рассмотрим множество $C = \cup C(J, i_1, i_2)$, где объединение берётся по всем конечным наборам J, содержащим i_1, i_2. Из предложения 112 получаем, что $i_3 \notin C$. Кроме того, для любого конечного набора $J \in \mathcal{I}$, $i_1, i_2 \in J$ имеем $C(J, i_1, i_2) = C \cap J$. Действительно, если $j \in (C \cap J) \setminus C(J, i_1, i_2)$, то $j \in C(J', i_1, i_2)$ для некоторого конечного набора J'. Тогда из предложения 112 имеем $j \in C(J' \cup J, i_1, i_2)$ и, следовательно, $j \in C(J, i_1, i_2)$.

Докажем, что $f(x_{\mathbb{A}}) = g(h(x_C)_{\{i_1\}}, x_{\mathbb{A}\setminus C})$. По предложению 105 достаточно доказать, что для любых аргументов $y_{\mathbb{A}\setminus C}$, y_C, y'_C из равенства $f(y_C, \overline{0}_{\mathbb{A}\setminus C}) = f(y'_C, \overline{0}_{\mathbb{A}\setminus C})$ следует равенство $f(y_C, y_{\mathbb{A}\setminus C}) = f(y'_C, y_{\mathbb{A}\setminus C})$. Рассмотрим произвольные $y, y' \in \mathcal{F}$, обозначим $J = \operatorname{supp} y \cup \operatorname{supp} y' \cup \{i_1, i_2, i_3\}$. Тогда

$$f(y) = f_J(y_J) = g(h(y_{J\cap C})_{\{i_1\}}, y_{J\setminus C}).$$

Из равенства $f(y_C, \overline{0}_{\mathbb{A}\setminus C}) = f(y'_C, \overline{0}_{\mathbb{A}\setminus C})$ имеем $h(y_{J\cap C}) = h(y'_{J\cap C}) = a$ для некоторого

$a \in Q_4$. Тогда

$$f(y_C, y_{\mathbb{A}\setminus C}) = f_J(y_C, y_{\mathbb{A}\setminus C}) = g(a_{\{i_1\}}, y_{\mathbb{A}\setminus C}) =$$

$$g(h(y'_{J\cap C})_{\{i_1\}}, y_{\mathbb{A}\setminus C}) = f_J(y'_C, y_{\mathbb{A}\setminus C}) = f(y'_C, y_{\mathbb{A}\setminus C}).$$

▲

§ 1.7.4. Полулинейность

Напомним, что мультиарная квазигруппа $f : \mathcal{F} \to Q_4$ порядка 4 называется полулинейной, если она удовлетворяет равенству $f(\{0,1\}^{\mathbb{A}} \cap \mathcal{F}) = \{0,1\}$ или f изотопна квазигруппе, удовлетворяющей этому равенству.

Полулинейные мультиарные квазигруппы разделяются на три класса R_1, R_2, R_3, так что в R_a содержатся квазигруппы главно изотопные a-полулинейным квазигруппам, т. е. мультиарным квазигруппам, удовлетворяющим равенству $f(\{0,a\}^{\mathbb{A}} \cap \mathcal{F}) = \{0,a\}$.

Из предложения 51(b) следует, что при $a \neq b$ множество $R_a \cap R_b$ совпадает с множеством линейных мультиарных квазигрупп.

В теореме 7 утверждается, что для любого конечного n каждая n-арная квазигруппа порядка 4 является разделимой или полулинейной. Для бесконечномерных квазигрупп, используя эту теорему, докажем следующую лемму.

Лемма 14 ([56]). *Пусть f — мультиарная квазигруппа порядка 4 и $M \in \mathcal{N}(f)$. Тогда мультиарная квазигруппа f_M полулинейна.*

Доказательство. Без ограничения общности считаем, что f приведённая. Если M конечное, то требуемое следует из теоремы 7. Далее полагаем, что множество M бесконечное. Поскольку $M \in \mathcal{N}(f)$, найдётся направление $S \subseteq \mathcal{I}$, которое сходится к M. Пусть $B_a = \{J \in \mathcal{I} \mid J \in S, f_J \in R_a\}$. Из предложения 106 следует, что как минимум одно из множеств B_a, $a \in \{1,2,3\}$ образует сходящееся к M направление. Из предложения 50(b) следует, что если $J \in B_a$ $J' \subset J$, то $J' \in B_a$. Следовательно, B_a состоит из всех конечных подмножеств в M.

Если найдутся такие $a \neq b$, что направления B_a и B_b сходятся к M, то все мультиарные квазигруппы f_J, $J \in S$, являются линейными по предложению 51. Тогда

квазигруппа f_M линейна. Если только одно из направлений B_a, $a \in \{1,2,3\}$ сходится к M, то определим $c_0 = a$.

Аналогичным образом определим c_i для каждого $i \in M$. А именно, рассмотрим мультиарную квазигруппу $f_M^{(i)}$, которая является обращением квазигруппы f по i-му аргументу, т. е. $\{(x,y) \mid x_i = f_M^{(i)}(x_{M\setminus\{i\}}y_{\{i\}})\} = \{(x,y) \mid y = f_M(x_M)\}$. Затем найдём элемент $c_0 \in \{1,2,3\}$ для квазигруппы $f_M^{(i)}$ и обозначим его через c_i.

Пусть $\theta_i = (1, c_i)$. Рассмотрим мультиарную квазигруппу $g_M(x_M) = \theta_0 f_M(\theta_M x_M)$. Нетрудно видеть, что $g_J(\{0,1\}^{|J|}) = \{0,1\}$ для любого $J \subseteq M$, $J \in \mathcal{I}$. Тогда мультиарные квазигруппы g_M и f_M полулинейные. ▲

Известно (см. предложение 60), что любая n-арная квазигруппа порядка 2 имеет вид

$$f(x_1, \ldots, x_n) = x_1 + \cdots + x_n + \sigma \mod 2,$$

где $\sigma \in \{0,1\}$, и любая n-арная квазигруппа порядка 3 изотопна n-арной квазигруппе

$$f(x_1, \ldots, x_n) = x_1 + \cdots + x_n \mod 3.$$

Отсюда методом подобным описанному выше нетрудно доказать следующее

Предложение 113. (a) *Пусть $f : \mathcal{F} \to \{0,1\}$ — мультиарная квазигруппа порядка 2. Тогда $f(x_{\mathbb{A}}) = p(x_{\mathbb{A}}) + \sigma$, где $\sigma \in \{0,1\}$ и $p(x_{\mathbb{A}}) = \sum\limits_{i\in\mathbb{A}} x_i \mod 2$.*

(b) *Пусть $f : \mathcal{F} \to \{0,1,2\}$ — мультиарная квазигруппа порядка 3. Тогда f изотопна квазигруппе g, где $g(x_{\mathbb{A}}) = \sum\limits_{i\in\mathbb{A}} x_i \mod 3$.*

Функция p называется *счётчиком чётности*. Пусть $J \in \mathcal{I}$, определим функцию $\chi : \mathcal{I} \to \{0,1\}^{\mathbb{A}}$ равенством $\chi(J) = \overline{\delta}$, где $\delta_i = 1$ тогда и только тогда, когда $i \in J$.

Предложение 114. *Пусть g — полулинейная мультиарная квазигруппа порядка 4. Тогда g изотопна некоторой мультиарной квазигруппе f, сужения которой $f^J = f|_{\{2,3\}^J \times \{0,1\}^{\mathbb{A}\setminus J}}$ имеют вид*

$$f^J(x) = 2p(\chi(J)) + (p(x \mod 2) + \sigma_J) \mod 2.$$

Доказательство. По определению полулинейности мультиарная квазигруппа g изотопна мультиарной квазигруппе f, удовлетворяющей равенству $f(\{0,1\}^{\mathbb{A}} \cap$

$\mathcal{F}) = \{0,1\}$. Тогда по определению мультиарной квазигруппы $f(\{2,3\}^J \times \{0,1\}^{\mathbb{A}\setminus J} \cap \mathcal{F}) = \{0,1\}$ при $p(\chi(J)) = 0$ и $f(\{2,3\}^J \times \{0,1\}^{\mathbb{A}\setminus J} \cap \mathcal{F}) = \{2,3\}$ при $p(\chi(J)) = 1$. Тогда требуемое следует из предложения 113 (a). ▲

Теорема 24 ([56]). *Пусть $f : \mathcal{F} \to Q_4$ — мультиарная квазигруппа порядка* 4.

(a) *Множество $\mathbb{A}$ неразделимое тогда и только тогда, когда мультиарная квазигруппа $f_{\mathbb{A}}$ неразделимая.*

(b) *Мультиарная квазигруппа f является разделимой или полулинейной.*

Доказательство.

(a) Если $\mathbb{A}$ конечное, то утверждение очевидно. Если $\mathbb{A}$ бесконечное, то утверждение следует из предложения 107 и лемм 12 и 13.

(b) Если $\mathbb{A}$ конечное, то применяем теорему 7. Если $\mathbb{A}$ бесконечное, то утверждение пункта (b) следует из пункта (a) и леммы 14.▲

§ 1.8. МДР-коды с расстоянием, большим чем 2

Пусть $M \subseteq Q_k^n$. Напомним,что кодовым расстоянием множества (кода) называется $d_M = \min\limits_{x,y\in M, x\neq y} d(x,y)$. Нетрудно видеть, что справедливы следующие утверждения.

Предложение 115. *Подмножество гиперкуба Q_k^n является* МДР-*кодом с расстоянием d ($d < n$) тогда и только тогда, когда все его ретракты, размерности не меньшей чем d, являются* МДР-*кодами с расстоянием d.*

Предложение 116 ([182], граница Синглтона). (a) *Для любого $M \subseteq Q_k^n$ верно неравенство $|M| \leq k^{n-d_M+1}$.*

(b) *Множество M является* МДР-*кодом с расстоянием d_M тогда и только тогда, когда $|M| = k^{n-d_M+1}$.*

Как было отмечено выше (предложение 24), МДР-коды с расстоянием 2 можно определить как графики мультиарных квазигрупп, т. е. каждый МДР-код с расстоянием 2 длины $n+1$ совпадает с множеством решений уравнения вида $x_{n+1} = f(x_1,\ldots,x_n)$, где f — некоторая n-арная квазигруппа. МДР-коды с большими расстояниями также можно представить как множества решений системы уравнений из

нескольких мультиарных квазигрупп. Действительно, рассмотрим МДР-код длины n с расстоянием d. По определению МДР-кода в каждой грани гиперкуба размерности $m = n - d + 1$ имеется ровно одна точка МДР-кода, т. е. например, первые m координат однозначно определяют оставшиеся $n - m$ координат. Значит, МДР-код является множеством решений системы уравнений

$$x_{m+1} = q_1(x_1, \ldots, x_m), \ldots, x_n = q_{n-m}(x_1, \ldots, x_m). \tag{1.33}$$

Из определения МДР-кода нетрудно видеть, что функции $q_1, \ldots, q_{n-m}$ являются m-арными квазигруппами.

Иногда МДР-код удобно представлять системой уравнений общего вида. Из определения МДР-кода следует

Предложение 117. *Пусть $f_1, \ldots, f_m$ — набор функций, действующих из Q_k^n в Q_k. Тогда множество решений системы уравнений $f_1(\overline{x}) = \cdots = f_m(\overline{x}) = 0$ является* МДР-*кодом тогда и только тогда, когда при любой фиксации любых $n - m$ переменных система имеет единственное решение.*

Перейдём к явному заданию МДР-кодов.

Система из n m-арных функций $f_1, \ldots, f_n$ $(n \geq m)$ называется *ортогональной*, если для любого поднабора $f_{i_1}, \ldots, f_{i_m}$ из m элементов этой системы имеем

$$\{(f_{i_1}(\overline{x}), \ldots, f_{i_n}(\overline{x})) \mid \overline{x} \in Q_k^m\} = Q_k^m.$$

Из определений следует

Предложение 118. *Система n-арных функций $f_1, \ldots, f_n$ ортогональна тогда и только тогда, когда множество $\{(f_1(\overline{x}), \ldots, f_n(\overline{x})) \mid \overline{x} \in Q_k^m\}$ является* МДР-*кодом с расстоянием $d_M = n - m + 1$.*

Если все наборы ретрактов (полученные одинаковой фиксацией переменных) системы ортогональных функций также являются ортогональными системами, то система называется *сильно ортогональной*. Из рассмотрения 1-мерных ретрактов следует, что система сильно ортогональных функций состоит из мультиарных квазигрупп. Из предложений 117 и 118 имеем

Предложение 119. *Подмножество $M \subset Q_k^n$ является* МДР-*кодом с расстоянием $d_M = m + 1$ тогда и только тогда, когда найдётся сильно ортогональная система из m квазигрупп $f_1, \ldots, f_m$ арности $(n - m)$, для которой верно равенство*

$$M = \{(x_1, \ldots, x_{n-m}, f_1(\overline{x}), \ldots, f_m(\overline{x})) \mid \overline{x} \in Q_k^{n-m}\}.$$

Функция $f : Q_k^n \to S$ называется *корреляционно-иммунной порядка* m, если для любого $a \in S$ её произвольный ретракт размерности $n - m$ принимает значение $a \in S$ одинаковое число раз. Другими словами мощность пересечения $f^{-1}\{a\} \cap G$ не зависит от $a \in S$ и выбора $(n - m)$-мерной грани G. Будем обозначать через $\mathrm{cor}(f)$ — максимальный порядок иммунности функции f. Если $S = \{0, 1\}$, то $f = \chi_M$ для некоторого множества $M \subset Q_k^n$. Тогда будем писать $\mathrm{cor}(M)$ вместо $\mathrm{cor}(\chi_M)$.

Замечание 10. *Если $M \subset Q_k^n$ —* МДР-*код с расстоянием d_M, то* $\mathrm{cor}(M) = n - d_M + 1$.

Множество единиц любой булевозначной функции χ_M можно рассматривать как кратный МДР-код с расстоянием $n - \mathrm{cor}(M) + 1$.

Ортогональным массивом $OA_\lambda(t, n, k)$ называется матрица размера $N \times n$, где $N = \lambda k^t$, составленная из элементов множества Q_k и удовлетворяющая следующему условию: если выделить из этой матрицы подматрицу, составленную из произвольных t столбцов, то для каждого $a \in Q_k^t$ среди строк подматрицы найдётся ровно λ наборов a. Число t называется *силой* ортогонального массива.

Для ортогональных массивов A, в которых каждая строка встречается однократно, обозначим через $\mathcal{C}(A)$ множество этих строк. Для таких ортогональных массивов из определений имеем

Предложение 120. *A — ортогональный массив $OA_\lambda(t, n, k)$ тогда и только тогда, когда $\mathcal{C}(A) \subset Q_k^n$, $t = \mathrm{cor}(\mathcal{C}(A))$, $|\mathcal{C}(A)| = \lambda k^t$.*

Следствие 12. *Если A — ортогональный массив $OA_\lambda(t, n, k)$, то $\mathcal{C}(A)$ — λ-кратный* МДР-*код с расстоянием $d = n - t + 1$.*

Как следует из сказанного выше, вопросы существования МДР-кодов, систем сильно ортогональных мультиарных квазигрупп и ортогональных массивов с $\lambda = 1$ эквивалентны друг другу при надлежащем выборе параметров. Нетрудно видеть, что

Предложение 121. (a) *Гиперкуб Q_k^n содержит* МДР-*коды с расстоянием* 2 *при любых натуральных n и k.*

(b) *Гиперкуб Q_k^n содержит* МДР-*коды с расстоянием n при любых натуральных n и k.*

Пункт (a) эквивалентен вопросу о существовании n-арных квазигрупп любых порядков для любых n. Диагонали гиперкуба $(0,\dots,0),\dots,(k-1,\dots,k-1)$ обеспечивают пункт (b).

Напомним, что ретрактом множества $M \subset Q_k^n$ называется множество $M(a_1,\dots,a_m,i_1,\dots,i_m)$, полученное фиксацией одной или нескольких координат

$$M(a_1,\dots,a_m,i_1,\dots,i_m) = \{(x_1,\dots,x_{i_1-1},x_{i_1+1},\dots,x_n) \mid (x_1,\dots,x_{i_1-1},a_1,x_{i_1+1},\dots,x_{i_m-1}a_m,x_{i_m+1},\dots,x_n) \in M\}.$$

Проекцией множества $M \subset Q_k^n$ называется множество $M'(i_1,\dots,i_m)$ наборов, полученных вычёркиванием координат из наборов, принадлежащих множеству M

$$M'(i_1,\dots,i_m) = \{(x_1,\dots,x_{i_1-1},x_{i_1+1},\dots,x_n) \mid \exists(a_1,\dots,a_m),(x_1,\dots,x_{i_1-1},a_1,x_{i_1+1},\dots,x_{i_m-1}a_m,x_{i_m+1},\dots,x_n) \in M\}.$$

Из определений следует

Предложение 122. (a) *Непустой ретракт* МДР-*кода с расстоянием d является* МДР-*кодом с расстоянием d.*

(b) *Проекция* МДР-*кода длины n с расстоянием d на грань размерности m, $m \geq n-d+1$, является* МДР-*кодом с расстоянием $d-n+m$.*

Аналогичное утверждение верно для ортогональных массивов и корреляционно-иммунных функций.

Предложение 122(b) можно уточнить:

Предложение 123.

(a) *Подмножество $M \subset Q_k^n$ мощности k^{n-d+1} является* МДР-*кодом с расстоянием d ($d \leq n$) тогда и только тогда, когда любая его проекция на грань размерности $n-d+1$ имеет мощность k^{n-d+1}.*

(b) *Подмножество $M \subset Q_k^n$ является* МДР-*кодом с расстоянием d ($d \leq n-1$) тогда и только тогда, когда любая его проекция на грань размерности $n-d+s$ ($1 < s < d$)*

является МДР-*кодом с расстоянием* s.

(c) *Подмножество* $M \subset Q_k^n$ *является* МДР-*кодом с расстоянием* $d = n - 1$ *тогда и только тогда, когда любая его проекция на 3-х мерную грань, заданную координатами с номерами* $i, i+1, i+j$ $(j > 1)$, *является* МДР-*кодом с расстоянием* 2.

Предложение 124 ([87],[114], неравенство Бирбрауэра — Фридмана). *Для любого ортогонального массива* $OA_\lambda(t, n, k)$ *справедливо неравенство*

$$\lambda k^{t-n} \geq 1 - \frac{n(k-1)}{k(t+1)}.$$

Известны следующие оценки на мощность ортогонального массива.

Предложение 125 ([174], неравенство Рао). *Для любого ортогонального массива* $OA_\lambda(t, n, k)$ *справедливо неравенство*

(a) $\lambda k^t \geq \sum\limits_{i=0}^{t/2} \binom{n}{i}(k-1)^i$, *при* t — *чётном,*

(b) $\lambda k^t \geq \sum\limits_{i=0}^{(t-1)/2} \binom{n}{i}(k-1)^i + \binom{n-1}{(t-1)/2}(k-1)^{(t+1)/2}$, *при* t — *нечётном.*

Доказательство неравенств Бирбрауэра — Фридмана и Рао можно получить, рассмотрев множество Q_k^n как абелеву группу и применяя дискретное преобразование Фурье (см. главу 2).

Замечание 11. *При* $k = 2$ *известна верхняя оценка на силу непустого ортогонального массива, в случае когда его мощность меньше половины мощности гиперкуба (см. теорему 39 и [113],[71]).*

Предложение 126. *Пусть* $M \subset Q_k^n$ — МДР-*код с расстоянием* d *и* $d \geq 3$. *Тогда* $|M| \leq k^{k-1}$ *и* $n \leq k + d - 2$.

Доказательство. Из неравенства Бирбрауэра — Фридмана и следствия 12 имеем[9], что если МДР-код с расстоянием 3 содержится в гиперкубе Q_k^n, то $n \leq k + 1$. Следовательно, мощность такого кода не превышает k^{k-1}. По предложению 122 у МДР-кода M найдётся проекция M' с кодовым расстоянием 3. Тогда $|M| = |M'| \leq k^{k-1}$. Поскольку $|M| = k^{n-d+1}$, получаем $n \leq k + d - 2$. ▲

Таким образом, число МДР-кодов фиксированного порядка k с фиксированным растоянием d $(n > d \geq 3)$ конечно. При $k = 2$ из предложения 126 вытекает

[9] Для получения этого результата можно также использовать границу Хэмминга.

Следствие 13. *Для любого n в гиперкубе Q_2^n нет* МДР-*кодов с расстоянием d при $2 < d < n$.*

Пара латинских квадратов — таблиц 2-квазигрупп f и g называется *ортогональной*, если все пары $(f(x_1, x_2), g(x_1, x_2))$, $(x_1, x_2) \in Q_k^2$, различны. Таким образом, система попарно ортогональных латинских квадратов (MOLS) является частным случаем сильно ортогональной системы. Известны следующие классические результаты относительно систем ортогональных латинских квадратов.

Предложение 127. *Если $f_1, \ldots, f_m$ — система ортогональных латинских квадратов (2-квазигрупп) на Q_k, то $m \leq k - 1$.*

Доказательство. Без ограничения общности можно считать, что первые ($x_1 = 0$) строчки всех ортогональных квадратов одинаковы и $f_i(0, 0) = 0$ для любого $i \in [m]$. Тогда элементы $f_i(1, 0)$ должны быть ненулевыми и различными для всех $i \in [m]$, т. е. $m \leq k - 1$. ▲

Из приведённого выше доказательства имеем

Следствие 14. *Пусть $M \subset Q_k^{k+1}$ —* МДР-*код с расстоянием k, тогда M не содержит точек на расстоянии $k + 1$.*

Рассмотрим МДР-код M длины $m + n$ с $d_M = m + 1$ и $n \geq 2$. По предложению 119 ему соответствует сильно ортогональная система n-арных квазигрупп $f_1, \ldots, f_m$. По предложению 123 любому непустому ретракту кода M соответствует сильно ортогональная система. В частности, найдётся система из m ортогональных латинских квадратов. Тогда из предложений 126 и 127 имеем

Следствие 15. *Для любого* МДР-*кода $M \subset Q_k^n$ с расстоянием d_M и $n > d_M \geq 3$ справедливы неравенства $d_M \leq k$ и $n \leq 2k - 2$.*

Перейдём к рассмотрению вопроса о существовании МДР-кодов.

Код называется *линейным* над полем $GF(k)$, если он является линейным множеством[10]. *Рангом* называется размерность аффинной оболочки кода, для линейного МДР-кода $M \subset Q_k^n$ с расстоянием d ранг равен $r = n - d + 1$. Из предложения 126 имеем

[10] Подразумевается, что число k — степень простого числа.

Замечание 12. *Ранг линейного кода не превосходит* $k-1$.

Удобно использовать представление линейного МДР-кода в виде решения системы линейных уравнений. Из предложения 117 следует

Предложение 128. *Множество решений системы линейных (над* $GF(k)$*) уравнений* $\sum_{j=1}^{n} a_{ij}x_j = 0$, $i \in [r]$, $n > r$, *является* МДР-*кодом (ранга* $n-r$ *с кодовым расстоянием* $d = r+1$*) в* Q_k^n *тогда и только тогда, когда любые* r *столбцов матрицы* $A = \{a_{ij}\}$ *образуют невырожденную матрицу.*

Для доказательства предложения 128 достаточно заметить, что все грани размерности r в Q_k^n содержат ровно одну точку кода, что следует из невырожденности соответствующих матриц. Отметим, что любой набор из r столбцов матрицы A является базисом над $GF(k)$. Матрица линейной системы, решениями которой являются кодовые вектора, называется *проверочной* матрицей кода.

В Q_k^n определено внутреннее произведение $\langle \overline{v}, \overline{u} \rangle = \sum_{i=1}^{n} v_i u_i$ над полем $GF(k)$. *Дуальным* к линейному коду $C \subset Q_k^n$ называется код $C^{\perp} = \{\overline{v} \in Q_k^n : \langle \overline{v}, \overline{u} \rangle = 0, \overline{u} \in C\}$.

Из предложения 128 и определения МДР-кода следует

Предложение 129. *Пусть* $C \subset Q_k^n$ *линейный* МДР-*код ранга* r, *тогда* $C^{\perp}$ *— линейный* МДР-*код ранга* $n-r$.

Следствие 16. *В* Q_k^n *линейные* МДР-*коды с расстоянием* d *и* $n-d+2$ *существуют одновременно.*

Предложение 130. *Если* $k = p^s$ *— степень простого числа, то в* Q_k^{k+1} *имеются линейные* МДР-*коды с расстоянием* d, $2 \le d \le k$.

Доказательство. Матрица $\begin{pmatrix} 0 & 1 & 1 & 1 & \dots & 1 \\ 0 & 0 & 1 & 2 & \dots & k-1 \\ 0 & 0 & 1 & 2^2 & \dots & (k-1)^2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 0 & 1 & 2^{r-1} & \dots & (k-1)^{r-1} \end{pmatrix}$ удовлетворяет условиям предложения 128 при $r < k$, поскольку любые её миноры порядка r можно выразить через определитель Вандермонда. ▲

Предложение 131. *В* Q_k^n *имеется линейный* МДР-*код ранга* $n-r$ *тогда и только*

тогда, когда найдётся матрица размера $r \times (n-r)$*, все миноры (всех размеров) которой невырождены.*

Доказательство. Система линейных функций вида $f_i(x_1, \ldots, x_{n-r}) = \sum_j a_{ij}x_j$, $i \in [r]$, ортогональна тогда и только тогда, когда матрица $A = \{a_{ij}\}$ имеет полный ранг. Тогда по предложению 119 система линейных мультиарных квазигрупп сильно ортогональна тогда и только тогда, когда все миноры матрицы A невырождены. ▲

Из предложения 131 имеем

Следствие 17. *Если* $k \neq 2$, $k = p^s$ *— степень простого числа, то над полем* $GF(k)$ *имеется система* $f_1, \ldots, f_{k-1}$ *попарно ортогональных* 2*-квазигрупп (латинских квадратов).*

Достаточно рассмотреть набор 2-квазигрупп вида $f_i(x_1, x_2) = x_1 + ix_2$, $i \in [k-1]$, где операции выполняются в поле $GF(k)$.

Предложение 132 (см. [40]). *Пусть* $k = 2^t$, $t \geq 2$, $n = k + 2$. *Существует* $C \subset Q_k^n$ *линейный* МДР*-код ранга* $n - 3$.

Доказательство. Заметим, что $a^2 \neq b^2$ при $a \neq b$ в $GF(k)$. Тогда матрица $\begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & 2 & \ldots & k-1 \\ 1 & 2^2 & \ldots & (k-1)^2 \end{pmatrix}$ удовлетворяет условиям предложения 131. ▲

Построенные в предложении 132 МДР-коды называют *астурийскими.*

Пусть α — примитивный элемент в поле $GF(k)$. Рассмотрим матрицу

$$A = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \alpha & \alpha^2 & \ldots & \alpha^{k-2} \\ 1 & \alpha^2 & \alpha^4 & \ldots & \alpha^{2(k-2)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha^r & \alpha^{2r} & \ldots & \alpha^{r(k-2)} \end{pmatrix}.$$

Любой набор из $r+1$ ($r < k-2$) столбцов матрицы A представляет собой матрицу Вандермонда. По предложению 128 матрица A является проверочной матрицей МДР-кода. Нетрудно видеть, что этот код является *циклическим*, т. е. слова вида $(y_1, y_2, \ldots, y_n)$ и $(y_2, \ldots, y_n, y_1)$ содержатся или отсутствуют в коде одновременно.

МДР-код с проверочной матрицей A называется циклическим кодом Рида — Соломона и по построению является МДР-кодом длины $k-1$ с расстоянием $r+1$.

Теорема 25 ([85]). *Пусть $S \subset Q_k^r$, $r \le k$, $k = p^s$, p — простое и любое подмножество в S из r элементов, является базисом (над полем $GF(k)$). Тогда*

(a) *если $s = 1$, $p \ne 2$, то $|S| \le k+1$;*

(b) *если $s > 1$, $p \ne 2$ и $r \le 2p-2$, то $|S| \le k+1$;*

(c) *если $p = 2$, то $|S| \le k+2$.*

Из теоремы 25 (a) и предложения 128, в частности, имеем

Следствие 18 ([84]). *Пусть k — простое и $M \subset Q_k^n$ линейный* МДР*-код с расстоянием $n > d_M > 2$. Тогда $n \le k+1$.*

Аффинной плоскостью называется система точек и прямых, удовлетворяющая следующим свойствам.

1) Через любые две различные точки проходит ровно одна прямая.

2) Через любую точку, которая не принадлежит прямой, проходит ровно одна прямая, не пересекающаяся (параллельная) с данной прямой.

3) Каждая прямая содержит не менее двух точек и существует не менее двух прямых.

Можно показать (см. [64], [185]), что в конечной аффинной плоскости каждая прямая содержит одинаковое количество точек k — *порядок* плоскости. Более того, все прямые разбиваются на $k+1$ класс по k параллельных прямых.

Предложение 133. *Аффинные плоскости порядка k взаимно однозначно соответствуют* МДР*-кодам Q_k^{k+1} с расстоянием k (системам из $k-1$ ортогональной 2-квазигруппы порядка k).*

Доказательство. Пусть дан МДР-код $M \subset Q_k^{k+1}$ с расстоянием k. Тогда элементы кода являются точками, а прямые — пересечения МДР-кода M с гиперплоскостями. Выполнение аксиомы 1) вытекает из следствия 14. Аксиомы 2) и 3) выполнены очевидно. Докажем, что аффинная плоскость порождает МДР-код. Занумеруем k прямых каждого параллельного класса числами $0, \dots, k-1$. Каждой точке сопоставим вектор из Q_k^{k+1} из номеров прямых, которым принадлежит точка.

Полученное подмножество гиперкуба является МДР-кодом по предложению 116 (b).
▲

Замечание 13. *Для любого k аффинная и проективная плоскости порядка k существуют одновременно (см.*[64], [185], [40]*).*

Пусть $M \subset Q_{k_1}^n$ — МДР-код с расстоянием d и $C_1, \ldots, C_{|M|} \subset Q_{k_2}^n$ — набор МДР-кодов с расстоянием d. Пусть $\alpha : M \to [|M|]$ — нумерация элементов кода M. Определим тензорное произведение (сплетение в [6])

$$T = \{((u_1, v_1), \ldots, (u_n, v_n)) \mid \overline{u} \in M, \overline{v} \in C_{\alpha(u)}\} \subset Q_{k_1 k_2}^n.$$

Из определения и предложения 116 нетрудно получить

Предложение 134. *Тензорное произведение T* МДР-*кодов с расстоянием d является* МДР-*кодом с расстоянием d.*

Из предложения 134 следует

Предложение 135. *Если существуют системы из s MOLS порядков k_1 и k_2, то существует система s MOLS порядка $k_1 k_2$.*

Замечание 14. *Аналогичное утверждение справедливо для систем сильно ортогональных мультиарных квазигрупп любой арности.*

Из следствия 17 и предложений 130, 134 имеем

Следствие 19. *Если $k > 1$, $k \neq 2 \mod 4$, то в Q_k найдётся пара ортогональных латинских квадратов.*

Следствие 20 (теорема Макниша, см. также [126]). *Если $k = p_1^{e_1} \ldots p_m^{e_m}$, где p_i — простое при $i \in [m]$, то существует система из s MOLS порядка k, где $s = \min\{p_i^{e_i} - 1 \mid i \in [m]\}$.*

Следствие 21 (см. [108]). *Если $k = p_1^{e_1} \ldots p_m^{e_m}$, где p_i — простое при $i \in [m]$, то существует* МДР-*код длины s с расстоянием d, $2 \leq d \leq s$, где $s = \min\{p_i^{e_i} - 1 \mid i \in [m]\}$.*

В [90] решён вопрос о существовании пар ортогональных латинских квадратов.

Теорема 26 ([90]). *При $k \neq 1, 2, 6$ найдётся пара ортогональных латинских квадра-*

тов порядка k.

Важный теоретический результат о несуществовании систем ортогональных латинских квадратов имеется в [92].

Теорема 27 ([92]). *Если $k = 1, 2 \mod 4$ и найдётся $k-1$ MOLS порядка k, то $k = p^2 + q^2$, где p, q — целые числа.*

Максимальное количество $M(k)$ попарно ортогональных латинских квадратов (MOLS) порядка k, не равного степени простого числа, является открытой комбинаторной проблемой. Минимальный порядок, при котором $M(k)$ неизвестно, равен 10. Вычислительный эксперимент показывает, что $M(10) \leq 8$ (см. [136]), но неизвестно даже, имеются ли три попарно ортогональных латинских квадрата порядка 10.

Справедлива следующая

Теорема 28 ([189]). *$M(k) \geq k^{1/17} - 2$ при достаточно больших k.*

Таким образом, для любого t и достаточно больших k существует система из t попарно ортогональных латинских квадратов порядка k. Пусть $n(t) = \max\{k \mid M(k) < t\}$. Имеются верхние оценки на величину $n(t)$ ([91], [126]):

t	$n(t) \leq$	t	$n(t) \leq$
2	6,	10	5804,
3	10,	11	7222,
4	22,	12	7286,
5	60,	13	7288,
6	74,	14	7874,
7	570,	15	8360,
8	2766,	30	52502.
9	3678,		

В [126] приводится таблица нижних оценок чисел $M(k)$ при $k \leq 10000$.

Выше были рассмотрены способы построения линейных МДР-кодов порядков, равных степени простого. Из предложений 130, 132 и теоремы 25 видно, что задача перечисления всех возможных параметров линейных МДР кодов близка к решению. В то время, как в задаче определения возможных параметров нелинейных МДР-

кодов продвижений немного.

Обзор конструкций систем попарно ортогональных латинских квадратов имеется в [100]. В [15] дан подробный обзор методов построения нелинейных систем MOLS с помощью теории групп.

Для построения нелинейных МДР-кодов составного порядка можно использовать конструкцию тензорного произведения. Рассмотрим способ построения нелинейных МДР-кодов произвольного порядка, предложенный в [18], [19].

Пусть $f : Q_k^2 \to Q_k$ — 2-квазигруппа. Определим функции $f_0(x, y) = f(x, y)$, $f_1(x, y) = f(y, f(x, y))$ и $f_i(x, y) = f(f_{i-2}(x, y), f_{i-1}(x, y))$. Функция f_i называется *i-ой рекурсивной производной* функции f.

Из предложения 123(c) можно вывести

Предложение 136 ([18]). *Все функции $f_0, \ldots, f_m$ являются* 2*-квазигруппами тогда и только тогда, когда множество $M = \{(x, f_0(x), \ldots, f_m(x)) \mid x \in Q_k^2\}$ является* МДР*-кодом (в этом случае код называется рекурсивным).*

В [19] предложено обобщение понятия рекурсивной производной на мультиарные квазигруппы и найдены оценки параметров рекурсивных МДР-кодов.

Глава 2

Совершенные раскраски, корреляционно-иммунные функции и их компоненты

§ 2.1. Совершенные раскраски

§ 2.1.1. Некоторые свойства совершенных раскрасок

Напомним, что совершенной раскраской гиперкуба Q_q^n в k цветов называется отображение $Col : Q_q^n \to \{0, 1, \ldots, k-1\}$, удовлетворяющее следующему условию: мощность пересечения $|Col^{-1}(i) \cap B_1(\overline{x})|$ зависит только от цветов i и $Col(\overline{x})$, но не от вершины $\overline{x} \in Q_q^n$. Каждой совершенной раскраске соответствует матрица параметров $P = \{p_{ij}\}$, где p_{ij} — число вершин цвета j в сфере радиуса 1 с центром в вершине цвета i.

Занумеруем вершины гиперкуба Q_q^n числами от 1 до q^n. Определим $(0,1)$-матрицу $M(n,q) = \{m_{ij}\}$ так: $m_{ij} = 1$, если i-я и j-я вершины находятся на расстоянии 1, и $m_{ij} = 0$ в противном случае. Матрица $M = M(n,q)$ называется *матрицей смежно-*

сти гиперкуба ΓQ_q^n. Например, матрица смежности для ΓQ_2^2 имеет вид $\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$.

По произвольной раскраске Col куба Q_q^n в k цветов определим матрицу F_{Col} размера $q^n \times k$, в которой i-я строка состоит из 0 с единственной 1 на позиции $j = Col(i)$. В следующих утверждениях дана линейно алгебраическая характеризация совершенных раскрасок.

Предложение 137. a) *Если Col — совершенная раскраска гиперкуба Q_q^n с матрицей P, то $MF_{Col} = F_{Col}P$.*

b) *Если для некоторой раскраски Col и матрицы P выполнено равенство $MF_{Col} = F_{Col}P$, то раскраска Col совершенная и P — её матрица параметров.*

Предложение можно доказать непосредственной проверкой равенства в п. (a) и проверкой определения совершенной раскраски в п. (b).

Предложение 138. *Пусть P матрица параметров совершенной раскраски гиперкуба Q_q^n, тогда собственные числа матрицы P являются собственными числами матрицы смежности M.*

Доказательство. Пусть $v \in \mathbb{C}^k$ — собственный вектор матрицы P. Тогда $Pv = \lambda v$ и $MF_{Col}v = F_{Col}Pv = \lambda F_{Col}v$, причём $F_{Col}v \neq \overline{0}$, если $v \neq \overline{0}$. Таким образом, λ — собственное число матрицы M. ▲

Предложение 139. *Пусть $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ матрица параметров совершенной раскраски гиперкуба Q_q^n. Тогда число $\frac{q^n b}{b+c}$ целое.*

Для доказательства предложения 139 достаточно заметить, что количества вершин разных цветов относятся друг к другу как b/c.

Для раскрасок в произвольное число цветов предложение 139 можно обобщить следующим образом.

Предложение 140. *Пусть P — матрица параметров совершенной раскраски Q_q^n в k цветов. Пусть b_i — количество вершин цвета i. Тогда*

(a) $P\bar{b} = n(q-1)\bar{b}$; *(b)* $\sum_{i=0}^{k-1} b_i = q^n$; *(c)* $p_{ij}b_j = p_{ji}b_i$ *для любых* $i, j \in \{0, 1, \ldots, k-1\}$.

Замечание 15. *Нетрудно видеть, что предложения 137–139 верны для произвольного регулярного графа.*

Предложения 137–139 были сообщены автору С.В.Августиновичем. В напечатанном виде они имеются, например, в [152].

Рассмотрим несколько конструкций 2-раскрасок булева гиперкуба.

Предложение 141. *Пусть* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *матрица параметров совершенной раскраски булева куба* Q_2^n. *Тогда существует совершенная раскраска булева куба* Q_2^{n+1} *с матрицей параметров* $\begin{pmatrix} a+1 & b \\ c & d+1 \end{pmatrix}$.

Для доказательства предложения 141 достаточно заметить, что если $f : Q_2^n \to \{0, 1\}$ раскраска с матрицей параметров $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, то раскраску куба Q_2^{n+1} с требуемой матрицей параметров можно определить равенством $f'(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n)$.

Предложение 142 (конструкция удвоения [68]). *Пусть* $f : Q_2^n \to Q_2$ *— совершенная раскраска с матрицей параметров* $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. *Тогда* $g : Q_2^{2n} \to Q_2$, *где* $g(x, y) = f(x \oplus y)$, *есть совершенная раскраска с матрицей параметров* $2P$.

Доказательство предложения 142 получается непосредственной проверкой, его можно обобщить следующим образом.

Предложение 143. *Пусть* P *матрица параметров совершенной 2-раскраски булева куба* Q_2^n. *Тогда существует совершенная раскраска с параметрами* tP *в* Q_2^{tn}.

Следующее утверждение обеспечивает свойство монотонности реализуемых параметров совершенных раскрасок в два цвета.

Предложение 144. *Для любой пары натуральных чисел* b, c *таких, что*[1] $\frac{b+c}{(b,c)} = 2^t$

[1] Здесь (b, c) — наибольший общий делитель чисел b и c.

найдётся такое a_0, что матрица Пусть $\begin{pmatrix} a & b \\ c & a+b-c \end{pmatrix}$ *является матрицей параметров совершенной раскраски булева куба если и только если $a \geq a_0$.*

Предложение 144 было доказано С.В.Августиновичем и А.Э.Фрид и опубликовано в статье Д.Г.Фон-Дер-Флаасса [68].

Обозначим через $L_t(\overline{x})$ сферу радиуса t с центром в точке $\overline{x}$. Теорема 29 была доказана сначала Г.С.Шапиро и Д.С.Злотником для 1-совершенных кодов в булевом кубе [180], а затем Д.С.Кротовым для любого дистанционно регулярного графа [152].

Теорема 29. *Для любой совершенной раскраски $Col : Q_q^n \to \{0, 1, \ldots, k-1\}$ и $t \in \mathbb{N}$ мощность пересечения $|Col^{-1}(i) \cap L_t(\overline{x})|$ зависит только от цветов i и $Col(\overline{x})$.*

Доказательство. Без ограничения общности считаем, что $x = \overline{0}$. Пусть r_t — число вершин из $L_{t-1}(\overline{0})$ смежных с одной вершиной из $L_t(\overline{0})$; l_t — число вершин из $L_{t+1}(\overline{0})$ смежных с одной вершиной из $L_t(\overline{0})$; u_t — число вершин из $L_t(\overline{0})$ смежных с одной вершиной из $L_t(\overline{0})$.

Пусть M_t — матрица смежности расстояний t в гиперкубе Q_q^n. Тогда

$$M_t M = M_{t+1} r_{t+1} + M_{t-1} l_{t-1} + M_t u_t,$$

$M_1 = M$, $M_0 = E$ — единичная матрица, $M_t = p_t(M)$, p_t — некоторый многочлен степени t.

$$M_t F_{Col} = p_t(M) F_{Col} = F_{Col} p_t(P).$$

Из предложения 137 следует, что F_{Col} — совершенная раскраска графа расстояний t в Q_q^n. ▲

По-существу теорема 29 означает, что совершенная раскраска по расстоянию 1 всегда является совершенной раскраской по любому расстоянию. Из доказательства теоремы 29 можно извлечь

Следствие 22. *Если две совершенные раскраски по расстоянию 1 имеют одинаковую матрицу параметров P, то они имеют одинаковые матрицы параметров $p_t(P)$ как раскраски по расстоянию t.*

§ 2.1.2. Совершенные коды

Напомним, что множество $C \subset Q_q^n$ называется 1-совершенным кодом, если для любой вершины $\overline{x} \in Q_q^n$ найдётся единственная вершина $\overline{y} \in C$, для которой $d(\overline{x}, \overline{y}) \leq 1$. Заметим, что $d(x, y) \geq 3$ для любых различных $x, y \in C$ и имеет место следующий простой критерий

Предложение 145. *Множество $C \subset Q_q^n$ является 1-совершенным кодом тогда и только тогда, когда*

1) $d(\overline{x}, \overline{y}) \neq 1, 2$ *для любых* $\overline{x}, \overline{y} \in C$;

2) $|C| \geq \frac{q^n}{n(q-1)+1}$.

Поскольку 1-совершенный код задаёт разбиение гиперкуба Q_q^n на шары мощности $n(q-1)+1$, справедливо

Предложение 146. *Для любого 1-совершенного кода выполняется равенство* $|C| = \frac{q^n}{n(q-1)+1}$.

Следствие 23. *Если q — степень простого числа, то 1-совершенные q-ичные коды длины n могут существовать только при $n = \frac{q^t-1}{q-1}$, где t — натуральное.*

Нетрудно видеть, что 1-совершенный код является частным случаем совершенной 2-раскраски. А именно, справедливо

Предложение 147. *Множество $C \subset Q_q^n$ является 1-совершенным кодом тогда и только тогда, когда характерестическая функция χ^C является совершенной раскраской гиперкуба Q_q^n в два цвета с матрицей параметров*[2] $\begin{pmatrix} 0 & n(q-1) \\ 1 & n(q-1)-1 \end{pmatrix}$.

Совершенная 2-раскраска (точнее множество вершин первого цвета) с параметрами $\begin{pmatrix} t-1 & n(q-1)-t+1 \\ t & n(q-1)-t \end{pmatrix}$ называется t-кратным совершенным кодом.

Известны следующие классические результаты о 1-совершенных кодах.

Теорема 30 ([123]). *Если $q = p^s$, где p — простое, то для любого $n = \frac{q^t-1}{q-1}$, где t — натуральное, существует линейный (над $GF(q)$) совершенный код $H \subset Q_q^n$ (код Хэмминга).*

[2] По традиции значение функции 1 считается первым цветом, а 0 — вторым.

Для доказательства теоремы 30 достаточно построить проверочную матрицу $n \times t$ кода H, никакие три столбца в которой не являются линейно зависимыми.

Существование нелинейных 1-совершенных кодов было установлено Ю.Л.Васильевым [8]. Через $|x| = x_1 \oplus x_2 \oplus \cdots \oplus x_n$ обозначим *чётность* вершины $x \in Q_2^n$.

Теорема 31 ([8]). *Пусть $C \subset Q_2^m$ — 1-совершенный код. Тогда множество $C_\lambda = \{(x, x \oplus y, |x| \oplus \lambda(y)) \mid x \in Q_2^m, y \in C\}$, где $\lambda : C \to \{0,1\}$ — произвольная функция, является 1-совершенным кодом в Q_2^{2m+1}.*

Доказательство. В соответствии с предложением 145 достаточно доказать, что $|C_\lambda| = \frac{2^{2m+1}}{2m+2} = |C| \cdot 2^m$ и $d(z, z') \geq 3$ для любых $z, z' \in C_\lambda$. Первое сразу следует из определения кода C_λ, второе нетрудно получить непосредственной проверкой. ▲

Поскольку λ — произвольная булева функция, из теоремы 31 имеем

Следствие 24 ([8]). *Число 1-совершенных кодов в Q_2^{2m+1} не меньше $2^{2^m/(m+1)}$, когда $m = 2^t - 1$, $t \geq 3$.*

Сравнив число различных функций λ и число различных аффинных подпространств, получаем

Следствие 25 ([8]). *Существуют нелинейные 1-совершенные коды.*

Дж. Шёнхейм [178] предложил подобную конструкцию для построения 1-совершенных кодов в Q_q^n, где $q = p^s$ — степень простого, $n = \frac{q^t-1}{q-1}$.

Теорема 32 ([178]). *Пусть $H \subset Q_q^n$ — 1-совершенный код и $f : H \to Q_q$ произвольная функция. Тогда множество*
$C(H, f) = \{((v_\alpha)_{\alpha \in Q_q}, pr) : v_\alpha \in Q_q^n, \sum\limits_{\alpha \in Q_q} v_\alpha = c \in H, \ pr \stackrel{def}{=} \sum\limits_{\alpha \in Q_q} \alpha |v_\alpha| + f(c)\}$,
является 1-совершенным кодом в Q_q^{qn+1}. Здесь $(v_\alpha)_{\alpha \in Q_q}$ — конкатенация наборов v_α, $|v_\alpha|$ — сумма n элементов набора v_α, все арифметические операции выполняются в поле $GF(q)$.

§ 2.1.3. Каскадные конструкции 1-совершенных кодов

Перейдём к рассмотрению конструкций совершенных кодов, использующих МДР-коды и мультиарные квазигруппы.

Пусть $q = 2$ и $C \in Q_2^n$ — совершенный код. Множества $C_0 = \{(\overline{x}, |\overline{x}|) \mid \overline{x} \in C\}$ и $C_1 = \{(\overline{x}, |\overline{x}| \oplus 1) \mid \overline{x} \in C, \}$ называются *расширенными совершенными кодами.* Код C_0 состоит из наборов чётного веса, а C_1 — нечётного.

Непосредственно из определения расширенного кода нетрудно получить следующие критерии.

Предложение 148. *Множество $C \subset Q_2^{n+1}$ является расширенным совершенным кодом тогда и только тогда, когда $|C| = 2^n/(n+1)$ и $d_C = 4$.*

Предложение 149. *Множество $C \subset Q_2^n$ является расширенным совершенным кодом чётного веса тогда и только тогда, когда для любой вершины $y \in Q_2^n$ нечётного веса найдётся единственная вершина $x \in C$ такая, что $d(x, y) = 1$.*

Предложение 150. *Множество $C \subset Q_2^n$ является расширенным совершенным кодом тогда и только тогда, когда любая его проекция на гиперграни является 1-совершенным кодом.*

Конструкция I, предложенная в работах [25] и [171], связывает МДР-коды и расширенные совершенные коды. Пусть m, k, $n = mk$ — степени двойки;
R, C — приведённые (т. е. содержащие $\overline{0}$) расширенные совершенные коды длин m и k соответственно;
$M_{\overline{r}}$ — МДР-коды[3] в Q_k^m (возможно, различные для разных $\overline{r} \in R$);
e_i – единичные орты[4] в Q_2^k;
$C_{i-1}^1 \stackrel{def}{=} C \oplus \overline{e}_i$ и $C_{i-1}^0 \stackrel{def}{=} C_{i-1}^1 \oplus \overline{e}_k$, $i \in [k]$. Заметим, что $Q_2^n = \bigcup_i (C_i^0 \cup C_i^1)$ и $C_i^a \cap C_{i'}^{a'} = \varnothing$, если $(i, a) \neq (i', a')$. В случае, когда $k = 4$, имеем $C_0^0 = \{(0000), (1111)\}$, $C_1^0 = \{(0110), (1001)\}$, $C_2^0 = \{(0101), (1010)\}$, $C_3^0 = \{(0011), (1100)\}$, $C_0^1 = \{(0001), (1110)\}$, $C_1^1 = \{(0111), (1000)\}, C_2^1 = \{(0100), (1011)\}$, $C_3^1 = \{(0010), (1101)\}$.

[3] Здесь и далее имеются ввиду МДР-коды с расстоянием 2

[4] Будем нумеровать орты элементами Q_k, полагая $\overline{e}_0 = \overline{e}_k$.

Определим множество $\widetilde{C} \subset Q_2^n$ равенством

$$\widetilde{C} = \bigcup_{\overline{r} \in R} \bigcup_{\overline{a} \in M_{\overline{r}}} C_{a_1}^{r_1} \times C_{a_2}^{r_2} \times \cdots \times C_{a_m}^{r_m}. \tag{2.1}$$

Используя предложение 148, нетрудно доказать

Предложение 151 ([171]). *Множество $\widetilde{C}$ является расширенным совершенным кодом.*

Поскольку для каждого $\overline{r} \in R$ можно выбрать свой МДР-код $M(\overline{r})$, из предложения 151 имеем

Следствие 26 ([171]). *Число различных расширенных совершенных кодов длины mk, где m, k — степени двойки, не меньше чем $N_{mds}(m-1,k)^{2^{m-1}/m}$.*

Учитывая оценку числа 4-ичных МДР-кодов (предложение 62), имеем

Следствие 27 ([31]). *Число различных расширенных совершенных кодов длины n не меньше чем $2^{2^{(n+1)/2-\log_2(n+1)}} 3^{2^{(n-3)/4}} 2^{2^{(n+5)/4-\log_2(n+1)}}$.*

Из замечания 146 нетрудно видеть, что ранг линейного 1-совершенного кода длины n равен $n-\log_2(n+1)$. Соответственно линейный расширенный совершенный код длины $n+1$ имеет тот же ранг. Описание линейных 1-совершенных кодов сводится к описанию их проверочных матриц. Совершенные коды рангов на 1 и на 2 больше, чем минимальный, можно описать посредством 4-ичных МДР-кодов.

Теорема 33 ([80]). *Расширенный совершенный код длины $n+1$ имеет ранг не более чем $n+2-\log_2(n+1)$ тогда и только тогда, когда его можно представить в виде* (2.1)*, где $k=4$ и в качестве R взят линейный код.*

Теорема 33 обеспечивает конструктивное описание совершенных кодов указанных рангов, поскольку используемые в конструкции 4-ичные МДР-коды конструктивно описаны в теореме 7.

Рассмотрим частный случай конструкции II из [127], обобщающий конструкцию I, приведённую выше.

Пусть $v, h : Q_k^{k-1} \to Q_k$ — две ортогональные $(k-1)$-арные квазигруппы (такие найдутся по предложениям 119, 130, если k — степень простого числа), $f_1, \ldots, f_t$ —

произвольный набор 2-квазигрупп порядка k, $R \subset Q_k^t$ — совершенный код. Пусть для каждого $\overline{r} \in R$ определён МДР-код $M_{\overline{r}} \subset Q_k^{t+1}$. Рассмотрим множество

$\widehat{C} = \{(\overline{x}_1, y_1, \overline{x}_2, y_2, \ldots, \overline{x}_t, y_t, z) \in Q_k^{tk+1} \mid$

$\overline{x}_i \in Q_k^{k-1}, i \in [t], \overline{r} = (f_1(v(\overline{x}_1), y_1), \ldots, f_t(v(\overline{x}_t), y_t)) \in R, (h_1(\overline{x}_1), \ldots, h(\overline{x}_t), z) \in M_{\overline{r}}\}$.

Предложение 152 ([127]). *Код $\widehat{C}$ является 1-совершенным.*

Поскольку для каждого $\overline{r} \in R$ МДР-код $M_{\overline{r}}$ можно выбирать произвольно, из предложения 152 имеем

Следствие 28 ([127]). *Пусть $k = p^s$, где p — простое. Тогда число различных совершенных кодов длины $n = \frac{k^m-1}{k-1}$ не меньше, чем $N_{mds}(t,k)^{k^t/((k-1)t+1)}$, где $t = \frac{k^{m-1}-1}{k-1}$.*

§ 2.1.4. Транзитивные 1-совершенные коды

Конструкция I позволяет строить из изотопно транзитивных МДР-кодов транзитивные расширенные совершенные коды.

Нетрудно заметить, что все совершенные расширенные коды длины 4 можно представить в виде $\{\overline{v}, \overline{v}+\overline{1}\}$, т. е. как смежные классы C_a^r кода $C_0 = \{\overline{0}, \overline{1}\} \subset Q_2^4$. Покажем, что при $k = 4$ перестановка координат соответствует перестановке смежных классов.

Предложение 153. (a) *Для любого $b \in Q_2^4$ найдётся такая перестановка $\sigma \in S_4$, что $C_a^r + \overline{e}_b + \overline{e}_4 = C_{\sigma(a)}^r$ для всех $a \in Q_2^4$ и $r \in \{0,1\}$.*

(b) *Для любой перестановки $\tau \in S_4$ найдётся такая перестановка $\sigma \in S_4$, что $\left(C_a^0\right)_\tau = C_{\sigma(a)}^0$ для всех $a \in Q_2^4$.*

(c) *Для любой перестановки $\sigma \in S_4$ найдётся перестановка $\tau \in S_4$ такая, что $C_{\sigma(a)}^r + \overline{e}_{\sigma(0)} + \overline{e}_4 = \left(C_a^r\right)_\tau$ для всех $a \in Q_2^4$ и $r \in \{0,1\}$.*

Доказательство. (a), (b) Рассмотрим разбиение J множества чётных вершин из Q_2^4 на коды $C_0^0, C_1^0, C_2^0, C_3^0$. Очевидно, что перестановка координат и прибавление набора с чётным числом единиц переводит элементы из J в элементы из J, т. е. порождает их перестановку. Так как $C_a^r = r\overline{e}_4 + C_a^0$, то перестановка σ не зависит от $r \in \{0,1\}$.

(c) Из (a) получаем равенство $C_{\sigma(a)}^r + \overline{e}_b + \overline{e}_4 = C_{\tau(a)}^r$, в котором перестановка τ

не зависит от $r \in \{0,1\}$. Поскольку $C^r_{\sigma(0)} + \overline{e}_{\sigma(0)} + \overline{e}_4 = C^r_0$, то $\tau(0) = 0$. Тогда, как нетрудно видеть, $C^r_{\tau(a)} = \left(C^r_a\right)_\tau$ при $a \neq 0$. Кроме того, $C^r_0 = \left(C^r_0\right)_\pi$ для произвольной перестановки π, оставляющей на месте последнюю координату. ▲

Лемма 15 ([48]). *Пусть R — линейный расширенный совершенный код, M — изотопно транзитивный* МДР*-код длины m. Тогда расширенный совершенный код C длины $4m$, заданный равенством* (2.1)*, где $M_{\overline{r}} = M$ для любого $\overline{r} \in R$, является транзитивным.*

Доказательство. Представим вершину $\overline{y} \in C$ в виде $\overline{y} = (\widetilde{y}_1, \widetilde{y}_2, \ldots, \widetilde{y}_m)$, где $\widetilde{y}_i = (1 + r_i)\overline{e}_4 + \overline{e}_{b_i} + \delta\overline{1}$, $\delta \in \{0,1\}$, $\overline{r} \in R$. Из линейности кода R вытекает, что если $\overline{y} = (\widetilde{y}_1, \widetilde{y}_2, \ldots, \widetilde{y}_m) \in C$, то $(\widetilde{y}_1 + r_1\overline{e}_4, \widetilde{y}_2 + r_2\overline{e}_4, \ldots, \widetilde{y}_m + r_m\overline{e}_4) \in C$ при любом $\overline{r} \in R$. Из определения C^r_a вытекает, что если $\overline{y} = (\widetilde{y}_1, \widetilde{y}_2, \ldots, \widetilde{y}_m) \in C$, то $(\widetilde{y}_1 + \delta_1\overline{1}, \widetilde{y}_2 + \delta_2\overline{1}, \ldots, \widetilde{y}_m + \delta_m\overline{1}) \in C$ при любом $\overline{\delta} \in Q_2^m$. Следовательно,

$$\overline{y} + C = v(\overline{b}) + C, \tag{2.2}$$

где $v(\overline{b}) = (\overline{e}_4 + \overline{e}_{b_1}, \ldots, \overline{e}_4 + \overline{e}_{b_m})$ и $\overline{b} \in M$. Так как код M изотопно транзитивный, то найдётся набор перестановок $\overline{\sigma}$, удовлетворяющий равенствам $\overline{\sigma}M = M$ и $\overline{\sigma}\overline{0} = \overline{b}$. Из пункта (c) предложения 153 следует, что найдутся перестановки $\tau_i \in S_4$, $i = 1, \ldots, m$ такие, что

$$C^r_{\sigma_i(a)} + \overline{e}_{b_i} + \overline{e}_4 = \left(C^r_a\right)_{\tau_i}, \tag{2.3}$$

при всех $a \in Q_4$ и $r \in \{0,1\}$. Из равенств (2.1)–(2.3) имеем

$$\overline{y} + C = v(\overline{b}) + \bigcup_{\overline{r}\in R}\bigcup_{\overline{a}\in M} C^{r_1}_{a_1} \times C^{r_2}_{a_2} \times \cdots \times C^{r_n}_{a_m} = v(\overline{b}) + \bigcup_{\overline{r}\in R}\bigcup_{\overline{a}\in \overline{\sigma}M} C^{r_1}_{a_1} \times C^{r_2}_{a_2} \times \cdots \times C^{r_n}_{a_m} =$$

$$= \bigcup_{\overline{r}\in R}\bigcup_{\overline{a}\in M} (\overline{e}_4 + \overline{e}_{b_1} + C^{r_1}_{\sigma_1(a_1)}) \times (\overline{e}_4 + \overline{e}_{b_2} + C^{r_2}_{\sigma_2(a_2)}) \times \cdots \times (\overline{e}_4 + \overline{e}_{b_m} + C^{r_m}_{\sigma_n(a_m)}) =$$

$$= \bigcup_{\overline{r}\in R}\bigcup_{\overline{a}\in M} \left(C^{r_1}_{a_1}\right)_{\tau_1} \times \left(C^{r_2}_{a_2}\right)_{\tau_2} \times \cdots \times \left(C^{r_m}_{a_m}\right)_{\tau_m} = C_\pi,$$

для соответствующей перестановки $\pi \in S_{4n}$. ▲

Пусть $M(C)$ — множество МДР-кодов, из которых посредством конструкции I получаются коды эквивалентные расширенному совершенному коду C, т. е. $M' \in M(C)$,

если найдётся расширенный совершенный приведённый код C', который эквивалентен коду C и удовлетворяет равенству (2.1) с МДР-кодом $M_{\overline{r}} = M'$.

Предложение 154 ([48]). *Пусть C — нелинейный расширенный совершенный код длины $4m$, удовлетворяющий равенству* (2.1)*. Тогда в множестве $M(C)$ содержится не более $2m - 1$ классов эквивалентности* МДР*-кодов.*

Из леммы 15, предложения 154 и теоремы 14 имеем

Предложение 155 ([48]). *Существует не менее $2^{\Omega(\sqrt{n})}$ неэквивалентных транзитивных совершенных двоичных кодов длины n.*

А применение следствия 7 обеспечивает нижнюю оценку $2^{\Omega(n^2)}$ числа транзитивных кодов близкую к верхней оценке (см. [157]).

§ 2.1.5. Нерасщепляемые кратные 1-совершенные коды

Обозначим через $\overline{E}^n$ и $\underline{E}^n$ множества чётных и, соответственно, нечётных наборов из Q_2^n.

Подмножество C множества $\overline{E}^n$ называется *l-кратным расширенным совершенным кодом*, если $|B_1(x) \cap C| = l$ для любого $x \in \underline{E}^n$.

Будем называть l-кратный расширенный совершенный код *нерасщепляемым*, если его нельзя представить в виде объединения l попарно не пересекающихся расширенных совершенных кодов и *вполне нерасщепляемым*, если он не содержит в качестве подмножества однократного расширенного совершенного кода. Следующее утверждение следует из предложения 149.

Предложение 156. *Пусть $C \subseteq Q_2^n$, $\overline{C} \subseteq Q_2^{n+1}$ и $\overline{C}$ получается из C добавлением проверки на чётность. Тогда C является l-кратным совершенным кодом (нерасщепляемым l-кратным совершенным кодом, вполне нерасщепляемым l-кратным совершенным кодом), если и только если $\overline{C}$ есть l-кратный расширенный совершенный код (соответственно нерасщепляемый l-кратный совершенный код, вполне нерасщепляемый l-кратный совершенный код).*

Аналогично предложению 145 имеем

Предложение 157. *Подмножество $C \subset \overline{E}^n$ является l-кратным расширенным совершенным кодом, если $|C| = l\frac{2^n}{2n}$ и $|B_1(x) \cap C| \geq l$ для любого x из $\underline{E}^n$.*

Аналогично предложению 151 с помощью предложения 157 нетрудно доказать, что если в конструкции I МДР-код $M_{\overline{r}}$ заменить на l-кратный МДР-код B, то множество, заданное формулой (2.1), является l-кратным расширенным совершенным кодом. Таким образом, справедливо

Предложение 158 ([34]). *Если B есть l-кратный МДР-код, то множество D, заданное формулой*

$$D = \bigcup_{(a_1,\ldots,a_m)\in H} \bigcup_{(i_1,\ldots,i_m)\in B} C_{i_1}^{a_1} \times C_{i_2}^{a_2} \times \ldots \times C_{i_m}^{a_m}, \tag{2.4}$$

есть l-кратный расширенный совершенный код.

Для произвольного набора $x = (x_1, ..., x_n) \in Q_2^n = Q_2^{mk}$ определим *обобщённую проверку на чётность*

$$p(x) = (x_1 \oplus \cdots \oplus x_k\,,\; x_{k+1} \oplus \cdots \oplus x_{2k}\,,\; \ldots\,,\; x_{(m-1)k+1} \oplus \cdots \oplus x_{mk}).$$

Справедливо следующее

Предложение 159 ([34]).

1) *Для любого x из D верно, что $p(x) \in H$.*

2) *$(\overline{e}_{i_1}, \ldots, \overline{e}_{i_m}) \in D$, если и только если $(i_1, \ldots, i_m) \in B$.*

3) *Пусть $A \subset D$ – расширенный совершенный код длины n и $B_0 = \{(i_1, \ldots, i_m) | (\overline{e}_{i_1}, \ldots, \overline{e}_{i_m}) \in A\}$. Тогда B_0 — МДР-код и $B_0 \subset B$.*

Доказательство. Пункты 1 и 2 непосредственно вытекают из формулы (2.4). Из пункта 2 следует, что $B_0 \subseteq B$. Покажем, что B_0 есть МДР-код с расстоянием 2. По предложению 116 достаточно вычислить кодовое расстояние и мощность.

Если наборы $(i_1, \ldots, i_m)$ и $(j_1, \ldots, j_m)$ из B_0 различны только в одной координате, то $(\overline{e}_{i_1}, \ldots, \overline{e}_{i_m})$ и $(\overline{e}_{j_1}, \ldots, \overline{e}_{j_m})$ из A различаются только в двух координатах, что противоречит тому, что A – расширенный совершенный код.

Для произвольных $i_2, \ldots, i_m$ рассмотрим $x = (\overline{0}, \overline{e}_{i_2}, \ldots, \overline{e}_{i_m})$. Поскольку $x \in \underline{E}^n$, существует единственный $y \in A$, отличный от x ровно в одной координате. Тогда

наборы $p(x)$ и $p(y)$ также различаются ровно в одной координате. Поскольку $p(x) = (0, 1, \ldots, 1)$ и $p(y) \in H \ni (1, 1, \ldots, 1)$, то $p(y) = (1, 1, \ldots, 1)$. Следовательно, $y = (\overline{e}_{i_1}, \overline{e}_{i_2}, \ldots, \overline{e}_{i_m})$ для некоторого i_1. Поскольку $y \in A$, то $(i_1, i_2, \ldots, i_m) \in B_0$. Таким образом, $|B_0| = k^{m-1}$. ▲

Теорема 34 ([34]).

1) *При $n = 2^s$, $1 < l < n/8$ в Q_2^n найдётся нерасщепляемый l-кратный расширенный совершенный код.*

2) *При $n = 2^s$, $1 \leq t \leq s - 3$ в Q_2^n найдётся вполне нерасщепляемый 2^t-кратный расширенный совершенный код.*

Доказательство.

1. Пусть $m = 4, k = 2^{s-2}$. Из теоремы 21 имеем нерасщепляемый l-кратный МДР-код $B \subset Q_k^m$ $(2 \leq l < n/8 = k/2)$. Вследствие предложения 158, множество D, полученное из B в соответствие с формулой (2.4), является l-кратным расширенным совершенным кодом. Покажем, что код D – нерасщепляем.

Пусть $D = C_0 \cup \cdots \cup C_{l-1}$, где $C_i \cap C_j = \varnothing$ при $i \neq j$ и C_i — расширенные совершенные коды. Тогда из предложения 159 следует, что при $0 \leq j \leq l - 1$ множества $B_j = \{(i_1, \ldots, i_m) | (\overline{e}_{i_1}, \ldots, \overline{e}_{i_m}) \in C_j\}$ являются МДР-кодами. Причём $B_j \subset B$ и коды B_j не пересекаются, так как коды C_j не пересекаются. Тогда из равенства

$$|B| = lk^{m-1} = \sum_{j=0}^{l-1} |B_j|$$

следует, что $B = B_0 \cup \cdots \cup B_{l-1}$. Из противоречия следует нерасщепляемость кода D.

2. Пусть $m = 2^{s-t-1}, k = 2^{t+1}$. Из теоремы 22 имеем вполне нерасщепляемый 2^t-кратный МДР-код $B \subset Q_k^m$. Вследствие предложения 158, множество D, полученное из B в соответствии с формулой (2.4), является 2^t-кратным расширенным совершенным кодом. Покажем от противного, что код D не содержит однократного подкода. Пусть $C \subset D$ – однократный расширенный совершенный код. Тогда из предложения 159 следует, что множество $B' = \{(i_1, \ldots, i_m) : (\overline{e}_{i_1}, \ldots, \overline{e}_{i_m}) \in C\}$ является МДР-кодом и содержится в B. Получили противоречие. ▲

Из теоремы 34 и предложения 156 следует

Теорема 35 ([34]). 1) *При $n = 2^s - 1$, $1 < l < 2^{s-3}$ в Q_2^n найдётся нерасщепляемый l-кратный 1-совершенный код.*

2) *При $n = 2^s - 1$, $1 \le t \le s-3$ в Q_2^n найдётся вполне нерасщепляемый 2^t-кратный 1-совершенный код.*

§ 2.1.6. Каскадная конструкции совершенных 2-раскрасок

Рассмотрим обобщение конструкции I, позволяющее строить совершенные 2-раскраски с матрицей параметров

$$\begin{pmatrix} 0 & k(2^s-1) \\ k & k(2^s-2) \end{pmatrix}. \tag{2.5}$$

Пусть $m = 2^{s-2}$, $n = (2^s-1)k$, $s \ge 2$. Зафиксируем $\widetilde{R} \subset Q_2^{m-1}$ — линейный 1-совершенный код (код Хэмминга). Пусть $r \in Q_2^{k(m-1)}$, определим $\widetilde{r} = \left(\bigoplus_{i=1}^{k} r_i, \dots, \bigoplus_{i=k(m-2)+1}^{k(m-1)} r_i \right)$ и $R = \{r \in Q_2^{k(m-1)} \mid \widetilde{r} \in \widetilde{R}\}$. Для каждого $r \in R$ зададим МДР-код $M_r \subset Q_4^{km}$ (с расстоянием 2). Напомним обозначения C_j^i и введём C_i:

$$C_0^0 = \{0000, 1111\}, \quad C_1^0 = \{1001, 0110\}, \quad C_2^0 = \{0101, 1010\}, \quad C_3^0 = \{0011, 1100\};$$
$$C_0^1 = \{0001, 1110\}, \quad C_1^1 = \{1000, 0111\}, \quad C_2^1 = \{0100, 1011\}, \quad C_3^1 = \{0010, 1101\};$$
$$C_0 = \{000\ , 111\ \}, \quad C_1 = \{100\ , 011\ \}, \quad C_2 = \{010\ , 101\ \}, \quad C_3 = \{001\ , 110\ \}.$$

Определим множество $S \subset Q_2^n$, где $n = (2^s-1)k$, равенством

$$S = \bigcup_{r \in R} \bigcup_{\alpha \in M_r} Y_{\alpha,r}, \qquad Y_{\alpha,r} = C_{\alpha_1}^{r_1} \times C_{\alpha_2}^{r_2} \times \dots \times C_{\alpha_{k(m-1)}}^{r_{k(m-1)}} \times C_{\alpha_{k(m-1)+1}} \times \dots \times C_{\alpha_{km}}. \tag{2.6}$$

Теорема 36 ([50]). *Пусть множество $S \subset Q_2^n$ определено равенством* (2.6)*, тогда χ^S — совершенная раскраска с матрицей параметров* (2.5)*.*

Доказательство. Аналогично предложению 157 видим, что достаточно доказать

(a) если $u, v \in S$, то $d(u, v) \ge 2$;

(b) $|\{v \in S \mid d(u, v) = 1\}| \ge k$ для любой вершины $u \notin S$;

(c) $|S| = 2^{n-s}$.

Докажем пункт (a). Если $u \in Y_{\alpha,r}$, $v \in Y_{\alpha',r'}$ и $\alpha \neq \alpha'$, то $d(\alpha, \alpha') \geq 2$ по определению МДР-кода. Поскольку множества C_i^δ попарно не пересекаются и множества C_i попарно не пересекаются, то $d(u, v) \geq 2$.

Пусть $u \in Y_{\alpha,r}$, $v \in Y_{\alpha,r'}$. Если $\widetilde{r} \neq \widetilde{r}'$, то из определения 1-совершенного кода следует, что $d(r, r') \geq 3$ и, следовательно, $d(u, v) \geq 3$. Если же $\widetilde{r} = \widetilde{r}'$, но $r \neq r'$, то $d(r, r') \geq 2$ из определения $\widetilde{r}$. Тогда $d(u, v) \geq 2$.

Пусть $u, v \in Y_{\alpha,r}$. Тогда $d(u, v)$ не меньше расстояния между различными вершинами одного из множеств C_i^δ или C_i, т. е. $d(u, v) \geq 3$.

Докажем пункт (b). Рассмотрим произвольный вектор $u \in Q_2^n$. Ясно, что найдутся единственные $\alpha \in Q_4^{km}$ и $r \in Q_2^{m-1}$, что $u \in Y_{\alpha,r}$. Поскольку $u \notin S$, то возможны следующие случаи (b1) $r \notin R$; (b2) $r \in R$ и $\alpha \notin M_r$.

В случае (b1) по определению 1-совершенного кода имеется ровно один вектор $\widetilde{x} \in \widetilde{R}$, что $d(\widetilde{r}, \widetilde{x}) = 1$. Без ограничения общности можно считать, что вектора $\widetilde{r}, \widetilde{x} \in Q_2^{m-1}$ различаются в 1-й координате. Тогда имеется ровно k таких векторов $x^i \in Q_2^{k(m-1)}$, $i = 1, \ldots, k$, что $\widetilde{x}^i = \widetilde{x}$ и вектора r и x^i отличаются в i-й координате. Пусть $i = 1$, $x_1^1 = 1$, $r_1 = 0$. По определению МДР-кода найдутся такие $\beta_1 \in Q_4$, что $(\beta_1, \alpha_2, \ldots, \alpha_{km}) \in M_{x^1}$, и вершина $(v_1, v_2, v_3, v_4) \in C_{\beta_1}^1$, находящаяся на расстоянии 1 от вершины $(u_1, u_2, u_3, u_4) \in C_{\alpha_1}^0$. Тогда $d(u, v^1) = 1$, где $v^1 = (v_1, v_2, v_3, v_4, u_5, \ldots, u_n) \in S$. Аналогично определяются вершины $v^i \in S$, соответствующие векторам x^i при $i = 1, \ldots, k$.

В случае (b2) для каждого $i \in \{k(m-1)+1, \ldots, km\}$ по определению МДР-кода M найдётся ровно одно $\beta_i \in Q_4$, что $(\alpha_1, \ldots, \alpha_{i-1}, \beta_i, \alpha_{i+1}, \ldots, \alpha_{km}) \in M$. При $\alpha_i \neq \beta_i$ для любой вершины из C_{α_i} найдётся единственная вершина из C_{β_i}, находящаяся на расстоянии 1.

Докажем (c). Известно, что

$$|\widetilde{R}| = 2^{m-s+1}, |R| = |\widetilde{R}| 2^{(k-1)(m-1)} \text{ и } |M_{\widetilde{r}}| = 4^{km-1}. \tag{2.7}$$

Из (2.6) имеем равенство

$$|S| = |C_0|^{km} |R| |M_r| = 2^{km} \cdot 2^{m-s+1} \cdot 4^{km-1} \cdot 2^{(k-1)(m-1)} = 2^{n-s}.$$

▲

Оценим число $N_{pc}(k,s)$ совершенных 2-раскрасок с параметрами (2.5), вычислив сколько из них могут быть получены с помощью конструкции (2.6). Следующая теорема является обобщением следствия 27 на случай $k > 1$.

Теорема 37 ([50]). $N_{pc}(k,s) \geq 2^{2^{k(2^{s-1}-1)-s+1}} \cdot 3^{k2^{k(2^{s-2}-1)}} \cdot 2^{2^{k(2^{s-2}-1)-s+2}}$.

Доказательство. Для любого $u \in Q_{\alpha,r}$ наборы $\alpha \in Q_4^{km}$ и $r \in Q_2^{k(m-1)}$ определяются единственным образом. Тогда по совершенной раскраске χ^S, удовлетворяющей равенству (2.6), можно однозначно восстановить множество R и МДР-коды M_r. Отсюда вытекает оценка $N_{pc}(k,s) \geq \#R(\#M)^{|R|}$, где $\#R$ — число совершенных кодов в Q_2^{m-1}, а $\#M$ — число МДР-кодов в Q_4^{km}.

Из предложения 62 имеем неравенства $3^{km}2^{2^{(km-1)}+1} \leq \#M \leq (3^{km}+1)2^{2^{(km-1)}+1}$ при $km \geq 5$. Тогда из (2.7) получаем неравенство

$$N_{pc}(k,s) \geq \left(3^{km}2^{2^{(km-1)}+1}\right)^{2^{k(m-1)-s+2}} = 2^{2^{k(2^{s-1}-1)-s+1}} \cdot 3^{k2^{k(2^{s-2}-1)}} \cdot 2^{2^{k(2^{s-2}-1)-s+2}}.$$

▲

§ 2.1.7. Свитчинговая эквивалентность совершенных кодов

i-Компонентой совершенного кода $C \subset Q_2^n$ называется такое подмножество $K \subset C$, что множество D, полученное из C инверсией i-й координаты во всех двоичных наборах из подмножества K, является совершенным кодом. При этом говорят, что код D получен из C *свитчингом* i-компоненты K. Будем говорить, что совершенные коды A и B *свитчинговo эквивалентны*, если один получается из другого конечным числом последовательных свитчингов i-компонент, где номера i, $i \in \{1,\ldots,n\}$, могут быть различными для разных свитчингов.

Справедливость следующего утверждения вытекает непосредственно из определений.

Предложение 160. *Пусть совершенный код $C \subset Q_2^{4m+3}$ удовлетворяет равенству (2.6) и m-арная квазигруппа $f_{\overline{r}} = F_{m+1}\langle M_{\overline{r}}\rangle$, $\overline{r} \in R$, имеет $\{a,b\}$-компоненту S. Тогда множество*

$$K = \bigcup_{\overline{a} \in S} C_{a_1}^{r_1} \times C_{a_2}^{r_2} \times \cdots \times C_{a_m}^{r_m} \times C_{f_r(a)}$$

является i-компонентой совершенного кода C, где $i = a \oplus b \in \{1, 2, 3\}$. При этом свитчинг $\{a, b\}$-компоненты S в квазигруппе $f_{\overline{r}}$ равносилен свитчингу i-компоненты в коде C.

Доказательство. Множества C_a и C_b определены так, что они получаются друг из друга инверсией в i-й координате, где $i = a + b$ и $\oplus$ групповая операция в $Z_2 \times Z_2$. Поэтому замена значений $a \leftrightarrow b$ в мультиарной квазигруппе $f_{\overline{r}}$ приводит к инверсии i-й координаты в соответствующем множестве слов. ▲

Следующее утверждение широко известно.

Предложение 161 (см., например,[35]). *Два линейных 1-совершенных кода одной и той же длины свитчингово эквивалентны.*

Ключевую роль в доказательстве последующей теоремы играет теорема 8, которая гласит: *любые две n-арные квазигруппы порядка 4 можно преобразовать друг в друга последовательными свитчингами $\{0, 1\}$-, $\{0, 2\}$- и $\{2, 3\}$-компонент.*

Теорема 38 ([35]). *Все 1-совершенные коды фиксированной длины и ранга, не больше чем на 2 превосходящего ранг линейного 1-совершенного кода той же размерности, свитчингово эквивалентны между собой.*

Доказательство. Теорема 33 сводит доказательство теоремы к рассмотрению кодов вида (2.1). Из теоремы 8 следует, что любой код вида (2.1) можно преобразовать в любой другой код вида (2.1), в том числе линейный (соответствующий линейному МДР-коду), последовательными свитчингами $\{0, 1\}$-, $\{0, 2\}$- и $\{2, 3\}$-компонент в n-арных квазигруппах $f_{\overline{r}}$, $\overline{r} \in R$. По предложению 160 любое такое преобразование суть свитчинг i-компоненты результирующего совершенного кода, $i \in \{0 + 1, 0 + 2, 2 + 3\} = \{1, 2\}$. Любые линейные 1-совершенные коды свитчингово эквивалентены по предложению 161. ▲

§ 2.2. Преобразование Фурье

§ 2.2.1. Корреляционно-иммунные функции

Будем рассматривать множество Q_q как группу со сложением по $\mod q$ и гиперкуб Q_q^n как абелеву группу $Q_q \times \cdots \times Q_q$. Для $x, y \in Q_q^n$ определим внутреннее произведение

$$\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n \mod q.$$

Количество неулевых элементов в наборе $y \in Q_q^n$ называется *весом набора* и обозначается через $wt(y)$.

Множество функций $f : Q_q^n \to \mathbb{C}$ будем рассматривать как векторное пространство $\mathbb{V}$ над полем со скалярным произведением

$$(f, g) = \frac{1}{q^n} \sum_{x \in Q_q^n} f(x)\overline{g(x)}.$$

Пусть $\xi = e^{2\pi i/q}$. *Характером* группы Q_q^n называется $\phi_z \in \mathbb{V}$, где $\phi_z(x) = \xi^{\langle x,z \rangle}$, $z \in Q_q^n$. При $q = 2$ можно рассматривать векторное пространство над $\mathbb{R}$ или $\mathbb{Q}$, поскольку $\xi = -1$.

Непосредственно из определения характера нетрудно вывести следующие равенства.

Предложение 162. 1) $\phi_z \cdot \phi_y = \phi_{z+y}$;

2) $\sum\limits_{j=0}^{q-1} \xi^{kj} = 0$ *при* $k \neq 0 \mod q$;

3) $\sum\limits_{x \in Q_q^n} \xi^{\langle x,z \rangle} = 0$ *при* $z \neq \overline{0}$.

Из предложения 162 получаем

Предложение 163. *Характеры образуют ортонормированный базис в* $\mathbb{V}$.

Преобразованием Фурье вектора f называется $\widehat{f}(z) = (f, \phi_z)$. Тогда

$$f(x) = \sum_{z \in Q_q^n} \widehat{f}(z)\phi_z(x) = \sum_{z \in Q_q^n} \widehat{f}(z)\phi_x(z) = q^n(\widehat{f}, \overline{\phi_x}). \tag{2.8}$$

Следовательно, справедливо равенство $\widehat{\widehat{f(x)}} = \frac{1}{q^n} f(-x)$.

В любом евклидовом пространстве справедливо *равенство Парсеваля*:

$$\frac{1}{q^n}\sum_{x\in Q_q^n}|f(x)|^2=(f,f)=\sum_{z\in Q_q^n}|\widehat{f}(z)|^2. \tag{2.9}$$

Напомним, что функция $f:Q_q^n\to\{0,\dots,k\}$ называется корреляционно-иммунной порядка $n-m$, если для любого $a\in\{0,\dots,k\}$ величина $|f^{-1}(a)\cap\Gamma|$ не зависит от выбора m-мерной грани Γ. Обозначим через $\mathrm{cor}(f)$ максимальный порядок иммунности функции f.

Постоянная функция Q_q^n имеет максимальный порядок иммунности n, линейная функция $f(x_1,\dots,x_n)=x_1+\dots+x_n \mod q$ имеет порядок иммунности $\mathrm{cor}(f)=n-1$.

Известно, что максимальный порядок иммунности характеризуется значениями коэффициентов Фурье. А именно, справедливы

Предложение 164 (см. [63, 38]). *Если f — корреляционно-иммунная функция порядка m, тогда $\widehat{f}(z)=0$ при $0<wt(z)\le m$.*

Доказательство. Рассмотрим $z=(z',\overline{0})$, $wt(z')\le m$.

$$\widehat{f}(z)=\frac{1}{q^n}\sum_{x\in Q_q^n}f(x)\overline{\phi_z(x)}=\frac{1}{q^n}\sum_{x'}(\xi^{-\langle x',z'\rangle}\sum_{x''}f(x)\xi^{-\langle x'',\overline{0}\rangle})=$$

$$=\frac{const}{q^n}\sum_{x'}\xi^{-\langle x',z'\rangle}=0.$$

▲

Предложение 165. *Если $f\in\mathbb{V}$ такова, что $\widehat{f}(z)=0$ при $0\le wt(z)\le m$. Тогда $\sum\limits_{x\in\Gamma}f(x)=0$ для любой грани Γ размерности $n-m$.*

Доказательство. $f(x)=\sum\limits_{wt(z)>m}\widehat{f}(z)\phi_z(x)$. Если $wt(z)>m$, то $\sum\limits_{x\in\Gamma}\phi_z(x)=0$ для любой грани Γ размерности $n-m$. ▲

Предложение 166 (см. [63, 38]). *Если $f:Q_q^n\to\{0,1\}$ и $\widehat{f}(z)=0$ при $0<wt(z)\le m$, то f — корреляционно-иммунная функция порядка m.*

Доказательство. Из предложения 165 следует, что величина $\sum\limits_{x\in\Gamma}f(x)$ не зависит от выбор грани Γ размерности $n-m$. Следовательно, число единиц функции во всех таких гранях одинаково. ▲

Определим *свёртку* двух функций $f, g \in \mathbb{V}$ равенством $f*g(z) = \sum\limits_{x \in Q_q^n} f(x)g(z-x)$. Из определений имеем равенства

Предложение 167. 1) $f * g = g * f$;

2) $Mf = \chi^{L_1(\overline{0})} * f$, *где* M — *матрица смежности гиперкуба* Q_q^n;

3) $\widehat{f * g} = q^n \widehat{f} \cdot \widehat{g}$.

Для булевых функций введём обозначение $\sigma_f(x) \stackrel{def}{=} (-1)^{f(x)}$. Числа $\widehat{\sigma_f}(v)$, $v \in Q_2^n$, называются *коэффициентами Уолша — Адамара* булевой функции f.

Корреляционно-иммунные функции можно описать в терминах коэффициентов Уолша — Адамара. Из предложений 164 и 165 имеем

Предложение 168. *Булева функция* $f = \chi^S$ *является корреляционно-иммунной порядка* m *тогда и только тогда, когда* $\widehat{\sigma_f}(v) = 0$ *при любых* $v \in Q_2^n$ *таких, что* $0 < wt(v) \leq m$.

Булеву функцию $f : Q_2^n \to \{0,1\}$ называют *уравновешенной*, если $|f^{-1}(0)| = |f^{-1}(1)|$.

Из предложения 167 (3) имеем

Предложение 169. *Для любой булевой функции* $f : Q_2^n \to Q_2$ *справедливо равенство* $\widehat{\sigma_f} * \widehat{\sigma_f} = \delta$, *где* $\delta(\overline{0}) = 1$ *и* $\delta(x) = 0$ *при* $x \neq \overline{0}$.

Доказательство. $\widehat{\widehat{\sigma_f} * \widehat{\sigma_f}} = 2^n \frac{\sigma_f}{2^n} \frac{\sigma_f}{2^n} = \frac{1}{2^n} e$, где e — функция всюду равная 1. Применяя преобразование Фурье к равенству $\delta = \widehat{e}$ имеем $\widehat{\delta} = \frac{1}{2^n} e$. ▲

Следующая гипотеза была высказана Ю.В.Таранниковым и доказана Д.Г.Фон-Дер-Флаассом. Ниже приводится доказательство, предложенное А.В.Халявиным [71].

Теорема 39 ([113]). *Пусть функция* $f : Q_2^n \to \{0,1\}$ *не уравновешенная и не константная (т.е.* $|f^{-1}(0)|, |f^{-1}(1)| \neq 0$*). Тогда* $\mathrm{cor}(f) < \frac{2n}{3}$.

Доказательство. Поскольку f не уравновешенная, имеем $\widehat{\sigma_f}(\overline{0}) \neq 0$. Пусть $\widehat{\sigma_f}(z) = 0$ при $0 < wt(z) \leq \frac{2n}{3} = m$. Рассмотрим $y \in Q_2^n$, $wt(y) > m$. Из предложения 169 имеем $0 = \widehat{\sigma_f} * \widehat{\sigma_f}(y) = \sum\limits_z \widehat{\sigma_f}(z)\widehat{\sigma_f}(y-z) = \widehat{\sigma_f}(\overline{0})\widehat{\sigma_f}(y)$, поскольку как минимум один из весов $wt(z)$ и $wt(y-z)$ всегда не превосходит m. Тогда $\widehat{\sigma_f}(y) = 0$, следовательно f — постоянная функция. Пришли к противоречию. ▲

§ 2.2.2. Характеризация совершенных 2-раскрасок

Следующие утверждения обеспечивают характеризацию совершенных 2-раскрасок в терминах коэффициентов Фурье.

Предложение 170. *Характеры $\phi_z(x)$ являются собственными векторами матрицы смежности куба Q_q^n с собственными числами $(n - wt(z))(q-1) - wt(z)$.*

Доказательство.

$$M\phi_z(x) = \sum_{y,d(x,y)=1} \xi^{\langle y-x,z\rangle+\langle x,z\rangle} = \xi^{\langle x,z\rangle} \sum_{j=1}^{n} \sum_{k\neq 0} \xi^{kz_j} =$$

$$= ((n - wt(z))(q-1) - wt(z))\phi_z(x).$$

▲

Предложение 171. *Пусть $f : Q_q^n \to \{0,1\}$ — совершенная раскраска с матрицей параметров $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Тогда $f - \frac{b}{c+b}$ есть собственная функция матрицы смежности булева куба Q_q^n с собственным числом $n(q-1) - (b+c)$.*

Предложение 171 нетрудно доказать непосредственной проверкой.

Предложение 172 (см. [63]).

1) *Если $f : Q_q^n \to \{0,1\}$ — совершенная раскраска с матрицей параметров $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, то $\widehat{f}(z) = 0$ при $wt(z) \neq 0, \frac{b+c}{q}$.*

2) *Если $\widehat{f}(z) = 0$ при $wt(z) \neq 0, s$ для некоторой функции $f : Q_q^n \to \{0,1\}$, то f — совершенная 2-раскраска.*

Доказательство. Пункт 1) следует из предложений 163, 170 и 171. Докажем пункт 2). Функция $g = f + t$ является собственным вектором матрицы смежности гиперкуба Q_q^n для некоторой константы $t \in \mathbb{Q}$. Пусть $g(x) = t$ и $b(x) = |L_1(x) \cap g^{-1}(1+t)|$. Тогда $b(x)(1+t) + (n(q-1) - b(x))t = \lambda t$, где λ — собственное число соответствующее характерам ϕ_z, $wt(z) = s$. Таким образом, число $b(x)$ не зависит от выбора $x \in Q_q^n$. ▲

Из утверждений 166 и 172 имеем

Следствие 29. *Пусть* $f : Q_q^n \to \{0,1\}$ *— совершенная 2-раскраска с матрицей параметров* $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. *Тогда* $\mathrm{cor}(f) = \frac{c+b}{q} - 1$.

Из доказательства теоремы 40 видно, что если не уравновешенная булева функция имеет максимально возможную корреляционную иммунность, то её преобразование Фурье имеет ненулевые значения только в точках фиксированного веса. Тогда, используя предложение 172, получаем следующую теорему

Теорема 40 ([113]). *Пусть* $f : Q_2^n \to \{0,1\}$ *корреляционно-иммунная функция порядка* $\mathrm{cor}(f) = \frac{2n}{3} - 1$. *Тогда* f *— совершенная раскраска.*

Известны достигающие границы $\mathrm{cor}(f) = \frac{2n}{3} - 1$ совершенные 2-раскраски в булевых кубах размерности 3 и 6 с параметрами: $\begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 5 \\ 3 & 3 \end{pmatrix}$.

С помощью конструкции удвоения (предложение 142) можно построить совершенные раскраски, достигающие этой границы, в гиперкубах сколь угодно большой размерности. Пусть $f : Q_q^n \to \{0,1\}$, будем называть *плотностью* булевой функции величину $\rho(f) = \frac{|\{x \in Q_q^n \mid f(x)=1\}|}{q^n}$. Определим число $\alpha(f)$ как среднее число единиц функции f, находящихся на расстоянии 1 от некоторого нуля функции f, т. е. $\alpha(f) = \frac{1}{q^n - |S|} \sum\limits_{x \notin S} |\{y \in S \mid d(x,y) = 1\}|$, где $S = f^{-1}(1)$.

Теорема 41 ([172]).

(a) *Для любой булевозначной функции* $f : Q_q^n \to \{0,1\}$ *справедливо неравенство* $\rho(f)q(\mathrm{cor}(f)+1) \le \alpha(f)$.

(b) *Булевозначная функция* f *является совершенной* 2*-раскраской тогда и только тогда, когда* $\rho(f)q(\mathrm{cor}(f)+1) = \alpha(f)$.

Доказательство. Из определений и основных свойств преобразования Фурье имеем следующие равенства.

$$\sum_z |(f, \phi_z)|^2 = \frac{1}{q^n} \sum_{x \in Q_q^n} |f(x)|^2 = \rho(f). \tag{2.10}$$

$$(f, \phi_{\overline{0}}) = \frac{1}{q^n} \sum_{x \in Q_q^n} f(x) = \rho(f). \tag{2.11}$$

$$(Mf, f) = \frac{1}{q^n} \sum_{x \in Q_q^n} \sum_{y, d(x,y)=1} f(x)\overline{f(y)} = \mathrm{nei}(f)\rho(f), \tag{2.12}$$

где $\mathrm{nei}(f) = \frac{1}{|S|} \sum\limits_{x \in S} |\{y \in S \mid d(x,y) = 1\}|$, $S = f^{-1}(1)$.

$$(Mf, f) = \sum_{z \in Q_q^n} (n(q-1) - wt(z)q)|(f, \phi_z)|^2. \tag{2.13}$$

Из (2.10–2.13) и предложения 164 получаем неравенство

$$\mathrm{nei}(f)\rho(f) = \rho(f)^2 n(q-1) + \sum_{z, wt(z) \geq \mathrm{cor}(f)+1} (n(q-1) - wt(z)q)|(f, \phi_z)|^2.$$

Поскольку $\sum\limits_{z, wt(z) \geq \mathrm{cor}(f)+1} |(f, \phi_z)|^2 = \rho(f) - \rho(f)^2$, имеем

$$\mathrm{nei}(f)\rho(f) \leq \rho(f)^2 n(q-1) + (n(q-1) - (\mathrm{cor}(f)+1)q)(\rho(f) - \rho(f)^2)$$

$$(\mathrm{cor}(f)+1)q(1-\rho(f)) \leq n(q-1) - \mathrm{nei}(f). \tag{2.14}$$

Подставим функцию $\overline{f} = f \oplus 1$ вместо функции f в неравенство (2.14). Поскольку $\mathrm{cor}(f) = \mathrm{cor}(\overline{f})$, $1 - \rho(\overline{f}) = \rho(f)$ и $n(q-1) - \mathrm{nei}(\overline{f}) = \alpha(f)$, получаем пункт (a) теоремы.

Кроме того, равенство

$$(\mathrm{cor}(f)+1)q(1-\rho(f)) = n(q-1) - \mathrm{nei}(f) \tag{2.15}$$

выполнено тогда и только тогда, когда $(f, \phi_z) = 0$ для любого набора z, удовлетворяющего неравенству $wt(z) \geq \mathrm{cor}(f) + 2$. Тогда из предложения 172 получаем, что f является совершенной 2-раскраской.

Из предложения 172 и следствия 29 следует, что любая совершенная 2-раскраска удовлетворяет равенству (2.15). Как замечено выше, равенство (2.15) эквивалентно равенству в пункте (b) теоремы. ▲

Поскольку $\mathrm{nei}(S) \geq 0$, из неравенства (2.14) следует неравенство Бирбрауэра — Фридмана (предложение 124)

$$\rho(f) \geq 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}.$$

Частным случаем теоремы 41 является

Теорема 42. *Булева функция f является характеристической функцией 1-совершенного кода тогда и только тогда, когда* $\mathrm{cor}(f) = \frac{n-1}{2}$, $\rho(f) = \frac{1}{n+1}$.

Необходимость в теореме 42 была доказана П.Дельсартом [103] в булевом и А.К.Пулатовым [58] в произвольном случае, а достаточность — П.Остергардом, О.Поттоненом и К.Т.Фелпсом [168].

§ 2.2.3. Верхняя оценка числа совершенных раскрасок

Граф называется *антиподальным*, если для каждой его вершины найдётся единственная вершина, находящаяся на максимальном расстоянии[5] от исходной. Такую вершину называют *антиподальной* исходной вершине. Булев гиперкуб ΓQ_2^n является анитиподальным графом. Вершины $x, y \in Q_2^n$ антиподальны, когда $x \oplus y = \overline{1}$.

Из следствия 22 имеем

Предложение 173. *В зависимости от матрицы параметров для любой совершенной 2-раскраски булева гиперкуба либо все пары антиподальных вершин имеют одинаковый цвет, либо все пары антиподальных вершин имеют различный цвет.*

Следующая теорема была вначале доказана С.В.Августиновичем для 1-совершенных кодов, а затем обобщена на совершенные раскраски дистанционно-регулярных графов. Здесь мы сформулируем её применительно к совершенным 2-раскраскам булева гиперкуба.

Теорема 43 ([1]). *Пусть f_1 и f_2 — совершенные 2-раскраски гиперкуба Q_2^n. Пусть $f_1|_{L_{(n-1)/2}(\overline{0})} = f_2|_{L_{(n-1)/2}(\overline{0})}$ (n — нечётно) или $f_1|_{L_{n/2}(\overline{0})} = f_2|_{L_{n/2}(\overline{0})}$ (n — нечётно). Тогда $f_1 = f_2$.*

Доказательство. Рассмотрим случай, когда n — нечётно. Из предложения 173 следует, что $f_1|_{L_{(n+1)/2}(\overline{0})} = f_2|_{L_{(n+1)/2}(\overline{0})}$. Тогда функция

$$f(x) = \begin{cases} f_1(x) & \text{при } wt(x) < n/2; \\ f_2(x) & \text{при } wt(x) > n/2. \end{cases}$$

[5] Расстояние в графе определяется как минимальное количество рёбер в пути, соединяющем вершины.

Является совершенной 2-раскраской по определению. Но из предложения 173 имеем

$$f_2|_{wt(x)<n/2} = f|_{wt(x)<n/2} = f_1|_{wt(x)<n/2},$$

и

$$f_1|_{wt(x)>n/2} = f|_{wt(x)>n/2} = f_2|_{wt(x)>n/2}.$$

Случай чётного n рассматривается аналогично. ▲

Отсюда сразу следует верхняя оценка $2^{2^{\binom{n}{(n-1)/2}}}$ (или $2^{2^{\binom{n}{n/2}}}$) числа совершенных 2-раскрасок булева n-мерного куба. Для совершенных 2-раскрасок f булева n-мерного куба с $\mathrm{cor}(f) > n/2$ эту оценку можно усилить.

Как и ранее через $N_{pc}(k,s)$ обозначаем число различных совершенных 2-раскрасок с матрицей параметров $\begin{pmatrix} 0 & k(2^s-1) \\ k & k(2^s-2) \end{pmatrix}$. При минимальном значении $s = 1$ совершенная раскраска с такой матрицей параметров является счётчиком чётности и $N_{pc}(k,s) = 2$.

Для двоичных векторов $x, y \in Q_2^n$ удобно определить операцию $[x,y] = (x_1y_1, \ldots, x_ny_n)$ Тогда каждому набору $y \in Q_2^n$ можно поставить в соответствие грань $E_y^n(z) = \{x \in Q_2^n : [x,y] = [z,y]\}$ размерности $n - wt(y)$. Докажем верхнюю оценку на число совершенных 2-раскрасок n-мерного булева куба. Идея доказательства этой оценки взята из [69].

Теорема 44 ([50]). *Пусть $N_{pc}(k,s)$ — число различных совершенных раскрасок с матрицей параметров $\begin{pmatrix} 0 & k(2^s-1) \\ k & k(2^s-2) \end{pmatrix}$. Тогда $\ln N_{pc}(k,s) \le 2^{k2^s-2k-s}k^2(k+s)(1+o(1))$ при $n = k(2^s-1) \to \infty$.*

Доказательство. Пусть $f = \chi^S$ — совершенная 2-раскраска с матрицей параметров $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$. Вычислив количество пар соседних вершин разных цветов (0 и 1), нетрудно видеть, что $|S| = \frac{c}{b+c}2^n$. Отметим, что $b + c = c'2^t$, где c' — нечётный делитель числа c. Определим функцию $a(u) = \begin{cases} b2^n & \text{при } u \in S; \\ -c2^n & \text{при } u \notin S, \end{cases}$ т. е. $a = 2^n(b\chi^S - c(1-\chi^S)) = (b+c)2^nf - 2^nc$. Тогда $\widehat{a}(\overline{0}) = 0$ по построению. Из предложения 172 и определения функции a имеем равенство $\widehat{a}(v) = 0$ для любых

$v \in Q_2^n$ веса $wt(v) \neq 0, \frac{b+c}{2}$. Из равенства Парсеваля (2.9) имеем

$$\sum_{wt(v)=\frac{b+c}{2}} \widehat{a}^2(v) = 2^n \left(b^2 \frac{c}{b+c} 2^n + c^2 \frac{b}{b+c} 2^n \right). \tag{2.16}$$

Зафиксируем вершину $w \in Q_2^n$, $wt(w) = (b+c)/2$ и возьмём содержащую $\overline{0}$ грань E размерности $l = n - (b+c)/2$, т. е. $E = E_w^n(\overline{0}) = \{x \in Q^n \mid [x, w] = \overline{0}\}$. Ясно, что скалярное произведение векторов $\phi_v(u) = (-1)^{\langle u,v \rangle}$ и χ^E в $\mathbb{V}$ равно 0, если $v \neq w$ и $wt(v) = (b+c)/2$. Рассмотрим скалярное произведение векторов a и χ^E в $\mathbb{V}$. Из формулы обращения (2.8) имеем

$$\widehat{a}(w) 2^{l-n} = (a(u), \chi^E(u)) = bm(w) - c(2^l - m(w)) = (b+c)m(w) - c2^l, \tag{2.17}$$

где $m(w) = |S \cap E_w^n(\overline{0})|$. Очевидно, что числа $\widetilde{a}(w) = \widehat{a}(w) 2^{l-n-t}$ целые для любой вершины $w \in Q_2^n$, $wt(w) = (b+c)/2$. Из (2.16) имеем

$$\sum_{wt(v)=\frac{b+c}{2}} \widetilde{a}^2(v) = 2^{2l-2t} \left(b^2 \frac{c}{b+c} + c^2 \frac{b}{b+c} \right) = 2^{2l-2t} bc.$$

Подставляя в это равенство $n = b = k(2^s - 1)$, $l = n - k2^{s-1}$, $c = k$, $t = s$, получаем

$$\sum_{wt(v)=k2^{s-1}} \widetilde{a}^2(v) = 2^{k(2^s-2)-2s} k^2 (2^s - 1). \tag{2.18}$$

Оценим мощность $N(M, R)$ множества целочисленных наборов $\{(\alpha_1, \ldots, \alpha_M) \mid \sum\limits_{i=1}^{M} \alpha_i^2 = R\}$ при $R \leq M$. Нетрудно видеть, что $N(M, R) \leq \binom{M}{R} C^R$, где C — некоторая константа. Применяя асимптотическое равенство $\ln \binom{M}{R} = R \ln \frac{M}{R} (1 + o(1))$, получаем что $\ln N(M, R) = R \ln \frac{M}{R} (1 + o(1))$ при $\frac{M}{R} \to \infty$. Тогда из равенства (2.18) заключаем, что

$$\ln N_{pc}(k, s) \leq 2^{k2^s - 2k - s} k^2 (k+s)(1 + o(1))$$

при $n = k(2^s - 1) \to \infty$.▲

В частности, при $s = 2$ из теоремы 44 вытекает следующая оценка на число совершенных раскрасок $\log \log N_{pc}(k, s) \leq \frac{2n}{3}(1 + o(1))$ при $3k = n \to \infty$.

§ 2.3. Компоненты совершенных 2-раскрасок и бент-функций

§ 2.3.1. Алгебраическая степень совершенных раскрасок и корреляционно-иммунных функций

Расстояние между булевыми функциями f и g определяется как $d(f,g) = |\{x \in Q_2^n : f(x) \neq g(x)\}|$. Булевы функции в Q_2^n при чётном n, находящиеся на максимальном расстоянии от множества аффинных функций, называются *бент-функциями*.

Пусть $S_1 \subset Q_2^n$ и функция χ^{S_1} является совершенной 2-раскраской, корреляционно-иммунной функцией или бент-функцией. Напомним, что множество $S_1 \setminus S_2$ называется компонентой совершенной раскраски (корреляционно-иммунной функции, бент-функции) χ^{S_1}, если существует совершенная раскраска (корреляционно-иммунная функция, бент-функция) χ^{S_2} с теми же параметрами (в случае корреляционно-иммунной функции — того же порядка и веса). Компоненту $S_2 \setminus S_1$ функции χ^{S_2} будем называть *альтернативной* к компоненте $S_1 \setminus S_2$. Объединение двух альтернативных компонент, т. е. симметрическую разность $S_1 \triangle S_2$ будем называть *двойной компонентой*.

Множество $S \subset Q_2^n$ и его характеристическую функцию χ^S будем называть *унитрейдом порядка*[6] $n-m$, если для любой грани Γ размерности m мощность пересечения $\Gamma \cap S$ чётная (возможно равна нулю). Отметим, что корреляционно-иммунная функция порядка $n-m$ является унитрейдом порядка $n-m-1$.

Каждая булева функция $f : Q_2^n \to Q_2$ может быть представлена в виде *многочлена Жегалкина* (в *алгебраической нормальной форме*)

$$f(x_1,\dots,x_n) = \bigoplus_{y \in Q_2^n} G[f](y) x_1^{y_1} \dots x_n^{y_n},$$

где $a^0 = 1, a^1 = a$, $G[f] : Q_2^n \to Q_2$ — булева функция.

Алгебраической степенью булевой функции f называется максимальная степень слагаемого в её многочлене Жегалкина, т. е. $\deg f = \max\limits_{G[f](y)=1} wt(y)$. Алгебраической

[6] В [53] унитрейды назывались битрейдами.

степенью множества $S \subset Q_2^n$ будем называть алгебраическую степень его характеристической функции.

Справедливо следующее

Предложение 174 (см. [63, 38]). *Для любой булевой функции f верно равенство* $G[f](y) = \bigoplus\limits_{x \in Q_2^n, [x,y]=x} f(x)$.

Поскольку $f(x) = \bigoplus\limits_{y \in Q^n, [x,y]=y} G[f](y)$, имеем равенство $G[G[f]] = f$ для любой булевой функции f.

Из предложения 174 непосредственно следует

Предложение 175. *Булева функция $f : Q_2^n \to Q_2$ является унитрейдом порядка $n - m$ тогда и только тогда, когда* $\deg f \leq m - 1$.

Пусть $S_1, S_2 \subset Q^n$ и корреляционно-иммунные функции χ^{S_1}, χ^{S_2} имеют порядок $n - m$ и одинаковый вес. Ясно, что множество S_1 является унитрейдом порядка $n - m - 1$, а двойная компонента $S_1 \triangle S_2$ является унитрейдом порядка $n - m$. Таким образом, из предложения 175 получаем

Предложение 176. *Пусть $f : Q_2^n \to Q_2$ — корреляционно-иммунная функция порядка $n - m$. Тогда*

(a) $\deg(f) \leq m$ *(неравенство Зигенталера* [181]*);*

(b) *алгебраическая степень двойной компоненты корреляционно-иммунной функции f не превосходит $m - 1$.*

Замечание 16. *Если корреляционно-иммунная функция f порядка $n - m$ имеет чётное число единиц в каждой грани размерности m, то f является унитрейдом порядка $n - m$. Тогда из предложения 175 имеем* $\deg f \leq m - 1$.

Поскольку совершенная 2-раскраска с матрицей параметров

$$\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix} \tag{2.19}$$

является корреляционно-иммунной функцией порядка $\frac{b+c}{2} - 1$ (см. следствие 29), из предложения 176 вытекает

Следствие 30. *Пусть $f : Q_2^n \to Q_2$ — совершенная раскраска с матрицей параметров* (2.19). *Тогда*

(a) $\deg(f) \le n - \frac{b+c}{2} + 1$;

(b) *алгебраическая степень двойной компоненты совершенной раскраски f не превосходит* $n - \frac{b+c}{2}$.

Поскольку количество мономов степени не более m равняется $\sum\limits_{i=0}^{m} \binom{n}{i}$, из следствия 30 имеем верхнюю оценку числа совершенных раскрасок.

Следствие 31. *Число совершенных раскрасок с матрицей параметров* $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$ *не превышает* $2^{\sum\limits_{i=0}^{m} \binom{n}{i}}$, *где* $m = n - \frac{b+c}{2} + 1$.

Из следствия 31 для числа 2-раскрасок с матрицей параметров $\begin{pmatrix} 0 & k(2^s-1) \\ k & k(2^s-2) \end{pmatrix}$ имеем оценку

$$\log N_{pc}(k,s) \le 2^{nh\ \frac{2^{s-1}-1}{2^s-1}\ (1+o(1))} \tag{2.20}$$

при $s \ge 2$, $n = k(2^s-1) \to \infty$, где $h(p) = -p\log p - (1-p)\log(1-p)$ — энтропия Шеннона.

Оценка (2.20) может быть переписана в виде $\log\log N_{pc}(k,s) \le nh(\frac{1}{2}(1-\frac{k}{n}))(1+o(1))$, а оценка из теоремы 44 в виде $\log\log N_{pc}(k,s) \le n(1-\frac{k}{n})(1+o(1))$. Вторая оценка сильнее, поскольку неравенство $h(\alpha/2) > \alpha$ следует из выпуклости вверх функции $h(\alpha/2)$ при $0 < \alpha < \frac{1}{2}$.

1-Совершенный код длины n (при $n \ne 3$) является не только корреляционно-иммунной функцией порядка $\frac{n-1}{2}$, но и унитрейдом порядка $\frac{n-1}{2}$, поскольку пересекается с гранями размерности $\frac{n+1}{2}$ по одинаковому числу вершин равному 2^t, где t — целое. Из предложения 176 имеем

Следствие 32. *Пусть $C \subset Q_2^n$ — 1-совершенный код. Тогда*

(a) $\deg(\chi^C) \le \frac{n-1}{2}$ *при* $n \ne 3$;

(b) *алгебраическая степень двойной компоненты 1-совершенного кода C не превосходит* $\frac{n-1}{2}$.

Булевы функции $f : Q_2^n \to Q_2$ можно рассматривать в виде набора значений как

элементы булева гиперкуба размерности 2^n. Множество унитрейдов порядка $n-m-1$ (булевых функций алгебраической степени не выше m) называется кодом Рида — Маллера типа $\mathcal{R}(m,n)$ в $Q_2^{2^n}$. В [40] рассмотрен весовой спектр кодов Рида — Маллера и, в частности, имеются следующие утверждения.

Предложение 177 ([40], глава 13, теоремы 3 и 5). *Для любой не тождественно нулевой булевой функции $f = \chi^S$ справедливо неравенство $|S| \geq 2^{n-\deg(f)}$. Если $|S| = 2^{n-\deg(f)}$, то множество S является линейным кодом.*

Напомним, что линейным кодом называется произвольное аффиное подмножество булева куба Q_2^n, который рассматривается как векторное пространство над $GF(2)$.

Предложение 178 ([134]; [40], глава 15, теорема 10). *Пусть $f = \chi^S$ — булева функция в Q_2^n, $\deg(f) \geq 2$ и $2^{n-\deg(f)+1} > |S|$. Тогда $|S| = 2^{n-\deg(f)+1} - 2^{n-\deg(f)+1-p}$, где $p \in \{1, \ldots, \mu\}$ и $\mu = \max\{(n-\deg(f)+2)/2, \min\{n-\deg(f), \deg(f)\}\}$.*

Отметим, что в [134] и [135] перечислены (с точностью до аффинных преобразований) все булевы функции в Q_2^n, соответствующие вершинам кода $\mathcal{R}(m,n)$ в $Q_2^{2^n}$ и имеющие вес не более чем в 2.5 раза превосходящий минимальный ненулевой вес 2^{n-m}.

Из предложений 175–178 докажем

Предложение 179 ([54]). *Пусть множество $S \subset Q_2^n$ есть компонента корреляционно-иммунной функции порядка $n-m$ и $2^{n-m+1} > |S|$. Тогда $|S| = 2^{n-m+1} - 2^p$, где $p \in \{0, \ldots, n-m\}$. Более того, компонента мощности 2^{n-m} является линейным кодом.*

Доказательство. Поскольку мощность компоненты равна половине мощности двойной компоненты, из предложений 176 и 178 получаем требуемые ограничения на мощности компонент. Из предложения 177 следует, что двойная компонента $A = S \cup S'$, $|A| = 2^{n-m+1}$, корреляционно-иммунной функции порядка $n-m$ является линейным кодом. Тогда множество A пересекается с любыми гранями гиперкуба Q_2^n либо по пустому множеству, либо по множеству мощности 2^t, где t — целое. Причём непустое пересечение множества A с $(m+1)$-мерной гранью имеет мощность не менее

4. Тогда компонента S является унитрейдом порядка $n-m-1$. Из предложений 175 и 177 получаем требуемое. ▲

Замечание 17. *Компонента корреляционно-иммунной функции f порядка $n-m$ имеет алгебраическую степень не более $2\deg f$. Поэтому при $m < \frac{n}{2}$ компонента имеет чётную мощность.*

Из предложений 179 и следствий 30, 32 получаем

Следствие 33 ([54]). *Пусть f — совершенная 2-раскраска с матрицей параметров $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$, множество $S \subset Q_2^n$ есть компонента f и $2^{\frac{b+c}{2}} > |S|$. Тогда $|S| = 2^{\frac{b+c}{2}} - 2^p$, где $p \in \{0, \ldots, \frac{b+c}{2} - 1\}$. Более того, компонента мощности $2^{\frac{b+c}{2}-1}$ является линейным кодом.*

Следствие 34 ([54]). *Пусть множество $S \subset Q_2^n$ есть компонента 1-совершенного кода $C \subset Q_2^n$ и $2^{\frac{n+1}{2}} > |S|$. Тогда $|S| = 2^{\frac{n+1}{2}} - 2^p$, где $p \in \{1, \ldots, \frac{n-1}{2}\}$. Более того, компонента мощности $2^{\frac{n-1}{2}}$ является линейным кодом.*

§ 2.3.2. Компоненты совершенных 2-раскрасок и корреляционно-иммунных функций

Минимальная мощность ($2^{\frac{n-1}{2}}$) компоненты 1-совершенного кода длины n хорошо известна, линейность минимальной компоненты была доказана С. В. Августиновичем. Компоненты минимально возможной мощности имеются в любом линейном коде (коде Хэмминга). В [110] найдены все возможные мощности пересечений линейных совершенных кодов. В частности, показано, что линейные совершенные коды могут пересекаться по четверти своих вершин. Нетрудно вычислить, что мощность совершенного кода в Q_2^7 равна 2^4 и вдвое превосходит минимальную мощность компоненты. Таким образом, при $n = 7$ два линейных кода, пересекающиеся по четверти вершин, порождают компоненту мощности в 1.5 раза больше минимальной. При $n > 7$ неизвестны компоненты совершенных кодов (длины n) мощности промежуточной между $2^{\frac{n-1}{2}}$ и $2^{\frac{n+1}{2}}$. Более того, можно показать, что i-компоненты промежуточной мощности отсутствуют в совершенных кодах (при $n > 7$), имеющих ранг (размерность

аффинной оболочки) не более чем на два превосходящий ранг линейного кода. Действительно, из теоремы 33 следует, что все совершенные коды такого ранга могут быть получены конструкцией I из 4-ичных МДР-кодов. Из предложения 160 следует, что в данной конструкции компоненты 4-ичных МДР-кодов взаимно однозначно соответствуют i-компонентам совершенных кодов; в следствии 3 указано, что 4-ичные МДР-коды не имеют компонент промежуточной мощности. Ниже будут построены двукратные 1-совершенные коды с компонентами промежуточной между минимальной и удвоенной минимальной мощностью.

В предложении 27 доказано, что для любых $t \geq 3$ и $p \in \{0, \ldots, t-1\}$ существует 2-МДР-код $B_t^p \subset Q_4^t$, имеющий компоненту мощности $2^t - 2^p$.

Рассмотрим ещё одно обобщение конструкции I. Будем следовать обозначениям из § 2.1.6. Рассмотрим множество

$$S_{p,m,k} = \bigcup_{r \in R} \bigcup_{\alpha \in B_{km}^p} Q_{\alpha,r}, \qquad Q_{\alpha,r} = C_{\alpha_1}^{r_1} \times C_{\alpha_2}^{r_2} \times \cdots \times C_{\alpha_{k(m-1)}}^{r_{k(m-1)}} \times C_{\alpha_{k(m-1)+1}} \times \cdots \times C_{\alpha_{km}}, \tag{2.21}$$

где B_{km}^p — двукратный МДР-код, определённый в предложении 27.

Теорема 45 ([54]). *Пусть $p \in \{0, \ldots, km-1\}$ и множество $S_{p,m,k} \subset Q_2^n$ определено равенством* (2.21)*, тогда*

(a) $\chi^{S_{p,m,k}}$ *— совершенная раскраска с матрицей параметров*

$$\begin{pmatrix} k & k(2^s-2) \\ 2k & k(2^s-3) \end{pmatrix}, \tag{2.22}$$

где $n = (2^s-1)k$, $m = 2^{s-2}$, $s \geq 2$, $k \geq 1$, $km \geq 3$;

(b) *совершенная раскраска $\chi^{S_{p,m,k}}$ имеет компоненту мощности $(2^{km} - 2^p)2^{km}$.*

Доказательство пункта (a) теоремы 45 вполне аналогично доказательству теоремы 36. Пункт (b) следует из предложения 27.

Как было указано выше, для совершенных 2-раскрасок имеется оценка их корреляционной иммунности, зависящая только от параметров раскраски. В частности, функция $\chi^{S_{p,m,k}}$ является корреляционно-иммунной порядка $2km-1$. Пусть $f : Q_2^n \to Q_2$ — корреляционно-иммунная функция порядка i. Тогда функция $g : Q_2^{n+n'} \to Q_2$,

определённая равенством $g(x,y) = f(x) \oplus y_1 \oplus \cdots \oplus y_{n'}$, является корреляционно-иммунной порядка $i+n'$. Таким образом, из теоремы 45, подставляя $m = 1$, получаем

Следствие 35 ([54]). *Пусть $n = 3k + n'$, $r = 2k + n' - 1$, $k \geq 3$. Для любого $p \in \{0, \ldots, k-1\}$ найдётся корреляционно-иммунная функция $g : Q_2^{n+n'} \to Q_2$ порядка r, имеющая компоненту мощности $(2^k - 2^p)2^{k+n'}$.*

§ 2.4. Компоненты бент-функций и подвижные множества

Пусть $f : Q_2^n \to Q_2$ — булева функция и $w \in Q^n$. Через $wt(f_w) = |\{x \in Q^n \mid f(x) = 1, [x, 1 \oplus w] = x\}|$ будем обозначать число единиц подфункции, полученный подстановкой 0 во все такие аргументы x_i функции f, что $w_i = 1$.

Предложение 180 ([176], см. также [63]). *Для любой булевой функции $f : Q_2^n \to Q_2$ справедливо равенство*

$$\sum_{v \in Q_2^n, [v,w]=v} \widehat{\sigma_f}(v) = 2^n - 2^{wt(w)+1} wt(f_w) \quad \textit{(тождество Саркара).}$$

Из тождества Саркара нетрудно вывести следующее

Предложение 181. *Пусть f булева функция и $\widehat{\sigma_f}(v) \equiv 0 \mod 2^k$ для любого $v \in Q^n$, тогда $\deg(f) \leq n - k + 1$.*

Доказательство. Пусть $\deg(f) > n - k + 1$. Рассмотрим ненулевое слагаемое максимальной степени в многочлене Жегалкина функции f. Пусть $G[f](y) = 1$ и $wt(y) = \deg(f)$. Тогда $wt(f_{y \oplus 1}) \equiv 1 \mod 2$. Из тождества Саркара имеем

$$\sum_{v \in Q^n, [v, y \oplus 1]=v} \widehat{\sigma_f}(v) = 2^n - 2^{n-wt(y)+1} wt(f_{y\oplus 1}) \equiv 1 \mod 2^{n-wt(y)+2} \not\equiv 0 \mod 2^k.$$

▲

Из тождества Саркара и предложения 164 следует

Предложение 182 (см. [63]). *Пусть $f : Q_2^n \to Q_2$ — корреляционно-иммунная функция порядка m, $m \leq n-1$. Тогда $\widehat{\sigma_f}(v) \equiv 0 \mod 2^{m+1}$ для любого $v \in Q_2^n$.*

В работе [9] используется понятие *подвижного множества* в Q_2^n как объединения

двух кодов C_1 и C_2 с кодовым расстоянием 3, имеющих одинаковую окрестность. Определим функцию $h : Q_2^n \to \mathbb{Q}$ равенством $h = \chi^{C_1} - \chi^{C_2}$. Из определения видно, что сумма значений функции h по любому шару радиуса 1 равняется 0, т. е. функция h является 0-*центрированной*. Известно

Предложение 183 (см. [2]). *Пусть $h : Q_2^n \to \mathbb{Q}$ — 0-центрированная функция. Тогда $\widehat{h}(v) = 0$ при $wt(v) \neq \frac{n+1}{2}$.*

В частности, из этого утверждения следует, что подвижные множества имеются в булевых кубах только нечётной размерности.

Предложение 184 ([54]). *Любое подвижное множество $C \subset Q_2^n$ является унитрейдом порядка $\frac{n-1}{2}$.*

Доказательство. По определению подвижное множество C является объединением кодов C_1 и C_2 с кодовым расстоянием 3 и $h = \chi^{C_1} - \chi^{C_2}$ есть 0-центрированная функция. Подпространство пространства $\mathbb{V}$, порождённое всеми функциями f^v, где $wt(v) \leq m$, содержит характеристические функций всех граней размерности не менее $n - m$. Тогда из предложения 183 следует, что скалярное произведение (h, χ^F) равно нулю для любой грани G размерности $\frac{n+1}{2}$. Следовательно, $|C_1 \cap G| = |C_2 \cap G|$ и число $|C \cap G|$ чётное.▲

Из предложений 177, 178 и 184 имеем

Следствие 36 ([54]). *Пусть $S \subset Q_2^n$ — подвижное множество и $2^{\frac{n+3}{2}} > |S|$. Тогда $|S| = 2^{\frac{n+3}{2}} - 2^p$, где $p \in \{1, \ldots, \frac{n+1}{2}\}$. Более того, подвижное множество мощности $2^{\frac{n+1}{2}}$ является линейным кодом.*

Отметим, что построенные в предыдущем разделе пары альтернативных компонент двукратных совершенных кодов, т. е. совершенных раскрасок с матрицей параметров $\begin{pmatrix} 1 & (2^s - 2) \\ 2 & (2^s - 3) \end{pmatrix}$ являются подвижными множествами.

Предложение 185 (см., например, [65]). *Булева функция f является бент-функцией тогда и только тогда, когда $\widehat{\sigma_f}(v) = \pm 2^{n/2}$ для любого $v \in Q_2^n$ и n — чётное.*

Теорема 46 ([54]). (a) *Пусть множество $S \subset Q_2^n$ есть компонента бент-функции f и*

$2^{\frac{n}{2}} > |S|$. *Тогда* $|S| = 2^{\frac{n}{2}} - 2^p$, *где* $p \in \{0, \ldots, \frac{n}{2}-1\}$. *Более того, компонента мощности* $2^{\frac{n}{2}-1}$ *является линейным кодом.*

(b) *Для любого* $p \in \{0, \ldots, \frac{n}{2}-1\}$ *существует бент-функция* $f : Q_2^n \to Q_2$, *имеющая компоненту мощности* $2^{\frac{n}{2}} - 2^p$.

Доказательство. Подобно доказательству предложения 181 из тождества Саркара и предложения 185 нетрудно получить, что $\deg(f) \leq n/2$ для любой бент-функции f в Q_2^n (см. также [38]). Тогда пункт (a) следует из предложений 177 и 178. Построим бент-функции с компонентами требуемой мощности. Пусть $x, y \in Q_2^{n/2}$ и λ — произвольная булева функция в $Q_2^{n/2}$. Известно (см., например, [38],[65]), что булева функция $f(x, y) = \langle x, y\rangle \oplus \lambda(y)$ является бент-функцией. Тогда функции $f^1(x, y) = \langle x, y\rangle \oplus y_1 \cdots y_{n/2}$ и $f_p^2(x, y) = \langle x, y\rangle \oplus y_1 \cdots y_p x_{p+1} \cdots x_{n/2}$ являются бент-функциями, причём $wt(f^1 \oplus f_p^2) = 2^p(2^{\frac{n}{2}-p+1} - 2)$. Следовательно, бент-функция f^1 имеет компоненту мощности $2^{\frac{n}{2}} - 2^p$.▲

Свойства минимальных по мощности компонент бент-функций рассматривались в [30], [96], [97]. В частности в [30] доказано, что компонента бент-функции мощности $2^{\frac{n}{2}-1}$ является линейным кодом, а в [96] доказано, что если бент-функция аффинна на аффинном множестве размерности $n/2$, то это множество является двойной компонентой.

§ 2.5. Компоненты совершенных 2-раскрасок в q-ичном гиперкубе

Унитрейдом порядка $n - m$ в Q_q^n как и в булевом гиперкубе называется множество, пересечения которого с гранями размерности m имеют чётную мощность. В q-ичном гиперкубе при $q \neq 2$ понятие унитрейда не связано с алгебраической степенью. Докажем некоторые утверждения из предыдущих разделов для q-ичного гиперкуба без привлечения понятия алгебраической степени.

Предложение 186. *Пусть* $B \subseteq Q_q^n$ — *непустой унитрейд порядка* m, $m < n$. *Тогда* $|B| \geq 2^{m+1}$.

Доказательство. Предположим, что утверждение верно для $n = k$. Докажем его для $n = k + 1$. Пусть $|B| \geq 2$, тогда найдутся две параллельные k-мерные грани F_1, F_2, такие что их пересечения с унитрейдом непусты. Ясно, что множество $F_i \cap S$ есть унитрейд порядка $m-1$ в $(n-1)$-мерном гиперкубе F_i. По предположению индукции имеем $|F_i \cap B| \geq 2^m$ при $i = 1, 2$, следовательно, $|B| \geq 2^{m+1}$. ▲

Предположим, что функции $f = \chi^{S_1}$ и $g = \chi^{S_2}$ являются совершенными 2-раскрасками с одинаковой матрицей параметров, следовательно $\mathrm{cor}(f) = \mathrm{cor}(g)$. Ясно, что двойная компонента корреляционно-иммунной функции порядка m является унитрейдом порядка m. Из предложения 186 и следствия 29 имеем

Предложение 187 ([172]).

(a) *Пусть f — совершенная 2-раскраска с матрицей параметров* $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$. *Для любой компоненты $S \subset Q_q^n$ 2-раскраски f имеем $|S| \geq 2^{\frac{c+b}{q}-1}$.*

(b) *Пусть $C \subset Q_p^n$ — 1-совершенный код. Для любой компоненты $S \subset Q_q^n$ кода C имеем $|S| \geq 2^{\frac{n(q-1)+1}{q}-1}$.*

Заметим, что компоненты мощности $|S| = 2^{\frac{c+b}{q}-1}$ имеются в совершенных 2-раскрасках с параметрами $\begin{pmatrix} n(q-2) & n \\ n(q-1) & 0 \end{pmatrix}$, т.е. в МДР-кодах.

При $q > 2$ верхняя оценка минимальной мощности компоненты S_0 1-совершенного кода, несовпадающая с приведённой выше нижней оценкой, была получена конструктивно.

Предложение 188 ([170], [39]). *Если $q = p^r$ и p — простое число, то $|S_0| \leq p^{\frac{q^{m-1}-1}{q-1}(r(q-2)+1)}$, где $n = \frac{q^m-1}{q-1}$.*

Глава 3

Кликосочетания, блок-схемы и гамильтоновы циклы в гиперкубах

§ 3.1. Перманенты

§ 3.1.1. Двумерные перманенты

Пусть $A = \{a_{ij}\}$ — матрица размера $m \times m$. *Перманентом* матрицы A называется

$$\operatorname{per}(A) = \sum_{\sigma \in S_m} \prod_{i=1}^{m} a_{i\sigma(i)}.$$

Если A — $(0,1)$-матрица, то неравенство $\operatorname{per}(A) \neq 0$ эквивалентно наличию в матрице A диагонали из 1.

Известны следующие классические теоремы о двумерных перманентах.

Теорема 47 (теорема Холла, [121]). *Для неотрицательной матрицы A размера $m \times m$ имеем $\operatorname{per}(A) = 0$ тогда и только тогда, когда A содержит подматрицу из нулей размера $k_1 \times k_2$, где $k_1 + k_2 > m$.*

Доказательство. Применяем индукцию по m. При $m = 1$ утверждение очевидно. Возможны два случая:

1) $\max(k_1 + k_2) \leq m$. Выберем ненулевой элемент a_{ij}. Вычеркнем i-ю строку и j-й столбец. У оставшейся матрицы положительный перманент по предположению

индукции.

2) $\max(k_1 + k_2) = m + 1$. Без ограничения общности считаем, что подматрица из нулей размера $k_1 \times k_2$ находится в правом верхнем углу. Тогда матрица A имеет блочную структуру и $\operatorname{per}(A) = \operatorname{per}(A_1) \cdot \operatorname{per}(A_2)$, где A_1 имеет размер $k_1 \times k_1$, A_2 имеет размер $k_2 \times k_2$.

Пусть $\operatorname{per}(A_1) = 0$, тогда по предположению индукции A_1 имеет подматрицу из нулей размера $m_1 \times m_2$, $m_1 + m_2 > k_1$. Тогда матрица A имеет подматрицу из нулей размера $m_1 \times (k_2 + m_2)$ и $m_1 + m_2 + k_2 > m + 1$. Пришли к противоречию.

Теорема 48 (теорема Кёнига, [141]). *Если* $(0,1)$*-матрица* A *содержит* t *единиц в каждом столбце и строке, то* $\operatorname{per}(A) \neq 0$.

Доказательство. Без ограничения общности считаем, что максимальная подматрица из нулей размера $k_1 \times k_2$ находится в правом верхнем углу. Пусть A_1 левая верхняя подматрица из первых k_1 строк и $m - k_2$ столбцов. Подсчитаем число единиц в A_1 по строкам и по столбцам: $k_1 t \leq (m - k_2)t$. Тогда $k_1 + k_2 \leq m$. ▲

Рассмотрим двудольный граф G_2 с N вершинами в каждой из долей и вершины каждой доли занумеруем числами $1, 2, \ldots, N$. *Матрицей смежности* графа G_2 называется квадратная $(0,1)$-матрица $A(G_2) = (a_{ij})$ порядка N такая, что $a_{ij} = 1$, если i-я вершина первой доли смежна с j-й вершиной второй доли; в противном случае $a_{ij} = 0$. Каждому совершенному паросочетанию в графе G_2 соответствует диагональ в матрице $A(G_2)$. Из теоремы 48 имеем хорошо известное

Следствие 37. *В регулярном двудольном графе имеются совершенные паросочетания.*

Известны следующие оценки перманента неотрицательной матрицы и, следовательно, числа совершенных паросочетаний в двудольном графе.

Теорема 49 ([7]). *Для перманента* $(0,1)$*-матрицы* B *порядка* N *справедлива оценка*

$$\operatorname{per} B \leq \prod_{i=1}^{N} (r_i!)^{1/r_i},$$

где r_i *— сумма элементов* i*-й строки матрицы* B.

Из этой теоремы непосредственно следует оценка

$$\operatorname{per} A(G_2) \leq (t!)^{\frac{N}{t}} \tag{3.1}$$

для числа различных совершенных паросочетаний в t-регулярном (t-однородном) двудольном графе G_2 с $2N$-вершинами. Обозначим через $SK_2(n)$ множество совершенных паросочетаний в булевом n-мерном кубе. Тогда из (3.1) имеем неравенство

$$|SK_2(n)| \leq (n!)^{2^{n-1}/n}. \tag{3.2}$$

Квадратная матрица, состоящая из неотрицательных элементов, называется *дважды стохастической*, если суммы элементов в каждой строке и в каждом столбце этой матрицы равны 1.

В 1980 году Г. П. Егорычев [21], [22] и Д. И. Фаликман [67] доказали гипотезу Ван дер Вардена:

Теорема 50. *Перманент произвольной дважды стохастической матрицы порядка N, содержащей хотя бы два различных элемента, строго больше перманента дважды стохастической матрицы порядка N с одинаковыми элементами.*

Перманент матрицы порядка N, составленной из чисел $1/N$, равен $N!/(N^N)$. Если G_2 — t-регулярный двудольный граф, то разделив каждый элемент матрицы $A(G)$ на t получим дважды стохастическую матрицу. Поэтому при $t < N$ из теоремы 50 следует неравенство

$$\operatorname{per} A(G_2) > (N!)\left(\frac{t}{N}\right)^N. \tag{3.3}$$

Ясно, что для дважды стохастических матриц теорема 50 даёт точную оценку перманента, но для $(0,1)$-матриц неравенство (3.3) может быть усилено. А именно, справедлива

Теорема 51 ([179]). *Если G_2 является t-регулярным двудольным графом с $2N$ вершинами, $N \geq t$, то в G_2 имеется не менее*

$$\left(\frac{(t-1)^{t-1}}{t^{t-2}}\right)^N \tag{3.4}$$

различных совершенных паросочетаний.

Из формулы Стирлинга следует, что при фиксированном t и $N \to \infty$ оценка (3.4) лучше оценки (3.3).

Из неравенств (3.2) и (3.4) (или (3.3)) имеем

Следствие 38 ([22]). $\ln |SK_2(n)| = 2^{n-1}(\ln n - 1 + o(1))$ *при* $n \to \infty$.

§ 3.1.2. Многомерные перманенты

Рассмотрим G_k — *k-дольный гиперграф* с N вершинами в каждой *доле*, каждое k-ребро которого состоит из k вершин по одной из каждой доли гиперграфа. Занумеруем вершины каждой доли числами $1, 2, \ldots, N$. Определим *массив смежности* $A(G_k) = (a_{i_1 \ldots i_k})$ гиперграфа G_k равенствами $a_{i_1 \ldots i_k} = 1$, если имеется k-ребро гиперграфа G_k, состоящее из вершин с номерами $i_1, i_2, \ldots, i_k$ из 1-й, 2-й и т. д. долей соответственно; в противном случае $a_{i_1 \ldots i_k} = 0$. *Диагональю* массива $F = \{1, \ldots, N\}^k$ будем называть множество, состоящее из N попарно различных во всех координатах элементов F. При $k = 2$ понятие диагонали массива совпадает с понятием диагонали матрицы. *k-Мерным перманентом* массива $A(G_k)$ называется величина

$$\operatorname{per}_k A(G_k) = \sum_{I \in D_N} \prod_{(i_1, \ldots, i_k) \in I} a_{i_1 \ldots i_k},$$

где D_N — множество всех диагоналей массива F.

Совершенным k-сочетанием в гиперграфе G_k будем называть набор попарно не пересекающихся k-рёбер гиперграфа G_k, покрывающих все вершины гиперграфа G_k. Из сказанного выше имеем

Предложение 189. *Число совершенных k-сочетаний в гиперграфе G_k равно* $\operatorname{per}_k A(G_k)$.

Напомним, что кликосочетанием в Q_q^n называется набор не пересекающихся по вершинам линий (клик в ΓQ_q^n) . При $q = 2$ понятие кликосочетания в Q_2^n совпадает с понятием паросочетания. Кликосочетание в гиперкубе Q_q^n будем называется совершенным, если оно является разбиением всех вершин гиперкуба на линии. *Разбиением* Q_q^n на МДР-коды будем называть набор попарно не пересекающихся МДР-кодов $M_0, \ldots, M_{q-1}$ с расстоянием 2.

Обозначим через $Q_q^n(w)$ множество $(n-w)$-мерных граней в гиперкубе Q_q^n. Рассмотрим гиперграф $G_q(n)$ с множеством вершин Q_q^n, q-рёбрами которого являются элементы множества $Q_q^n(n-1)$ (максимальные клики в гиперкубе ΓQ_q^n). В качестве набора долей гиперграфа $G_q(n)$ рассмотрим произвольное разбиение гиперкуба Q_q^n на МДР-коды. Как нетрудно видеть, совершенному q-сочетанию в гиперграфе $G_q(n)$ соответствует совершенное кликосочетание в гиперкубе Q_q^n. Тогда из предложения 189 имеем

Следствие 39. *Число совершенных кликосочетаний в гиперкубе Q_q^n равно q-мерному перманенту массива $A(G_q(n))$.*

Утверждение аналогичное теореме 48 Кёнига неверно для многомерных перманентов. А именно, существуют трёхмерные (и большей размерности) $(0,1)$-матрицы с одинаковым ненулевым числом единиц в каждой гиперграни и нулевым перманентом. Примерами таких матриц, могут случить характеристические функции МДР-кодов, представляющие латинские квадраты без трансверсалей. Примеры таких латинских квадратов для произвольного чётного порядка приведены в предложении 22.

Пусть G — двудольный бирегулярный граф. Множество вершин C, принадлежащих одной из долей будем называть *совершенным кодом в графе G*, если их окрестности не пересекаются и покрывают вторую долю графа G. Предположим одна из долей графа допускает разбиение $C = \{C_1, \ldots, C_k\}$ на совершенные коды. Занумеруем элементы каждого из кодов $C_1, \ldots, C_k$ числами $1, 2, \ldots, N$. Определим массив $M(G, C) = (m_{i_1 \ldots i_k})$ графа G равенством $m_{i_1 \ldots i_k} = |B_{i_1}^1 \cap \cdots \cap B_{i_k}^k|$, где $B_{i_j}^j$ окрестность вершины с номером i_j из кода C_j. Нетрудно видеть, что

Предложение 190. *Число совершенных кодов во второй доле графа G равно* $\operatorname{per}_k M(G, C)$.

Как было сказано во введении, совершенные кликосочетания являются частным случаем A-дизайнов (A-схем), а МДР-коды — H-дизайнов (H-схем). Число A-дизайнов и H-дизайнов также можно представить как многомерный перманент некоторого массива. Для фиксированных w, t $(n \geq w \geq t \geq 1)$, определим двудольный граф

$G(n,q,w,t)$ с долями $Q_q^n(w)$ и $Q_q^n(t)$, состоящими из всевозможных граней размерностей $n-w$ и $n-t$ соответственно. Пару вершин $\overline{c} \in Q_q^n(w)$ и $\overline{b} \in Q_q^n(t)$ соединим ребром в графе $G(n,q,w,t)$, если $\overline{c} \subset \overline{b}$. По определению дизайн типа $H(n,q,w,t)$ является таким подмножеством в $Q_q^n(w)$, которое однократно протыкает все элементы множества $Q_q^n(t)$, т.е. в графе $G(n,q,w,t)$ окрестности вершин из H-дизайна не пересекаются покрывают все вершины, соответствующие граням из $Q_q^n(t)$. Предположим, что существует разбиение $H = \{H_1, \ldots, H_k\}$, где $k = \binom{n-t}{n-w} q^{w-t}$, множества $Q_q^n(w)$ на дизайны типа $H(n,q,w,t)$. Тогда из предложения 190 имеем

Предложение 191 ([173]). *Число различных дизайнов типа $A(n,q,w,t)$ равно* $\mathrm{per}_k M(G,H)$.

Аналогично, по определению каждый дизайн типа $A(n,q,w,t)$ является таким подмножеством в $Q_q^n(t)$, которое однократно покрывает все грани из $Q_q^n(w)$. Т. е. является совершенным кодом в $G(n,q,w,t)$. Предположим, что существует разбиение $A = \{A_1, \ldots, A_m\}$, где $m = \binom{w}{t}$, множества $Q_q^n(t)$ на дизайны типа $A(n,q,w,t)$. Тогда из предложения 190 имеем

Предложение 192 ([173]). *Число различных дизайнов типа $H(n,q,w,t)$ равно* $\mathrm{per}_m M(G,A)$.

Конструкции из параграфа 3.3 обеспечивают примеры параметров, для которых существует разбиение граней гиперкуба на H-дизайны или A-дизайны. Это обеспечивает область применения предложений 191 и 192.

§ 3.2. Число кликосочетаний

Кликосочетание можно рассматривать как функцию, ставящую в соответствие каждой вершине из Q_q^n направление i линии кликосочетания, в которой лежит вершина, или 0, если вершина не содержится ни в одной грани кликосочетания. Нетрудно видеть, что функция $f : Q_q^n \to \{0,1,\ldots,n\}$ определяет кликосочетание, если удовлетворяет следующему условию

$$f(a_1,.,a_{i-1},a_i,a_{i+1},.,a_n) = i \neq 0 \;\Rightarrow\; \forall x \in Q_q \; f(a_1,.,a_{i-1},x,a_{i+1},.,a_n) = i. \qquad (3.5)$$

В дальнейшем будем называть кликосочетанием и определяющую кликосочетание функцию. Кликосочетание f является совершенным тогда и только тогда, когда $0 \notin f(Q_q^n)$. Обозначим через $K_q(n)$ множество кликосочетаний и через $SK_k(n)$ — множество совершенных кликосочетаний в Q_q^n. Из определения следует тривиальная верхняя оценка $|SK_q(n)| \leq n^{q^n}$ числа кликосочетаний в Q_q^n.

Напомним, что *изотопией* называется упорядоченный набор из n перестановок $(\theta_1, \ldots, \theta_n)$, $\theta_i : Q_q \to Q_q$, где $i \in [n]$. Обозначим через S_q^n множество изотопий гиперкуба Q_q^n. Пусть $\bar{\theta} = (\theta_1, ..., \theta_n) \in S_q^n$ и $f \in K_q(n)$. Нетрудно видеть, что функция $g(x_1, \ldots, x_n) = f(\theta_1 x_1, \ldots, \theta_n x_n)$ является кликосочетанием. Введём обозначение $g = \bar{\theta} f$. Определим *изотопное замыкание* множества $A \subseteq K_q(n)$ равенством $\overline{A} = \{\bar{\theta} f \mid f \in A, \bar{\theta} \in S_q^n\}$. Справедливо следующее

Предложение 193. *Пусть $A \subseteq K_q(n)$ и $A = \overline{A}$. Тогда величины $P_{A,i}(\overline{x}) = \frac{|\{f \in A \mid f(\overline{x}) = i\}|}{|A|}$ не зависят от $\overline{x} \in Q_q^n$ и равны для любых $i \in [n]$ и $\overline{x} \in Q_q^n$.*

Обозначим через $K_q(n, p)$ множество кликосочетаний, принимающих значение 0 с вероятностью p, т. е. $K_q(n, p) = \left\{ f \in K_q(n, p) \mid p = \frac{|\{\overline{x} \in Q_q^n \mid f(\overline{x}) = 0\}|}{q^n} \right\}$.

Теорема 52 ([52]). *Пусть $0 < p < 1$ и $K_q(m, p) \neq \varnothing$ для некоторого натурального m. Тогда $|K_q(n, p)| \geq n^{cq^{n-2}(1+o(1))}$ при $n \to \infty$, где $c = p^{q-1}(1-p)\ln 2$.*

Доказательство. Докажем неравенство

$$|K_q(n+1, p)| \geq |K_q(n, p)|^q 2^{\frac{q^{n-1} p^{q-1} (1-p)}{n}}. \tag{3.6}$$

Рассмотрим произвольную вектор-функцию $F \in (K_q(n, p))^q$, $F = (f_0, \ldots, f_{q-1})$. Нетрудно видеть, что вектор-функция F определяет кликосочетание $\widehat{F}$ в гиперкубе Q_q^{n+1} по правилу $\widehat{F}(x_1, \ldots, x_n, z) = f_z(x_1, \ldots, x_n)$. Однако, построенных таким способом кликосочетаний в Q_q^{n+1} оказывается недостаточно для требуемой асимптотической оценки числа $|K_q(n, p)|$. Ниже описан способ получения из кликосочетаний вида $\widehat{F}$ кликосочетаний другого типа посредством некоторых локальных преобразований.

Двумерную грань $\alpha_{x_2, \ldots, x_n} = \{(y, x_2, \ldots, x_n, z) \mid y, z \in Q_q\}$ в Q_q^{n+1} будем называть *сдвигаемой* относительно F, если $(f_0(y_0, x_2, \ldots, x_n), \ldots, f_{q-1}(y_0, x_2, \ldots, x_n)) = (0, \ldots, 0, 1)$ для некоторого $y_0 \in Q_q$. Определим функцию $g_\alpha^0[F] : \alpha \to Q_q$ на про-

извольной грани $\alpha = \alpha_{x_2,\ldots,x_n}$ равенством

$$g^0_\alpha[F](y, x_2, \ldots, x_n, z) = f_z(y, x_2, \ldots, x_n)$$

и функцию $g^1_\alpha[F] : \alpha \to Q_q$ на сдвигаемой грани $\alpha = \alpha_{x_2,\ldots,x_n}$ равенством

$$g^1_\alpha[F](y, x_2, \ldots, x_n, z) = \begin{cases} n+1 & \text{при } \ z \in Q_q \text{ и } y = y_0, \\ 0 & \text{при } \ z = q-1 \text{ и } y \neq y_0, \\ f_z(y, x_2, \ldots, x_n) & \text{при } \ z \neq q-1 \text{ и } y \neq y_0. \end{cases}$$

Если $y_0 \in Q_q$ можно выбрать несколькими способами, то для определённости полагаем y_0 минимальным из возможных. Рассмотрим произвольный набор Ω сдвигаемых граней $\alpha_{x_2,\ldots,x_n}$, $x_i \in Q_q$, относительно фиксированной вектор-функции $F \in (K_q(n,p))^q$. Нетрудно видеть, что функция $h_\Omega[F] : Q_q^{n+1} \to Q_q$ определённая как

$$h_\Omega[F]|_\alpha = \begin{cases} g^0_\alpha[F] & \text{при } \ \alpha \notin \Omega, \\ g^1_\alpha[F] & \text{при } \ \alpha \in \Omega \end{cases}$$

является кликосочетанием, более того, $h_\Omega[F] \in K_q(n+1,p)$.

Вектор-функция F восстанавливается из кликосочетания $h_\Omega[F]$ однозначно заменой подфункции $g^1_\alpha[F]$ на подфункцию $g^0_\alpha[F]$ во всех тех гранях $\alpha_{x_2,\ldots,x_n}$, $x_i \in Q_q$, где кликосочетание $h_\Omega[F]$ принимает значение $n+1$. Тогда из равенства $h_\Omega[F] = h_{\Omega'}[F']$ следует, что $F = F'$ и $\Omega = \Omega'$. Следовательно, имеем неравенство

$$|K_q(n+1,p)| \geq \sum_{F \in (K_q(n,p))^q} 2^{d_F}, \tag{3.7}$$

где d_F — число сдвигаемых граней относительно вектор-функции F.

Оценим количество сдвигаемых граней во всех функциях $F \in (K_q(n,p))^q$. Имеем

$$|\{F \in (K_q(n,p))^q \mid F(\overline{x}) = (0,\ldots,0,1)\}| = |K_q(n,p))|^q (P_0(\overline{x}))^{q-1} P_1(\overline{x}),$$

где $P_i(\overline{x}) = \frac{|\{f \in K_q(n,p) \mid f(\overline{x}) = i\}|}{|K_q(n,p)|}$. Поскольку каждая двумерная грань состоит из q одномерных, справедливо неравенство

$$\sum_{F \in (K_q(n,p))^q} d_F \geq \frac{1}{q} |K_q(n,p))|^q \sum_{\overline{x} \in Q_q^n} (P_0(\overline{x}))^{q-1} P_1(\overline{x}), \tag{3.8}$$

Без ограничения общности полагаем, что $\sum\limits_{\overline{x}\in Q_q^n} P_1(\overline{x}) = \max\limits_{1\le i\le n} \sum\limits_{\overline{x}\in Q_q^n} P_i(\overline{x}) \ge \frac{1}{n}(1-p)q^n$. Поскольку $K_q(n,p) = \overline{K_q(n,p)}$, из предложения 193 и равенства (3.8) имеем

$$\sum_{F\in(K_q(n,p))^q} d_F \ge \frac{1}{q}|K_q(n,p))|^q \sum_{\overline{x}\in Q_q^n} (P_0(\overline{x}))^{q-1} P_1(\overline{x}) \ge q^{n-1}|K_q(n,p))|^q \frac{p^{q-1}(1-p)}{n}.$$

Тогда из (3.7) и выпуклости (вниз) функции $y(t) = 2^t$ получаем неравенство (3.6).

Введём обозначение $\beta_n = \frac{\ln|K_q(n,p)|}{q^{n-1}}$. Подразумевается, что $K_q(n,p) \ne \varnothing$. Это верно, например, при $n = 2$ и $p = 1 - \frac{1}{q}$. Тогда из неравенства (3.6) имеем $\beta_{n+1} \ge \beta_n + \frac{c}{qn}$, следовательно, $\beta_n \ge \frac{c}{q}\ln n(1+o(1))$ при $n\to\infty$. ▲

Следствие 40 ([52]). $|SK_q(n)| \ge n^{c_n q^{n-4}}$ *при* $n\to\infty$, *где* $c_n = \frac{\ln 2(1+o(1))}{e}$.

Доказательство. Пусть $f \in K_q(n)$. Определим функцию

$$\widetilde{f}(x_1,\dots,x_{n+1}) = \begin{cases} f(x_1,\dots,x_n), & \text{если } f(x_1,\dots,x_n)\ne 0,\\ n+1, & \text{если } f(x_1,\dots,x_n) = 0.\end{cases}$$

Нетрудно видеть, что $\widetilde{f} \in SK_q(n)$. Тогда $|SK_q(n)| \ge |K_q(n-1,p)|$ для любого p, $0<p<1$. Выберем $p = 1-\frac{1}{q}$. Тогда $p^{q-1} > 1/e$ и из теоремы 52 получаем требуемое неравенство. ▲

Поскольку $\ln|SK_q(n)| \le \ln|K_q(n)| \le q^n \ln n$, справедливо

Следствие 41 ([52]). $\ln|SK_q(n)| \asymp q^n \ln n$ *при* $n\to\infty$.

На основе этой оценки (3.2) в следующем утверждении предлагается некоторое усиление тривиальной верхней оценки числа совершенных кликосочетаний в случае чётного q.

Предложение 194 ([52]). *Пусть* q *чётно, тогда* $|SK_q(n)| \le \left(\frac{n}{e}\right)^{q^{n-1}(1+o(1))}$ *при* $n\to\infty$.

Доказательство. Пусть $q = 2m$, представим элементы $a \in Q_{2m}$ в виде $a = (\alpha,\beta) \in Q_2 \times Q_m$. Пусть M — некоторый МДР-код в Q_m^n. Совершенное кликосочетание $f : (Q_2\times Q_m)^n \to [n]$ однозначно определяется набором своих сужений на множества $Q_2^n \times \overline{c}$, где $\overline{c} \in M$. Поскольку $|M| = m^{n-1}$, из неравенства (3.2) получаем оценку $|SK_{2m}(n)| \le (n!)^{m^{n-1}2^{n-1}/n}$. Отсюда требуемое асимтотическое неравенство

получается при помощи формулы Стирлинга $n! = \left(\frac{n}{e}\right)^n \sqrt{2\pi n}(1 + o(1))$ при $n \to \infty$.
▲

§ 3.3. Конструкции точных кликосочетаний и блок-схем

§ 3.3.1. Точные кликосочетания

Будем говорить, что кликосочетание f *не содержит близких параллельных клик*, если никакие две клики из f не лежат в одной двумерной грани. Совершенное кликосочетание f будем называть *точным*, если в каждой двумерной грани лежит ровно одна клика из кликосочетания f. В [33], [122] и [186] построены совершенные паросочетания без близких параллельных рёбер в булевом гиперкубе. Точнее в [33] и [186] построены тернарные коды, эквивалентность которых паросочетаниям показана в [33]. В частности, в [33] доказано, что при $n = 2^j$, $j \geq 2$ в булевом n-мерном кубе Q_2^n имеются совершенные паросочетания без параллельных рёбер в трёхмерных гранях. Из мощностных соображений нетрудно доказать, что при $q > 2$ в гиперкубе Q_q^n не существует совершенных кликосочетаний без параллельных клик в трёхмерных гранях. В [45] построены совершенные паросочетания в булевом n-мерном кубе, сужения которых на любую грань размерности больше 1 и меньше n не является паросочетанием в этой грани и, следовательно, не содержит близких параллельных рёбер.

Выясним при каких q и n в гиперкубе Q_q^n могут существовать совершенные кликосочетания без близких параллельных клик и точные кликосочетания.

Предложение 195. (a) *Если в Q_q^n существует совершенное кликосочетание без близких параллельных клик, то $n \geq 2q$.*

(b) *Совершенное кликосочетание без близких параллельных клик в Q_q^n является точным, если и только если $n = 2q$.*

Доказательство. Совершенное кликосочетание B в гиперкубе Q_q^n содержит q^{n-1} клик и каждая клика (одномерная грань) содержится в $n - 1$ двумерной грани. Если в кликосочетании B нет близких параллельных клик, то $q^{n-1}(n-1)$ не

меньше числа различных двумерных граней в гиперкубе Q_q^n, т. е. справедливо неравенство

$$q^{n-1}(n-1) \leq \frac{n(n-1)}{2} q^{n-2},$$

из которого следует утверждение (a). Причём это неравенство превращается в равенство тогда и только тогда, когда совершенное кликосочетание без близких параллельных клик является точным. Отсюда имеем (b). ▲

Предложение 196 ([52]). *Если в Q_q^n существует точное кликосочетание, то $n = 4m$, $q = 2m$, m — натуральное.*

Доказательство. Покажем, что точное кликосочетание содержит равное количество клик каждого из направлений. Пусть z_i — число клик направления i, $i \in [n]$, в точном кликосочетании $B \subset Q_q^n(n-1)$. Число двумерных граней в гиперкубе Q_q^n одинаково для каждой пары направлений и равно q^{n-2}. Имеем систему из $\frac{n(n-1)}{2}$ линейных уравнений $z_i + z_j = q^{n-2}$, где $i \neq j$, $i, j \in [n]$. Нетрудно видеть, что соответствующая однородная система имеет единственное (нулевое) решение при $n \geq 3$. Поэтому исходная неоднородная система имеет единственное решение $z_i = \frac{q^{n-2}}{2}$ при любом $i \in [n]$. Поскольку z_i — целое число, то q делится на 2; $n = 2q$ из предложения 195 (b). ▲

Перейдём к построению точных кликосочетаний в Q_q^n при $q = 2^t$ и $n = 2^{t+1}$. Занумеруем произвольным образом элементы поля Галуа $x_i \in GF(2^{t+1})$ числами из множества $i \in [n]$. Поле Галуа $GF(2^{t+1})$ можно рассматривать как $(t+1)$-мерное векторное пространство над полем $GF(2)$. Выберем в этом векторном пространстве произвольный базис $\{b_1, \ldots, b_{t+1}\}$. Элементам множества $Q_q = \{0, \ldots, 2^t - 1\}$ поставим во взаимно однозначное соответствие элементы линейной оболочки векторов $\{b_1, \ldots, b_t\}$ в $GF(2^{t+1})$. Ниже, с целью упрощения формул, будем отождествлять элементы множества Q_q с соответствующими элементами $GF(2^{t+1})$. Зададим функцию $f : Q_q^n \to [n]$ равенством

$$f(a_1, \ldots, a_n) = l, \qquad \text{где } x_l = \frac{\sum\limits_{i=1}^{n} x_i a_i}{b_{t+1} + \sum\limits_{i=1}^{n} a_i}, \tag{3.9}$$

где все арифметические операции производятся в $GF(2^{t+1})$.

Теорема 53 ([52]). *Функция f, определённая формулой (3.9), является точным кликосочетанием.*

Доказательство. Поскольку b_{t+1} не содержится в линейной оболочке множества $\{b_1, \ldots, b_t\}$, то знаменатель в выражении (3.9) не обращается в ноль. Следовательно функция f определена всюду на Q_q^n.

Покажем, что f определяет кликосочетание. Достаточно доказать, что из равенства $f(a_1, \ldots, a_l, \ldots, a_n) = l$ следует $f(a_1, \ldots, a_{l-1}, c, a_{l+1}, \ldots, a_n) = l$ для любого $c \in Q_q$. Из (3.9) имеем

$$x_l \left(b_{t+1} + \sum_{i=1}^{n} a_i \right) = \sum_{i=1}^{n} x_i a_i.$$

Прибавив к правой и левой частям последнего равенства величину $x_l(c - a_l)$ получаем, что $f(a_1, \ldots, a_{l-1}, c, a_{l+1}, \ldots, a_n) = l$.

Покажем, что кликосочетание f не содержит близких параллельных клик, т. е. для любого $c \in Q_q$, $c \neq a_m$ и $m \neq l$ имеем $f(a_1, \ldots, a_{m-1}, c, a_{m+1}, \ldots, a_n) \neq l$ когда $f(a_1, \ldots, a_l, \ldots, a_n) = l$. Предположим, что $f(a_1, \ldots, a_{m-1}, c, a_{m+1}, \ldots, a_n) =$
$f(a_1, \ldots, a_l, \ldots, a_n) = l$. Тогда из (3.9) имеем равенства

$$x_l \left(b_{t+1} + \sum_{i=1}^{n} a_i \right) = \sum_{i=1}^{n} x_i a_i,$$

$$x_l(c - a_m) + x_l \left(b_{t+1} + \sum_{i=1}^{n} a_i \right) = \sum_{i=1}^{n} x_i a_i + x_m(c - a_m).$$

Вычитая из второго равенства первое, имеем $x_l(c - a_m) = x_m(c - a_m)$. Если $a_m \neq c$, то $x_m = x_l$. Пришли к противоречию.

Из предложения 195(b) следует, что кликосочетание f точное. ▲

При $t = 1$ паросочетание, определяемое формулой (3.9), совпадает с построенным в [122].

Рассмотрим вопрос построения совершенных кликосочетаний без близких параллельных клик.

Предложение 197 ([52]). *При $q = 2^t$ и $n = 2^{t+1}$ (t - натуральное) в гиперкубе Q_q^n существует разбиение множества клик $Q_q^n(n-1)$ на n точных кликосочетаний.*

Доказательство. Определим кликосочетание f_j, $j \in [n]$, формулой:

$$f_j(a_1, \ldots, a_n) = l, \qquad \text{где } x_l + x_j = \frac{\sum\limits_{i=1}^{n}(x_i + x_j)a_i}{b_{t+1} + \sum\limits_{i=1}^{n} a_i}.$$

По теореме 3.9 кликосочетания f_j являются точными при $j \in [n]$. Ясно, что из равенства $f_j(a_1, \ldots, a_n) = f_{j'}(a_1, \ldots, a_n)$ следует $x_j = x_{j'}$. Таким образом, набор $\{f_j\}_{j=1,\ldots,n}$ представляет собой разбиение множества $Q_q^n(n-1)$ на попарно не пересекающиеся точные кликосочетания. ▲

Предложение 198 ([52]). *При $2 \le q \le 2^t$ и $n \ge 2^{t+1}$ (t - натуральное) в гиперкубе Q_q^n существует совершенное кликосочетание без близких параллельных клик.*

Доказательство. В предложении 197 доказано, что при $m = 2^t$ существует разбиение множества $Q_m^{2m}(2m-1)$ на $2m$ совершенных кликосочетания без близких параллельных клик. Представим произвольные m из этих $2m$ кликосочетаний в виде функций $f_0, \ldots, f_{m-1} : Q_m^{2m} \to [2m]$. Пусть $\varphi : Q_m^{n-2m} \to Q_m$ некоторая $(n-2m)$-арная квазигруппа. Тогда функция $F : Q_m^{2m} \times Q_m^{n-2m} \to [2m]$, заданная равенством

$$F(c_1, \ldots, c_{2m}, a_1, \ldots, a_{n-2m}) = f_{\varphi(a_1,\ldots,a_{n-2m})}(c_1, \ldots, c_{2m}),$$

соответствует совершенному кликосочетанию без близких параллельных клик в Q_m^n.

Пусть $q < m$. Тогда сужение $g = F|_{Q_q^n}$ также является совершенным кликосочетанием без близких параллельных клик. ▲

Таким образом, остаются открытыми вопросы о существовании в Q_q^n точных кликосочетаний при $q = 2m$, $n = 4m$, где m — не степень числа 2 и совершенных кликосочетаний без близких параллельных клик при q и n таких, что $2^{t-1} < q < 2^t, 2q \le n < 2^{t+1}$.

§ 3.3.2. Конструкции комбинаторных A- и H-схем

Далее предложены несколько конструкций H-дизайнов (H-схем) и A-дизайнов (A-схем). Напомним, что словам в алфавите Q_{q*} соответствуют грани гиперкуба, причём

размерность грани равна числу символов $*$ в слове, т. е. разности между длиной и весом слова.

Конструкция I. Пусть $S \subset Q_{q*}^n$ является дизайном типа $H(n, q, w, t)$ и $R \subset Q_{q'*}^w$ является дизайном типа $H(w, q', w, t)$ (т.е. МДР-кодом). Для наборов произвольных $(a^1, \dots, *, \dots, a^i, \dots, *, \dots, a^w) \in S$ и $(b_1, \dots, b_w) \in R$ составим кодовое слово $((a^1, b_1), \dots, *, \dots, (a^i, b_i), \dots, *, \dots, (a^w, b_w)) \in Q_{qq'*}^n$. Пусть T — множество всех таких кодовых слов. Тогда

Предложение 199 ([173]). *T есть дизайн типа $H(n, qq', w, t)$.*

Доказательство. Пусть $c^i \in Q_q$, $d^i \in Q_{q'}$ и $((c^1, d^1), \dots, *, \dots, (c^i, d^i), \dots, *, \dots, (c^t, d^t))$ — произвольный элемент из $Q_{qq'*}^n$ веса t. По определению H-дизайна имеется единственное слово $(a^1, \dots, *, \dots, a^i, \dots, *, \dots, a^w) \in S$ такое, что $(n-w)$-мерная грань $(a^1, \dots, *, \dots, a^i, \dots, *, \dots, a^w)$ содержится в $(n-t)$-мерной грани $(c^1, \dots, *, \dots, c^i, \dots, *, \dots, c^t)$. Преобразуем слово $(d^1, \dots, *, \dots, d^i, \dots, *, \dots, d^t) \in Q_{q'*}^n$ в новое слово длины w, удалив позиции i, если слово $(a^1, \dots, *, \dots, a^i, \dots, *, \dots, a^w)$ имеет $*$ на позиции i. Так мы получим слово $\overline{d} \in Q_{q'*}^w$. По определению H-дизайна имеется ровно одно кодовое слово $(b_1, \dots, b_w) \in R$ такое, что $(b_1, \dots, b_w) \subset \overline{d}$. Тогда T есть дизайн типа $H(n, qq', w, t)$ по определению. ▲

Из теоремы 53 следует, что дизайны типа $H(2k, k, 2k-1, 2k-2)$ существуют при $k = 2^t$, $t \geq 1$. Поскольку МДР-коды с расстоянием 2 (дизайны типа $H(m, q, m, m-1)$) существуют при всех $q \geq 2$ и $m \geq 2$, имеем

Следствие 42. *Для любых $s, t \geq 1$ существуют дизайны типа $H(2^{t+1}, s2^t, 2^{t+1} - 1, 2^{t+1} - 2)$.*

Замечание 18. *Заметим, что* МДР-*код R в Конструкции I может быть выбран независимо для каждого элемента из S. Число s-чных* МДР-*кодов растёт экспоненциально при $s \geq 3$ (см. § 1.4). Тогда число дизайнов типа $H(2^{t+1}, s2^t, 2^{t+1} - 1, 2^{t+1} - 2)$ растёт дважды экспоненциально относительно размерности 2^{t+1} при $s \geq 3$.*

Конструкция II. Пусть $S \subset Q_{q*}^n$ является дизайном типа $A(n, q, w, t)$. Для каждой пары наборов $(a^1, \dots, *, \dots, a^i, \dots, *, \dots, a^t) \in S$ и $(b_1, \dots, b_t) \in Q_{q'}^t$ составим ко-

довое слово $((a^1, b_1), \ldots, *, \ldots, (a^i, b_i), \ldots, *, \ldots, (a^t, b_t)) \in Q^n_{qq'*}$. Пусть U — множество всех таких слов. Тогда

Предложение 200 ([173]). *U есть дизайн типа $A(n, qq', w, t)$.*

Доказательство этого утверждения аналогично доказательству предложения 199.

Как было отмечено во введении, системы Штейнера типа $S(n-w, n-t, n)$ эквивалентны А-дизайнам типа $A(n, 1, w, t)$. Из предложеия 200 получаем следствие

Следствие 43. *Если существует система Штейнера типа $S(n-w, n-t, n)$, то для любого $q \geq 1$ существуют дизайны типа $A(n, q, w, t)$.*

Конструкция III. Пусть $S \subset Q^n_{q*}$ является дизайном типа $A(n, q, n-1, n-2)$. Определим $V = (S \times Q^n_q) \cup (Q^n_q \times S)$. Тогда

Предложение 201 ([173]). *V есть дизайн типа $A(2n, q, 2n-1, 2n-2)$.*

Доказательство. Предположим, что $(c_1, \ldots, c_{i-1}, *, c_{i+1}, \ldots, c_{2n})$ — набор веса $2n-1$. Если $i \leq n$, то существует единственное кодовое слово $\overline{a} \in S$ такое, что грань $(c_1, \ldots, c_{i-1}, *, c_{i+1}, \ldots, c_n) \subset \overline{a}$. Ясно, что $(c_1, \ldots, c_{i-1}, *, c_{i+1}, \ldots, c_{2n}) \subset (\overline{a}, \overline{d})$, где $\overline{d} = (c_{n+1}, \ldots, c_{2n})$. Случай $n < i \leq 2n$ рассматривается подобным же образом. ▲

Подставляя в перечисленные конструкции дизайны из разбиения гиперкуба на дизайны, можно получить разбиения гиперкуба (с новыми параметрами) на дизайны с новыми параметрами.

§ 3.4. Гамильтоновы циклы в булевом гиперкубе

§ 3.4.1. Свойства гамильтоновых циклов

Гамильтоновым циклом в графе G называется цикл, проходящий через все вершины графа по одному разу. В двудольном графе, в частности в графе ΓQ^n_2, рёбра каждого гамильтонова цикла разделяются на два совершенных паросочетания. Спектром гамильтонова цикла в булевом n-мерном кубе (n-кубе) называется набор $a = (a_1, a_2, \ldots, a_n)$, где a_i — число рёбер i-го направления в гамильтоновом цикле. Аналогичным образом определяется спектр совершенного паросочетания в ΓQ^n_2.

Предложение 202 ([46]). *Набор целых чисел $(a_1, \ldots, a_n)$ является спектром совершенного паросочетания в ΓQ_2^n если и только если*

a_i — неотрицательное четное число для любого $i \in [n]$;

$\sum_{i=1}^{n} a_i = 2^{n-1}$.

Необходимость перечисленных условий очевидна. Достаточность можно доказать по индукции.

Известны также необходимые условия для того, чтобы целочисленный набор $(a_1, \ldots, a_n)$ являлся спектром некоторого гамильтонова цикла в ΓQ_2^n.

Предложение 203 (см. [137]).

(*) *a_i — неотрицательное четное число для любого $i \in [n]$;*

(**) $\sum_{i=1}^{n} a_i = 2^n$;

(***) $\sum_{i=1}^{k} a_{\pi(i)} \geq 2^k$ *для любой перестановки $\pi \in S_n$ и $k \in [n-1]$.*

Условия (*) и (**) очевидны, условие (***) следует из связности цикла.

Без ограничения общности можно полагать, что спектр гамильтонова цикла упорядочен: $a_i \leq a_j$ при $i \leq j$. В этом случае условие (***) приобретает более простой вид: $\sum_{i=1}^{k} a_i \geq 2^k$ при любом $k \leq n$. Для упорядоченного спектра a определим неотрицательную функцию μ_a равенством $\mu_a(k) = \sum_{i=1}^{k} a_i - 2^k$.

Целочисленный набор будем называть *допустимым*, если он удовлетворяет указанным выше необходимым условиям (*)–(***). Множество допустимых n-мерных наборов будем обозначать через $\mathbb{D}_n$. Очевидно, что любой гамильтонов цикл в ΓQ_2^n содержит рёбра всех направлений, в то время как совершенное паросочетание в ΓQ_2^n может содержать рёбра от одного до n направлений включительно. Паросочетание в ΓQ_2^n, содержащее ребра всех n направлений, будем называть паросочетанием *полного ранга*. Гамильтоновы циклы, содержащие совершенные паросочетания полного ранга, будем называть циклами, имеющими полный ранг.

Предложение 204. *Если для некоторого n любой допустимый целочисленный набор является спектром некоторого гамильтонова цикла в ΓQ_2^n, то это же верно при любых m, $2 \leq m \leq n$.*

Доказательство. Действительно, пусть $(a_1, \ldots, a_m)$ некоторый допустимый набор, тогда набор $(a_1, \ldots, a_m, 2^m, \ldots, 2^{n-1})$ также является допустимым. При этом проекция гамильтонова цикла со спектром $(a_1, \ldots, a_m, 2^m, \ldots, 2^{n-1})$ на первые m направлений порождает гамильтонов цикл со спектром $(a_1, \ldots, a_m)$.▲

Каждому простому (в частности гамильтонову) циклу C в графе ΓQ_2^n можно поставить в соответствие циклическое *переходное слово* X в алфавите $[n] = \{1, \ldots, n\}$, в котором j-я буква x_j определяется как направление j-го ребра в цикле C. Через $S(X) = (s_1, \ldots, s_n)$ будем обозначать *набор состава* слова X по модулю 2, т е. $s_i = 0$, если буква $i \in [n]$ встречается в слове $S(X)$ чётное число раз и $s_i = 1$ в противном случае.

Следующее предложение является критерием того, что слово определяет простой цикл.

Предложение 205 ([45]). *Циклическое слово X в алфавите $[n]$ определяет простой цикл в графе ΓQ_2^n тогда и только тогда, когда $S(X) = \overline{0}$ и для любого его подслова Y, $Y \neq X$, имеем $S(Y) \neq \overline{0}$.*

Откуда немедленно получаем

Следствие 44. *Циклическое слово X в алфавите $[n]$ определяет гамильтонов цикл в графе ΓQ_2^n тогда и только тогда, когда длина слова X равна 2^n, $S(X) = \overline{0}$ и для любого его подслова Y, $Y \neq X$, имеем $S(Y) \neq \overline{0}$.*

§ 3.4.2. Конструкция гамильтонова цикла

Далее докажем, что любой допустимый набор является спектром гамильтонова цикла в любом булевом n-кубе, если это верно для булева N-куба при некотором достаточно большом N. В доказательстве применяется конструкция гамильтонова цикла, использующая представление булева n-куба как декартова произведения кубов размерности k и $n - k$.

Рассмотрим некоторый гамильтонов цикл в ΓQ_2^n, состоящий из ребер непересекающихся совершенных паросочетаний P_1 и P_2. Естественным образом вложим паросочетание P_1 в ΓQ_2^n. Поскольку каждой вершине из ΓQ_2^k в декартовом произведении

$\Gamma Q_2^k \times \Gamma Q_2^{n-k}$ соответствует булев $(n-k)$-куб, каждому ребру из P_1 можно поставить в соответствие пару параллельных $(n-k)$-кубов, т. е. один $(n-k+1)$-куб. Заменим каждое ребро $v \in P_1$ гамильтоновым циклом H_v в соответствующем $(n-k+1)$-кубе, проходящим через это ребро. Удалив теперь паросочетание P_1 из объединения P_2 и циклов H_v, $v \in P_1$, получим новый гамильтонов цикл в $\Gamma Q_2^k \times \Gamma Q_2^{n-k} = \Gamma Q_2^n$. Сформулируем описанную выше конструкцию в виде леммы

Лемма 16 ([53]). *Пусть паросочетания в ΓQ_2^k со спектрами $(b_1, \ldots, b_k)$ и $(b'_1, \ldots, b'_k)$, составляют гамильтонов цикл и имеется 2^{k-1} гамильтоновых циклов в ΓQ_2^{n-k+1} со спектрами $(a_1^i, \ldots, a_{n-k}^i, c^i)$, $i \in [2^{k-1}]$. Тогда в ΓQ_2^n имеется гамильтонов цикл со спектром $(d_1, \ldots, d_n)$, где $d_{k+j} = \sum\limits_{i=1}^{2^{k-1}} a_j^i$ при $j \in [n-k]$ и $d_j = b_j + \sum\limits_{p=s_j+1}^{s_{j+1}} (c^p - 1)$ при $j \in [k]$, $s_j = \sum\limits_{p=1}^{j-1} b'_p$.*

Доказательство. Пусть $X = x_1 y_1 x_2 \ldots x_{2^{k-1}} y_{2^{k-1}}$ — переходное слово гамильтонова цикла в ΓQ_2^k, где паросочетание соответствующее слову $x_1 x_2 \ldots x_{2^{k-1}}$ имеет спектр $(b_1, \ldots, b_k)$, а слову $y_1 y_2 \ldots y_{2^{k-1}}$ — спектр $(b'_1, \ldots, b'_k)$. Обозначим через $y_i Z^i$ переходное слово гамильтонова цикла в ΓQ_2^{n-k+1} в алфавите $\{k+1, \ldots, n, y_i\}$ со спектром $(a_1^i, \ldots, a_{n-k}^i, c^i)$, $i \in [2^{k-1}]$, причём буква y_i встречается $c^i - 1$ раз в слове Z^i.

Рассмотрим слово Z, полученное подстановкой в слово X слов Z^i вместо букв y_i, т. е. $Z = x_1 Z^1 x_2 Z^2 \ldots x_{2^{k-1}} Z^{2^{k-1}}$. Покажем, что слово Z является переходным словом некоторого гамильтонова цикла в ΓQ_2^n. Рассмотрим произвольное подслово $W = U_i x_{i+1} Z^{i+1} \ldots Z^{j-1} x_j V_j$ слова Z, где U_i — суффикс слова Z^i и V_j — префикс слова Z^j (префикс и суффикс могут быть пустыми). Если $i = j$, то $S(W) \neq \overline{0}$ поскольку W подслово переходного слова $y_i Z^i$. Пусть $i < j$, без ограничения общности будем полагать, что $y_i = 1$, $y_j \in \{1, 2\}$. Рассмотрим случай, когда $y_j = 1$. Пусть $0 = S(W)_t = S(x_{i+1} y_{i+1} \ldots x_j)_t = S(y_i x_{i+1} y_{i+1} \ldots x_j)_t$ при любом $t = 2, \ldots, k$. Поскольку всегда либо $S(x_{i+1} y_{i+1} \ldots x_j)_1 = 0$, либо $S(y_i x_{i+1} y_{i+1} \ldots x_j)_1 = 0$ приходим к противоречию с тем, что X переходное слово гамильтонова цикла. Случай, когда $y_j = 2$ рассматривается аналогично. Нетрудно видеть, что $S(Z) = S(X) = \overline{0}$. Следовательно, для слова Z выполнены условия следствия 44 и Z является переходным словом гамильтонова цикла в ΓQ_2^n. Соответствующий слову Z гамильтонов цикл имеет требуемый спектр

по построению. ▲

Замечание 19. *Если паросочетание со спектром* $(b'_1, \ldots, b'_k)$ *и хотя бы один из использованных в конструкции циклов в* ΓQ_2^{n-k+1} *имеют полный ранг, то в результате конструкции (лемма 16) можно получить гамильтонов цикл полного ранга.*

§ 3.4.3. Существование гамильтонова цикла с заданным спектром

Докажем две леммы о спектрах гамильтоновых циклов, которые можно построить посредством описанной выше конструкции.

Лемма 17 ([53]). *Если любой допустимый целочисленный набор длины* $n-k+1$ *является спектром гамильтонова цикла в* ΓQ_2^{n-k+1}*, и имеется гамильтонов цикл со спектром* $(b_1, \ldots, b_k)$ *в* ΓQ_2^k*, то любой допустимый целочисленный набор* $(b_1, \ldots, b_k, a_{k+1}, \ldots, a_n)$ *является спектром гамильтонова цикла в* ΓQ_2^n*.*

Доказательство. На множестве упорядоченных допустимых целочисленных наборов $A = \{a \in \mathbb{D}_n \mid a_i = b_i, 1 \leq i \leq k\}$ рассмотрим лексикографический порядок. Минимальный в этом порядке набор $(b_1, \ldots, b_k, 2^k, \ldots, 2^{n-1})$ является спектром гамильтонова цикла в ΓQ_2^n. Действительно, в приведённой выше конструкции достаточно выбрать $(2, 4 \ldots, 2^{n-k}, 2)$ в качестве спектра $(a_1^i, \ldots, a_{n-k}^i, c^i)$ для любого $i \in [2^{k-1}]$. Предположим некоторые допустимые наборы из множества A не являются спектрами гамильтоновых циклов, построенных посредством конструкции из леммы 16, выберем из таких наборов лексикографически минимальный набор $d \in A$. Рассмотрим предыдущий в лексикографическом порядке набор $d' \in A$. Очевидно наборы d и d' отличаются в двух позициях $i, j \in \{k+1, \ldots, n\}$, $i < j$, причём $d'_i = d_i - 2$, $d'_j = d_j + 2$, $d'_j \geq d'_i + 4$. Тогда для спектра f одного из гамильтоновых циклов в ΓQ_2^{n-k+1}, использованных при построении цикла со спектром d' верно неравенство $f_j - f_i \geq 4$ (или $f_j - f_i = 2$ в спектрах двух циклов). Очевидно, что если в целочисленном наборе f заменить f_i на $f_i + 2$ и f_j на $f_j - 2$, то новый набор f' также будет спектром гамильтонова цикла в ΓQ_2^{n-k+1} по условию леммы. При замене в конструкции из леммы 16 цикла со спектром f на цикл со спектром f' получим, что набор

d является спектром гамильтонова цикла. Получили противоречие. В случае когда $f_j - f_i = 2$ в двух спектрах, нужно в каждом из них поменять количества рёбер направлений i и j местами и применить ту же конструкцию. ▲

Лемма 18 ([53]). *Пусть $4 \le s < k < n-1$, любые допустимые целочисленные наборы длины $n - s + 1$ являются спектрами гамильтоновых циклов,* (a) *для некоторого допустимого упорядоченного набора $b \in \mathbb{D}_n$ имеется допустимый набор, являющийся спектром гамильтонова цикла полного ранга $b' \in \mathbb{D}_s$ такой, что $b'_i \le b_i$ при $i \in [s]$ и справедливы неравенства* (b) $b_s \le 2^{n-s-1}$ *и* (c) $\sum\limits_{i=s+1}^{k} b_i \ge 2^k - 2^s$ *при таких k, что $2^{k-s-1} \le b_s$. Тогда набор b является спектром гамильтонова цикла.*

Доказательство. Пусть $d_i = b_i - b'_i$ при $i \in [s]$ и $d = \sum\limits_{i=1}^{s} d_i$. Из доказательства леммы 17 следует, что целочисленный набор $(b'_1, \ldots, b'_s, 2^s, \ldots, 2^{n-1})$ является спектром гамильтонова цикла в ΓQ_2^n, построенного посредством описанной выше конструкции с $s = k$. Пусть m — наименьшее целое число, для которого $2^{m-s-1} > b_s$. Поскольку $d_i \le b_s < 2^{m-s-1}$, набор $(2, \ldots, 2^{m-s-1}, 2^{m-s} - d_i, 2^{m-s+1}, \ldots, 2^{n-s}, 2 + d_i)$ является допустимым для любого i, $i \in [s]$.

Теперь заменим в этой конструкции s гамильтоновых циклов (по одному на каждое направление) со спектром $(2, 4, \ldots, 2^{n-s}, 2)$ на гамильтонов цикл со спектром $(2, \ldots, 2^{m-s} - d_i, 2^{m-s+1}, \ldots, 2^{n-s}, 2 + d_i)$ так, что в итоге получится цикл со спектром $(b_1, \ldots, b_s, 2^s, \ldots, 2^m - d, 2^{m+1}, \ldots, 2^{n-1})$. Рассмотрим теперь множество упорядоченных допустимых целочисленных наборов

$$A = \{a \in \mathbb{D}_n \mid a_i = b_i, 1 \le i \le s, \text{ и спектр } a \text{ удовлетворяет условию } (c)\}.$$

Выше доказано, что лексикографически наименьший спектр из A принадлежит гамильтонову циклу, построенному с помощью нашей конструкции (лемма 16). Предположим некоторые из наборов $a \in A$ не являются спектрами гамильтоновых циклов, которые могут быть получены посредством нашей конструкцией. Тогда среди таких спектров имеется лексикографически наименьший. Аналогично доказательству леммы 17 приходим к противоречию. ▲

Предложение 206. *Пусть $2 \le s \le k \le n$, $a \in \mathbb{D}_n$ и k таково, что $\sum\limits_{i=s+1}^{k} a_i < 2^k - 2^s$ и*

$2^{k-s-1} \le a_s$. *Тогда* $\mu_a(s) - \mu_a(k) \ge 2$ *и* $k \le 2s + \log \mu_a(s)$.

Доказательство. Поскольку $2^{k-s-1} \le a_s \le 2^{s-1} + \mu_a(s) \le 2^{s-1}\mu_a(s)$, имеем $k \le 2s + \log \mu_a(s)$. Если $\sum\limits_{i=s+1}^{k} a_i < 2^k - 2^s$, то $\sum\limits_{i=s+1}^{k} a_i \le 2^k - 2^s - 2$. Тогда

$$\mu_a(k) = \sum_{i=1}^{k} a_i - 2^k = \sum_{i=1}^{s} a_i - 2^s + \sum_{i=s+1}^{k} a_i - 2^k + 2^s \le \mu_a(s) - 2.$$

▲

Теорема 54 ([53]). *Существует такое число* N*, что если любой допустимый целочисленный набор длины* N *является спектром некоторого гамильтонова цикла (полного ранга в случае когда* $\sum\limits_{i=1}^{k} a_i > 2^k$ *при любом* $k < N$*), то для любого целого* $n \ge 2$ *любой допустимый целочисленный набор длины* n *является спектром некоторого гамильтонова цикла в* ΓQ_2^n.

Доказательство. Пусть $a \in \mathbb{D}_n$. Простым перебором упорядоченных допустимых наборов нетрудно установить, что $a_2 \ge 4$ и $a_4 \ge 6$ за исключением случаев, когда $a_1 = a_2 = 2$ и $a_1 = a_2 = a_3 = a_4 = 4$. Гамильтонов цикл в ΓQ_2^4 с переходной последовательностью 1213414243212343 имеет спектр $(4, 4, 4, 4)$. Существование гамильтонова цикла со спектром $a \in \mathbb{D}_n$ при $n \ge 5$ и $a_1 = a_2 = a_3 = a_4 = 4$ (или $a_1 = a_2 = 2$) следует из леммы 17.

Пусть $a_2 \ge 4, a_4 \ge 6$. Нетрудно видеть, что в любом упорядоченном допустимом наборе $a_1 \ge 2$ и $a_3 \ge 4$. Имеется гамильтонов цикл полного ранга ΓQ_2^4 с переходной последовательностью 4212312141312313 и спектром $(2, 4, 4, 6)$. Таким образом, при $s = 4$ выполнено условие (a) леммы 18 или условие леммы 17. Рассмотрим условия (b) и (c) леммы 18 при $s = 4$. Пусть $n \ge 35$, тогда $a_4 \le \frac{2^n}{n-3} \le 2^{n-5}$. Предположим условие (c) не выполнено, т. е. для некоторого $k \ge 5$ имеем $2^{k-5} \le a_4$ и $\sum\limits_{i=5}^{k} a_i < 2^k - 2^4$. Тогда $(k-4)2^{k-5} \le (k-4)a_4 < 2^k - 2^4$. Откуда имеем $k \le 35$ и $a_4 < \frac{2^{35}-2^4}{31}$. Тогда $\mu_a(4) < \mu^* = 4 \cdot \frac{2^{35}-2^4}{31}$.

Пусть $n \ge N = 2^{2^{\mu^*/2}(4+\log \mu^*)}$. Далее доказательство будем проводить по индукции. Предположим, что при m, $m < n$, любой допустимый набор является спектром гамильтонова цикла (I), причём если $m > 4$ и $\sum\limits_{i=1}^{k} a_i > 2^k$ при любом $k < m$, то набор $a \in \mathbb{D}_m$ является спектром гамильтонова цикла полного ранга (II). Для обоснова-

ния шага индукции проверим выполнение условий лемм 17 и 18, т. е. покажем, что найдётся такое $s^0 \in [n]$, для которого выполнены условия леммы 18 или условие леммы 18 — $\mu_a(s^0) = 0$. Условие (a) леммы 18 выполнено по предположению индукции. Нетрудно видеть, что $a_s \leq \frac{2^n}{n-s+1}$ для любого $s \in [n]$. Поэтому неравенство (b) $a_s \leq 2^{n-s-1}$ справедливо при $s \leq 2^{\mu^*/2}(4 + \log \mu^*) - 1$. Если $\mu(4) \geq \mu^*$, то как было показано выше условие (c) выполнено. Пусть $\mu_a(4) < \mu^*$. Определим последовательность чисел s_i рекуррентно. Пусть $s_0 = 4$. Если уже выбрано s_i, то в качестве s_{i+1} выберем такое минимальное k, для которого не выполнено условие (c) леммы 18, т. е. $\sum\limits_{i=s_i+1}^{s_{i+1}} a_i < 2^{s_{i+1}} - 2^{s_i}$. Из утверждения 206 следует, что найдётся не более $M = \mu^*/2$ таких элементов последовательности $s_1 < s_2 < \cdots < s_M$, для которых $\mu_a(s_i) > 0$. Кроме того, из утверждения 206 следует, что $s_M \leq 2^M(4 + \log \mu^*) - 1$. Если очередное s_j невозможно выбрать, то для построения искомого гамильтонова цикла применяем лемму 18, а если $\mu_a(s_j) = 0$, то применяем лемму 17. Таким образом, предположение индукции (I) обоснованно; предположение (II) вытекает из замечания 19. Для завершения доказательства теоремы достаточно применить утверждение 204. ▲

Для полного решения задачи о спектрах кодов Грея нужно обеспечить базу индукции для применения теоремы 54. Для построения гамильтоновых циклов в ΓQ_2^n при $n \leq N$ со всевозможными допустимыми спектрами можно использовать как описанную выше конструкцию, так и другие известные конструкции, в частности, конструкцию Бакоша (см. [187]).

Литература

1. Августинович С. В. Об одном свойстве совершенных двоичных кодов // Дискретн. анализ и исслед. опер. — 1995. — Т. 2, № 1. — С. 4–6.

2. Августинович С. В., Васильева А. Ю. Вычисление центрированной функции по ее значениям на средних слоях булева куба // Дискретн. анализ и исслед. опер., Сер. 1. — 2003. — Т. 10, №2. — С. 3–16.

3. Августинович С. В. Многомерные перманенты в задачах перечисления // Дискретн. анализ и исслед. опер. — 2008. — Т. 15, № 5. — С. 3–5.

4. Белоусов В. Д. n-Арные квазигруппы. — Кишинёв: "Штиинца", 1972.

5. Белоусов В. Д., Сандик М. Д. n-Арные квазигруппы и лупы // Сиб. матем. журн. — 1966. — Т. 7, № 1. — С.31–54.

6. Борисенко В. В. Неприводимые n-квазигруппы на конечных множествах составного порядка // Квазигруппы и лупы. — Кишинёв:"Штиинца", 1979. — Т. 51. из Мат. исслед. — С. 38–42.

7. Брэгман Л. М. Некоторые свойства неотрицательных матриц и их перманентов // Докл. АН СССР. — 1973. — Т. 211, №1. — С. 27–30.

8. Васильев Ю. Л. О негрупповых плотно упакованных кодах // Проблемы кибернетики. — 1962. — Вып. 8. — С. 337–339.

9. Васильев Ю.Л., Августинович С.В., Кротов Д.С. О подвижных множествах в двоичном гиперкубе // Дискретн. анализ и исслед. опер. — 2008. — Т. 15. №3. — С. 11–21.

10. Визинг В. Г. Дистрибутивная раскраска вершин графа // Дискретн. анализ и исслед. опер. — 1995. —Т. 2. №4. — С. 3–12.

11. Воробьёв К. В., Фон-дер-Флаасс Д. Г. О совершенных 2-раскрасках гиперкуба // Сиб. электрон. матем. изв. — 2010. — Т. 7. — С. 65–75.

12. Глухов М. М. О многообразиях (i, j)-приводимых n-квазигрупп // Сети и квазигруппы. — Кишинёв:"Штиинца", 1976. — Т. 39. из Мат. исслед. — С. 67–72.

13. Глухов М. М. К вопросу о приводимости главных парастрофов n-квазигрупп // Квазигруппы и их системы. — Кишинёв: "Штиинца", 1990. — Т. 113. из Мат. исслед. — С. 37–41.

14. Глухов М. М. О применениях квазигрупп в криптографии // Прикладная дискретная математика. — 2008. —Т. 2, №2. — С. 28–32.

15. Глухов М. М. О методах построения систем ортогональных квазигрупп с использованием групп // Математические вопросы криптографии. — 2011. —Т. 2, №4. — С. 5–24.

16. Гольберг В. В. Об инвариантной характеристике некоторых условий замыкания в тернарных квазигруппах // Сиб. матем. журн. — 1975. — Т. 16, № 1. — С. 22–34.

17. Гольберг В. В. О приводимых, групповых $(2n + 2)$-эдричных $(n + 1)$-тканях многомерных поверхностей // Сиб. матем. журн. — 1976. — Т. 17, № 1. — С. 44–57.

18. Гонсалес С., Коусело Е., Марков В. Т., Нечаев А. А. Рекурсивные МДР-коды и рекурсивно дифференцируемые квазигруппы // Дискрет. матем. — 1998. — Т. 10, № 2. — С. 3–29.

19. Гонсалес С., Коусело Е., Марков В., Нечаев А. Параметры рекурсивных МДР-кодов // Дискрет. матем. — 2000. — Т. 12, № 4. — С. 3–24.

GKP Горкунов Е. В., Кротов Д. С., Потапов В. Н. Об оценках числа автотопий n-арных квазигрупп порядка 4 // Тезисы докладов Межд. конф. «Мальцевские чтения» (Новосибирск, Россия. 12-15 ноября 2013). — С. 86.

20. Денисов О. В. Асимптотическая формула для числа корреляционно-иммунных порядка k булевых функций // Дискрет. матем. — 1991. — Т. 3, № 2. — С. 25–46.

21. Егорычев Г. П. Решение проблемы Ван дер Вардена для перманентов // Институт физики им. Л. В. Киренского СО АН СССР, Препринт ИФСО — 13М. Красноярск. 1980.

22. Егорычев Г. П. Доказательство гипотезы Ван дер Вардена для перманентов // Сиб. матем. журн. — 1981. — Т. 22, № 6. — С. 65–71.

23. Емеличев В. А., Ковалев М. М., Кравцов М. К. Многогранники, графы, оптимизация. — М.: Наука, 1981.

24. Зиновьев В. А., Леонтьев В. К. Несуществование совершенных кодов над полями Галуа // Проблемы управления и теории информации. — 1973. — Вып. 2. — С. 123–132.

25. Зиновьев В. А. Обобщенные каскадные коды // Пробл. передачи информ. — 1976. — Т. 12, № 1. — С. 5–15.

26. Зиновьев В. А., Зиновьев Д. В. Двоичные расширенные совершенные коды длины 16, построенные обобщенной каскадной конструкцией // Пробл. передачи информ. — 2002. — Т. 38, № 4. — С. 56–84.

27. Зиновьев В. А., Зиновьев Д. В. Двоичные расширенные совершенные коды длины 16 ранга 14 // Пробл. передачи информ. —2006. — Т. 42, № 2. — С. 63–80.

28. Зиновьев В. А., Рифа Д. О новых полностью регулярных q-ичных кодах // Пробл. передачи информ. — 2007. — Т. 43, № 2. — С. 34–51.

29. Зиновьев В. А., Зиновьев Д. В. Двоичные совершенные и расширенные совершенные коды длины 15 и 16 с рангами 13 и 14 // Пробл. передачи информ. — 2010. — Т. 46, № 1. — С. 20–24.

30. Коломеец Н. А., Павлов А. В. Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. — 2009. — №4. — С. 5–20.

31. Кротов Д. С. Нижние оценки числа m-квазигрупп порядка 4 и числа совершенных двоичных кодов // Дискретн. анализ и исслед. опер. Сер. 1. — 2000. — Т. 7, № 2. — С. 47–53.

32. Кротов Д. С. Z_4-линейные совершенные коды // Дискретн. анализ и исслед. опер. Сер. 1. — 2000. — Т. 7, № 4. — С. 78–90.

33. Кротов Д. С. Индуктивные конструкции совершенных троичных равновесных кодов с расстоянием 3 // Пробл. передачи информ. — 2001. — Т. 37, № 1. — С. 3–11.

34. Кротов Д. С., Потапов В. Н. О кратных МДР- и совершенных кодах, не расщепляемых на однократные // Пробл. передачи информ. — 2004. — Т. 40, №1. — С. 6–14.

35. Кротов Д. С., Потапов В. Н. О свитчинговой эквивалентности n-арных квазигрупп порядка 4 и совершенных двоичных кодов // Пробл. передачи информ. — 2010. — Т. 46, №3. — С. 22–28.

36. Кротов Д. С. О связи свитчинговой разделимости графа и его подграфов // Дискретн. анализ и исслед. опер. — 2010. — Т. 17, №2. — С. 46–56.

37. Курош А. Г. Общая алгебра (лекции 1969–1970 года). — М.: Наука, 1974.

38. Логачёв О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. — М.: Изд-во МЦНМО, 2004.

39. Лось А. В. Построение совершенных q-ичных кодов свитчингами простых компонент // Пробл. передачи информ. — 2006. — Т. 42, № 2. — С. 34–42.

40. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. — М.: Связь, 1979.

41. Марков А. А. О преобразованиях, не распространяющих искажения, Избранные тру- ды. Т. II. Теория алгоритмов и конструктивная математика, математическая логика, информатика и смежные вопросы. — М.: МЦНМО, 2003.

42. Минк Х. Перманенты. — М.: Мир, 1982.

43. Нечаев А. А. Код Кердока в циклической форме // Дискрет. матем. — 1989. — Т. 1, № 4. — С. 123–139.

44. Пережогин А. Л., Потапов В. Н. О числе гамильтоновых циклов в булевом кубе // Дискретн. анализ и исслед. опер. Сер. 1. — 2001. — Т. 8, № 2. — С. 52–62.

45. Пережогин А. Л. О специальных совершенных паросочетаниях в булевом кубе // Дискретн. анализ и исслед. опер. Сер. 1. — 2005. — Т. 12, № 4. — С. 51–59.

46. Пережогин А. Л., Потапов В. Н. О совершенных паросочетаниях в двоичном кубе // Дискретные модели в теории управляющих систем: VII Международная конференция, Покровское, 4–6 марта 2006 г.: Труды. М.:МАКС Пресс, 2006. — С. 272–277.

47. Пережогин А. Л. Об автоморфизмах циклов в n-мерном булевом кубе // Дискретн. анализ и исслед. опер., Сер. 1. — 2007. — Т. 14, № 3. — С. 67–79.

48. Потапов В. Н. О нижней оценке числа транзитивных совершенных кодов // Дискрет. анализ и исслед. опер. Сер. 1. — 2006. — Т. 13, № 4. — С. 49–59.

49. Потапов В. Н., Кротов Д. С. Асимптотика числа n-квазигрупп порядка 4 // Сиб. матем. журн. — 2006. — Т. 47, № 4. — С. 873–887.

50. Потапов В.Н. О совершенных раскрасках булева n-куба и корреляционно-иммунных функциях малой плотности // Сиб. электрон. матем. изв. — 2010. — Т. 7. — С. 372–382.

51. Потапов В. Н. О дополняемости частичных n-квазигрупп порядка 4 // Матем. тр. — 2011. — Т. 14, № 2. — С. 147–172.

52. Потапов В. Н. Кликосочетания в k-значном n-мерном кубе // Сиб. матем. журн. — 2011. — Т. 52, № 2. — С. 384–392.

53. Потапов В. Н. Построение гамильтоновых циклов с заданным спектром направлений рёбер в булевом n-мерном кубе // Дискретн. анализ и исслед. опер. — 2012. — Т. 19, № 2. — С. 75–83.

54. Потапов В.Н. Спектр мощностей компонент корреляционно-иммунных функций, бент-функций, совершенных раскрасок и кодов // Пробл. передачи информ. — 2012. — Т. 48, №1. — С. 54–63.

55. Потапов В. Н., Кротов Д. С. О числе n-арных квазигрупп конечного порядка // Дискрет. матем. — 2012. — Т. 24, № 1. — С. 60–69.

56. Потапов В. Н. Бесконечномерные квазигруппы конечного порядка // Матем. заметки. — 2013. — Т. 97, Вып.3. — С. 457–465.

57. Потапов В. Н. Многомерные латинские битрейды // Сиб. матем. журн. — 2013. — Т. 54, № 2. — С. 407–416.

58. Пулатов А. К. О структуре плотно упакованных $(n, 3)$-кодов // Дискретный Анализ. — 1976. — Вып. 29. — С. 53–60.

59. Сапоженко А. А. К вопросу о числе совершенных кодов // Материалы XVI Международной конференции "Проблемы теоретической кибернетики"(Н.Новгород, 20–25 июня 2011 г.) Н.Новгород: Изд-во Нижегородского госуниверситета. — 2011. — С. 416–419.

60. Сачков В. Н., Тараканов В. Е. Комбинаторика неотрицательных матриц.. — М.: Научное издательство «ТВП», 2000.

61. Соловьёва Ф. И. О построении транзитивных кодов // Пробл. передачи информ. — 2005. — Т. 41, №3. — С. 23–31.

62. Соловьёва Ф. И., Лось А. В. О пересечениях q-значных совершенных кодов // Сиб. матем. журн. — 2008. — Т. 49. №2. — С. 464–474.

63. Тарannиков Ю. В. О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Выпуск 11. М.: Физматлит. — 2002. — С. 91–148.

64. Тарannиков Ю. В. Комбинаторные свойства дискретных структур и приложения к криптологии. — М.:Изд-во МЦНМО, 2011

65. Токарева Н. Н. Бент-функции: результаты и приложения. Обзор работ // Прикладная дискретная математика. — 2009. — №1. —С. 15–37.

66. Тужилин М. Э. Латинские квадраты и их применение в криптографии // Прикладная дискретная математика. Приложение. — 2012. — № 5. — С. 30–32.

67. Фаликман Д. И. Доказательство гипотезы Ван дер Вардена о перманенте дважды стохастической матрицы // Матем. заметки. — 1981. — Т. 29, Вып. 6. — С. 931–938.

68. Фон-Дер-Флаасс Д. Г. Совершенные 2-раскраски гиперкуба // Сиб. матем. журн. — 2007. — Т. 48. №4. — С. 923–930.

69. Фон-Дер-Флаасс Д. Г. Совершенные 2-раскраски 12-мерного куба, достигающие границы корреляционной иммунности // Сиб. электрон. матем. изв. — 2007. — Т. 4. — С. 292–295.

70. Френкин Б. Р. О приводимости и сводимости в некоторых классах n-группоидов II. — Кишинёв: "Штиинца", 1972. — Т. 7:1(23) из Мат. исслед. — С. 150–162.

71. Халявин А. В. Оценка мощности ортогональных массивов большой силы // Вестник МГУ. Серия 1. Математика. Механика. — 2010. — Т. 65, №3. — С. 49–51.

72. Холл М. Комбинаторика. — М: Мир,1970.

73. Черёмушкин А. В. Каноническое разложение n-арных квазигрупп // Исследование операций и квазигрупп. — Кишинёв:"Штиинца", 1988. — Т. 102. из Мат. исслед. — С. 97–105.

74. Черёмушкин А. В. Бесповторная декомпозиция сильно зависимых функций // Дискрет. матем. — 2004. — Т. 16, Вып. 3. — С. 3–42.

75. Черёмушкин А. В. Почти все латинские квадраты имеют тривиальную группу автострофий // Прикладная дискретная математика. — 2009. — №3. — С. 29–32.

76. Эндрюс Г. Э. Теория разбиений. — М.:Наука, 1982.

77. Abbott H. L. Hamiltonian circuits and paths on the n-cube // Canad. Math. Bull. — 1966. — V. 9, N 5. — P. 557–562.

78. Akivis M. A. and Goldberg V. V. Solution of Belousov's Problem // Discuss. Math., Gen. Algebra Appl. — 2001. — V. 21, N 1. — P. 93-103.

79. Avgustinovich S.V., Lobstein A.C., Soloveva F.I. Intersection matrices for partitions by binary perfect codes // IEEE Trans. Inform. Theory. — 2001. — V. 47, N 4. — P. 1621–1624.

80. Avgustinovich S. V., Heden O., Solov'eva F. I. The classification of some perfect codes // Des. Codes and Cryptography. — 2004. — V. 31, N. 3. — P. 313–318.

81. Avgustinovich S. V., Heden O., Solov'eva F. I. On intersections of perfect binary codes // Bayreuth. Math. Schr. — 2005. — N 74. — P. 1–6.

82. Avgustinovich S. V., Heden O., Solov'eva F. I. On intersection problem for perfect binary codes // Des. Codes Cryptography. — 2006. — V. 39., N 3. — P. 317–322.

83. Ball S. A proof of the MDS conjecture over prime fields // Proceedings of 3rd International Castle Meeting on Coding Theory and Application (September 11-15, 2011, Cardona, Spain). — 2011. —P. 43–46.

84. Ball S. On sets of vectors of a finite vector space in which every subset of basis size is a basis // J. Eur. Math. Soc. — 2012. — V. 14, N. 3. — P. 733–748.

85. Ball S., De Beule J. On sets of vectors of a finite vector space in which every subset of basis size is a basis II // Des. Codes Cryptogrophy. — 2012. — V. 65, N. 1-2. — P. 5–14.

86. Bhat G. S., Savage C. D. Balanced Gray codes // The Electronic J. of Combinatorics. — 1996. — V. 3. — paper 25.

87. Bierbrauer J. Bounds on orthogonal arrays and resilient functions // J. of Combinatorial Designs. — 1995. — V. 3, N. 3. — P. 179–183.

88. Borges J., Mogilnykh I.Y., Rifa J., Solov'eva F.I. Structural properties of binary propelinear codes // Advances in Mathematics of Communications. — 2012 — V. 6, N. 3. — P. 329–346.

89. Borges J., Mogilnykh I. Yu., Rifa J., Solov'eva F. I. On the number of nonequivalent propelinear extended perfect codes // arXiv:1303.0680 [math.CO]

90. Bose R. C., Shrikhande S. S., Parker E. T. Further results on the construction of mutually orthogonal latin squares and the falsity of Euler's conjecture // Can. J. Math. — 1960. — V. 12. — P. 189–203.

91. Brouwer A. E., van Rees C. H. J. More mutually orthogonal Latin squares // Discrete Math. — 1982. — V. 39, N. 3. — P. 263–281.

92. Bruck R. H., Ryser H. J. The nonexistence of certain finite projective planes // Can. J. Math. — 1949. — V. 1. — P. 88–93.

93. Bryant D., Cavenagh N. J., Maenhaut B., Pula K., Wanless I.M. Nonextendible latin cuboids // SIAM J. on Discrete Math. — 2012. —V. 26, N. 1. — P. 239–249.

94. Canfield R. E., Gao Z., Greenhill C., McKay B., Robinson R. W. Asymptotic enumeration of correlation-immune Boolean functions // Cryptogr. Commun. — 2010. —V. 2. — P. 111–126.

95. Carlet C., Gouget A. An upper bound on the number of m-resilient Boolean functions // Advances in cryptology-ASIACRYPT 2002, Lecture Notes in Comput. Sci., no. 2501, Berlin: Springer. — 2002. — P. 484–496.

96. Carlet C. Boolean functions for cryptography and error correcting codes. Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science,

and Engineering"published by Cambridge University Press, Yves Crama and Peter L. Hammer (eds.) — 2010. — P. 257–397.

97. Carlet C. Two new classes of bent functions // Advances in Cryptology - EUROCRYPT'93, Lecture Notes in Comput. Sci., no. 765, Berlin: Springer-Verlag. — 1994. — P. 77–101.

98. Cavenagh N. J. The theory and application of latin bitrades: A survey // Math. Slovaca. — 2008. — V. 58, N. 6. — P. 691–718.

99. Camion P., Courteau B., Delsarte P. On r-partition designs in Hamming spaces // Appl. Algebra Engenr. Comm. Comput. — 1992. — V. 2, N. 3. — P. 147–162.

100. Colbourn C. J., Dinitz J. H. Mutually orthogonal Latin squares: a brief survey of constructions // J. Statist. Plann. Inference. — 2001. — V. 95, N. 1-2. — P. 9–48.

101. Cruse A. B. On the finite complection of partial latin cube // J. Comb. Theory, Ser. A. — 1974. — V. 17, N 1. — P. 112–119.

102. Cutler J., Öhman, L.-D. Latin squares with forbidden entries // Electron. J. Combin. — 2006. — V. 13. — R. Paper 47.

103. Delsarte P. Bounds for unrestricted codes by linear programming // Philips Res. Reports. — 1972. — V. 27. — P. 272–289.

104. Delsarte P. An algebraic approach to the association schemes of coding theory // Philips Res. Reports. — 1973. — V. 10. — P. 1–97.

105. Denes J., Keedwel A. D. Latin squares and their applications. — New York: Academic Press, 1974.

106. Dixon E., Goodman S. On the number of Hamiltonian circuits in the n-cube // Proc. Amer. Math. Soc. — 1975. — V. 50. — P. 500–504.

107. Douglas R. G. Bounds on the number of Hamiltonian circuits in the n-cube // Discrete Math. — 1977. — V. 17, N 2. — P. 143–146.

108. Ethier J. T., Mullen G. L. Strong forms of orthogonality for sets of hypercubes // Discrete Math. — 2012. — V. 312, N 12-13. — P. 2050–2061.

109. Etzion T. Optimal constant weight codes over Z_k and generalized designs // Discrete Math. — 1997. — V. 169. — P. 55–82.

110. Etzion T., Vardy A. Perfect binary codes and tilings: problems and solutions // SIAM J. Discrete Math. — 1998. — V. 11, N 2. — P. 205–223.

111. Feder T., Subi C. Nearly tight bounds on the number of Hamiltonian circuits of the hypercube and generalizations // Inform. Process. Lett. — 2009. — V. 109, N 5. — P. 267–272.

112. Fink J. Perfect matchings extend to Hamilton cycles in hypercubes // J. Comb. Theory, Ser. B. — 2007. — V. 97, N 6. — P.1074–1076.

113. Fon-Der-Flaass D. G. A bound of correlation immunity // Sib. Ehlektron. Mat. Izv. — 2007. — V. 4. — P. 133–135.

114. Friedman J. On the bit extraction problem // Proc. 33rd IEEE Symposium on Foundations of Computer Science. — 1992. — P. 314–319.

115. Fu H.-L. On latin $(n \times n \times (n-2))$-parallelepipeds // Tamkang J. Math. —1986. — V. 17. — P. 107–111.

116. Gilbert E. N. Gray codes and paths on the n-cube // Bell System Tech. J. — 1958. — V. 37. — P. 815–826.

117. Godsil C. D. Equitable partitions. Combinatorics, Paul Erdos is eighty, Vol. 1, 173-192, Bolyai Soc. Math. Stud., Janos Bolyai Math. Soc., Budapest, 1993.

118. Golay M. J. E. Notes on digital coding // Proc. IRE. — 1949. — V. 37. — P. 657.

119. Goodaire E. G., Robinson D. A. A class of loops which are isomorphic to all loop isotopes // Can. J. Math. — 1982. — V. 34, N 3. — P. 662–672.

120. Guskov G. K., Mogilnykh I. Yu., Solov'eva F. I. Ranks of propelinear perfect binary codes // arXiv:1210.8253 [math.CO]

121. Hall M. Jr. An existance theorem for latin squares // Bull. Amer. Math. Soc. — 1945. — V. 51. — P. 387–388.

122. Hamburger P., Pippert R. E., Weakley W. D. On a leverage problem in the hypercube // Networks. — 1992. — V. 22. — P. 435-439.

123. Hamming R. W. Error detecting and error correcting codes // Bell System Tech. J. — 1950. — V. 29, N 2. — P. 147–160.

124. Hammons A. R. Jr., Kumar P. V., Calderbank A. R., Sloane N. J. A., Sole P. The Z4-linearity of Kerdock, Preparata, Goethals, and related codes // IEEE Trans. Inform. Theory — 1994. —V. 40, N 2. — P. 301–319.

125. Hanani H. On some tactical configurations // Can. J. Math. — 1963. — V. 15. — P. 702–722.

126. Handbook of combinatorial designs / Ed. by C. J. Colbourn and J. H. Dinitz. Discrete Mathematics and its Applications. — Second edition. — Chapman & Hall/CRC, 2007.

127. Heden O., Krotov D. S. On the structure of non-full-rank perfect q-ary codes // Adv. Math. Commun. — 2011. — V. 5, N 2. — P. 149–156.

128. Heden O., Soloveva F. I., Mogilnykh I. Yu. Intersections of perfect binary codes // Proc. of IEEE Int. Conf. on Computational Technologies in Electrical and Electronics Engineering (Irkutsk, Russia. July 11–15, 2010). Piscataway: IEEE, 2010. — P. 50–51.

129. Horak P. Latin parallelepipeds and cubes // J. of Comb. Theory, Ser. A. — 1982. — V. 33, N. 2. — P. 213–214.

130. Hulpke A., Kaski P., Östergård P. R. J. The number of Latin squares of order 11 // Math. Comp. — 2011. — V. 80, N 274. — P. 1197–1219.

131. Ito T. Creation method of table, creation apparatus, creation program and program storage medium. — 2004. — http://www.freepatentsonline.com/y2004/0243621.html.

132. Ji L. An improvement on H design //J. Combin. Des. — 2009. — V. 17. — P. 25–35.

133. Jia X. W., Qin Z. P. The number of Latin cubes and their isotopy classes // J. Huazhong Univ. Sci. Technol. — 1999. — V. 27, N. 11. — P. 104–106.

134. Kasami T., Tokura N. On the weight structure of Reed—Muller codes // IEEE Trans. Inform. Theory. — 1970. — V. IT-16. — P. 752–759.

135. Kasami T., Tokura N., Azumi S. On the weight enumeration of weights less than $2.5d$ of Reed — Muller codes // Inform. and Control. —1976. — V. 30. — P. 380–395.

136. Kaski P., Östergård P. R. J. Classification algorithms for codes and designs. — Berlin: Springer-Verlag, 2006. Vol. 15 of Algorithms and Computation in Mathematics.

137. Knuth D. E. The art of computer programming, Vol. 4. — Addison-Wesley, 2004.

138. Kochol M. Latin $(n \times n \times (n-2))$-parallelepipeds not completing to a Latin cube // Math. Slovaka. — 1989. — V. 39, N. 2. — P. 121–125.

139. Kochol M. Relatively narrow latin parallelepipeds that cannot be extended to a Latin cube // Ars Combin. — 1995. — V. 40. — P. 247–260.

140. Kochol M. Non-extendible latin psrallelepipeds // Information Processing Letters. — 2012. — V. 112, N. 24. — P. 942–943.

141. König D. Grafok es alkalmazasuk a determinansok es a halmazok elmeletere // Matematikai es Termeszettudomanyi Ertesito. — 1916. — V. 34. — P. 104–119.

142. Kreweras G. Matchings and Hamiltonian cycles on hypercubes // Bull. Inst. Comb. Appl. — 1996. — V. 16. — P. 87–91.

143. Krotov D. S., Potapov V. N. On the reconstruction of n-quasigroups of order 4 and the upper bounds on their numbers // Proc. of the Conference devoted to the 90th

anniversary of Alexei A. Lyapunov (Novosibirsk, Russia, 2001). — 2001. — P. 323–327. http://www.sbras.ru/ws/Lyap2001/2363.

144. Krotov D. S. Z_4-linear Hadamard and extended perfect codes // International Workshop on Coding and Cryptography (Paris, France, 8-12 January 2001), Electronic Notes in Discrete Mathematics, 6, eds. D. Augot, C. Carlet, Amsterdam: Elsevier, — 2001. — P. 107-112.

145. Krotov D. S. On irreducible n-ary quasigroups with reducible retracts // European J. Comb. — 2008. — V. 29, N 2. — P. 507–513.

146. Krotov D. S. On decomposability of 4-ary distance 2 MDS codes, double-codes, and n-quasigroups of order 4 // Discrete Math. — 2008. — V. 308, N 15. — P. 3322–3334.

147. Krotov D. S. On reducibility of n-ary quasigroups // Discrete Math. — 2008. — V. 308, N 22. — P. 5289–5297.

148. Krotov D. S., Potapov V. N., Sokolova P. V. On reconstructing reducible n-ary quasigroups and switching subquasigroups // Quasigroups and Related Systems. — 2008. — V. 16, N 1. — P. 55–67.

149. Krotov D. S., Avgustinovich S. V. On the number of 1-perfect binary codes: a lower bound // IEEE Trans. Inform. Theory. — 2008. — V. 54, N 4. — P. 1760–1765.

150. Krotov D. S., Potapov V. N. n-Ary quasigroups of order 4 // SIAM J. Discrete Math. — 2009. — V. 23, N 2. — P. 561–570.

151. Krotov D. S. On the binary codes with parameters of doubly-shortened 1-perfect codes // Des. Codes and Cryptography. — 2010. — V. 57, N 2. — P. 181–194.

152. Krotov D. S. On weight distributions of perfect colorings and completely regular codes // Des. Codes and Cryptography. — 2011. — V. 61, N 3. — P. 315–329.

153. Krotov D. S., Ostergard P. R. J., Pottonen O. On Optimal Binary One-Error-Correcting Codes of Lengths 2^m-4 and 2^m-3 // IEEE Trans. on Inform. Theory. — 2011. — V. 57, N 10. — P. 6771–6779.

154. Krotov D. S., Potapov V. N. On connection between reducibility on an n-ary quasigroup and that of its retracts // Discrete Math. — 2011. — V. 311, N 1. — P. 58–66.

155. Krotov D. S. On the binary codes with parameters of triply-shortened 1-perfect codes // Des. Codes and Cryptography. — 2012. — V. 64, N 3. — P. 275–283.

156. Krotov D. S., Potapov V. N. Constructions of transitive latin hypercubes // arXiv.org eprint math., math.CO/1303.0004.

157. Krotov D. S., Potapov V. N. Propelinear 1-perfect codes from quadratic functions // IEEE Trans. Inform. Theory. 2014. — V. 60, N 4. — P. 2065–2068.

158. Kunen K. G-loops and permutation groups // J. Algebra — 1999. — V. 220, N 2. — P. 694–708.

159. Laywine C. F., Mullen G. L. Discrete mathematics using Latin squares. — New York: Wiley, 1998.

160. Linial N., Luria Z. An upper bound on the number of high-dimensional permutations // Combinatorica — 2014. — V. 34, N 4. — P. 471–486.

161. Markovski S., Dimitrova V., Mileva A. A new method for computing the number of n-quasigroups // Buletinul Academiei de Stiinte a Republicii Moldova. Matematica. — 2006. — V. 52, N 3. — P. 57–64.

162. McKay B. D., Wanless I. M. On the number of Latin squares // Ann. Comb. — 2005. — V. 9, N 3. — P. 335–334.

163. McKay B. D., Wanless I. M. A census of small Latin hypercubes // SIAM J. Discrete Math. — 2008. — V. 22, N 2. — P. 719–736.

164. Mills W. H. On the existence of H design // Proceedings of the Twenty-First Southeastern Conference on Combinatorics, Graph Theory, and Computing, Congr. Numer. 79, 1990. — P. 129–141.

165. Mullen, G. L., Weber, R. E. Latin Cubes of Order ≤ 5 // Discrete Math. — 1988. — V.32, N 3. — P. 291-298.

166. P. R. J. Östergård. Switching codes and designs // Discrete Math. — 2012. — V. 312, N 3. — P. 621–632.

167. Östergård P. R. J., Pottonen O. The perfect binary one-error-correcting codes of length 15. I. Classification // IEEE Trans. Inform. Theory. — 2009. — V. 55, N 10. — P. 4657–4660.

168. Östergård P. R. J., Pottonen O., Phelps K. T. The perfect binary one-error-correcting codes of length 15: Part II-properties // IEEE Trans. Inform. Theory. — 2010. — V. 56, N 6. — P. 2571–2582.

169. Phelps K. T. A general product construction for error correcting codes // SIAM J. Algebraic Discrete Methods. — 1984. — V. 5, N 2. — P. 224–228.

170. Phelps K. T., Villanueva M. Ranks of q-ary 1-perfect codes // Des. Codes and Cryptography. — 2002. — V. 27, N 1-2. — P. 139–144.

171. Phelps K. T. A general product construction for error correcting codes // SIAM J. Algebraic and Discrete Methods. — 1984. — V. 5, N 2. — P. 224–228.

172. Potapov V. N. On perfect 2-colorings of the q-ary n-cube // Discrete Math. — 2012. — V. 312, N 6. — P. 1269–1272.

173. Potapov V. N. On the multidimensional permanent and q-ary designs // Сибирские Электронные Математические Известия, Siberian Electronic Mathematical Reports. 2014. — V. 11, — P. 451–456.

174. Rao C. R. Factorial experiments derivable from combinatorial arguments of array // J. Royal Statist. Soc. — 1947. — V. 9, N 1. — P. 128–139.

175. Ryser H. J. A combinatorial theorem with an application to latin rectangles // Proc. Amer. Math. Soc. — 1951. — V. 2. — P. 550–552.

176. Sarkar P. Spectral domain analysis of correlation immune and resilient Boolean fuctions // Cryptology ePrint archive (http://eprint.iacr.org/), Report 2000/049, September 2000, 14 p.

177. Shcherbacov V. A. Quasigroups in cryptology // Comput. Sci. J. Mold. — 2009. — V. 17, N 2. — P. 193–228.

178. Schönheim J. On linear and nonlinear single-error-correcting q-nary perfect codes // Inform. and Control. — 1968. — V. 12, N 1. — P. 23–26.

179. Schrijver A. Counting 1-factors in regular bipartite graphs // J. Comb. Theory, Ser. B. — 1998. — V. 72, N 1. — P. 122–135.

180. Shapiro G. S., Slotnik D. S. On the mathematical theory of error correcting codes // IBM Journal of Research Development. — 1959. — V. 3, N 1. — P. 68–72.

181. Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Trans. Inform. Theory. — 1984. —V. 30, N 5. — P. 776–780.

182. Singleton R. Minimum distance q-nary codes // IEEE Trans. Inform. Theory. — 1964. —V. 10, N 2. — P. 116–118.

183. Soedarmadji E. Latin hypercubes and MDS Codes // Discrete Math. — 2006. — V. 306, N 12. — P. 1232–1239.

184. Sokhatsky F. The deepest repetition-free decompositions of nonsingular functions of finite-valued logics // Proceeding of the Twenty-Sixth International Sumposium on Multiple-Valued Loggic. — Santiago de Compostela, Spain. 1996. — P. 279–282.

185. Stinson D. R. Combinatorial designs: construction and analysis. — New York: Springer-Verlag, 2004.

186. Svanström M. A class of 1-perfect ternary constant-weight codes // Des. Codes and Cryptography. — 1999. — V. 18, N 1–3. — P. 223–230.

187. Suparta I. N. A simple proof for the existence of exponentially balanced Gray codes // Electron. J. Combin. — 2005. — V. 12. — Note 19.

188. Tietäväinen A. On the nonexistance of perfect codes over finite fields // SIAM J. Appl. Math. — 1973. — V. 24— P. 88–96.

189. Wilson R. L. Jr. Isotopy-isomorphy loops of prime order // J. Algebra — 1974. — V. 31, N 1. — P. 117–119.

190. Wilson R. M. Concerning the number of mutually orthogonal Latin squares // Discrete Math. — 1979. — V. 9, N 2. — P. 181–198.

191. Zaslavsky, T. Quasigroup associativity and biased expansion graphs // Electron. Res. Announc. of the Amer. Math. Soc. — 2006. — V. 12. — P. 13–18.

192. Zaslavsky T. Associativity in multary quasigroups: the way of biased expansions // Aequationes Mathematicae. — 2012. — V. 83, N 1-2. — P. 1–66.