Совершенные структуры в кодировании и криптографии

В. Н. Потапов

Содержание

1 Графы и их раскраски **5**
1.1 Некоторые определения и обозначения в теории графов . . 5
1.2 Раскраски графов 8
1.3 Совершенные раскраски и передача сообщений 10
1.4 Совершенные и МДР-коды в гиперкубах 11

2 Алгебраические свойства совершенных раскрасок **14**
2.1 Стохастические матрицы 14
2.2 Матричное уравнение совершенной раскраски 16
2.3 Теорема о спектральном разложении матрицы смежности 19
2.4 Совершенные раскраски и собственные функции 21
2.5 Ортогональность совершенных раскрасок 23

3 Экстремальные свойства совершенных раскрасок **25**
3.1 Разрезы и независимые множества в графах 25
3.2 Дельсартовы клики 29
3.3 Раскраски графов, регулярных по расстоянию 2 30

4 Дистанционно-регулярные графы **35**
4.1 Определение дистанционно-регулярного графа 35
4.2 Полиномы Кравчука 38
4.3 Теорема Шапиро–Злотника–Мартина 39
4.4 Нижняя граница мощности носителя 40
4.5 Полностью регулярные коды 43
4.6 Дельсартовы клики II 46
4.7 Теорема о восстановлении совершенной раскраски по среднем слою 49

5 Декартовы произведения графов **52**
5.1 Собственные функции декартова произведения графов . . 52
5.2 Раскраски декартова произведения графов 54
5.3 Существенные переменные и теорема Вегенера 56

6 Конструкции совершенных раскрасок **58**
6.1 Склеивание цветов 58
6.2 Алгоритм Вейсфейлера—Лемана и индуцирование 59
6.3 Накрытия 62
6.4 Орбитные раскраски и раскраски графов Кэли 66

7 Совершенные раскраски мультиграфов и гиперграфов **72**

8 Латинские квадраты и 1-факторизации графов 77
8.1 Латинские квадраты 77
8.2 Теоремы Визинга и Райзера 78
8.3 Теоремы Холла, Кёнига и Эгервари 81
8.4 Совершенные паросочетания 83
8.5 Перманенты и дважды стохастические матрицы 84
8.6 Симметричные латинские квадраты 86

9 МДР-коды с кодовым расстоянием большим чем 2 89
9.1 Основные свойства МДР-кодов 89
9.2 Ортогональные системы квазигрупп 91
9.3 Линейные МДР-коды 95
9.4 Системы попарно ортогональных латинских квадратов . . 98

10 Комбинаторные t-дизайны 103
10.1 Дизайны как совершенные раскраски графов и гиперграфов 103
10.2 Системы Штейнера 106
10.3 Симметричные дизайны и проективные плоскости 109

11 Преобразование Фурье 111
11.1 Характеры абелевых групп 111
11.2 Многочлены Кравчука и характеры в гиперкубах 117
11.3 Матрицы Адамара 118
11.4 Определение и свойства преобразования Фурье 120
11.5 Преобразования Фурье и свёртка 125

12 Корреляционно-иммунные функции 128
12.1 Функции, уравновешенные в гранях 128
12.2 Корреляционная иммунность и преобразование Фурье . . . 130
12.3 Корреляционная иммунность совершенных раскрасок . . . 132
12.4 Ортогональные массивы и неравенство Рао 134
12.5 Неравенство Бирбрауэра—Фридмана 135
12.6 Теорема Фон-дер-Флаасса 139

13 Дуальный код, тождества Мак-Вильямс и Саркара 141
13.1 Дуальный код 141
13.2 Код Адамара 144
13.3 Расширенный 1-совершенный код и матрицы Адамара . . 145
13.4 Тождество Саркара 146
13.5 Число существенных переменных и тестирующие множества совершенных раскрасок 148
13.6 Преобразование Мак-Вильямс 150
13.7 Граница линейного программирования 151
13.8 Весовые спектры совершенной раскраски 154

14 Бент-функции, разностные множества и сильно регулярные графы 158
14.1 Определение и основные свойства бент-функций 158
14.2 Булевы бент-функции и платовидные функции 161
14.3 Нелинейность q-ичных функций 163
14.4 Разностные множества 166
14.5 Разностные множества и сильно регулярные графы как совершенные раскраски 169
14.6 Бент-функции как совершенные раскраски 171
14.7 Спреды 175

15 Полиномиальное представление булевых функций 178
15.1 Преобразование Мёбиуса 178
15.2 Степень булевой функции 180
15.3 Алгебраическая иммунность 184
15.4 Представление линейного кода многочленом 185

16 Замощения и совершенные коды 187
16.1 Замощения 187
16.2 Совершенные коды с расстоянием большим, чем 3 189
16.3 Совершенные коды в гиперкубах 190

1 Графы и их раскраски

1.1 Некоторые определения и обозначения в теории графов

Рассмотрим неориентированный *граф* G без кратных рёбер и петель[1]. Такие графы называют *простыми*. Всюду в дальнейшем при использовании термина "граф" имеется ввиду простой граф, если явно не указано противное. Через $V(G)$ обозначается множество *вершин* графа G, через $E(G) \subset \binom{V(G)}{2}$ — множество *рёбер* графа $G = (V(G), E(G))$.[2]

Граф называется *связным*, если любые две его вершины соединены *путём* из рёбер. Связному графу соответствует дискретное метрическое пространство: точки пространства — вершины графа, расстояние между двумя точками — количество ребёр в кратчайшем пути, соединяющим точки. И наоборот, некоторые метрические пространства могут быть представлены в виде графа, в котором находящиеся на расстоянии 1 вершины, соединены рёбрами. Максимальное расстояние между вершинами графа называется *диаметром* графа.

Пример 1. Рассмотрим $Q_q = \{0, 1, \ldots, q-1\}$. На множестве Q_q^n определим расстояние Хэмминга $d(x, y)$ равное числу позиций, в которых различаются упорядоченные наборы $x, y \in Q_q^n$. Метрическое пространство (Q_q^n, d) и соответствующий ему граф называются *n-мерным q-ичным гиперкубом*, если $q = 2$, то булевым n-кубом.

Кликой в графе называется подграф, все вершины которого попарно соединены рёбрами. Одномерный q-ичный куб является кликой на q вершинах. В теории графов клика на q вершинах имеет стандартное обозначение K_q. Однако, мы в дальнейшем будем для удобства придерживаться обозначения Q_q и Q_q^n в многомерном случае, как для метрического пространства так и для соответствующего ему графа, а также множества его вершин.

Степенью вершины графа называется число *инцидентных* ей рёбер. В случае простого графа степень вершины равна числу *смежных* с ней вершин.

Граф называется *регулярным (однородным)*, если степени всех его вершин равны. Если степень любой вершины графа равна r, то граф будем называть *r-регулярным*. Произвольно занумеруем вершины графа: $V(G) = \{v_i\}$.

Матрица смежности графа определена равенством

$$M_{n\times n}(G) = (m_{ij}) = \begin{cases} 1, \text{ если} (v_i, v_j) \in E(G); \\ 0, \text{ иначе.} \end{cases}$$

[1] Петлёй называется ребро с началом и концом в той же вершине.

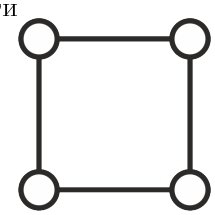
[2] Здесь и далее через $\binom{A}{k}$ — множество неупорядоченных k-элементных подмножеств множества A.

Неориентированный граф без кратных рёбер имеет симметричную $(0,1)$-матрицу смежности. Если G — регулярный граф, то в каждой строке и в каждом столбце матрицы смежности имеется одинаковое количество единиц, равное степени вершин графа.

Дополнением графа G называется граф $\overline{G}$ с таким же множеством вершин $V(\overline{G}) = V(G)$ и дополнительным множеством рёбер $E(\overline{G}) = \binom{V(G)}{2} \setminus E(G)$.

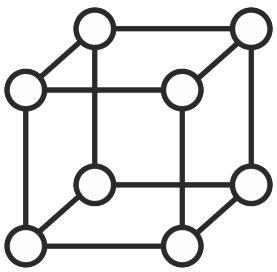
Матрица смежности дополнения графа, удовлетворяет равенству $\overline{M} = J - I - M$, где I — единичная матрица, а J — матрица, все элементы которой равны 1.

Пример 2. Простейший граф Q_2 состоит из одного ребра. Цикл на четырех вершинах, он же булев 2-куб Q_2^2 имеет следующую матрицу смежности



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

Пример 3. Матрица смежности булева куба Q_2^3, имеющего восемь вершин, приведена ниже.



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

В рассмотренных выше примерах матриц смежности вершины булева квадрата и булева куба занумерованы лексикографически.

Граф G называется *k-дольным*, если его вершины можно разделить на k долей так, что вершины каждой доли не смежны, т. е. нет рёбер соединяющих две вершины, входящих в одну долю. Если нумеровать вершины графа так, чтобы каждая доля была занумерована подряд, то матрица смежности k-дольного графа будет содержать нулевые квадратные подматрицы на диагонали. Например, матрица смежности двудольного графа при такой нумерации вершин имеет вид $M = \begin{pmatrix} O & B \\ B^T & O \end{pmatrix}$, где O — матрица, состоящая из нулей, а B — матрица смежности долей. Булев n-куб Q_2^n при любом n является двудольным графом. В частности, после перенумерации вершин матрица смежности 2-мерного булева куба

приобретает вид $\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$. Двудольный граф, у которого степень вершины зависит только от доли, в которую попала вершина, называется *бирегулярным*.

Два графа называются *изоморфными*, если можно установить взаимно однозначное соответствие между их вершинами, при котором рёбра одного графа переходят в рёбра другого графа.

Заметим, что графы изоморфны тогда и только тогда, когда их матрицы смежности переходят друг в друга синхронной перестановкой строк и столбцов.

Множество вершин гиперкуба Q_q^n, у которых зафиксировано значение одной координаты, например $x_n = 0$, называется *гипергранью*. Подграф гиперкуба, порождённый вершинами гиперграни, изоморфен гиперкубу на единицу меньшей размерности, т. е. Q_q^{n-1}. Зафиксировав m координат, мы получаем *грань* размерности $n-m$, которой соответствует подграф[3] изоморфный гиперкубу Q_q^{n-m}.

Произвольное подмножество вершин графа мы будем, для краткости, называть *кодом*. Такое название связано с тем, что основным приложением излагаемой далее теории совершенных структур является теория кодирования.

Автоморфизмом графа G называется такая перестановка его вершин $\pi : V(G) \to V(G)$, при которой рёбра переходят в рёбра, т. е. $\{u, v\} \in E(G) \Leftrightarrow \{\pi(u), \pi(v)\} \in E(G)$.

Множество автоморфизмов графа является группой и обозначается $Aut(G)$. *Автоморфизмами кода* $C \subset V(G)$ называются автоморфизмы $\pi \in Aut(G)$, графа G, сохраняющие код, т. е. $\pi(C) = C$.

Пример 4. Автоморфизмами булева n-куба являются любые перестановки координат и прибавление (по модулю 2) произвольного двоичного вектора.

По определению, автоморфизмами графа являются те и только те перестановки его вершин, которые сохраняют расстояние 1, а значит и все остальные расстояния в соответствующем графу дискретном метрическом пространстве. То есть множество автоморфизмов графа совпадает с множеством изометрий этого пространства. Поэтому автоморфизмы графа, особенно гиперкуба, часто называют изометриями, а изоморфные подмножества вершин графа – изометричными или эквивалентными кодами.

Граф G назвается *вершинно транзитивным*, если для любых двух вершин графа $v, v' \in V(G)$ найдётся такой $\pi \in Aut(G)$, что $v' = \pi(v)$. Код

[3] Здесь и далее имеется ввиду порождённый подграф, т. е. подмножество вершин графа с инцидетными только этим вершинам рёбрами.

$C \subset V(G)$ называется вершинно транзитивным, если для любых двух вершин кода найдётся автоморфизм кода, переводящий одну вершину в другую.

Вершинно транзитивный граф G называется *рёберно транзитивным*[4], если для любых двух ребер графа $e, e' \in V(G)$ найдётся такой $\pi \in Aut(G)$, что $e' = \pi(e)$, где $e = \{u, v\}$ и $\pi(e) = \{\pi(u), \pi(v)\}$.

Примерами рёберно транзитивных графов являются q-ичные гиперкубы любой размерности. Группы автоморфизмов q-ичных гиперкубов рассмотрены в разделе 6.4.

1.2 Раскраски графов

Определение 1. *Пусть $\{1, \ldots, k\}$ — множество из k цветов. Тогда раскраской вершин графа G называется функция $f : V(G) \to \{1, \ldots, k\}$.*

В комбинаторике рассматриваются раскраски не только вершин, но и рёбер графов. В дальнейшим под раскраской графа подразумевается раскраска его вершин, если явно не указано противное.

Для каждой вершины $x \in V(G)$ определим окрестность вершины (единичную сферу с центром в вершине) следующим образом: $S_1(x) = \{y \in V(G) \mid \{x, y\} \in E(G)\}$. Множество $S_1(x)$ состоит из вершин, смежных с вершиной x. Будем также говорить, что вершина x "видит" смежные с ней вершины.

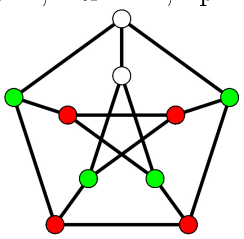
Пусть $f(x) = i$, обозначим $s_{ij}(x) = |S_1(x) \cap f^{-1}(j)|$.

Определение 2. *Раскраска называется совершенной, если величина $s_{ij}(x) = s_{ij}$ не зависит от выбора вершины x цвета i.*

Определение 3. *Матрицей параметров совершенной раскраски называется матрица*

$$S_{k \times k} = (s_{ij})$$

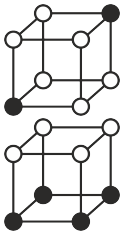
Пример 5. Совершенная раскраска графа Петерсена, порядок цветов: белый, зелёный, красный.



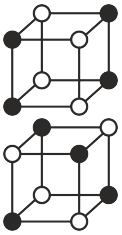
$$S = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & 1 \end{pmatrix}$$

Пример 6. Совершенные раскраски булева куба в 2 цвета. Первому цвету соответствует черный цвет, второму — белый.

[4] Обычное определение рёберной транзитивности не включает вершинной транзитивности. Наше определение совпадает не с "edge transitive а с "arc transitive".



$$S = \begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix}$$



$$S = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

$$S = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

$$S = \begin{pmatrix} 0 & 3 \\ 3 & 0 \end{pmatrix}$$

Как нередко бывает с полезными и несложно определяемыми математическими объектами, понятия, эквивалентные совершенной раскраске графа, независимо вводились в разных разделах дискретной математики. В частности, термин "equitable partition" используется в работах К.Годсила, Ж.Кулина и их учеников [37]. Здесь под словом "partition" имеется в виду разбиение вершин графа по цветам. Эквивалентный термин "partition design" введён в статье Ф.Дельсарта с соавторами и использовался специалистами в области комбинаторных дизайнов [18]. Имеется в виду групповой дизайн, где группами являются множества вершин одного цвета, а блоками единичные сферы. Термины "intriguing set" [53] в области исследования конечных геометрий и "extremal graphical designs" [43] в области экстремальных задач на графах используются для обозначения множества вершин одного цвета в двуцветной совершенной раскраске. Специалисты по булевым функциям используют термин "(c_0, c_1)-регулярная функция" для наименования совершенных раскрасок в два цвета булева гиперкуба [133]. В работах В.Г.Визинга использовался также эквивалентный термин "дистрибутивная раскраска" [113]. Термин "совершенная раскраска" ввел С.В. Августинович. Впервые в печати термин "совершенная раскраска" был использован в работе [129]. Эпитет "совершенная" возник в силу того, что множество вершин первого цвета в раскраске с параметрами $\begin{pmatrix} 0 & r \\ 1 & r-1 \end{pmatrix}$ оказывается совершенным кодом в графе (см. следующий раздел).

Комбинаторные конфигурации, которые допускают описание как совершенные раскраски в некотором графе, мультиграфе или гиперграфе, мы будем считать совершенными структурами.

Другой известной разновидностью раскрасок графов являются правильные раскраски.

Определение 4. *Раскраска называется правильной, если любая вершина не имеет соседей такого же цвета, как она сама.*

Очевидно, что совершенная раскраска, матрица параметров которой имеет нули на главной диагонали, является правильной. Правильные раскраски могут быть весьма хаотичными. В отличие от совершенных, правильные раскраски не обязаны обладать однородной локальной структурой.

1.3 Совершенные раскраски и передача сообщений

Совершенные раскраски нередко возникают как решение некоторой экстремальной задачи, т. е. как результат оптимизации раскраски по каким-то параметрам. Несколько таких задач, возникающих в теории кодирования и криптографии, будут рассмотрены далее. Здесь мы рассмотрим два простых примера, связанных с передачей сообщений по каналам связи, допускающим ошибки.

Рассмотрим следующую модель передачи сообщений по каналу связи. Каждому возможному сообщению поставим в соответствие вершину графа. Соединим рёбрами две вершины u и v, если при передаче по каналу связи какая-либо ошибка может превратить сообщение u в сообщение v. Канал связи называют симметричным, если вероятности ошибок, превращающих u в v и v в u, равны. Такому каналу связи соответствует неориентированный граф G.

Определение 5. *Подможество вершин графа называется кодом, исправляющим одну ошибку, если шары радиуса* 1 *с центрами в кодовых вершинах не пересекаются.*

Будем передавать только те сообщения, которые соответствуют вершинам кода. Тогда после любой ошибки на приёмном конце канала связи можно выяснить какое сообщение было передано. Чем больше мощность множества кодовых вершин, тем больше информации можно передать по каналу связи за единицу времени. Пусть все шары радиуса 1 в графе G имеют одинаковую мощность $r+1$, т. е. граф G — r-регулярный. Тогда для мощности кода C, исправляющего ошибку, справедливо неравенство $(r+1)|C| \leq |V(G)|$. Это неравенство носит название границы Хэмминга мощности кода. Нетрудно видеть, что код имеет максимальную мощность, когда граф полностью разбивается на шары радиуса 1 с центрами в кодовых вершинах. Это означает, что раскраска кодовых вершин в один цвет, а некодовых — в другой является совершенной с матрицей параметров $\begin{pmatrix} 0 & r \\ 1 & r-1 \end{pmatrix}$. Множество вершин первого цвета в такой раскраске называется совершенным[5] кодом.

Теперь предположим, что нам достаточно знать произошла ли ошибка при передаче сообщения. Например, можно полагать, что мы всегда можем запросить повторную передачу испорченного сообщения.

Определение 6. *Подможество вершин графа называется независимым, если оно не содержит смежных вершин.*

[5] Такой код называется также 1-совершенным, поскольку может быть исправлена 1 ошибка. Теория совершенных кодов и кодов, исправляющих ошибки, изложена в [33], [125], [66], [131], [90].

Если передавать по каналу связи только сообщения, соответствующие некоторому множеству независимых вершин, то ошибочное сообщение всегда распознаётся.

Нетрудно видеть, что в r-регулярном графе независимое множество не может содержать больше половины вершин графа. А если в графе найдётся независимое множество такой мощности, то вторая половина вершин также оказывается независимым множеством и раскраска двух долей графа в разные цвета является совершенной с матрицей параметров $\begin{pmatrix} 0 & r \\ r & 0 \end{pmatrix}$. В разделе 3.1 будет получена верхняя оценка мощности независимого множества для регулярных недвудольных графов и будет показано, что при достижении этой оценки независимое множество также оказывается совершенной раскраской.

В примере 6 первая раскраска булева гиперкуба соответствует совершенному коду, а последняя — разделению гиперкуба на независимые множества: двоичные наборы с чётным и нечётным числом единиц.

1.4 Совершенные и МДР-коды в гиперкубах

Подмножество Q_q^n называется кодом с кодовым расстоянием d, если расстояние Хэмминга между любыми двумя различными вершинми кода не меньше d. Пусть $q = p^k$ — степень простого числа p. Тогда на множестве Q_q можно задать структуру поля Галуа $GF(q)$ и множество Q_q^n можно рассматривать как n-мерное векторное пространство над $GF(q)$. Линейные подпространства в Q_q^n называют q-ичными линейными кодами.

Рассмотрим произвольную матрицу A размера $m \times n$ с элементами из Q_q и множество решений системы уравнений $Ax = \bar{0}$ над полем $GF(q)$.

Утверждение 1 ([46],[140]). *Если матрица A не содержит коллинеарных и нулевых столбцов, то множество $C = \{x \in Q_q^n \mid Ax = \bar{0}\}$ не содержит различных векторов на расстоянии Хэмминга менее 3.*

Доказательство. Пусть $Ax = Ay = 0$. Тогда $A(x-y) = 0$. Вектор $(x-y)$ задаёт линейную зависимость на столбцах матрицы A. Поскольку в матрице нет коллинеарных столбцов, то вектор $(x-y)$ имеет как минимум три ненулевые координаты. Следовательно $d(x,y) \geq 3$. □

Утверждение 2. *Если $n = \frac{q^t-1}{q-1}$ и q — степень простого числа, то в гиперкубе Q_q^n имеется 1-совершенный код C, т. е. существует совершенная раскраска χ_C с матрицей параметров $\begin{pmatrix} 0 & n(q-1) \\ 1 & n(q-1)-1 \end{pmatrix}$.*

Доказательство. Рассмотрим подмножество $\mathcal{A} \subset Q_q^t$, состоящее из всевозможных векторов, первая ненулевая координата которых равна 1. Очевидно, что множество $\{ax \mid a \in Q_q \setminus \{0\}, x \in \mathcal{A}\}$ состоит из всех

ненулевых векторов из Q_q^t, причём каждый вектор представлен в нём единственным способом. Тогда $|\mathcal{A}| = \frac{|Q_q^t|-1}{q-1} = n$. Очевидно, что никакие два вектора из $\mathcal{A}$ не коллинеарны. Из утверждения 1 следует, что матрица A, столбцами которой являются вектора из $\mathcal{A}$, определяет множество $C = \{x \in Q_q^n \mid Ax = \bar{0}\}$ с расстоянием между вершинами не менее 3. Матрица A содержит единичную подматрицу порядка t, поэтому имеет ранг не меньше t. Следовательно, код C является линейным подпространством размерности $n-t$. Тогда $|C| = q^{n-t}$. Каждая некодовая вершина $x \notin C$ видит не более одной кодовой, поскольку расстояния между кодовыми вершинами не меньше 3. Поскольку число вершин в единичном шаре равно $n(q-1)+1 = q^t$, число вершин гиперкуба, которые содержатся в C или смежны с вершинами из C, равно $q^t|C|$. Из равенства $|Q_q^n| = q^t|C|$ следует, что каждая некодовая вершина видит кодовую вершину. Таким образом, код C — 1-совершенный. □

Матрица A называется проверочной матрицей кода C. Линейный 1-совершенный код C называется кодом Хэмминга. Можно показать, что все линейные 1-совершенный коды в гиперкубе эквивалентны и получаются из кода, построенного в утверждении 2 линейным автоморфизмом гиперкуба.

Пример 7. Проверочная матрица двоичного кода Хэмминга длины $n = 7$: $A = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$.

Из утверждения 4 следует, что условие $n = \frac{q^t-1}{q-1}$ является необходимым для существования 1-совершенного кода в гиперкубе Q_q^n. Известна гипотеза о том, что при q не равном степени простого числа 1-совершенных кодов в Q_q^n, $n > 1$, не существует.

Зададим на множестве Q_q структуру группы с операцией $\circ$, например, структуру циклической абелевой группы $\mathbb{Z}_q$. Рассмотрим множество $L = \{x \in Q_q^n \mid x_1 \circ x_2 \circ \cdots \circ x_n = \varepsilon\}$, где ε — нейтральный элемент группы.

Утверждение 3. *Функция χ_L является совершенной раскраской с матрицей параметров* $\begin{pmatrix} 0 & n(q-1) \\ n & n(q-2) \end{pmatrix}$.

Доказательство. Пусть $x \in L$ и $d(x,y) = 1$ для некоторой вершины $y \in Q_q^n$. Предположим $y_i \neq x_i$. Тогда имеем $x_1 \circ \cdots \circ x_i = (x_{i+1} \circ \cdots \circ x_n)^{-1}$, а $y_1 \circ \cdots \circ y_i \neq (x_{i+1} \circ \cdots \circ x_n)^{-1}$. Поэтому $y \notin L$. Из определения группы следует, что равенство $x_1 \circ x_2 \circ \cdots \circ x_n = \varepsilon$ эквивалентно $(x_1 \circ x_2 \circ \cdots \circ x_{n-1})^{-1} = x_n$. Следовательно все координаты вершины $x \in L$ кроме одной можно выбрать произвольно. Поэтому $|L| = q^{n-1}$. Поскольку $|L|q = |Q_q^n|$, в

каждой клике (одномерной грани гиперкуба Q_q^n) имеется ровно одна вершина из L. Каждая вершина гиперкуба входит в n клик (одна по каждой координате), поэтому любая некодовая вершина видит ровно n кодовых. $\square$

Как будет показано ниже, первый цвет совершенной раскраски $\begin{pmatrix} 0 & (q-1)n \\ n & (q-2)n \end{pmatrix}$ является максимальным по мощности независимым множеством в гиперкубе Q_q^n. Точнее будет доказано, что минимальное собственное число матрицы смежности гиперкуба Q_q^n равно $-n$, поэтому мощность множества вершин первого цвета достигает границы Дельсарта—Хоффмана (утверждение 15). Такие подмножества гиперкуба называются МДР-кодами с кодовым расстоянием 2.

Задача 1. Докажите, что сумма собственных чисел матрицы смежности любого графа (с учётом кратности) равна нулю.

Задача 2. Докажите, что если матрица смежности двудольного графа имеет собственное число λ, то она имеет и собственное число $-\lambda$.

Задача 3. Докажите, что матрицы смежности связного регулярного графа G и его дополнения имеют одинаковые собственные вектора. Вычислите собственные числа матрицы смежности дополнения, если известны собственные числа матрицы смежности графа G.

Задача 4. Матрицей Зайделя графа $G = (V, E)$ определена равенством

$$Z_{n\times n}(G) = \begin{cases} 1, \text{ если} & (v_i, v_j) \in E(G); \\ -1, \text{ если} & (v_i, v_j) \notin E(G); \\ 0, \text{ если} & i = j. \end{cases}$$

Докажите, что матрица Зайделя регулярного связного графа имеет те же собственные вектора, что и матрица смежности графа. Вычислите собственные числа матрицы Зайделя, если известны собственные числа матрицы смежности графа.

Задача 5. Докажите, что совершенная раскраска графа является совершенной раскраской его дополнения.

Задача 6. Докажите, что раскраска регулярного графа G является совершенной, если подграфы, порождённые вершинами любых двух разных цветов являются бирегулярными двудольными и любого одного цвета, являются регулярными.

Задача 7. Докажите, что любое линейное множество (код) в Q_q^n (над полем $GF(q)$) можно задать проверочной матрицей A. Найдите необходимое и достаточное условие на столбцы матрицы A, которое обеспечивает кодовое расстояние d.

Задача 8. Подмножество булева гиперкуба S называется множеством Сидона, если все попарные суммы элементов из S различны. Докажите, что линейный двоичный код имеет кодовое расстояние не менее 5 тогда и только тогда, когда столбцы его проверочной матрицы вместе с нульвектором образуют множество Сидона.

2 Алгебраические свойства совершенных раскрасок

2.1 Стохастические матрицы

Простым необходимым условием того, чтобы целочисленная матрица являлась матрицей параметров некоторой совершенной раскраски, является симметричность носителя (множества позиций ненулевых элементов) матрицы. Действительно, если вершина первого цвета видит вершины второго цвета, то и вершина второго цвета видит вершины первого. Но это условие не является достаточным. В этом разделе будут установлены необходимые и достаточные условия.

Определение 7. *Квадратная матрица из неотрицательных элементов называется стохастической, если суммы её элементов по строкам равны* 1.

Из определений видно, что если S — матрица параметров совершенной раскраски r-регулярного графа, то матрица $\frac{1}{r}S$ является стохастической. Пусть n_i — количество вершин i-го цвета, $\sum_{i=1}^{k} n_i = n$ — число вершин в графе. Посчитав двумя способами количество ребер цвета ij, получаем следующее соотношение:

$$n_i s_{ij} = n_j s_{ji}. \tag{1}$$

Утверждение 4. *Если имеется совершенная раскраска графа на n вершинах с матрицей параметров S, то система уравнений (1) имеет целые неотрицательные решения n_i.*

Пусть N — диагональная матрица размера $k \times k$, состоящая из элементов n_i:

$$N = \begin{pmatrix} n_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & n_k \end{pmatrix}.$$

Из равенства (1) можно сделать вывод, что NS — симметричная матрица, поскольку мы можем переписать соотношение (1) в матричном виде:

$$S^T N = NS.$$

Матрицы S с таким свойством будем называть симметризуемыми диагональной матрицей. Нетрудно видеть, что матрицу N можно выбрать неотрицательной и целочисленной, если S неотрицательна и целочисленна.

Из этого вытекает следующее

Утверждение 5. *Матрица S параметров совершенной раскраски симметризуема диагональной матрицей и имеется базис, состоящий из собственных векторов матрицы S.*

Доказательство. Поскольку $n_i \geq 0$, можно рассмотреть диагональную матрицу $N^{\frac{1}{2}}$. Имеем равенство $N^{-\frac{1}{2}} S^T N^{\frac{1}{2}} = N^{\frac{1}{2}} S N^{-\frac{1}{2}}$. Таким образом, матрица $N^{\frac{1}{2}} S N^{-\frac{1}{2}}$ симметрична, а, следовательно, имеется базис пространства $\mathbb{R}^k$, состоящий из её собственных векторов. Матрица S подобна матрице $N^{\frac{1}{2}} S N^{-\frac{1}{2}}$, и значит тоже найдётся базис из её собственных векторов. □

Оказывается, свойство симметризуемости стохастической матрицы не только необходимо, но и достаточно для того, чтобы рациональная стохастическая матрица после домножения на общий знаменатель элементов была матрицей параметров совершенной раскраски некоторого графа. А именно, справедлива[6]

Теорема 1 ([121],[?]). *Пусть элементы целочисленной неотрицательной симметризуемой матрицы S удовлетворяют равенствам $\sum_{j=1}^{k} s_{ij} = r$. Тогда найдутся r-регулярный граф G и его совершенная раскраска с матрицей параметров S.*

Доказательство. Вначале покажем, что при выполнении равенства $n_i s_{ij} = n_j s_{ji}$ найдётся двудольный бирегулярный граф с мощностями долей n_i и n_j, а степенями вершин в долях s_{ij} и s_{ji}. Для этого достаточно построить матрицу смежности долей B (размера $n_i \times n_j$) такого бирегулярного графа. Пусть k-ая строка матрицы B содержит блок из единиц на позициях с $(k-1)s_{ij}+1$ по ks_{ij}, где оба номера позиций рассматриваются по модулю n_j. Остальные элементы матрицы B заполним нулями. В каждой строке матрицы B ровно s_{ij} единиц по построению. Кроме того, по построению количество единиц в столбцах матрицы B отличается не более чем на один. А при выполнении равенства (1) их оказывается поровну, т. е. по $s_{ji} = n_i s_{ij} / n_j$.

По условию найдётся такая диагональная неотрицательная матрица N, что матрица NS симметрична. Элементы матрицы N, будем считать чётными, поскольку умножение на 2 сохраняет равенство (1). Для каждого $i = 1, \ldots, k$ возьмём множество V_i из n_i вершин, где n_i — iй диагональный элемент матрицы N. Для каждой пары i, j, $i \neq j$, проведём рёбра так, чтобы получился двудольный бирегулярный граф с

[6] Эту теорему можно обобщить на нерегулярные графы [94].

долями V_i и V_j, а степенями вершин в долях s_{ij} и s_{ji}. Это возможно, поскольку $|V_i|s_{ij} = |V_j|s_{ji}$. Для каждого $i = 1, \ldots, k$ вершины iй доли разделим на две равные доли V_i' и V_i'' и построим двудольный s_{ii}-регулярный граф. Это возможно, поскольку выполняется требуемое равенство $|V_i'|s_{ii} = |V_i''|s_{ii}$. Искомый граф построен, осталось раскрасить вершины из V_i в iй цвет для всех $i = 1, \ldots, k$. □

Таким образом, установлены необходимые и достаточные условия для того, чтобы матрица являлась матрицей параметров совершенной раскраски некоторого графа. Но можно ли заданный граф раскрасить в соответствии с заданной матрицей параметров? Этот вопрос во многих конкретных случаях остаётся нерешённым.

Замечание 1. Любую стохастическую матрицу $T = (t_{ij})$ можно рассматривать как матрицу переходных вероятностей марковской цепи, где t_{ij} — условные вероятности переходов из состояния i в состояние j. Таким образом, случайные блуждания по раскрашеному совершенно графу G порождают марковскую цепь, состояния которой — цвета вершин, а выбор ребра, по которому нужно двигаться дальше, равновероятен. Отметим, что набор частот цветов раскраски $q = \left(\frac{n_1}{n}, \ldots, \frac{n_k}{n}\right)$ является вектором стационарных вероятностей состояний марковской цепи, поскольку удовлетворяет уравнению $q^{\mathrm{T}}T = q$.

Однако, не каждая дискретная марковская цепь может быть интерпретирована как блуждание по неориентированному раскрашенному графу, а только та, у которой вероятности траекторий (наборов состояний в порядке прохождения) не зависят от порядка прохождения состояний цепи: справа налево или слева направо. Это свойство эквивалентно симметризуемости матрицы T.

2.2 Матричное уравнение совершенной раскраски

Пусть $f : V(G) \to \{1, \ldots, k\}$ — раскраска графа. Рассмотрим матрицу $F = F[f]$ размера $n \times k$, у которой столбец f_i является характеристической функцией цвета i:

$$f_i(x) = \begin{cases} 1 & \text{при } f(x) = i, \\ 0 & \text{при } f(x) \neq i. \end{cases} \tag{2}$$

Матрицы $F[f]$ мы будем также называть раскрасками графа, поскольку они взаимно однозначно соответствуют функциям $f : V(G) \to \{1, \ldots, k\}$. Отметим, что в каждой строке матрицы F стоит ровно одна единица. Кроме того, мы везде будем полагать, что функция, заданная на вершинах графа, является вектором-столбцом.

Утверждение 6 ([70],[45],[38]). *Пусть M — матрица смежности графа G. $F = F[f]$ является совершенной раскраской[7] графа G с матрицей параметров S тогда и только тогда, когда $MF = FS$.*

Доказательство. Для доказательства равенства рассмотрим (vj)-ые элементы матриц в левой и правой части равенства $MF = FS$, $j = 1, \ldots, k$, $v \in V(G)$. $(MF)_{vj}$ — число соседей цвета j, которых видит вершина v. Теперь рассмотрим правую сторону равенства. В строке F^v единица стоит в позиции, соответствующей цвету $f(v)$ вершины v. Отсюда получаем, что $(FS)_{vj}$ — количество вершин цвета j, соседних с вершиной цвета $f(v)$. Таким образом, правая часть зависит только от цвета вершины v. □

Отметим, что если матрица S является решением уравнения $MF = FS$, где M — неотрицательная целочисленная матрица, а F удовлетворяет условию (2), то матрица S также является неотрицательной и целочисленной.

Следствие 1 (теорема Ллойда). *Пусть z — собственный вектор матрицы параметров S совершенной раскраски F графа с матрицей смежности M, т. е. $Sz = \lambda z$ и $z \neq \mathbf{0}$. Тогда Fz является собственным вектором матрицы смежности M с тем же собственным числом λ.*

Доказательство. Используя утверждение 6 и ассоциативность умножения матриц, имеем следующую цепочку равенств:

$$MFz = FSz = F\lambda z = \lambda Fz.$$

В силу определения матрицы F вектор $Fz \neq \mathbf{0}$, если $z \neq \mathbf{0}$. □

Поскольку M — симметричная матрица, все её собственные числа вещественные.

Следствие 2. *Спектр матрицы параметров совершенной раскраски состоит из вещественных чисел.*

Поскольку M — симметричная матрица, имеется базис, состоящий из её собственных векторов. То есть $\mathbb{R}^n = X_{\lambda_1} \oplus \ldots \oplus X_{\lambda_m}$, где X_{λ_i} — собственное подпространство матрицы M, соответствующее λ_i.

Следствие 3. *Любой цвет совершенной раскраски F (т. е. вектор f_i, $i = 1, \ldots, k$) содержится в подпространстве $X_{\lambda_1} \oplus \ldots \oplus X_{\lambda_{m'}}$, где λ_1, $\ldots$, $\lambda_{m'}$ — собственные числа матрицы S.*

[7] Исследование произвольных матриц F, удовлетворяющих уравнению $MF = FS$, имеется в [94].

Доказательство. По утверждению 5 матрица S имеет базис из собственных векторов. Следовательно, вектор $e_i = (0 \dots \underset{i}{1} \dots 0)$ можно разложить по этому базису: $e_i = \sum \alpha_j z_j$, где z_j — собственные векторы матрицы S. Получаем:

$$f_i = Fe_i = F \sum \alpha_j z_j = \sum \alpha_j F z_j$$

По следствию 1 Fz_j является собственным вектором матрицы M, таким образом, мы получили требуемое разложение. □

Подпространство V называется *инвариантным* относительно матрицы M, если $MV \subseteq V$. В частности, собственные подпространства матрицы инвариантны. Рассмотрим подпространство V_F, порождённое столбцами матрицы раскраски F. Из определения совершенной раскраски следует

Утверждение 7. *F — совершенная раскраска тогда и только тогда, когда V_F — инвариантное подпространство.*

Доказательство. F — совершенная раскраска, если и только если совпадают строки матрицы MF, соответствующие вершинам одного цвета. А это значит только, что все столбцы матрицы MF являются линейными комбинациями столбцов матрицы F. □

Пусть F — некоторая раскраска в k цветов графа с матрицей смежности M. Тогда $N = F^{\mathrm{T}}F$ — диагональная матрица размера $k \times k$, (ii)-й элемент которой равен n_i — числу вершин цвета i.

Утверждение 8. *Линейный оператор, заданный матрицей $P = FN^{-1}F^{\mathrm{T}}$, является проектором[8] на подпространство V_F, порождённое характеристическими векторами цветов раскраски F.*

Доказательство. Пусть f_i — i-ый столбец матрицы F, т. е. характеристический вектор i-го цвета. Нетрудно видеть, что $Pf_i = f_i$ для любого i, $i = 1, \dots, k$. Поскольку ранг матрицы F равен k, то ранг матрицы P не больше чем k. Следовательно, размерность образа оператора P равна k и вектора f_i составляют базис образа. Оператор является проектором, если $P^2 = P$. Имеем $P^2 = FN^{-1}F^{\mathrm{T}}FN^{-1}F^{\mathrm{T}} = FN^{-1}NN^{-1}F^{\mathrm{T}} = P$. □

Утверждение 9. *Раскраска F является совершенной для графа G с матрицей смежности M тогда и только тогда, когда справедливо равенство $MP = PM$, где P — соответствующий раскраске проектор.*

Доказательство. 1. Умножим равенство $MFN^{-1}F^{\mathrm{T}} = FN^{-1}F^{\mathrm{T}}M$ на матрицу F справа. Имеем $MF = FN^{-1}F^{\mathrm{T}}MF$. Тогда из утверждения

[8] Проектором на линейное подпространство называется линейный оператор, действующий в это подпространство и тождественный на нём.

6 следует, что F — совершенная раскраска G с матрицей параметров $S = N^{-1}F^{\mathrm{T}}MF$.

2. Пусть раскраска F является совершенной с матрицей параметров S. Тогда по утверждению 6 имеем равенство $MF = FS$. По определению P имеем $PF = F$. Тогда $MF = PFS = PMF$. Домножая слева равенство $MF = PMF$ на $N^{-1}F^T$, получаем $MP = PMP$. Поскольку матрицы P и M симметричные, имеем $PM = (MP)^T = (PMP)^T = PMP$. $\square$

2.3 Теорема о спектральном разложении матрицы смежности

Пусть X_{λ_i} — собственное подпространство симметричной матрицы M, соответствующее собственному числу λ_i. Рассмотрим некоторый ортонормированый базис $\{u_1^i, \ldots, u_{m_i}^i\}$ пространства X_{λ_i} и матрицу U_i размера $n \times m_i$, столбцами которой являются вектора u_j^i, $j = 1, \ldots, m_i$. Определим матрицу E_{λ_i} размера $n \times n$ равенством $E_{\lambda_i} = U_i U_i^T$.

Теорема 2 (о спектральном разложении [38]). *Для любой симметричной матрицы M матрицы E_{λ_i} удовлетворяют условиям*
1) $E_{\lambda_i}^2 = E_{\lambda_i}$; $E_{\lambda_i}E_{\lambda_j} = 0$ при $i \neq j$;
2) $\sum_i E_{\lambda_i} = I_n$; матрица E_{λ_i} не зависит от выбора ортонормированного базиса пространства X_{λ_i};
3)$ME_{\lambda_i} = \lambda_i E_{\lambda_i}$; для любого полинома p верно: $p(M) = \sum_i p(\lambda_i)E_{\lambda_i}$.

Доказательство. 1) По определению $E_{\lambda_i} = U_i U_i^T$. Из ортонормированности базиса имеем[9] $U_i^T U_i = I_{m_i}$. Тогда $E_{\lambda_i}^2 = U_i(U_i^T U_i)U_i^T = E_{\lambda_i}$. Собственные подпространства симметричной матрицы, соответствующие разным собственным числам, ортогональны, поэтому $U_i^T U_j = 0$ при $i \neq j$. Тогда $E_{\lambda_i}E_{\lambda_j} = U_i(U_i^T U_j)U_j^T = 0$.

2) Квадраты собственных чисел матрицы M являются собственными числами матрицы M^2. Из равенства $E_{\lambda_i}^2 = E_{\lambda_i}$ следует, что собственные числа матрицы E_{λ_i} равны 0 или 1. Ранг матрицы E_{λ_i} равен размерности подпространства X_{λ_i}, поскольку ранг матрицы $I_{m_i} = U_i^T(U_i U_i^T)U_i$ равен m_i и не превосходит ранга матрицы $E_{\lambda_i} = U_i U_i^T$. Тогда собственное число 1 имеет кратность m_i и $\mathrm{tr}(E_{\lambda_i}) = m_i$. Пусть $E = \sum_i E_{\lambda_i}$. Имеем $\mathrm{tr}(E) = \sum_i \mathrm{tr}(E_{\lambda_i}) = \sum_i m_i = n$. Кроме того, из п. 1) следует, что $E^2 = E$ и матрица E — симметричная, благодаря симметричности слагаемых. Значит кратность собственного числа 1 равна размерности матрицы. Следовательно, $E = I_n$. Если изменить ортонормированный базис в одном из собственных подпространств X_{λ_i}, то в равенстве $\sum_i E_{\lambda_i} = I_n$ может поменяться только одно слагаемое. Однако, в равенстве это невозможно.

[9] Здесь и далее I_n — единичная матрица размера $n \times n$.

3) $ME_{\lambda_i} = (MU_i)U_i^T = \lambda_i U_i U_i^T = \lambda_i E_{\lambda_i}$. Тогда $M^k E_{\lambda_i} = \lambda_i^k E_{\lambda_i}$ для любого натурального k. Из п. 2) имеем $M^k I_n = \sum_i \lambda_i^k E_{\lambda_i}$. Тогда для любого полинома p имеем равенство $p(M) = \sum_i p(\lambda_i) E_{\lambda_i}$. □

Следствие 4. *Матрицы E_λ можно представить в виде многочленов от матрицы M.*

Доказательство. Из теоремы о спектральном разложении имеем равенство $p(M) = \sum_i p(\lambda_i) E_{\lambda_i}$, где p — произвольный полином. Рассмотрим полином $q(t) = (\prod_i (t - \lambda_i))/(t - \lambda)$. Имеем $q(M) = q(\lambda) E_\lambda$. □

Следствие 5. *Размерность линейного пространства матриц, порождённых степенями симметричной матрицы M, равна числу различных собственных чисел матрицы M.*

Доказательство. Матрицы E_{λ_i} линейно независимы по п. 1) и составляют базис этого пространства по п. 3) теоремы о спектральном разложении. □

Обозначим через J_n матрицу размера $n \times n$, все элементы которой равны 1. Для максимального собственного числа r-регулярного связного графа собственное подпространство X_r состоит из векторов, коллинеарных вектору $\mathbf{1}$ (см. задачу 12). Поэтому $E_r = \frac{1}{n} J_n$. Тогда J_n можно представить в виде многочленов от матрицы смежности M по следствию 4. Покажем, что это свойство регулярного графа является критерием.

Теорема 3 (Хоффман [38])**.** *Граф G является регулярным и связным тогда и только тогда, когда найдётся полином p, для которого $J_n = p(M)$, где M — матрица смежности графа G.*

Доказательство. ($\Leftarrow$) Если $J_n = p(M)$ для некоторого полинома p, то $Mp(M) = p(M)M$ и $MJ_n = J_n M$, что означает регулярность графа G. Если граф G — несвязен, то найдутся вершины с номерами i и j такие, что элемент (i, j) в матрице M^d равен нулю для любой степени d.

($\Rightarrow$) Пусть G — r-регулярный связный граф и $p(x) = (x - r)(x - \lambda_1) \cdots (x - \lambda_l) = (x - r)q(x)$, где $r, \lambda_1, \ldots, \lambda_l$ — все различные собственные числа матрицы M. Так как $p(M) = 0$, то $Mq(M) = rq(M)$. Следовательно, столбцы матрицы $q(M)$ — это собственные вектора для максимального собственного числа r. Поскольку граф G связен, все они коллинеарны вектору $\mathbf{1}$. Так как матрица $q(M)$ является симметричной, то все эти столбцы равны. Следовательно $q(M) = cJ_n$ для некоторого c. □

2.4 Совершенные раскраски и собственные функции

Рассмотрим совершенную раскраску связного r-регулярного графа в два цвета. Пусть $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} r-b & b \\ c & r-c \end{pmatrix}$ — матрица параметров этой раскраски. Основными параметрами раскраски считаются числа b, c, т. е. число вершин другого цвета, которые видит исходная вершина. Собственные числа этой матрицы равны $\lambda_1 = r$, $\lambda_2 = r - (b + c)$.

Замечание 2. Собственное число матрицы смежности регулярного графа, соответствующее совершенной раскраске графа в 2 цвета является целым.

Вычислим количество вершин каждого цвета (n_1 и n_2 соответственно) из системы уравнений:
$n_1 b = n_2 c$ — количество двухцветных ребер;
$n_1 + n_2 = n = |V(G)|$.
Откуда получаем равенства $n_1 = \frac{nc}{b+c} = \frac{n}{1+\frac{b}{c}}$ и $n_2 = \frac{nb}{b+c} = \frac{n}{1+\frac{c}{b}}$.

В данном случае необходимое условие существования совершенной раскраски графа (утверждение 4) означает делимость чисел nc и nb на $b + c$.

Пусть A — множество вершин первого цвета и $\mathbf{1}$ — вектор из единиц, который является собственным вектором матрицы S с собственным числом r. Из следствия 3 получаем, что $\chi_A = f + \alpha\mathbf{1}$, где f — собственная функция, соответствующая числу λ_2. Имеем $n_1 = (\chi_A, \mathbf{1}) = \alpha(\mathbf{1}, \mathbf{1}) = \alpha n$, откуда получаем:

$$f(x) = \begin{cases} 1 - \frac{c}{b+c} & x \in A; \\ -\frac{c}{b+c} & x \notin A. \end{cases}$$

Следовательно, совершенной раскраске в 2 цвета можно поставить в соответствие собственную функцию, принимающую разные значения только в точках разного цвета. Ниже мы покажем, что верно и обратное. Для раскрасок в большее число цветов такое соответствие возникает при некоторых дополнительных условиях.

Замечание 3. Рассмотрим совершенную раскраску регулярного графа G в k цветов с матрицей параметров S. Пусть $v = (v_1, \ldots, v_k)$ — собственный вектор матрицы S с собственным числом λ, причём все компоненты вектора v различны. Тогда по следствию 1 функция Fv является собственной функцией графа G, которая принимает значения v_i в точках цвета i. А значит по ней можно восстановить совершенную раскраску.

Утверждение 10. *Пусть f — некоторая раскраска регулярного графа G в k цветов и имеется k линейно независимых собственных функций матрицы смежности графа, которые можно получить как линейные комбинации характеристических функций цветов раскраски. Тогда f является совершенной раскраской.*

Доказательство. Пусть собственные функции $(h_1, \ldots, h_k)$ являются линейными комбинациями характеристических функций цветов $(f_1, \ldots, f_k)$ раскраски f, т. е. $(h_1, \ldots, h_k) = (f_1, \ldots, f_k)A$ или $H = FA$, где функции являются столбцами матриц H и F. Матрица A невырождена, поскольку собственные функции $h_1, \ldots, h_k$ линейно независимы по условию. Поскольку $h_1, \ldots, h_k$ — собственные вектора матрицы M смежности графа G, имеем равенство $MH = H\Lambda$, где Λ — диагональная матрица и λ_{ii} — собственное число, соответствующее вектору h_i. Получаем равенство $MFA = FA\Lambda$. Тогда по утверждению 6 раскраска f является совершенной с матрицей параметров $A\Lambda A^{-1}$. □

Следствие 6 ([34]). *Пусть функция f принимает только два значения на вершинах r-регулярного графа G и $f = g + c\mathbf{1}$, где g — собственная функция матрицы смежности графа G с собственным числом отличным от r. Тогда f является совершенной раскраской в два цвета.*

Доказательство. Пусть v_0 — некоторая вершина. Определим характеристические функции цветов $f_1(v) = 1$, если $f(v) = f(v_0)$ и $f_1(v) = 0$, если $f(v) \neq f(v_0)$; $f_2 = \mathbf{1} - f_1$. Тогда $f_1 + f_2 = \mathbf{1}$ — собственная функция с собственным числом r и $g = f - c\mathbf{1}$ является линейной комбинацией f_1 и f_2. Тогда f — совершенная раскраска. □

Пусть $f : V(G) \to \{1, 2\}$ — некоторая раскраска графа G. Обозначим через $a(x)$ — количество вершин первого цвета, которое видит произвольная вершина x первого цвета, а через $c(y)$ — количество вершин первого цвета, которое видит произвольная вершина y второго цвета.

Утверждение 11. *Пусть для некоторой раскраски f графа G и любой пары вершин x и y верно, что $a(x) \leq a$, $c(y) \leq c$. Причём доля вершин первого цвета в r-регулярном графе G не меньше чем $\frac{c}{r-a+c}$. Тогда f — совершенная раскраска графа G с матрицей параметров $S = \begin{pmatrix} a & r-a \\ c & r-c \end{pmatrix}$.*

Доказательство. Пусть $n = |V(G)|$, $n_i = |f^{-1}(i)|$ и f_i — характеристическая функция i-го цвета. Из условия на величины $a(x)$ и $c(y)$ имеем неравенства

$$(Mf_1, f_1) \leq an_1, \quad (Mf_1, \mathbf{1} - f_1) = (f_1, Mf_2) \leq cn_2 = c(n - n_1) \qquad (3)$$

и $(Mf_1, \mathbf{1}) = rn_1$. Пусть хотя бы для одной вершины первого цвета верно $a(x) < a$ или для одной вершины второго цвета верно $c(y) < c$. Тогда одно из неравенств (3) становится строгим. Имеем $(Mf_1, \mathbf{1}) = (Mf_1, \mathbf{1} - f_1) + (Mf_1, f_1)$. Когда хотя бы одно из неравенств (3) строгое, имеем $rn_1 < c(n-n_1)+an_1$, т. е. $\frac{n_1}{n} < \frac{c}{r+c-a}$. Однако из условия имеем обратное неравенство. Следовательно, $a(x) = a$ для любых вершин первого цвета и $c(y) = c$ для любых вершин второго цвета. □

Следствие 7. *Пусть G — r-регулярный граф и A — подмножество его вершин. Пусть в любом шаре радиуса 1 содержится не более одной вершины из A. Если $\frac{|A|}{|V(G)|} \geq \frac{1}{r+1}$, то A — совершенный код.*

Доказательство. Будем считать, что вершины из A покрашены в первый цвет, а остальные — во второй. Тогда по условию $a = 0$ и $c = 1$. Раскраска является совершенной с матрицей параметров $\begin{pmatrix} 0 & r \\ 1 & r-1 \end{pmatrix}$. □

2.5 Ортогональность совершенных раскрасок

Утверждение 12. *Пусть G — связный r-регулярный граф, g и h — совершенные раскраски графа G, причём множества собственных чисел матриц параметров раскрасок g и h пересекаются только по максимальному собственному числу r. Тогда для любого цвета i раскраски g и любого цвета j раскраски h, доля вершин цвета j среди вершин цвета i будет та же, что и вершин цвета j во всем графе.*

Доказательство. Обозначим через B множество вершин цвета i и через A множество вершин цвета j. Определим функцию $f = \chi_B - \frac{|B|}{|V(G)|}\mathbf{1}$. По построению $(f, \mathbf{1}) = 0$. По следствию 3 функция f содержится в объединении подпространств с собственными числами раскраски g без собственного числа r. Тогда $(f, \chi_A) = 0$, поскольку по условию функция χ_A лежит в подпространстве, которое перпендикулярно функции f (см. следствие 3). Следовательно, $(f, \chi_A) = |B \cap A| - \frac{|B||A|}{|V(G)|} = 0$. Тогда $\frac{|B \cap A|}{|B|} = \frac{|A|}{|V(G)|}$. □

В теории вероятностей два разбиения $\{A_i\}$ и $\{B_j\}$ пространства событий называют независимыми, если попарно независимы события A_i и B_j для любых i и j, т. е. выполнены равенства $Pr(A_iB_j) = Pr(A_i)Pr(B_j)$. Таким образом, совершенные раскраски, спектры которых пересекаются только по максимальному собственному числу, можно рассматривать как независимые разбиения вершин графа (здесь $Pr(A) = |A|/|V(G)|$).

Доказательство следующего утверждения аналогично доказательству утверждения 12.

Утверждение 13. *Пусть два набора собственных подпространств связного регулярного графа G, содержащие характеристические функции множеств его вершин A и B соответственно, пересекаются только по подпространству, состоящему из постоянных функций. Тогда $\frac{|A|}{|V(G)|} = \frac{|A \cap B|}{|B|}$.*

Для гиперкубов утверждение 13 является частным случаем утверждения 82, которое будет сформулировано и доказано в разделе 11.

Утверждение 14. *Пусть $f, g : V(G) \to \{0,1\}$ — совершенные раскраски связного регулярного графа G в два цвета. Пусть множества вершин первого цвета $f^{-1}(1)$ в раскраске f и множество вершин первого цвета $g^{-1}(1)$ в раскраске g не пересекаются ($f^{-1}(1) \cap g^{-1}(1) = \varnothing$). Тогда раскраска $f + g$ является совершенной.*

Доказательство. Из утверждения 12 следует, что собственные числа матриц параметров раскрасок f и g совпадают. Поэтому раскраскам f и g соответствуют собственные функции $f_1 = f - \frac{|f^{-1}(1)|}{|V(G)|}\mathbf{1}$ и $g_1 = g - \frac{|g^{-1}(1)|}{|V(G)|}\mathbf{1}$ с одинаковым собственным числом. Обозначим $c = \frac{|f^{-1}(1)|+|g^{-1}(1)|}{|V(G)|}$. Сумма $h = f_1 + g_1$ также является собственной функцией и принимает два значения $1 - c$ и $-c$. Значит по следствию 6 функция h является совершенной раскраской. Функция $f + g = h + c\mathbf{1}$ отличается от h на константу, следовательно, является совершенной раскраской со значениями 0 и 1. □

Задача 9. Докажите, что раскраска F графа с матрицей смежности M является совершенной тогда и только тогда, когда справедливо равенство $MF = PMF$. Другими словами столбцы матрицы MF являются собственными векторами проектора P (см. утверждение 8).

Задача 10. Докажите, что для любого инвариантного подпространства симметричной матрицы A найдутся матрицы F и S такие, что образ $F(\mathbb{R}^k)$ является этим инвариантным подпространством и выполнено равенство $AF = FS$.

Задача 11. Докажите, что многочлен $\det(S - xI)$ делит многочлен $\det(M - xI)$.

Задача 12. Докажите, что максимальные собственные числа матриц M и S совпадают и равны r — степени регулярного графа, а собственное подпространство X_r связного графа одномерно.

Задача 13. Определим носитель матрицы A как матрицу $\mathrm{supp}(A)$ равенством $(\mathrm{supp}(A))_{ij} = \begin{cases} 1 & \text{при } (A)_{ij} \neq 0, \\ 0 & \text{при } (A)_{ij} = 0. \end{cases}$ Докажите, что для любая симметричная $(0,1)$-матрица является носителем некоторой симметризуемой стохастической матрицы.

Задача 14. Пусть d — диаметр графа. Докажите, что его матрица смежности имеет не менее $d + 1$ различных собственных чисел.

Задача 15. Докажите, что для любого конечного набора чисел существует лишь конечное число (возможно 0) связных регулярных графов с таким набором собственных чисел.

Задача 16. Докажите, что половина вершин любого 1-совершенного кода в булевом гиперкубе имеет чётный вес (число единиц), а другая половина — нечётный.

Задача 17. Пусть $v = (v_1, \ldots, v_k)$ — собственный вектор матрицы параметров S совершенной раскраски F связного регулярного графа G в k цветов, причём все компоненты вектора v различны. Докажите, что линейная оболочка столбцов матрицы F совпадает с линейной оболочкой набора векторов $f^0, f^1, \ldots, f^{k-1}$, где $f = Fv$.

3 Экстремальные свойства совершенных раскрасок

3.1 Разрезы и независимые множества в графах

Пусть A и B подмножества вершин в простом графе G. Определим величину $e(A,B) = |\{\{a,b\} \in E(G) : a \in A, b \in B\}|$ — число рёбер, соединяющих вершины из множества A с вершинами из множества B, причём если $a, b \in A \cap B$, то ребро $\{a,b\}$ считается дважды. Заметим, что $e(A,B) = (\chi_A, M\chi_B)$, где M — матрица смежности графа G.

Лемма 1 (expander mixing lemma [1], [30]). *Пусть G — r-регулярный связный граф и λ — максимальное по модулю, за исключением r, собственное число его матрицы смежности M, т. е. $|\lambda| > |\lambda'|$ для всех собственных чисел λ', $\lambda' \neq \lambda$, $\lambda' \neq r$. Тогда для любых подмножеств вершин A и B справедливо неравенство*

$$|e(A,B) - \frac{r|A||B|}{|V(G)|}| \leq |\lambda|\sqrt{|A||B|(1-|A|/|V(G)|)(1-|B|/|V(G)|)}.$$

Причём, если в неравенстве достигается равенство, то χ_A — совершенная раскраска с собственным числом λ и $B = A$ или $B = V(G) \setminus A$.

Доказательство. Характеристические функции χ_A и χ_B представимы в виде $\chi_A = \sum_i \alpha_i \phi_i$ и $\chi_B = \sum_i \beta_i \phi'_i$, где ϕ_i и ϕ'_i — нормированные собственные функции матрицы M, соответствующие собственному числу λ_i. Нормированной собственной функцией, соответствующей собственному числу r, является константа $\phi_0 = \phi'_0 = \mathbf{1}/\sqrt{n}$, $n = |V(G)|$. Имеем $\alpha_0 = (\chi_A, \phi_0) = |A|/\sqrt{n}$, $\beta_0 = (\chi_B, \phi_0) = |B|/\sqrt{n}$. Тогда

$$(\chi_A - \alpha_0\phi_0, M(\chi_B - \beta_0\phi_0)) = \sum_{i \neq 0} \lambda_i \alpha_i \beta_i (\phi_i, \phi'_i). \tag{4}$$

Из неравенства Коши—Буняковского имеем

$$|\sum_{i\neq 0} \lambda_i \alpha_i \beta_i (\phi_i, \phi'_i)| \leq |\lambda| \sum_{i \neq 0} |\alpha_i \beta_i| \leq |\lambda| (\sum_{i \neq 0} \alpha_i^2)^{1/2} (\sum_{i \neq 0} \beta_i^2)^{1/2}. \tag{5}$$

С другой стороны

$$(\chi_A - \alpha_0\phi_0, M(\chi_B - \beta_0\phi_0)) = (\chi_A, M\chi_B) - \beta_0(\chi_A, M\phi_0) - (\alpha_0\phi_0, M(\chi_B - \beta_0\phi_0))$$

$$= e(A,B) - \frac{r|A||B|}{n}, \tag{6}$$

поскольку $(\phi_0, M(\chi_B - \beta_0\phi_0)) = (M\phi_0, \chi_B - \beta_0\phi_0) = (r\phi_0, \chi_B - \beta_0\phi_0) = 0$.

Из равенства $(\chi_A, \chi_A) = \sum_i \alpha_i^2$ следует, что $\sum\limits_{i\neq 0} \alpha_i^2 = (\chi_A, \chi_A) - \alpha_0^2 = |A| - |A|^2/n$. Аналогичное неравенство верно для множества B. Тогда из формул (4–6) имеем

$$\left| e(A,B) - \frac{r|A||B|}{n} \right| = |(\chi_A - \alpha_0\phi_0, M(\chi_B - \beta_0\phi_0))| \leq$$

$$\leq |\lambda| \sqrt{(|A| - |A|^2/n)(|B| - |B|^2/n)}.$$

Для достижения равенства в неравенстве Коши—Буняковского необходимо, чтобы вектор $\chi_A - \alpha_0\phi_0$ был коллинеарен вектору $\chi_B - \beta_0\phi_0$, т. е. $\alpha_i = \beta_i$ или $\alpha_i = -\beta_i$ для всех $i \neq 0$. Тогда для достижения равенства в первом неравенстве формулы (5) необходимо, чтобы функция $\chi_B - \beta_0\phi_0$ была собственной, с собственным числом λ. Из следствия 6 получаем, что χ_B — совершенная раскраска в два цвета. Если вектор $\chi_A - \alpha_0\phi_0$ сонаправлен вектору $\chi_B - \beta_0\phi_0$, то получаем $B = A$, если противоположно направлен — $B = V(G) \setminus A$. □

Рассмотрим подробнее случаи, когда $B = V(G) \setminus A$ и $B = A$.

Определение 8. *Разрезом графа G называется пара множеств вершин $A \subset V(G)$ и $B = V(G) \setminus A$ или множество рёбер между ними, величиной разреза называется число $e(A,B)$.*

В теории графов рассматриваются задачи поиска как минимального, так и максимального разрезов графа.

Следствие 8 ([43]). *Пусть G — r-регулярный связный граф и $\lambda_k < \lambda_{k-1} < \cdots < \lambda_1 < \lambda_0 = r$ — собственные числа его матрицы смежности M. Пусть $A \subset V(G)$, $B = V(G) \setminus A$. Тогда справедливы неравенства*[10]

$$\frac{(r-\lambda_1)|A||B|}{|V(G)|} \leq e(A,B) \leq \frac{(r-\lambda_k)|A||B|}{|V(G)|}.$$

Причём, если для некоторого множества A в одном из неравенств достигается равенство, то его характеристическая функция есть совершенная раскраска.

[10] Неравенство было доказано ранее в работах [2], [92].

Доказательство. Действуем аналогично доказательству леммы 1. В этом случае имеем $\chi_B = \sqrt{n}\phi_0 - \chi_A$, поэтому равенство (4) принимает вид

$$(\chi_A - \alpha_0\phi_0, M(\chi_B - \beta_0\phi_0)) = -\sum_{i\neq 0}\lambda_i\alpha_i^2$$

и

$$-\lambda_1\sum_{i\neq 0}\alpha_i^2 \leq -\sum_{i\neq 0}\lambda_i\alpha_i^2 \leq -\lambda_k\sum_{i\neq 0}\alpha_i^2.$$

Используя равенство (6), получаем требуемое неравенство. Очевидно в неравенстве достигается равенство только в случае, когда функция $\chi_A - \alpha_0\phi_0$ является собственной функцией матрицы M с собственным числом λ_1 или λ_k. □

Из следствия 8 вытекает

Следствие 9. *Мощность максимального разреза графа G не больше $(r-\lambda_k)|V(G)|/4$ и в случае равенства разрез соответствует совершенной раскраске в два цвета с минимальным собственным числом.*

Следствие 10 (Хемерс [44])**.** *Пусть G — r-регулярный связный граф и $\lambda_k < \lambda_{k-1} < \cdots < \lambda_1 < \lambda_0 = r$ — собственные числа его матрицы смежности M. Пусть $C \subset V(G)$, $C \neq V(G)$ и $e(C,C)$ — удвоенное число пар смежных вершин в множестве C. Тогда справедливы неравенства*

$$\lambda_k|C| + \frac{(r-\lambda_k)|C|^2}{|V(G)|} \leq e(C,C) \leq \lambda_1|C| + \frac{(r-\lambda_1)|C|^2}{|V(G)|}.$$

Причём, если для некоторого множества C в одном из неравенств достигается равенство, то его характеристическая функция есть совершенная раскраска.

Доказательство. Действуем аналогично доказательству леммы 1. В этом случае имеем $\chi_C = \chi_B = \chi_A$, поэтому равенство (4) принимает вид

$$(\chi_C - \alpha_0\phi_0, M(\chi_C - \beta_0\phi_0)) = \sum_{i\neq 0}\lambda_i\alpha_i^2$$

и

$$\lambda_k\sum_{i\neq 0}\alpha_i^2 \leq \sum_{i\neq 0}\lambda_i\alpha_i^2 \leq \lambda_1\sum_{i\neq 0}\alpha_i^2.$$

Используя равенство (6), получаем требуемое неравенство. Очевидно в неравенстве достигается равенство только в случае, когда функция $\chi_A - \alpha_0\phi_0$ является собственной функцией матрицы M с собственным числом λ_1 или λ_k. □

Определение 9. *Независимым подмножеством вершин графа называется подмножество, не содержащее смежных вершин.*

Определение 10. *Подмножество вершин графа называется доминирующим, если любая вершина графа либо в нём содержится, либо смежна с некоторыми из его вершин.*

Из определения видно, что максимальное по включению независимое подмножество вершин графа является доминирующим. Нетрудно видеть, что если в графе имеется совершенный код, то он является минимальным по мощности доминирующим подмножеством.

Утверждение 15 (граница Дельсарта—Хоффмана [49])**.** *Пусть G — r-регулярный граф и λ_{min} — минимальное собственное число его матрицы смежности M. Тогда мощность любого независимого множества в графе G не превосходит $\frac{\lambda_{min}|V(G)|}{\lambda_{min}-r}$. Независимое множество имеет мощность $\frac{\lambda_{min}|V(G)|}{\lambda_{min}-r}$ тогда и только тогда, когда его характеристическая функция есть совершенная раскраска с матрицей параметров $S = \begin{pmatrix} 0 & r \\ -\lambda_{min} & r+\lambda_{min} \end{pmatrix}$.*

Доказательство. Без ограничения общности можно считать, что граф G связен, поскольку в противном случае компоненты связности можно рассматривать по отдельности. Определение независимого множества C эквивалентно равенству $e(C,C) = 0$. Тогда из следствия 10 имеем требуемое неравенство $\lambda_{min}|C| + \frac{(r-\lambda_{min})|C|^2}{|V(G)|} \leq 0$.

Кроме того, в следствии 10 утверждается, что равенство $\frac{|C|}{|V(G)|} = \frac{\lambda_{min}}{\lambda_{min}-r}$ имеет место только в случае когда χ_C — совершенная раскраска. Из незавависимости C следует, что $a = s_{11} = 0$. Коэффициент $c = s_{21}$ матрицы S можно найти из соотношения на число рёбер с разноцветными концами: $|C|r = c(|V(G)| - |C|)$.

Поскольку $s_{11} = 0$, первый цвет совершенной раскраски с матрицей параметров S является независимым множеством. Число вершин первого цвета нетрудно вычислить из соотношения $|C|r = -\lambda_{min}(|V(G)|-|C|)$. Таким образом, мощность множества вершин первого цвета достигает границы Дельсарта—Хоффмана. □

Замечание 4. Вместо матрицы M смежности графа можно рассмотреть любую другую неотрицательную симметричную матрицу M' с суммой r' элементов в строках с тем же или меньшим множеством ненулевых элементов, что и у матрицы M. При этом условии для любой характеристической функции f из $(Mf, f) = 0$ следует, что $(M'f, f) = 0$. В доказательстве границы Дельсарта—Хоффмана нигде не использовалось то, что матрица M содержит только нули и единицы, а только неотрицательность и симметричность матрицы M. Поэтому справедлива верхняя оценка $\frac{\lambda'_{min}|V(G)|}{\lambda'_{min}-r'}$ на мощность независимого множества в графе G, где λ'_{min} — минимальное собственное число матрицы M'.

3.2 Дельсартовы клики

Напомним, что кликой в графе называется подграф, все вершины которого попарно соединены рёбрами. Нетрудно видеть, что в дополнении к графу клика переходит в независимое множество и наоборот. Для r-регулярного связного графа G на n вершинах нетрудно показать, что минимальное собственное число его дополнения равно $-\lambda_2-1$, где $\lambda_2 < r$ — максимальное нетривиальное собственное число графа G, и $n-r-1$ — степень дополнения. Тогда из границы Дельсарта—Хоффмана следует, что максимальное независимое множество в дополнении к G, а значит и клика в G, по мощности не превосходят $\frac{(\lambda_2+1)n}{\lambda_2+n-r}$. Для размера клики в рёберно транзитивном графе можно получить другую, обычно более сильную, оценку.

Теорема 4 (о дельсартовой клике [38]). *Мощность клики в рёберно транзитивном r-регулярном графе G не превышает $1-\frac{r}{\lambda_{min}}$, где λ_{min} — минимальное собственное число графа G.*

Доказательство. Пусть $u_1,\dots,u_m$ — ортонормированный базис собственного подпространства $X_{\lambda_{min}}$. Рассмотрим автоморфизм π графа G. Очевидно, что при автоморфизме графа один ортонормированный базис собственного подпространства $X_{\lambda_{min}}$ переходит в другой. Пусть Q_π — соответствующая этому преобразованию ортогональная матрица размера $m\times m$.

Рассмотрим вектора $w(x)=(u_1(x),\dots,u_m(x))$, где $x\in V(G)$. Покажем, что их скалярные произведения одинаковы для всех пар соседних вершин x и y. Действительно, рассмотрим автоморфизм π графа G, переводящий ребро $\{x,y\}$ в ребро $\{\pi(x),\pi(y)\}$. Тогда $(u_1(x),\dots,u_m(x))Q_\pi = (u_1(\pi(x)),\dots,u_m(\pi(x)))$. Имеем $(w(x),w(y)) = (w(x)Q_\pi, w(y)Q_\pi) = (w(\pi(x)),w(\pi(y))$. Пусть $(w(x),w(y))=\beta$ для любых соседних вершин $x,y\in V(G)$. Аналогично, рассмотрев автоморфизмы графа G, переводящие вершину в любую другую вершину, получим $(w(x),w(x))=\alpha$ для любой вершины $x\in V(G)$.

Из определения собственной функции имеем равенство $\sum\limits_{y\in S_1(x)} u_i(y) = \lambda_{min}u_i(x)$, т. е. $\sum\limits_{y\in S_1(x)} w(y) = \lambda_{min}w(x)$. Скалярно умножая предыдущее равенство на $w(x)$, имеем соотношение $r\beta=\lambda_{min}\alpha$.

Пусть $C\subset V(G)$ клика в графе G. Рассмотрим матрицу Грама W размера $|C|\times|C|$, элементами которой являются $(w(x),w(y))$, $x,y\in C$. По доказаному выше

$$W=\begin{pmatrix} \alpha & \beta & \beta & \dots & \beta \\ \beta & \alpha & \beta & \dots & \beta \\ \dots & \dots & \dots & \dots & \dots \\ \beta & \dots & \dots & \beta & \alpha \end{pmatrix}.$$

Матрица Грама неотрицательно определена, поэтому $(W\overline{1},\overline{1}) \geq 0$, следовательно, $\alpha + (|C|-1)\beta \geq 0$. Поскольку минимальное собственное число λ_{min} отрицательное (см. задачу 1), отсюда и из равенства $r\beta = \lambda_{min}\alpha$ имеем $|C| \leq 1 - \frac{r}{\lambda_{min}}$. □

Определение 11. *Клика мощности* $1 - \frac{r}{\lambda_{\min}}$ *в* r*-регулярном графе* G *называется дельсартовой.*

Следствие 11. *Пусть рёберно транзитивный граф* G *имеет дельсартовы клики и содержит независимое множество* C*, достигающее границы Дельсарта – Хоффмана. Тогда каждая дельсартова клика содержит ровно одну вершину из* C *и каждая вершина из* C *содержится в одинаковом числе дельсартовых клик.*

Доказательство. Поскольку граф транзитивный, каждая вершина содержится в одинаковом количестве дельсартовых клик. Обозначим это число s. Тогда количество дельсартовых клик равно $s|V(G)|/(1 - \frac{r}{\lambda_{\min}})$. Независимое множество C пересекается с $|C|s = s|V(G)|/(1 - \frac{r}{\lambda_{\min}})$ кликами. Поэтому каждая клика содержит вершину из C. □

3.3 Раскраски графов, регулярных по расстоянию 2

Пусть M — матрица смежности некоторого графа G. Тогда $M\mathbf{1}$ — вектор степеней вершин графа, $n = (\mathbf{1},\mathbf{1})$ — число вершин в графе и $(M\mathbf{1},\mathbf{1})/n$ — средняя степень вершины графа G. Тогда i-ая координата вектора $M(M\mathbf{1})$ равна суммарному числу вершин, которые видят соседи i-ой вершины (если какую-то вершину видят k соседей, то она считается k раз) или, иными словами, i-ая координата вектора $M(M\mathbf{1})$ равна числу путей длины 2, которые заканчиваются в i-ой вершине графа. Таким образом, $(M^2\mathbf{1},\mathbf{1})/n$ есть средняя сумма степеней соседей вершин графа G.

Утверждение 16. *Для любого графа квадрат средней степени вершины не превышает среднюю сумму степеней соседей вершины. Причём в случае равенства граф является регулярным.*

Доказательство. Из неравенства Коши—Буняковского имеем

$$(M\mathbf{1},\mathbf{1})^2 \leq (M\mathbf{1},M\mathbf{1})(\mathbf{1},\mathbf{1}),$$

отсюда

$$\left(\frac{(M\mathbf{1},\mathbf{1})}{(\mathbf{1},\mathbf{1})}\right)^2 \leq \frac{(M^2\mathbf{1},\mathbf{1})}{(\mathbf{1},\mathbf{1})}.$$

Причём равенство достигается только когда вектора $M\mathbf{1}$ и $\mathbf{1}$ коллинеарны, что эквивалентно регулярности графа. □

Рассмотрим раскраску $f : V(G) \to \{0, 1\}$ регулярного графа G в два цвета. Пусть G_i — подграф, порождённый вершинами цвета $i \in \{0, 1\}$. Для каждого из этих подграфов справедливо утверждение 16. Введём обозначения $g = f \cdot Mf$ и $g' = f' \cdot Mf'$, где $f' = \mathbf{1} - f$ и умножение векторов поэлементное. Из неравенства Коши—Буняковского имеем $(g, f)^2 \leq (g, g)(f, f)$ и $(g', f')^2 \leq (g', g')(f', f')$. Покажем, что равенство в обоих неравенствах одновременно достигается тогда и только тогда, когда раскраска f совершенная.

Удалим из графа все вершины цвета 0, тогда для порождённого подграфа G_1 функции f и g играют роль функций $\mathbf{1}$ и $M\mathbf{1}$. В случае равенства все вершины цвета 1 видят одинаковое число вершин цвета 1, а значит из регулярности графа G, одинаковое число вершин цвета 0. Аналогичные рассуждения верны для характеристической функции f' цвета 0. Верно и обратное, если раскраска f совершенная, то вектора f и g, а также f' и g' коллинеарны.

Другим примером экстремального свойства совершенной раскраски служит следующая теорема, для формулировки которой нам понадобятся несколько обозначений.

Обозначим через M_2 матрицу расстояний 2 между вершинами графа, т. е.

$$M_2(x, y) = \begin{cases} 1, & d(x, y) = 2; \\ 0, & \text{иначе.} \end{cases}$$

Как отмечено выше, матрица M^2 задает количество путей длины 2 между вершинами. Двукратное прохождение ребра рассматривается как путь длины 2, который начинается и заканчивается в одной и той же вершине. Определим некоторое усиление свойства регулярности, которое на английском называется amply regular.

Определение 12. *Граф называется регулярным по расстоянию* 2*, если любые смежные вершины имеют одинаковое число общих соседей и любые вершины на расстоянии 2 также имеют одинаковое число общих соседей.*

Иными словами любая пара смежных вершин такого графа имеет λ общих соседей, а любая пара несмежным вершин 0 или $\mu > 0$ общих соседей. Рассмотрим граф, регулярный по расстоянию 2. Ясно, что между любыми двумя вершинами на расстоянии 1 одинаковое число $a_1 = \lambda$ путей длины 2 и между любыми двумя вершинами на расстоянии 2 одинаковое число $c_2 = \mu$ путей длины 2. Тогда для его матрицы M^2 путей длины 2 справедливо равенство $M^2 = c_2 M_2 + a_1 M + b_0 I$, где b_0 — степень вершин графа. Обозначения c_2, a_1, b_0 согласованы со стандартными обозначениями для дистанционно-регулярных графов (см. раздел 4.1). Таким образом, $M_2 = p_2 M^2 + p_1 M + p_0 I$, для некоторых p_0, p_1, p_2. Пусть f — произвольная раскраска графа G в k цветов, f_i — характеристическая

функция цвета i, а n_i — количество вершин цвета i. Через $s_{ij}(x)$, как и раньше, обозначается число вершин цвета j, которые видит вершина x цвета i. Определим матрицу усреднённого цветового окружения S_f так, что $\bar{s}_{ij}$ — среднее число вершин цвета j, которое видит вершина цвета i, т. е. $\bar{s}_{ij} = \frac{1}{n_i} \sum\limits_{f(x)=i} s_{ij}(x)$.

Теорема 5 (Кротов [56]). *Пусть граф G регулярен по расстоянию 2, т. е. для его матрицы смежности M_2 по расстоянию 2 справедливо равенство $M_2 = P(M) = p_2M^2 + p_1M + p_0I$, и пусть f — некоторая раскраска графа G в k цветов с матрицей усреднённого цветового окружения S_f. Тогда для любого цвета i число пар вершин цвета i на расстоянии 2 друг от друга не превосходит $n_i(p(S_f))_{ii}/2$, и если для каждого цвета i достигается равенство, то f — совершенная раскраска с матрицей параметров S_f.*

Доказательство. Пусть f_i — характеристическая функция множества вершин i-го цвета. Любую функцию на вершинах графа, можно представить в виде суммы функций, каждая из которых ненулевая только на вершинах определенного цвета. Тогда можно определить функции g^i_j так, что $Mf_i = \sum_j g^i_j$, где $\operatorname{supp}(g^i_j) \subseteq \operatorname{supp}(f_j)$.

По условию $(g^i_j, f_j) = (Mf_i, f_j) = \bar{s}_{ij}n_i = \bar{s}_{ji}n_j$. Из неравенства Коши – Буняковского имеем $(g^i_j, f_j)^2 \le (g^i_j, g^i_j)(f_j, f_j)$, причём равенство возможно только в случае, когда векторы g^i_j и f_j коллинеарны. Поскольку $g^i_j(x) = s_{ji}(x)f_j(x)$ для любой вершины цвета j, имеем равенство $g^i_j = \bar{s}_{ji}f_j$, когда векторы g^i_j и f_j коллинеарны.

Удвоенное число пар вершин цвета i на расстоянии 2 друг от друга равно (M_2f_i, f_i). В итоге имеем следующие соотношения

$$(M_2f_i, f_i) = (P(M)f_i, f_i) = (p_0f_i + p_1Mf_i + p_2M^2f_i, f_i) =$$
$$= p_0(f_i, f_i) + p_1(Mf_i, f_i) + p_2(Mf_i, Mf_i) =$$
$$= p_0n_i + p_1\bar{s}_{ii}n_i + p_2(\sum_j g^i_j, \sum_j g^i_j) = p_0n_i + p_1\bar{s}_{ii}n_i + p_2\sum_j (g^i_j, g^i_j) \ge$$
$$\ge p_0n_i + p_1\bar{s}_{ii}n_i + p_2\sum_j (g^i_j, f_j)^2/n_j =$$
$$= p_0n_i + p_1\bar{s}_{ii}n_i + p_2\sum_j \bar{s}_{ij}\bar{s}_{ji}n_in_j/n_j = n_i(p(S_f))_{ii}.$$

Причём равенство достигается только тогда, когда $g^i_j = \bar{s}_{ij}f_j$ для всех i, j, т. е. когда f — совершенная раскраска с матрицей параметров S_f. □

Из определения совершенной раскраски ясно, что матрица параметров совершенной раскраски определяет сколько вершин одного цвета

видит вершина другого цвета, а для графа, регулярного по расстоянию 2, можно вычислить сколько вершин одного цвета находятся на расстоянии 2 от некоторой вершины другого цвета. В частности, для множества вершин C первого цвета в раскраске с матрицей параметров $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ справедливы равенства $(M\chi_C, \chi_C) = a|C|$, $(M_2\chi_C, \chi_C) = (p_2(a^2 + bc) + p_1 a + p_0)|C|$ и $|C| = \frac{c|V(G)|}{b+c}$. Если ввести обозначение $\beta = p_2(a^2 + bc) + p_1 a + p_0$, то $\frac{c}{b+c} = \frac{bc}{b^2+bc} = \frac{\beta - P(a)}{p_2 b^2 + \beta - P(a)}$.

Покажем, что из ограничения сверху на среднее число $(M_2\chi_C, \chi_C)/|C|$ вершин на расстоянии 2 в некотором множестве C можно получить ограничение сверху на мощность $|C|$. Более того, если эта верхняя оценка числа вершин достигается, то характеристическая функция множества C оказывается совершенной раскраской в два цвета.

Теорема 6. *Пусть r-регулярный граф G регулярен по расстоянию 2, т. е. для его матрицы смежности M_2 по расстоянию 2 справедливо равенство $M_2 = P(M) = p_2 M^2 + p_1 M + p_0 I$. Тогда для любого $C \subset V(G)$ имеем если $(M\chi_C, \chi_C) = a|C|$ и $(M_2\chi_C, \chi_C) \le \beta|C|$, то $\frac{|C|}{|V(G)|} \le \frac{\beta - P(a)}{p_2(r-a)^2 + \beta - P(a)}$; равенство в последнем неравенстве достигается только если в первом неравенстве также достигается равенство, в этом случае χ_C — совершенная раскраска.*

Доказательство. Можно считать, что граф G связен, иначе компоненты связности нужно рассмотреть по отдельности. Характеристическую функцию χ_C можно представить в виде линейной комбинации: $\chi_C = \sum_i \alpha_i \phi_i$, где ϕ_i — нормированная собственная функция матрицы M с собственным числом λ_i. Собственной функцией, соответствующей собственному числу r, является $\phi_0 = \mathbf{1}/\sqrt{|V(G)|}$. Из равенства $(\chi_C, \chi_C) = \sum_i \alpha_i^2$ следует, что

$$\text{(I)} \qquad \sum_{i \neq 0} \alpha_i^2 = (\chi_C, \chi_C) - \alpha_0^2 = |C| - \varrho|C|,$$

где $\varrho = |C|/|V(G)|$. Из равенств $(M\chi_C, \chi_C) = a|C|$ и $(M\chi_C, \chi_C) = \sum_i \alpha_i^2 \lambda_i$, где λ_i — собственные числа функций ϕ_i, имеем

$$\text{(II)} \quad r\varrho|C| + \sum_{i \neq 0} \alpha_i^2 \lambda_i = a|C|.$$

Из условия теоремы получаем

$$(M^2\chi_C, \chi_C) = \frac{1}{p_2}((M_2 - p_1 M - p_0 I)\chi_C, \chi_C) \le \frac{|C|}{p_2}(\beta - p_1 a - p_0).$$

Тогда

$$\text{(III)} \quad r^2\varrho|C| + \sum_{i \neq 0} \alpha_i^2 \lambda_i^2 \le \frac{|C|}{p_2}(\beta - p_1 a - p_0).$$

Сложим левые и правые части выражений (I)–(III) по формуле (III) -2θ(II) $+\theta^2$(I). Получаем неравенство

$$r^2\varrho|C|-2r\varrho\theta|C|+\sum_{i\neq 0}\alpha_i^2(\lambda_i-\theta)^2 \leq \frac{|C|}{p_2}(\beta-p_1a-p_0)-2a\theta|C|+|C|(1-\varrho)\theta^2,$$

$$r^2\varrho-2r\varrho\theta \leq \frac{1}{p_2}(\beta-p_1a-p_0)-2a\theta+(1-\varrho)\theta^2,$$

$$\varrho \leq \frac{\frac{1}{p_2}(\beta-P(a))+(a-\theta)^2}{(r-\theta)^2}.$$

Выберем $\theta = a-\frac{\beta-P(a)}{p_2(r-a)}$. Тогда

$$\varrho \leq \frac{(a-\theta)(r-a)+(a-\theta)^2}{(r-a+a-\theta)^2} = \frac{a-\theta}{r-\theta} = \frac{\beta-P(a)}{p_2(r-a)^2+\beta-P(a)}.$$

Равенство имеет место только в случае когда $\sum\limits_{i\neq 0}\alpha_i^2(\lambda_i-\theta)^2=0$, т. е. $\mathbf{1}_C = \phi+\alpha_0\phi_0$, где ϕ — собственная функция с собственным числом θ. Из следствия 6 получаем, что χ_C — совершенная раскраска. □

Если C — независимое множество, то $a=0$, $P(0)=-rp_2$ и $\varrho \leq 1/(1+\frac{p_2r^2}{\beta+rp_2})$. Если и $\beta=0$, то получаем границу Хэмминга $\varrho \leq 1/(1+r)$.

Задача 18. Пусть G — r-регулярный граф и $f: V(G)\to\mathbb{C}$. Докажите равенство $((rI-M)f,f) = \sum\limits_{\{x,y\}\in E(G)}|f(x)-f(y)|^2$.

Задача 19. Пусть $f: V(G)\to\{0,1\}$ — некоторая раскраска r-регулярного графа G. Ребро графа G назовём "пёстрым если его концы покрашены в разные цвета. Докажите неравенство
$(r-\lambda)|f^{-1}(1)||f^{-1}(0)| \geq p|V(G)|$, где p — число пёстрых рёбер и λ — минимальное собственное число матрицы смежности графа G. Докажите, что если в этом неравенстве достигается равенство, то раскраска f — совершенная.

Задача 20. Пусть r-регулярный граф G и λ — минимальное собственное число его матрицы смежности M. Докажите, что если любая вершина из множества A видит не более $t<r$ вершин из множества A, то $|A| \leq \frac{(t-\lambda)|V(G)|}{r-\lambda}$. И если множество A имеет мощность $\frac{(t-\lambda)|V(G)|}{r-\lambda}$, то его характеристическая функция есть совершенная раскраска графа G.

Задача 21. Хроматическим числом $\chi(G)$ графа G называется минимальное число цветов в его правильной раскраске. Докажите, что $\chi(G) \geq \frac{\lambda-r}{\lambda}$ для r-регулярного графа G с минимальным собственным числом λ. Докажите, что если $\chi(G)=\frac{\lambda-r}{\lambda}$, то любая правильная раскраска графа G в $\chi(G)$ цветов является совершенной.

Задача 22. Пусть G — r-регулярный граф и λ — второе после r максимальное собственное число его матрицы смежности M. Докажите, что мощность любой клики в графе G не превосходит числа $\frac{\lambda+1}{1-(r-\lambda)/|V(G)|}$.

Задача 23. Докажите, что для любого независимого подмножества C r-регулярного и регулярного по расстоянию 2 графа G справедливо неравенство $\frac{(M_2\chi_C,\chi_C)}{|C|} \leq -p_2 r(\lambda_{min}+1)$, где λ_{min} — минимальное собственное число графа G, а p_2 — коэффициент при старшей степени в полиномиальном представлении M_2 — матрицы смежности по расстоянию 2 в графе G.

Задача 24. Пусть выполнены условия предыдущей задачи и $\beta = \frac{(M_2\chi_C,\chi_C)}{|C|}$. Докажите, что для независимого множества граница из теоремы 6 не хуже границы Дельсарта — Хоффмана, т. е. $1/(1+\frac{p_2 r^2}{\beta+p_2 r}) \leq \frac{-\lambda_{min}}{r-\lambda_{min}}$.

4 Дистанционно-регулярные графы

4.1 Определение дистанционно-регулярного графа

Определение 13. *Связный граф G называется дистанционно-регулярным*[11], *если для любых двух его вершин x и y, которые находятся на расстоянии $d(x,y)=i$, и любых двух чисел j и k число вершин в множестве $\{z \in V(G) \mid d(x,z)=j,\ d(y,z)=k\}$ зависит только от чисел i,j,k, но не от выбора вершин x и y.*

Зафиксируем некоторую вершину x_0 и рассмотрим дистанционное расслоение графа G относительно неё: $A_t = \{x \in V(G) \mid d(x,x_0)=t\}$. Рассмотрим слой A_t. Вершина $x \in A_t$ смежна с a_t вершинами в своем слое, с b_t вершинами в следующем слое и с c_t вершинами в предыдущем слое. В дистанционно-регулярном графе эти параметры не зависят от выбора x_0 и вершины $x \in A_t$. И наоборот, если параметры a_t, b_t, c_t не зависят от выбора x_0 и вершины $x \in A_t$, то граф является дистанционно-регулярным.

Любой дистанционно-регулярный граф является регулярным, степень каждой вершины в нём равна $b_0 = r$. Поэтому $a_t + b_t + c_t = r$ для любого $t > 0$, не превышающего диаметр графа.

Определение 14. *Набор значений $(b_0,\ldots,b_{d-1};c_1,\ldots,c_d)$ называется массивом пересечений дистанционно-регулярного графа диаметра d.*

Из определения видно, что дистанционная относительно любой вершины x_0 раскраска дистанционно-регулярного графа: $\varphi(x)=t$ при $x \in$

[11] Подробное изложение теории дистанционно-регулярных графов имеется в [14].

A_t является совершенной с матрицей параметров дистанционно-регулярного графа $S[G] = \begin{pmatrix} 0 & b_0 & 0 & 0 & \dots & 0 \\ c_1 & a_1 & b_1 & 0 & \dots & 0 \\ 0 & c_2 & a_2 & b_2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & c_d & a_d \end{pmatrix}$, где d — диаметр графа.

Непосредственно из определений следует, что если дистанционная (относительно любой вершины) раскраска графа является совершенной с независящей от вершины матрицей параметров, то граф является дистанционно-регулярным.

Пример 8. Булев n-куб $Q_2^n = \{0,1\}^n$ является дистанционно-регулярным графом диаметра n с параметрами $a_t = 0$, $b_t = n - t$, $c_t = t$.

Пример 9. Гиперкуб Q_q^n является дистанционно-регулярным графом диаметра n с параметрами $a_t = (q-2)t$, $b_t = (n-t)(q-1)$, $c_t = t$.

Пример 10. *Граф Джонсона* $J(n,k)$ определяется следующим образом. В качестве множества вершин нужно взять все двоичные наборы длины n и веса k. Вершины соединены ребром, если расстояние Хэмминга между двумя наборами равно двум. Граф Джонсона $J(n,k)$ является дистанционно-регулярным с параметрами $a_t = nt - t^2$, $b_t = (k-t)(n-k-t)$, $c_t = t^2$.

Возникает естественный вопрос: однозначно ли задается дистанционно-регулярный граф своим массивом пересечений? Оказывается нет. Например, одинаковый массив пересечений $(b_0, b_1; c_1, c_2) = (6, 3; 1, 2)$ имеют Q_4^2 и граф Шрикханде (см. пример 24). Декартовы произведения (см. раздел 5) этих графов с одинаковым количеством сомножителей являются неэквивалентными дистанционно-регулярными графами с совпадающими массивами пересечений.

Пусть M_t — матрица смежности графа по расстоянию t, иными словами:

$$M_t(x,y) = \begin{cases} 1, & d(x,y) = t; \\ 0, & \text{иначе.} \end{cases}$$

Выясним, как в дистанционно-регулярном графе матрица смежности графа по расстоянию t выражается через матрицу смежности (по расстоянию 1). Заметим, что элементы матрицы M^k задают количество путей длины k между вершинами графа. Например, при $k = 2$ количество путей длины 2 из произвольной фиксированной вершины складывается из путей, проходящих дважды по одному ребру; путей, соединяющих исходную вершину с вершиной, находящейся на расстоянии 2 от неё.

Пример 11. Пусть M — матрица смежности булева n-куба $Q_2^n = \{0,1\}^n$. В любую вершину, находящуюся на расстоянии 2 от исходной, можно

попасть двумя способами: двигаясь сначала по ребру направления i, а затем j, $j \neq i$, и наоборот. Тогда

$M_0 = I_{2^n}$, $M_1 = M$,

$MM = 0 + b_0 I_{2^n} + c_2 M_2$, где $b_0 = n$, $c_2 = 2$.

$M^2 = nI_{2^n} + 2M_2$.

Зафиксируем некоторую вершину дистанционно-регулярного графа, возьмем вершину на расстоянии t от неё и рассмотрим её соседей. Для матриц смежности (по разным расстояниям) дистанционно-регулярного графа справедливо равенство

$$M_t M = a_t M_t + b_{t-1} M_{t-1} + c_{t+1} M_{t+1}. \tag{7}$$

Действительно, в матрице $M_t M$ на позиции (i, j) указано число способов попасть из вершины x_i в x_j, сначала переместившись в промежуточную, смежную с x_j, вершину, находящуюся на расстояние t от x_i, а потом из неё в вершину x_j. Очевидно, элемент матрицы $(a_t M_t)_{ij}$ равен числу способов проделать такой путь, если $d(x_i, x_j) = t$; $(b_{t-1} M_{t-1})_{ij}$, если $d(x_i, x_j) = t - 1$; $(c_{t+1} M_{t+1})_{ij}$, если $d(x_i, x_j) = t + 1$. Таким образом имеют место рекуррентные соотношения (7). Нетрудно видеть, что верно и обратное. Если для некоторого графа матрицы M_t смежности по расстоянию t при $t = 2, \ldots, d$, где d — диаметр графа, удовлетворяют рекуррентным соотношениям (7) для некоторых неотрицательных целых чисел a_t, b_t, c_t, то граф G является дистанционно-регулярным.

По индукции получаем, что $M_t = P_t(M)$, где P_t — полином степени t. Откуда видно, что умножение матриц смежности по различным расстояниям коммутативно, т. е. $M_t M_s = M_s M_t$. Кроме того из (7) следует рекуррентное соотношение

$$x P_t(x) = a_t P_t(x) + b_{t-1} P_{t-1}(x) + c_{t+1} P_{t+1}(x). \tag{8}$$

Из соотношения 8 по индукции нетрудно сделать следующее заключение.

Замечание 5. В дистанционно-регулярном графе диаметра d степень M^t, $t = 2, \ldots, d$ его матрицы смежности M представима как линейная комбинация его матриц смежности по расстоянию i, $i = 0, \ldots, t$.

Любой дистанционно-регулярный граф определяет некоторую ассоциативную схему[12].

Определение 15. *Ассоциативной схемой $\mathcal{A}$ на множестве X называется набор бинарных отношений $R_0, \ldots, R_m \subset X \times X$, удовлетворяющий условиям:*

1) $R_0 = \{(x, x) \mid x \in X\}$, $R_0 \in \mathcal{A}$;

[12] Подробное изложение теории дистанционно-регулярных графов имеется в [105].

2) $R^* = \{(x,y) \mid (y,x) \in R\}$, $R \in \mathcal{A} \Rightarrow R^* \in \mathcal{A}$;

3) *если* $(x,y) \in R_k$, *то число таких* $z \in X$, *что* $(x,z) \in R_i$ *и* $(z,y) \in R_j$, *зависит только от* i,j,k.

Чтобы определить ассоциативную схему по дистанционно-регулярному графу нужно в качестве множества X взять множество вершин $V(G)$ дистанционно-регулярного графа G, а в качестве R_i рассмотреть множество пар вершин на расстоянии i.

4.2 Полиномы Кравчука

В случае булева n-куба полином P_t называется полиномом Кравчука[13]. Если же рассматривается q-ичный куб, то полином P_t называется q-полином Кравчука $P_t[n,q](y)$. Для графов Джонсона полином P_t называется полиномом Эберлейн.

Замечание 6. Стоит отметить, что классический полином Кравчука $K_t[n,q](x)$ отличается от полинома $P_t[n,q](y)$ линейной заменой переменной $y = n(q-1) - qx$ при этом $K_0[n,2] = 1$, $K_1[n,2] = n - 2x$.

Замечание 7. Граф по расстоянию t, т. е. граф с матрицей смежности M_t, полученный из дистанционно-регулярного графа (с матрицей смежности M), обычно уже не является дистанционно-регулярным. Но имеются исключения, например, граф по расстоянию 2, полученный из графа булева n-куба для произвольного n, является дистанционно-регулярным.

Найдём явное выражение степенных функций через полиномы Кравчука, т. е. явное выражение коэффициентов из замечания 5 в случае булева n-куба. Как отмечено выше, $(M^r)_{ij}$ — число путей длины r между вершинами x_i и x_j в графе G. В данном случае предполагается, что по одному и тому же ребру можно проходить несколько раз. Коэффициенты полиномов P_t определяют треугольную матрицу с ненулевой диагональю, поэтому имеются обратные соотношения:

$$M^r = \alpha_0^r I_N + \alpha_1^r M_1 + \cdots + \alpha_r^r M_r$$

с некоторыми коэффициентами a_i^r, $i = 1, \ldots r$.

В случае булева n-куба из предыдущего равенства и равенств $M_i M = (n-i+1)M_{i-1} + (i+1)M_{i+1}$ при $i = 1, \ldots r$ получаем равенства

$$M^{r+1} = \alpha_0^r M + \alpha_1^r (nI_{2^n} + 2M_2) + \cdots + \alpha_r^r ((n-r+1)M_{r-1} + (r+1)M_{r+1}).$$

Отсюда имеем рекуррентные соотношения $\alpha_i^{r+1} = i\alpha_{i-1}^r + (n-i)\alpha_{i+1}^r$ при $i = 1, \ldots r$ и $\alpha_{r+1}^r = 0$. Известные равенства $\alpha_i^r = (\mathrm{ch}^{n-i} x \,\mathrm{sh}^i x)^{(r)} \mid_{x=0}$,

[13] Подробнее о свойствах многочленов Кравчука можно прочитать в обзоре [119].

можно проверить, получив те же рекуррентные соотношения для производных функций $\mathrm{ch}^{n-i}x\,\mathrm{sh}^i x$. Таким образом, чтобы найти кооэффициенты α_i^r для булева гиперкуба достаточно посчитать производную r-го порядка в точке $x = 0$ от произведения степеней гиперболических косинусов и синусов.

4.3 Теорема Шапиро–Злотника–Мартина

Теорема 7 (Шапиро и Злотник, Мартин [70]). *Пусть G — дистанционно-регулярный граф, G_t — граф по расстоянию t, полученный из G, т. е. $V(G_t) = V(G)$, $M(G_t) = M_t$. Если f — совершенная раскраска графа G с матрицей параметров S, то f — совершенная раскраска графа G_t с матрицей параметров $P_t(S)$.*

Доказательство. Имеем $MF = FS$, где F — матрица, соответствующая раскраске f. Из равенства $M_t = P_t(M)$ следует равенство $M_tF = P_t(M)F$. Кроме того, имеем равенства $M^tF = M^{t-1}MF = M^{t-1}(FS) = FS^t$. Тогда $P_t(M)F = FP_t(S)$. □

Следствие 12. *Для любой совершенной раскраски дистанционно-регулярного графа цветовой состав сферы радиуса t зависит только от цвета центра сферы.*

Изначально этот факт был установлен Ллойдом [67] для совершенных кодов в булевом n-кубе. Шапиро и Злотник [88] нашли весовое распределение (см. ниже) совершенного кода.

Теорема 7 даёт способ доказательства несуществования раскраски. Подставив матрицу параметров S совершенной раскраски в многочлен P_t, мы должны получить матрицу, все элементы которой неотрицательные целые числа. Кроме того, вектор пропорций цветов, вычисленный по матрице $P_t(S)$ и умноженный на мощность графа, также должен быть целочисленным. Однако, отсутствуют такие примеры, чтобы матрица S удовлетворяла необходимым условиям (теорема 1) для матрицы параметров, а матрица $P_t(S)$ нет.

Утверждение 17. *Связный регулярный граф G ровно с тремя различными собственными числами является дистационно-регулярным.*

Доказательство. Пусть M — матрица смежности r-регулярного графа G. Матрица является корнем своего характеристического многочлена, поэтому $(M - rI)p(M) = 0$, где $p(x) = (x - \lambda_1)(x - \lambda_2)$ и $\lambda_1 < \lambda_2 < r$ — собственные числа матрицы M. Из равенства $(M - rI)p(M) = 0$ следует, что матрица M^3 равна линейной комбинации матриц I, M и M^2. Тогда любой путь длины 3 в графе G соединяет вершины, находящиеся на расстоянии 0, 1 или 2. Следовательно, граф G имеет диаметр

2. Из связности графа G следует, что матрица M имеет единственный собственный вектор $\mathbf{1}$ с собственным числом r. Тогда из уравнения $(M - rI)p(M) = 0$ следует, что все столбцы матрицы $p(M)$ коллинеарны вектору $\mathbf{1}$. Аналогично, все строки матрицы $p(M)$ коллинеарны вектору $\mathbf{1}$. Тогда $p(M) = \alpha J$, где все компоненты матрицы J равны 1. Имеем $M_2 = J - M - I$ и $p(M) = \alpha(M_2 + M + I)$. Таким образом, мы получили частный случай равенства (7), эквивалентного дистанционной регулярности графа. □

Определение 16. *Дистанционно-регулярный граф диаметра* 2 *называется сильно регулярным.*

4.4 Нижняя граница мощности носителя

Определение 17. *Весовым распределением функции* $f : V(G) \to \mathbb{C}$ *относительно вершины* $a \in V(G)$ *графа* G *называется набор* $[f(a), \ldots, \sum\limits_{d(y,a)=t} f(y), \ldots, \sum\limits_{d(y,a)=d} f(y)]$, *где* d *— диаметр графа* G.

Утверждение 18. *Пусть* f *— собственная функция дистанционно-регулярного графа* G *с собственным числом* λ, *т. е.* $Mf = \lambda f$. *Тогда* $\sum\limits_{d(y,a)=t} f(y) = P_t(\lambda) f(a)$.

Доказательство. Аналогично доказательству теоремы Шапиро–Злотника–Мартина имеем равенства $M^i f = \lambda^i f$ и $M_t f = P_t(M) f = P_t(\lambda) f$. Следовательно, $\sum\limits_{d(y,a)=t} f(y) = (M_t f)(a) = P_t(\lambda) f(a)$. □

Таким образом, в дистанционно-регулярном графе сумма значений собственной функции по сфере зависит только от собственного числа и значения функции в центре сферы. Для определённости можно считать, что $f(a) = 1$. Тогда набор $[1, P_1(\lambda), \ldots, P_d(\lambda)]$ является весовым распределением (спектром) собственной функции с собственным числом λ.

Любую функцию $g : V(G) \to \mathbb{C}$ можно представить в виде линейной комбинации собственных функций графа: $g = \sum_i \alpha_i f_i$, где f_i — собственная функция дистанционно-регулярного графа G с собственным числом λ_i. Тогда имеем

Следствие 13. *Пусть функция* g *задана на вершинах дистанционно-регулярного графа* G. *Тогда* $\sum\limits_{d(y,a)=t} g(y) = \sum_i \alpha_i P_t(\lambda_i) f_i(a)$.

Носителем функции называется множество $\operatorname{supp}(f) = \{x \in V(G) \mid f(x) \neq 0\}$.

Утверждение 19 ([58]). *Пусть f — собственная функция с собственным числом λ в дистанционно-регулярном графе. Тогда* $|\mathrm{supp}(f)| \geq \sum_{t=0}^{d} |P_t(\lambda)|$, *где d — диаметр графа.*

Доказательство. Выберем такую вершину a, в которой f имеет максимальное абсолютное значение, то есть $|f(a)| = \max_{x \in V(G)} |f(x)|$. Из утверждения 18 имеем $\sum_{d(y,a)=t} f(y) = P_t(\lambda) f(a)$, откуда получаем: $|\{y \mid d(y,a) = t, f(y) \neq 0\}| \geq |P_t(\lambda)|$, что и требовалось доказать. □

Рассмотрим совершенные раскраски f_1 и f_2 дистанционно-регулярного графа G в два цвета 0 и 1 с одинаковой матрицей параметров. Тогда их разность $f_1 - f_2$ является собственной функцией с некоторым собственным числом λ. Количество вершин, в которых раскраски f_1 и f_2 отличаются можно оценить из утверждения 19: $|\mathrm{supp}(f_1 - f_2)| \geq \sum_{t=0}^{d} |P_t(\lambda)|$.

Подробный обзор нижних оценок для мощности носителей собственных функций графов имеется в [91].

Определение 18. *Функция $u : V(G) \to \{0, \pm 1\}$ называется шаровым битрейдом в графе G если для любого шара $B(x)$, $x \in V(G)$, радиуса 1 выполняется*
$\begin{cases} |B(x) \cap u^{-1}(1)| = 1, \\ |B(x) \cap u^{-1}(-1)| = 1, \end{cases}$ *или* $u(B(x)) = \{0\}$.

Иными словами, функция принимает значения 0 и ± 1 и при этом либо принимает ровно по одному значению 1 и -1 в шаре радиуса 1, либо нулевая в этом шаре. Разность характеристических функций двух 1-совершенных кодов является битрейдом. Нетрудно видеть, что битрейд — собственная функция с собственным значением -1. По утверждению 19 имеем $|\mathrm{supp}(u)| \geq \sum_{t=0}^{d} |P_t(-1)|$, где d — диаметр графа.

Пусть A_t — множество вершин, находящихся на расстоянии t от некоторой фиксированной вершины x_0 дистанционно-регулярного графа G.

Утверждение 20. *Пусть f_1, f_2 — собственные функции дистанционно-регулярного графа G диаметра d с одинаковым собственным числом λ, $P_d(\lambda) \neq 0$. Если функции f_1 и f_2 совпадают на множестве $A_t \cup A_{t-1}$, где $t < d/2$, то $f_1|_{A_i} = f_2|_{A_i}$ при $i < t$.*

Доказательство. Пусть $x' \in A_i$ и $f_1(x') \neq f_2(x')$. A'_d — множество вершин, находящихся на расстоянии d от некоторой фиксированной вершины x'. Из неравенства треугольника следует, что $A'_d \cap A_i = \emptyset$ при $i \leq t$. Из условия $P_d(\lambda) \neq 0$ и утверждения 18 следует, что $\sum_{x \in A'_d} f_1(x) \neq \sum_{x \in A'_d} f_2(x)$.

Рассмотрим функцию f_3, заданную равенством

$$f_3(x) = \begin{cases} f_1(x), & x \in A_i, i \le t \\ f_2(x), & x \in A_i, i > t. \end{cases}$$

Поскольку функции f_1 и f_2 совпадают на множестве $A_t \cup A_{t-1}$, f_3 является собственной функцией с собственным числом λ и из утверждения 18 следует, что

$$\sum_{x \in A'_d} f_3(x) = P_d(\lambda) f_3(x') = P_d(\lambda) f_1(x') = \sum_{x \in A'_d} f_1(x).$$

Но по построению $f_3|_{A'_d} = f_2|_{A'_d}$. Получили противоречие. □

В частности, для булева гиперкуба Q_2^n диаметр равняется n, собственные числа $\lambda_k = n - 2k$, $k = 0, \ldots, n$ и $P_d(\lambda_k) = (-1)^{k+1}$ (см. раздел 11.2).

Следствие 14. *Если $P_d(-1) \neq 0$, то носитель шарового битрейда имеет диаметр меньше $\lceil d/2 \rceil - 2$.*

Обозначим $s_t = |A_t|$. Поскольку тождественно единичная функция является собственной функцией графа с собственным числом r (степень вершин графа), то из утверждения 18 имеем $s_t = P_t(r)$.

Утверждение 21. *Пусть λ — собственное число дистанционно-регулярного графа G диаметра d и $z_t(\lambda) = P_t(\lambda)/s_t$, $t = 0, \ldots, d$. Тогда вектор $z(\lambda) = (z_0(\lambda), \ldots, z_d(\lambda))$ является собственным вектором матрицы параметров $S[G]$ дистанционно-регулярного графа G с собственным числом λ.*

Доказательство. Рассмотрим некоторую собственную функцию f графа G с собственным числом λ. По определению собственной функции для произвольной вершины $x \in A_t$ имеем равенство

$$\lambda f(x) = \sum_{y: y \in A_{t-1}, d(x,y)=1} f(y) + \sum_{y: y \in A_t, d(x,y)=1} f(y) + \sum_{y: y \in A_{t+1}, d(x,y)=1} f(y). \tag{9}$$

Просуммируем обе стороны равенства по всем вершинам $x \in A_t$. Из дистанционной регулярности графа G следует, что каждая вершина $y \in A_{t-1}$ входит в сумму с одинаковой кратностью $\frac{c_t|A_t|}{|A_{t-1}|}$. Имеем равенство $\sum\limits_{x \in A_t} \sum\limits_{y: y \in A_{t-1}, d(x,y)=1} f(y) = \frac{c_t|A_t|}{|A_{t-1}|} \sum\limits_{y \in A_{t-1}} f(y)$. Аналогичным образом преобразуя другие слагаемые и применяя утверждение 18, получаем равенство

$$\lambda P_t(\lambda) = \frac{c_t|A_t|P_{t-1}(\lambda)}{|A_{t-1}|} + \frac{a_t|A_t|P_t(\lambda)}{|A_t|} + \frac{b_t|A_t|P_{t+1}(\lambda)}{|A_{t+1}|},$$

которое эквивалентно требуемому равенству $\lambda z_t(\lambda) = c_t z_{t-1}(\lambda) + a_t z_t(\lambda) + b_t z_{t+1}(\lambda)$. □

Замечание 8. Поскольку граф G диаметра d имеет не менее $d+1$ различных собственных чисел (см. задачу 14), матрица $S[G]$ имеет $d+1$ различных собственных чисел и множества собственных чисел графа G и матрицы $S[G]$ совпадают.

Следствие 15. *Пусть $\bar{z}^\lambda(x) = z_t(\lambda)$, если $x \in A_t$. Тогда $\bar{z}^\lambda$ — собственная функция графа G с собственным числом λ.*

Доказательство. Для функции $f = \bar{z}^\lambda$ уравнение $\lambda z_t(\lambda) = c_t z_{t-1}(\lambda) + a_t z_t(\lambda) + b_t z_{t+1}(\lambda)$ эквивалентно равенству (9), которое совпадает с определением собственной функции. □

Следствие 16 (ортогональность многочленов Кравчука)**.** *Введём обозначение $\widetilde{z}_t(\lambda) = \sqrt{s_t} z_t(\lambda) = P_t(\lambda)/\sqrt{s_t}$. Если $\lambda_1 \neq \lambda_2$ — собственные числа дистанционно-регулярного графа G, то вектора $\widetilde{z}(\lambda_1)$ и $\widetilde{z}(\lambda_2)$ ортогональны.*

Доказательство. Из ортогональности собственных функций $\bar{z}^{\lambda_1}$ и $\bar{z}^{\lambda_2}$ графа G с различными собственными числами имеем равенство

$$0 = \sum_x \bar{z}^{\lambda_1}(x)\bar{z}^{\lambda_2}(x) = \sum_{t=0}^{d} s_t (P_t(\lambda_1)/s_t)(P_t(\lambda_2)/s_t) = \sum_{t=0}^{d} \widetilde{z}_t(\lambda_1)\widetilde{z}_t(\lambda_2).$$

□

4.5 Полностью регулярные коды

Определение 19. *Подмножество вершин графа называется полностью регулярным кодом, если дистанционная раскраска относительно него является совершенной раскраской*[14].

В этом случае код является нулевым цветом раскраски, вершины на расстоянии 1 от кода — первым цветом и так далее. 1-Совершенный код в любом регулярном графе является полностью регулярным по своему определению. Нетрудно показать, что в дистанционно-регулярном графе любой совершенный код с произвольным кодовым расстоянием является полностью регулярным.

Рассмотрим некоторый граф G и вершину $x_0 \in V(G)$. Через A_i будем обозначать множество вершин на расстоянии i от вершины x_0. Пусть C — некоторый код и $|A_i \cap C|$ — вес его пересечения с i-ым слоем A_i. Тогда весовым распределением (спектром) кода (относительно вершины x_0, $A_0 = \{x_0\}$) называется весовое распределение его характеристической функции, т. е. набор $[|A_1 \cap C|, |A_2 \cap C|, \ldots, |A_d \cap C|]$.

В дистанционно-регулярных графах по теореме Шапиро–Злотника–Мартина весовое распределение полностью регулярных кодов зависит

[14] Алгебраические аспекты теории полностью регулярных кодов изложены в [54].

только от параметров порождаемой ими раскраски и цвета "нулевой" вершины, относительно которой рассматривается дистанционное расслоение. Так что у всех совершенных кодов в дистанционно-регулярном графе, с одинаковым кодовым расстоянием и содержащих "нулевую" вершину, весовое распределение одинаковое.

Пусть G — дистанционно-регулярный граф, а C — код в G. Пусть $C_t \neq \varnothing$, $t = 0, \ldots, d$, — множество вершин графа на расстоянии t от кода C. Число d называется радиусом покрытия кода C.

Теорема 8. *Код C в дистанционно-регулярном графе G является полностью регулярным тогда и только тогда, когда для любого t и $i \geq t$ каждая вершина $x \in C_t$ видит на расстоянии i одинаковое число вершин из C.*

Доказательство. ($\Rightarrow$) Следует из теоремы Шапиро–Злотника–Мартина.

($\Leftarrow$) Из матричного уравнения совершенной раскраски (утверждение 6) следует, что для любого j достаточно доказать равенство

$$M\chi_{C_j} = \sum_{i=0}^{d} s_{ji}\chi_{C_i} \tag{10}$$

с некоторыми коэффициентами s_{ji}. Из условия имеем, что величина $M_i\chi_C(x)$ зависит только от t, где $x \in C_t$. Таким образом, для любого i, $i = 0, \ldots, d$, имеем равенство

$$M_i\chi_C = \sum_{j=0}^{d} p_{ji}\chi_{C_j}.$$

По определению C_t имеем $p_{ti} = 0$ при $t > i$ и $p_{tt} > 0$. Соотношение (10) выполнено при $t = 0$ по условию, предположим оно доказано при $j < t$. Тогда

$$M_tM\chi_C = MM_t\chi_C = \sum_{j=0}^{t} p_{jt}M\chi_{C_j} = \sum_{j=0}^{t-1} p_{jt}\left(\sum_{i=0}^{d} s_{ji}\chi_{C_i}\right) + p_{tt}M\chi_{C_t}. \tag{11}$$

Из равенства (7) для дистанционно регулярного графа имеем

$$M_tM\chi_C = a_tM_t\chi_C + b_{t-1}M_{t-1}\chi_C + c_{t+1}M_{t+1}\chi_C.$$

Поэтому

$$M_tM\chi_C = \sum_{i=0}^{d} q_{ti}\chi_{C_i},$$

для некоторых коэффициентов q_{ti}. Из (11) и последнего равенства следует равенство (10) при $j = t$. Таким образом шаг индукции доказан. $\square$

Пример 12. Рассмотрим гиперкуб Q_q^n. Множество $C = V(Q_q^k) \times \{a\}$ является k-мерной гранью гиперкуба Q_q^n. Тогда произвольная грань гиперкуба размерности k является полностью регулярным кодом с матрицей параметров $S = S[Q_q^{n-k}]$.

Пример 13. Примером полностью регулярных кодов являются коды Препараты [66], которые состоят из вершин первого цвета в совершенной раскраске булева n-куба с матрицей параметров $\begin{pmatrix} 0 & n & 0 & 0 \\ 1 & 0 & n-1 & 0 \\ 0 & 2 & n-3 & 1 \\ 0 & 0 & n & 0 \end{pmatrix}$. Коды Препараты существуют в булевых гиперкубах размерности $n = 2^{2t} - 1$, где t — натуральное.

Утверждение 22. *Пусть G — дистанционно-регулярный граф, а C — полностью регулярный код в G с радиусом покрытия d. Тогда если код C является линейной комбинацией некоторого набора собственных функций графа G, то и для любого t, $t \leq d$, код C_t является линейной комбинацией тех же собственных функций.*

Доказательство утверждения 22аналогично доказательству утверждения 8.

Пусть G — регулярный граф и $C \subset V(G)$ — полностью регулярный код. Рассмотрим расслоение вершин графа по расстоянию от кода C: $C_j = \{x \in V(G) \mid \min_{y \in C} d(x, y) = j\}$. Ясно, что $C_0 = C$. По определению полностью регулярного кода C_j — множество вершин j-го цвета в некоторой совершенной раскраске h с матрицей параметров S_C. Пусть $f : V(G) \to \{1, \ldots, k\}$ — произвольная совершенная раскраска графа G. Будем называть весовым распределением раскраски f относительно кода C наборы чисел $w_0 = (|C_0 \cup f^{-1}(1)|, \ldots, |C_0 \cup f^{-1}(k)|), \ldots, w_j = (|C_j \cup f^{-1}(1)|, \ldots, |C_j \cup f^{-1}(k)|), \ldots$.

Теорема 9 (Кротов [55])**.** *Весовое распределение $w_0, \ldots, w_j, \ldots$ совершенной раскраски f графа G относительно полностью регулярного кода $C \subset V(G)$ можно восстановить из w_0.*

Доказательство. Пусть M — матрица смежности графа G и S_f матрица параметров раскраски f. Тогда из утверждения 6 и определения полностью регулярного кода имеем равенства $MF = FS_f$ и $MH = HS_C$, где $H_{ij} = 1$ только если i-я вершина графа G находится на расстоянии j от кода C.

Рассмотрим матрицу $X = F^{\mathrm{T}}H$. По построению её столбцами являются наборы w_j. Имеем равенства $S_f^{\mathrm{T}}F^{\mathrm{T}}H = F^{\mathrm{T}}M^{\mathrm{T}}H = F^{\mathrm{T}}MH = F^{\mathrm{T}}HS_C$. По условию нам известен первый (с расстоянием 0 от кода C) столбец матрицы X.

Поскольку S_C — матрица дистанционной раскраски, она трёхдиагональна $S_C = \begin{pmatrix} a_0 & b_0 & 0 & 0 & \dots & 0 \\ c_1 & a_1 & b_1 & 0 & \dots & 0 \\ 0 & c_2 & a_2 & b_2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & c_d & a_d \end{pmatrix}$, где d — максимально возможное расстояние от кода C до произвольной вершины в графе G. Причём $c_i \neq 0$ и $b_i \neq 0$ для всех i поскольку вершины соседних слоёв в расслоении по расстоянию от кода видят друг друга. Восстановим последовательно все столбцы $x_1, x_2, \dots, x_d$ матрицы X. Из уравнения $XS_C = S_f^{\mathrm{T}} X$ имеем $a_0x_1 + c_1x_2 = S_f^{\mathrm{T}}x_1$, т. е. $x_2 = (S_f^{\mathrm{T}}x_1 - a_0x_1)/c_1$. Аналогично, для столбца x_i, $i = 1, \dots, d-1$, имеем равенство $b_{i-1}x_{i-1} + a_ix_i + c_{i+1}x_{i+1} = S_f^{\mathrm{T}}x_i$. Из этих равенств можно последовательно вычислить все столбцы матрицы X, а значит, восстановить весовое распределение раскраски f относительно кода C. □

Для кода $C \subset V(G)$ определим $s^*(C)$ так, что $s^*(C) + 1$ минимальное количество собственных функций графа G, линейной комбинацией которых является характеристическая функция χ_C.

Теорема 10 ([15]). *Пусть G — дистанционно-регулярный граф диаметра d, тогда*
(1) для любого кода C справедливо равенство $\mathrm{diam}(C) + s^*(C) \geq d$;
(2) если $\mathrm{diam}(C) + s^*(C) = d$, *то код C — полностью регулярный.*

Доказательство. Пусть M_t — матрица смежности графа G по расстоянию t. Рассмотрим матрицу B размера $(d+1) \times V(G)$, строками которой являются вектора $M_t\chi_C$, $t = 0, \dots, d$. Пусть $C_0, \dots, C_d$ дистанционное расслоение вершин графа G относительно кода C.

(1) Из определения дистанционно-регулярного графа следует, что ранг матрицы B равен $s^*(C)+1$. Из определения диаметра кода следует, что в столбцах матрицы B, соответствующих вершинам из C_i ненулевыми являются только позиции с iой по $\mathrm{diam}(C) + i$. Поэтому столбцевой ранг матрицы B не меньше $d + 1 - \mathrm{diam}(C)$.

(2) Если $\mathrm{diam}(C) + s^*(C) = d$, то ранг матрицы B равняется числу различных носителей столбцов. Отсюда заключаем, что столбцы с одинаковыми носителями коллинеарны. Поскольку сумма элементов в каждом столбце равна $|V(G)|$, то столбцы с одинаковыми носителями совпадают. По теореме 8 это условие эквивалентно определению полностью регулярного кода. □

4.6 Дельсартовы клики II

Пусть λ — собственное число дистанционно-регулярного графа G диаметра d. Пусть $u_1, \dots, u_m$ — ортонормированный базис собственного подпространства X_λ графа G. Рассмотрим вектора $w^\lambda(x) = (u_1(x), \dots, u_m(x))$,

где $x \in V(G)$. Их скалярные произведения являются элементами матрицы E_λ[15].

Из следствия 4 и замечания 5 имеем

Следствие 17. *Если G — дистанционно-регулярный граф диаметра d, то матрицы E_λ можно представить в виде линейных комбинаций матриц смежности по расстояниям $0, \dots, d$ графа G.*

Следствие 18. *Если G — дистанционно-регулярный граф диаметра d, то элемент $E_\lambda(x, y)$ зависит только от расстояния между вершинами x и y в графе G.*

Определим вектор $\gamma(\lambda) = (\gamma_0, \dots, \gamma_d)$, где $\gamma_t = E_\lambda(x, y)$ при $d_G(x, y) = t$. Зафиксируем произвольную вершину $x_0 \in V(G)$ в качестве нулевой и дистанционное расслоение $[A_0, \dots, A_d]$ графа G относительно неё. Напомним обозначение из раздела 4.4: $z_t(\lambda) = P_t(\lambda)/s_t$, $t = 0, \dots, d$, где $s_t = |A_t|$.

Утверждение 23. *Пусть G — дистанционно-регулярный граф диаметра d. Тогда вектора $z(\lambda)$ и $\gamma(\lambda)$ коллинеарны.*

Доказательство. Рассмотрим собственную функцию u_i, $i = 1, \dots, m$, графа G с собственным числом λ. По определению собственной функции для произвольной вершины $x \in A_t$ имеем равенство

$$\lambda u_i(x) = \sum_{y: y \in A_{t-1}, d(x,y)=1} u_i(y) + \sum_{y: y \in A_t, d(x,y)=1} u_i(y) + \sum_{y: y \in A_{t+1}, d(x,y)=1} u_i(y).$$

Тогда

$$\lambda w^\lambda(x) = \sum_{y: y \in A_{t-1}, d(x,y)=1} w^\lambda(y) + \sum_{y: y \in A_t, d(x,y)=1} w^\lambda(y) + \sum_{y: y \in A_{t+1}, d(x,y)=1} w^\lambda(y). \tag{12}$$

Скалярно перемножив равенство (12) на вектор $w^\lambda(x_0)$ получаем равенство

$$\lambda\gamma_t(\lambda) = c_t\gamma_{t-1}(\lambda) + a_t\gamma_t(\lambda) + b_t\gamma_{t+1}(\lambda),$$

где a_t, c_t, b_t — коэффициенты дистанционно-регулярного графа G.

Тогда вектор $\gamma(\lambda)$ является собственным вектором матрицы параметров $S[G]$ дистанционно-регулярного графа G с собственным числом λ. По утверждению 21 вектор $z(\lambda)$ содержится в том же собственном подпространстве матрицы $S[G]$, по замечанию 8 оно одномерно. □

Докажем аналог теоремы 4 для дистанционно-регулярного графа.

[15] E_λ — матрица, построенная в разделе 2.3 по собственному подпространству X_λ.

Теорема 11 (о дельсартовой клике [38]). *Мощность клики в дистанционно r-регулярном графе G не превышает $1 - \frac{r}{\lambda_{min}}$, где λ_{min} — минимальное собственное число графа G.*

Доказательство. Пусть $u_1, \ldots, u_m$ — ортонормированный базис собственного подпространства $X_{\lambda_{min}}$. Рассмотрим вектора $w(x) = (u_1(x), \ldots, u_m(x))$, где $x \in V(G)$. Их скалярные произведения являются элементами матрицы $E_{\lambda_{min}}$. По следствию 18 их скалярные произведения одинаковы для всех пар соседних вершин x и y, а также для пар совпадающих вершин. Пусть $(w(x), w(y)) = \beta$ для любых соседних вершин $x, y \in V(G)$ и $(w(x), w(x)) = \alpha$ для любой вершины $x \in V(G)$.

Из определения собственной функции имеем равенство $\sum\limits_{y \in S_1(x)} u_i(y) = \lambda_{min} u_i(x)$, т. е. $\sum\limits_{y \in S_1(x)} w(y) = \lambda_{min} w(x)$. Скалярно умножая предыдущее равенство на $w(x)$, имеем соотношение $r\beta = \lambda_{min}\alpha$.

Пусть $C \subset V(G)$ клика в графе G. Рассмотрим матрицу Грама W размера $|C| \times |C|$, элементами которой являются $(w(x), w(y))$, $x, y \in C$. Имеем

$$W = \begin{pmatrix} \alpha & \beta & \beta & \ldots & \beta \\ \beta & \alpha & \beta & \ldots & \beta \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \beta & \ldots & \ldots & \beta & \alpha \end{pmatrix}.$$

Матрица Грама неотрицательно определена, поэтому $(W\overline{1}, \overline{1}) \geq 0$, следовательно, $\alpha + (|C| - 1)\beta \geq 0$. Поскольку минимальное собственное число λ_{min} отрицательное (см. задачу 1), отсюда и из равенства $r\beta = \lambda_{min}\alpha$ имеем $|C| \leq 1 - \frac{r}{\lambda_{min}}$. □

Вспомним, что клика мощности $1 - \frac{r}{\lambda_{\min}}$ в r-регулярном графе G называется дельсартовой.

Теорема 12 ([38]). *Любая дельсартова клика в дистанционно-регулярном графе диаметра d является полностью регулярным кодом с радиусом покрытия $d - 1$.*

Доказательство. Пусть C — дельсартова клика и C_t — множество вершин на расстоянии t от $C = C_0$. По теореме 8 достаточно проверить, что для любого t и $i \geq t$ каждая вершина $x \in C_t$ видит одинаковое число вершин из C на расстоянии i. Ясно, что достаточно проверить число вершин только на расстоянии t, поскольку из определения клики расстояние может быть только t или $t + 1$.

Далее будем использовать обозначения из доказательства теоремы 11. Из доказательства теоремы 11 видно, что для дельсартовой клики верно равенство $\alpha + (|C| - 1)\beta = 0$, т. е. $(\sum\limits_{x \in C} w(x), \sum\limits_{x \in C} w(x)) = 0$. Следовательно, $\sum\limits_{x \in C} w(x) = 0$.

По определению $E_{\lambda_{min}}(x,y) = (w(x), w(y))$. Из следствия 18 имеем, что $(w(x), w(y))$ зависит только от расстояния между вершинами x и y. Пусть $(w(x), w(y)) = \gamma_t$ при $d(x,y) = t$. Рассмотрим $y \in C_t$. Имеем равенство

$$0 = (w(y), \sum_{x \in C} w(x)) = (w(y), \sum_{x \in C, d(x,y)=t} w(x)) + (w(y), \sum_{x \in C, d(x,y)=t+1} w(x)) =$$

$$= \gamma_t k_t(y) + \gamma_{t+1}(|C| - k_t(y)) = (\gamma_t - \gamma_{t+1})k_t(y) + \gamma_{t+1}|C|,$$

где $k_t(y) = |\{x \in C, d(x,y) = t\}|$. Если $\gamma_t - \gamma_{t+1} = 0$, то $\gamma_{t+1} = 0$ и далее по индукции получим $\alpha = 0$. Поэтому $\gamma_t - \gamma_{t+1} \neq 0$ при $t = 1, \ldots, d$. Тогда $k_t(y) = \frac{\gamma_{t+1}|C|}{\gamma_{t+1} - \gamma_t}$ не зависит от y.

Кроме того, в графе нет вершин на расстоянии $d+1$. Поэтому $\gamma_d k_d(y) = 0$. □

Следствие 19. *Пусть C — дельсартова клика в дистанционно-регулярном графе G с минимальным собственным числом λ_{min}. Тогда функция χ_C ортогональна собственному подпространству $X_{\lambda_{min}}$ графа G.*

Доказательство. Поскольку $u_1, \ldots, u_m$ — ортонормированный базис собственного подпространства $X_{\lambda_{min}}$, имеем $(\chi_C, u_i) = \sum\limits_{x \in C} (w(x))_i$. Тогда требуемое эквивалентно равенству $\sum\limits_{x \in C} w(x) = \bar{0}$. □

4.7 Теорема о восстановлении совершенной раскраски по среднем слою

Определение 20. *Граф G диаметра d называется антиподальным, если для любой вершины $x \in V(G)$ найдётся единственная (противоположная) вершина $y \in V(G)$ на максимальном расстоянии d от x.*

Например, булев n-куб является антиподальным поскольку на расстоянии n от вершины x находится единственная вершина $x \oplus \bar{1}$. Отметим, что q-ичные гиперкубы при $q > 2$ не являются антиподальными графами.

Утверждение 24. *Для совершенной раскраски в антиподальном дистанционно-регулярном графе цвет любой вершины однозначно определяется цветом противоположной вершины.*

Доказательство. По теореме Шапиро–Злотника–Мартина совершенная раскраска вершин графа остаётся совершенной и в графе по расстоянию равному диаметру d графа. В антиподальном графе на расстоянии d от каждой вершины имеется ровно одна вершина, т. е. граф по расстоянию d является 1-регулярным и цвет вершины определяется цветом её соседа. □

Теорема 13 (о восстановлении раскраски по среднем слою [103]). *Пусть n — нечётное, f_1 и f_2 — совершенные раскраски булева гиперкуба Q_2^n с одинаковыми параметрами и для любой вершины $x \in Q_2^n$ веса $\mathrm{wt}(x) = \frac{n-1}{2}$ (или $\mathrm{wt}(x) = \frac{n+1}{2}$), имеем $f_1(x) = f_2(x)$. Тогда $f_1 \equiv f_2$.*

Доказательство. Вершины, противоположные вершинам веса $\mathrm{wt}(x) = \frac{n-1}{2}$, имеют вес $\frac{n+1}{2}$. Поэтому из утверждения 24 следует, что между цветами найдётся такое соответствие φ, $f_1(x \oplus \bar{1}) = \varphi(f_1(x)) = \varphi(f_2(x)) = f_2(x \oplus \bar{1})$, где $i = 1, 2$, $\mathrm{wt}(x) = \frac{n+1}{2}$ (или $\mathrm{wt}(x) = \frac{n-1}{2}$).

Рассмотрим раскраску $f(x) = \begin{cases} f_1(x), & \mathrm{wt}(x) \le \frac{n-1}{2} \\ f_2(x), & \mathrm{wt}(x) \ge \frac{n-1}{2} \end{cases}$. Раскраска f является совершенной с теми же параметрами, что f_1 и f_2, так как в любом шаре радиуса 1 она совпадает с одной из них. Из утверждения 24 имеем $f_1(x) = f(x) = \varphi(f(x \oplus \bar{1})) = \varphi(f_2(x \oplus \bar{1})) = f_2(x)$ и при $\mathrm{wt}(x) \le \frac{n-1}{2}$. Следовательно, $f_2(x) = f_1(x)$. □

Определение 21. *Тестовое множество для функции из некоторого класса есть подмножество, по значениям функции на котором можно восстановить функцию полностью.*

Здесь речь идёт только про "безусловное" тестовое множество, когда тестовое множество не зависит от функции. Иногда бывает полезно рассматривать "условное" тестовое множество, когда выбор следующей тестовой точки зависит от значения функции в предыдущих тестовых точках.

Таким образом, средний слой является тестовым множеством для совершенных раскрасок булева n-куба. В частности, из теоремы 13 можно получить верхнюю оценку на число 1-совершенных кодов в булевом n-кубе.

Задача 25. Докажите, что код в дистанционно-регулярном графе является полностью регулярным тогда и только тогда, когда весовое распределение кода относительно вершины зависит только от расстояния от этой вершины до кода.

Задача 26. Докажите, что для многочленов P_t в дистанционно-регулярном графе G справедливо равенство $(x - b_0)\sum\limits_{t=0}^{s} P_t(x) = c_{s+1}P_{s+1}(x) - b_s P_s(x)$, где $s+1$ не превосходит диаметр графа G.

Задача 27. Докажите равенство
$2n\sum\limits_{t=0}^{s}(-1)^{t+1}\binom{n}{t} = (-1)^{s+1}\left((s+1)\binom{n}{s+1} + (n-s)\binom{n}{s}\right)$.

Задача 28. Докажите, что если граф, являющийся дополнением сильно регулярного графа связен, то он сильно регулярен.

Задача 29. Опишите все графы с ровно двумя собственными числами матрицы смежности.

Задача 30. Докажите, что матрица смежности M_i графа по любому расстоянию является многочленом от его матрицы смежности по расстоянию 1, то граф является дистанционно-регулярным.

Задача 31. Докажите, что для матрицы параметров $S[G]$ любого дистанционно-регулярного графа G последовательность b_i убывает (нестрого), а последовательность c_i возрастает (нестрого).

Задача 32. Докажите, что мощность клики в дистанционно-регулярном графе G не превышает $1 - \frac{r}{\lambda}$, где λ — минимальное собственное число графа G, r — степень вершины.

Задача 33. Докажите, что в сильно регулярном графе G характеристическая функция клики мощности $1-\frac{r}{\lambda}$, где λ — минимальное собственное число графа G и r — степень вершины, является совершенной раскраской графа G.

Задача 34. Докажите, что для любого дистанционно-регулярного графа справедливо равенство $|A_2|P_1(-1) = |A_1|P_2(-1)$.

Задача 35. Докажите, что для любого дистанционно-регулярного графа число положительных значений собственной функции с собственным числом α не меньше, чем $\sum\limits_{t=0}^{d} \max\{P_t(\alpha), 0\}$.

Задача 36. Пусть C — полностью регулярный код в дистанционно-регулярном графе. Докажите, что матрица параметров дистанционной раскраски относительно кода C имеет собственные числа, совпадающие с собственными числами минимального набора собственных подпространств, содержащих функцию χ_C.

Задача 37. Пусть f — совершенная раскраска булева куба. Грани булева куба, у которых совпадает множество фиксированых координат, но различны все фиксированные значения координат, называются противоположными. Докажите, что если у двух граней булева гиперкуба совпадает цветовой состав (т. е. равное число вершин любого цвета в обоих гранях), то и цветовой состав противоположных им граней тоже совпадает.

Задача 38. Пусть $C \subset Q_2^n$ (n – нечётное) — полностью регулярный код. Докажите, что код C полностью восстанавливается по множеству своих вершин веса $\frac{n+1}{2}, \frac{n+1}{2}+1, \ldots, \frac{n+1}{2}+r$, где r — радиус покрытия кода C, т. е. любая вершина булева гиперкуба находится на расстоянии r или менее от кода.

5 Декартовы произведения графов

5.1 Собственные функции декартова произведения графов

Напомним, что кронекеровым произведением матриц A размера $n_1 \times m_1$ на B размера $n_2 \times m_2$ называется матрица $A \otimes B$ размера $n_1 n_2 \times m_1 m_2$, состоящая из элементов $(A \otimes B)_{(i_1,i_2),(j_1,j_2)} = A_{i_1,j_1} B_{i_2,j_2}$. При подходящих размерах матриц A, B, C, D имеем равенства $(A \otimes B) \cdot (C \otimes D) = (AC) \otimes (BD)$ и $(A \otimes B) + (A \otimes D) = A \otimes (B + D)$.

Определение 22. *Декартовым произведением двух графов $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$ называется такой граф $G = G_1 \square G_2$, что $V(G) = V_1 \times V_2$, $E(G) = \{\{(v_1, v_2), (u_1, u_2)\} \mid \{v_1, u_1\} \in E_1 \ \& \ v_2 = u_2$ или $\{v_2, u_2\} \in E_2 \ \& \ v_1 = u_1\}$.*

Пусть $|V_1| = n$ и $|V_2| = m$. Тогда матрицу смежности M графа G можно выразить через кронекеровы произведения матриц смежности M_1 и M_2 графов G_1 и G_2 с единичными матрицами. При подходящей нумерации вершин графа G справедливо равенство $M = M_1 \otimes I_m + I_n \otimes M_2$. Таким образом, чтобы получить матрицу M, на место всех единиц в матрице M_1 нужно вставить I_m, а по главной диагонали нужно вставить матрицы M_2.

В частности, n-мерный q-ичный куб Q_q^n определяется как декартовое произведение кубов меньшей размерности, а именно $Q_q^n = Q_q^{n-1} \square Q_q$. Получаем следующее рекуррентное представление его матрицы смежности

$$M_n = \begin{pmatrix} M_{n-1} & I_{q^{n-1}} & \cdots & I_{q^{n-1}} \\ I_{q^{n-1}} & M_{n-1} & \cdots & I_{q^{n-1}} \\ \cdots & \cdots & \cdots & \cdots \\ I_{q^{n-1}} & I_{q^{n-1}} & \cdots & M_{n-1} \end{pmatrix}$$

Из определения декартова произведения графов следует, что подграф графа $G = G_1 \square G_2$, порождённый множеством вершин $V(G_1) \times \{y\}$ изоморфен графу G_1 для любой вершины $y \in V(G_2)$. Аналогично, граф $\{x\} \times V(G_2)$ изоморфен графу G_2.

Из определения декартова произведения графов для любой функции $f(x, y) : V(G) \to \mathbb{R}$ имеем равенство
$Mf(x, y) = \sum\limits_{x\prime \in S_1^1(x)} f(x\prime, y) + \sum\limits_{y\prime \in S_1^2(y)} f(x, y\prime)$,
где $S_1^1(x)$ и $S_1^2(y)$ — единичные сферы в графах G_1 и G_2 соответственно.

Утверждение 25 ([94]). *Пусть $f_1, \ldots, f_n$ — ортогональный базис из собственных функций графа G_1 с собственными числами $\alpha_1, \ldots, \alpha_n$; а $g_1, \ldots, g_m$ — ортогональный базис из собственных функций графа G_2 с собственными числами $\beta_1, \ldots, \beta_m$. Тогда $\{f_i \otimes g_j\}$ — ортогональный*

базис из собственных функций графа $G = G_1 \square G_2$ с собственными числами $\alpha_i + \beta_j$.

Доказательство. $M(f_i \otimes g_j) = (M_1 \otimes I_m) \cdot (f_i \otimes g_j) + (I_n \otimes M_2) \cdot (f_i \otimes g_j) = M_1 f_i \otimes g_j + f_i \otimes M_2 g_j = \alpha_i f_i \otimes g_j + \beta_j f_i \otimes g_j = (\alpha_i + \beta_j) f_i \otimes g_j$.

Теперь проверим ортогональность базиса. $(f_{i_1} \otimes g_{j_1}) \cdot ((f_{i_2})^T \otimes (g_{j_2})^T) = (f_{i_1} \cdot (f_{i_2})^T) \otimes g_{j_1} \cdot (g_{j_2})^T = 0$, если $i_1 \neq i_2$ или $j_1 \neq j_2$. Произведения $f_i \otimes g_j$ составляют базис, поскольку размерность пространства этих функций равна $|V(G)| = nm$.

Ниже те же вычисления проведены поэлементно.

$M(f_i \otimes g_j)(x, y) = M f_i(x) g_j(y) = \sum\limits_{x\prime \in S_1^1(x)} f_i(x\prime) g_j(y) + \sum\limits_{y\prime \in S_1^2(x)} f_i(x) g_j(y\prime) =$
$g_j(y) \sum\limits_{x\prime \in S_1^1(x)} f_i(x\prime) + f_i(x) \sum\limits_{y\prime \in S_1^2(y)} g_j(y\prime) = \alpha_i g_j(y) f_i(x) + \beta_j f_i(x) g_j(y) =$
$(\alpha_i + \beta_j) f_i(x) g_j(y)$

$\sum\limits_{(x,y) \in V(G)} f_{i_1}(x) g_{j_1}(y) \cdot f_{i_2}(x) g_{j_2}(y) = \sum\limits_x f_{i_1}(x) f_{i_2}(x) \sum\limits_y g_{j_1}(y) g_{j_2}(y).$ $\square$

Покажем, как из собственных функций декартова произведения графов и одного из сомножителей можно получить собственную функцию второго сомножителя.

Лемма 2 (о ϕ-проектировании, [94])**.** *Пусть $G = G_1 \square G_2$; $f(x, y)$ — собственная функция G с собственным числом λ; ϕ_0 — собственная функция графа G_2 с собственным числом α_0. Тогда $c_0(x) = \sum\limits_{y \in V(G_2)} f(x, y) \cdot \phi_0(y)$ — собственная функция графа G_1 с собственным числом $(\lambda - \alpha_0)$.*

Доказательство. Известно, что любой вектор можно включить в некоторый ортогональный базис, содержащий этот вектор. Поэтому без ограничения общности можно считать, что $\phi_0, \ldots, \phi_{m-1}$ — ортонормированный базис из собственных функций графа G_2 с собственными числами $\alpha_0, \ldots, \alpha_{m-1}$. Функцию f при любом фиксированном $x \in V(G_1)$ можно разложить по базису $f(x, y) = \sum\limits_{i=0}^{m-1} c_i(x) \phi_i(y)$, поскольку по определению декартова произведения, фиксируя x, мы получаем граф, изоморфный графу G_2. Таким образом, имеем $f = \sum\limits_{i=0}^{m-1} c_i \otimes \phi_i$ и $\sum\limits_{y \in V(G_2)} f(x, y) \phi_i(y) = c_i(x)$ в силу ортонормированности базиса.

Поскольку f собственная функция графа G, справедливо равенство

$$(M_1 \otimes I_m + I_n \otimes M_2) \left(\sum_{i=0}^{m-1} c_i \otimes \phi_i \right) = \lambda \left(\sum_{i=0}^{m-1} c_i \otimes \phi_i \right).$$

Поскольку ϕ_i, $i = 0, \ldots, m-1$, собственные функции графа G_2 получаем новое равенство

$$\sum_{i=0}^{m-1}(M_1c_i + \alpha_i c_i) \otimes \phi_i = \sum_{i=0}^{m-1} \lambda c_i \otimes \phi_i. \qquad (13)$$

Нетрудно видеть, что при скалярном умножении одного из сомножителей в декартовом произведении получаются следующие равенства

$$g(x)(h_1, h_2) = \sum_{y \in V(G_2)} g(x)h_1(y)h_2(y) = \sum_{y \in V(G_2)} (g \otimes h_1)(x, y) \cdot h_2(y).$$

Поэтому, умножая обе части равенства (13) скалярно на функцию ϕ_0 получаем равенство $M_1c_0 + \alpha_0 c_0 = \lambda c_0$. □

Пример 14. Рассмотрим граф Q_q, изоморфный клике на q вершинах. Собственными функциями графа Q_q являются

$\Phi_0 = (1, 1, 1, \ldots, 1)$ — собственная функция с собственным числом $q-1$,

и для любых $i, j \in \{1, \ldots, q\}$ $\Phi_{ij} = (0, \ldots, \underset{i}{1}, 0, \ldots, 0, \underset{j}{-1}, 0, \ldots, 0)$ — собственные функции с собственным числом -1. Среди перечисленных функций можно выбрать базис всего пространства, поэтому других собственных чисел у графа Q_q нет.

Рассмотрим некоторую собственную функцию f с собственным числом λ в гиперкубе $Q_q^{n+1} = Q_q^n \square Q_q$. Из леммы о ϕ-проектировании следует, что если просуммировать функцию f ортогонально гиперграни, т. е. взять $g(x_1, \ldots, x_n) = \sum\limits_{z \in Q_q} f(x_1, \ldots, x_n, z)$, то получится собственная функция гиперкуба Q_q^n с собственным числом $\lambda - q + 1$. А если взять разность функции f в двух гипергранях одного направления $g_{ij}(x_1, \ldots, x_n) = f(x_1, \ldots, x_n, i) - f(x_1, \ldots, x_n, j)$, то получится собственная функция гиперкуба Q_q^n с собственным числом $\lambda + 1$.

5.2 Раскраски декартова произведения графов

Рассмотрим способы построения совершенных раскрасок декартова произведения графов из совершенных раскрасок сомножителей.

Утверждение 26. *Пусть f_i — совершенная раскраска графа G_i в k_i цветов матрицей переметров S_i, $i = 1, 2$. Тогда $f_1 \times f_2$ — совершенная раскраска графа $G = G_1 \square G_2$ в $k_1 \cdot k_2$ цветов с матрицей параметров $S_1 \otimes I_{k_2} + I_{k_1} \otimes S_2$.*

Доказательство. Рассмотрим окрестность точки (x, y). Она состоит из точек (x, y'), $y' \in S_1^2(y)$ цветов $(f_1(x), f_2(y'))$ и из точек (x', y), $x' \in S_1^1(x)$ цветов $(f_1(x'), f_2(y))$, где наборы цветов $f_2(y')$ и $f_1(x')$ зависят только от цветов $f_2(y)$ и $f_1(x)$, т. е. от цвета вершины (x, y).

Вычислим матрицу параметров получившейся раскраски и независимо проверим, что раскраска является совершенной. Как указано ранее, матрица смежности графа $G_1 \square G_2$ имеет вид $M = M_1 \otimes I_{m_2} + I_{m_1} \otimes M_2$, где M_i — матрица смежности графа G_i на m_i вершинах, $i = 1, 2$. Пусть F_1 — матрица размера $m_1 \times k_1$, соответствующая совершенной раскраске графа G_1, а F_2 — матрица размера $m_2 \times k_2$, соответствующая совершенной раскраске графа G_2. Покажем, что матрица $F_1 \otimes F_2$, которая соответствует функции $f_1 \times f_2$ определяет совершенную раскраску с матрицей параметров $S = S_1 \otimes I_{k_2} + I_{k_1} \otimes S_2$, где S_1 и S_2 — матрицы параметров исходных раскрасок. Из утверждения 6 имеем $M_i F_i = F_i S_i$, $i = 1, 2$. Используя следующее равенство $(A_1 \otimes B_1)(A_2 \otimes B_2) = (A_1 A_2) \otimes (B_1 B_2)$ для кронекеровых произведений матриц подходящего размера, получим равенства

$$(M_1 \otimes I_{m_2} + I_{m_1} \otimes M_2)(F_1 \otimes F_2) = (F_1 S_1) \otimes F_2 + F_1 \otimes (F_2 S_2) = (F_1 \otimes F_2)(S_1 \otimes I_{k_2} + I_{k_1} \otimes S_2).$$

Таким образом, раскраска $f_1 \times f_2$ является совершенной по алгебраическому критерию совершенной раскраски (утверждение 6). □

Рассмотрим случай, когда f_2 — тривиальная раскраска в один цвет. Пусть f_1 — совершенная раскраска графа G_1 с матрицей параметров S. Тогда $f(x, y) = f_1(x)$ — совершенная раскраска графа $G_1 \square G_2$ с матрицей параметров $S + rI$, где r — степень G_2.

Утверждение 27. *Пусть $g : V(G) \to \{0, 1\}$ — совершенная раскраска графа G с матрицей параметров $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ и $h : V(H) \to \{0, 1\}$ — совершенная раскраска графа H с матрицей параметров $\begin{pmatrix} c & d \\ d & c \end{pmatrix}$. Тогда раскраска $f(x, y) = g(x) \oplus h(y)$, где $\oplus$ — сложение по модулю 2, является совершенной с матрицей параметров $\begin{pmatrix} a+c & b+d \\ b+d & a+c \end{pmatrix}$ в графе $G \square H$.*

Доказательство. Рассмотрим число соседей цвета 1 вершины (x, y). Если $g(x) = h(y) = 0$, то имеется b соседей $(g(x'), h(y))$ и d соседей $(g(x), h(y'))$ цвета 1. Если $g(x) = h(y) = 1$, то имеется b соседей $(g(x'), h(y)))$ и d соседей $(g(x), h(y'))$ цвета 1. Аналогично можно рассмотреть оставшиеся случаи. □

Рассмотрим декартово произведение $G_1 \square G_2$, в котором G_1 — r-регулярный граф, а G_2 — дистанционно-регулярный граф с матрицей параметров $S[G_2]$. Рассмотрим множество вершин $C = V(G_1) \times \{a\}$, $a \in G_2$.

Утверждение 28. *Дистанционная раскраска графа $G_1 \square G_2$ по расстоянию от кода C: $f(x, y) = d(y, a)$ является совершенной с матрицей параметров $S[G_2] + rI$. Таким образом, код C является полностью регулярным в графе $G_1 \square G_2$.*

Доказательство. Пусть вершина $y \in V(G_2)$ находится на расстоянии i от вершины a. По определению дистанционно-регулярного графа в графе G_2 она смежна с c_i, a_i, b_i вершинами на расстоянии $i-1, i, i+1$ от a соответственно. Тогда по определению декартова произведения для вершины (x, y) графа $G_1 \square G_2$ c_i соседей цвета $i-1$, b_i соседей цвета $i+1$ и $a_i + r$ соседей цвета i. $\square$

5.3 Существенные переменные и теорема Вегенера

Говорят, что функция многих переменных существенно зависит от некоторой переменной, если найдётся такая пара значений аргументов, отличающихся только в этой переменной, что функция принимает на них различные значения. В этом случае переменную называют существенной, в противном случае — несущественной. Раскраску декартова произведения графов $G = G_1 \square \cdots \square G_n$ можно рассматривать как функцию от n переменных. Вершинам графа G соответствуют наборы вершин графов $G_1, \ldots, G_n$ и значением i-ой переменной является номер вершины в графе G_i. Таким образом, для раскрасок декартова произведения графов можно рассмотреть вопрос существенной зависимости раскраски от переменных.

Раскраска булева куба $f : Q_2^n \to \{1, \ldots, k\}$ может быть рассмотрена как функция от n булевых переменных. Обозначим через $\eta(f)$ число существенных переменных раскраски f. Для каждой вершины $x \in Q_2^n$ можно определить число $c(x)$ соседних вершин, цвет которых отличен от цвета вершины x. Введём обозначение $c(f) = \max_x c(x)$.

Теорема 14 (Вегенер [100])**.** *Для любой раскраски f булева гиперкуба справедливо неравенство $\eta(f) \leq c(f) 2^{2c(f)-2}$.*

Доказательство. Вначале докажем по индукции следующее утверждение. Если в некотором непустом подграфе булева n-куба все степени вершин не меньше $r \leq n$, то число вершин в подграфе не меньше 2^r. При $n = 1$ утверждение очевидно. Докажем шаг индукции. Пусть утверждение верно для n-мерного куба. Рассмотрим множество вершин T в Q_2^{n+1}, степени вершин в котором не меньше r. Рассмотрим произвольное ребро, содержащееся в подграфе на множестве вершин T. Без ограничения общности считаем, что это ребро n-го направления. Следовательно, множества $T_0 = Q_2^n \square \{0\} \cap T$ и $T_1 = Q_2^n \square \{1\} \cap T$ непусты. Подграфы, на множествах вершин T_0 и T_1, имеют степени вершин не меньше $r-1$, поскольку любая вершина из T_0 смежна не более чем с одной вершиной из T_1 и наоборот. Тогда по предположению индукции имеем $|T| = |T_0| + |T_1| \geq 2 \cdot 2^{r-1}$.

Перейдём к доказательству теоремы. Без ограничения общности можно считать, что n-ая переменная раскраски f гиперкуба Q_2^n является существенной. Тогда найдётся "пёстро" раскрашенное ребро n-го направ-

ления $\{x, y\}$ в булевом гиперкубе. Т. е. инцидентные ему вершины имеют разные цвета: $f(x) = \alpha$ в подкубе $Q_2^{n-1}\square\{0\}$ и $f(y) = \beta \neq \alpha$ в подкубе $Q_2^{n-1}\square\{1\}$. Оценим количество соседних с ребром $\{x, y\}$ "пёстро" раскрашенных рёбер n-го направления. Не более чем $c(f) - 1$ вершин в $Q_2^n\square\{0\}$, смежных с вершиной x, имеют цвет отличный от α. Аналогично, не более чем $c(f) - 1$ вершин в $Q_2^n\square\{1\}$, смежных с вершиной y, имеют цвет отличный от β. Смежные с вершинами x и y вершины попарно соединены соседними с $\{x, y\}$ рёбрами n-го направления. Значит из $n-1$ рёбер n-го направления, соседних с ребром $\{x, y\}$, не менее $n-1-2(c(f)-1)$ рёбер раскрашены "пёстро". Рассмотрим подграф графа $Q_2^{n-1}\square\{0\}$, состоящий из вершин, которым инцидентны "пёстрые" рёбра n-го направления. Как мы показали выше, степени вершин этого подграфа не меньше $n - 2c(f) + 1$. Следовательно, число "пёстро" раскрашенных рёбер n-го и любого другого существенного направления не меньше $2^{n-2c(f)+1}$.

По определению величины $c(f)$ в булевом n-кубе не более $c(f)2^{n-1}$ "пёстро" раскрашенных рёбер. Поэтому $\eta(f)2^{n-2c(f)+1} \leq c(f)2^{n-1}$. $\square$

Следствие 20. *Для любых $c, b \in \mathbb{N}$ найдётся такое $n_0 \in \mathbb{N}$, что при $n > n_0$ любая совершенная раскраска булева n-куба с матрицей параметров $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$ имеет несущественные переменные.*

Доказательство. По определению совершенной раскраски $c(f) = \max\{c, b\}$. Таким образом, по теореме Вегенера число существенных переменных раскраски не превосходит константы $n_0 = \max\{c, b\}2^{2\max\{c,b\}-2}$. $\square$

Любую функцию, имеющую несущественную переменную, удобно рассматривать как тривиальное продолжение функции от меньшего числа переменных. Нетрудно видеть, что если совершенная раскраска булева гиперкуба с матрицей параметров $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$ имеет несущественную переменную, то её можно рассматривать как декартово произведение одноцветного ребра и совершенной раскраски с матрицей параметров $\begin{pmatrix} n-b-1 & b \\ c & n-c-1 \end{pmatrix}$. Проблема нахождения максимальной размерности n, при которой существует совершенная раскраска без несущественных переменных с матрицей параметров $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$ возникает при перечислении двуцветных совершенных раскрасок булевых гиперкубов.

6 Конструкции совершенных раскрасок

6.1 Склеивание цветов

В этом разделе мы рассмотрим полурешётку, которую образуют совершенные раскраски произвольного регулярного графа. Одна раскраска является разбиением другой, если каждый цвет первой раскраски является объединением (склеиванием) цветов второй раскраски. Таким образом, полурешётка совершенных раскрасок является подрешёткой разбиений множества вершин графа на подмножества (полурешётки произвольных раскрасок вершин графа в конечное число цветов). Ясно, что максимальным элементом этой полурешётки является "пёстрая"раскраска, когда каждая вершина графа раскрашена в свой цвет, а минимальным элементом в случае регулярного графа является раскраска всех вершин в один цвет.

Пусть S — матрица параметров некоторой совершенной раскраски размера $k \times k$. Рассмотрим $(0,1)$-матрицу $H = (h_{ij})$ размера $k \times m$, $m < k$, которая определяет операцию склеивания (объединения) исходных k цветов в m новых цветов: $h_{ij} = 1$ если, и только если i-ый цвет старой раскраски переходит в j-ый цвет в новой раскраске.

Утверждение 29 ([8]). *Склеивание H цветов совершенной раскраски с матрицей параметров S приводит к совершенной раскраске с матрицей параметров S' тогда и только тогда, когда $SH = HS'$.*

Доказательство. Пусть F — матрица совершенной раскраски (с матрицей параметров S) графа с матрицей смежности M. Тогда FH — матрица раскраски, полученной склеиванием цветов. Тогда из равенства $MF = FS$ и условия $SH = HS'$ имеем равенства $MFH = FSH = FHS'$. Из утверждения 6 следует, что склеивание является совершенной раскраской.

Наоборот, из равенств $MFH = FHS'$ и $MFH = FSH$, а также невырожденности матрицы F, получаем, что $SH = HS'$. □

Для произвольных, не обязательно совершенных, раскрасок f_1 и f_2 вершин некоторого графа определим раскраску $f_0 = f_1 \wedge f_2$ как раскраску в максимальное число цветов, которая получается склеиванием из раскраски f_1 и из раскраски f_2. Это операция взятия минимума двух разбиений в полурешётке.

Утверждение 30. *Если раскраски f_1 и f_2 совершенные, то раскраска $f_0 = f_1 \wedge f_2$ тоже совершенная.*

Доказательство. Пусть V_i — подпространство, порождённое столбцами матрицы f_i. По утверждению 7 V_i является инвариантным подпространством матрицы смежности графа, если и только если раскраска F_i совершенная. По определению операции склеивания имеем $V_0 \subset V_1 \cap V_2$.

Ясно, что пересечение инвариантых подпространств является инвариантным подпространством. Поэтому из максимальности f_0 следует, что $V_0 = V_1 \cap V_2$. □

Декартово произведение совершенно раскрашенных графов порождает совершенные раскраски в большое число цветов. Рассмотрим при каких условиях число цветов в совершенной раскраске можно сократить, т. е. объединить некоторые наборы цветов.

Определение 23. *Два цвета i и j совершенной раскраски называются эквивалентными, если i-ая и j-ая строки в матрице параметров раскраски совпадают, за возможным исключением i-ых и j-ых координат в каждой строке.*

Утверждение 31. *Отношение эквивалентности цветов совершенной раскраски удовлетворяет свойству транзитивности.*

Доказательство. Предположим, что первый цвет эквивалентен второму и третьему цвету в совершенной раскраске с матрицей параметров S. Тогда из определения эквивалентных цветов следует, что $s_{13} = s_{23}$ и $s_{12} = s_{32}$. Пусть n_i — число вершин цвета i. Тогда из равенства (1) имеем соотношения $n_1 s_{13} = n_3 s_{31}$, $n_2 s_{21} = n_1 s_{12}$ и $n_3 s_{32} = n_2 s_{23}$. Перемножив правые и левые части равенств и применив равенства $s_{13} = s_{23}$ и $s_{12} = s_{32}$, получаем $s_{21} = s_{31}$. Значит второй и третий цвета эквивалентны. □

Утверждение 32. *Пусть раскраска f' получена из совершенной раскраски f ругулярного графа обьединением пары эквивалентных цветов. Тогда f' — совершенная раскраска.*

Доказательство. В этом случае для доказательства равенства $SF = FS'$ достаточно убедиться, что $s_{ii} + s_{ij} = s_{jj} + s_{ji} = s'_{ii}$, где i — номер цвета в раскраске f', полученного объединением i-го и j-го цветов исходной раскраски f. □

Нетрудно видеть, что объединение пары или большего количества цветов из некоторого класса эвивалентности, сохраняет объединённый цвет в том же классе эквивалентности. Поэтому объединение любого набора эвивалентных цветов совершенной раскраски даёт совершенную раскраску.

6.2 Алгоритм Вейсфейлера—Лемана и индуцирование

Здесь мы рассмотрим алгоритм, позволяющий для любой раскраски графа найти её минимальное разбиение, которое уже является совершенной раскраской. Пусть имеется граф, раскрашенный в несколько цветов. Рассмотрим вершины некоторого фиксированного цвета. Разделим их на

группы, каждая из которых состоит из вершин с окрестностью одинакового цветового состава. Покрасим каждую группу в свой (новый) цвет. Проделаем такую операцию с вершинами каждого цвета. Процесс перекраски останавливается, если получена совершенная раскраска, т. е. никакой цвет не разделяется на группы. Иначе повторяем процедуру перекраски. Поскольку на каждом шаге алгоритма число цветов увеличивается, но не может превысить число вершин в графе, то в результате мы всегда придём к совершенной раскраске в конечном графе. Возможно, в итоге получится раскраска всех вершин в разные цвета. Этот процесс перекраски называется алгоритмом Вейсфейлера—Лемана[16] [111]. Заметим, что никакие две вершины, уже имеющие различные цвета, не могут в процессе выполнения алгоритма получить одинаковый цвет. Вариант алгоритма, когда изначально раскрашена только часть графа можно рассматривать как частный случай: нераскрашенные вершины будем считать вершинами ещё одного цвета.

Покажем, что алгоритм Вейсфейлера—Лемана даёт именно такое минимальное разбиение раскраски, которое является совершенной раскраской.

Теорема 15 (Визинг [113]). *Пусть $g : V(G) \to \{1, \dots, k\}$ — раскраска некоторого графа G. Пусть f такая совершенная раскраска, что любой цвет раскраски g получается склеиванием цветов раскраски f. Тогда совершенная раскраска, полученная в результате применения алгоритма Вейсфейлера—Лемана к раскраске g, не разбивает цвета раскраски f.*

Доказательство. Будем доказывать теорему по индукции. Пусть на i-ом шаге алгоритма все полученные цвета текущей раскраски получаются склеиванием цветов раскраски f. Покажем, что и на $(i+1)$-ом шаге это положение сохранится. База индукции верна по условию. Рассмотрим две вершины $x_1, x_2 \in f^{-1}(j)$ одинакового цвета в раскраске f. Тогда у них одинаковое окружение (т. е. раскраски сфер $S_1(x_1)$, $S_1(x_2)$) в раскраске f, а значит, по предположению индукции у них будет одинаковое окружение и в текущей раскраске. Тогда очередной шаг алгоритма Вейсфейлера—Лемана красит вершины x_1 и x_2 в один цвет. □

Из теоремы 15 Визинга и утверждения 30 следует, что в алгоритме Визинга результирующую совершенную раскраску можно записать в виде $g = \wedge_i f_i$, где операция взятия минимума применяется к множеству таких совершенных раскрасок f_i, из которых склеиванием можно получить исходную раскраску f. Действительно, по утверждению 30 g

[16] Иногда алгоритмом Вейсфейлера—Лемана для графа G называют аналогичную процедуру применённую к рёберному графу полного графа, в котором изначально рёбра, имеющиеся в графе G, покрашены в один цвет, а отсутствующие в графе G — в другой.

— совершенная раскраска, раскраску f можно получить из неё склеиванием и раскраску g можно получить склеиванием из любой f_i.

Алгоритм Вейсфейлера—Лемана можно применять для проверки, является ли множество A вершин графа цветом какой-либо совершенной раскраски. Достаточно применить алгоритм к раскраске в два цвета: в первый цвет красим вершины множества A и во второй — остальные. Если алгоритм на каком-то шаге разбивает вершины первого цвета, то из теоремы Визинга следует, что множество A не является цветом никакой совершенной раскраски. В противном случае обозначим полученную алгоритмом Вейсфейлера—Лемана совершенную раскраску через f_A. Имеем

Следствие 21. *Любая совершенная раскраска f с множеством A вершин первого цвета может быть получена из f_A разбиением других цветов.*

Определение 24. *Рассмотрим двудольный граф. Пусть одна доля графа раскрашена некоторым образом, а вторая не раскрашена. Тогда раскраска, полученная одним шагом алгоритма Вейсфейлера—Лемана, называется индуцированной.*

Утверждение 33 ([122])**.** *Если раскраска первой доли двудольного графа дополняется до совершенной раскраски графа, то индуцированная раскраска также является совершенной.*

Доказательство. Пусть раскраска первой доли двудольного графа дополняется до некоторой совершенной раскраски g всего графа. Если какой-то из цветов i раскраски g встречается в первой и во второй долях графа, то вершины цвета i в первой и во второй долях можно выделить в отдельные цвета и раскраска останется совершенной. Поэтому без ограничения общности можно считать, что в долях графа непересекающиеся наборы цветов раскраски g. Рассмотрим раскраску f, которая совпадает с g на первой доле графа и красит вторую долю в некий другой цвет. Цвета раскраски f из первой доли не расщепляются ни на каком шаге алгоритма Вейсфейлера—Лемана по теореме 15. Тогда цветовой состав окрестностей вершин из второй доли не изменяется. Следовательно, алгоритм Вейсфейлера—Лемана заканчивает работу после первого шага и даёт индуцированную раскраску. □

Заметим, что при индуцировании получается непересекающийся набор цветов в двух долях. Возможно в индуцированной раскраске некоторые цвета из разных долей можно объединить. Индуцирование является полезным методом сокращения перебора при поиске совершенных раскрасок двудольных графов, в частности, булева гиперкуба.

6.3 Накрытия

Наиболее эффективным методом, позволяющим переносить совершенные раскраски с одного графа на другой, является метод накрытий.

Определение 25. *Пусть G_1 и G_2 — регулярные графы одинаковой степени. Накрытием $\phi : V(G_1) \to V(G_2)$ называется такое отображение, что $\forall x \in V(G_1)$ $\phi(S_1^1(x)) = S_1^2(\phi(x))$, где $S_1^1(x)$ и $S_1^2(y)$ — сферы радиуса 1 с центрами в вершинах $x \in V(G_1)$ и $y \in V(G_2)$ в графах G_1 и G_2 соответственно.*

Из определения видно, что композиция двух накрытий является накрытием.

Утверждение 34. *Пусть $\phi : V(G_1) \to V(G_2)$ накрытие и $f : V(G_2) \to \{1, \ldots, k\}$ — совершенная раскраска графа G_2. Тогда $f \circ \phi : V(G_1) \to \{1, \ldots, k\}$ — совершенная раскраска графа G_1 с теми же параметрами.*

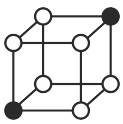
Доказательство. Пусть цвета вершин x_1, $x_2 \in V(G_1)$ совпадают, т. е. $f \circ \phi(x_1) = f \circ \phi(x_2)$. Тогда вершины $\phi(x_1)$ и $\phi(x_2)$ тоже имеют одинаковый цвет. Цветовое окружение вершин x_i и $\phi(x_i)$ при $i = 1, 2$ одинаковое, поскольку совпадают мультимножества цветов $f(\phi(S_1^1(x_i))) = f(S_1^2(\phi(x_i)))$. В силу того, что цвета вершин $\phi(x_1)$ и $\phi(x_2)$ совпадают, цветовой состав их окрестностей также будет одинаковым. □

Заметим, что вершины графов G_1 и G_2 имеют одинаковые степени, но число вершин в графах может сильно различаться. Графы (или один из них) могут иметь бесконечное число вершин. Таким образом, накрытия "маленького" графа "большим" позволяет из совершенной раскраски "маленького" графа получить совершенную раскраску "большого" графа с теми же параметрами.

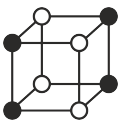
Пример 15. Зададим накрытие $\phi : Q_2^3 \to Q_4$ по правилу: каждой паре противоположных вершин булева куба поставлена в соответствие одна вершина полного графа Q_4.

$$\begin{gathered}\phi^{-1}(0) = \{(000), (111)\},\\ \phi^{-1}(1) = \{(100), (011)\},\\ \phi^{-1}(2) = \{(010), (101)\},\\ \phi^{-1}(3) = \{(001), (110)\}.\end{gathered}$$

Любая раскраска полного графа является совершенной. Раскраски булева куба, которые получаются этим накрытием из раскрасок полного графа в два цвета на рисунке ниже.



$$S = \begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix}$$



$$S = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

Из определений следует, что накрытие $\phi : V(G_1) \to V(G_2)$ является совершенной раскраской вершин графа G_1 в цвета — вершины графа G_2. И наоборот, справедливо утверждение

Утверждение 35. *Пусть имеется совершенная раскраска f с симметричной $(0,1)$-матрицей параметров S с нулями по диагонали. Тогда отображение $f : V(G_1) \to V(G_2)$, где G_2 — граф с матрицей смежности S, является накрытием.*

Здесь вершинами графа G_2 являются цвета раскраски f, цвета соединены рёбрами, если видят друг друга.

Поскольку накрытие можно рассматривать как совершенную раскраску, накрытию ϕ соответствует прямоугольная матрица Φ, для которой выполнено равенство $M_1\Phi = \Phi M_2$, где M_1 и M_2 матрицы смежности графов G_1 и G_2. Следовательно утверждение 34 является частным случаем утверждения 29 о склеивании цветов. Действительно, из равенств $M_2F = FS$ и $M_1\Phi = \Phi M_2$ следует, что $M_1\Phi F = \Phi FS$. Кроме того, накрытие переводит собственные функции графа накрываемого графа в собственные функции накрывающего графа. Действительно, аналогично следствию 1, из равенства $M_2 f = \lambda f$ следует, что $M_1(\Phi f) = \Phi(M_2 f) = \lambda(\Phi f)$. Изоморфизм двух графов эквивалентен взаимно однозначному накрытию. В этом случае матрица Φ является квадратной матрицей перестановки вершин и имеются равенства $M_1\Phi = \Phi M_2$, $M_2\Phi^{-1} = \Phi^{-1}M_1$.

Из равенства (1) для параметров совершенной раскраски следует, что отношение числа вершин двух цветов $\frac{n_i}{n_j}$ равно отношению элементов матрицы параметров $\frac{s_{ji}}{s_{ij}}$ (когда $s_{ij} \neq 0$). В случае накрытия матрице параметров раскраски соответствует матрица смежности накрываемого графа, элементами которой являются нули или единицы. Поэтому при отображении накрытия $\phi : V(G_1) \to V(G_2)$ прообразы всех вершин графа G_2 имеют одинаковую мощность $k = |V(G_1)|/|V(G_2)|$. Такое накрытие называют k-накрытием. Заметим, что накрытие графом G полного графа Q_q является одновременно правильной и совершенной раскраской графа G в q цветов.

Утверждение 36. *Если существует накрытие q-регулярным графом G полного графа Q_{q+1}, то граф G содержит совершенный код.*

Доказательство. Поскольку любая раскраска полного графа является совершенной, найдётся совершенная раскраска графа Q_{q+1} с матрицей параметров $S = \begin{pmatrix} 0 & q \\ 1 & q-1 \end{pmatrix}$. По утверждению 34 существует совершенная раскраска графа G с той же матрицей параметров. Тогда первый цвет этой раскраски является совершенным кодом по определению. $\square$

Утверждение 37. *Если отображения $\phi_i : V(G_i) \to V(H_i)$, $i = 1, 2$, — накрытия, то отображение $\bar{\phi} : V(G_1 \square G_2) \to V(H_1 \square H_2)$, где $\bar{\phi}(x, y) = (\phi_1(x), \phi_2(y))$ также является накрытием.*

Доказательство. Имеем $M_i\Phi_i = \Phi_i N_i$, где матрица Φ_i соответствует накрытию ϕ_i, а M_i — матрица смежности графа G_i и N_i — матрица смежности графа H_i, $i = 1, 2$. По определению отображение $\bar{\phi}$ имеет матрицу $\Phi_1 \otimes \Phi_2$. Матрица $M_1 \otimes I_{m_2} + I_{m_1} \otimes M_2$ является матрицей смежности декартова произведения графов G_1 и G_2 с матрицами смежности M_1 и M_2, а матрица $N_1 \otimes I_{n_2} + I_{n_1} \otimes N_2$ является матрицей смежности декартова произведения графов H_1 и H_2 с матрицами смежности N_1 и N_2 . Тогда имеем

$$(M_1 \otimes I_{m_2} + I_{m_1} \otimes M_2)(\Phi_1 \otimes \Phi_2) = M_1\Phi_1 \otimes \Phi_2 +$$

$$+\Phi_1 \otimes M_2\Phi_2 = (\Phi_1 \otimes \Phi_2)(N_1 \otimes I_{n_2} + I_{m_1} \otimes N_2),$$

что эквивалентно требуемому. □

Пример 16. Отображение $\bar{\phi}_n : Q_2^{3n} \to Q_4^n$, $\bar{\phi}_n(x_1, \ldots, x_n) = (\phi(x_1), \ldots, \phi(x_n))$, где ϕ определено в примере 15, является накрытием.

Теорема 16 ([4])**.** *Для любых двух r-регулярных графов G_1 и G_2 найдётся граф G_0, которым можно накрыть каждый из них.*

Доказательство. Сначала построим накрытие ϕ графа G_1 двудольным графом G_1'. Множество вершин двудольного графа G_1' состоит из удвоенного множества вершин графа G_1, т. е. $V(G_1') = V \cup V'$ причём имеется отображение $\phi_1 : V \cup V' \to V(G_1)$, взаимно однозначное на V и на V'. Вершины $u \in V$ и $u' \in V'$ графа G_1' соединены ребром тогда и только тогда, когда вершины $\phi_1(u)$ и $\phi_1(u')$ смежны в G_1. Легко видеть, что отображение ϕ_1 является накрытием по построению. Аналогично определим двудольный граф G_2', который накрывает граф G_2, и накрытие ϕ_2.

Теперь определим граф G_0, который накрывает графы G_1' и G_2'. По следствию 25 теоремы Кёнига, которая будет доказана в разделе 8.2, рёбра двудольного r-регулярного графа можно раскрасить в r цветов так, чтобы каждая вершина была инцидентна r рёбрам, по одному каждого из r цветов. Раскрасим таким образом рёбра графов G_1' и G_2'. Пусть $V(G_0) = V(G_1') \times V(G_2')$. Вершины (u_1, u_2) и (v_1, v_2) соединим ребром в графе G_0 тогда и только тогда, когда вершины u_1 и v_1 в графе G_1' были соединены ребром того же цвета, что и вершины u_2 и v_2 в графе G_2'. По построению отображение $\psi_1 : V(G_0) \to V(G_1')$, определённое равенством $\psi_1(u_1, u_2) = u_1$, является накрытием графа G_1'. Действительно, каждому цвету ребра соответствует по одной вершине v_1, смежной с u_1 в графе G_1', и по одной вершине (v_1, v_2), смежной с (u_1, u_2) в графе G_0. Аналогично отображение $\psi_2 : V(G_0) \to V(G_2')$, определённое равенством $\psi_2(u_1, u_2) = u_2$, является накрытием графа G_2'. Композиции $\psi_1 \circ \phi_1$ и $\psi_2 \circ \phi_2$ являются накрытиями графов G_1 и G_2, соответственно, графом G_0. □

Теорему 16 можно обобщить на нерегулярные графы. А именно, у двух графов найдётся общее накрытие, если и только если они допускают совершенную раскраску с одинаковой матрицей параметров (см. [63]).

Определение 26. *Пусть G_1 — mr-регулярный граф и G_2 — r-регулярный граф. m-Кратным накрытием $\phi : V(G_1) \to V(G_2)$ называется такое отображение, что $\forall x \in V(G_1)$ $\phi(S_1^1(x)) = S_1^2(\phi(x))$ и $\forall y \in S_1^2(\phi(x))$ $|\phi^{-1}(y) \cap S_1^1(x)| = m$.*

Утверждение 38. *Пусть $\phi : V(G_1) \to V(G_2)$ — m-кратное накрытие и $f : V(G_2) \to \{1, \dots, k\}$ — совершенная раскраска графа G_2 с матрицей параметров S. Тогда $f \circ \phi : V(G_1) \to \{1, \dots, k\}$ — совершенная раскраска графа G_1 с матрицей параметров mS.*

Доказательство. Накрытию ϕ соответствует $(0,1)$-матрица Φ. Из определения m-кратного накрытия имеем $M_1\Phi = \Phi(mM_2)$, где M_1 и M_2 — матрицы смежности графов G_1 и G_2 соответственно. Из утверждения 6 следует равенство $M_2F = FS$. Тогда $M_1\Phi F = \Phi(mM_2)F = \Phi F(mS)$. $\square$

Пример 17. Пусть функция $pch : Q_2^k \to Q_2$ — "счётчик чётности" — совершенная раскраска с матрицей параметров $\begin{pmatrix} 0 & k \\ k & 0 \end{pmatrix}$, т. е. $pch(x) = 1$, если x содержит нечётное число единиц и $pch(x) = 0$, если x содержит чётное число единиц. Тогда отображение $p_m^k : Q_2^{km} \to Q_2^m$, заданное равенством $p_m^k(x_1, \dots, x_m) = (pch(x_1), \dots, pch(x_m))$, $x_i \in Q_2^k$, является k-кратным накрытием.

Пример 18. Пусть на множестве Q_q задана некоторая группа с операцией $*$. Рассмотрим отображение $\ell : Q_q^n \to Q_q$, заданное равенством $\ell(x_1, \dots, x_n) = x_1 * x_2 * \dots * x_n$. Нетрудно показать, что ℓ — n-кратное накрытие графа Q_q. Если id — раскраска графа Q_q в q разных цветов (матрица параметров $J - I$), то матрица параметров раскраски $id \circ \ell$ равна $n(J - I) = \begin{pmatrix} 0 & n & \dots & n \\ n & 0 & \dots & n \\ \vdots & \vdots & \ddots & \vdots \\ n & \dots & \dots & 0 \end{pmatrix}$ — матрица размера $q \times q$, у которой по главной диагонали стоят нули, а в остальных позициях — n. Такая раскраска называется латинской, а гиперкуб с такой раскраской вершин — латинским.

Пример 19. Рассмотрим раскраску h графа Q_q в два цвета: одна вершина — первого цвета, остальные — второго. Раскраска $h \circ \ell$, где отображение ℓ определено в примере 18, является совершенной раскраской графа Q_q^n с матрицей параметров $\begin{pmatrix} 0 & n(q-1) \\ n & n(q-2) \end{pmatrix}$. Таким образом, вершины первого цвета образуют МДР-код, а некодовые вершины можно

рассматривать как объединение остальных цветов латинской раскраски $h \circ \ell = h \circ (id \circ \ell)$.

Пример 20. Рассмотрим накрытие $\bar{\phi}_n : Q_2^{3n} \to Q_4^n$ из примера 16 и МДР-код в гиперкубе Q_4^n, т. е. раскраску f с матрицей параметров $S = \begin{pmatrix} 0 & 3n \\ n & 2n \end{pmatrix}$. Тогда из утверждения 34 следует, что $f \circ \bar{\phi}_n$ — совершенная раскраска с матрицей параметров S булева гиперкубе Q_2^{3n}. Совершенную раскраску с этими параметрами можно задать и как $\phi \circ p_3^n$, где отображение p_3^n определено в примере 17, а отображение ϕ — примере 15. Раскраска с такими параметрами достигает границы Фон-дер-Флаасса корреляционной иммунности (см. раздел 12.6).

6.4 Орбитные раскраски и раскраски графов Кэли

Пусть G — некоторый граф и H — подгруппа группы автоморфизмов графа, $H \leq Aut(G)$.

Определение 27. *Орбитой относительно подгруппы H называется минимальное по включению множество $O \subset V(G)$ такое, что $\pi(O) = O$ для любого автоморфизма $\pi \in H$.*

Нетрудно видеть, что каждая орбита O совпадает с образом $H(v) = \{\pi(v) \mid \pi \in H\}$ любого своего элемента $v \in O$. Множество вершин графа разбивается на непересекающиеся орбиты.

Утверждение 39. *Пусть $\{O_1, \ldots, O_k\}$ — разбиение вершин графа G на орбиты относительно подгруппы H. Тогда раскраска h, заданная равенством $h(v) = i$ при $v \in O_i$, является совершенной.*

Доказательство. Пусть элементы v и v' содержатся в одной орбите, т. е. $h(v) = h(v')$. Тогда $v' = \pi(v)$ для некоторого автоморфизма $\pi \in H$. Рассмотрим произвольную вершину u смежную с вершиной v. Тогда по определению автоморфизма вершина $u' = \pi(u)$ смежна с вершиной $\pi(v)$. Следовательно вершины u и u' принадлежат одной орбите и $h(u') = h(u)$. Отображение π взаимно однозначно, поэтому цветовой состав окрестностей вершин v и v' совпадает. □

Определённую в утверждении 39 совершенную раскраску будем называть *орбитной*.

Следствие 22. *Пусть $C \subset V(G)$ — транзитивный код в графе G. Тогда C является цветом некоторой орбитной раскраски.*

Пример 21. Рассмотрим граф, вершинами которого являются числа $0, \ldots, 8$, и вершины x и y соединены ребром, если $(x - y) \mod 9 \in$

$\{\pm 1, \pm 2\}$. Нетрудно видеть, что отображение $\varphi(x) = (x+3) \mod 9$ является автоморфизмом графа и порождает подгруппу[17] $H = \{\varepsilon, \varphi, \varphi^2\}$. Относительно H граф разбивается на три орбиты в зависимости от остатка при делении на 3. Раскраска $h(x) = x \mod 3$ является совершенной с матрицей параметров $\begin{pmatrix} 0 & 2 & 2 \\ 2 & 0 & 2 \\ 2 & 2 & 0 \end{pmatrix}$.

Описание всех орбитных раскрасок сводится к нахождению группы автоморфизмов графа. Изометрии (автоморфизмы) гиперкубов описывает теорема Маркова. Для её формулировки нам понадобятся некоторые определения.

Определение 28. *Изотопией называется изометрия гиперкуба Q_q^n, определённая равенством $\overline{\sigma}(x_1, x_2, \ldots, x_n) = (\sigma_1 x_1, \sigma_2 x_2, \ldots, \sigma_n x_n)$, где σ_i — перестановка элементов множества Q_q.*

Определение 29. *Парастрофией называется изометрия гиперкуба Q_q^n, определённая равенством $\tau(x_1, x_2, \ldots, x_n) = (x_{\tau 1}, x_{\tau 2}, \ldots, x_{\tau n})$, где τ — перестановка множества $\{1, \ldots, n\}$.*

Теорема 17 (Марков [126])**.** *Любая изометрия гиперкуба является композицией изотопии и парастрофии.*

Некоторые изометрии гиперкуба можно рассматривать как аффинные преобразования в векторном пространстве над конечным полем. Если q — степень простого числа, то существует поле Галуа $GF(q)$ мощности q. Тогда можно отождествить элементы Q_q с элементами поля и определить на вершинах гиперкуба Q_q^n структуру векторного пространства. Рассмотрим линейное преобразование гиперкуба, матрица которого содержит по одной единице в каждой строке и каждом столбце, а остальные элементы равны нулю. Ясно, что такое линейное преобразование является парастрофией. Рассмотрим отображение переноса, которое прибавляет к каждой вершине гиперкуба некий фиксированный вектор. Ясно, что такое аффинное преобразование является изотопией. Можно показать (см. задачу 50), что при $q = 2, 3$ все изометрии гиперкубов Q_q^n являются аффинными преобразованиями.

Граф на q вершинах, который имеет циклическую подгруппу $\mathbb{Z}_q$ группы автоморфизмов, действующую регулярно[18] на его вершинах, называется *циркулянтным*. Рассмотренный в примере 21 граф является циркулянтным.

[17] Здесь и далее ε — нейтральный элемент группы (тождественная перестановка).

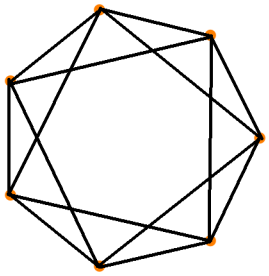
[18] Действие группы на графе называется регулярным, если для каждой упорядоченной пары вершин графа найдётся единственный элемент группы, переводящий первую вершину во вторую.

Описание совершенных раскрасок некоторых циркулянтных графов в два цвета имеется в работах [139], [77].

Вершинно транзитивный граф имеет ровно одну орбиту относительно своей группы автоморфизмов. Транзитивные графы с богатой подгруппами группой автоморфизмов допускают множество орбитных раскрасок. Примерами транзитивных графов являются графы Кэли.

Определение 30. *Пусть Gr — некоторая группа, $A \subset Gr$ — множество образующих такое, что $A^{-1} = A$ (иначе получится ориентированный граф), $\varepsilon \notin A$ (граф без петель). Графом Кэли $Cay(Gr, A)$ называется граф, вершинами которого являются элементы группы, и две вершины $x, y \in Gr$ соединены ребром, когда $y = xa$ для некоторого $a \in A$.*

Замечание 9. Элементы группы $g \in Gr$ определяют автоморфизмы ϕ_g графа $Cay(Gr, A)$ по правилу $\varphi_g(x) = gx$. Группа Gr является подгруппой группы автоморфизмов графа $Cay(Gr, A)$. Таким образом, любой граф Кэли является вершинно транзитивным. Графы Кэли $Cay(\mathbb{Z}_q, A)$ являются циркулянтными.



На рисунке изображён граф $Cay(\mathbb{Z}_7, A)$, где $A = \{\pm 1, \pm 2\}$.

Нетрудно показать, что граф Кэли декартова квадрата группы $Gr \times Gr$ с набором образующих $A \times \{\varepsilon\} \cup \{\varepsilon\} \times A$, является декартовым произведением графов Кэли $Cay(Gr, A) \square Cay(Gr, A)$.

Замечание 10. Полный граф Q_q можно рассматривать как граф Кэли группы $\mathbb{Z}_q$ с множеством образующих, состоящим из всех ненулевых элементов группы. Гиперкуб Q_q^n можно рассматривать как граф Кэли $Cay(\mathbb{Z}_q^n, A)$, где A — множество наборов, содержащих ровно один ненулевой элемент.

Специальным случаем графа Кэли является выбор в качестве множества образующих $A = A^{-1}$ набора представителей смежных классов по некоторой подгруппе H, т. е. $A \simeq (Gr/H) \backslash \{\varepsilon\}$. Тогда любой элемент $g \in Gr$ группы единственным образом представляется в виде $g = ha$ или $g = h \in H$, т. е. каждая вершина графа $Cay(Gr, A)$ видит ровно один элемент подгруппы H, либо сама принадлежит подгруппе H. Таким образом, множество H образует 1-совершенный код в $Cay(Gr, A)$.

Как доказано в утверждении ниже, в качестве H можно взять любую нормальную[19] подгруппе.

Утверждение 40. *Пусть H нормальная подгруппа группы Gr. Тогда из смежных классов по H можно выбрать набор представителей A, удовлетворяющий свойству $A = A^{-1}$.*

Доказательство. Поскольку H — нормальная подгруппа, то из равенства $Ha = Hb$ следует равенство $Ha^{-1} = Hb^{-1}$ ($b = ha \Rightarrow b^{-1} = a^{-1}h^{-1} = h'a^{-1}$), а значит элементы множества A можно выбирать парами $\{a, a^{-1}\}$, когда a и a^{-1} принадлежат разным смежным классам. Докажем, что если пара взаимно обратных элементов a и a^{-1} содержится в одном смежном классе, то в нём есть элемент второго порядка ($b^2 = \varepsilon$), который можно выбрать в качестве представителя класса в множестве A. Пусть, $a^{-1} = ha$ для некоторого $h \in H$, т е. $\varepsilon = ha^2$. Следовательно, a^2 и все чётные степени элемента a содержатся в H, а все нечётные степени содержатся в смежном классе Ha. Поскольку группа H конечна, найдётся минимальное целое $s > 0$, для которого $a^{2s} = \varepsilon$. Причём чётность числа s противоречит условию, поэтому $a^s \in Ha$. □

Пример 22. Рассмотрим группу перестановок S_n и подгруппу H, состоящую из перестановок, фиксирующих некоторый элемент. Без ограничения общности можно полагать, что $\pi(1) = 1$ для всех $\pi \in H$. Положим $A = (S_n/H)\backslash\{\varepsilon\}$. Нетрудно видеть, что $A = \{(1i) \mid i = 2, \ldots, n\}$ и $H \simeq S_{n-1}$. Граф $Cay(S_n, A)$ называется *star-графом*. Подгруппа H образует в star-графе совершенный код[20].

Утверждение 41. *Пусть Gr_1, Gr_2 — некоторые группы, и имеется гомоморфизм[21] $\varphi : Gr_1 \to Gr_2$, который действует взаимно однозначно на множестве образующих $A \subset Gr_1$. Тогда отображение φ является накрытием графа $Cay(Gr_2, \varphi(A))$ графом $Cay(Gr_1, A)$.*

Доказательство. Пусть $g \in Gr_1$. Тогда $\{ga \mid a \in A\} = S_1^1(g)$. Из определения гомоморфизма имеем $\varphi(ga) = \varphi(g)\varphi(a)$. Таким образом $\varphi(S_1^1(g)) = S_1^2(\varphi(g))$ и отображение φ взаимно однозначно на $S_1^1(g)$ для любого $g \in Gr_1$ по условию. □

Отображение $f : Gr_1 \times Gr_2 \to Gr_1$, действующее по правилу $f((a, b)) = a$ является естественным гомоморфизмом из прямого произведения $Gr_1 \times Gr_2$ в сомножитель. Рассмотрим другие примеры.

[19] Нормальной называется подгруппа H, для которой $gH = Hg$ для любого $g \in Gr$.

[20] Примеры негрупповых совершенных кодов в стар-графах имеются в [73].

[21] Гомоморфизмом называется отображение, удовлетворяющее равенству $\varphi(x * y) = \varphi(x) \circ \varphi(y)$ для любых элементов $x, y \in Gr_1$. Здесь $*$ и $\circ$ — групповые операции в Gr_1 и Gr_2 соответственно.

Пример 23. Отображение $\varphi(n) = n(\mod 4)$ является гомоморфизмом группы $\mathbb{Z}$ в группу $\mathbb{Z}_4$. Тогда отображение $\varphi : Cay(\mathbb{Z}, \pm 1) \to Cay(\mathbb{Z}_4, \pm 1)$ является накрытием.

Группы $\mathbb{Z}_2 \times \mathbb{Z}_2$ и $\mathbb{Z}_4$ не изоморфны. Однако их графы Кэли (с любыми двумя образующими) изоморфны квадрату $Q_2 \square Q_2$. Изоморфизм $\iota : Cay(\mathbb{Z}_2 \times \mathbb{Z}_2, \{(0,1),(1,0)\}) \leftrightarrow Cay(\mathbb{Z}_4, \pm 1)$, при котором $\iota((0,0)) = 0$ называется *отображением Грея*.

Рассмотрим группу $\mathbb{Z}_4^n$. Пусть $e_i = (0, \ldots, \underset{i}{1}, \ldots, 0)$. Имеем изоморфизмы графов $Cay(\mathbb{Z}_4^n, \{\pm e_i\}) \leftrightarrow Cay(\mathbb{Z}_2^{2n}, \{e_i\}) \leftrightarrow Q_2^{2n}$. Из утверждения 37 и примера 23 следует существование накрытия графа Q_2^{2n} графом n-мерной прямоугольной решётки $Cay(\mathbb{Z}^n, \{\pm e_i\})$. Следовательно, из любой совершенной раскраски $2n$-мерного булева гиперкуба можно получить совершенную раскраску n-мерной прямоугольной решётки с той же матрицей параметров.

Пример 24. Рассмотрим накрытие ψ графа Q_5 двумерной прямоугольной решёткой, т. е. графом $Cay(\mathbb{Z}^2, \{(\pm 1, 0), (0, \pm 1)\})$, заданное формулой $\psi(x, y) = x + 2y(\mod 5)$. Любая раскраска полного графа Q_5 является совершенной. Тогда двумерную прямоугольную решётку можно раскрасить с матрицами параметров $\begin{pmatrix} 0 & 4 \\ 1 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix}$, $\begin{pmatrix} 0 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 2 & 1 \end{pmatrix}$.

Графом Шрикханде называется граф
$Sh = Cay(\mathbb{Z}_4^2, \{(1,0), (-1,0), (0,1), (0,-1), (1,1), (-1,-1)\})$.
Определим равенством $\theta(x_1e_1 + x_2e_2 + x_3e_3) = x_1(1,0) + x_2(0,1) + x_3(1,1)$ отображение

$$\theta : Cay(\mathbb{Z}_4^3, \{\pm e_i\}) \to Sh.$$

Можно непосредственно проверить, что отображение θ является накрытием. Достаточно рассмотреть образ окрестности одной точки, поскольку оба графа транзитивны. Как замечено выше, граф $Cay(\mathbb{Z}_4^3, \{\pm e_i\})$ изоморфен графу Q_2^6. Следовательно имеется накрытие графа Шрикханде 6-мерным булевым кубом. В графе Шрикханде нетрудно найти совершенную раскраску в два цвета с матрицей параметров $\begin{pmatrix} 1 & 5 \\ 3 & 3 \end{pmatrix}$. Тогда в кубе $\mathbb{Z}_2^6$ есть совершенная раскраска с этими же параметрами. Эта раскраска была впервые найдена Ю.В.Таранниковым. Она является примером раскраски достигающей границы Фон-дер-Флаасса корреляционной иммунности (см. раздел 12.6).

Пример 25. Рассмотрим группу перестановок S_n и множество всех транспозиций T_n. Граф $Cay(S_n, T_n)$ называется *графом транспозиций*. Выберем произвольное подмножество $\{a_1, \ldots, a_k\}$ мощности $k, 1 < k <$

n, в множестве, на котором определены перестановки. Определим отображение $\nu : V(Cay(S_n, T_n)) \to V(J(n,k))$ по правилу: в наборе $\nu(\sigma)$ единицы находятся на позициях $\sigma(a_i)$, $i = 1, \ldots, k$, $\sigma \in S_n$. Нетрудно видеть, что отображение ν осуществляет накрытие графа Джонсона (см. пример 10) с добавленными $\binom{k}{2} + \binom{n-k}{2}$ петлями в каждой вершине графа Джонсона.

Задача 39. Пусть G — дистанционно регулярный граф и характеристическая функция χ_C множества $C \subset V(G)$ представима в виде суммы k собственных функций графа G с k различными собственными значениями. Докажите, что 1) если множество C является цветом некоторой совершенной раскраски, то в ней не менее k цветов; 2) если после $k-1$ шага алгоритма Вейсфейлера—Лемана из функции χ_C получилась раскраска в k цветов, то полученная раскраска является совершенной.

Задача 40. Пусть G — дистанционно регулярный граф и C — множество вершин фиксированного цвета в некоторой совершенной раскраске графа G. Докажите, что для двух вершин любого другого цвета число путей произвольной фиксированной длины до вершин выбранного цвета совпадает. Приведите пример, показывающий, что совпадение длин путей до вершин множества C не является достаточным условием для того, чтобы алгоритм Визинга, начиная с двуцветной раскраски $\{C, V(G)\backslash C\}$, раскрасил вершины в одинаковый цвет.

Задача 41. Докажите, что если в совершенной раскраске двудольного связного графа вершины хотя бы одного цвета содержатся только в одной доле, то это верно для вершин любого цвета.

Задача 42. Пусть имеется такая раскраска графа G в цвета из множеств A и B, что при объединении всех цветов из A в один цвет и сохранении всех цветов из B, а также наоборот при объединении всех цветов из B и сохранении всех цветов из A получаются совершенные раскраски. Докажите, что исходная раскраска является совершенной.

Задача 43. Пусть имеется совершенная раскраска булева гиперкуба Q_2^k с матрицей параметров S. Докажите, что имеется раскраска булева гиперкуба Q_2^{mk} с матрицей параметров mS.

Задача 44. Пусть имеется совершенная раскраска гиперкуба Q_q^k с матрицей параметров S. Докажите, что имеется раскраска гиперкуба Q_{pq}^k с матрицей параметров $pS + k(p-1)I$.

Задача 45. Пусть $\phi : V(G_1) \to V(G_2)$ накрытие. Докажите, что число общих соседей у вершин $u, v \in V(G_1)$ не больше, чем число общих соседей у вершин $\phi(u), \phi(v) \in V(G_2)$. Докажите, что размер максимальной клики в накрывающем графе не больше, чем в накрываемом.

Задача 46. Пусть имеется накрытие графа G_2 графом G_1. Докажите, что если граф G_2 имеет совершенное паросочетание (см. раздел 8.4), то граф G_1 также имеет совершенное паросочетание.

Задача 47. Докажите, что бесконечное дерево степени r накрывает любой r-регулярный граф.

Задача 48. Докажите, что в k-мерной прямоугольной решётке имеется совершенный код.

Задача 49. Докажите, что в k-мерная прямоугольная решётка накрывает граф Q_3^k.

Задача 50. Докажите (с помощью теоремы Маркова), что при $q = 2$ и $q = 3$ все изометрии гиперкубов Q_q^n являются аффинными преобразованиями.

Задача 51. Пусть q — степень простого числа, A — матрица размера $k \times n$ над полем $GF(q)$. Определим множество вершин цвета $b \in Q_q^n$ как $\{x \in Q_q^n : Ax = b\}$. Докажите, что такая раскраска гиперкуба Q_q^n является совершенной.

Задача 52. Рассмотрим группу перестановок S_n и множество образующих $A \subset S_n$, $A^{-1} = A$, $|A| = n$. Для каждой перестановки $\pi \in A$ определим матрицу перестановки P_π, где $P_\pi(i, j) = 1$, если $\pi(i) = j$, и $P_\pi(i, j) = 0$ в остальных случаях. Рассмотрим раскраску графа $Cay(S_n, A)$ в n цветов по правилу: перестановка $\sigma \in S_n$ имеет цвет i, если $\sigma(0) = i$. Докажите, что предложенная раскраска является совершенной с матрицей параметров $S = \sum\limits_{\pi \in A} P_\pi$.

7 Совершенные раскраски мультиграфов и гиперграфов

Граф называется ориентированным, если вместо рёбер — неупорядоченных пар вершин рассматриваются дуги — упорядоченные пары. Мультиграф — одно из обобщений понятия графа, при котором допускаются кратные рёбра и петли. Матрицей смежности ориентированного мультиграфа может быть любая неотрицательная целочисленная квадратная матрица. Определение совершенной раскраски ориентированного мультиграфа аналогично определению совершенной раскраски простого графа. Имеется ввиду, что вершина ориентированного мультиграфа видит только те вершины, которые находятся на концах дуг с началом в рассматриваемой вершине. Нетрудно понять, что линейно-алгебраический критерий совершенной раскраски (утверждение 6) верен и для мультиграфов. Заметим, что матрицу параметров любой совершенной раскраски можно рассматривать как матрицу смежности некоторого ориентированного мультиграфа. Тогда совершенную раскраску графа с этой

матрицей параметров можно трактовать как накрытие графа ориентированным мультиграфом. Кроме того, описанное в разделе 6.1 склеивание цветов раскраски можно рассматривать как совершенную раскраску этого мультиграфа.

Пусть G — двудольный граф с долями V и U. Рассмотрим неориентированный мультиграф $\mathcal{M}_{12}(G)$, вершинами которого являются вершины первой доли графа G и вершины $v_i, v_j \in V$ соединены m_{ij} ребрами, если в графе G имеется m_{ij} различных вершин из U смежных с вершинами v_i и v_j одновременно. Для удобства дальнейших вычислений будем полагать, что мультиграф $\mathcal{M}_{12}(G)$ содержит в своих вершинах петли кратности равной степени вершины в графе G. Если G бирегулярен, то петли в $\mathcal{M}_{12}(G)$ имеют одинаковую кратность. Пусть граф G бирегулярен по расстоянию 2, т. е. пары вершин каждой из долей, находящиеся на расстоянии 2, видят одинаковое число вершин другой доли. Тогда все рёбра в мультиграфе $\mathcal{M}_{12}(G)$ имеют одинаковую кратность. В таком случае во всех утверждениях этого раздела вместо мультиграфа $\mathcal{M}_{12}(G)$ можно рассматривать обыкновенный граф, полученный из $\mathcal{M}_{12}(G)$ удалением петель и кратности рёбер. Ниже мы полагаем граф G бирегулярным (не обязательно регулярным) и рассматриваем только такие совершенные раскраски графа G, у которых все цвета в разных долях различны.

Утверждение 42. *Пусть имеется совершенная раскраска $f : V \cup U \to \{1, \dots, k\}$ двудольного графа G с долями V и U. Тогда $f|_V$ является совершенной раскраской мультиграфа $\mathcal{M}_{12}(G)$.*

Доказательство. Матрица смежности графа G может быть представлена в виде $M = \begin{pmatrix} 0 & Y \\ Y^{\mathrm{T}} & 0 \end{pmatrix}$. Пусть $S = \begin{pmatrix} 0 & S_1 \\ S_2 & 0 \end{pmatrix}$ — матрица параметров совершенной раскраски. Тогда из утверждения 6 имеем равенство $MF = FS$, которое эквивалентно паре равенств $YF_2 = F_1S_1$ и $Y^{\mathrm{T}}F_1 = F_2S_2$, где $F = \begin{pmatrix} F_1 & 0 \\ 0 & F_2 \end{pmatrix}$, матрицы F_1 и F_2 соответствуют раскраскам 1-й и 2-й долей графа G. Имеем $YY^{\mathrm{T}}F_1 = YF_2S_2 = F_1S_1S_2$. Осталось заметить, что матрица YY^{T} является матрицей смежности мультиграфа $\mathcal{M}_{12}(G)$ и по утверждению 6 матрица S_1S_2 является матрицей параметров совершенной раскраски $f|_V$. □

Обратное утверждение, вообще говоря, неверно. Совершенная раскраска мультиграфа $\mathcal{M}_{12}(G)$ может не быть сужением никакой совершенной раскраски графа G. В частности, такие примеры нетрудно найти, когда $\mathcal{M}_{12}(G)$ — полный граф.

Гиперграфом называется другое обобщение понятия графа, когда в качестве рёбер рассматриваются неупорядоченные наборы из более чем

двух вершин. Гиперграф называется k-униформным, если любое его ребро состоит из k вершин. Матрицей инцидентности гиперграфа G называется $(0,1)$-матрица $Y = (y_{ij})$ размера $n \times m$, где n — число вершин и m — число рёбер в G. Причём

$$y_{ij} = \begin{cases} 1, \text{ если } v_i \in e_j \in E(G); \\ 0, \text{ иначе.} \end{cases}$$

Для гиперграфа G определим двудольный граф $\mathcal{D}(G)$, первой долей которого являются вершины графа G, а второй — рёбра графа G. Вершина первой доли $v \in V(G)$ смежна с вершиной второй доли $e \in E(G)$, если $v \in e$. Нетрудно видеть, что матрица смежности графа $\mathcal{D}(G)$ может быть представлена в виде $\begin{pmatrix} 0 & Y \\ Y^{\mathrm{T}} & 0 \end{pmatrix}$, где Y — матрица инцидентности гиперграфа G.

Определение 31. *Раскраска вершин гиперграфа G называется совершенной, если индуцированная ей (см. раздел 6.2), как раскраской первой доли, раскраска двудольного графа $\mathcal{D}(G)$ является совершенной.*

Другими словами, раскраска гиперграфа является совершенной[22], если для любого фиксированного цветового состава ребра любые две вершины одного цвета инцидентны равному числу рёбер с этим цветовым составом. Аналогично утверждению 6 получаем, что определение совершенной раскраски гиперграфа эквивалентно уравнению

$$\begin{pmatrix} 0 & Y \\ Y^{\mathrm{T}} & 0 \end{pmatrix} \begin{pmatrix} 0 & F_1 \\ F_2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & F_1 \\ F_2 & 0 \end{pmatrix} \begin{pmatrix} 0 & S_1 \\ S_2 & 0 \end{pmatrix},$$

где матрицы F_1 и F_2 соответствуют раскраскам вершин и гиперрёбер гиперграфа G. Ясно, что это уравнение эквивалентно паре равенств $YF_2 = F_1S_1$ и $Y^{\mathrm{T}}F_1 = F_2S_2$.

Рассмотрим матрицу M смежности мультиграфа $\mathcal{M}_{12}(\mathcal{D}(G))$. Нетрудно видеть, что компонента m_{ij} матрицы M равна числу рёбер гиперграфа G, которые содержат одновременно i-ю и j-ю вершины. В частности, m_{ii} — степень i-й вершины в гиперграфе G. Ясно, что $M = YY^{\mathrm{T}}$, где Y — матрица инцидентности гиперграфа G.

Из утверждения 42 имеем

Следствие 23. *Совершенная раскраска гиперграфа G является совершенной раскраской мультиграфа $\mathcal{M}_{12}(\mathcal{D}(G))$.*

Покажем, что для графа определение его совершенной раскраски эквивалентно определению его совершенной раскраски как 2-униформного

[22] Впервые такое определение было предложено Годсилом [39]. Подробное изложение теории совершенных раскрасок гиперграфов имеется в [95].

гиперграфа. Действительно, совершенная раскраска графа индуцирует раскраску рёбер в пары цветов, соответствующих его концам. Это будет совершенная раскраска $\mathcal{D}(G)$ по определению совершенной раскраски. Обратное тоже верно, по индуцированным цветам рёбер, инцидентных вершине, однозначно определяются цвета смежных с ней вершин.

Определение 32. *Пусть G — k-униформный гиперграф. Рёберным графом $\mathcal{E}(G)$ гиперграфа G называется называется мультиграф, вершинами которого являются рёбра графа G и две вершины графа $\mathcal{E}(G)$ соединены l рёбрами, если пересечение соответствующих им рёбер графа G имеет мощность l.*

Из определения видно, что матрица смежности рёберного графа $\mathcal{E}(G)$ равна $M = Y^{\mathrm{T}}Y - kI$, где Y — матрица инцидентности гиперграфа G. Конечно, рёберный граф простого графа всегда является простым графом.

Будем называть некоторую раскраску f' мультиграфа $\mathcal{E}(G)$ индуцированной раскраской f графа G, если в качестве цвета вершины e графа $\mathcal{E}(G)$ используется набор (с учётом кратности) цветов вершин графа G, содержащихся в соответствующем ребре, т. е. $f'(e) = \{f(v_1), f(v_2), \ldots, f(v_k)\}$, где $e = \{v_1, v_2, \ldots, v_k\}$.

Утверждение 43. *Раскраска графа $\mathcal{E}(G)$, индуцированная совершенной раскраской гиперграфа G, является совершенной.*

Доказательство. Пусть f — совершенная раскраска гиперграфа G в t цветов. Рассмотрим ребро e цвета $\{i_1, \ldots, i_t\}$, т. е. ребро, содержащее i_j вершин цвета j. По определению совершенной раскраски гиперграфа, вершина цвета j содержится в известном количестве рёбер каждого цветового состава. Сложим вектора этих цветовых составов для всех вершин ребра и получим цветовой состав смежных с ним рёбер. Возможно какое-то ребро e' пересекается с ребром e по $s > 1$ вершинам, тогда его цветовой состав будет учтён s раз, но в графе $\mathcal{E}(G)$ между вершинами, соответствующими e и e' имеется ровно s рёбер. □

Определение 33. *Трансверсалью гиперграфа называется набор вершин, однократно протыкающих все рёбра.*

В частности, в двудольном графе трансверсалью является любая из его долей. Нетрудно видеть, что в k-униформном r-регулярном гиперграфе трасверсаль является цветом совершенной раскраски в два цвета. Более того, справедливо следующее

Утверждение 44 ([128])**.** *Функция $f : V \to \{0, 1\}$ является характеристической функцией трансверсали k-униформного r-регулярного гиперграфа G тогда и только тогда, когда она является совершенной раскраской мультиграфа $\mathcal{M}_{12}(\mathcal{D}(G))$ с матрицей параметров $S = \begin{pmatrix} r & (k-1)r \\ r & (k-1)r \end{pmatrix}$.*

Доказательство. Поскольку граф G является r-регулярным, вершины первой доли графа $\mathcal{D}(G)$ имеют степени r. Тогда каждой вершине мультиграфа $\mathcal{M}_{12}(\mathcal{D}(G))$ инцидентны r петель. Вершины из трансверсали не видят других вершин из трансверсали в мультиграфе $\mathcal{M}_{12}(\mathcal{D}(G))$. Кроме того, каждая вершина не из трансверсали видит в мультиграфе $\mathcal{M}_{12}(\mathcal{D}(G))$ вершины транверсали r-кратно, поскольку каждая вершина входит ровно в r рёбер, каждое из которых содержит одну вершину из трансверсали. Поэтому функция f является совершенной раскраской мультиграфа $\mathcal{M}_{12}(\mathcal{D}(G))$. Кроме того, этот факт следует из утверждения 42, поскольку трансверсаль порождает раскраску в три цвета графа $\mathcal{D}(G)$.

Если же f является совершенной раскраской с матрицей параметров S. То любая вершина первого цвета видит себя r-кратно и не видит других вершин первого цвета в графе $\mathcal{M}_{12}(\mathcal{D}(G))$. Значит в каждом ребре гиперграфа G не более одной вершины первого цвета. Кроме того, любая вершина второго цвета видит r вершин первого цвета, значит в каждом инцидентном ей гиперребре имеется вершина первого цвета. □

Задача 53. Сформулируйте определение совершенной раскраски мультиграфа. Докажите аналог теоремы 1 для мультиграфов.

Задача 54. Пусть f — собственная функция двудольного графа G. Докажите, что функция f, суженная на первую долю, является собственной функцией мультиграфа $\mathcal{M}_{12}(G)$.

Задача 55. Докажите, что собственные числа мультиграфа $\mathcal{M}_{12}(\mathcal{D}(G))$ неотрицательны.

Задача 56. Пусть F_1 и F_2 — совершенные раскраски вершин и гиперрёбер гиперграфа с матрицами параметров S_1 и S_2. Докажите равенство $F_1F_1S_1 = S_2F_2F_2$.

Задача 57. Пусть T — трансверсаль униформного регулярного гиперграфа G. Докажите, что T — независимое множество в мультиграфе $\mathcal{M}_{12}(\mathcal{D}(G))$. Докажите, что если $\mathcal{D}(G)$ регулярен по расстоянию 2, множество T достигает границы Дельсарта—Хоффмана в графе, которой получен из $\mathcal{M}_{12}(\mathcal{D}(G))$ удалением петель и кратности рёбер.

Задача 58. Докажите, что сужение собственной функции f с собственным числом λ регулярного двудольного графа G на вершины первой доли является собственной функцией в мультиграфе $\mathcal{M}_{12}(G)$ с собственным числом λ^2. И наоборот, собственная функция мультиграфа $\mathcal{M}_{12}(G)$ с положительным собственным числом продолжается до собственной функции графа G.

Задача 59. Пусть G — бирегулярный двудольный граф и мультиграф $\mathcal{M}_{12}(G)$ является графом, если удалить из него петли. Докажите, что

сужение любой совершенной раскраски графа G на граф $\mathcal{M}_{12}(G)$ является совершенной раскраской.

Задача 60. Расширением графа G будем называть мультиграф $e(G)$, в котором ребрами соединены вершины на расстоянии 1 и 2 в графе G с учётом кратности. Докажите, что если φ — накрытие графа G_2 графом G_1, то φ — накрытие мультиграфа $e(G_2)$ мультиграфом $e(G_1)$.

8 Латинские квадраты и 1-факторизации графов

8.1 Латинские квадраты

Определение 34. *Латинским прямоугольником называется таблица $m_1 \times m_2$, заполненная символами (например элементами Q_q) так, чтобы в каждой линии (строке или столбце) любой символ не встречался больше одного раза.*

Если число строк, столбцов и различных символов равны q, то такой латинский прямоугольник называется латинским квадратом порядка q. Введённую выше латинскую раскраску графа Q_q^2 можно рассматривать как эквивалентное определение латинского квадрата[23].

Пример 26. Латинские квадраты порядков $3, 4, 5$.

0	1	2
1	2	0
2	0	1

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

0	1	2	3	4
1	0	3	4	2
2	3	4	0	1
3	4	1	2	0
4	2	0	1	3

Определение 35. *Бинарная операция $\circ : A^2 \to A$ называется квазигруппой[24], если уравнения $x \circ a = b$ и $a \circ x = b$ однозначно разрешимы для любых $a, b \in A$. Мощность множества A называется порядком квазигруппы.*

Мы будем рассматривать только квазигруппы конечного порядка. Природа множества, на котором действует квазигрупповая операция не важна, поэтому мы всегда будем полагать, что $A = Q_q$ для некоторого $q \in \mathbb{N}$. Из определений непосредственно следует

Утверждение 45. *Таблица размера $q \times q$, заполненная q различными символами, является латинским квадратом тогда и только тогда, когда это таблица значений (таблицей Кэли) некоторой квазигруппы.*

[23] Теория латинских квадратов подробно изложена в [29].

[24] Точнее, квазигруппой называется пара из бинарной операции и множества элементов на котором она действует, в данном случае A.

Утверждение 46. *Если квазигруппа $(Q_q, \circ)$ является полугруппой (операция $\circ$ ассоциативна), то она является группой.*

Доказательство. Рассмотрим $a \in Q_q$. По определению квазигруппы найдётся $e \in Q_q$ такое, что $a \circ e = a$. Тогда для любого $b \in Q_q$ из ассоциативности операции $\circ$ следует равенство $a \circ (e \circ b) = (a \circ e) \circ b = a \circ b$. Из определения квазигруппы имеем $e \circ b = b$, в частности, $e \circ a = a$. Тогда аналогично получаем, что $b \circ e = b$ для всех $b \in Q_q$. Таким образом, e — единичный элемент. □

Пусть $\tau_i, i = 0, 1, 2,$ — перестановки элементов множества Q_q. Нетрудно видеть, что операция $x*y = \tau_0(\tau_1 x \circ \tau_2 y)$ является квазигруппой, если $\circ$ — квазигрупповая операция. Перестановки τ_1 и τ_2, действующие на аргументы квазигруппы, соответствуют перестановкам строк и столбцов в латинском квадрате, а перестановка τ_0 переименовывает элементы в нём.

Кроме того, нетрудно показать, что квазигруппой будет обращение квазигруппы по любому аргументу, т. е. операции $*$ и $*'$, заданные равенством $x * z = y \Leftrightarrow x \circ y = z$ или равенством $z *' y = x \Leftrightarrow x \circ y = z$, тоже является квазигрупповыми.

8.2 Теоремы Визинга и Райзера

Как известно матрица смежности двудольного графа имеет блочную структуру $\begin{pmatrix} 0 & M \\ M^{\mathrm{T}} & 0 \end{pmatrix}$, где M — прямоугольная матрица размера $n_1 \times n_2$, n_1 и n_2 — мощности первой и второй долей графа. Матрица M называется приведённой матрицей смежности двудольного графа.

Пусть $A = \{a_{ij}\}$ — некоторая матрица размера $n_1 \times n_2$. Определим граф $g(A)$ следующим образом: множество вершин $V(g(A)) = \{(i, j) \mid a_{ij} \neq 0\}$ состоит из ненулевых ячеек матрицы, будем говорить, что вершины (i, j) и (i', j') соединены ребром первого направления, если $i = i'$ и ребром второго направления, если $j = j'$. Если A — приведённая матрица смежности некоторого двудольного графа G, то по определению граф $g(A)$ изоморфен рёберному графу по отношению к графу G. Нетрудно видеть, что справедливо следующее

Утверждение 47. *Если в графе $g(A)$ две вершины находятся в одной компоненте связности, то между ними есть путь из рёбер чередующихся направлений.*

Докажем один из вариантов теоремы Визинга, которая наряду с теоремой Холла о системах представителей является одним из базовых утверждений в комбинаторике.

Теорема 18 (Визинг)**.** *Если число единиц в любых строке или столбце прямоугольной* $(0,1)$*-матрицы* A *не превышает* q*, то единицы матрицы можно правильно раскрасить в* q *цветов, т. е. так, чтобы соседние единицы имели разный цвет.*

Доказательство. Предположим требуемой раскраски не существует. Пусть $f : W \to Q_q$ — правильная раскраска подмножества $W \subset V(g(A))$ вершин графа $g(A)$, причём подмножество W максимально возможное по мощности для таких раскрасок. Тогда имеется вершина $x \in V(g(A))\setminus W$, в окрестности которой имеются вершины всех q цветов. Поскольку соседей вершины x по каждому из двух направлений не более $q-1$, то найдутся два различных цвета, которые не встречаются среди соседей одного из направлений. Пусть вершины цветов 0 и 1 встречаются только у соседей вершины x первого и, соответственно, второго направления. Обозначим две соседние с x вершины этих цветов через y и z. Рассмотрим подграф графа $g(A)$, состоящий из всех вершин цвета 0 и 1. Он является двудольным, поскольку раскраска правильная. Если вершины y и z принадлежат одной компоненте связности этого подграфа, то добавление вершины x к пути, соединяющему вершины y и z в этом подграфе приводит к циклу нечётной длины с чередующимися направлениями рёбер. Это невозможно (см. утверждение 47), следовательно, y и z принадлежат разным компонентам связности. Поменяем местами цвета 0 и 1 в компоненте, содержащей вершину z. Раскраска останется правильной, поскольку как и прежде вершины одного цвета не будут соседями. Теперь вершине x можно придать цвет 1 без нарушения правильности раскраски. Пришли к противоречию с максимальностью множества W. □

Из теоремы следует, что если степени вершин некоторого двудольного графа не превосходят r, то существует правильная раскраска рёбер этого графа в r цветов. Это частный случай известной теоремы Визинга [112], утверждающей, что для правильной раскраски рёберного графа достаточно $r+1$ цветов, если степени вершин графа не превосходят r.

Теорема 19 (Райзер)**.** *Латинский прямоугольник* P *размера* $m_1 \times m_2$ *продолжается до латинского квадрата размера* $q \times q$ *тогда и только тогда, когда каждый из* q *различных символов встречается не менее* $m_1 + m_2 - q$ *раз.*

Доказательство. ($\Rightarrow$) В последних $q-m_1$ строках латинского квадрата любая буква встречается $q-m_1$ раз, а в последних $q-m_2$ столбцах — $q-m_2$ раза. Значит эта буква встречается не более $2q-m_1-m_2$ раз вне P. Поскольку всего в квадрате она встречается q раз, то в P — не менее m_1+m_2-q раз.

($\Leftarrow$) Вначале предположим, что $m_2 = q$. В этом случае условие, что каждый символ встречается не менее $m_1 + m_2 - q$ раз выполнено автоматически, поскольку любой символ должен встречаться ровно один раз в каждой из m_1 строк, т. е. m_1 раз. Построим по латинскому прямоугольнику P таблицу $A = Inv(P)$ размера $q \times q$ по правилу

$$A(i,j) = \begin{cases} k, \text{ если найдётся } k \in \{1,\dots,m_1\}, \text{ для которого } P(k,j) = i; \\ 0, \text{ иначе.} \end{cases}$$

Отметим, что если прямоугольник P продолжается до латинского квадрата, то операция Inv соответствует обращению по первому аргументу квазигруппы, которая задаёт этот латинский квадрат.

Здесь нам удобно считать, что алфавит латинского прямоугольника состоит из символов $1, 2, \dots, q$, а символ 0 нужно рассматривать как "специальный" символ означающий, что ячейка в таблице не заполнена. Через $\mathrm{supp}(A)$ обозначаем матрицу, в которой все ненулевые элементы матрицы A заменены на единицы.

Например,

$$P = \begin{array}{|c|c|c|c|}\hline 4&1&2&3\\\hline 1&4&3&2\\\hline 0&0&0&0\\\hline 0&0&0&0\\\hline\end{array} \qquad A = \begin{array}{|c|c|c|c|}\hline 2&1&0&0\\\hline 0&0&1&2\\\hline 0&0&2&1\\\hline 1&2&0&0\\\hline\end{array} \qquad \mathrm{supp}(A) = \begin{array}{|c|c|c|c|}\hline 1&1&0&0\\\hline 0&0&1&1\\\hline 0&0&1&1\\\hline 1&1&0&0\\\hline\end{array}.$$

В любых столбце или строке матрицы $\mathrm{supp}(A)$ ровно m_1 единиц. Рассмотрим матрицу $B = J - \mathrm{supp}(A)$. В каждой линии матрицы B ровно по $q - m_1$ единиц, поэтому по теореме Визинга единицы матрицы B можно правильно раскрасить цветами $m_1 + 1, \dots, q$. Очевидно, что объединение матриц A и B является латинским квадратом L. Вычислим $Inv(L)$. Из определения операции Inv видно, что она переводит латинский квадрат в латинский квадрат, причём $Inv(Inv(L)) = L$. Поэтому первые m_1 строк латинского квадрата $Inv(L)$ совпадают с исходным латинским прямоугольником P.

Теперь перейдём к рассмотрению случая $m_2 < q$. Тогда в результате операции Inv из прямоугольника P получится прямоугольник $A = Inv(P)$ размера $q \times m_2$. В каждом столбце матрицы $\mathrm{supp}(A)$ ровно m_1 единиц, а в каждой строке не менее $m_1 + m_2 - q$ единиц по условию. Пусть $B = J - \mathrm{supp}(A)$, где J — матрица размера $q \times m_2$, состоящая из единиц. В каждом столбце матрицы B имеется $q - m_1$ единиц, а в каждой строке не более $m_2 - (m_1 + m_2 - q) = q - m_1$ единиц. По теореме Визинга матрицу B можно правильно раскрасить в $q - m_1$ цветов, и в объединении с матрицей A получаем латинский прямоугольник размера $q \times m_2$. Из первой части доказательства следует, что прямоугольник можно дополнить до латинского квадрата L и латинский квадрат $Inv(L)$ содержит исходный прямоугольник P. $\square$

Следствие 24. *Латинский прямоугольник размера $m_1 \times q$, содержащий q различных символов можно дополнить до латинского квадрата.*

Операция Inv, применённая к L — таблице Кэли некоторой квазигруппы, определяет латинский квадрат $Inv(L)$. Он является таблицей Кэли квазигруппы — обращения исходной квазигруппы относительно аргумента, нумерующего строки.

Отметим, что прямое обобщение следствия 24 на латинские параллелепипеды невозможно, поскольку имеется латинский параллелепипед размера $2 \times 5 \times 5$, который нельзя продолжить даже до латинского параллелепипеда размера $3 \times 5 \times 5$ в алфавите из 5 элементов [72].

8.3 Теоремы Холла, Кёнига и Эгервари

Определение 36. *Паросочетанием в графе G называется такой набор его рёбер, что любая вершина графа G инцидентна не более, чем одному ребру из этого набора.*

Из теоремы Визинга следует, что степени вершин двудольного графа не превышают r, то множество рёбер графа можно разбить на r паросочетаний. Далее мы рассмотрим вопрос о максимальной мощности паросочетания в графе.

Определение 37. *Вершинным покрытием в графе G называется такой набор вершин графа, что любое ребро графа содержит вершину из покрытия.*

Теорема 20 (Кёниг — Эгервари)**.** *В любом двудольном графе мощность максимального (по мощности) паросочетания равна мощности минимального (по мощности) вершинного покрытия.*

Сформулируем теорему Кёнига — Эгенвари для матриц.

Теорема 21 (Кёниг, Эгервари)**.** *Пусть A некоторая матрица. Минимальное суммарное число строк и столбцов матрицы A, в которых содержатся все ненулевые элементы матрицы равно мощности максимального независимого множества в графе $g(A)$.*

Эквивалентность формулировок очевидна, если мы рассмотрим $\mathrm{supp}(A)$ как приведённую матрицу смежности двудольного графа. Строки и столбцы, покрывающие ненулевые элементы матрицы соответствуют вершинному покрытию графа, а независимое множество в $g(A)$ — паросочетанию. Теперь докажем теорему.

Доказательство. Очевидно, что в каждой линии из покрытия матрицы $\mathrm{supp}(A)$ можно выбрать не более одного элемента независимого множества. Значит $|C|$ не больше числа строк и столбцов в покрытии матрицы $\mathrm{supp}(A)$.

Пусть C — максимальное независимое множество в $g(A)$. Тогда любая вершина из $V(g(A)) \setminus$ смежна с некоторой вершиной из C. Предположим $c \in C$ имеет таких двух соседей $a_1, a_2 \in V(g(A))$ по разным направлениям, которые не смежны с другими вершинами из C. Тогда множество $C' = C \cup \{a_1, a_2\} \setminus \{c\}$ оказывается независимым в $g(A)$, что противоречит максимальности C. Значит каждая вершина $c \in C$, может иметь смежные вершины $a \in V(g(A))$, несмежные с другими вершинами из C, только по одному из двух направлений: по строке или по столбцу. Обозначим через C_1 множество вершин первого типа и через C_2 — множество вершин второго типа.

Пусть пара вершин $c_1 \in C_1$ и $c_2 \in C_2$ соединены таким путём в $g(A)$, что в нём чередуются вершины из C и из $V(g(A)) \setminus C$. Найдутся две вершины $a_i \in V(g(A)) \setminus C$ смежные только с вершинами c_i, $i = 1, 2$. Тогда из C можно удалить чётные вершины этого пути и добавить в C нечётные вершины этого пути, включая a_1 и a_2. Мы получили независимое множество в $g(A)$ на единицу большего размера чем C, что противоречит условию.

Теперь вершины из C можно разбить на три части: C'_1 — те что соединяются чередующимся путём с вершинами из C_1, C'_2 — те что соединяются чередующимся путём с вершинами из C_2 и оставшиеся.

Для каждой вершины $c \in C'_1$ возьмём содержащую её строку и для каждой вершины $c \in C'_2$ возьмём содержащий её столбец. Пусть $X \subset V(g(A))$ множество вершин, покрытых этими линиями. Рассмотрим $a \in V(g(A)) \setminus X$. Имеются смежные с a как по строке так и по столбцу вершины из C, причём по построению обе эти вершины принадлежат множеству $C \setminus (C'_1 \cup C'_2)$, поскольку если одна из них принадлежит C'_i, то и вторая тоже принадлежит C'_i. Для каждой вершины $c \in C \setminus (C'_1 \cup C'_2)$ возьмём, содержащую её строку. Ясно, что выбранные линии в совокупности покрывают $\mathrm{supp}(A)$ и их число равно $|C|$. □

Рассмотрим двудольный граф с долями U и W. Обозначим через $S(U') \subseteq W$ множество вершин смежных с вершинами из $U' \subseteq U$.

Теорема 22 (Ф.Холл). *В двудольном графе с долями U и W найдётся паросочетание мощности $|U|$ тогда и только тогда, когда $|U'| \leq |S(U')|$ для любого $U' \subset U$.*

Сформулируем вариант теоремы Холла для матриц.

Теорема 23 (Ф.Холл). *Пусть A некоторая матрица размера $n_1 \times n_2$. Мощность максимального независимого множества в графе $g(A)$ равна n_1 тогда и только тогда, когда матрица $\mathrm{supp}(A)$ не содержит подматрицы из нулей размера $k_1 \times k_2$, где $k_1 + k_2 > n_2$.*

Эквивалентность формулировок очевидна, если мы рассмотрим $\mathrm{supp}(A)$ как приведённую матрицу смежности двудольного графа. Условие $|U'| \leq$

$|S(U')|$ эквивалентно тому, что для любого набора строк мощности k_1, содержащаяся в этих строках максимальная нулевая подматрица имеет размер $k_1 \times n_2 - |S(U')|$. Теперь докажем теорему.

Доказательство. Пусть в A найдётся подматрица из нулей размера $k_1 \times k_2$ $k_1 + k_2 > n_2$. Тогда в этих k_1 строках можно выбрать не больше $n_2 - k_2 < k_1$ независимых вершин графа $g(A)$.

Рассмотрим максимальную нулевую подматрицу в A размера $k_1 \times k_2$. Тогда минимальное покрытие $\mathrm{supp}(A)$ состоит из $n_1 - k_1 + n_2 - k_2$ линий. Из условия $k_1 + k_2 \leq n_2$ следует, что $n_1 - k_1 + n_2 - k_2 \geq n_1$. Тогда по теореме Эгервари мощность максимального независимого множества в графе $g(A)$ не меньше n_1. □

8.4 Совершенные паросочетания

Определение 38. *Совершенным паросочетанием (1-фактором) в графе (гиперграфе) G называется такой набор рёбер (гиперрёбер), что любая вершина графа G инцидентна ровно одному ребру из этого набора.*

Ясно, что необходимым условием существования совершенного паросочетания в графе является чётность числа вершин графа, а в случае двудольного графа — равенство мощностей долей графа.

Определение 39. 1-*Факторизацией графа G называется разбиение множества рёбер графа на совершенные паросочетания.*

Для существования 1-факторизации графа G необходимо, чтобы граф G был регулярным. Рассмотрим вначале r-регулярный двудольный граф G. Из регулярности следует, что обе доли графа G равны и его приведённая матрица смежности M имеет по r единиц в каждом столбце и каждой строке. Состоящие из единиц диагонали в матрице M соответствуют паросочетаниям в графе G, а правильная раскраска приведённой матрицы смежности в r цветов эквивалентна 1-факторизации графа G. Тогда из теоремы Визинга имеем

Следствие 25. *Регулярный двудольный граф допускает* 1-*факторизацию.*

Перейдём к рассмотрению произвольных, возможно не двудольных, графов. Совершенное паросочетание в графе G соответствует симметричной (относительно главной диагонали) диагонали в его матрице смежности M. Тогда 1-факторизации графа G соответствует симметричная правильная раскраска матрицы смежности графа.

Рассмотрим граф $g(M)$, который является рёберным по отношению к r-регулярному графу G. Из определений видно, что граф $g(M)$ является $2(r-1)$ регулярным и 1-факторизация графа G порождает со-

вершенную раскраску графа $g(M)$ с матрицей параметров $2(J-I) = \begin{pmatrix} 0 & 2 & \dots & 2 \\ 2 & 0 & 2 & \dots \\ \dots & \dots & \dots & \dots \\ 2 & \dots & 2 & 0 \end{pmatrix}$.

8.5 Перманенты и дважды стохастические матрицы

Определение 40. *Перманентом* $\mathrm{per}(A)$ *прямоугольной матрицы* A *размера* $k \times m$, $k \le m$, *называется* $\sum_\sigma a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{k\sigma(k)}$, *где сумма берётся по всем инъективным функциям* $\sigma : \{1, \dots, k\} \to \{1, \dots, m\}$.

Заметим, что $\mathrm{per}(A) = 0$ и $\mathrm{per}(\mathrm{supp}(A)) = 0$ одновременно для любой неотрицательной матрицы A. Если M — приведённая матрица смежности двудольного графа G, то из определений следует, что $\mathrm{per}(M)$ равен числу паросочетаний максимальной возможной мощности k, а если $k = m$, то числу совершенных паросочетаний.

Теорема 24 ([3])**.** *Пусть* M *— матрица смежности графа* G. *Тогда число совершенных паросочетаний в графе* G *не превосходит* $\sqrt{\mathrm{per}(M)}$.

Доказательство. Рассмотрим произвольную пару совершенных паросочетаний в графе G. Порождённый ими однородный подграф степени 2 в графе G, возможно, содержащий кратные рёбра называется 2-фактором. Если 2-фактор состоит только из циклов чётной длины (пару одинаковых рёбер считаем циклом длины 2), то рёбра 2-фактора f можно разделить на 2 совершенных паросочетания $2^{s(f)}$ способами, где $s(f)$ — число циклов длины не менее 4 в 2-факторе f. Если 2-фактор содержит цикл нечётной длины, то его нельзя представить как объединение рёбер двух совершенных паросочетаний. Значит квадрат числа совершенных паросочетаний в графе G равен $\sum_f 2^{s(f)}$, где сумма берётся по всем 2-факторам с чётными циклами.

Рассмотрим произвольную диагональ, состоящую из единиц, в матрице смежности M. Каждая вершина графа смежна двум рёбрам по диагонали: одна единица в строке и другая единица в столбце, соответствующем вершине. Поэтому диагонали из единиц соответствует некоторый 2-фактор в графе G. Причём мы может заменить единицы на симметричные им в любом цикле 2-фактора длины не меньше 3 без изменения 2-фактора. Тогда число диагоналей из единиц — $\mathrm{per}(M)$ не меньше чем $\sum_f 2^{s(f)}$, где сумма берётся по всем 2-факторам f. □

Нетрудно видеть, что для двудольного графа G (с равными по мощности долями) квадратный корень из перманента его матрицы смежности равен перманенту его приведённой матрицы смежности и, следовательно, равен числу совершенных паросочетаний в графе.

Утверждение 48. *Пусть G — двудольный граф и M — его приведённая матрица смежности размера $k \times m$. Тогда число паросочетаний в графе G равно* $\mathrm{per}(A)$*, где $A = (I_k|M)$ — матрица размера $k \times (k+m)$.*

Доказательство. Покажем, что диагоналям из k единиц в матрице A взаимно однозначно соответствуют паросочетания в графе G. Единичная диагональ в матрице A состоит из единиц на частичной диагонали матрицы M, которые задают рёбра графа G, и единиц на главной диагонали матрицы I_k, которые соответствуют вершинам первой доли не инцидентным рёбрам паросочетания. Поскольку каждое ребро двудольного графа инцидентно некоторой вершине первой доли, вершины второй доли, инцидентные рёбрам из паросочетания, заданы частичной диагональю матрицы M. Таким образом, диагональ из k единиц в матрице A определяет одно паросочетание в G. □

Неотрицательная матрица называется дважды стохастической, если сумма её элементов по любой строке и по любому столбцу равняется 1, т. е. сама матрица и результат её транспонирования являются стохастическими одновременно. В частности, дважды стохастическими являются матрицы перестановки

$$P_{ij}(\tau) = \begin{cases} 1, \text{ если } j = \tau(i); \\ 0, \text{ иначе;} \end{cases}$$

содержащие единицы на одной из диагоналей и нули в остальных позициях.

Теорема 25 (Кёниг, Фробениус)**.** *Для любой дважды стохастической матрицы A верно, что* $\mathrm{per}(A) > 0$.

Доказательство. Если для некоторой дважды стохастической матрицы A размера $m \times m$ ровно m элементов отличны от нуля ($|V(g(A))| = m$), то A — матрица перестановки и $\mathrm{per}(A) = 1$. Предположим, что найдутся дважды стохастические матрицы размера $m \times m$ с нулевым перманентом, выберем из них матрицу B, имеющую минимальное число элементов b_{ij}, для которых $0 < b_{ij} < 1$. Как отмечено выше $|V(g(B))| > m$, следовательно найдётся элемент b_{ij} такой, что $0 < b_{ij} < 1$. Для любого элемента $0 < b_{ij} < 1$ найдутся такие соседние элементы, что $0 < b_{i'j} < 1$, $0 < b_{ij'} < 1$, где $i' \neq i$ и $j' \neq j$. Таким образом, степень любой вершины в подграфе графа $g(B)$, состоящим из элементов $0 < b_{ij} < 1$, не меньше двух. Тогда в графе найдётся цикл c чётной длины, в котором чередуются рёбра первого и второго направления. Пусть $\alpha = b_{i_0 j_0} = \min b_{ij} \leq \beta = \min(1 - b_{ij})$, где минимум берётся по всем вершинам цикла c. Рассмотрим матрицу C, которая состоит из нулей, элементов $-\alpha$ в вершинах цикла c, находящихся на чётном (в том числе нулевом) расстоянии по циклу от вершины (i_0, j_0), и элементов α, в вершинах цикла c, находящихся на нечётном

расстоянии от вершины (i_0, j_0). Сумма элементов матрицы C по любому столбцу или строке равна 0. Поэтому матрица $B + C$ — дважды стохастическая. Кроме того, матрица $B + C$ имеет меньше элементов вида $0 < b_{ij} < 1$ чем B, поэтому из $\mathrm{per}(B) = 0$ следует $\mathrm{per}(B + C) = 0$. Пришли к противоречию с минимальным числом элементов вида $0 < b_{ij} < 1$ в матрице B. Случай, когда $\beta < \alpha$, можно рассмотреть аналогично. □

Из теоремы Кёнига—Фробениуса следует, что любая $(0, 1)$-матрица с одинаковым числом единиц в каждой строке и каждом столбце имеет положительный перманент.

Теорема 26 (Биркгоф)**.** *Любая дважды стохастическая матрица является выпуклой комбинацией матриц перестановок.*

Доказательство. Если в некоторой дважды стохастической матрицы A размера $m \times m$ имеется только m ненулевых элементов, то A — матрица перестановки. Предположим найдутся такие дважды стохастические матрицы размера $m \times m$, которые не представимы в виде выпуклой комбинации перестановок. Выберем из них матрицу B, имеющую минимальное число ненулевых элементов. По теореме Кёнига—Фробениуса имеем $\mathrm{per}(B) > 0$, следовательно, найдётся такая диагональ d, что $\alpha = \min\{b_{ij} \mid (i, j) \in d\} > 0$. Рассмотрим матрицу перестановки P, которая имеет единицы на диагонали d. Тогда матрица $\frac{1}{1-\alpha}(B - \alpha P)$ является дважды стохастической и имеет меньше ненулевых элементов, чем B. По предположению найдутся $\beta_i > 0$, матрицы перестановок P_i, для которых $\frac{1}{1-\alpha}(B - \alpha P) = \sum \beta_i P_i$. Тогда $B = \alpha P + (1 - \alpha) \sum \beta_i P_i$. Пришли к противоречию. □

8.6 Симметричные латинские квадраты

Рассмотрим Q_q — полный граф на q вершинах.

Утверждение 49. *Если q — чётное, то 1-факторизация графа Q_q эквивалентна симметричному латинскому квадрату порядка q с нулями на главной диагонали.*

Доказательство. Рассмотрим 1-факторизацию графа Q_q. Ребру e соответствует пара симметрично расположенных единиц в матрице смежности графа Q_q, заменим их символами i, если ребро e содержится в i-ом 1-факторе. Получится симметричная матрица порядка q, у которой в каждой строке и каждом столбце однократно присутствуют символы $0, 1, \ldots, q - 1$, поскольку любая вершина инцидентна ровно одному ребру из каждого 1-фактора. Ясно, что обратив эти рассуждения можно получить 1-факторизацию полного графа из симметричного латинского квадрата с нулями по главной диагонали. □

1-Факторизацию графа Q_q можно использовать как расписание спортивного турнира: участникам турнира соответствуют вершины графа, если ребро $\{u, v\}$ графа Q_q содержится в i-ом паросочетании, то участники u и v встречаются в i-ом туре.

Определение 41. *Квазигруппу $f : Q_q^2 \to Q_q$ и её таблицу Кэли (латинский квадрат) будем называть идемпотентными, если $f(a, a) = a$ для любого $a \in Q_q$. Квазигруппу $f : Q_{2q}^2 \to Q_{2q}$ и её таблицу Кэли (латинский квадрат) будем называть полуидемпотентными, если $f(a, a) = a$ для любого $a \in Q_q$ и $f(a, a) = a - q$ для любого $a \in Q_{2q} \setminus Q_q$.*

Докажем существование 1-факторизации полного графа чётного порядка, а также существование 1-факторизации полного графа нечётного порядка с петлями.

Теорема 27 ([82]). 1) *Для любого чётного $q \geq 2$ найдётся 1-факторизация графа Q_q и полуидемпотентный симметричный латинский квадрат порядка q.*
2) *Для любого нечётного $q \geq 1$ найдётся идемпотентный симметричный латинский квадрат порядка q.*

Доказательство. Будем обозначать через $A_q[Q]$ симметричный латинский квадрат порядка q в алфавите Q с одинаковыми символами по главной диагонали, через $B_q[Q]$ — симметричный полуидемпотентный латинский квадрат порядка q в алфавите Q, через $C_q[Q]$ — симметричный идемпотентный латинский квадрат порядка q в алфавите Q.

Построим латинские квадраты $A_q[Q]$, $B_q[Q]$ для чётных q и $C_q[Q]$ для нечётных q по индукции. Имеем $A_2[Q_2] = B_2[Q_2] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $C_3[Q_3] = \begin{pmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}$. Пусть уже построены $A_{2q}[Q_{2q}]$, $B_{2q}[Q_{2q}]$ и $C_{2q+1}[Q_{2q+1}]$. Тогда

$$A_{4q}[Q_{4q}] = \begin{pmatrix} A_{2q}[Q_{2q}] & A_{2q}[Q_{4q} \setminus Q_{2q}] \\ A_{2q}[Q_{4q} \setminus Q_{2q}] & A_{2q}[Q_{2q}] \end{pmatrix},$$

$$B_{4q+2}[Q_{4q+2}] = \begin{pmatrix} C_{2q+1}[Q_{2q+1}] & C_{2n+1}[Q_{4q+2} \setminus Q_{2q+1}] \\ C_{2q+1}[Q_{4q+2} \setminus Q_{2q+1}] & C_{2q+1}[Q_{2q+1}] \end{pmatrix}.$$

Рассмотрим произвольный латинский квадрат E порядка $2q + 1$ в алфавите Q_{2q+1} с нулями на главной диагонали. В латинском квадрате

$$\begin{pmatrix} C_{2q+1}[Q_{4q+2} \setminus Q_{2q+1}] & E \\ E^{\mathrm{T}} & C_{2q+1}[Q_{4q+2} \setminus Q_{2q+1}] \end{pmatrix}$$

поменяем местами главные диагонали подквадратов $C_{2q+1}[Q_{4q+2} \setminus Q_{2q+1}]$ и подквадратов E, E^{T}. Получим латинский квадрат $A_{4q+2}[Q_{4q+2}]$.

В латинском квадрате

$$\begin{pmatrix} B_{2q}[Q_{2q}] & B_{2q}[Q_{4q} \setminus Q_{2q}] \\ B_{2q}[Q_{4q} \setminus Q_{2q}] & B_{2q}[Q_{2q}] \end{pmatrix}$$

поменяем местами вторые половины главных диагоналей в подквадратах $B_{2q}[Q_{2q}]$ и $B_{2q}[Q_{4q} \setminus Q_{2q}]$. Получим латинский квадрат $B_{4q}[Q_{4q}]$.

Осталось построить латинские квадраты $C_{4q+1}[Q_{4q+1}]$ и $C_{4q-1}[Q_{4q-1}]$. В латинском квадрате $A_{4q}[Q_{4q}]$ можно так переименовать символы, чтобы в первой строке и первом столбце символы шли в порядке возрастания. После переименования в квадрате $A_{4q}[Q_{4q}]$ заменим 0 в позиции (i, i) на элемент i для всех $i \in Q_{4q}$. Удалив из квадрата первую строку и первый столбец, получим латинский квадрат $C_{4q-1}[Q_{4q} \setminus \{0\}]$. Теперь достаточно переименовать символы для получения латинского квадрата $C_{4q-1}[Q_{4q-1}]$. Аналогичным образом, из латинского квадрата $A_{4q+2}[Q_{4q+2}]$ получается латинский квадрат $C_{4q+1}[Q_{4q+1}]$. Таким образом, индукционный шаг доказан. □

Задача 61. Докажите, что в любом двудольном графе есть паросочетание, рёбра которого инцидентны всем вершинам максимальной степени.

Задача 62. Докажите, что дважды стохастическая матрица размера $n \times n$ не содержит нулевой подматрицы размера $m_1 \times m_2$, где $m_1 + m_2 > n$.

Задача 63. Докажите, что неотрицательная матрица размера $n \times n$ имеет нулевой перманент тогда и только тогда, когда у неё найдётся нулевая подматрица размера $m_1 \times m_2$, где $m_1 + m_2 > n$.

Задача 64. [68] Пусть $(0, 1)$-матрица A размера $m \times n$ содержит по ka единиц в каждой строке и по kb единиц в каждом столбце, где $k > 0$ — целое. Докажите, что в матрице A можно выбрать по a единиц в каждой строке так, что в каждом столбце окажется выбрано по b единиц.

Задача 65. [68] Докажите, что в любой двудольный граф можно добавить рёбра и вершины в одну из долей так, чтобы максимальная степень вершин графа не увеличилась и получившийся двудольный граф был регулярным.

Задача 66. Докажите, что для любого регулярного графа найдётся накрывающий его граф, который имеет 1-факторизацию.

Задача 67. Докажите, что любой частичный латинский квадрат порядка q, т. е. квадрат размера $q \times q$, в котором часть ячеек заполнена не более чем q различными элементами и одинаковые элементы не встречаются в одной строке или столбце, дополняется до латинского квадрата порядка $2q$.

9 МДР-коды с кодовым расстоянием большим чем 2

9.1 Основные свойства МДР-кодов

Пусть $C \subseteq Q_q^n$. Кодовым расстоянием множества (кода) C называется $d_C = \min\limits_{x,y \in C, x \neq y} d(x,y)$.

Определение 42. *Множество $C \subset Q_q^n$ называется* МДР-*кодом*[25] *с расстоянием d, если $|C \cap \Gamma| = 1$ для любой $(d-1)$-мерной грани $\Gamma \subset Q_q^n$.*

Как было указано выше (см. пример 19), при кодовом расстоянии $d = 2$ характеристическая функция МДР-кода в Q_q^n является совершенной раскраской в два цвета с матрицей параметров $\begin{pmatrix} n & n(q-2) \\ 0 & n(q-1) \end{pmatrix}$. Нетривиальное собственное число этой матрицы $\lambda = -n$ является минимальным собственным числом n-мерного гиперкуба.

Рассмотрим гиперграф, гиперрёбрами которого являются грани гиперкуба размерности $d-1$, а вершинами — вершины гиперкуба. Непосредственно из определений вытекает, что МДР-код с растоянием d эквивалентен трансверсали этого гиперграфа.

Из определения МДР-кода следует следующее утверждение, известное как граница Синглтона.

Утверждение 50.
(a) *Для любого $C \subseteq Q_q^n$ верно неравенство $|C| \leq q^{n-d_C+1}$.*
(b) *Код C с расстоянием d_C является* МДР-*кодом тогда и только тогда, когда $|C| = q^{n-d_C+1}$.*

Доказательство. Пункт (a) следует из того, что в грани размерности $d_C - 1$ содержится не более одного кодового слова и что гиперкуб Q_q^n является объединением q^{n-d_C+1} непересекающихся граней размерности $d_C - 1$.

(b) Если множество C является МДР-кодом, то оно содержит ровно по одному элементу в каждой из q^{n-d_C+1} непересекающихся граней размерности $d_C - 1$. Если $|C| = q^{n-d_C+1}$, то для любого направления граней в каждой грани размерности $d_C - 1$ имеется кодовая вершина. □

Определение 43. *Ретрактом множества $C \subset Q_q^n$ по m-мерной грани Γ называется подмножество $C[\Gamma]$ гиперкуба Q_q^m, состоящее из всех наборов $v \in \Gamma \cap C$, из которых удалены все фиксированные в грани Γ координаты.*

[25] Аббревиатуру МДР-код можно расшифровывать как "код с максимальным достижимым расстоянием" или "разделимый код с максимальным расстоянием" от английского "maximum distance separable code" (MDS code).

Таким образом, характеристическая функция $\chi_{C[\Gamma]}$ есть сужение функции χ_C на грань Γ.

Определение 44. *Проекцией множества $C \subset Q_q^n$ на m-мерную грань Γ называется подмножество гиперкуба Q_q^m, состоящее из всех наборов $v \in C$, из которых удалены все фиксированные в грани Γ координаты.*

Таким образом, проекция на грань есть объединение ретрактов по всем граням того же направления. Код, соответствующий ретракту кода, называется выколотым, а соответствующий проекции — укороченным. Свойство быть МДР-кодом сохраняется при переходе к ретрактам и проекциям.

Утверждение 51. *Подмножество гиперкуба Q_q^n является* МДР-*кодом с расстоянием d ($2 \le d \le n-1$) тогда и только тогда, когда*

(a) *все его ретракты размерности не меньше d являются* МДР-*кодами с расстоянием d; или*

(b) *все его проекции на грани фиксированной размерности m, $m \ge n-d+1$, являются* МДР-*кодами с расстоянием $d-n+m$.*

Доказательство. (a) Определение МДР-кода эквивалентно тому, что для любой грани размерности не меньше d любая её подграань размерности $d-1$ содержит одну кодовую вершину.

(b) Следует из утверждения 50. Действительно, при проекции на грань размерности m в одну точку переходят все вершины грани размерности $n-m$. Если $n-m \le d-1$, то мощность проекции равна мощности кода, а кодовое расстояние уменьшается не более чем на $n-m$. Из утверждения 50(a) следует, что при проекции кодовое расстояние уменьшилось ровно на $n-m$ и по утверждению 50(b) проекция есть МДР-код. Наоборот, если проекция на некоторую грань размерности m есть МДР-код с расстоянием $d-n+m$, то в каждой грани гиперкуба размерности $d-1$, содержащей все направления по которым происходит проекция, есть кодовые вершины. Из произвольности направления грани, на которую осуществляется проекция, следует, что любая грань размерности $d-1$ содержит кодовую вершину. Если бы в коде имелись две вершины на расстоянии $d' < d$, то нашлась бы проекция, с меньшим кодовым расстоянием, чем требуется в МДР-коде. □

Утверждение 52. *Пусть $C \subset Q_q^n$ — МДР-код с расстоянием d_C и $d_C \ge 3$. Тогда $|C| \le q^{q-1}$ и $n \le q + d_C - 2$.*

Доказательство. По утверждению 51 найдётся проекция C' МДР-кода C на грань размерности $m = n - d_C + 3$ с кодовым расстоянием 3. Имеем $|C'| = |C| = q^{n-d_C+1} = q^{m-2}$. Граница Хэмминга мощности кода утверждает, что произведение мощности кода на мощность шара не меньше мощности гиперкуба, т. е. $|C'|(m(q-1)+1) \le q^m$. Тогда $q^2 \ge m(q-1)+1$. Откуда получаем $m \le q+1$ и $n \le q + d_C - 2$. □

9.2 Ортогональные системы квазигрупп

Определение 45. *Функция $f : Q_q^n \to Q_q$ называется n-арной квазигруппой*[26] *порядка q, если $f(x) \neq f(y)$ при $d(x, y) = 1$.*

Определённое выше понятие квазигруппы совпадает с понятием 2-арной квазигруппы.

Пример 27. Пусть $\circ$ — групповая операция на множестве Q_q. Тогда функция $f(x_1, \ldots, x_n) = x_1 \circ \cdots \circ x_n$ является n-арной квазигруппой, а именно n-арной итерированной группой.

Из определения легко видеть, что n-арная квазигруппа является совершенной раскраской с матрицей параметров $n(J-I) = \begin{pmatrix} 0 & n & n & \ldots & n \\ n & 0 & n & \ldots & n \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ n & n & \ldots & n & 0 \end{pmatrix}$ с единственным нетривиальным собственным числом $\lambda = -n$. Заметим, что каждый цвет раскраски, заданный n-арной квазигруппой является МДР-кодом с расстоянием 2. Кроме того, график n-арной квазигруппы, т. е. множество $\{\overline{x} \in Q_q^{n+1} \mid x_{n+1} = f(x_1, \ldots, x_n)\}$ является МДР-кодом в Q_q^{n+1}.

Определение 46. *Таблица Кэли значений n-арной квазигруппы называется латинским n-кубом, а при $n = 2$ — латинским квадратом.*

Любой МДР-код с большим расстоянием также можно представить как множество решений системы уравнений из нескольких m-арных квазигрупп [31]. Действительно, рассмотрим МДР-код длины n с расстоянием d. По определению МДР-кода в каждой грани гиперкуба размерности $n - m = d - 1$ имеется ровно одна точка МДР-кода, например, первые m координат однозначно определяют $(n-m)$-мерную грань и, следовательно, оставшиеся $n-m$ координат. Значит, МДР-код является множеством решений системы уравнений

$$x_{m+1} = f_1(x_1, \ldots, x_m), \ldots, x_n = f_{n-m}(x_1, \ldots, x_m). \tag{14}$$

Из определения МДР-кода нетрудно видеть, что функции $f_1, \ldots, f_{n-m}$ являются m-арными квазигруппами. Поскольку координаты равноправны, не только первые m, но и любые m координат определяют оставшиеся из системы уравнений вида (14), но с другими функциями.

Если множество решений некоторой системы (14) является МДР-кодом, то набор m-арных квазигрупп $f_1, \ldots, f_{n-m}$ называется *ортогональным*. Из утверждения 51(а) следует, что любой поднабор ортогонального набора тоже является ортогональным.

[26] Точнее n-арной квазигруппой называется пара из n-местной операции и множества элементов, на котором она действует (в данном случае Q_q).

МДР-коды применяются в различных алгоритмах обработки информации. Рассмотрим задачу передачи сообщения по каналу связи со стиранием, т. е. при передаче сообщение $(a_1, a_2, \ldots, a_n)$ преобразуется в сообщение вида $(a_1, *, a_3, \ldots, *, \ldots, a_n)$, где символ $*$ заменяет утраченную букву. Предположим, что мы передаём в качестве кодовых слов элементы МДР-кода с расстоянием d, тогда мы можем восстановить $d-1$ утраченную букву. Конечно, любой код с расстоянием d содержит не более одного элемента в грани размерности меньше чем d и позволяет восстанавливать $d-1$ стёртую букву, но наличие ровно одной буквы в каждой грани взято в качестве определения МДР-кода. Рассмотрим задачу распределённого хранения информации. Пусть информация хранится на n серверах и нужно уметь восстанавливать всю информацию при потере менее d серверов. В этом случае, информацию удобно представлять в виде слов некоторого МДР-кода с расстоянием d так, что i-ый символ кодового слова хранится на i-ом сервере. Тогда потеря $d-1$ серверов эквивалентна стиранию $d-1$ буквы в каждом кодовом слове. Значит информация может быть полностью восстановлена после потери менее d серверов.

Кроме того, МДР-код можно использовать для решения задачи разделения ключа. Задача состоит в следующем. Пусть имеется коллектив из $n-1$ участников. Требуется так разделить между участниками информацию о секретном ключе, чтобы любые m участников вместе могли узнать секретный ключ, а любые $m-1$ участников не только не могли, но и даже не имели бы никакой информации о секретном ключе.

Пусть имеется МДР-код длины n с кодовым расстоянием $n-m+1$. Сам МДР-код считается общеизвестным. Рассмотрим произвольное кодовое слово $(a_1, a_2, \ldots, a_n)$. В качестве индивидуального ключа i-го участника возьмём $a_i \in Q_q$, а в качестве секретного ключа $a_n \in Q_q$. Какой бы ни была группа из m участников мы можем представить МДР-код как решение системы уравнений вида (14) именно от переменных этой группы и вычислить все остальные координаты a_j вершины МДР-кода, в частности, a_n. Если в группе только $m-1$ участник, то известны значения только $m-1$ переменной. Тогда m-арная квазигруппа $f_{n-m}(x_1, \ldots, x_m) = x_n$ принимает по одному разу все возможные q значений в зависимости от остающейся неизвестной переменной.

Пара таблиц Кэли (латинских квадратов) 2-квазигрупп f и g называется ортогональной, если все пары $(f(x_1, x_2), g(x_1, x_2))$, $(x_1, x_2) \in Q_q^2$, различны. Таким образом, система попарно ортогональных латинских квадратов[27] является частным случаем ортогонального набора квазигрупп. В зависимости от числа переменных m система ортогональных m-арных квазигрупп называется системой ортогональных латинских квадратов, ортогональных латинских кубов или гиперкубов.

[27] Называемая также система MOLS (mutually orthogonal latin squares).

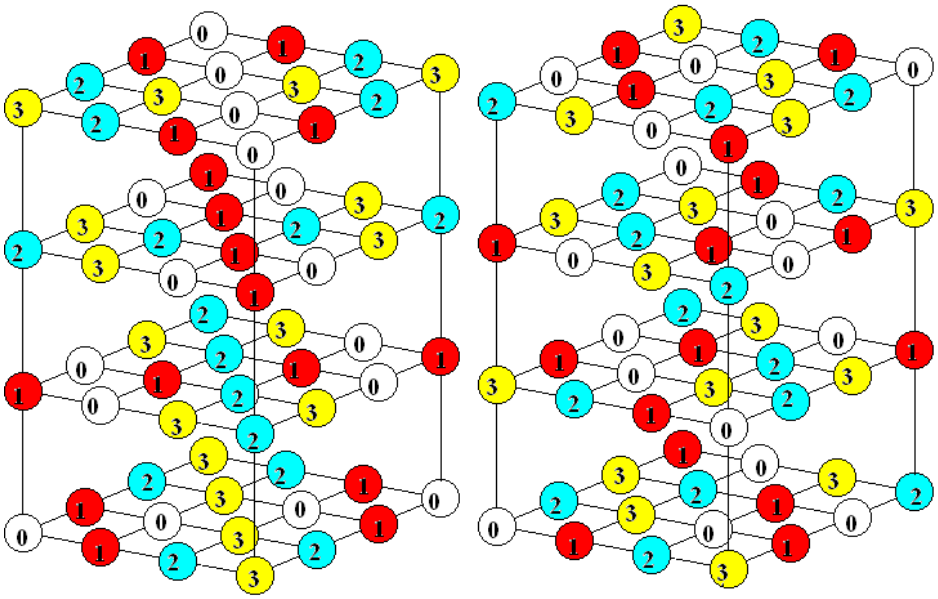
Пример 28. Попарно ортогональные латинские квадраты порядка 4.

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

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

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

Пример 29. Ортогональные латинские кубы порядка 4.



Пусть K — абелева группа порядка q. Рассмотрим набор перестановок $\pi_1, \ldots, \pi_k$ на q элементах, удовлетворяющий условию: разность $\pi_i - \pi_j$ (в группе K) является перестановкой при всех $i \neq j$.

Утверждение 53. *Набор функций $f_i(x, y) = x + \pi_i(y)$, $i = 1, \ldots, k$, является ортогональным.*

Доказательство. Достаточно проверить, что для любых $i \neq j$ все q^2 пар $(f_i(x, y), f_j(x, y))$ различны. Пусть $f_i(x_1, y_1) = f_i(x_2, y_2)$ и $f_j(x_1, y_1) = f_j(x_2, y_2)$. Тогда $f_i(x_1, y_1) - f_j(x_1, y_1) = f_i(x_2, y_2) - f_j(x_2, y_2)$. Имеем $(\pi_i - \pi_j)(y_1) = (\pi_i - \pi_j)(y_2)$. По условию $(\pi_i - \pi_j)$ — перестановка. Тогда $y_1 = y_2$. Из уравнения $f_i(x_1, y_1) = f_i(x_2, y_1)$ получаем, что $x_1 = x_2$. □

Утверждение 54. *Если $f_1, \ldots, f_m$ — система попарно ортогональных латинских квадратов (2-квазигрупп) на Q_q, то $m \leq q - 1$.*

Доказательство. Без ограничения общности можно считать, что первые строки ($x_1 = 0$) всех ортогональных квадратов одинаковы и $f_i(0, 0) = 0$ для любого $i \in \{1, \ldots, m\}$. Это значит, что в каждой паре латинских квадратов уже использованы все пары вида (i, i). Тогда элементы $f_i(1, 0)$

должны быть ненулевыми и различными для всех $i \in \{1, \ldots, m\}$, т. е. $m \leq q - 1$. □

Из приведённого выше доказательства имеем

Следствие 26. *Пусть $C \subset Q_q^{q+1}$ — МДР-код с расстоянием q, тогда код не содержит вершин на расстоянии $q + 1$.*

Доказательство. МДР-код с такими параметрами эквивалентен системе попарно ортогональных латинских квадратов. Изометриями гиперкуба любую вершину кода можно перевести в вершину $\bar{0}$ и добиться, чтобы все первые строки соответствующих латинских квадратов были одинаковыми. Из доказательства предыдущего утверждения видно, что вершины вида $(i, \ldots, i)$ не содержатся в C, поскольку $(0, i, \ldots, i) \in C$ для любого $i = 0, \ldots, q - 1$. Значит в C нет вершин на расстоянии $q + 1$ от вершины $\bar{0}$. □

Утверждение 55. *Для любого* МДР-*кода $C \subset Q_q^n$ с расстоянием d_C и $n > d_C \geq 3$ справедливы неравенства $d_C \leq q$ и $n \leq 2q - 2$.*

Доказательство. Рассмотрим МДР-код C длины n с расстоянием $d_C = m+1$ и $m \geq 2$, $n \geq m+2$. Ему соответствует ортогональная система $(n-m)$-арных квазигрупп $f_1, \ldots, f_m$. По утверждению 51 любому ретракту кода C размерности $m+2$ соответствует ортогональная система, которая является системой из m попарно ортогональных латинских квадратов. Тогда из утверждения 54 имеем $m \leq q - 1$ и из утверждения 52 имеем $n \leq q + d_C - 2 \leq 2q - 2$. □

При $q = 2$ из утверждения 55 вытекает

Следствие 27. *Для любого n в булевом гиперкубе Q_2^n нет* МДР-*кодов с расстоянием d при $2 < d < n$.*

Таким образом, МДР-коды фиксированного порядка q неограниченной длины n существуют только при для кодовых расстояний 2 и n. МДР-кодам с кодовым расстоянием 2 соответствуют латинские гиперкубы, а МДР-код в гиперкубе Q_q^n с расстоянием n является диагональю гиперкуба.

Определение 47. *Трансверсалью латинского гиперкуба, в частности, латинского квадрата, называется диагональ гиперкуба, состоящая из попарно различных элементов.*

Ясно, что для латинского квадрата найдётся ортогональный латинский квадрат тогда и только тогда, когда он разбивается на трансверсали. А для латинского гиперкуба необходимым условием для существования ортогонального ему латинского гиперкуба является разбиение на трансверсали всех латинских квадратов в его двумерных гранях, а не разбиение на трансверсали самого гиперкуба.

Утверждение 56. *Пусть q и n — чётные, тогда латинский гиперкуб, заданный равенством $f(x_1, \ldots, x_n) = x_1 + \cdots + x_n \mod q$ не имеет трансверсалей.*

Доказательство. Имеем $\sum\limits_{j=0}^{q-1} j = \frac{q(q-1)}{2} \mod q$. Пусть латинский гиперкуб содержит трансверсаль $y^0, y^1, \ldots, y^{q-1} \in Q_q^n$. Тогда

$$\sum_{i=1}^{n}\sum_{j=0}^{q-1} y_i^j = \sum_{i=1}^{n} \frac{q(q-1)}{2} = q\frac{n(q-1)}{2} = 0 \mod q.$$

В то время как

$$\sum_{j=0}^{q-1} f(y^j) = \sum_{j=0}^{q-1} j = \frac{q(q-1)}{2} \neq 0 \mod q.$$

Пришли к противоречию с равенством, которое определяет латинский гиперкуб. □

Замечание 11. Известна гипотеза Райзера о том, что любой латинский квадрат нечётного порядка имеет трансверсаль. Я.Уонлес [99] обобщил эту гипотезу на латинские гиперкубы нечётных порядков. Из утверждения 56 ясно, что не все латинские квадраты чётного порядка содержат трансверсаль. Однако, можно ставить вопрос о наличии в латинских квадратах частичной трансверсали как можно большей длины. Монтгомери [74] доказал, что латинские квадраты достаточно большого чётного порядка q содержат частичную трансверсаль длины $q - 1$.

9.3 Линейные МДР-коды

Перейдём к способам построения МДР-кодов. Вначале будем строить линейные коды над полем $GF(q)$, где q — степень простого числа. Гиперкуб Q_q^n теперь будем рассматривать как n-мерное векторное пространство над полем $GF(q)$. В этом смысле к подмножествам гиперкуба применяются понятия линейности, аффинной оболочки, размерности и т.п.

Определение 48. *Рангом кода называется размерность аффинной оболочки кода.*

Для линейного МДР-кода $C \subset (GF(q))^n$ с расстоянием d ранг равен $r = n - d + 1$. Из утверждения 52 замечаем, что ранг линейного МДР-кода с расстоянием большим чем 2 не превосходит $q - 1$.

Будем использовать представление линейного МДР-кода в виде решения системы линейных уравнений.

Утверждение 57. *Множество решений системы линейных (над $GF(q)$) уравнений $C = \{x \in (GF(q))^n \mid Ax = \bar{0}\}$, где A — матрица размера $r \times n$, $n > r$, является* МДР-*кодом ранга $n - r$ с кодовым расстоянием $d = r + 1$ в $(GF(q))^n$ тогда и только тогда, когда любые r столбцов матрицы $A = \{a_{ij}\}$ образуют невырожденную матрицу.*

Доказательство. Любой линейный код является множеством решений системы линейных уравнений. Достаточно заметить, что любая грань размерности r в $(GF(q))^n$ содержат ровно одну точку кода C тогда и только тогда, когда соответствующий минор в матрице A не равен 0, т. е. любой набор из r столбцов матрицы A является линейно независимым базисом. □

Матрица A называется проверочной для кода C. Определим код $C^\perp = \{x \in GF(q))^n : \sum_i x_i y_i = 0$ для всех $y \in C\}$, который называется дуальным[28] над $GF(q)$ к коду C.

Из утверждения 57 и определения МДР-кода следует

Утверждение 58. *Пусть $C \subset (GF(q))^n$ — линейный* МДР-*код ранга $n - r$, тогда $C^\perp$ — линейный* МДР-*код ранга r.*

Доказательство. Пусть $C = \{x \in (GF(q))^n \mid Ax = \bar{0}\}$, где A — матрица размера $r \times n$ и линейные комбинации строк матрицы A образуют код $C^\perp$. Рассмотрим некоторый набор из r координат кодовых слов кода $C^\perp$. Любой набор из r столбцов матрицы A, в частности, соответствующий этим координатам, является базисом. Тогда для любого $u \in (GF(q))^r$ в коде $C^\perp$ имеется ровно один вектор, содержащий набор u в этих координатах. Таким образом, множество $C^\perp$ является линейным МДР-кодом ранга r. □

Следствие 28. *В $(GF(q))^n$ линейные* МДР-*коды с расстоянием d и $n - d + 2$ существуют одновременно.*

Утверждение 59. *Если $q = p^s$ — степень простого числа, то в $(GF(q))^{q+1}$ имеются линейные* МДР-*коды с расстоянием d, для любого d, $3 \le d \le q$.*

Доказательство. Матрица $V_r = \begin{pmatrix} 0 & 1 & 1 & 1 & \dots & 1 \\ 0 & 0 & 1 & 2 & \dots & q-1 \\ 0 & 0 & 1 & 2^2 & \dots & (q-1)^2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 0 & 1 & 2^{r-1} & \dots & (q-1)^{r-1} \end{pmatrix}$ удовлетворяет условиям утверждения 57 при $r < q$, поскольку любые её миноры порядка r ненулевые. Точнее любые r из последних $q-1$ столбцов матрицы составляют определитель Вандермонда, а другие наборы

[28] В разделе 13.1 будут рассмотрены коды дуальные над кольцом $\mathbb{Z}_q$. Эти понятия дуальности совпадают в случае простого q.

из r столбцов можно выразить с помощью определителя Вандермонда меньшего порядка. □

Из утверждения 57 имеем

Следствие 29. *Если $q \neq 2$, $q = p^s$ — степень простого числа, то имеется система $f_1, \ldots, f_{q-1}$ попарно ортогональных 2-квазигрупп (латинских квадратов) порядка q.*

Доказательство. Достаточно рассмотреть набор 2-квазигрупп вида $f_i(x_1, x_2) = x_1 + ix_2$, $i \in GF(q)$, $i \neq 0$, где операции выполняются в поле $GF(q)$. Искомый код есть множество решений системы уравнений $x_{i+2} = f_i(x_1, x_2)$, $i \in GF(q)$, $i \neq 0$. □

Утверждение 60. *Пусть $q = 2^t$, $t \geq 2$, $n = q + 2$. Существует линейный* МДР*-код $C \subset (GF(2^t))^n$ ранга $n - 3$.*

Доказательство. Заметим, что $a^2 - b^2 = (a - b)^2$ в $GF(2^t)$, т. е. $a^2 \neq b^2$ при $a \neq b$. Нетрудно проверить, что все миноры размерности 3 матрицы $\begin{pmatrix} 1 & 0 & 0 & 1 & \ldots & 1 \\ 0 & 1 & 0 & 2 & \ldots & q-1 \\ 0 & 0 & 1 & 2^2 & \ldots & (q-1)^2 \end{pmatrix}$ не равны нулю. Тогда требуемое следует из утверждения 57. □

Построенные в утверждении 60 МДР-коды называют *астурийскими.*

Замечание 12. С.Бол [7] доказал, что если q — простое, то длина линейного МДР-кода не превосходит $q+1$ (когда $q = 2^t$, $t > 1$, длина линейного МДР-кода не превосходит $q + 2$) за исключением случаев, когда кодовое расстояние равно 2 или длине кода.

Результат С.Бола усиливает утверждение 55 для линейных кодов. Известна гипотеза о том, что аналогичное утверждение верно для произвольных МДР-кодов при $q \neq 2^t$. В частности, Е.Беспалов [9] доказал, что при нечётном q не существует МДР-кодов длины $q + 2$ и более с кодовым расстоянием 4.

Пусть α — примитивный элемент в поле $GF(q)$. Рассмотрим матрицу

$$A = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \alpha & \alpha^2 & \ldots & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & \ldots & \alpha^{2(q-2)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha^r & \alpha^{2r} & \ldots & \alpha^{r(q-2)} \end{pmatrix}.$$

Любой набор из $r + 1$ ($r < q - 2$) столбцов матрицы A представляет собой матрицу Вандермонда. По утверждению 57 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 утверждению 57 является МДР-кодом длины $q-1$ с расстоянием $r+1$.

Особенно полезными для приложений являются коды Рида—Соломона над полем $GF(2^t)$. В частности, при $t=8$ элементами алфавита являются байты. При длине 2^t-1 и расстоянии $r+1$ код может исправить до $r/2$ испорченных символов — двоичных блоков длины t. Код Рида—Соломона используется в контроллерах оперативной памяти, при записи информации на жесткие диски и на CD/DVD диски.

9.4 Системы попарно ортогональных латинских квадратов

Рассмотрим построение МДР-кодов в гиперкубах, порядок которых не является степенью простого числа. Если $x \in Q_q$, а $y \in Q_p$, то пару (x,y) можно рассматривать как элемент множества Q_{pq}. Следующая теорема утверждает, что произведение МДР-кодов над алфавитами Q_p и Q_q есть МДР-код над алфавитом Q_{pq}.

Теорема 28 (МакНиш). *Если множества $M_1 \subset Q_q^n$ и $M_2 \subset Q_p^n$ являются* МДР-*кодами с расстоянием d, то множество*

$$M = \{(x,y) = ((x_1,y_1),\ldots,(x_n,y_n)) \mid x \in M_1, y \in M_2\}$$

также является МДР-*кодом с расстоянием d в Q_{pq}^n.*

Доказательство. Из условия теоремы и утверждения 50 следует, что $|M| = q^{n-d+1}p^{n-d+1}$. Осталось доказать, что в множестве M нет элементов на расстоянии меньше d. Если такая пара элементов есть в M, то их первые компоненты x и x' находятся на расстоянии меньше d. Поскольку x и x' содержатся в коде M_1, они совпадают. Аналогично совпадают и вторые компоненты y и y'. Пришли к противоречию. □

Замечание 13. П.Киваш [52] доказал, что для любого фиксированого $n \in \mathbb{N}$ и кодового расстояния $d \le n$ найдётся такое $q_0 \in \mathbb{N}$, что при $q \ge q_0$ в гиперкубе Q_q^n найдётся МДР-код с расстоянием d.

В частном случае при $d = n-1$ это означает, что для любого k найдётся такое $q_0(k) \in \mathbb{N}$, что при $q \ge q_0(k)$ имеется система из k ортогональных латинских квадратов порядка q. Р.Боуз, Э.Паркер и С.Шрикханде доказали, что $q_0(2) = 7$, точнее при любом $q \ne 2,6$ найдётся пара ортогональных латинских квадратов. Для доказательства этой теоремы нам понадобится несколько вспомогательных утверждений.

Утверждение 61. *Пусть число k имеет следующее разложение в произведение простых: $k = 2^{\delta_1}3^{\delta_2}\cdots p_i^{\delta_i}\cdots$. Тогда имеется система из $\min\limits_{i,\delta_i\ne 0}(p_i^{\delta_i}-1)$ попарно ортогональных латинских квадратов порядка k.*

Доказательство. Из следствия 29 получаем, что имеется система из $p_i^{\delta_i} - 1$ попарно ортогональных латинских квадратов порядка $p_i^{\delta_i}$. Из теоремы 28 следует, что если имеются системы из m попарно ортогональных латинских квадратов порядка k_1 и k_2, то имеется система из m попарно ортогональных латинских квадратов порядка k_1k_2. □

Следствие 30. *Если $k \not\equiv 2 \mod 4$, то имеется пара ортогональных латинских квадратов порядка k.*

Лемма 3 ([29]). *Пусть имеются пары ортогональных латинских квадратов порядков k_1, k_1+1, k_3 и три попарно ортогональных латинских квадрата порядка k_2, $k_2 \geq k_3$. Тогда имеется пара ортогональных латинских квадратов порядка $k_1k_2 + k_3$.*

Доказательство. Пусть $f_i : Q_{k_2}^2 \to Q_{k_2}$, $i = 1, 2, 0$, — три попарно ортогональных латинских квадрата порядка k_2; $g_i : Q_{k_1}^2 \to Q_{k_1}$, $i = 1, 2$, — пара ортогональных латинских квадрата порядка k_1; $h_i : (Q_{k_1} \cup \{q\})^2 \to Q_{k_1} \cup \{q\}$, $i = 1, 2$, — пара ортогональных латинских квадрата порядка $k_1 + 1$ таких, что $h_1(q, q) = h_2(q, q) = q$; $t_i : Q_{k_3}^2 \to Q_{k_3}$, $i = 1, 2$, — пара ортогональных латинских квадрата порядка k_3.

Алфавит R мощности $k_1k_2 + k_3$ представим в виде $(Q_{k_1} \times Q_{k_2}) \cup Q_{k_3}$, где $Q_{k_3} = \{q_0, \ldots, q_{k_3-1}\}$. Определим пару ортогональных латинских квадратов F_1, F_2 в алфавите R по следующему правилу.

Если $x_1, x_2 \in Q_{k_1}$, $y_1, y_2 \in Q_{k_2}$ и $f_0(y_1, y_2) \geq k_3$, то $F_i((x_1, y_1), (x_2, y_2)) = (g_i(x_1, x_2), f_i(y_1, y_2))$, $i = 1, 2$.

Если $x_1, x_2 \in Q_{k_1}$, $y_1, y_2 \in Q_{k_2}$ и $f_0(y_1, y_2) < k_3$, то при $h_i(x_1, x_2) \neq q$ определим $F_i((x_1, y_1), (x_2, y_2)) = (h_i(x_1, x_2), f_i(y_1, y_2))$, $i = 1, 2$, а при $h_i(x_1, x_2) = q$ определим $F_i((x_1, y_1), (x_2, y_2)) = q_j$, где $j = f_0(y_1, y_2)$. Заметим, что по определению $h_1(x_1, x_2)$ и $h_2(x_1, x_2)$ не могут равняться q одновременно.

Если $x_1 \in Q_{k_1}$, $y_1 \in Q_{k_2}$ и $q_j \in \{q_0, \ldots, q_{k_3-1}\}$, то определим $F_i((x_1, y_1), q_j) = (h_i(x_1, q), f_i(y_1, y))$, $i = 1, 2$, где $f_0(y_1, y) = j$.

Симметрично, если $x_2 \in Q_{k_1}$, $y_2 \in Q_{k_2}$ и $q_j \in \{q_0, \ldots, q_{k_3-1}\}$, то определим $F_i(q_j, (x_2, y_2)) = (h_i(q, x_2), f_i(y, y_2))$, $i = 1, 2$, где $f_0(y, y_2) = j$.

При $q_{j_1}, q_{j_2} \in \{q_0, \ldots, q_{k_3-1}\}$ определим $F_i(q_{j_1}, q_{j_2}) = t_i(q_{j_1}, q_{j_2})$, $i = 1, 2$.

Достаточно проверить, что F_1 и F_2 являются латинскими квадратами в алфавите R и для любой пары $(a, b) \in R$ найдётся такая пара $u, v \in R$, что $a = F_1(u, v)$, $b = F_2(u, v)$. По построению латинский квадрат F_i разделяется на латинские подквадраты эквивалентные g_i, h_i и t_i в алфавитах определяемых латинским квадратом f_i, $i = 1, 2$. Отсюда видно, что F_1 и F_2 являются латинскими квадратами.

Пусть $a = (x_3, y_3)$ и $b = (x_4, y_4)$, где $x_3, x_4 \in Q_{k_1}$, $y_3, y_4 \in Q_{k_2}$. Найдутся $y_1, y_2 \in Q_{k_2}$ такие, что $f_1(y_1, y_2) = y_3$ и $f_2(y_1, y_2) = y_4$. Пусть $f_0(y_1, y_2) \geq k_3$, найдутся $x_1, x_2 \in Q_{k_1}$ такие, что $g_1(x_1, x_2) = x_3$, $g_2(x_1, x_2) =$

x_4. Тогда $u = (x_1, y_1)$, $v = (x_2, y_2)$. Пусть $f_0(y_1, y_2) < k_3$, либо найдутся $x_1, x_2 \in Q_{k_1}$ такие, что $h_1(x_1, x_2) = x_3$, $h_2(x_1, x_2) = x_4$ и тогда $u = (x_1, y_1)$, $v = (x_2, y_2)$; либо $x_1 \in Q_{k_1}$ такое, что $h_1(x_1, q) = x_3$, $h_2(x_1, q) = x_4$ и тогда $u = (x_1, y_1)$, $v = q_j$, где $j = f_0(y_1, y_2)$; либо $x_2 \in Q_{k_1}$ такое, что $h_1(q, x_2) = x_3$, $h_2(q, x_2) = x_4$ и тогда $u = q_j$, где $j = f_0(y_1, y_2)$, $v = (x_2, y_2)$.

Пусть $a = (x_3, y_3)$ и $b = q_j$, где $x_3 \in Q_{k_1}$, $y_3 \in Q_{k_2}$, $q_j \in Q_{k_3}$. Найдутся $y_1, y_2 \in Q_{k_2}$ такие, что $f_0(y_1, y_2) = j$ и $f_1(y_1, y_2) = y_3$. Пусть $f_2(y_1, y_2) = y_4$. Найдутся такие $x_1, x_2 \in Q_{k_1}$, что $h_1(x_1, x_2) = x_3$ и $h_2(x_1, x_2) = q$. Тогда $u = (x_1, y_1)$, $v = (x_2, y_2)$. Аналогично можно рассмотреть случай $a = q_j$ и $b = (x_4, y_4)$, где $x_4 \in Q_{k_1}$, $y_4 \in Q_{k_2}$, $q_j \in Q_{k_3}$.

Если $a, b \in Q_{k_3}$, то требуемое следует из ортогональности латинских квадратов t_1 и t_2. □

Отметим, что в лемме 3 можно взять $k_3 = 1$.

Лемма 4 ([29]). *При $k \equiv 1 \mod 4$, $k \geq 5$, имеется тройка попарно ортогональных латинских квадратов порядка k.*

Доказательство. Пусть $k = 4t + 1 = 3p$. Тогда t не делится на 3. Если $t = 2$ или $t = 4$, то требуемое следует из утверждения 61. Если $t = 2^\delta$, $\delta \geq 3$, или все делители t не меньше 5, то имеется система из 4 попарно ортогональных латинских квадратов f_0, f_1, f_2, f_3 порядка t по утверждению 61. Пусть g_1, g_2, g_3 и h_1, h_2, h_3 тройки попарно ортогональных латинских квадратов порядков 4 и 5 соответственно. Из доказательства леммы 3 ($k_1 = 4$, $k_2 = t$, $k_3 = 1$) видно, что можно построить пары ортогональных латинских квадратов порядка k, используя тройку f_0, f_i, f_j, и две пары g_i, g_j и h_i, h_j, где $i, j \in \{1, 2, 3\}$. Таким образом, получена тройка попарно ортогональных латинских квадратов порядка k.

Если k не делится на 3, то тройка попарно ортогональных латинских квадратов порядка k найдётся по утверждению 61. □

Теорема 29 ([13]). *При $k \neq 2, 6, 10, 14$, имеется пара ортогональных латинских квадратов порядка k.*

Доказательство. По следствию 30 остаётся исследовать случай $k \equiv 2 \mod 4$. Возможны три случая $k \equiv 2, 6, 10 \mod 12$. Тогда возможны три варианта $k = 3(4t + 1) + 11$, $k = 3(4t + 1) + 3$ или $k = 3(4t + 1) + 7$. Из лемм 3 и 4 получаем требуемое при $k_1 = 3$, $k_2 = 4t + 1$ и $k_3 = 11, 3, 7$, за исключением случаев $k = 2, 6, 10, 14, 22, 26, 38$. При $k = 22$ и $k = 26$ можно применить лемму 3 при $k_1 = 3$, $k_2 = 7$, $k_3 = 1$ и $k_3 = 5$. При $k = 38$ можно применить лемму 3 при $k_1 = 7$, $k_2 = 5$ и $k_3 = 3$. □

Пар ортогональных латинских квадратов порядков 2 и 6 не существует. Пары ортогональных латинских квадратов порядков 10 и 14 найдены с помощью компьютера. В [50] построены пары ортогональных кубов

всех порядков, за исключением 3 и $k \equiv 2 \mod 4$. Вопросы о существовании тройки попарно ортогональных латинских квадратов порядка 10 и пары ортогональных латинских кубов порядка 10 остаются пока нерешёнными.

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, что в конечной аффинной плоскости каждая прямая содержит одинаковое количество точек k, называемое порядоком плоскости. Более того, все прямые разбиваются на $k+1$ класс по k параллельных прямых в каждом. Таким образом, аффинная плоскость содержит k^2 точек.

Утверждение 62. *Аффинные плоскости порядка k взаимно однозначно соответствуют* МДР-*кодам в Q_k^{k+1} с расстоянием k (системам из $k-1$ попарно ортогонального латинского квадрата порядка k).*

Доказательство. Пусть дан МДР-код $C \subset Q_k^{k+1}$ с расстоянием k. Назовём элементы кода точками, а прямыми будем считать пересечения МДР-кода с гиперплоскостями. Выполнение свойства 1) вытекает из следствия 26. Свойства 2) и 3) выполнены по построению. Докажем, что аффинная плоскость порождает МДР-код. Занумеруем k прямых каждого параллельного класса числами $0, \ldots, k-1$. Каждой точке сопоставим набор из Q_k^{k+1}, где на i-ом месте находится номер прямой из i-го класса, которой принадлежит эта точка. По построению полученное множество имеет мощность k^2 и из свойства 1) следует, что расстояния между точками равны k. Полученное подмножество гиперкуба является МДР-кодом по утверждению 50 (b). □

Неизвестно ни одной системы из $k-1$ попарно ортогонального латинского квадрата порядка k, когда k не является степенью простого числа. Гипотеза о том, что таких систем и, следовательно, аффинных плоскостей порядка не равного степени простого числа не существует, является одной из классических проблем комбинаторики.

Определение 49. *Связный граф G называется сильно регулярным с параметрами (v, k, λ, μ), если $|V(G)| = v$, степень любой вершины равна k, любые две смежные вершины имеют λ общих соседей и любые две несмежные вершины имеют μ общих соседей.*

Сильно регулярный граф является дистанционно-регулярным графом с диаметром 2 (если $k \neq v-1$) с параметрами $(b_0, b_1, c_1, c_2) = (k, k-\lambda-1, 1, \mu)$.

Пусть $C \subset Q_q^n$ — некоторый код с кодовым расстоянием d. Рассмотрим граф минимальных расстояний $G(C)$, вершинами которого являются вершины кода C и две вершины соединены ребром, если расстояние Хэмминга между ними равно d.

Утверждение 63. *Если $C \subset Q_q^n$ — МДР-код с расстоянием $n-1$, то $G(C)$ — сильно регулярный граф.*

Доказательство. Поскольку МДР-код с расстоянием $n-1$ в Q_q^n определяется системой из $n-2$ попарно ортогональных латинских квадратов, то по утверждению 54 имеем $n \leq q+1$. Из следствия 26 вытекает, что при $n = q+1$ граф $G(C)$ является полным. Далее полагаем, что $n \leq q$. Если две вершины МДР-кода находятся на расстоянии $n-1$, то их общие соседи — это все вершины, находящиеся в общей для них $(n-1)$-мерной грани. Тогда $\lambda = \frac{|C|}{q} - 2 = q-2$. Пусть две вершины $u, v \in C$ находятся на расстоянии n. Пересечение любых двух $(n-1)$-мерных граней разных направлений, содержащих вершины u и v, является гранью размерности $n-2$. По определению МДР-кода любая $(n-2)$-мерная грань гиперкуба содержит ровно одну кодовую вершину. Тогда μ равняется числу пар таких $(n-1)$-мерных граней, т. е. $\mu = n(n-1)$. □

Любой латинский квадрат порядка q соответствует МДР-коду с расстоянием 2 в Q_q^3. Более того, любая система из $n-2$ ортогональных латинских квадратов порядка q определяет МДР-код с расстоянием $n-1$ в гиперкубе Q_q^n и, следовательно, сильно регулярный граф.

Задача 68. Докажите, что если латинский параллелепипед размера $q \times q \times (q-1)$ заполнен элементами Q_q так, что в каждой линии никакой элемент не встречается дважды, то этот параллелепипед можно дополнить до латинского куба.

Задача 69. Докажите, что для любого $n \geq 2$ в Q_3^n имеется один с точностью до изометрии гиперкуба МДР-код с расстоянием 2.

Задача 70. Докажите, что если имеется пара ортогональных латинских гиперкубов в q-ичном алфавите, то их размерность не превышает $q-1$.

Задача 71. Докажите, что набор из $q-2$ попарно ортогональных латинских квадратов порядка q всегда дополняется до набора из $q-1$ попарно ортогональных латинских квадратов порядка q.

Задача 72. Докажите, что МДР-код с расстоянием 3 является полностью регулярным кодом в Q_q^n точнее первым цветом совершенной раскраски с параметрами $\begin{pmatrix} 0 & n(q-1) & 0 \\ 1 & (n-2)(n-1)+q-2 & (n-1)(q-n+1) \\ 0 & n(n-1) & n(q-n) \end{pmatrix}$.

Задача 73. Докажите, что дополнение сильно регулярного графа также является сильно регулярным графом.

Задача 74. Пусть матрица A размера $r \times n-r$ имеет только ненулевые миноры всех размеров над полем $GF(q)$. Докажите, что матрица $(I_r|A)$ размера $r \times n$ является проверочной матрицей МДР-кода.

Задача 75. Представим матрицу V_r из утверждения 59 в виде $V_r = (B|A)$, где B размера $r \times r$. Докажите, что матрица $B^{-1}A$ не содержит нулевых миноров никакого порядка.

Задача 76. Пусть $a_1, \ldots, a_n, b_1 \ldots, b_n$ попарно различные элементы поля $GF(q)$. Докажите, что матрица Коши C, где $c_{ij} = \frac{1}{a_i - b_j}$, не имеет нулевых миноров никаких порядков.

Задача 77. Пусть $C \subset Q_q^n$ и в каждом шаре радиуса ρ содержится не более L элементов из C. Докажите, что $|C| \leq Lq^{n-\lfloor \frac{(L+1)\rho}{L} \rfloor}$ (обобщённая граница Синглтона).

10 Комбинаторные t-дизайны

10.1 Дизайны как совершенные раскраски графов и гиперграфов

Вспомним, что графом Джонсона $J(n,k)$ называется граф, вершинами которого являются все двоичные наборы длины n и веса k. Две вершины графа соединены ребром, если расстояние Хэмминга между соответствующими им двоичными наборами равно двум. Таким образом, матрица смежности графа Джонсона является подматрицей матрицы расстояний 2 в булевом гиперкубе. Вершины графа Джонсона $J(n,k)$ можно рассматривать как точки целочисленного симплекса $\{(x_1, \ldots, x_k) \mid x_i \in \mathbb{N}, \sum_{i=1}^{k} x_i \leq n\}$, где $\sum_{i=1}^{j} x_i$ — номер координаты, в которой находится j-я единица двоичного набора.

Определение 50. *Комбинаторным дизайном*[29] *(точнее t-дизайном) с параметрами $t-(n,k,\lambda)$ называется такой набор блоков — k-элементных подмножеств n-элементного множества, что любое t-элементное подмножество содержится ровно в λ блоках.*

Блоки дизайна с параметрами t-(n,k,λ) можно рассматривать как вершины графа $J(n,k)$. Комбинаторный t-дизайн удобно представлять в виде списка блоков. Блок можно задать набором номеров элементов блока или характеристической функций блока, т. е. как булев вектор длины n и веса k.

[29] Подробное изложение теории комбинаторных дизайнов имеется в [48].

Пример 30. Таблица блоков дизайна с параметрами 2-(13,4,1).

2	3	5	11
3	4	6	12
4	5	7	13
1	5	6	8
2	6	7	9
3	7	8	10
4	8	9	11
5	9	10	12
6	10	11	13
1	7	11	12
2	8	12	13
1	3	9	13
1	2	4	10

Утверждение 64. *Характеристическая функция дизайна D с параметрами $(k-1)$-(n,k,λ) является совершенной раскраской графа $J(n,k)$ с матрицей параметров* $S = \begin{pmatrix} k(\lambda-1) & k(n-k-\lambda+1) \\ k\lambda & k(n-k-\lambda) \end{pmatrix}$.

Доказательство. Два блока $u, v \in V(J(n,k))$ смежны если и только если их пересечение содержит $(k-1)$ элемент. Любой $(k-1)$-элементное множество содержится в λ блоках дизайна D. Следовательно, блок $u \in D$ видит $\lambda-1$ вершин $v \in D$, которые пересекаются с ним по некоторому $(k-1)$-элементному множеству. В то время как k-элементный блок $u \notin D$ видит λ вершин $v \in D$, которые пересекаются с ним по фиксированному $(k-1)$-элементному множеству. Поскольку блок $u \in D$ включает ровно k подмножеств мощности $k-1$, имеем $s_{11} = k(\lambda-1)$ и $s_{21} = k\lambda$. Степень графа $J(n,k)$ равна $k(n-k)$. Отсюда имеем $s_{12} = k(n-k-\lambda+1)$ и $s_{22} = k(n-k-\lambda)$. □

При $\lambda = 1$ комбинаторные дизайны с параметрами t-(n,k,λ) обычно обозначают $S(t,k,n)$, а при $t = k-1$ дополнительно, их называют системами Штейнера (при $k = 3$ тройками Штейнера) порядка n.

При $\lambda = 1$ комбинаторный дизайн с параметрами t-$(n,k,1)$ можно рассматривать как трансверсаль в гиперграфе $G_{n,k,t}$, вершинами которого являются всевозможные k-элементные блоки, а гиперрёбра — это наборы блоков, содержащих фиксированное t-элементное множество.

В случае, когда $t = k-1$ мультиграф $\mathcal{M}_{12}(\mathcal{D}(G_{n,k,t}))$ смежности вершин в гиперграфе $G_{n,k,t}$, если из него удалить петли, совпадает с графом $J(n,k)$.

Как частный случай утверждения 64 при $\lambda = 1$ (см. также задачу 57 и утверждение 15 о границе Дельсарта—Хоффмана) имеем

Следствие 31. *Системы Штейнера $S(k-1,k,n)$ являются максимальными независимыми множествами в $J(n,k)$.*

Рассмотрим мультиграф $(J(n,k))_{k-t}$ как граф $\mathcal{M}_{12}(\mathcal{D}(G_{n,k,t}))$ с удалёнными петлями. Он получается из графа Джонсона $J(n,k)$, если в графе $J(n,k)$ соединить рёбрами вершины, находящиеся на расстоянии не более $k-t$, соответствующим числом рёбер.

Утверждение 65 ([128]). *Характеристическая функция дизайна D с параметрами t-(n,k,λ) является совершенной раскраской мультиграфа $(J(n,k))_{k-t}$ с матрицей параметров $S = \begin{pmatrix} \binom{k}{t}(\lambda-1) & \binom{k}{t}(\binom{n-k}{k-t}-\lambda+1) \\ \binom{k}{t}\lambda & \binom{k}{t}(\binom{n-k}{k-t}-\lambda) \end{pmatrix}$ и дизайн D является максимальным независимым множеством в $(J(n,k))_{k-t}$ при $\lambda = 1$.*

Доказательство. Покажем, что при $\lambda = 1$ дизайн D — максимальное независимое множество. Рассмотрим гиперграф $G_{n,k,t}$. Вершины графа $(J(n,k))_{k-t}$ соединены ребром тогда и только тогда, когда они содержатся в некотором ребре гиперграфа $G_{n,k,t}$. Любое независимое множество в $(J(n,k))_{k-t}$ пересекается с ребром гиперграфа не более чем по одному элементу, поэтому его мощность не больше мощности трансверсали гиперграфа. Поскольку дизайн D является трансверсалью в $G_{n,k,t}$, он является максимальным независимым множеством в $(J(n,k))_{k-t}$. Доказательство, того что характеристическая функция дизайна D с параметрами t-(n,k,λ) является совершенной раскраской мультиграфа $(J(n,k))_{k-t}$ аналогично доказательству утверждения 64. □

Верно и обратное: первый цвет совершенной раскраска мультиграфа $(J(n,k))_{k-t}$ с матрицей параметров S является t-(n,k,λ) дизайном. Докажем это в частном случае $\lambda = 1$.

Утверждение 66 ([128]). *Множество D является дизайном с параметрами t-$(n,k,1)$ тогда и только тогда, когда его характеристическая функция является совершенной раскраской мультиграфа $(J(n,k))_{k-t}$ с матрицей параметров $S = \begin{pmatrix} 0 & \binom{k}{t}\binom{n-k}{k-t} \\ \binom{k}{t} & \binom{k}{t}(\binom{n-k}{k-t}-1) \end{pmatrix}$.*

Доказательство. ($\Rightarrow$) Следует из утверждений 64 и 65.

($\Leftarrow$) Рассмотрим множество D вершин первого цвета в раскраске с матрицей параметров S. Любое t-элементное множество содержится в не более чем в одном k-блоке из D, поскольку $s_{00} = 0$. Рассмотрим k-блок $u \notin D$. Он содержит ровно $s_{10} = \binom{k}{t}$ различных t-элементных подмножеств. Поскольку никакое из них не содержится сразу в двух k-блоках из D, можно заключить, что любое t-элементное подмножество содержится в k-блоке из D. □

Отметим, утверждение 66 по существу является частным случаем утверждения 44.

10.2 Системы Штейнера

Напомним, что совершенным кодом с расстоянием $2e{+}1$ или e-совершенным кодом в графе называется такое подмножество C вершин графа, что шары радиуса e с центрами в вершинах из C не пересекаются и покрывают все вершины графа[30].

Утверждение 67. *Пусть C — e-совершенный код в Q_2^n и $\bar{0} \in C$. Тогда множество $\{u \in C \mid \mathrm{wt}(u) = 2e{+}1\}$ является $S(e{+}1, 2e{+}1, n)$ дизайном.*

Доказательство. Рассмотрим произвольную вершину веса $e+1$. По определению e-совершенного кода она принадлежит ровно одному шару с центром в точке $u \in C$. В коде C нет вершин веса менее $2e+1$, поскольку шары радиуса e с центром в такой вершине и в вершине $\bar{0} \in C$ пересекаются. Тогда $\mathrm{wt}(u) = 2e+1$. □

В частности, множество вершин веса 3 в 1-совершенном двоичном коде образуют систему троек Штейнера. Систему троек Штейнера, которая содержится в коде Хэмминга, можно задать следующим образом $\{\{x, y, x \oplus y\} \mid x, y \in Q_2^t \setminus \{\bar{0}\}, x \neq y\}$, где длина кода Хэмминга равна $2^t - 1$. Номера x и y координат вершин в n-мерном булевом кубе, содержащем код Хэмминга, можно рассматривать как элементы множества $Q_2^t \setminus \{\bar{0}\}$ — столбцы проверочной матрицы кода Хэмминга.

Утверждение 68. *Пусть D — комбинаторный дизайн с параметрами $t-(n,k,\lambda)$. Тогда его ретракт $D' = \{u' \in Q_2^{n-1} \mid (u',1) \in D\}$ является комбинаторным дизайном с параметрами $(t-1)$-$(n-1, k-1, \lambda)$.*

Доказательство. Рассмотрим блоки дизайна D, которые содержат n-ый элемент. Любое $(t-1)$-элементное подмножество, не содержащее n-ый элемент, содержится в λ таких блоков по определению дизайна. Таким образом, удалив из этих блоков n-ый элемент, мы получим дизайн с требуемыми параметрами. □

Дизайн D' называется укорочением исходного дизайна D.

Утверждение 69. *Если комбинаторный дизайн с параметрами t-(n,k,λ) существует, то числа $\lambda\binom{n-i}{t-i}/\binom{k-i}{t-i}$ при $i = 0, \ldots, t-1$ являются целыми.*

Доказательство. Пусть N — число блоков в дизайне с параметрами t-(n,k,λ). Рассмотрим двудольный граф, одной долей которого являются блоки дизайна, а другой всевозможные t-элементные наборы. Соединим каждый t-элементный набор ребрами с блоками, в которых он содержится. Из определения дизайна следует, что число рёбер в графе равно $\lambda\binom{n}{t} = N\binom{k}{t}$. Аналогичное соотношение верно для любого укорочения исходного дизайна. □

[30] Подробнее про e-совершенные коды в гиперкубах в разделе 16.3.

Теорема 30 (Киркман [82]). *Система троек Штейнера $S(2,3,n)$ существует тогда и только тогда, когда $n \equiv 1 \mod 6$ или $n \equiv 3 \mod 6$.*

Доказательство. Из утверждения 69 следует, что необходимым условием существования системы троек Штейнера порядка n является делимость числа $n(n-1)$ на 6 и числа $n-1$ на 2. Это условие выполняется только если $n \equiv 1 \mod 6$ или $n \equiv 3 \mod 6$.

Докажем существование систем троек Штейнера при $n \equiv 3 \mod 6$. Заметим, что число $m = n/3$ нечётное. По теореме 27 существует идемпотентная симметричная квазигруппа $f : Q_m^2 \to Q_m$ порядка m. Рассмотрим n-элементное множество $Q_m \times Q_3$, элементы которого будем записывать в виде xi, где $x \in Q_m$, а $i \in \{0,1,2\}$. Определим множество S, состоящее из троек элементов $Q_m \times Q_3$ двух типов
$\{\{x0, x1, x2\} \mid x \in Q_m\}$ и
$\{\{xi, yi, f(x,y)(i+1 \mod 3)\} \mid i \in Q_3, x, y \in Q_m, x \neq y\}$.
Проверим, что S — система троек Штейнера. Рассмотрим пару элементов $xi, zj \in Q_m \times Q_3$. Если $x = z$, то пара содержится в тройке первого типа, а если $i = j$ — второго. Пусть $x \neq z$ и $i \neq j$. Тогда $j = i+1 \mod 3$ или наоборот $i = j+1 \mod 3$ (что безразлично, поскольку пара $\{xi, zj\}$ неупорядочена). Не теряя общности, положим $j = i+1 \mod 3$. Из определения квазигруппы найдётся единственное $y \in Q_m$ такое, что $z = f(x,y)$, кроме того, $y \neq x$ из идемпотентности квазигруппы. Тогда имеется тройка второго типа $\{xi, yi, zj\}$. Тройка, содержащая произвольную пару элементов, находится единственным образом, поэтому S — система Штейнера.

Докажем существование систем троек Штейнера при $n \equiv 1 \mod 6$. Заметим, что число $m = (n-1)/3$ чётное. По теореме 27 существует полуидемпотентная симметричная квазигруппа $f : Q_m^2 \to Q_m$ порядка m. Рассмотрим n-элементное множество $(Q_m \times Q_3) \cup \{\delta\}$, где δ — специальный дополнительный символ. Определим множество S, состоящее из троек элементов множества $(Q_m \times Q_3) \cup \{\delta\}$ трёх типов
$\{\{x0, x1, x2\} \mid x \in Q_{m/2}\}$,
$\{\{xi, yi, f(x,y)(i+1 \mod 3)\} \mid i \in Q_3, x, y \in Q_m, x \neq y\}$ и
$\{\{(x+m/2)i, x(i+1 \mod 3), \delta\} \mid i \in Q_3, x \in Q_{m/2}\}$.
Пары элементов $\{xi, \delta\}$ содержатся в тройках третьего типа. Доказательство того, что остальные пары элементов, за исключением пар $\{(x+m/2)i, (x+m/2)(i+1 \mod 3)\}$ и $\{(x+m/2)i, x(i+1 \mod 3)\}$, $x \in Q_{m/2}$, покрыты тройками второго типа аналогично предыдущему случаю $n \equiv 3 \mod 6$. Для доказательства однократности покрытия пар достаточно показать, что пары $\{(x+m/2)i, x(i+1 \mod 3)\}$, $x \in Q_{m/2}$, не содержатся в тройках второго типа. В то время как пары $\{(x+m/2)i, (x+m/2)(i+1 \mod 3)\}$, $x \in Q_{m/2}$, наоборот, содержатся в тройках второго типа. Действительно, $f(x+m/2, y) \neq x$ при $y \neq x+m/2$, поскольку $f(x+m/2, x+m/2) = x$ из полуидемпотентности квазигруппы f; но для

любого $x \in Q_{m/2}$ найдётся $y \neq x+m/2$ такой, что $f(x+m/2, y) = x+m/2$. □

Использованные в теореме конструкции систем троек Штейнера придуманы Р.Боузом [12] и Т.Сколемом [89].

Замечание 14. Х.Ханани [47] доказал существование систем четвёрок Штейнера для любого n, удовлетворяющего необходимым условиям $n \equiv 2 \mod 6$ или $n \equiv 4 \mod 6$ (утверждение 69). Р.М.Вильсон [102](для $t = 2$) и П.Киваш [51] (для произвольных t) доказали[31], что для фиксированных t, k, λ найдётся такое $n_0 \in \mathbb{N}$, что комбинаторный дизайн с параметрами t-(n, k, λ) существует при $n \geq n_0$ и выполнении необходимых условий из утверждения 69.

Пусть D — система Штейнера $S(2, k, n)$ и $M \subset Q_k^k$ — МДР-код с расстоянием $k-1$, содержащий подкод $\{\underbrace{(i, \ldots, i)}_{k} \mid i = 1, \ldots, k\}$. Кодовое расстояние $k-1$ МДР-кода M гарантирует, что его вектора, за исключением векторов вида $(i, \ldots, i)$ не содержат одинаковых символов. Следовательно, наборы из M можно рассматривать как перестановки $(\pi 1, \ldots, \pi k)$. Определим множество $E[D, M] \subset Q_n^k$ по правилу: $(x_{a_{\pi 1}}, \ldots, x_{a_{\pi k}}) \in E[D, M]$ тогда и только тогда, когда $\{x_{a_1}, \ldots, x_{a_k}\} \in D$ и набор $(\pi 1, \ldots, \pi k) \neq (i, \ldots, i)$ содержится M. Отметим, что одному блоку из D соответствует $k(k-1)$ различных вершин из $E[D, M]$.

Утверждение 70. *Множество* $C = E[D, M] \cup \{\underbrace{(i, \ldots, i)}_{k} \mid i = 1, \ldots, n\}$ *является* МДР-*кодом с расстоянием* $k-1$ *в гиперкубе* Q_n^k.

Доказательство. Кодовое расстояние множества $E[D, M]$ равняется $k-1$. Действительно, поскольку D — система Штейнера, то каждая пара содержится только в одном блоке, а поскольку M — МДР-код с расстоянием $k-1$, перестановки элементов одного блока различаются как минимум в $k-1$ позициях. Поскольку $E[D, M]$ состоит из перестановок, то вершины вида $(i, \ldots, i)$ находятся на расстоянии $k-1$ от вершин из $E[D, M]$. Число элементов в коде равно $n + k(k-1)\binom{n}{2}/\binom{k}{2} = n^2$. Из утверждения 50 о границе Синглтона следует, что C — МДР-код. □

Если $k = 3$, то в качестве M можно использовать идемпотентный латинский квадрат порядка 3. Полученные из системы троек Штейнера МДР-коды с расстоянием 2 являются графиками квазигрупп, которые называются тотально симметричными. При $k > 3$ в результате конструкции из утверждения 70 получается МДР-код эквивалентный набору попарно ортогональных латинских квадратов.

[31] Имеется альтернативное доказательство этой теоремы [36].

10.3 Симметричные дизайны и проективные плоскости

Проективной плоскостью называется система точек и прямых, удовлетворяющая следующим свойствам.

1) Через любые две различные точки проходит ровно одна прямая.

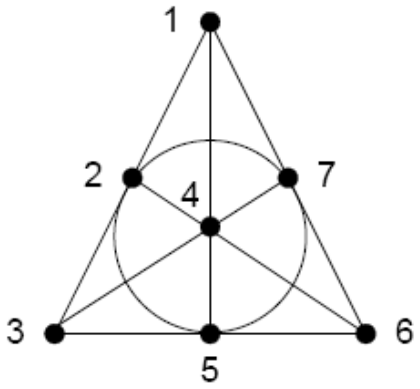
2) Любые две прямые имеют общую точку.

3) Существуют три точки, не лежащие на одной прямой.

4) Каждая прямая содержит не менее трёх точек.

Можно показать, что в конечной проективной плоскости каждая прямая содержит одинаковое количество точек — $k+1$, где k порядок плоскости. Из симметрии точек и прямых в определении проективной плоскости следует, что через каждую точку проходит $k+1$ прямая. Всего проективная плоскость порядка k содержит k^2+k+1 точку, поскольку каждая из $k+1$ прямых, проходяших через фиксированную точку содержит по k точек, кроме фиксированной точки. Из свойств 1)-2) следует, что все эти точки различны и других точек на плоскости нет. Проективные плоскости порядка k являются штейнеровыми дизайнами $S(2, k+1, k^2+k+1)$, где точки соответствуют элементам, а прямые — блокам.

Пример 31. Проективная плоскость порядка 2 (плоскость Фано) содержит 7 прямых $\{1,2,3\}, \{1,4,5\}, \{1,6,7\}, \{2,4,6\}, \{2,5,7\}, \{3,4,7\}, \{3,5,6\}$.



Аффинная плоскость порядка k может быть получена из проективной плоскости того же порядка путём удаления одного блока и всех точек этого блока из проективной плоскости. Обратная операция: добавление к каждой прямой аффинной плоскости по одной точке (одинаковой параллельных прямых) и дополнительной прямой, состоящей из всех добавленных точек, позволяет получить из аффинной плоскости проективную плоскость того же порядка. Аффинную плоскость порядка k можно рассматривать как дизайн $S(2, k, k^2)$.

Из равенства $\binom{k^2+k+1}{2} = (k^2+k+1)\binom{k+1}{2}$ следует, что проективная плоскость содержит столько же прямых, а именно k^2+k+1, сколько и точек. Любые две прямые в проективной плоскости пересекаются ровно

в одной точке, поэтому развернув отношение принадлежности и рассмотрев точки как блоки, а прямые как элементы дизайна мы получим дизайн с теми же параметрами. Проективные плоскости переходящие друг в друга таким преобразованием называются *дуальными*.

Утверждение 71. *Из любого дизайна D мощности v с параметрами 2-(v,k,λ) после замены вершин на блоки, т. е. после обращения отношения принадлежности, получается дизайн с теми же параметрами.*

Доказательство. Пусть M — матрица инцидентности дизайна $D = \{b_j : j = 1,\dots,v\}$, т. е.

$$M_{v\times v} = (m_{ij}) = \begin{cases} 1, \text{ если } x_i \in b_j \in D; \\ 0, \text{ иначе.} \end{cases}$$

Из определения дизайна следует, что каждый столбец матрицы M содержит k единиц. Из утверждения 68 следует, что каждая строка матрицы D содержит одинаковое количество единиц, а поскольку D — квадратная матрица, то тоже k единиц. Рассмотрим произвольную пару строк, по определению дизайна имеется ровно λ столбцов, в которых обе эти строки имеют единицы. Пусть числа a и b удовлетворяют уравнению $\lambda a^2 + 2(k-\lambda)ab + (v-2k-\lambda)b^2 = 0$. Рассмотрим матрицу Q, которая получается из M заменой 1 на a и 0 на b. Из выбора чисел a и b следует, что матрица Q ортогональна. С другой стороны, произвольная ортогональная матрица Q, элементы которой принимают только два значения, соответствует матрице инцидентности некоторого дизайна. Ясно, что матрице Q^T соответствует дизайн, полученный обращением отношения принадлежности и матрицы Q и Q^T ортогональны одновременно. □

2-Дизайны, у которых число блоков равно числу точек называют *симметричными*.

В [24], [17] доказаны следующие условия существовании симметричных 2-дизайнов.

Теорема 31 (Брука – Райзера – Човлы)**.** *Пусть существует симметричный 2-(v,k,λ) дизайн.*

Если v чётно, то $k-\lambda = x^2$ для некоторого натурального x.

Если v нечётно, то найдутся такие натуральные числа x, y и z (не равные нулю одновременно), что справедливо равенство

$$z^2 = (k-\lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2.$$

Эта теорема даёт бесконечную серию арифметически допустимых параметров дизайнов, при которых дизайны однако же не существуют. Отметим, что утверждение о существовании 2-(v,k,λ) с арифметически допустимыми параметрами [102] становится верным лишь для достаточно больших v при фиксированных k и λ.

Замечание 15. Из теоремы Брука – Райзера – Човлы можно доказать, что не существует конечных проективных плоскостей порядков 14, 21 и 22. Несуществование проективной плоскости порядка 6 следует из отсутствия пары ортогональных латинских квадратов порядка 6. Несуществование проективной плоскости порядка 10 показано с помощью компьютера в [62]. Также с помощью компьютера доказано [61], что для каждого из порядков 3, 4, 5, 7 и 8 существует единственная проективная плоскость, соответствующая полной системе линейных ортогональных латинских квадратов; а для порядка 9 имеется четыре проективные плоскости, две из которых дуальны.

Задача 78. Докажите, что дизайн с параметрами t-(n,k,λ) является одновременно и дизайном с параметрами i-(n,k,λ') при $i=1,\ldots,t-1$ и $\lambda'=\lambda\binom{n-i}{t-i}/\binom{k-i}{t-i}$.

Задача 79. Докажите, что дизайнам с параметрами 2-(n,k,λ) взаимно однозначно соответствуют дизайны с параметрами 2-$(n,n-k,\lambda')$, где $\lambda'=\lambda\binom{n}{2}/\binom{k}{2}-2\lambda\frac{n-1}{k-1}+\lambda$.

Задача 80. Докажите, что максимальная клика в графе $J(n,k)$ является дельсартовой.

Задача 81. Докажите, что дизайн с параметрами $S(k-2,k,n)$ является полностью регулярным кодом в графе $J(n,k)$.

Задача 82. В конструкции аналогичной построению множества $E(D,M)$ (см. утверждение 70) рассмотрим в качестве D систему четвёрок Штейнера порядка n, а в качестве M — множество чётных перестановок. Докажите, что множество $E[D,M]\cup\{(i,i,j,j),(i,j,i,j),(i,j,j,i)\mid\ i,j=1,\ldots,n\}$ является МДР-кодом с расстоянием 3 в гиперкубе Q_n^4.

Задача 83. Докажите, что МДР-код в Q_k^{k+1} с расстоянием k не содержит вершин на расстоянии $k+1$. Докажите, что любой такой код порождает дизайн с параметрами 2-$(k^2,k,1)$.

Задача 84. Пусть M — матрица инцидентности дизайна D с параметрами 2-(n,k,λ). Докажите равенство $MM^{\mathrm{T}}=\lambda(J_n+\frac{n-k}{k-1}I_n)$.

Задача 85. Докажите, что при $n\equiv 1,3(\mod 6)$ в графе перестановок $Cay(S_n,T_n)$ имеются совершенные раскраски с матрицей параметров $S=\begin{pmatrix}3+\binom{n-3}{2} & 3(n-3)\\ 3 & 3(n-3)+\binom{n-3}{2}\end{pmatrix}$.

11 Преобразование Фурье

11.1 Характеры абелевых групп

Множество функций действующих из группы $(K,\circ)$ в поле комплексных чисел обозначим через $\mathbb{V}(K)\stackrel{df}{=}\{f:K\to\mathbb{C}\}$.

Определение 51. *Скалярным*[32] *характером группы называется отображение* $\phi \in \mathbb{V}(K)$*, удовлетворяющее следующим условиям:*

$$\forall x \in K \quad |\phi(x)| = 1; \qquad \forall x, y \in K \quad \phi(x \circ y) = \phi(x) \cdot \phi(y). \tag{15}$$

Таким образом любой характер является гомоморфизмом, действующим из группы K в группу точек единичной окружности $T = \{x \in \mathbb{C} : \quad |x| = 1\}$ с операцией умножения. Группа T изоморфна унитарной группе U(1) и специальной ортогональной группе SO(2).

Покажем, что характеры образуют абелеву группу, которую будем обозначать $X(K)$. Определим произведение характеров равенством

$$(\phi_1 \cdot \phi_2)(x) = \phi_1(x)\phi_2(x).$$

Проверим, что произведение характеров $\phi_1, \phi_2 \in X(K)$ является характером:

$$|(\phi_1 \cdot \phi_2)(x)| = |\phi_1(x)||\phi_2(x)| = 1;$$

$$(\phi_1 \cdot \phi_2)(x \circ y) = \phi_1(x \circ y)\phi_2(x \circ y) = \phi_1(x)\phi_1(y)\phi_2(x)\phi_2(y) = (\phi_1 \cdot \phi_2)(x)(\phi_1 \cdot \phi_2)(y).$$

Ассоциативность и коммутативность умножения характеров следует из ассоциативности и коммутативности операции умножения комплексных чисел. Единица группы $X(K)$ — это тождественно единичная функция $\mathbf{1}(x) \equiv 1$. Обратный элемент — это характер $(\phi)^{-1} = \bar{\phi}$ комплексно сопряжённый исходному. Группа характеров $X(K)$ называется двойственной к группе K.

Далее будем рассматривать только абелевы группы $(K, +)$, т. е. групповую операцию $+$ считаем коммутативной. Рассмотрим характеры группы характеров $X(K)$. Определим характер $\Theta_x \in X(X(K))$ равенством $\Theta_x(\phi) = \phi(x)$ для всех $\phi \in X(K)$. Для абелевых групп справедливо свойство[33]: $x \neq y \Leftrightarrow \Theta_x \neq \Theta_y$, поскольку верно, что $\forall x, y \in K \quad \exists \phi \in X(K) \quad \phi(x) \neq \phi(y)$. Поэтому K является подгруппой группы $X(X(K))$.

Теорема 32 (двойственности Понтрягина—ван Кампена [127], [81])**.** *Если* K *— локально компактная коммутативная группа, то* $K \simeq X(X(K))$.

Пояснение термина "локально компактный". На элементах группы можно определить топологию так, чтобы групповая операция и операция взятия обратного были непрерывны. Группа снабжённая такой топологией называется топологической. Характерами топологической группы называются только непрерывные (относительно этой топологии) функции, удовлетворяющие условиям (15). Топологическая группа локально

[32] В дальнейшем слово "скалярный" мы будем опускать, поскольку при рассмотрении абелевых групп нам не понадобятся матричные характеры.

[33] Заметим, что скалярные характеры не различают сопряжённые элементы группы $\phi(a^{-1}ba) = \phi(b)$. Поэтому этого свойства нет для неабелевых групп.

компактна, если у каждого элемента группы есть компактная окрестность. В случае любой конечной группы и группы $\mathbb{Z}$ необходимыми свойствами обладает дискретная топология. Для $\mathbb{R}$ и $\mathbb{C}$ подходит стандартная топология, заданная модулем числа.

В случае, когда $K \simeq X(X(K))$ можно ввести оператор $\Phi : K \times X(K) \to \mathbb{C}$ такой, что при фиксированном $y \in X(K)$ функция $\Phi(x, y)$ является характером группы K, а при фиксированном $x \in K$ — характером группы $X(K)$.

Пример 32. Рассмотрим группу $(\mathbb{R}, +)$. Она локально компактна относительно естестественной топологии, заданной с помощью абсолютной величины числа. Нетрудно проверить, что функции вида $\phi_y(x) = e^{ixy}$, $y \in \mathbb{R}$, удовлетворяют условиям (15). Действительно, $\phi_y(x_1 + x_2) = e^{i(x_1+x_2)y} = e^{ix_1y} \cdot e^{ix_2y} = \phi_y(x_1) \cdot \phi_y(x_2)$, $|\phi_y(x)| = |e^{ixy}| = 1$. Можно показать, что нет других непрерывных на $\mathbb{R}$ функций, удовлетворяют условиям (15).

Из равенства $\phi_{y_1}(x) \cdot \phi_{y_2}(x) = e^{ixy_1} \cdot e^{ixy_2} = e^{ix(y_1+y_2)} = \phi_{y_1+y_2}(x)$ следует, что $X(\mathbb{R}, +) \simeq (\mathbb{R}, +)$.

Пример 33. Рассмотрим группу $(\mathbb{Z}, +)$, как подгруппу в $(\mathbb{R}, +)$. Имеем $\phi_y(n) = e^{iyn}$, $n \in \mathbb{Z}$. Поскольку $\phi_{y+2\pi}(n) = \phi_y(n)$, каждому характеру ϕ_y можно поставить в соответствие точку на единичной окружности, имеющую угол y. Используя естественный изоморфизм $\phi_y \leftrightarrow e^{iy}$, $y \in \mathbb{R}$, получаем[34], что $X(\mathbb{Z}, +) \simeq U(1) \simeq SO(2)$. Ясно, что группа характеров не изменится (с точностью до эквивалентности) при замене аргумента y, поэтому можно определить $\phi_z(n) = e^{2\pi izn}$, $z \in [0, 1)$. По теореме Понтрягина—ван Кампена имеем $X(U(1)) \simeq (\mathbb{Z}, +)$. Действительно, если рассматривать операторы $\phi_z(n)$ как функции от переменной z, имеем равенство $\phi_z(n_1)\phi_z(n_2) = \phi_z(n_1 + n_2)$.

Пример 34. Рассмотрим фактор-группу $\mathbb{Z}_q = (\mathbb{Z}, +)/q\mathbb{Z}$. Теперь нам нужны характеры группы $(\mathbb{Z}, +)$, неразличающие элементы сравнимые по модулю q, т. е. такие, что $\phi_y(n + q) = \phi_y(n)$ для любого $n \in \mathbb{Z}$. Снова ищем характеры в виде $\phi_y(n) = e^{iyn}$. Тогда $y(n + q) = yn + 2\pi k$, т. е. $y = \frac{2\pi k}{q}$. Положим $\xi = e^{2\pi i/q}$, тогда характеры группы $\mathbb{Z}_q$ можно представить в виде $\phi'_k(n) = \xi^{n \cdot k} = e^{\frac{2\pi ink}{q}}$. Поскольку $\phi'_{k_1}(n) \cdot \phi'_{k_2}(n) = e^{\frac{2\pi in}{q}(k_1+k_2)} = e^{\frac{2\pi in}{q}((k_1+k_2) \mod q)} = \phi'_{(k_1+k_2) \mod q}(n)$, имеем $X(\mathbb{Z}_q) \simeq \mathbb{Z}_q$.

Утверждение 72. *Если ϕ — характер конечной группы K, то имеют место равенства*

$$\sum_{x \in K} \phi(x) = 0, \text{ если } \phi \not\equiv 1;$$

[34] Строго говоря, мы показали только, что $U(1) \leq X(\mathbb{Z}, +)$. Однако из того, что $X(U(1)) \geq (\mathbb{Z}, +)$ и теоремы двойственности в обоих случаях имеется изоморфизм.

$$\sum_{x\in K}\phi(x) = |K|, \text{ если } \phi \equiv 1.$$

Доказательство. Для любого $a \in K$ справедливы равенства

$$\sum_{x\in K}\phi(x) = \sum_{x\in K}\phi(x+a) = \phi(a)\sum_{x\in K}\phi(x)$$

Если $\phi \not\equiv 1$, то найдётся $a \in K$, для которого $\phi(a) \neq 1$. Откуда следует $\sum\limits_{x\in K}\phi(x) = 0$. Иначе $\sum\limits_{x\in K}\phi(x) = |K|$. □

Из теоремы 32 и утверждения 72 имеем

Следствие 32. *Для конечной абелевой группы K имеют место равенства*

$$\sum_{\phi\in X(K)}\phi(x) = |X(K)|, \text{ если } x - \text{нейтральный элемент группы } K;$$

$$\sum_{\phi\in X(K)}\phi(x) = 0 \text{ в противном случае.}$$

В пространстве $\mathbb{V}(K)$ можно определить скалярное произведение. В случае конечной группы K пространство $\mathbb{V}(K)$ конечномерно и скалярное произведение в $\mathbb{V}(K)$ можно определить равенством $(f,g) = \sum\limits_{x\in K} f(x)\overline{g(x)}$.

Утверждение 73. *Множество характеров конечной абелевой*[35] *группы образует ортогональный базис в пространстве $\mathbb{V}(K)$.*

Доказательство. Начнём с доказательства ортогональности характеров. Пусть $a \in K$. Из определения характеров и инвариантности скалярного произведения относительно сдвига аргумента имеем равенства $(\phi_1,\phi_2) = \sum\limits_{x\in K}\phi_1(x)\overline{\phi_2(x)} = \sum\limits_{x\in K}\phi_1(x+a)\overline{\phi_2(x+a)} = \phi_1(a)\cdot\overline{\phi_2(a)}\cdot(\phi_1,\phi_2)$.

Если $\phi_1 \neq \phi_2$, то найдётся $a \in K$ такой, что $\phi_1(a)\overline{\phi_2(a)} \neq 1$. Следовательно $(\phi_1,\phi_2) = \sum\limits_{x\in K}\phi_1(x)\cdot\overline{\phi_2(x)} = 0$.

Теперь докажем что система характеров полна. Имеем неравенство $\dim\mathbb{V}(K) = |K| \geq |X(K)|$. Обратное неравенство следует из теоремы двойственности Понтрягина—ван Кампена. Рассмотрим характеры на группе $X(K)$: $\dim\mathbb{V}(X(K)) = |X(K)| \geq |X(X(K))| = |K|$, так как $X(X(K)) \simeq K$. Таким образом, число характеров совпадает с размерностью пространства $\mathbb{V}(K)$. □

[35] Как видно из доказательства, характеры любой, в частности неабелевой, группы ортогональны.

Следствие 33. *Для конечной абелевой группы K имеем $|X(K)| = |K|$.*

Заметим, что если построенное множество характеров составляет базис пространства $\mathbb{V}(K)$, то других характеров у группы K нет. Отсюда следует, что в примерах 33 и 34 определены все характеры групп $U(1)$ и $\mathbb{Z}_q$.

Утверждение 74. *Пусть K_1 и K_2 — конечные абелевы группы и $K = K_1 \times K_2$ — прямое произведение групп. Тогда $X(K) = X(K_1) \times X(K_2)$.*

Доказательство. Рассмотрим характеры $\phi_{z_1} \in X(K_1)$, $\phi_{z_2} \in X(K_2)$. Их произведение $(\phi_{z_1} \cdot \phi_{z_2})(x_1, x_2) \stackrel{df}{=} \phi_{z_1}(x_1) \cdot \phi_{z_2}(x_2)$ является характером группы K. Условия (15) легко проверить непосредственно. Число построенных характеров равно $|X(K_1)||X(K_2)|$. Оно совпадает с мощностью группы $X(K)$ равной $|K_1||K_2|$. □

Известно, что любая конечная абелева группа K изоморфна декартову произведению (прямой сумме) циклических групп $\mathbb{Z}_q$, $q \in \mathbb{N}$. Тогда из утверждения 74 и примера 34 следует, что $K \simeq X(K)$ для любой конечной абелевой группы K.

Утверждение 75. *Пусть K_1 — подгруппа абелевой группы K. Тогда для любого характера $\phi \in X(K_1)$ найдётся характер $\widetilde{\phi} \in X(K)$ такой, что $\phi = \widetilde{\phi}|_{K_1}$.*

Доказательство. Рассмотрим факторгруппу K/K_1. Каждый элемент $x \in K$ единственным образом представим в виде суммы $x = x_1 + x_2$, где $x_1 \in K_1$, $x_2 \in K_2$, группа K_2 изоморфна факторгруппе K/K_1. Определим $\widetilde{\phi}(x) = \phi(x_1)$. Нетрудно проверить, что $\widetilde{\phi}$ удовлетворяет условию (15). □

Пусть $K_1 \subset K$ определим подгруппу $K_1^\perp$ в $X(K)$ равенством

$$K_1^\perp = \{z \in X(K) \mid \phi_z(x) = 1, \text{ если } x \in K_1\}.$$

Если конечная абелева группа K представима в виде декартова произведения групп $K = K_1 \times K_2$, то можно рассматривать подгруппы $K_1 \simeq K_1 \times \{e_2\}$ и $K_2 \simeq \{e_1\} \times K_2$ как подмножества K, где e_1 и e_2 — нейтральные элементы групп K_1 и K_2. Из утверждения 74 имеем, что $X(K) = X(K_1) \times X(K_2)$. Нетрудно видеть, что в этом случае $K_1^\perp \simeq X(K_2)$. Докажем аналогичный факт в несколько более общем случае.

Утверждение 76. *Пусть K_1 — подгруппа конечной абелевой группы K. Тогда $K_1^\perp \simeq X(K/K_1)$.*

Доказательство. Рассмотрим факторгруппу K/K_1. Каждый элемент $x \in K$ единственным образом представим в виде суммы $x = x_1 + x_2$, где $x_1 \in K_1$, $x_2 \in K_2$, группа K_2 изоморфна факторгруппе K/K_1. Для любого $\phi \in X(K_2)$ определим характер $\widetilde{\phi} \in X(K)$ равенством $\widetilde{\phi}(x) = \phi(x_2)$. Имеем $\widetilde{\phi} \in K_1^{\perp}$, поскольку $\widetilde{\phi}(x_1) = \widetilde{\phi}(x_1 + e) = \phi(e) = 1$. Таким образом, $X(K/K_1)$ содержится в $K_1^{\perp}$.

Рассмотрим в $X(X(K))$ две подгруппы: $X(X(K_1))$ и $X(K_1^{\perp})$. Нетрудно видеть, что они пересекаются только по нейтральному элементу. Поэтому $|K_1||K_1^{\perp}| = |X(X(K_1))||X(K_1^{\perp})| \leq |X(X(K))| = |K|$. Тогда $|K_1^{\perp}| \leq |K|/|K_1| = |X(K/K_1)|$. □

Пример 35. Как показано в примере 34, характерами группы $\mathbb{Z}_q$ являются функции $\phi_y(x) = \xi^{x \cdot y}$, где $\xi = e^{2\pi i/q}$ и $x, y \in \mathbb{Z}_q$. Тогда характерами группы $\mathbb{Z}_q^n$ являются функции $\xi^{\langle x,y \rangle}$, где $x, y \in \mathbb{Z}_q^n$ и $\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n \mod q$.

Отметим, что в формуле характера $\xi^{\langle x \cdot y \rangle}$ произведение $\langle x \cdot y \rangle = x_1 y_1 + \cdots + x_n y_n$ можно рассматривать как по модулю q так и в целых числах, поскольку $\xi^a = \xi^{a \mod q}$.

Пусть K — конечная абелева группа. $A \subset K$, $0 \notin A$, $-A = A$. Рассмотрим[36] $Cay(K, A)$ — граф Кэли группы K с множеством образующих A.

Утверждение 77. *Характер ϕ группы K является собственным вектором матрицы смежности M графа $Cay(K, A)$ с собственным числом $\sum\limits_{a \in A} \phi(a)$.*

Доказательство. $(M\phi)(x) = \sum\limits_{a \in A} \phi(x+a) = \sum\limits_{a \in A} \phi(x)\phi(a) = \phi(x) \left(\sum\limits_{a \in A} \phi(a) \right)$. □

Следствие 34. *Каждое собственное подпространство матрицы смежности графа $Cay(K, A)$ имеет базис, состоящий их характеров группы K.*

Утверждение 78. *Характер ϕ группы K является совершенной раскраской[37] графа $Cay(K, A)$.*

Доказательство. Вершина цвета $\phi(x)$ смежна с вершинами цветов $\{\phi(x+a) \mid a \in A\} = \{\phi(x)\phi(a) \mid a \in A\}$. Значит если цвета двух вершин совпадают, т. е. $\phi(x_1) = \phi(x_2)$, то цветовой состав их окрестностей тоже совпадает. □

[36] О спектре графов Кэли смотри также в [6]

[37] Здесь комплексные числа называем цветами раскраски.

Следствие 35. *Характеры ϕ_z группы $\mathbb{Z}_q^n$ являются совершенными раскрасками гиперкуба Q_q^n с матрицей параметров, зависящей только от* $\mathrm{wt}(z)$.

11.2 Многочлены Кравчука и характеры в гиперкубах

Гиперкуб Q_q^n является графом Кэли группы $\mathbb{Z}_q^n$ с множеством образующих, состоящим из наборов веса 1. Найдём собственные числа, соответствующие характерам $\phi_z(x) = \xi^{\langle x \cdot z \rangle}$. Пусть $\mathrm{wt}(z) = d(z, \bar{0}) = |\mathrm{supp}(z)|$ — вес набора z. Имеем равенства

$$\sum_{a \in A} \phi_z(a) = \sum_{a \in A} \xi^{<a,z>} = \sum_{\substack{a \in A \\ \mathrm{supp}(z) \cap \mathrm{supp}(a) = \varnothing}} \xi^{<a,z>} + \sum_{\substack{a \in A \\ \mathrm{supp}(z) \cap \mathrm{supp}(a) \neq \varnothing}} \xi^{<a,z>}.$$

Вычислим слагаемые отдельно. Любой элемент $a \in A$ имеет вид $a = (0, \ldots, 0, a_i, 0, \ldots, 0)$ для некоторого $a_i = b \in \mathbb{Z}_q$, $b \neq 0$. Для любого фиксированного $z \in \mathbb{Z}_q$ представим обе суммы в виде

$$\sum_{\substack{a \in A \\ \mathrm{supp}(z) \cap \mathrm{supp}(a) = \varnothing}} \xi^{<a,z>} = \sum_{i : z_i = 0} \sum_{a \in A, a_i \neq 0} \xi^{<a,z>}; \qquad \sum_{\substack{a \in A \\ \mathrm{supp}(z) \cap \mathrm{supp}(a) \neq \varnothing}} \xi^{<a,z>} = \sum_{i : z_i \neq 0} \sum_{a \in A, a_i \neq 0} \xi^{<a,z>}.$$

Имеем

$$\sum_{a \in A, a_i \neq 0} \xi^{<a,z>} = \sum_{b \in \mathbb{Z}_q \setminus \{0\}} 1 = q - 1, \text{ если } z_i = 0; \tag{16}$$

$$\sum_{a \in A, a_i \neq 0} \xi^{<a,z>} = \sum_{b \in \mathbb{Z}_q \setminus \{0\}} \xi^{z_i b} = -1, \text{ если } z_i \neq 0;$$

где последнее равенство следует из Утверждения 72. Тогда

$$\sum_{a \in A} \phi_z(a) = (n - \mathrm{wt}(z))(q-1) + (-1)\mathrm{wt}(z) = n(q-1) - \mathrm{wt}(z)q.$$

Значит собственными числами гиперкуба Q_q^n являются числа $-n, -n + q, \ldots, n(q-1)$.

Вычислим значения многочленов Кравчука $P_t[n, q]$ для гиперкубов Q_q^n. Из утверждения 18 имеем

$$P_t[n,q](n(q-1) - \mathrm{wt}(z)q) = \phi_z(\bar{0}) \left(\sum_{x : \mathrm{wt}(x) = t} \phi_z(x) \right).$$

Без ограничения общности полагаем, что $z = (1, \ldots, 1, 0, \ldots, 0)$, $\mathrm{wt}(z) = k$. Разделим множество векторов веса t на группы, в каждой из которых содержатся вектора с одинаковым носителем. Пусть в некоторую группу

входят вектора, точно m ненулевых координат которых находятся с 1-ой по k-ую позицию. Из формул (16) сумма $\sum_x \phi_z(x)$ по всем векторам x из такой группы равна $(q-1)^{t-m}\sum\limits_x \xi^{x_{i_1}+\cdots+x_{i_m}} =$

$= (q-1)^{t-m}(\sum\limits_{x_{i_1}\neq 0}\xi^{x_{i_1}})\cdots(\sum\limits_{x_{i_m}\neq 0}\xi^{x_{i_m}}) = (-1)^m(q-1)^{t-m}$. Для каждого m число таких групп равно $\binom{n-k}{t-m}\binom{k}{m}$. Тогда справедливо равенство

$$P_t[n,q](n(q-1)-kq) = \sum_{m=0}^{t}(-1)^m(q-1)^{t-m}\binom{n-k}{t-m}\binom{k}{m},$$

где при $k < m$ или $n-k < t-m$ соответствующие слагаемые равны нулю.

Найдём производящую функцию для многочленов Кравчука. Обозначим через y независимую переменную. Для любого $x \in Q_q^n$ верно равенство $y^{\mathrm{wt}(x)} = y^{\mathrm{wt}(x_1)}\cdots y^{\mathrm{wt}(x_n)}$. По-прежнему полагаем, что $z = (1,\ldots,1,0,\ldots,0)$, $\mathrm{wt}(z) = k$. Используя утверждение 18 и формулы (16), получаем равенства

$$\sum_{x\in Q_q^n}\phi_z(x)y^{\mathrm{wt}(x)} = \sum_{t=0}^{n} y^t\left(\sum_{x:\mathrm{wt}(x)=t}\phi_z(x)\right) = \sum_{t=0}^{n} y^t P_t[n,q](n(q-1)-\mathrm{wt}(z)q);$$

$$\sum_{x\in Q_q^n}\phi_z(x)y^{\mathrm{wt}(x)} = \sum_{x\in Q_q^n}\xi^{x_1}\cdots\xi^{x_k}y^{\mathrm{wt}(x_1)}\cdots y^{\mathrm{wt}(x_n)} =$$

$$= \left(\prod_{i=1}^{k}\sum_{x_i\in Q_q}\xi^{x_i}y^{\mathrm{wt}(x_i)}\right)\left(\prod_{i=k+1}^{n}\sum_{x_i\in Q_q}y^{\mathrm{wt}(x_i)}\right) = (1-y)^k(1+(q-1)y)^{n-k}.$$

Таким образом,

$$(1+(q-1)y)^{n-k}(1-y)^k = \sum_{t=0}^{n}P_t[n,q](\lambda_k)y^t, \tag{17}$$

где $\lambda_k = n(q-1)-kq$.

11.3 Матрицы Адамара

Рассмотрим матрицу $H_{q,n}$ размера $q^n \times q^n$, строками которой являются характеры $\phi_z(x)$, т. е. $H_{q,n}(z,x) = \phi_z(x)$. Из свойств характеров следует, что $H_{q,n}H_{q,n}^* = mI_m$, где $m = q^n$.

Определение 52. *Матрицей Адамара H размера $m \times m$ называется матрица, удовлетворяющая равенству $HH^{\mathrm{T}} = mI_m$ и состоящая только из ± 1.*

Матрицы, состоящие только из степеней ξ, $\xi = e^{2\pi i/q}$, и удовлетворяющие равенству $HH^* = mI_m$,называются обобщёнными матрицами Адамара.

Очевидно, матрица Адамара становится ортогональной (унитарной) при домножении на $\frac{1}{\sqrt{m}}$. Из определений матриц и характеров видно, что матрицы $H_{q,n}$ являются симметричными. Матрица $H_{2,n}$ размера $2^n \times 2^n$ называется матрицей Адамара—Сильвестра.

Ясно, что перестановки строк или столбцов обобщённой матрицы Адамара не выводят её из класса таких матриц. Кроме того, умножение на ξ^j столбца или строки обобщённой матрицы Адамара, составленной из степеней $\xi = e^{2\pi i/q}$, не выводит матрицу из этого класса. Обобщённые матрицы Адамара, полученные друг из друга такими преобразованиями, называются эквивалентными.

Утверждение 79. *Если H_{n_1} и H_{n_2} — обобщённые матрицы Адамара, то $H_{n_1} \otimes H_{n_2}$ является обобщённой матрицей Адамара.*

Доказательство. $(H_{n_1} \otimes H_{n_2})(H_{n_1} \otimes H_{n_2})^* = (H_{n_1} \otimes H_{n_2})(H_{n_1}^* \otimes H_{n_2}^*) = (H_{n_1} H_{n_1}^*) \otimes (H_{n_2} H_{n_2}^*) = n_1 I_{n_1} \otimes n_2 I_{n_2} = n_1 n_2 I_{n_1 n_2}$. □

Пример 36. Матрица Адамара—Сильвестра

$$H_{2,3} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}.$$

Нетрудно показать, что матрицы Адамара размера $m \times m$ могут существовать только, когда число m делится на 4 (за исключением $m = 1, 2$). Известна гипотеза о том, что это условие является достаточным для существования матриц Адамара.

Домножением строк и столбцов на -1 любую матрицу Адамара можно преобразовать так, чтобы первый столбец и первая строка состояли из одних единиц. Тогда в других строках и столбцах окажется ровно по половине элементов 1 и -1. Рассмотрим матрицу A_m размера $(4m+3) \times (4m+3)$, которая получается из приведённой матрицы Адамара удалением первой строки, первого столбца и заменой -1 на 0. Строки матрицы A_m можно рассматривать как наборы из Q_2^{4m+3} веса $2m+1$.

Утверждение 80. *Набор строк матрицы A_m является комбинаторным дизайном с параметрами $2-(4m+3, 2m+1, m)$.*

Доказательство. Достаточно проверить, что для каждой пары столбцов матрицы A_m имеется ровно m строк, в пересечении с которыми в столбцах находятся единицы. Действительно, в исходной матрице Адамара имелось по $2m$ элементов 1 и -1 в каждом столбце (за исключением первого). Тогда $s(1,1) + s(1,-1) = s(-1,1) + s(-1,-1) = 2m+2$, где

$s(\delta_1, \delta_2)$ — число пар (δ_1, δ_2) в двух столбцах. Из ортогональности матрицы Адамара следует равенство $s(1,1)+s(-1,-1) = s(1,-1)+s(-1,1)$. Тогда $s(1,1) = m+1$ и исключив первую строку из рассмотрения получаем требуемое. □

Как видно из построения, число блоков в дизайне с параметрами $2-(4m+3, 2m+1, m)$ равняется числу элементов, т. е. $4m+3$. Поэтому такой дизайн является симметричным. Нетрудно видеть, что если из наборов дизайна с параметрами $2-(4m+3, 2m+1, m)$ составить матрицу, заменить в ней 0 на -1 и добавить строку и столбец из единиц, то мы получим матрицу Адамара. Ортогональность столбцов полученной матрицы следует из параметров дизайна.

11.4 Определение и свойства преобразования Фурье

Определение 53. *Пусть ϕ_z — характеры группы K. Преобразованием Фурье функции $f \in V(K)$ называется функция $\widehat{f}(z) = \mu \cdot (f, \phi_z)$, действующая из группы характеров $X(K)$ в $\mathbb{C}$. Множитель $\mu \in \mathbb{R}$ выберем так, чтобы преобразование Фурье сохраняло норму функции $\|\widehat{f}\|_2 = \|f\|_2 = \sqrt{(f,f)}$.*

Пример 37. Если $K = (\mathbb{R}, +)$, то скалярное произведение определяется равенством

$$(a,b) = \int\limits_{\mathbb{R}} a(x)\overline{b(x)}dx$$

и

$$\widehat{f}(z) = \frac{1}{\sqrt{2\pi}} \int\limits_{\mathbb{R}} f(x)e^{-ixz}dx.$$

Пример 38. Если $K = U(1)$, то скалярное произведение определяется равенством

$$(a,b) = \int\limits_{0}^{2\pi} a(x)\overline{b(x)}dx$$

и

$$\widehat{f}(n) = \frac{1}{\sqrt{2\pi}} \int\limits_{0}^{2\pi} f(x)e^{-inx}dx.$$

В этом случае результат преобразования Фурье можно рассматривать как набор коэффициентов разложения в ряд Фурье.

Пример 39. Если $K = \mathbb{Z}_q^n$, то скалярное произведение определяется равенством

$$(a,b) = \sum_{x \in \mathbb{Z}_q^n} a(x)\overline{b(x)}$$

и

$$\widehat{f}(z) = \frac{1}{q^{n/2}} \sum_{x \in \mathbb{Z}_q^n} f(x) \overline{\xi}^{\langle x,z \rangle}.$$

В случае $K = \mathbb{Z}_q$, т. е. когда $n = 1$, данное преобразование Фурье называется дискретным преобразованием Фурье.

Рассмотрим частный случай $K = \mathbb{Z}_2^n$. Имеем $\xi = -1$ и

$$\widehat{f}(z) = \frac{1}{2^{n/2}} \sum_{(x_1,\ldots,x_n) \in \mathbb{Z}_2^n} f(x_1,\ldots,x_n) \cdot (-1)^{x_1 z_1} \cdots (-1)^{x_n z_n} = \frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}_2^n} f(x) (-1)^{<x,z>}.$$

Отметим, что во всех перечисленных случаях, за исключением $K = U(1)$, группа $X(K)$ изоморфна группе K. Как было отмечено выше, группа $X(K)$ изоморфна группе K для любой конечной абелевой группы. В этом случае можно считать, что преобразование Фурье действует из $\mathbb{V}(K)$ в $\mathbb{V}(K)$. Далее всюду считаем, что K — конечная абелева группа и преобразование Фурье действует из $\mathbb{V}(K)$ в $\mathbb{V}(K)$ по формуле:

$$\widehat{f}(z) = \frac{1}{|K|^{1/2}} (f, \phi_z) = \frac{1}{|K|^{1/2}} \sum_{x \in K} f(x) \overline{\phi_z(x)}.$$

Замечание 16. Строки обобщённой матрицы Адамара $H_{q,n}$ являются векторами значений характеров в группе $\mathbb{Z}_q^n$. Поэтому преобразование Фурье от функции на группе $\mathbb{Z}_q^n$ совпадает с умножением матрицы $H_{q,n}$ на вектор значений функции, т. е. $\widehat{f} = \frac{1}{q^{n/2}} H_{q,n} f$.

Утверждение 81. *Справедливо равенство*

$$f(x) = \frac{1}{|K|^{1/2}} \sum_{z \in K} \widehat{f}(z) \phi_z(x).$$

Доказательство. Из определения характера имеем $\phi_z(x)\phi_z(-x) = \phi_z(0) = 1$. Значит $\phi_z(-x) = \overline{\phi_z(x)}$.

Тогда имеем равенство $\|\phi_z\|_2^2 = \sum\limits_{x \in K} \phi_z(x) \overline{\phi_z(x)} = \sum\limits_{x \in K} \phi_z(x) \phi_z(-x) = |K|$. Из утверждения 73 следует, что функции $\phi_z / |K|^{1/2}$ образуют ортонормированный базис. Из определения преобразования Фурье следует, что числа $\widehat{f}(z)$ есть коэффициенты разложения функции f по базису характеров. □

Утверждение 82 (теорема Планшереля)**.** *Для функций на конечных абелевых группах справедливо равенство* $(f, g) = (\widehat{f}, \widehat{g})$.

Доказательство. Применим комплексное сопряжение к равенству из утверждения 81

$$\overline{g(x)} = \frac{1}{|K|^{1/2}} \sum_{z \in K} \overline{\widehat{g}(z) \phi_z(x)}.$$

Используя ортогональность характеров, получаем равенства

$$(f,g) = \frac{1}{|K|}\sum_{z\in K}\widehat{f}(z)\overline{\widehat{g}(z)}\|\phi_z\|^2 = \sum_{z\in K}\widehat{f}(z)\overline{\widehat{g}(z)} = (\widehat{f},\widehat{g}).$$

□

Из утверждения 82 при $f = g$ следует равенство Парсеваля

$$\|f\|_2^2 = (f,f) = \frac{1}{|K|}\sum_{z\in K}|\widehat{f}(z)|^2\|\phi_z\|_2^2 = \sum_{z\in K}|\widehat{f}(z)|^2 = \|\widehat{f}\|_2^2.$$

Утверждение 83. $\widehat{\widehat{f}}\,(x) = f(-x)$.

Доказательство. Из определения преобразования Фурье имеем равенство

$$\widehat{\widehat{f}}\,(x) = \frac{1}{|K|^{1/2}}(\widehat{f},\phi_x) = \frac{1}{|K|^{1/2}}\sum_{z\in K}\widehat{f}(z)\overline{\phi_x(z)}.$$

Из утверждения 81 имеем

$$f(-x) = \frac{1}{|K|^{1/2}}\sum_{z\in K}\widehat{f}(z)\phi_z(-x).$$

Из теоремы двойственности Понтрягина—ван Кампена следует, что имеется следующее представление характеров: $\Phi(x,z) = \phi_z(x) = \phi_x(z)$. А из определения характера имеем равенство $\phi_z(-x) = \overline{\phi_z(x)}$. □

Утверждение 84. *Ненулевая функция $f : Q_q^n \to \mathbb{C}$ является собственной с собственным числом $\lambda = n(q-1)-kq$ тогда и только тогда, когда $\widehat{f}(z) = 0$ для всех $z \in Q_q^n$, $\mathrm{wt}(z) \neq k$.*

Доказательство. Как было показано выше характеры составляют базис пространства $\mathbb{V}(K)$ и являются собственными функциями гиперкуба Q_q^n. Тогда из них можно составить базисы собственных подпространств гиперкуба. Следовательно характеры ϕ_z такие, что $\mathrm{wt}(z) = k$, составляют базис собственного подпространства с собственным числом $\lambda = n(q-1) - kq$. □

Утверждение 85 (свойства преобразования Фурье)**.**
1) $\widehat{f+g} = \widehat{f} + \widehat{g}$; $\widehat{c\cdot f} = c\cdot\widehat{f}$, *где c — константа (линейность);*
2) $\widehat{f(-x)}(z) = \widehat{f}(-z)$, *причём если f — вещественная функция, то* $\widehat{f}(-z) = \overline{\widehat{f}(z)}$;
3) $\widehat{f(x+a)}(z) = \phi_z(a)\widehat{f}(z)$ *и* $\widehat{f}(z+a) = \widehat{f\cdot\overline{\phi_a}(x)}(z)$ *(сдвиг аргумента).*

Доказательство. Линейность преобразования Фурье (п.1)) очевидна из определения. Докажем п.2)

$$\widehat{f(-x)}(z) = \frac{1}{|K|^{1/2}} \sum_{x\in K} f(-x)\overline{\phi_z(x)} = \frac{1}{|K|^{1/2}} \sum_{y\in K} f(y)\overline{\phi_z(-y)}.$$

Из теоремы двойственности и определения характера имеем равенства $\phi_z(-y) = \phi_{-z}(y) = \overline{\phi_z(y)}$. Тогда

$$\widehat{f(-x)}(z) = \frac{1}{|K|^{1/2}} \sum_{y\in K} f(y)\overline{\phi_{-z}(y)} = \widehat{f}(-z).$$

Если $f(y) = \overline{f(y)}$, то

$$\widehat{f(-x)}(z) = \frac{1}{|K|^{1/2}} \sum_{y\in K} \overline{f(y)\phi_z(-y)} = \frac{1}{|K|^{1/2}} \sum_{y\in K} \overline{f(y)}\phi_z(y) = \overline{\widehat{f}(z)}.$$

Докажем свойство сдвига аргумента. Заменяя переменную x на $y = x + a$, получаем равенства

$$\widehat{f(x+a)}(z) = \frac{1}{|K|^{1/2}} \sum_{x\in K} f(x+a)\overline{\phi_z(x)} = \frac{1}{|K|^{1/2}} \sum_{y\in K} f(y)\overline{\phi_z(y-a)} =$$

здесь мы воспользуемся равенствами

$$\overline{\phi_z(y-a)} = \overline{\phi_z(y)} \cdot \overline{\phi_z(-a)} = \overline{\phi_z(y)} \cdot \phi_z(a)$$

и продолжим цепочку равенств

$$= \frac{\phi_z(a)}{|K|^{1/2}} \sum_{y\in K} f(y)\overline{\phi_z(y)} = \phi_z(a)\widehat{f}(z).$$

Докажем свойство последнее равенство.

$$\widehat{f\cdot\overline{\phi_a}(x)}(z) = \frac{1}{|K|^{1/2}} \sum_{x\in K} f(x)\overline{\phi_a(x)}\cdot\overline{\phi_z(x)} = \frac{1}{|K|^{1/2}} \sum_{x\in K} f(x)\overline{\phi_{a+z}(x)} = \widehat{f}(z+a).$$

□

Определим дельта-функцию Дирака на группе K:

$$\delta(x) = \begin{cases} |K|^{1/2}, & x = 0 \\ 0, & x \neq 0. \end{cases}$$

Применим преобразование Фурье к характеру:

$$\widehat{\phi_z(x)}(y) = \frac{1}{|K|^{1/2}}(\phi_z(x), \phi_y(x)) = \delta(y-z).$$

Имеем равенство $\widehat{\phi_0} = \widehat{\mathbf{1}} = \delta$. Из утверждения 83 следует обратное равенство $\widehat{\delta} = \mathbf{1}$.

Утверждение 86 (принцип неопределённости [93]). *Для любой функции $f \in \mathbb{V}(K)$ верно неравенство*

$$|K| \leq |\mathrm{supp}(f)| \cdot |\mathrm{supp}(\widehat{f})|.$$

Доказательство. Из равенства Парсеваля следует, что $\|f\|_2^2 = \sum\limits_{z \in K} |\widehat{f}(z)|^2 \leq (\max\limits_z |\widehat{f}(z)|^2) \cdot |\mathrm{supp}(\widehat{f})|$.

Из равенства $|\phi_z(x)|^2 = 1$ для любого $x \in K$ и неравенства Коши—Буняковского: $(u, v)^2 \leq \|u\|_2^2 \cdot \|v\|_2^2$ получаем

$$|\widehat{f}(z)|^2 = \frac{1}{|K|} \Big| \sum_{x \in \mathrm{supp}(f)} f(x) \overline{\phi_z(x)} \Big|^2 \leq \frac{1}{|K|} \|f\|_2^2 \cdot |\mathrm{supp}(f)|.$$

Если неравенство выполняется для любого $z \in K$, то оно справедливо и для максимального $|\widehat{f}(z)|^2$. Теперь продолжим исходную цепочку неравенств:

$$\|f\|_2^2 \leq \frac{1}{|K|} \|f\|_2^2 \cdot |\mathrm{supp}(f)| \cdot |\mathrm{supp}(\widehat{f})|.$$

□

Равенство в неравенстве из принципа неопределённости достигается, например, когда f — характер или когда f — характеристическая функция подгруппы группы K, умноженная на характер.

Утверждение 87 (формула суммирования Пуассона). *Пусть K_1 подгруппа конечной абелевой группы K. Для любой функции $f \in \mathbb{V}(K)$ верно равенство*

$$|K|^{1/2} \sum_{x \in K_1} f(x) = |K_1| \sum_{z \in K_1^\perp} \widehat{f}(z).$$

Доказательство.

$$\sum_{z \in K_1^\perp} \widehat{f}(z) = \frac{1}{|K|^{1/2}} \sum_{z \in K_1^\perp} \sum_{x \in K} f(x) \overline{\phi_z(x)} = \frac{1}{|K|^{1/2}} \sum_{x \in K} f(x) \sum_{z \in K_1^\perp} \overline{\phi_z(x)}.$$

Как замечено выше, элемент $x \in K$ можно рассматривать как элемент $X(X(K))$, то есть любой $x \in K$ порождает характер подгруппы $K_1^\perp$, $K_1^\perp \subset X(K)$. Причём любой $x \in K_1$ порождает тождественно единичный характер подгруппы $K_1^\perp$ по определению группы $K_1^\perp$. Благодаря равенству $K \simeq X(X(K)$, из утверждения 76 имеем $|(K_1^\perp)^\perp| = |X(K)|/|K_1^\perp| = |K|/|K_1^\perp| = |K_1|$. Тогда $x \in K$ порождает тождественно единичный характер подгруппы $K_1^\perp$ только если $x \in K_1$. По следствию 32 имеем

$$\sum_{z \in K_1^\perp} \overline{\phi_z(x)} = 0, \text{ если } x \notin K_1,$$

$$\sum_{z\in K_1^\perp} \overline{\phi_z(x)} = |K_1^\perp|, \text{ если } x \in K_1.$$

Тогда

$$\frac{1}{|K|^{1/2}} \sum_{x\in K} f(x) \sum_{z\in K_1^\perp} \overline{\phi_z(x)} = \frac{|K_1^\perp|}{|K|^{1/2}} \sum_{x\in K_1} f(x).$$

Из утверждения 76 имеем $\frac{|K_1^\perp|}{|K|^{1/2}} = \frac{|K|^{1/2}}{|K_1|}$. □

11.5 Преобразования Фурье и свёртка

Определение 54. *Пусть K — некоторая конечная группа и $f, g : K \to \mathbb{C}$. Определим свертку двух функций следующим образом:*

$$(f * g)(y) = \sum_{x\in K} f(x) \cdot g(y - x).$$

Заметим, что для вещественных функций свёртка определяется аналогичным образом, только вместо суммы нужно взять интеграл. Далее мы продолжаем всюду полагать, что группа K абелева.

Утверждение 88 (свойства свёртки)**.** *1. $f * g = g * f$;*

2. $f * (g * h) = (f * g) * h$;

3. $f * (g_1 + g_2) = f * g_1 + f * g_2$;

4. $f * (\alpha g) = \alpha(f * g)$;

5. $f * \delta = |K|^{1/2} f$.

Утверждение 89. $\widehat{f * g} = |K|^{\frac{1}{2}} \widehat{f} \cdot \widehat{g}$.

Доказательство. Из определения характера имеем $\phi_z(y) = \phi_z(x)\phi_z(y - x)$. Тогда из определения свёртки получаем равенства

$$\widehat{f * g}(z) = \frac{1}{|K|^{1/2}} \sum_{y\in K} \overline{\phi_z(y)} \sum_{x\in K} f(x)g(y - x) =$$

$$= \sum_{x\in K} f(x)\overline{\phi_z(x)} \frac{1}{|K|^{1/2}} \sum_{y\in K} g(y - x)\overline{\phi_z(y - x)} = |K|^{1/2} \cdot \widehat{f} \cdot \widehat{g}.$$

□

Утверждение 90. $\widehat{f} * \widehat{g} = |K|^{\frac{1}{2}} \widehat{f \cdot g}$.

Доказательство. Подставим в равенство $\widehat{f * g} = |K|^{\frac{1}{2}} \widehat{f} \cdot \widehat{g}$ функции $\widehat{f}$ и $\widehat{g}$ вместо функций f и g и применим к двум частям равенства преобразование Фурье. Пользуясь тем, что $\widehat{\widehat{f}}(z) = f(-z)$ получаем равенство

$$(\widehat{f} * \widehat{g})(-z) = |K|^{1/2}[f(-\widehat{x) \cdot g}(-x)](z).$$

Воспользуемся равенством $\widehat{f(-x)}(z) = \widehat{f}(-z)$ из утверждения 85(2). Имеем $[f(-\widehat{x) \cdot g}(-x)](z) = [(f \cdot \widehat{g)(-x)}](z) = [(\widehat{f \cdot g)(x)}](-z)$. После замены переменной z на $-z$ получаем требуемое равенство. □

Определение 55. *Преобразование* $\widehat{(-1)^f}$ *булевозначной функции* $f : K \to \{0, 1\}$ *называется преобразованием Адамара—Уолша.*

Теорема 33 (Титсворт, см. [134])**.** *Для любой функции* $f : K \to \{0, 1\}$ *справедливо*

$$\widehat{(-1)^f} * \widehat{(-1)^f} = |K|^{1/2}\delta$$

Доказательство. Из утверждения 90 получаем равенства

$$\widehat{(-1)^f} * \widehat{(-1)^f} = |K|^{1/2}(-1)^{\widehat{f \cdot (-1)}^f} = |K|^{1/2}\widehat{\mathbf{1}} = |K|^{1/2}\delta.$$

□

Таким образом, для функции $h = \widehat{(-1)^f}$, где f — произвольная булевозначная функция имеем

$$h * h(y) = \sum_{z \in K} h(z) \cdot h(y - z) = 0 \text{ при } y \neq 0.$$

Из утверждения 85(2) имеем равенство $h(-z) = \overline{h(z)}$, поскольку $(-1)^f$ — вещественная функция. Тогда

$$(h(z), h(z - y)) = \sum_{z \in K} h(z) \cdot \overline{h(z - y)} = 0 \text{ при } y \neq 0.$$

Отсюда следует, что семейство функций $\{h(z - y) \mid y \in K\}$ является ортогональным базисом пространства $\mathbb{V}(K)$.

Задача 86. Докажите, что все собственные числа любого графа Кэли на группах $\mathbb{Z}_2^n$ и $\mathbb{Z}_4^n$ целые.

Задача 87. Докажите равенство $P_k[n, q](\lambda_m)|S_m| = P_m[n, q](\lambda_k)|S_k|$, где $\lambda_t = n(q - 1) - tq$ и S_t — сфера радиуса t в Q_q^n.

Задача 88. Докажите равенство $\sum\limits_{k=0}^{t} P_k[n, q](\lambda_m) = P_t[n - 1, q](\lambda_{m-1})$.

Задача 89. Докажите равенство
$\sum\limits_{m=0}^{n} P_k[n,q](\lambda_m) = \frac{1}{q}\binom{n+1}{k+1}((q-1)^{k+1} - (-1)^{k+1})$.

Задача 90. Докажите, что $|P_n[n,q](\lambda_m)| = 1$ при любом $m = 0, \ldots, n$.

Задача 91. Докажите, что для любого $x \in Q_2^n$ число булевых функций f, для которых коэффициент Адамара—Уолша $\widehat{(-1)^f}(x)$ равен нулю, равняется $\binom{2^n}{2^{n-1}}$.

Задача 92. Пусть функция $f : Q_2^n \to \mathbb{C}$ равна нулю в вершинах нечётного веса. Докажите, что её коэффициенты Фурье совпадают в противоположных точках булева гиперкуба, т. е. $\widehat{f}(z) = \widehat{f}(z \oplus \bar{1})$.

Задача 93. Докажите, что для любой булевой функции $f : Q_2^n \to Q_2$ r-ые моменты $\sum\limits_{z \in Q_2^n} \widehat{f}^r(z) \geq 0$ неотрицательны. Докажите, что при фиксированном $\mathrm{wt}(f)$ минимальное значение r-ых моментов достигается на характистической функции столбцов проверочной матрицы кода с расстоянием $d+1$.

Задача 94. Докажите, что умножение на счётчик чётности $(-1)^{\mathrm{wt}(x)}$ переводит собственную функцию булева гиперкуба с собственным числом λ в собственную функцию с собственным числом $-\lambda$. Найдите преобразование, переводящее совершенные раскраски булева гиперкуба с матрицей параметров $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ в совершенные раскраски булева гиперкуба с матрицей параметров $\begin{pmatrix} b & a \\ a & b \end{pmatrix}$.

Задача 95. Пусть $C \subset Q_2^n$ и $\widehat{\chi_C}(z) \neq 0$ только если вес $\mathrm{wt}(z)$ нечётен или $z = \bar{0}$. Докажите, что $|C| = 2^{n-1}$, за исключением случаев $C = Q_2^n$ и $C = \varnothing$.

Задача 96. Пусть S_t — множество вершин веса t в Q_q^n. Докажите, что $\widehat{\chi_{S_t}}(z) = \frac{1}{q^{n/2}} P_t[n,q](n(q-1) - \mathrm{wt}(z)q)$.

Задача 97. Пусть $f : Q_2^n \to \mathbb{R}$ — собственная функция булева гиперкуба с собственным числом $\lambda_k = n - 2k$. Докажите, что $|\mathrm{supp}(f)| \geq 2^{(n+|\lambda_k|)/2}$. Приведите примеры функций, для которых в этом неравенстве достигается равенство.

Задача 98. Пусть $g, f : Q_q^n \to \mathbb{C}$. Определим матрицу A_f равенством $A_f(x,y) = f(x-y)$. Докажите, что $A_f A_g = A_{f*g}$. Докажите, что $\det A_f = q^{n/2} \prod\limits_{y \in Q_q^n} \widehat{f}(-y)$.

Задача 99. Рассмотрим булев n-куб ориентированный так, что все его рёбра направлены от вершины меньшего веса к вершине большего веса. Матрица смежности ориентированного графа кососимметрична, она содержит 1 в позиции i, j, если ребро направлено от вершины i к вершине j, и -1 , если ребро направлено от вершины j к вершине i. Найдите собственные числа и собственные векторы матрицы смежности ориентированного n-куба.

Задача 100. Докажите, что если $f \in \mathbb{V}(K)$ собственная функция графа $Cay(K, A)$, то и $f * g$ тоже собственная функция (или тождественно нулевая функция) графа $Cay(K, A)$ для любой функции $g \in \mathbb{V}(K)$.

Задача 101. Докажите, что если $f, g \in \mathbb{V}(K)$ собственные функции графа $Cay(K, A)$ с разными собственными числами, то их свёртка $f * g$ тождественно нулевая функция.

Задача 102. Пусть $f : Q_q^n \to \mathbb{C}$. Докажите, что функция f существенно зависит от переменной x_i тогда и только тогда, когда найдётся вершина $z \in Q_q^n$, $z_i \neq 0$, для которой $\widehat{f}(z) \neq 0$.

Задача 103. Пусть функция $f : Q_q^n \to \mathbb{C}$ принимает только два различных значения. Докажите, что найдутся константы $c_1, c_2 \in \mathbb{C}$ такие, что $\widehat{f} * \widehat{f} = c_1 \widehat{f} + c_2 \delta$.

Задача 104. Пусть $C \subset Q_p^n$, p — простое. Докажите, что если мощность множества C не делится на p, то $\mathrm{supp}(\widehat{\chi_C}) = Q_p^n$.

12 Корреляционно-иммунные функции

12.1 Функции, уравновешенные в гранях

В этом разделе в качестве графа мы будем рассматривать только гиперкубы Q_q^n, поэтому характеры ϕ_z всюду имеют вид $\phi_z(x) = \xi^{\langle x,z\rangle}$, где $\xi = e^{\frac{2\pi i}{q}}$. Однако многие результаты этого раздела могут быть обобщены произвольные графы Кэли абелевых конечных групп.

Вспомним, что гранью Γ размерности $\dim \Gamma = k$ в n-мерном q-ичном кубе Q_q^n называется подмножество его вершин, которое состоит из векторов с зафиксированными некоторыми $n - k$ координатами и произвольными значениями в оставшихся k координатах.

Говорят, что две грани одинаковой размерности имеют одинаковое направление, если номера фиксированных (и свободных) координат у них совпадают. Грань у которой зафиксирована только одна координата называется гипергранью. Подграф в гиперкубе Q_q^n, порождённый гранью размерности k, изоморфен гиперкубу Q_q^k размерности k.

Определение 56. *Функция $f : Q_q^n \to \mathbb{C}$ называется уравновешенной в гранях размерности k, если для любой грани Γ размерности k, выполняется равенство $\sum\limits_{x\in\Gamma} f(x) = 0$.*

Заметим, что если функция уравновешена в гранях размерности k, то она уравновешена и в гранях большей чем k размерности.

Утверждение 91. *Пусть функция $f : Q_2^n \to \mathbb{C}$ уравновешена в гранях размерности k. Тогда f однозначно восстанавливается по своим значениям в шаре радиуса $k-1$ (т. е. по значениям в вершинах веса не более $k-1$).*

Доказательство. Докажем утверждение по индукции. Рассмотрим произвольную вершину z веса k. Найдётся грань размерности k, которая содержит z и все вершины y такие, что вектор y не содержит единиц в нулевых координатах вектора z. Очевидно, что z — единственная вершина веса k в этой грани. Из уравновешенности следует, что значение $f(z)$ определяется однозначно. Если f уравновешена в гранях размерности k, то она уравновешена в гранях $k+i$, $i \geq 0$. Поэтому, после нахождения значений $f(z)$ для всех вершин z веса k мы можем найти значения $f(z)$ во всех вершинах веса $k+1$ и т. д. □

Функции, уравновешенные в гранях фиксированной размерности, образуют линейное подпространство в $\mathbb{V}(Q_q^n)$. Покажем, что базис этого пространства можно составить из характеров группы $\mathbb{Z}_q^n$.

Утверждение 92. *Если $\mathrm{wt}(z) = k$, то характер ϕ_z уравновешен в гранях размерности $n-k+1$ и найдётся такое направление граней размерности $(n-k)$, что во всех гранях направления функция ϕ_z постоянна.*

Доказательство. Без ограничения общности можно считать, что $z = (z_1, \ldots, z_k, 0, \ldots, 0)$, $z_i \neq 0$.

Рассмотрим произвольную грань Γ размерности $n-k+1$, она имеет хотя бы одну свободную координату x_i из первых k. Можно считать, что $i = 1$. Из утверждения 72 имеем $\sum\limits_{x\in Q_q} \xi^{xz_i} = 0$. Тогда

$$\sum_{x\in\Gamma} \phi_z(x) = \sum_{x_{i_2},\ldots,x_{i_{n-k}}} \sum_{x_1} \phi_z(x) = \sum_{x_{i_2},\ldots,x_{i_{n-k}}} \xi^{\langle (z_2,\ldots,z_n),(x_2,\ldots,x_n)\rangle} \sum_{x_1} \xi^{z_1 x_1} = 0.$$

Теперь рассмотрим грань грань Γ размерности $n-k$, у которой фиксированы первые k координат: $x_1 = a_1, \ldots, x_k = a_k$. Для любой вершины $x \in \Gamma$ верно равенство

$$\phi_z(x) = \xi^{\langle (z_1,\ldots,z_n),(x_1,\ldots,x_n)\rangle} = \xi^{z_1 a_1 + \cdots + z_k a_k}.$$

□

Утверждение 93. *Функция $f : Q_q^n \to \mathbb{C}$ уравновешена в гранях размерности k тогда и только тогда, когда $\widehat{f}(z) = 0$ для всех $z \in Q_q^n$ веса $\mathrm{wt}(z) \leq n - k$.*

Доказательство. ($\Leftarrow$) Пусть $\widehat{f}(z) = 0$ при $\mathrm{wt}(z) \leq n-k$. Из утверждения 81 имеем

$$f(x) = \frac{1}{q^{n/2}} \sum_{\mathrm{wt}(z)>n-k} \widehat{f}(z)\phi_z(x).$$

По утверждению 92 все функции $\phi_z(x)$ при $\mathrm{wt}(z) \geq n - k + 1$ уравновешены в гранях размерности k.

($\Rightarrow$) Рассмотрим

$$\widehat{f}(z) = \frac{1}{q^{n/2}}(f, \phi_z), \text{ где } \mathrm{wt}(z) \leq n - k.$$

По утверждению 92 функция ϕ_z постоянна на гранях Γ размерности k (или больше k) некоторого направления. Так как функция f уравновешена, то $\sum\limits_{x\in\Gamma} f(x)\overline{\phi_z(x)} = \overline{\phi_z(a)} \sum\limits_{x\in\Gamma} f(x) = 0$. Поскольку вершины гиперкуба разбиваются на грани любого направления, имеем $\widehat{f}(z) = 0$. □

12.2 Корреляционная иммунность и преобразование Фурье

Пусть $E(f)$ — множество значений, которое принимает функция f.

Определение 57. *Функция f называется корреляционно-иммунной порядка k, если для любого $b \in E(f)$ она принимает значение b одинаковое число раз во всех гранях размерности $n - k$.*

Если функция равномерно распределена в гранях малой размерности, то это же свойство будет выполняться и для граней большей размерности. В силу этого удобно ввести обозначение $\mathrm{cor}(f)$ для максимума порядка корреляционной иммунности функции f.

Из определения МДР-кода следует, что $\mathrm{cor}(\chi_C) = n - d + 1$, где χ_C — характеристическая функция МДР-кода с кодовым расстоянием d. Ясно, что если МДР-код существует, то это минимальное по мощности непустое множество с такой корреляционной иммунностью.

Пример 40. Для постоянной функции в n-мерном гиперкубе $\mathrm{cor}(const) = n$. Булев счётчик чётности $f(x_1, \ldots, x_n) = x_1 + \cdots + x_n \mod 2$ имеет $\mathrm{cor}(f) = n - 1$.

Пример 41. Латинские раскраски (см. пример 18) являются корреляционно-иммунными функциями порядка $n - 1$ в n-мерном q-ичном гиперкубе.

Корреляционно-иммунные функции применяются в криптографии для моделирования случайного распределения значений в вершинах гиперкуба. Рассмотрим задачу нахождения значения функции при частично известном аргументе. Пусть злоумышленнику известны функция $f : Q_q^n \to E(f)$ и значения k из n переменных. Его задача состоит в том, чтобы определить значение функции. Если $\mathrm{cor}(f) \geq k$, то в каждой грани размерности $n-k$ функция принимает любое значение b с той же частотой, что и во всём гиперкубе. Поэтому знание значений k переменных не добавляет никакой новой информации о значении функции. Также можно рассмотреть задачу, когда злоумышленнику известно значение функции $f(x) = b$ и значения k из n переменных, а его задача состоит в определении остальных аргументов. Если $\mathrm{cor}(f) \geq k$, то имеющаяся у злоумышленника информация никак не помогает найти значения оставшихся переменных, поскольку в каждой грани размерности $n-k$ функция принимает любое значение b с одинаковой частотой. Собственно само название "корреляционно-иммунный" происходит от того, что набор из $k+1$ случайной величины: значение функции и k любых переменных, является независимым (некоррелированным).

В криптографических алгоритмах чаще всего рассматриваются булевозначные и даже булевы функции. Использование булева счётчика чётности, обладающего максимальной для непостоянных функций корреляционной иммунностью, имеет ограничения, поскольку в этом случае частоты 0 и 1 равны. Кроме того, заранее неизвестная функция создаёт дополнительные сложности злоумышленнику. Возможность построения достаточно разнообразных корреляционно-иммунных булевозначных функций с различной долей единиц будет рассмотрена ниже.

Утверждение 94. *Пусть* $f : Q_q^n \to \mathbb{C}$ *и* $\mathrm{cor}(f) = k$. *Тогда функция* $g = f - \frac{\mathrm{wt}(f)}{q^n}\mathbf{1}$, *где* $\mathrm{wt}(f) = \sum_x f(x)$, *уравновешена в гранях размерности* $n-k$.

Доказательство. По условию сумма значений функции f в каждой грани размерности $n-k$ одинакова и добавление постоянной функции не изменяет это свойство. По определению функция g уравновешена в гиперкубе, следовательно уравновешена в гранях размерности $n-k$. □

Теорема 34 ([133])**.** *Для функции* $f : Q_q^n \to \{0,1\}$ *равенство* $\mathrm{cor}(f) = k$ *верно тогда и только тогда, когда* $\widehat{f}(z) = 0$ *для всех* $z \in Q_q^n$ *веса* $0 < \mathrm{wt}(z) \leq k$ *и* $\widehat{f}(v) \neq 0$ *для некоторого* $v \in Q_q^n$ *веса* $\mathrm{wt}(v) = k+1$.

Доказательство. ($\Rightarrow$) Пусть $g = f - \frac{\mathrm{wt}(f)}{q^n}\mathbf{1}$. По утверждению 94 функция g уравновешена в гранях размерности $n-k$. Тогда $\widehat{g}(z) = 0$ для всех $z \in Q_q^n$ веса $\mathrm{wt}(z) \leq k$ по утверждению 93. Преобразование Фурье от $\mathbf{1}$ является δ-функцией, поэтому функции $\widehat{f}$ и $\widehat{g}$ отличаются только в $\bar{0}$.

Если $\widehat{f}(v) = 0$ для всех $v \in Q_q^n$ веса $\mathrm{wt}(v) = k+1$, то функция g уравновешена и в гранях размерности $n-k-1$ по утверждению 93. Тогда суммы $\sum_{x\in\Gamma} f(x)$ одинаковы для всех граней Γ размерности $n-k-1$. Поскольку f принимает только два значения 0 и 1, то она должна принимать значение 1 одинаковое число раз в каждой грани размерности $n-k-1$. Тогда $\mathrm{cor}(f) \geq k+1$, пришли к противоречию.

($\Leftarrow$) Нетрудно видеть, что $\widehat{g}(\bar{0}) = 0$. Из условия имеем $\widehat{g}(z) = 0$ при $0 < \mathrm{wt}(z) \leq k$. Тогда из утверждения 93 получаем уравновешенность функции g в гранях размерности $n-k$. По утверждению 93 наличие ненулевого коэффициента Фурье $\widehat{g}(v) \neq 0$ для некоторого $v \in Q_q^n$ веса $\mathrm{wt}(v) = k+1$ влечёт неуравновешенность функции g в некоторой грани размерности $n-k-1$. Поскольку функция g принимает только два значения, имеем $\mathrm{cor}(g) = k$. Функции f и g отличаются на постоянную величину, поэтому $\mathrm{cor}(f) = \mathrm{cor}(g)$. □

Если функция f принимает больше двух различных значений (цветов), то $\mathrm{cor}(f)$ равняется минимуму корреляционных иммунностей характеристических функций цветов. Действительно, если все цвета равномерно распределены по граням некоторой размерности, то также и каждый цвет в отдельности. Если хотя бы один из цветов не распределён равномерно по граням некоторой размерности k, то и функция в целом по определению не является корреляционно-иммунной порядка $n-k$.

Теорему 34 можно рассматривать как аналог утверждения 12 и следствие ортогональности собственных пространств матрицы смежности графа с разными собственными числами. Действительно, характеристическая функция грани размерности $n-k$ является линейной комбинацией характеров ϕ_z, где $\mathrm{wt}(z) \leq k$. И наоборот, характеры являются линейными комбинациями индикаторов граней соответствующей размерности. Значит любая любая линейная комбинация характеров ϕ_z, где $\mathrm{wt}(z) > k$ ортогональна грани размерности $n-k$ и, наоборот, любая функция, ортогональная всем граням размерности $n-k$, представима в виде такой линейной комбинации.

12.3 Корреляционная иммунность совершенных раскрасок

Утверждение 95. *Пусть f — совершенная раскраска гиперкуба Q_q^n с матрицей параметров S. Тогда $\widehat{f}(z) \neq 0$ только если $\lambda = (n-\mathrm{wt}(z))(q-1) - \mathrm{wt}(z)$ — собственное число матрицы S.*

Доказательство. Функция f может быть представлена как линейная комбинация собственных функций гиперкуба Q_q^n с теми же собственными числами, что и у матрицы S (см. следствие 3). Как было отмечено

в следствии 34, характеры образуют базис любого собственного подпространства графа Кэли конечной абелевой группы, в частности, гиперкуба. Собственная функция содержится в собственном подпространстве, следовательно, является линейной комбинацией характеров. Из формул, полученных в разделе 11.2, следует, что характеру ϕ_v соответствует собственное число $(n - \mathrm{wt}(z))(q-1) - \mathrm{wt}(z)$. □

Утверждение 96. *Пусть f — совершенная раскраска гиперкуба Q_q^n с матрицей параметров $S = \begin{pmatrix} n(q-1)-b & b \\ c & n(q-1)-c \end{pmatrix}$. Тогда* $\mathrm{cor}(f) = \frac{b+c}{q} - 1$.

Доказательство. Собственными числами матрицы параметров S являются $\lambda_0 = n(q-1)$ и $\lambda_1 = n(q-1) - (b+c)$. Вычислим $\mathrm{wt}(z)$ из равенств $(n - \mathrm{wt}(z))(q-1) - \mathrm{wt}(z) = \lambda_0 = n(q-1)$, т. е. $\mathrm{wt}(z) = 0$, и $(n - \mathrm{wt}(z))(q-1) - \mathrm{wt}(z) = \lambda_1 = n(q-1) - (b+c)$, т. е. $\mathrm{wt}(z) = \frac{b+c}{q}$. Тогда по теореме 34 и утверждению 95 получаем $\mathrm{cor}(f) = \frac{b+c}{q} - 1$. □

Следствие 36. *Для характеристической функции f 1-совершенного кода в гиперкубе Q_q^n верно равенство* $\mathrm{cor}(f) = \frac{(n-1)(q-1)}{q}$.

Построение совершенных раскрасок в два цвета является одним из методов получения корреляционно-иммунных функций с нужными параметрами. Ниже будет показано, что корреляционно-иммунные функции максимально возможного порядка для некоторых параметров являются совершенными раскрасками.

Следующая теорема является некоторым обобщением теоремы 13 о восстановлении совершенной раскраски по среднему слою. Однако, здесь для восстановления функции требуются два слоя. Обобщение теоремы 13 о восстановлении совершенной раскраски по одному слою с другими дополнительными условиями имеется в [108].

Теорема 35. *Пусть f — совершенная раскраска булева гиперкуба Q_2^n с матрицей параметров S. Пусть v — собственный вектор матрицы S, соответствующий собственному числу λ_k матрицы S, причём $-n < \lambda_k = n - 2k < 0$. Если все координаты вектора v различны, то функция f однозначно определяется своими значения на векторах веса $n-k$ и $n-k-1$.*

Доказательство. По замечанию 3 найдётся собственная функция f' гиперкуба с собственным числом λ_k, разные значения которой соответствуют разным цветам раскраски. Поскольку f' является собственной функцией, то $\widehat{f'}(z) = 0$ при $\mathrm{wt}(z) \neq k$. по утверждению 84. Тогда по утверждениям 91 и 93 функция f' однозначно восстанавливается по своим значениям в вершинах веса не больше $n-k$. По утверждению 20 для

восстановления f' внутри шара радиуса $n-k$ достаточно значений функции f' на сферах радиуса $n-k$ и $n-k-1$, когда $n-k < n/2$. Последнее неравенство выполнено по условию. $\square$

Отметим, что в теореме 35 условие $-n < \lambda_k = n - 2k < 0$ можно заменить на условие $0 < \lambda_k = n - 2k < n$, а сферы радиуса $n-k$ и $n-k-1$ на сферы k и $k-1$, поскольку умножение на счётчик чётности $(-1)^{\mathrm{wt}(x)}$ переводит собственную функцию с собственным числом λ в собственную функцию с собственным числом $-\lambda$. Это следует из равенства $\widehat{((-1)^{\mathrm{wt}(x)} f)} = \widehat{f}(y \oplus \bar{1})$.

12.4 Ортогональные массивы и неравенство Рао

Определение 58. *Простым ортогональным массивом силы k называется таблица, множество строк которой совпадает с множеством наборов $f^{-1}(1)$, где $f : Q_q^n \to \{0,1\}$ — корреляционно-иммунная функция порядка k.*

Ортогональный массив общего вида может содержать повторяющиеся строки и соответствует таблице функции $f : Q_q^n \to \{0,1,\ldots,m\}$: если $f(x) = s$, то строка x повторяется в таблице s раз. Здесь функция f является суммой уравновешенной в $n-k$-мерных гранях функции и константы.

Пример 42. Двоичный ортогональный массив силы 2:

$$\begin{array}{ccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}.$$

Корреляционно-иммунные функции в форме ортогональных массивов используются для планирования экспериментов. Предположим у нас имеется программа, имеющая n параметров, каждый из которых может принимать q значений. Чтобы протестировать программу при всех возможных наборах параметров нужно выполнить q^n вычислительных экспериментов, что может потребовать неоправданно много ресурсов. Предположим нам достаточно проверить работу программы при любых значениях наборов любых k параметров. Тогда нужно задавать параметры как строчки ортогонального массива силы k минимально возможной мощности. Аналогичное решение можно применять не только для проверки корректности работы программы, но и при сборе статистики для оценки эффективности работы программы. Конечно для решения такой

задачи нужны ортогональные массивы как можно меньшей мощности или, что эквивалентно, корреляционно-иммунные функции с как можно меньшей мощностью носителя.

Ниже доказаны несколько теорем для булевозначных корреляционно-иммуных функций, которые естественным образом обобщаются на функции, принимающие целые неотрицательные значения и соответствующие им ортогональные массивы.

Теорема 36 (неравенство Рао [80])**.**
Пусть $f : Q_q^n \to \{0,1\}$, $f \neq \mathbf{0}$ *и* $k = \mathrm{cor}(f)$. *Тогда,*
если k *— чётное, то* $|\mathrm{supp}(f)| \geq \sum\limits_{i=0}^{k/2} \binom{n}{i}(q-1)^i$;
если k *— нечётное, то* $|\mathrm{supp}(f)| \geq \binom{n-1}{(k-1)/2}(q-1)^{\frac{k+1}{2}} + \sum\limits_{i=0}^{(k-1)/2} \binom{n}{i}(q-1)^i$.

Доказательство. Поскольку f принимает значения только 0 и 1, а характеры принимают значения вида ξ^a, для любых $u, v \in Q_q^n$ справедливы равенства
$(f\phi_v, f\phi_u) = (f\phi_v, \phi_u) = (f, \phi_{-v}\phi_u) = (f, \phi_{u-v}) = q^{n/2}\widehat{f}(u-v)$.

Из теоремы 34 следует, что $\widehat{f}(z) = 0$ для всех $z \in Q_q^n$ веса $0 < \mathrm{wt}(z) \leq k$. Отсюда и из равенств выше следует, что все функции $f\phi_v$ при $0 \leq \mathrm{wt}(v) \leq k/2$ ортогональны между собой.

Попарно ортогональных векторов длины N не может быть больше чем N. Имеем $\mathrm{supp}(f\phi_v) = \mathrm{supp}(f)$. Тогда различных векторов $f\phi_v$, где $0 \leq \mathrm{wt}(v) \leq k/2$, не больше чем $|\mathrm{supp}(f)|$. Отсюда получаем при чётном k неравенство $|\mathrm{supp}(f)| \geq \sum\limits_{i=0}^{k/2} \binom{n}{i}(q-1)^i$.

В случае когда k нечётно можно рассмотреть все функции $f\phi_v$ при $0 \leq \mathrm{wt}(v) \leq (k-1)/2$ и все функции $f\phi_u$, $u_1 \neq 0$, $\mathrm{wt}(u) = (k+1)/2$. Тогда вес их попарных разностей не превосходит k. □

Отметим, что для любой булевозначной функции f число $q^{\mathrm{cor}(f)}$ делит $|\mathrm{supp}(f)|$, поскольку в каждой грани размерности $n - \mathrm{cor}(f)$ имеется одинаковое количество единиц функции f.

12.5 Неравенство Бирбрауэра—Фридмана

Определим плотность множества $A \subset Q_q^n$ и его характеристической функции как $\rho(A) = \rho(\chi_A) = |A|/q^n = |\mathrm{supp}(\chi_A)|/q^n$.

Теорема 37 (неравенство Бирбрауэра—Фридмана [10], [35])**.**
Пусть $f : Q_q^n \to \{0,1\}$, $f \neq \mathbf{0}$, *тогда* $\rho(f) \geq 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}$.

Доказательство. Пусть M — матрица смежности q-ичного гиперкуба. Характеры являются её собственными функциями: $M\phi_z(x) = \lambda_z\phi_z(x)$

(см. утверждение 77). Из теоремы 34 следует, что $\widehat{f}(z) = 0$ при $0 < \mathrm{wt}(z) \leq \mathrm{cor}(f)$. Тогда

$$0 \leq (Mf, f) = \frac{1}{q^n}(M \sum_{z \in Q_q^n} \widehat{f}(z)\phi_z, \sum_{z \in Q_q^n} \widehat{f}(z)\phi_z) =$$

$$= \sum_{z \in Q_q^n} |\widehat{f}(z)|^2 \lambda_z = \lambda_0 |\widehat{f}(\bar{0})|^2 + \sum_{\substack{z \in Q_q^n, \\ \mathrm{wt}(z) \geq \mathrm{cor}(f)+1}} |\widehat{f}(z)|^2 \lambda_z. \qquad (18)$$

Рассмотрим каждое из слагаемых в правой части выражения (18) по отдельности. Вычислим первое слагаемое

$$|\widehat{f}(\bar{0})|^2 = \left(\frac{1}{q^{n/2}}(f, \mathbf{1})\right)^2 = \frac{|\mathrm{supp}(f)|^2}{q^n} = q^n \rho^2, \text{ где } \rho = \rho(f).$$

Для оценки второго слагаемого воспользуемся равенством Парсеваля:

$$\sum_{z \in Q_q^n} |\widehat{f}(z)|^2 = \sum_{x \in Q_q^n} |f(x)|^2 = (f, f) = \mathrm{wt}(f) = q^n \rho.$$

Тогда $\sum_{\substack{z \in Q_q^n, \\ \mathrm{wt}(z) \geq \mathrm{cor}(f)+1}} |\widehat{f}(z)|^2 = (\rho - \rho^2) q^n$.

Цепочку неравенств (18) мы можем продолжить, оценив снизу λ_z. А именно, если $\mathrm{wt}(z) \geq \mathrm{cor}(f) + 1$, то $\lambda_z = n(q-1) - q\mathrm{wt}(z) \leq n(q-1) - q(\mathrm{cor}(f)+1)$. Разделим оба слагаемых на q^n. Имеем эквивалентные неравенства:

$$0 \leq n(q-1)\rho^2 + (n(q-1) - q(\mathrm{cor}(f)+1))(\rho - \rho^2),$$

$$q(\mathrm{cor}(f)+1) - n(q-1) \leq q\rho(\mathrm{cor}(f)+1),$$

$$1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)} \leq \rho.$$

□

Следствие 37. *Если для функции $f : Q_q^n \to \{0, 1\}$ выполнено равенство $\rho(f) = 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}$, то f является совершенной раскраской.*

Доказательство. Равенство означает, что неравенство $\lambda_z = n(q-1) - q\mathrm{wt}(z) \leq n(q-1) - q(\mathrm{cor}(f)+1)$ на самом деле является равенством. То есть ненулевые коэффициенты Фурье функции f соответствуют только двум собственным числам $\lambda_z = n(q-1)$ и $\lambda_z = n(q-1) - q(\mathrm{cor}(f)+1)$. Тогда функция f является совершенной раскраской по утверждению 10 (либо по следствию 6, если рассмотреть собственную функцию $g = f - \rho(f) \cdot \mathbf{1}$). □

Отметим, что равенство в неравенстве Бирбрауэра–Фридмана не может достигаться на непростом ортогональном массиве, поскольку в этом случае $(f,f) = \sum\limits_{x \in Q_q^n} |f(x)|^2 > |\mathrm{supp}(f)|$.

Следствие 38 ([76]).

Пусть $f : Q_q^n \to \{0,1\}$. Функция f является характеристической функцией 1-совершенного кода тогда и только тогда, когда $\rho = \frac{1}{n(q-1)+1}$ и $\mathrm{cor}(f) = \frac{n(q-1)+1}{q} - 1$.

Доказательство. ($\Rightarrow$) Равенство $\rho = \frac{1}{n(q-1)+1}$ очевидно. Число $\mathrm{cor}(f)$ получаем из утверждения 96, подставив конкретные значения $b = 1$, $c = n(q-1)$.

($\Leftarrow$) Подставляем в неравенство

$$\rho(f) \geq 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}$$

равенства $\rho = \frac{1}{n(q-1)+1}$ и $\mathrm{cor}(f) = \frac{n(q-1)+1}{q} - 1$. Имеем

$$\frac{1}{n(q-1)+1} \geq 1 - \frac{n(q-1)}{q \cdot \frac{n(q-1)+1}{q}},$$

$$\frac{1}{n(q-1)+1} \geq \frac{1}{n(q-1)+1}.$$

Следовательно, имеет место равенство. Тогда по следствию 37 получаем, что f является совершенной раскраской в два цвета.

Из значения плотности следует, что в среднем в каждом шаре функция f принимает значение 1 один раз. Поскольку f — совершенная раскраска в два цвета, то в каждом шаре должны присутствовать вершины обоих цветов. Следовательно, в каждом шаре ровно одна единица и f — характеристическая функция совершенного кода. □

Из доказательства нетрудно видеть, что равенство в неравенстве Бирбрауэра—Фридмана может достигаться только тогда, когда $(Mf, f) = 0$, т. е. совершенная раскраска f не содержит соседних единиц. Однако, можно показать, что любая совершенная раскраска гиперкуба в два цвета является экстремальной функцией в смысле достижения равенства в некотором неравенстве подобном неравенству Бирбрауэра—Фридмана.

Утверждение 97 ([79]). *Пусть $f : Q_q^n \to \{0,1\}$. Справедливо неравенство*

$$\rho(f) \cdot q(\mathrm{cor}(f)+1) \leq s_{01}(f), \tag{19}$$

где $\bar{s}_{01}(f)$ — среднее количество вершин цвета 1, которое видит вершина цвета 0 (см. раздел 3.3). Неравенство (19) обращается в равенство тогда и только тогда, когда f — совершенная раскраска.

Доказательство теоремы аналогично доказательству неравенства Бирбрауэра—Фридмана.

Пусть $f : Q_q^n \to \{0,1\}$. Обозначим через $I[f]$ число рёбер, в концах которых значения функции f отличаются. Для константы эта величина равна нулю, а для булева счётчика чётности — $n2^{n-1}$. Отметим, что $I[f]$ равняется величине разреза $I[f] = e(f^{-1}(0), f^{-1}(1))$ в графе Хэмминга.

Утверждение 98 ([75]). $I[f] = \frac{q}{4} \sum\limits_{z \in Q_q^n} \mathrm{wt}(z) |\widehat{(-1)^f}(z)|^2$.

Доказательство. Пусть M — матрица смежности q-ичного n-куба. Нетрудно непосредственно проверить, что

$$2I[f] - (n(q-1)q^n - 2I[f]) = -(M(-1)^f, (-1)^f), \tag{20}$$

поскольку в правой сумме каждое ребро учитывается два раза.

Напомним, что характеры являются собственными функциями матрицы M: $M\phi_z = \lambda_z \phi_z$, где $\lambda_z = (q-1)n - q\mathrm{wt}(z)$ (см. утверждение 77). Представим функцию $(-1)^f$ в виде линейной комбинации характеров $(-1)^f = \frac{1}{q^{n/2}} \sum\limits_{z \in Q_q^n} \widehat{(-1)^f}(z)\phi_z$. Подставляя это выражение в (20) и используя ортогональность характеров, а также равенство Парсеваля $\sum\limits_{z \in Q_q^n} |\widehat{(-1)^f}(z)|^2 = q^n$, получаем равенства

$$4I[f] = n(q-1)q^n - \sum_{z \in Q_q^n} \lambda_z |\widehat{(-1)^f}(z)|^2 = \sum_{z \in Q_q^n} q\mathrm{wt}(z) |\widehat{(-1)^f}(z)|^2.$$

□

Следствие 39. $\frac{I[f]}{q^{n+1}} \geq (\mathrm{cor}(f)+1)(\rho(f) - \rho^2(f))$.

Доказательство. Поскольку $(-1)^f = \mathbf{1} - 2f$, коэффициенты $\widehat{(-1)^f}(z)$ и $\widehat{f}(z)$ равны нулю одновременно при $\mathrm{wt}(z) > 0$. Тогда из теоремы 34 следует, что $\widehat{(-1)^f}(z) = 0$ при $0 < \mathrm{wt}(z) \leq \mathrm{cor}(f)$. Следовательно, из утверждения 98 имеем неравенство

$$4I[f] \geq \sum_{z \in Q_q^n \setminus \bar{0}} q(\mathrm{cor}(f)+1)(\widehat{(-1)^f}(z))^2.$$

Оценим величину $\sum\limits_{z \in Q_2^n \setminus \bar{0}} |\widehat{(-1)^f}(z)|^2$. Из равенства Парсеваля имеем $\sum\limits_{z \in Q_q^n} |\widehat{(-1)^f}(z)|^2 = q^n$, кроме того $\widehat{(-1)^f}(\bar{0}) = q^{n/2}(1 - \rho(f) - \rho(f))$. Тогда

$$\sum_{z \in Q_q^n \setminus \bar{0}} |\widehat{(-1)^f}(z)|^2 = q^n - q^n(1-2\rho(f))^2 = 4q^n\rho(f)(1-\rho(f)).$$

□

Для фиксированной плотности $\rho(f)$ величина $I[f]$ достигает своего наибольшего значения, если все вершины, на которых функция f равна 1, несмежны. Поэтому $\frac{I[f]}{q^n} \leq (q-1)\rho(f)n$. Тогда из следствия 39 следует неравенство Бирбрауэра—Фридмана. Аналогично доказательству следствия 37 нетрудно доказать

Следствие 40. *Если* $\frac{I[f]}{q^{n+1}} = (\mathrm{cor}(f)+1)(\rho(f)-\rho^2(f))$, *то* f *— совершенная 2-раскраска.*

12.6 Теорема Фон-дер-Флаасса

Определение 59. *Булева коррелляционно-иммунная функция называется устойчивой (resilient), если* $|f^{-1}(0)| = |f^{-1}(1)|$, *то есть число нулей и единиц среди значений функции совпадает.*

Нетрудно видеть, что булева функция f устойчива тогда и только тогда, когда функция $(-1)^f$ уравновешена в булевом кубе, т. е. когда $\widehat{(-1)^f}(\bar{0}) = 0$.

Теорема 38 (Фон-дер-Флаасс [34])**.** *Если булева функция* $f : Q_2^n \to \{0,1\}$ *не постоянная и не устойчивая, то* $\mathrm{cor}(f) \leq \frac{2n}{3} - 1$. *Причём если в этом неравенстве достигается равенство, то* f *— совершенная раскраска.*

Доказательство. Возьмём $g = \widehat{(-1)^f}$. Поскольку функция f не является постоянной, найдётся такое $y \neq \bar{0}$, что $g(y) = \widehat{(-1)^f}(y) \neq 0$. Поскольку функция f не устойчивая, $g(\bar{0}) = \widehat{(-1)^f}(\bar{0}) \neq 0$. По теореме Титсворта для выбранного y имеем

$$0 = (g * g)(y) = \sum_{x \in Q_2^n} g(x)g(y-x).$$

Значит в сумме есть ещё как минимум одно ненулевое слагаемое, кроме $g(\bar{0})g(y)$. Заметим, что $\mathrm{cor}(f) = \mathrm{cor}((-1)^f)$. По теореме 34 имеем $g(x) = 0$ при $0 < \mathrm{wt}(x) \leq \mathrm{cor}(f)$.

Продолжим цепочку равенств:

$$0 = (g * g)(y) = g(\bar{0})g(y) + g(y)g(\bar{0}) + \sum_{\substack{x \in Q_2^n \\ \mathrm{wt}(x) \geq \mathrm{cor}(f)+1 \\ \mathrm{wt}(y-x) \geq \mathrm{cor}(f)+1}} g(x)g(y-x).$$

Посмотрим, когда множество, по которому идёт сумирование, содержит ненулевые слагаемые. Предположим, что $\mathrm{cor}(f) > \frac{2n}{3} - 1$. Тогда $\mathrm{wt}(y) > \frac{2n}{3}$ и найдётся x, для которого $g(x)g(y-x) \neq 0$. Откуда из следует, что $\mathrm{wt}(x) > \frac{2n}{3}$ и $\mathrm{wt}(y-x) > \frac{2n}{3}$. Однако, из неравенства треугольника

для метрики Хэмминга имеем $\mathrm{wt}(y-x) = d(x,y) \le d(\overline{1},x) + d(\overline{1},y) = n - \mathrm{wt}(x) + n - \mathrm{wt}(y) < \frac{2n}{3}$. Пришли к противоречию.

Пусть $\mathrm{cor}(f) = \frac{2n}{3} - 1$. Если $g(y) \neq 0$ в некоторой вершине веса $\mathrm{wt}(y) > \frac{2n}{3}$, то аналогичным образом получаем противоречие. Следовательно, в этом случае преобразование Фурье $g(y)$ не равно нулю только в нуле и в вершинах веса $\frac{2n}{3}$. Тогда f — совершенная раскраска по утверждению 10. □

Неравенство в теореме 38 называется границей Фон-дер-Флааса. Приведённое выше доказательство принадлежит Халявину. Как показано Халявиным [138] граница Фон-дер-Флааса остаётся справедливой и для двоичных ортогональных массивов. В отличие от неравенств Рао и Бирбрауэра—Фридмана, обобщение теоремы Фон-дер-Флааса на случай $q \neq 2$ неизвестно.

Задача 105. Пусть $f : Q_2^n \to \mathbb{C}$ и $\mathrm{cor}(f) = n - k$. Докажите, что f однозначно восстанавливается по своим значениям в шаре радиуса $k-1$ (т. е. по значениям в вершинах веса не более $k-1$).

Задача 106. Пусть $f : Q_q^n \to \mathbb{C}$ и $\mathrm{cor}(f) = n - k$. Докажите, что f однозначно восстанавливается по своим значениям вне шара радиуса $n-k$ (т. е. по значениям в вершинах веса не менее $n-k+1$).

Задача 107. Пусть q — простое. Рассмотрим Q_q^n как n-мерное векторное пространство над полем $GF(q)$. Докажите, что если функция $f : Q_q^n \to C$ уравновешена во всех гиперподпространствах, то f тождественно равна нулю.

Задача 108. Докажите, что мощность носителя функции $f : Q_2^n \to \mathbb{C}$, уравновешенной в гранях размерности k, не меньше, чем 2^{n-k+1}.

Задача 109. Докажите, что функции $f : Q_q^n \to \mathbb{C}$, уравновешенные в гранях размерности k образуют линейное подпространство и это подпространство является ортогональным дополнением к линейной оболочке $L(n,k,q)$ множества индикаторов всех граней размерности k.

Задача 110. Пусть $f \in L(n,k_1,q)$ и $g \in L(n,k_2,q)$. Докажите, что $fg \in L(n,k_2+k_1-n,q)$ при $k_2+k_1 > n$.

Задача 111. Пусть f — совершенная раскраска булева n-мерного булева гиперкуба и λ — максимальное отличное от n собственное число её матрицы параметров. Докажите, что $\mathrm{cor}(f) = \frac{n-\lambda}{2} - 1$.

Задача 112. Пусть f — некоторая раскраска булева n-мерного булева гиперкуба и λ — максимальное отличное от n собственное число матрицы усреднённого цветового окружения S_f (см. раздел 3.3). Докажите, что $\mathrm{cor}(f) \le \frac{n-\lambda}{2} - 1$.

Задача 113. Рассмотрим матрицу Адамара A порядка n, у которой первая строка и первый столбец состоят из 1. Заменим все -1 в матрицах A и $-A$ на 0. Докажите, что ортогональный массив, состоящий из $2n$ строк этих матриц, имеет силу 2. Докажите, что если $n = 2^k$, то ортогонального массива силы 2 меньшей мощности не существует.

Задача 114. Протыкающим массивом (covering array) силы k называется таблица, строками которой являются наборы из $P \subset Q_q^n$, если множество P пересекается со всеми k-мерными гранями в Q_q^n. Докажите, что число строк протыкающего массива силы 2 в Q_2^n не меньше $\lceil \log n \rceil$.

Задача 115. Пусть не постоянная и не устойчивая булева функция $f : Q_2^n \to \{0,1\}$ достигает границы корреляционной иммунности Фон-дер-Флаасса. Докажите, что в каждой грани размерности больше $n/3$ число единиц функции f в чётных и нечётных вершинах совпадает.

13 Дуальный код, тождества Мак-Вильямс и Саркара

13.1 Дуальный код

Введём обозначение $v \perp C \subset Q_q^n$, если для всех $u \in C$ имеется равенство $\langle v, u \rangle = \sum v_i u_i = 0 \mod q$.

Определение 60. *Множество $C^\perp = \{v \in Q_q^n \mid v \perp C\}$ называется кодом, дуальным коду C.*

Нетрудно проверить, что множество $C^\perp$ замкнуто относительно операций сложения и умножения в кольце $\mathbb{Z}_q$. Из определения ясно, что $C \subset (C^\perp)^\perp$.

Утверждение 99. *Пусть Γ — k-мерная грань в Q_q^n, причём $\bar{0} \in \Gamma$ и $I \subset \{1, \ldots, n\}$ — номера её свободных координат. Тогда $\Gamma^\perp$ является $(n-k)$-мерной гранью в Q_q^n, причём $\bar{0} \in \Gamma^\perp$ и $\{1, \ldots, n\} \setminus I$ — номера её свободных координат.*

Доказательство. Множества свободных координат двух граней не пересекаются, поэтому для любого $i \in \{1, \ldots, n\}$ для любых вершин u из одной и v из другой грани $u_i = 0$ или $v_i = 0$. Осталось показать, что набор v, имеющий ненулевую координату $v_i \neq 0$, $i \in I$, не содержится в $\Gamma^\perp$. Действительно, имеем $e_i \in \Gamma$ и $\langle v, e_i \rangle = v_i \neq 0$. □

Утверждение 100. *Если $v \perp C$, то $\widehat{\chi_C}(v) = \frac{|C|}{q^{n/2}}$. Обратное тоже верно.*

Доказательство. Имеем равенство $\widehat{\chi_C}(v) = \frac{1}{q^{n/2}} \sum\limits_{x \in C} \overline{\phi_v(x)} = \frac{1}{q^{n/2}} \sum\limits_{x \in C} \xi^{-\langle v,x \rangle}$. Очевидно, что $\sum\limits_{x \in C} \xi^{-\langle v,x \rangle} = |C|$, если и только если все слагаемые равны 1. А это эквивалентно условию $v \perp C$. □

Следствие 41. *Для любой грани* $\Gamma \subset Q_q^n$, $\bar{0} \in \Gamma$, *верно равенство*

$$\widehat{\chi}_\Gamma = \frac{q^{\dim \Gamma}}{q^{n/2}} \chi_{\Gamma^\perp}.$$

Доказательство. $\widehat{\chi}_\Gamma(v) = \frac{q^{\dim \Gamma}}{q^{n/2}}$ при $v \in \Gamma^\perp$ по утверждению 100. Из равенства Парсеваля следует, что $\widehat{\chi}_\Gamma(u) = 0$ при $u \notin \Gamma^\perp$. □

Произвольную грань в гиперкубе можно представить в виде $\Gamma + a$, где грань Γ содержит нуль. Найдём преобразование Фурье характеристической функции произвольной грани. Из свойств преобразования Фурье следует, что $(\widehat{\chi_{\Gamma+a}(x)})(z) = (\widehat{\chi_\Gamma(x+a)})(z) = \frac{\phi_a(z) q^{\dim \Gamma}}{q^{n/2}} \chi_{\Gamma^\perp}(z)$. Таким образом, для любого $z \in \mathrm{supp}(\widehat{\chi}_{\Gamma+a})$ имеем $\mathrm{wt}(z) \leq \dim(\Gamma^\perp) = n - \dim(\Gamma)$.

Из утверждения 12 об ортогональности совершенных раскрасок можно получить другое доказательство оценки их корреляционной иммунности.

Утверждение 101. *Пусть* f *— совершенная раскраска гиперкуба* Q_q^n *и* $\lambda_1 < n(q-1)$ *— максимальное нетривиальное собственное число её матрицы параметров. Тогда* $\mathrm{cor}(f) \geq \frac{n(q-1)-\lambda_1}{q} - 1$.

Доказательство. Из утверждения 13 следует, что если $\mathrm{supp}(\widehat{\chi_C}) \cap \mathrm{supp}(\widehat{\chi}_\Gamma) = \bar{0}$, то цвет C раскраски f в грани Γ имеют ту же плотность, что и во всём гиперкубе.

Следствие 3 утверждает, что характеристическая функция любого цвета в раскраске f содержится в объединении собственных подпространств матрицы смежности гиперкуба с теми же собственными собственными числами, что и у её матрицы параметров. Таким образом, $\widehat{\chi_C}(z) \neq 0$ только если число $n(q-1) - \mathrm{wt}(z)q$ является собственным числом этой матрицы. Следовательно, $\widehat{\chi_C}(z) = 0$ при $n(q-1) - \mathrm{wt}(z)q > \lambda_1$, $z \neq \bar{0}$.

Рассмотрим произвольную грань Γ. Из сказанного выше следует, что $z \in \mathrm{supp}(\widehat{\chi}_\Gamma)$ только если $n - \dim \Gamma \leq \mathrm{wt}(z)$. Таким образом, $\mathrm{supp}(\widehat{\chi_C}) \cap \mathrm{supp}(\widehat{\chi}_\Gamma) = \bar{0}$ когда $n - \dim \Gamma \leq (n(q-1) - \lambda_1)/q$, т. е. $\dim \Gamma \geq n - (n(q-1) - \lambda_1)/q$. Тогда по определению корреляционной иммунности имеем $\mathrm{cor}(f) \geq \frac{n(q-1)-\lambda_1}{q} - 1$. □

Если q — простое, то Q_q можно рассматривать как конечное поле $GF(q)$ с операциями сложения и умножения по модулю q. Из линейной

алгебры известно, что множество решений однородной системы уравнений

$$C = \{x \in Q_q^n | Hx = \bar{0}\} \tag{21}$$

есть линейное подпространство и наоборот, любое линейное подпространство $C \subset Q_q^n$ можно представить как множество решений системы уравнений (21). В таком случае $H = \{h_{ij}\}$ называется проверочной матрицей кода C. Строки матрицы H принадлежат линейному коду $C^\perp$ и в случае, когда они линейно независимы, составляют его базис. Для линейного кода $C^\perp$ матрица H называется порождающей.

Замечание 17. Заметим, что на множестве мощности q можно определить алтебраическую структуру поля в том и только в том случае, когда $q = p^t$ — степень простого числа. При $t > 1$ операции сложения и умножения в поле $GF(p^t)$ не будут совпадать с операциями сложения и умножения по модулю q. Поэтому определение дуального кода, используемое здесь и далее, и определение дуального кода, введённое в разделе 9.3, совпадают только для простых q.

Далее, когда мы будем говорить о линейном коде в гиперкубе Q_q^n будем подразумевать, что q — простое число.

Стандартными методами линейной алгебры нетрудно доказать

Утверждение 102. *Если C — линейный код в Q_q^n, то $C = (C^\perp)^\perp$.*

Следствие 42. *Код $C \subset Q_q^n$ является линейным, если и только если $\widehat{\chi_C} = \frac{|C|}{q^{n/2}} \chi_{C^\perp}$.*

Доказательство. Из определений линейного и дуального кода имеем $\dim C + \dim C^\perp = n$. Поэтому $|C||C^\perp| = q^n$. Тогда из утверждения 100 и равенства Парсеваля следует необходимость.

Из равенства $\widehat{\chi_C} = \frac{|C|}{q^{n/2}} \chi_{C^\perp}$ имеем $\chi_{-C} = \frac{|C|}{q^{n/2}} \widehat{\chi_{C^\perp}}$. Поскольку код $C^\perp$ является линейным независимо от линейности кода C, имеем $-C = (C^\perp)^\perp$ по уже доказанному. Очевидно, что коды C и $-C$ линейны одновременно. □

Аффинным подпространством является сдвиг линейного подпространства на произвольный вектор. Мощность любого аффинного подпространства в Q_q^n равна q^s, для некоторого целого $s \geq 0$. Пересечение двух аффинных подпространств является аффинным подпространством. В частности, верно следующее

Утверждение 103. *Пусть $C \subset Q_q^n$ — линейный код и Γ — некоторая грань гиперкуба Q_q^n и $\bar{0} \in \Gamma$. Тогда мощность пересечения $|C \cap (x + \Gamma)|$ равна 0 или q^s для каждого $x \in Q_q^n$, где s не зависит от x.*

Доказательство. Система линейных уравнений над полем $GF(q)$ имеет 0 или q^s решений в зависимости от правой части. Число решений зависит только от ранга проверочной матрицы кода $C \cap \Gamma$. □

13.2 Код Адамара

Из утверждения 100 имеется ещё одно следствие.

Утверждение 104. *Пусть $C \subset Q_q^n$ — множество вершин некоторого цвета в совершенной раскраске. Тогда $\lambda = n(q-1) - \mathrm{wt}(v)q$ является собственным числом матрицы параметров совершенной раскраски для любого $v \in C^\perp$.*

Доказательство. Из утверждения 100 имеем $\widehat{\chi_C}(v) = \frac{|C|}{q^{n/2}} \neq 0$. Тогда требуемое следует из утверждения 95. □

Утверждение 105. *Пусть q — простое и $C \subset Q_q^n$ — код Хэмминга. Тогда код $C^\perp$ имеет кодовое расстояние $n - \frac{n-1}{q}$ и мощность $n(q-1)+1$.*

Доказательство. Поскольку C — линейный код, имеем $|C^\perp| = q^n/|C|$. Поскольку C — 1-совершенный код, число $q^n/|C|$ равно мощности шара единичного радиуса — $n(q-1)+1$. Из утверждения 104 получаем, что для ненулевого $v \in C^\perp$ справедливо равенство $n(q-1) - \mathrm{wt}(v)q = -1$ ($\lambda = -1$ — нетривиальное собственное число 1-совершенного кода). Поскольку код $C^\perp$ является линейным, то ему принадлежат все разности пар кодовых слов и его кодовое расстояние равно минимальному весу ненулевых элементов. □

Код, дуальный к коду Хэмминга, называется кодом Адамара. Рассмотрим подробнее двоичный случай $q = 2$. В двоичном случае код Адамара длины n содержит $n+1$ вектор, и все ненулевые вектора кода Адамара длины n имеют вес $\frac{n+1}{2}$. Докажем, что это оптимальный код, т. е. не существует кода большей мощности той же длины с тем же (или большим) кодовым расстоянием.

Утверждение 106. *Пусть кодовое расстояние кода $C \subset Q_2^n$ не меньше βn, где $\beta > \frac{1}{2}$. Тогда $|C| \leq \frac{1}{2\beta - 1} + 1$.*

Доказательство. Рассмотрим вектора $(-1)^v = ((-1)^{v_1}, \ldots, (-1)^{v_n})$, где $v \in C$. Скалярный квадрат $((-1)^v, (-1)^v)$ равен n для любого вектора v. Если $d(u,v) = d$, то $((-1)^v, (-1)^u) = n - 2d$. Имеем неравенства

$$0 \leq (\sum_{v \in C} (-1)^v, \sum_{v \in C} (-1)^v) \leq mn + 2\binom{m}{2}(n - 2\beta n),$$

где $m = |C|$. Тогда $0 \leq 1 + (m-1)(1-2\beta)$. □

Доказанное в утверждении 106 неравенство называется границей Плоткина. Подставляя в него кодовое расстояние и мощность кода Адамара, нетрудно убедиться, что он достигает границы Плоткина.

Для существования 1-совершенного кода в Q_2^n необходимо и достаточно, чтобы $n = 2^t - 1$ (см. утверждение 2), поэтому кодовое расстояние $\frac{n+1}{2}$ кода Адамара чётно. Значит шары радиуса $\frac{n-1}{4}$ с центрами в вершинах кода Адамара не пересекаются, а вершины на расстоянии $\frac{n+1}{4}$ от кодовой не содержатся в таких шарах. Следовательно, двоичный код Адамара позволяет исправлять $\frac{n-1}{4}$ ошибок и диагностировать $\frac{n+1}{4}$ ошибок при передаче сообщений.

13.3 Расширенный 1-совершенный код и матрицы Адамара

Добавим к каждому вектору v 1-совершенного двоичного кода C ещё одну координату равную $|v| = v_1 + \cdots + v_n \mod 2$, которая называется проверкой на чётность веса вектора. Полученный код $\overline{C} = \{(|v|, v) \mid v \in C\}$ называется расширенным 1-совершенным кодом. Поскольку все вектора кода $\overline{C}$ имеют чётный вес, то кодовое расстояние кода $\overline{C}$ чётно и не меньше кодового расстояния нерасширенного кода C. Поэтому кодовое расстояние кода $\overline{C}$ равно 4.

Расширенный 1-совершенный код можно рассматривать как совершенную раскраску булева гиперкуба в три цвета. Пусть $f = \chi_C$ — совершенная раскраска с матрицей параметров $S = \begin{pmatrix} 0 & n \\ 1 & n-1 \end{pmatrix}$. Раскраска $f'(x_0, \overline{x}) = f(\overline{x})$, полученная копированием раскраски f в параллельных гипергранях, имеет матрицу параметров $S + I = \begin{pmatrix} 1 & n \\ 1 & n \end{pmatrix}$. Немаксимальное собственное число 0 этой раскраски не совпадает с немаксимальным собственным числом $-(n+1)$ раскраски по счётчику чётности в Q_2^{n+1}. Поэтому из утверждения 12 следует, что половина вершин каждого цвета имеет чётный вес, а другая половина — нечётный. Поскольку вершины одинаковой чётности в булевом гиперкубе несмежны, мы можем разделить каждый из цветов на два "оттенка": чётный и нечётный, и получим совершенную раскраску с матрицей параметров $\begin{pmatrix} 0 & 0 & 1 & n \\ 0 & 0 & 1 & n \\ 1 & n & 0 & 0 \\ 1 & n & 0 & 0 \end{pmatrix}$. Первый цвет в полученной совершенной раскраске есть расширенный 1-совершенный код по построению. Из матрицы видно, что два первых — чётных цвета (как и два нечётных) являются эквивалентными. По следствию 32 после склеивания двух нечётных цветов получим совершенную раскраску с матрицей параметров $\overline{S} = \begin{pmatrix} 0 & 0 & n+1 \\ 0 & 0 & n+1 \\ 1 & n & 0 \end{pmatrix}$.

Добавление проверки на чётность есть линейная операция, поэтому из линейности кода C следует линейность кода $\overline{C}$. Нетрудно видеть, что

проверочная матрица $\overline{H}$ кода $\overline{C}$ получается из проверочной матрицы двоичного кода Хэмминга добавлением сначала столбца из одних нулей, а затем строки из одних единиц.

Пример 43. Проверочная матрица расширенного кода Хэмминга длины $n = 8$: $\overline{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$.

Собственные числа матрицы параметров $\overline{S}$ равны $0, \pm(n+1)$. Тогда из утверждения 104 (или из свойств проверочной матрицы нерасширенного кода) следует, что все кодовые вершины дуального кода $\overline{C}^{\perp}$ имеют вес 0, m или $m/2$, где $m = n+1$ — размерность булева гиперкуба. Тогда для любых векторов $u, v \in \overline{C}^{\perp}$ верно либо $(-1)^u = -(-1)^v$, либо $((-1)^v, (-1)^u) = m - 2d(u,v) = 0$. Из равенств $|\overline{C}||\overline{C}^{\perp}| = 2^m$ и $|\overline{C}| = |C| = 2^{m-1}/m$ имеем $|\overline{C}^{\perp}| = 2m$. Выбрав из каждой пары противоположных векторов кода $\overline{C}^{\perp}$ по одному, получим набор из m ортогональных векторов в m-мерном пространстве. Из определения матрицы $\overline{H}$ можно показать, что эти вектора являются наборами значений характеров $\pm(-1)^{\langle x,y\rangle}$, где $x, y \in Q_2^t$, $m = 2^t$. Таким образом, линейно независимые вектора $(-1)^u$, где $u \in \overline{C}^{\perp}$, образуют матрицу эквивалентную матрице Адамара—Сильвестра (см. раздел 11.3). Код $\overline{C}^{\perp}$ называют расширенным кодом Адамара. Код Адамара (код Хэмминга) получается из расширенного кода Адамара (расширенного кода Хэмминга) проекцией на гиперграань, содержащую нулевую вершину.

13.4 Тождество Саркара

Теорема 39 (тождество Саркара[38])**.** *Пусть $f : Q_q^n \to \mathbb{C}$. Тогда*
1. Для любой грани $\Gamma \subset Q_q^n$, $\bar{0} \in \Gamma$, верно равенство $\widehat{f} * \chi_{\Gamma^{\perp}} = q^{n-\dim\Gamma}\widehat{f \cdot \chi_{\Gamma}}$.
2. Для любого линейного кода $C \subset Q_q^n$, q — простое, верно равенство $\widehat{f} * \chi_{C^{\perp}} = q^{n-\dim C}\widehat{f \cdot \chi_C}$.

Доказательство. 1. Из утверждения 90 имеем равенство $\widehat{f} * \widehat{\chi_{\Gamma}} = q^{n/2}\widehat{f \cdot \chi_{\Gamma}}$. Используем равенство $\widehat{\chi}_{\Gamma} = \frac{q^{\dim\Gamma}}{q^{n/2}}\chi_{\Gamma^{\perp}}$ из следствия 41 и получаем требуемое.

2. Аналогично пункту 1, применяя следствие 42 вместо следствия 41, получаем требуемое равенство. □

Из тождества Саркара или из теоремы 87 можно вывести

[38] Это равенство было известно и до статьи Саркара [87] (см. [114] и [125]).

Следствие 43. *Пусть* $f : Q_q^n \to \mathbb{C}$ *и грань* Γ *содержит* $\bar{0}$. *Тогда* $\sum\limits_{z\in\Gamma^\perp} \widehat{f}(z) = q^{n/2-\dim\Gamma} \sum\limits_{x\in\Gamma} f(x)$.

Доказательство. Из тождества Саркара имеем равенства

$$\widehat{f} * \chi_{\Gamma^\perp}(0) = q^{n-\dim\Gamma}\widehat{f\cdot\chi_\Gamma}(0), \text{ откуда}$$

$$\sum_{z\in\Gamma^\perp} \widehat{f}(z) = q^{n-\dim\Gamma} \cdot \frac{1}{q^{n/2}} \sum_{x\in Q_q^n} f(x)\chi_\Gamma(x)\phi_0(x).$$

Поскольку $\phi_0(x) = 1$, получаем требуемое равенство. □

Отметим, что это следствие может быть получено также из утверждения 82 (теорема Планшереля).

Следствие 44 ([133]). *Пусть* $f : Q_2^n \to \{0,1\}$ *— булева функция,* $\mathrm{cor}(f) = k$. *Тогда* $\widehat{f}(z) = 2^{k-\frac{n}{2}} \cdot m$, *где* m *— целое. Если функция* f *является устойчивой, то* $\widehat{f}(z) = 2^{1+k-\frac{n}{2}} \cdot m$, *где* m *— целое.*

Доказательство. По теореме 34 $\widehat{f}(z) = 0$ при $0 < \mathrm{wt}(z) \le k$. Вначале докажем утверждение для коэффициентов $\widehat{f}(z)$, где $\mathrm{wt}(z) = k+1$. Рассмотрим грань Γ размерности $n-k-1$. Грань $\Gamma^\perp$, $\bar{0} \in \Gamma$, имеет размерность $\dim\Gamma^\perp = k+1$ и содержит ровно один набор z веса $k+1$. Тогда из теоремы 34 и следствия 43 имеем равенство.

$$\widehat{f}(z) + \widehat{f}(\bar{0}) = 2^{\frac{n}{2}-(n-k-1)} \cdot \sum_{x\in\Gamma} f(x).$$

Пусть $m'' = \sum\limits_{x\in\Gamma} f(x)$ — число единиц функции f в грани Γ, а m' — число единиц функции f в каждой из 2^k граней размерности $n-k$. Таким образом получаем:

$$\widehat{f}(z) = 2^{k+1-\frac{n}{2}} \cdot m'' - 2^{-\frac{n}{2}+k} \cdot m'.$$

Для устойчивой функции имеем $\widehat{f}(\bar{0}) = \frac{1}{2^{n/2}} \sum\limits_{x\in Q_2^n} f(x) = 2^{\frac{n}{2}-1}$. При $k \le n-2$ верно, что $k+1-\frac{n}{2} \le \frac{n}{2}-1$.

Для коэффициентов $\widehat{f}(z)$, где $\mathrm{wt}(z) = k+s$, $s > 1$, утверждение можно доказать индукцией по s. Рассмотрим грань Γ размерности $n-k-s$. Действительно, грань $\Gamma^\perp$ размерности $k+s$ содержит только одну вершину веса $k+s$, а для вершин меньшего веса требуемое уже известно из индукционного предположения.

Устойчивыми булевыми функциями с корреляционной иммунностью $n-1$ являются счётчик чётности и его отрицание, для которых требуемое равенство легко проверить непосредственно. □

Замечание 18. Если рассмотреть вместо булевой функции f функцию $(-1)^f$, то аналогично имеем $\widehat{(-1)^f}(z) = 2^{k-n/2+1}m$, где m — целое, поскольку функция $(-1)^f$ имеет чётные суммы во всех гранях ненулевой размерности. Если функция f устойчива, то $\widehat{(-1)^f}(z) = 2^{k-n/2+2}m$, где m — целое, поскольку в этом случае второе слагаемое $\widehat{(-1)^f}(\bar{0})$ равно нулю.

Следствие 45. *Пусть* $f : Q_2^n \to \{0,1\}$. *Если* $\widehat{(-1)^f}(z) = 0$ *при* $\mathrm{wt}(z) \geq k$, *то все коэффициенты* $\widehat{(-1)^f}(z)$ *имеют вид* $m2^{\frac{n}{2}-k+1}$, *где* m — *целое.*

Доказательство. Пусть $g(x) = f(x)+x_1+\cdots+x_n$. Очевидно, $\widehat{(-1)^g}(z) = \widehat{(-1)^f}(z+\bar{1})$. Тогда $\widehat{(-1)^g}(z) = 0$ при $\mathrm{wt}(z) \leq n-k$. Следовательно, $\widehat{(-1)^g}(z) = 2^{n-k-n/2+1}m$, где m — целое. □

13.5 Число существенных переменных и тестирующие множества совершенных раскрасок

Следующая теорема является непосредственным приложением теоремы Н.Нисана и М.Сегеди [75] к совершенным раскраскам.

Теорема 40 (Валюженич). *Пусть* f — *совершенная раскраска гиперкуба* Q_2^n *с матрицей параметров* $S = \begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$. *Тогда число существенных переменных функции* f *не превышает* $\frac{bc2^{(b+c)/2}}{b+c}$.

Доказательство. Без ограничения общности полагаем, что f принимает значения ± 1. Из утверждения 95 следует, что $\widehat{f}(z) \neq 0$ только если $n-(b+c) = n-2\mathrm{wt}(z)$, т. е. $\mathrm{wt}(z) = (b+c)/2$ или $z = \bar{0}$. Тогда из следствия 45 все коэффициенты $\widehat{f}(z)$ имеют вид $m2^{\frac{n-(b+c)}{2}+1}$, где m — целое. Пусть f_0 и f_1 сужения функции f на гиперграни $x_n = 0$ и $x_n = 1$ соответственно. Нетрудно непосредственно проверить, что

$$\widehat{(f_0 - f_1)}(z_1,\ldots,z_{n-1}) = \frac{1}{\sqrt{2}}(\widehat{f(x) - f(x \oplus e_n)})(z_1,\ldots,z_{n-1},1).$$

Поэтому коэффициенты $\widehat{(f_0 - f_1)}$ делятся на $2^{\frac{n-(b+c)+1}{2}}$ нацело.

Обозначим $h = f_0 - f_1$. Поскольку h принимает значения 0 и ± 2, из равенства Парсеваля имеем

$$4|\mathrm{supp}(h)| = \|h\|^2 = \|\widehat{h}\|^2 \geq 2^{n-(b+c)+1}|\mathrm{supp}(\widehat{h})|.$$

Тогда из утверждения 86 имеем

$$|\mathrm{supp}(h)| \geq \frac{2^{n-1}}{|\mathrm{supp}(\widehat{h})|} \geq \frac{2^{2n-(b+c)-2}}{|\mathrm{supp}(h)|}.$$

Таким образом, $|\mathrm{supp}(h)| \geq 2^{n-1-(b+c)/2}$.

Следовательно, если функция f существенно зависит от n-ой координаты, то значения функции f различаются не менее чем в $2^{n-1-(b+c)/2}$ вершинах, соседних по этой координате. Значит если функция f существенно зависит от t координат, то $I(f) \geq t2^{n-1-(b+c)/2}$. С другой стороны из утверждения 98 и следствия 39 имеем

$$I[f] = 2^{n-1}(b+c)(\rho(f) - \rho^2(f)),$$

где $\rho(f)(1-\rho(f)) = \frac{c}{b+c}\frac{b}{b+c}$. Тогда $t \leq \frac{2^{(b+c)/2}bc}{b+c}$. □

Рассмотрим обобщённую матрицу Адамара $H_{q,n}$, строки которой являются характерами, т. е. $H_{q,n}(z,x) = \phi_z(x)$. Рассмотрим квадратную матрицу A_d, которая получается из $H_{q,n}$ выделением строк и столбцов, соответствующих вершинам веса не меньше d.

Утверждение 107. (*a*) *При любом $d \geq 0$ матрица A_d невырождена.*

(*b*) *Если $f(x) = 0$ при всех $x \in Q_q^n$, $\mathrm{wt}(x) \leq d$ и $\widehat{f}(z) = 0$ при всех $z \in Q_q^n$, $\mathrm{wt}(z) > d$, то $f = 0$.*

Доказательство. Матрица A_d вырождена тогда и только тогда, когда найдётся такая ненулевая функция $f : Q_q^n \to \mathbb{C}$, что $f(x) = 0$ если $\mathrm{wt}(x) > d$ и $\widehat{f}(z) = 0$ при $\mathrm{wt}(x) \leq d$. JОтсюда следует эквивалентность условий (a) и (b). Докажем (b).

По условию $f \cdot \chi_\Gamma = 0$ для любой грани Γ размерности d и содержащей $\bar{0}$. Из тождества Саркара имеем $\widehat{f} * \chi_{\Gamma^\perp} = 0$. Это значит, что сумма значений функции f по любой грани размерности $n-d$ (необязательно содержащей $\bar{0}$) равняется нулю. Очевидно, что функция f уравновешенна и в гранях большей размерности. Для каждой вершины a веса d найдётся грань $\Gamma_a = \{y \in Q_q^n : y_i = a_i, \text{ если } a_i \neq 0\}$ размерности $n-d$, которая содержит ровно одну вершину веса d, а остальные вершины большего веса. Из условия $\widehat{f}$ имеем $\widehat{f}(a) = 0$. Таким образом, мы показали что функция $\widehat{f}$ равна нулю на любой вершине веса d. С помощью граней размерности $n-d+1$ мы аналогичным образом можем показать, что функция f равняется нулю и на вершинах веса $d-1$. Далее, по индукции получим, что $\widehat{f} = 0$. Тогда и $f = 0$. □

Утверждение 108. *Собственная функция f в Q_q^n с собственным числом $\lambda_k = n(q-1) - qk$ однозначно восстанавливается по своим значениям в шаре $B_k = \{x \in Q_q^n : \mathrm{wt}(x) \leq k\}$.*

Доказательство. Предположим функция f восстанавливается неоднозначно по своим значениям в шаре $B_k = \{x \in Q_q^n : \mathrm{wt}(x) \leq k\}$, т. е. имеется собственная функция f' с собственным числом λ_k такая, что $f|_{B_k} = f'|_{B_k}$. Рассмотрим разность $g = f - f'$. По утверждению 84 $\widehat{g}(z) \neq 0$ только если $\mathrm{wt}(z) = k$. Следовательно, $g|_{B_k} = 0$ и $\widehat{g}|_{Q_q^n \setminus B_k} = 0$. По утверждению 107 (b), $g = 0$. □

Из утверждений 20, 108 и утверждения задачи 90 вытекает

Следствие 46. *Если $k < n/2$, то собственная функция f в Q_q^n с собственным числом $\lambda_k = n(q-1) - qk$ однозначно восстанавливается по своим значениям на двух сферах S_k и S_{k-1}.*

В статье [109] приведены достаточные условия восстановления собственной функции по одной сфере. Следствие 46 и замечание 3 позволяют обобщить теорему 35 на q-ичный гиперкуб.

Следствие 47. *Пусть f — совершенная раскраска гиперкуба Q_q^n с матрицей параметров S. Пусть v — собственный вектор матрицы S, соответствующий собственному числу $\lambda_k = n(q-1) - qk$ матрицы S, причём $k < n/2$. Если все координаты вектора v различны, то функция f однозначно определяется своими значениям на двух сферах S_k и S_{k-1}.*

13.6 Преобразование Мак-Вильямс

Пусть M — матрица смежности гиперкуба Q_q^n. Вспомним, что $M_k = P_k(M)$, где M_k — матрица смежности по расстоянию k, P_k — q-полином Кравчука степени k. Если $M\psi = \lambda\psi$, то из утверждения 18 имеем равенство $\sum\limits_{x,d(x,a)=k} \psi(x) = (M_k\psi)(a) = P_k(\lambda)\psi(a)$. Поскольку собственное число характера ϕ_z зависит только от веса $\mathrm{wt}(z)$, далее будем нумеровать собственные числа весами соответствующих им характеров $M\phi_z(x) = \lambda_{\mathrm{wt}(z)}\phi_z(x)$.

Рассмотрим произвольную функцию $f : Q_q^n \to \mathbb{C}$. Введём обозначения $A_k[f] = \sum\limits_{x,d(x,0)=k} f(x)$ и $\widehat{A}_k[f] = \sum\limits_{z,d(z,0)=k} \widehat{f}(z)$ для весового спектра функции и её преобразования Фурье.

Утверждение 109 ([125])**.** *Пусть $f : Q_q^n \to \mathbb{C}$. Тогда $\widehat{A}_k[f] = \frac{1}{q^{n/2}} \sum\limits_m P_k(\lambda_m) A_m[f]$.*

Доказательство. Учитывая, что $\overline{\phi_z} = \phi_{-z}$ из определений получаем цепочку равенств

$$\widehat{A}_k[f] = \frac{1}{q^{n/2}} \sum_{z,d(z,0)=k} \sum_x f(x)\overline{\phi_z(x)} = \frac{1}{q^{n/2}} \sum_x f(x) \sum_{z,d(z,0)=k} \phi_z(x) =$$

$$= \frac{1}{q^{n/2}} \sum_x f(x) \sum_{z,d(z,0)=k} \phi_x(z) = \frac{1}{q^{n/2}} \sum_x f(x) P_k(\lambda_{\mathrm{wt}(x)}) = \frac{1}{q^{n/2}} \sum_m P_k(\lambda_m) A_m[f].$$

□

Отметим, что утверждение 109 может рассматриваться как частный случай утверждения 82 (теоремы Планшереля), где в качестве второй функции взят индикатор сферы радиуса k.

Определение 61. *Линейное преобразование, переводящее коэффициенты $A_m[f]$ в коэффициенты $\widehat{A}_k[f]$ называется преобразованием Мак-Вильямс.*

Из формулы $\widehat{\widehat{f(x)}} = f(-x)$ следует, что преобразование Мак-Вильямс невырожденно и идемпотентно при $q = 2$.

Предположим, что порядок гиперкуба q — простое число и что C — линейный код. Обозначим $A_k(C) = A_k[\chi_C]$. Тогда из утверждения 109 и следствия 42 имеем

$$|C|A_k(C^\perp) = \sum_m P_k(\lambda_m)A_m(C).$$

Последнее равенство называется тождеством Мак-Вильямс[39]. Отметим, что тождество Мак-Вильямс можно доказать, используя задачи 96 и 116.

Пусть C — некоторый код. Заметим, что число $f_C(a) = (\chi_C * \chi_{-C})(a)$ есть количество упорядоченных пар $(x, x-a)$ вершин кода, отличающихся на вектор a. Определим весовой спектр $(A_0[C], \ldots, A_n[C])$ кода C как $\frac{1}{|C|}(A_0[f_C], \ldots, A_n[f_C])$. Отметим, что $A_0[f_C] = \sum_x \chi_C^2(x) = |C|$ и

$$\sum_m A_m[C] = \frac{1}{|C|}\sum_x f_C(x) = \frac{1}{|C|}\sum_x\sum_a \chi_C(x)\chi_C(x-a) = |C|.$$

По определению линейного кода $\chi_C * \chi_{-C} = |C|\chi_C$. Поэтому для линейного кода $(A_0[C], \ldots, A_n[C]) = (A_0(C), \ldots, A_n(C))$.

Тогда $\widehat{A}_k[\chi_C * \chi_{-C}] = \widehat{A}_k[f_C] = \frac{1}{q^{n/2}}\sum\limits_m P_k(\lambda_m)A_m[f_C]$. Но $\widehat{\chi_C * \chi_{-C}} = q^{n/2}|\widehat{\chi_C}|^2$ из утверждений 85 и 89. Из утверждения 109 для любого k, $0 \le k \le n$, имеем равенство

$$q^n \cdot \sum_{z,\mathrm{wt}(z)=k} |\widehat{\chi_C}(z)|^2 = |C|\sum_m P_k(\lambda_m)A_m[C]. \qquad (22)$$

13.7 Граница линейного программирования

На использовании равенств (22) основано применение методов линейного программирования для вычисления верхней оценки мощности кода с кодовым расстоянием d. Действительно, если код C не содержит двух вершин на расстоянии меньше d, то $A_m[C] = 0$ при $m = 1, \ldots, d-1$, поскольку $\chi_C * \chi_{-C}(y) = 0$ при $0 < \mathrm{wt}(y) < d$. Отсюда получаем задачу линейного программирования на набор величин $A_m[C]$ для нахождения верхней оценки мощности кода с кодовым расстоянием d:

$$P_k(\lambda_0) + \sum_{m \ge d} P_k(\lambda_m)A_m[C] \ge 0 \text{ для любого } k \qquad (23)$$

[39] Равенствами и теоремами Мак-Вильямс называют также утверждения задач в конце этого раздела

$$|C| = 1 + \sum_{m \geq d} A_m[C] \to \max.$$

Известно, что верхней оценкой для значения целевой функции задачи линейного программирования, т. е. в данном случае для мощности кода, является любое решение двойственной задачи на минимум. На этом основана граница линейного программирования мощности кода с известным кодовым расстоянием, которая доказана в следующей теореме.

Теорема 41 (Дельсарт [115]). *Пусть C — некоторый код в гиперкубе Q_q^n с кодовым расстоянием d, а вектор $(y_0, \ldots, y_n) \in \mathbb{R}^{n+1}$ удовлетворяет условиям $y_0 > 0$, $y_i \geq 0$ при $i = 1, \ldots, n$ и $\sum\limits_{k=0}^{n} y_k P_k(\lambda_m) \leq 0$ при $m \geq d$. Тогда $|C| \leq \frac{1}{y_0} \sum\limits_{k=0}^{n} y_k P_k(\lambda_0)$.*

Доказательство. Как и раньше формально полагаем, что многочлен $P_0(x)$ тождественно равен единице. Тогда $|C| = P_0(\lambda_0) + \sum\limits_{m \geq d} P_0(\lambda_m) A_m[C]$. Из условия и неравенства (23) имеем неравенства

$$y_0|C| \leq \sum_{k=0}^{n} y_k \left(P_k(\lambda_0) + \sum_{m \geq d} P_k(\lambda_m) A_m[C] \right) \leq$$

$$\sum_{k=0}^{n} y_k P_k(\lambda_0) + \sum_{m \geq d} A_m[C] \left(\sum_{k=0}^{n} y_k P_k(\lambda_m) \right) \leq \sum_{k=0}^{n} y_k P_k(\lambda_0).$$

□

Обсудим как с помощью линейного программирования получать верхние оценки мощности кода. Предположим мы хотим оценить мощность кода, попарные расстояния между вершинами которого принимают только значения из списка $W = \{w_1, \ldots, w_m\}$. Рассмотрим многочлен R степени m такой, что $R(\lambda_{w_i}) \leq 0$, где $\lambda_{w_i} = n(q-1) - qw_i$ при $i = 1, \ldots, m$. Любой многочлен степени не выше m представим в виде линейной комбинации многочленов P_i при $i = 0, 1, \ldots, m$. Пусть $R = \sum\limits_{i=0}^{m} y_i P_i$. Если $y_0 > 0$ и $y_i \geq 0$ при $i = 1, \ldots, m$, то рассуждения, аналогичные приведённым выше, приводят к неравенству $|C| \leq \frac{1}{y_0} \sum\limits_{i=0}^{m} y_i P_i(\lambda_0)$, где $P_i(\lambda_0)$ — мощность шара радиуса i в Q_q^n.

В качестве примера докажем границу Плоткина мощности кода с большим кодовым расстоянием. Пусть кодовое расстояние $d_C > (1 - \frac{1}{q})n$, т. е. если $w_i \in W$, то $\lambda_{w_i} = n(q-1) - qw_i < 0$. Рассмотрим многочлен $R(x) = 1 - \frac{x}{n(q-1) - qd_C}$. По определению $R(\lambda_{w_i}) \leq 0$ для всех $w_i \in W$. Тогда

$$|C| \leq R(\lambda_0) = 1 - \frac{n(q-1)}{n(q-1) - qd_C} = \frac{qd_C}{qd_C - n(q-1)}. \qquad (24)$$

Неравенство (24) называется границей Плоткина. В случае $q = 2$ и $d_C = \frac{n+1}{2}$, n — нечётное, получаем границу Адамара $|C| \le n + 1$.

Заметим, что теорема 41 остается верной не только для кодов, но и для любых функций $F : Q_q^n \to \mathbb{R}$, если $A'_k[F] = \sum_{\mathrm{wt}(x)=k} F(x) \ge 0$ и $A'_0[F] = 1$. В этом случае роль мощности кода играет сумма значений функции F, т. е. $\sum\limits_{k=0}^{n} A'_k[F]$. Рассмотрим корреляционно иммунную функцию $f = {}_C$, $\mathrm{cor}(f) + 1 > (1 - \frac{1}{q})n$ и определим $F = q^{n/2}\widehat{f * f}/|C|^2$. Тогда $F(x) = q^n|\widehat{f}(x)|^2/|C|^2$, т. е. $A'_k[F] \ge 0$, $A'_0[F] = 1$, $A'_k[F] = 0$ при $k \le \mathrm{cor}(f)$. Для этой функции также верна граница Плоткина (24):

$$\sum_{k=0}^{n} A'_k[F] \le \frac{q(\mathrm{cor}(f)+1)}{q(\mathrm{cor}(f)+1) - n(q-1)}.$$

Кроме того, из равенства Парсеваля имеем $\sum\limits_{k=0}^{n} A'_k[F] = q^n/|C|$. Тогда имеем

$$\frac{|C|}{q^n} \ge 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}.$$

Таким образом, мы вновь получили неравенство Бирбрауэра–Фридмана (теорема 37), которое в [11] называется дуальной границей Плоткина.

Теорема 42 (Дельсарт [27]). *Пусть $f : Q_q^n \to \mathbb{C}$, найдутся k таких ненулевых весов $W = \{w_1, \dots, w_k\}$, что $\widehat{f}(x) = 0$ при $\mathrm{wt}(x) \notin W$ и $\widehat{f}(\bar{0}) \ne 0$. Тогда $|\mathrm{supp}(f)| \ge q^n/b(q,k)$, где $b(q,k)$ — мощность шара радиуса k.*

Доказательство. Пусть $\lambda_i = n(q-1) - qw_i$ — собственное число соответствующее весу w_i. По условию имеем $f = \rho\mathbf{1} + \sum_i \varphi_i$, где φ_i — собственная функция с собственным числом λ_i и $\rho \ne 0$. Пусть $A = (M - \lambda_1 I)\cdots(M - \lambda_k I)$, где M — матрица смежности гиперкуба Q_q^n. Имеем $Af = \rho A\mathbf{1}$, поскольку $A\varphi_i = \bar{0}$. Из равенства $M\mathbf{1} = n(q-1)$ следует, что $A\mathbf{1} = (n(q-1) - \lambda_1)\cdots(n(q-1) - \lambda_k)\mathbf{1} = \alpha\mathbf{1}$, где $\alpha \ne 0$.

С другой стороны $A = \sum\limits_{i=0}^{k} \beta_i M_i$, где M_i — матрица смежности по расстоянию i. Поэтому $Af = g * f$, где $\mathrm{supp}(g)$ содержится в шаре радиуса k. Для любого $x \in Q_q^n$ имеем $0 \ne Af(x) = g * f(x)$. Поэтому в каждом шаре радиуса k найдётся такая вершина y, что $f(y) \ne 0$. □

Следствие 48. *Пусть линейный код $C \subset Q_q^n$ содержит слова только различных k ненулевых весов. Тогда $|C| \le b(q,k)$.*

Доказательство. Рассмотрим дуальный код $C^\perp$. По теореме Дельсарта получаем $|C^\perp| \ge q^n/b(q,k)$. Из равенства $|C||C^\perp| = q^n$ получаем требуемое. □

Однако, утверждение следствия 48 остаётся верным и для нелинейных кодов. Докажем это в случае $q = 2$.

Теорема 43 (Дельсарт [27]). *Пусть код $C \subset Q_2^n$ состоит из кодовых слов, попарные расстояния между которыми принимают только k различных ненулевых значений. Тогда $|C| \le b(2,k)$.*

Доказательство. Пусть D — множество попарных расстояний кода C, $|D| = k$. Рассмотрим множество функций $f : \{-1,1\}^n \to \mathbb{R}$ как 2^n-мерное линейное пространство V_n. Нетрудно видеть, что мономы вида $x_{i_1} \cdots x_{i_m}$, $m = 0, \ldots, n$, являются ортогональным базисом V_n, которой соответствует базису характеров группы $\mathbb{Z}_2^n$.

Каждому кодовому слову $v \in C$ поставим в соответствие функцию $f_v(x) = \prod\limits_{t \in D} (((-1)^v, x) - (n - 2t))$. Поскольку $((-1)^v, (-1)^u) = n - 2d(u,v)$, $f_v((-1)^u) = 0$ для любого такого $u \in Q_2^n$, что $d(u,v) \in D$, и $f_v((-1)^v) \ne 0$. Покажем, что множество функций $\{f_v : v \in C\}$ линейно независимо. Пусть $L = \sum\limits_{v \in C} \alpha_v f_v = 0$. Тогда $L((-1)^v) = \alpha_v f_v((-1)^v) = 0$ и $\alpha_v = 0$.

Нетрудно видеть, что множество $\{f_v : v \in C\}$ состоит из функций степени не выше k, в котором базисом являются мономы степени не выше k. Таких мономов ровно $b(2,k)$. □

13.8 Весовые спектры совершенной раскраски

Любая совершенная 2-раскраска гиперкуба определяется своим усреднённым весовым спектром.

Утверждение 110. *Пусть C — некоторый код в гиперкубе Q_q^n, и его весовой спектр $(A_0[C], \ldots, A_n[C])$ такой же, как у некоторой совершенной раскраски f в два цвета. Тогда χ_C — совершенная раскраска с параметрами раскраски f.*

Доказательство. Функция χ_C является совершенной раскраской, если и только если $\mathrm{supp}(\widehat{\chi_C})$ содержит только нулевой вектор и векторы некоторого фиксированного веса (см. утверждения 10 и 95). Тогда требуемое следует из формулы $q^n \cdot \sum\limits_{z, \mathrm{wt}(z)=k} |\widehat{\chi_C}(z)|^2 = |C| \sum\limits_m P_k(\lambda_m) A_m[C]$. Параметры 2-раскраски нетрудно найти из прямого и дуального весового распределения. □

Из теоремы 5 следует более сильное утверждение.

Утверждение 111. *Пусть f — некоторая k-раскраска графа, регулярного по расстоянию 2. Предположим, что для любого i, $i = 1, \ldots, k$, усреднённый цветовой состав окружения i-го цвета C_i раскраски f такой же как у i-го цвета D_i совершенной раскраски g. Если $A_2[C_i] = A_2[D_i]$, то f — совершенная раскраска с параметрами раскраски g.*

По утверждению 85 для любой функции, принимающей только вещественные значения, верны равенства $\widehat{f(-x)} = \overline{\widehat{f(x)}}$ и $\widehat{\widehat{f(-x)}} = f(x)$. Поэтому равенство $\widehat{A}_k[f] = \frac{1}{q^{n/2}} \sum\limits_m P_k(\lambda_m) A_m[f]$ можно обратить

$$A_k[f] = \frac{1}{q^{n/2}} \sum_m P_k(\lambda_m) \widehat{A}_m[f(-x)] = \frac{1}{q^{n/2}} \sum_m P_k(\lambda_m) \overline{\widehat{A}_m[f]}.$$

Кроме того, его можно обобщить на случай декартовых произведений. Предположим, что $K = Q_{q_1}^{n_1} \times Q_{q_2}^{n_2}$. Из утверждения 74 следует, что базис характеров на K состоит из произведений характеров на $Q_{q_1}^{n_1}$ и характеров на $Q_{q_2}^{n_2}$. Для функции $f : K \to \mathbb{C}$ определим $A_{k_1 k_2}[f] = \sum\limits_{\mathrm{wt}(x_1)=k_1} \sum\limits_{\mathrm{wt}(x_2)=k_2} f(x_1, x_2)$ и $\widehat{A}_{k_1 k_2}[f] = \sum\limits_{wt(z_1)=k_1} \sum\limits_{\mathrm{wt}(z_2)=k_2} \widehat{f}(z_1, z_2)$. Тогда аналогично доказательству утверждения 109 получаем равенство

$$\widehat{A}_{k_1 k_2}[f] = \frac{1}{q_1^{n_1/2} q_2^{n_2/2}} \sum_{m_1, m_2} P_{k_1}[n_1, q_1](\lambda_{m_1}) P_{k_2}[n_2, q_2](\lambda_{m_2}) A_{m_1 m_2}[f]. \tag{25}$$

В равенстве (25) коэффициенты $\widehat{A}_{k_1 k_2}[f]$ и $A_{k_1 k_2}[f]$ также можно поменять местами (с добавлением комплексного сопряжения при $q \neq 2$).

Пусть $f : Q_q^n \to \mathbb{C}$ и $\Gamma \subset Q_q^n$ — некоторая грань. Определим локальное распределение функции f в грани Γ как весовой спектр сужения $f|_\Gamma$ функции f на грань Γ.

Теорема 44 (Васильева [107]). *Пусть $g : Q_q^n \to \mathbb{C}$ есть собственная функция гиперкуба Q_q^n. Тогда локальное распределение функции g в грани $\Gamma^\perp$ линейно зависит от локального распределения функции g в грани Γ.*

Доказательство. Представим гиперкуб Q_q^n как декартово произведение граней: $Q_q^n = \Gamma \times \Gamma^\perp$. Из равенства (25) имеем равенства

$$A_{k_1 k_2}[g] = \frac{1}{q^{n/2}} \sum_{m_1, m_2} P_{k_1}[n_1, q](\lambda_{m_1}) P_{k_2}[n_2, q](\lambda_{m_2}) \overline{\widehat{A}_{m_1 m_2}[g]},$$

где $n_1 = \dim \Gamma$ и $n_2 = n - n_1 = \dim \Gamma^\perp$.

Из определения $\widehat{A}_{m_1 m_2}[g]$ следует, что $\widehat{A}_{m_1 m_2}[g] = 0$ при $m_1 + m_2 \neq m$, где $n(q-1) - mq = \lambda$ — собственное число функции g. Отметим, что $P_0[n_2, q] \equiv 1$. Тогда при $k_1 = 0, \ldots, \dim \Gamma$ имеем равенства

$$A_{k_1 0}[g] = \frac{1}{q^{n/2}} \sum_{m_1 + m_2 = m} P_{k_1}[n_1, q](\lambda_{m_1}) \overline{\widehat{A}_{m_1 m_2}[g]}. \tag{26}$$

Преобразование Мак-Вильямс обратимо, поэтому из последнего равенства линейно выражаются коэффициенты $\overline{\widehat{A}_{m_1 m_2}[g]}$ для любых $m_1 + m_2 = m$. Аналогично при $k_2 = 0, \ldots, \dim \Gamma^\perp$ имеем равенства

$$A_{0 k_2}[g] = \frac{1}{q^{n/2}} \sum_{m_1 + m_2 = m} P_{k_2}[n_2, q](\lambda_{m_2}) \overline{\widehat{A}_{m_1 m_2}[g]}.$$

Набор величин $A_{0k_2}[g]$ является локальным распределением функции g в грани $\Gamma^\perp$. Мы показали, что его можно выразить линейно через набор величин $A_{k_10}[g]$, который является локальным распределением функции g в грани Γ. $\square$

Следствие 49. *Пусть $f : Q_q^n \to \{0,1\}$ — совершенная раскраска с матрицей параметров S. Тогда весовое распределение раскраски f в грани Γ определяет весовое распределение f в грани $\Gamma^\perp$.*

Доказательство. Пусть f_1 и f_2 — две совершенные раскраски с матрицей параметров S. Рассмотрим функцию $g = f_1 - f_2$. Поскольку f_1 и f_2 раскраски в два цвета с одинаковыми параметрами, из утверждения 10 следует, что g — собственная функция в Q_q^n. Из теоремы Васильевой следует, что если функция g имеет нулевое локальное распределение в грани Γ, то она имеет нулевое локальное распределение и в грани $\Gamma^\perp$. Очевидно, $A_{m_1m_2}[g] = A_{m_1m_2}[f_1] - A_{m_1m_2}[f_2]$. Поэтому, если локальные распределения f_1 и f_2 совпадают в грани Γ, то они совпадают и в грани $\Gamma^\perp$. $\square$

Теорема Васильевой утверждает, что весовые спектры собственной функции g в ортогональных гранях связаны линейными соотношениями. Предположим, что все коэффициенты в этих соотношениях ненулевые. Покажем, что в этом случае значения собственной функции $g : Q_2^n \to \mathbb{C}$ в вершинах веса меньше d однозначно восстанавливается по своим значениям в вершинах веса $d \le n/2$. Пусть собственные функции g и g' совпадают на вершинах веса d. Рассмотрим функцию $f = g - g'$. Пусть u — вершина минимального веса $\mathrm{wt}(u) = d' < d$, для которой $f(u) \neq 0$. Рассмотрим грань Γ размерности d', содержащую вершины $\bar{0}$ и u. Соответствующие этой грани локальные весовые коэффициенты равны $A_{00}[f] = 0, \ldots, A_{(d'-1)0}[f] = 0$, $A_{d'0}[f] = f(u) \neq 0$. Рассмотрим грань $\Gamma^\perp$. С одной стороны, $A_{0d}[f] = 0$, поскольку $f(v) = 0$ для всех вершин веса $\mathrm{wt}(v) = d$. Но $A_{0d}[f] = \alpha A_{d'0}[f]$, где $\alpha \neq 0$ по условию. Пришли к противоречию.

Задача 116. Пусть $f : Q_q^n \to \mathbb{C}$ и $C \subset Q_q^n$ — линейный код. Докажите равенство $\frac{1}{q^{n/2}} \sum\limits_{x \in C} f(x) = \frac{1}{|C^\perp|} \sum\limits_{z \in C^\perp} \widehat{f}(z)$.

Задача 117. Пусть $A \subset Q_q^n$, q — простое и $C = \mathrm{supp}(\widehat{\mathbf{1}_A})$. Докажите, что для любого $v \in Q_q^n$ равенство $A + v = A$ верно тогда и только тогда, когда $v \in C^\perp$.

Задача 118. Пусть $C \subset Q_q^n$, q — простое и $f = \widehat{\mathbf{1}_C}$. Докажите, что $|f| = \mathbf{1}_A$ для некоторых $c > 0$ и $A \subset Q_q^n$ тогда и только тогда, когда C и A аффинные подпространства.

Задача 119. Пусть $A \subset Q_q^n$ — аффинный код, все слова которого имеют одинаковый вес w. Докажите, что $|A| \leq q^n/L(w)$, где $L(w)$ — минимальная мощность носителя собственной функции с собственным числом $\lambda = n(q-1) - qw$.

Задача 120. Пусть $A \subset Q_2^n$ — аффинный код, все слова которого имеют одинаковый вес w. Докажите, что $|A| \leq 2^{(n-|n-2w|)/2}$ (см. задачу 97). Докажите, что эта оценка достигается для аффинных кодов $A = \{(x, x \oplus \bar{1}, \bar{0}) : x \in Q_2^{(n-i)/2}\}$, $i = n - 2k$.

Задача 121. Пусть χ_C — совершенная раскраска в два цвета в гиперкубе. Докажите, что $C^\perp$ — эквидистантный код, т. е. расстояние между любыми парами его вершин одинаково.

Задача 122. Докажите, что если пары векторов в n-мерном евклидовом пространстве образуют только тупые и прямые углы, то их число не превосходит $2n$. Докажите, что мощность двоичного кода длины $2n$ с кодовым расстоянием не меньше n не превосходит $4n$.

Задача 123. Код в Q_q^n называется равновесным, если все его вершины (за возможным исключением вершины $\bar{0}$) имеют одинаковый вес. Докажите, что линейный равновесный код не может содержать больше чем $n(q-1)+1$ вершин.

Задача 124. Пусть $f : Q_2^n \to \{0,1\}$ — совершенная раскраска с максимальным, не считая n, собственным числом $\lambda = n - 2k$. Докажите, что функция f полностью определяется своими значениями в шаре радиуса $n-k$.

Задача 125. Пусть $f : Q_3^n \to \{0,1\}$ — совершенная раскраска с собственным числом $\lambda = 2n - 3k$. Докажите, что $|\widehat{f}(z)| \geq 3^{k-\frac{n}{2}}$, если $\widehat{f}(z) \neq 0$.

Задача 126. Докажите, что две различные корреляционно-иммунные функции порядка k в булевом гиперкубе отличаются друг от друга на множестве мощности не меньше 2^{k+1}.

Задача 127. Пусть $\Gamma \subset Q_2^n$ — произвольная грань, содержащая $\bar{0}$ и две булевы функции f и g таковы, что $\widehat{f}|_\Gamma = \widehat{g}|_\Gamma$. Докажите, что равенство $\sum\limits_{x \in z \oplus \Gamma^\perp} (-1)^{f(x)} = \sum\limits_{x \in z \oplus \Gamma^\perp} (-1)^{g(x)}$ верно для любого $z \in Q_2^n$.

Задача 128. Докажите равенство $2^{n-t}\binom{t}{k} = \sum\limits_{m=0}^{n-t} P_k[n,2](\lambda_m)\binom{n-t}{m}$ при $0 < k < t < n$.

Задача 129. Применяя производящую функцию многочленов Кравчука (17), докажите, что для любой функции $f : Q_q^n \to \mathbb{C}$ справедливо равенство многочленов $q^{n/2} \sum\limits_{k=0}^{n} \widehat{A}_k[f] z^k = \sum\limits_{m=0}^{n} A_m[f](1-z)^m(1+(q-1)z)^{n-m}$.

В частности, для линейного кода $C \subset Q_q^n$ справедливо равенство
$|C| \sum\limits_{k=0}^{n} A_k(C^\perp) z^k = \sum\limits_{m=0}^{n} A_m(C)(1-z)^m(1+(q-1)z)^{n-m}$.

Задача 130. Для любой функции $f : Q_q^n \to \mathbb{C}$ и числа $i = 0, \ldots, n$ докажите равенства многочленов
$\sum\limits_{k=0}^{n} \widehat{A}_k[f]\binom{k}{i} = q^{\frac{n}{2}-i} \sum\limits_{m=0}^{n} (-1)^m (q-1)^{i-m} A_m[f]\binom{n-m}{n-i}$, где биномиальные коэффициенты $\binom{a}{b}$ считаются равными нулю при $a < b$.

Задача 131. Докажите, что для любой функции $f : Q_q^n \to \mathbb{C}$ справедливо равенство $\sum\limits_{k=0}^{n} k\widehat{A}_k[f] = q^{\frac{n}{2}-1}((q-1)nA_0[f] - A_1[f])$. В частности, для линейного кода $C \subset Q_q^n$ размерности m справедливо равенство
$\sum\limits_{k=0}^{n} kA_k(C) = q^{m-1}((q-1)n - A_1(C^\perp))$.

Задача 132. Для линейного кода $C \subset Q_2^n$ докажите равенство многочленов от двух переменных
$|C| \sum\limits_{v \in C^\perp} x^{\mathrm{wt}(v)} y^{n-\mathrm{wt}(v)} = \sum\limits_{u \in C} (y-x)^{\mathrm{wt}(u)} (x+y)^{n-\mathrm{wt}(u)}$.

Задача 133. Пусть $C \subset Q_q^n$ — эквидистантный код с кодовым расстоянием $d > n(q-1)/q$. Докажите, что $|C| \leq 1/(1 - \frac{(q-1)n}{qd})$.

Задача 134. Пусть $C \subset Q_2^n$ — код с расстоянием d нечётной мощности. Докажите неравенство $P_k(\lambda_0) + \sum\limits_{m \geq d} P_k(\lambda_m) A_m[C] \geq \frac{\binom{n}{k}}{|C|}$ для любого k, $0 \leq k \leq n$.

Задача 135. Пусть код $C \subset Q_2^n$ состоит из кодовых слов, попарные расстояния между которыми принимают значения только из множества D, причём числа t и $n-t$ содержатся в D одновременно и $0, n \notin D$. Докажите, что
1) если $n/2 \notin D$, то $|C| \leq 1 + \binom{n}{2} + \binom{n}{4} + \cdots + \binom{n}{|D|}$;
2) если $n/2 \in D$, то $|C| \leq \binom{n}{1} + \binom{n}{3} + \cdots + \binom{n}{|D|}$.

14 Бент-функции, разностные множества и сильно регулярные графы

14.1 Определение и основные свойства бент-функций

Определение 62. *Отображение $b : Q_q^n \to Q_q$ называется бент-функцией, если $|\widehat{\xi^b}(z)| = \frac{1}{q^{n/2}}|(\xi^b, \phi_z)| = 1$ для всех $z \in Q_q^n$.*

Будем рассматривать прямые $\{\alpha\phi_z \mid \alpha \in \mathbb{C}\}$, заданные характерами, как оси координат. Тогда расстоянием вектора g до оси координат можно считать длину вектора g', где $g = g' + \alpha_z\phi_z$ и $(g', \phi_z) = 0$. Имеем $\|g'\|_2^2 = \|g\|_2^2 - q^n|\alpha_z|^2$. Поскольку $q^n \sum_z |\alpha_z|^2 = \|g\|_2^2$ (равенство Парсеваля), наиболее удалённой от координатных осей будет функция, у которой все коэффициенты Фурье равны по абсолютной величине.

Для любой бент-функции[40] b верно, что $q^{n/2}|\alpha_z| = |\widehat{\xi^b}(z)| = 1$ по определению. Следовательно, ξ^b — это ровно те функции, которые находятся на максимальном расстоянии от осей, заданных характерами, т. е. функциями вида $\xi^{\langle x,a\rangle}$. Эти оси содержат в качестве показателей не только линейные, но и все аффинные функции $\langle x, a\rangle + c$. В этом смысле, но не в смысле расстояния Хэмминга, бент-функции одинаково удалены от всех аффинных функций.

Замечание 19. В этом разделе мы для простоты изложения полагаем, что q — простое, т. е. гиперкуб Q_q^n можно рассматривать как векторное пространство $(GF(q))^n$. В этом случае можно показать, что все аффинные функции $f : Q_q^n \to Q_q$ исчерпываются функциями вида $\langle x, a\rangle + c$. При не простом q представление $f(x) = \langle x, a\rangle + c$ считается определением аффинной функции.

Бент-функции применяются в блочных и поточных шифрах для повышению стойкости шифров к линейному криптоанализу, когда злоумышленник пытается найти наилучшую аппроксимацию неизвестной функции, используя аффинные функции.

Утверждение 112. *Функция b является бент-функцией тогда и только тогда, когда $\xi^b * \xi^{\tilde{b}}(z) = q^{n/2}\delta$, где $\tilde{b}(x) = -b(-x)$.*

Доказательство. Применим преобразование Фурье к равенству $\xi^b * \xi^{\tilde{b}}(z) = q^{n/2}\delta$. Из свойств преобразования Фурье $\widehat{f(-x)} = \overline{\widehat{f(x)}}$ и $\widehat{f * g} = q^{n/2}\widehat{f} \cdot \widehat{g}$ получаем равносильное равенство $\widehat{\xi^b} \cdot \widehat{\xi^{\tilde{b}}} = \widehat{\xi^b} \cdot \overline{\widehat{\xi^b}} = \mathbf{1}$. □

Утверждение 113. *Пусть $b : Q_q^n \to Q_q$ — бент-функция и $\widehat{\xi^b} = \xi^f$ для некоторой функции $f : Q_q^n \to Q_q$. Тогда f — бент-функция.*

Доказательство. Имеем равенства $\widehat{\xi^{f(x)}} = \widehat{\widehat{\xi^{b(x)}}} = \xi^{b(-x)}$. Тогда $|\widehat{\xi^f}| = |\xi^{b(-x)}| = 1$. □

Бент-функция называется регулярной, если для неё выполнено условие утверждения 113, при $q = 2$ все бент-функции регулярные. Бент-функция b называется слабо регулярной, если $\widehat{\xi^b} = \alpha\xi^f$ для некоторой q-ичной функции f и константы α, $|\alpha| = 1$.

[40] Подробное изложение теории бент-функций имеется в [71] и [136].

Пример 44. Определим квадратичную форму $g : Q_q^{2n} \to Q_q$ равенством $g(x,y) = \langle x,y\rangle = \sum\limits_{i=1}^{n} x_i y_i \mod q$. Покажем, что g — бент-функция. Справедливы равенства

$$\widehat{\xi^g}(u,v) = \frac{1}{q^n}\sum_{x,y} \xi^{\langle x,y\rangle - \langle x,u\rangle - \langle y,v\rangle} = \frac{1}{q^n}\sum_{y} \xi^{-\langle y,v\rangle}\sum_{x} \xi^{\langle x,y-u\rangle}.$$

Сумма значений характера во всех вершинах равна нулю, за исключением характера ϕ_0 (см. утверждение 72). Поэтому $\sum\limits_{x} \xi^{\langle x,y-u\rangle} = 0$ при $y \neq u$. Тогда $\widehat{\xi^g}(u,v) = \xi^{-\langle u,v\rangle}$ и g — бент-функция по определению.

Лемма 5. *Пусть $f : Q_q^n \to \mathbb{C}$ — некоторая функция. Определим матрицу A размера $q^n \times q^n$ равенством $A_f(x,y) = f(x-y)$. Тогда $A_f A_g = A_{f*g}$.*

Доказательство. Имеем равенства

$$A_f A_g(x,z) = \sum_{y\in Q_q^n} f(x-y)g(y-z) = \sum_{u\in Q_q^n} f(u)g(x-z-u) = (f*g)(x-z) = A_{f*g}(x,z).$$

□

Нам понадобится следующее утверждение из алгебры.

Утверждение 114 ([64]). *Если q — простое, то рациональная линейная комбинация $\sum\limits_{a\in Q_q} \alpha_a \xi^a$, $\xi = e^{2\pi i/q}$, равна нулю тогда и только тогда, когда все коэффициенты α_a равны.*

Заметим, что $\sum\limits_{a\in Q_q} \xi^a = 0$ для произвольных целых q, что является частным случаем утверждения 32 для группы $\mathbb{Z}_q$.

Утверждение 115. *Функция b является бент-функцией тогда и только тогда, когда $H(x,y) = \xi^{b(x-y)}$ — обобщённая матрица Адамара.*

Доказательство. Имеем $H^*(x,y) = \xi^{\widetilde{b}(x-y)}$. Тогда из леммы 5 получаем равенство $HH^*(x,y) = [\xi^b * \xi^{\widetilde{b}}](x-y) = NI_N$, где $N = q^n$. □

При $q = 2$ матрица $H(x,y) = (-1)^{b(x-y)}$ является матрицей Адамара.

Для произвольной функции $f : Q_q^n \to Q_q$ определим оператор $D_y[f](x) = f(x+y) - f(x)$, который можно назвать *дискретной производной* функции f по направлению y.

Утверждение 116. *Для любого ненулевого y функция $D_y[f]$ принимает все q значений одинаковое число раз тогда и только тогда, когда f — бент-функция.*

Доказательство. Имеем равенство

$$\xi^f * \xi^{\widetilde{f}}(z) = \sum_{x \in Q_q^n} \xi^{f(z-x)} \xi^{-f(-x)} = \sum_{y \in Q_q^n} \xi^{f(z+y)-f(y)}.$$

Из равенства $\sum\limits_{a \in Q_q} \xi^a = 0$ следует, что $\xi^f * \xi^{\widetilde{f}}(z) = 0$ при $z \neq \bar{0}$. Тогда из утверждения 112 следует, что f — бент-функция.

Обратное утверждение следует из утверждения 114. □

14.2 Булевы бент-функции и платовидные функции

Рассмотрим подробнее случай $q = 2$. Вспомним, что преобразование Адамара—Уолша булевой функции $f : Q_2^n \to Q_2$ определяется как $\widehat{(-1)^f}$. Следовательно, булева функция является бент-функцией тогда и только тогда, когда все её коэффициеты Адамара—Уолша равны единице по модулю.

Утверждение 117. *Если f — булева бент-функция, то $\widehat{f}(\bar{0}) = \frac{1}{2}(2^{n/2} - \widehat{(-1)^f}(\bar{0})) = \frac{1}{2}(2^{n/2} \pm 1)$.*

Доказательство. Нетрудно видеть, что $(-1)^f = \mathbf{1} - 2f$, поэтому $\widehat{(-1)^f} = \delta - 2\widehat{f}$. В частности, $\widehat{(-1)^f}(\bar{0}) = 2^{n/2} - 2\widehat{f}(\bar{0})$. Из определения бент-функции и равенства Парсеваля следует, что $|\widehat{(-1)^f}(\bar{0})| = 1$. □

Пусть $\mathcal{A}$ — множество аффинных булевых функций, т. е. функций вида $f(x) = \langle x, z \rangle$ или $f(x) = \langle x, z \rangle \oplus 1$.

Определение 63. *Нелинейностью булевой функции f называется расстояние Хэмминга от f до множества аффинных функций: $nl(f) = \min\limits_{\ell \in \mathcal{A}} d_H(f, \ell)$, где $d_H(f, \ell) = |\mathrm{supp}(f \oplus \ell)|$.*

Расстояние Хэмминга между булевыми функциями f и g можно выразить через скалярное произведение функций $(-1)^f$ и $(-1)^g$, которое определяет евклидово расстояние между функциями $(-1)^f$ и $(-1)^g$. Для любых двух булевых функций справедливо равенство $d_H(f, g) = \frac{1}{2}(2^n - ((-1)^f, (-1)^g))$, поскольку $2^n - 2d_H(f, g) = ((-1)^f, (-1)^g))$ — это разность числа вершин, в которых булевы функции f и g совпадают и не совпадают.

Утверждение 118. $nl(f) = \frac{1}{2}(2^n - 2^{n/2} \max\limits_z |\widehat{(-1)^f}(z)|)$.

Доказательство. Булева функция ℓ является аффинной тогда и только тогда, когда $(-1)^\ell = \phi_z$ или $(-1)^\ell = -\phi_z$. Из определения преобразования Фурье имеем $((-1)^f, \pm\phi_z) = \pm 2^{n/2} \widehat{(-1)^f}(z)$. □

Утверждение 119 ([84]). *Справедливо неравенство* $nl(f) \leq \frac{1}{2}(2^n - 2^{n/2})$. *В неравенстве достигается равенство тогда и только тогда, когда* f *— бент-функция.*

Доказательство. Из равенства Парсеваля имеем $\sum\limits_{z \in Q_2^n} |\widehat{(-1)^f}(z)|^2 = \sum\limits_{x \in Q_2^n} |(-1)^f(x)|^2 = 2^n$. Поэтому $\max\limits_z |\widehat{(-1)^f}(z)|^2 \geq 1$. Равенство возможно только если $|\widehat{(-1)^f}(z)| = 1$ для всех $z \in Q_2^n$. Осталось воспользоваться утверждением 118. □

Очевидно, нелинейность булевой функции может принимать только целые значения, поэтому для нечётных n булевы бент-функции не существуют. Из примера 44 следует, что для любых чётных n бент-функции существуют.

Определение 64. *Булева функция* f *называется платовидной, если её коэффициенты Адамара—Уолша принимают только три различных значения* $0, \pm a$ *для некоторого* $a \in \mathbb{R}$.

Из равенства Парсеваля следует, что число a^2 делит нацело 2^n. Поэтому $a^2 = 2^s$, где s — неотрицательное целое. Платовидную функцию, коэффициенты Адамара—Уолша которой принимают значения $0, \pm 2^{s/2}$, называют s-платовидной. В частности, 0-платовидная функция является бент-функцией.

Утверждение 120. *Булева функция* f *является платовидной, если и только если* $(-1)^f * (-1)^f * (-1)^f = a^2 2^n (-1)^f$ *для некоторого* $a \in \mathbb{R}$.

Доказательство. Из свойств преобразования Фурье от свёртки двух функций (утверждение 89) следует, что равенство $(-1)^f * (-1)^f * (-1)^f = a^2 2^n (-1)^f$ эквивалентно равенству

$$2^n(\widehat{(-1)^f})^3 - a^2 2^n \widehat{(-1)^f} = \widehat{(-1)^f} 2^n (\widehat{(-1)^f})^2 - a^2) = 0.$$

Последнее равенство выполнено тогда и только тогда, когда коэффициенты Адамара—Уолша функции f принимают только три различных значения $0, \pm a$. □

Теорема 45 (Тарannиков [96]). *Пусть* f *—булева функция и* $\mathrm{cor}(f) \leq n - 1$. *Тогда справедливы неравенства* $nl(f) \leq 2^{n-1} - 2^{\mathrm{cor}(f)}$ *(если* f *не устойчива) и* $nl(f) \leq 2^{n-1} - 2^{1+\mathrm{cor}(f)}$ *(если* f *устойчива).*
Если в неравенствах достигается равенство, то функция f *— платовидная.*

Доказательство. Пусть функция f не устойчива. По следствию 44 из тождества Саркара видим, что коэффициенты Адамара —Уолша имеют вид $m 2^{1+\mathrm{cor}(f)-\frac{n}{2}}$, где m — целое. Из утверждения 118 имеем $nl(f) \leq$

$2^{n-1}-2^{\mathrm{cor}(f)}$. Если в этом неравенстве достигается равенство, то все ненулевые коэффициенты Адамара — Уолша функции f имеют вид $\pm 2^{\mathrm{cor}(f)+1-\frac{n}{2}}$. Случай, когда функция f устойчива рассматривается аналогично. $\square$

Опишем способ построения бент-функций и платовидных функций, обобщающий пример 44. Пусть $x \in Q_2^n$, $k \le n$. Через x^k обозначим вектор из первых k координат вектора x.

Утверждение 121 (конструкция Майораны–МакФарланда). *Пусть $x, y, u, v \in Q_2^n$, $z, w \in Q_2^k$, $k \le n$. Рассмотрим перестановки $\tau : Q_2^n \to Q_2^n$ and $\sigma : Q_2^k \to Q_2^k$ и произвольную функцию $f : Q_2^n \to Q_2$. Тогда $F(x,y,z) = \langle \tau(x), y\rangle + \langle \sigma(x^k), z\rangle + f(x)$ является k-платовидной функцией от $2n+k$ переменных.*

Доказательство.
$2^{n+\frac{k}{2}}\widehat{(-1)^F}(u,v,w) = \sum\limits_{x,y,z\in Q_2^n} (-1)^{\langle \tau(x),y\rangle + \langle \sigma(x^k),z\rangle + f(x) - \langle x,u\rangle - \langle v,y\rangle - \langle w,z\rangle} =$
$\sum\limits_{x\in Q_2^n} (-1)^{f(x)-\langle x,u\rangle} \sum\limits_{y\in Q_2^n} (-1)^{\langle \tau(x),y\rangle - \langle v,y\rangle} \sum\limits_{z\in Q_2^k} (-1)^{\langle \sigma(x^k),z\rangle - \langle w,z\rangle}$.

Нетрудно видеть, что суммы $\sum\limits_{z\in Q_2^k} (-1)^{\langle \sigma(x^k),z\rangle - \langle w,z\rangle}$ равны 2^k, если $w = \sigma(x^k)$, и равны 0 в остальных случаях. Аналогично суммы $\sum\limits_{y\in Q_2^n} (-1)^{\langle \tau(x),y\rangle - \langle v,y\rangle}$ равны 2^n, если $v = \tau(x)$ и равны 0 в остальных случаях.

Следовательно, $2^{n+\frac{k}{2}}\widehat{(-1)^F}(u,v,w) = 2^{n+k}(-1)^{f(x)-\langle x,u\rangle}$ если $v = \tau(x)$ и $w = \sigma(x)$; в остальных случаях $2^{n+\frac{k}{2}}\widehat{(-1)^F}(u,v,w) = 0$. $\square$

14.3 Нелинейность q-ичных функций

Каждая аффинная функция $g : Q_q^n \to Q_q$ может быть представлена в виде $g(x) = \langle z, x\rangle + a$. Для произвольной функции $f : Q_q^n \to Q_q$ определим следующие величины $\delta_f^{z,a} = \frac{q-1}{q} - \frac{d_H(f,g)}{q^n}$, где $g(x) = \langle z, x\rangle + a$.

Из определения нетрудно установить следующие свойств величин $\delta_f^{z,a}$.

Утверждение 122. *1. Для любой фиксированной пары $a \in Q_q$ и $z \in Q_q^n$ имеем $\sum\limits_f \delta_f^{z,a} = 0$, где сумма берётся по всем функциям f.*

2. Для любой функции f и $z \in Q_q^n$ имеем $\sum\limits_{a\in F_q} \delta_f^{z,a} = 0$.

3. Минимальное значение величины $\delta_f^{z,a}$ равно $-\frac{1}{q}$, а максимальное $\frac{q-1}{q}$.

Также как и в булевом случае, определим нелинейность q-ичной функции $f : Q_q^n \to Q_q$ как расстояние Хэмминга от f до множества аффинных функций. Из определений следует равенство

$$nl(f) = q^{n-1}(q-1) - q^n \max_{z,a} \delta_f^{z,a}. \qquad (27)$$

Следующая теорема по существу является новым представлением равенства Парсеваля.

Теорема 46 (Рябов [85], Теорема 3). $\sum\limits_{z\in Q_q^n, a\in Q_q} (\delta_f^{z,a})^2 = \frac{q-1}{q}$.

Доказательство. Докажем теорему по индукции. Для $n = 0$ равенство легко проверяется непосредственно. Докажем шаг индукции. Из определений имеем

$$\delta_f^{z,a} = \frac{1}{q}\sum_{c\in Q_q} \delta_{f|_{x_n=c}}^{z',a+cz_n}, \qquad \text{где} \quad z = (z', z_n).$$

Тогда

$$(\delta_f^{z,a})^2 = \frac{1}{q^2}\sum_{c_1,c_2\in Q_q} \delta_{f|_{x_n=c_1}}^{z',a+c_1z_n}\delta_{f|_{x_n=c_2}}^{z',a+c_2z_n} = \frac{1}{q^2}\sum_{c_1\neq c_2} \delta_{f|_{x_n=c_1}}^{z',a+c_1z_n}\delta_{f|_{x_n=c_2}}^{z',a+c_2z_n} + \frac{1}{q^2}\sum_{c\in Q_q} (\delta_{f|_{x_n=c}}^{z',a+cz_n})^2.$$

По предположению индукции имеем

$$\sum_{z\in Q_q^n, a\in Q_q} \frac{1}{q^2}\sum_{c\in Q_q} (\delta_{f|_{x_n=c}}^{z',a+cz_n})^2 = \frac{1}{q^2}\sum_{c\in Q_q}\sum_{z_n\in Q_q}\sum_{z'\in Q_p^{n-1}, a\in Q_q} (\delta_{f|_{x_n=c}}^{z',a+cz_n})^2 = \frac{q^2}{q^2}\frac{q-1}{q}.$$

$$\sum_{z\in Q_q^n, a\in Q_q}\sum_{c_1\neq c_2} \delta_{f|_{x_n=c_1}}^{z',a+c_1z_n}\delta_{f|_{x_n=c_2}}^{z',a+c_2z_n} = \sum_{c_1\neq c_2}\sum_{z'\in Q_q^{n-1}}\sum_{z_n\in Q_q}\sum_{a\in Q_q} \delta_{f|_{x_n=c_1}}^{z',a+c_1z_n}\delta_{f|_{x_n=c_2}}^{z',a+c_2z_n} =$$

$$= \sum_{c_1\neq c_2}\sum_{z'\in Q_q^{n-1}} \left(\sum_{a_1\in Q_q} \delta_{f|_{x_n=c_1}}^{z',a_1}\right)\left(\sum_{a_2\in Q_q} \delta_{f|_{x_n=c_2}}^{z',a_2}\right) = 0.$$

Предпоследнее равенство следует из того, что система уравнений $\begin{cases} a + c_1z_n = a_1; \\ a + c_2z_n = a_2. \end{cases}$ имеет одно решение относительно переменных a и z_n. Последнее равенство следует из утверждения 122(2). □

Утверждение 123. *1.* $\widehat{\xi^f}(z) = q^{n/2}\sum\limits_{a\in Q_q} \delta_f^{z,a}\xi^a$.

2. Если $\delta_f^{z,a} = 0$ *для всех* $a \in Q_q$, *то* $\widehat{\xi^f}(z) = 0$. *Обратное верно, если* q *простое.*

Доказательство. 1. Пусть $L_a = |\{x \in Q_q^n : f(x) - \langle x, z\rangle = a\}|$. Выразим $\widehat{\xi^f}(z)$ и $\delta_f^{z,a}$ в терминах L_a.

$$\widehat{\xi^f}(z) = \frac{1}{q^{n/2}}\sum_{x\in Q_q^n} \xi^{f(x)-\langle x,z\rangle} = \frac{1}{q^{n/2}}\sum_{a\in Q_q} L_a\xi^a. \tag{28}$$

$$\delta_f^{z,a} = \frac{q-1}{q} - \frac{q^n - L_a}{q^n} = \frac{L_a}{q^n} - \frac{1}{q}.$$

Тогда из равенства $\sum_{a \in Q_q} \xi^a = 0$ мы имеем

$$\widehat{\xi^f}(z) = \frac{1}{q^{n/2}} \sum_{a \in Q_q} (q^n \delta_f^{z,a} + q^{n-1}) \xi^a = q^{n/2} \sum_{a \in Q_q} \delta_f^{z,a} \xi^a.$$

2. Используя равенство (28) и утверждение 114, мы заключаем, что если q — простое и $\widehat{\xi^f}(z) = 0$, то $L_a = q^{n-1}$ для любого $a \in Q_q$. Следовательно, $\delta_f^{z,a} = 0$ для любого $a \in Q_q$. Нетрудно видеть, что обратное тоже верно. □

Теорема 47 (Рябов, [86]). *1. Для любой функции $f : Q_q^n \to Q_q$ верно неравенство $nl(f) \le (q-1)q^{n-1} - q^{\frac{n}{2}-1}$.*
2. Если $nl(f) = (q-1)q^{n-1} - q^{\frac{n}{2}-1}$, то f — слабо регулярная бент-функция и n чётно.

Доказательство. Чтобы максимизировать $nl(f)$ нужно решить следующую оптимизационную проблему:
$\sum_{z \in Q_q^n, a \in Q_q} (\delta_f^{z,a})^2 = \frac{q-1}{q}$,
$\sum_{a \in Q_q} \delta_f^{z,a} = 0$ для всех $z \in Q_q^n$,
$\max_{z \in Q_q^n, a \in Q_p} \delta_f^{z,a} \to \min$.

Рассмотрим следующую вспомогательную задачу: $\sum_{a \in Q_q} \sigma_a = 0$, $\sum_{a \in Q_q} \sigma_a^2 = A\frac{q-1}{q}$ and $\max_a \sigma_a \to \min$. Нетрудно видеть, что единственным с точностью до перестановки решением вспомогательной задачи является$\sigma_0 = -\frac{q-1}{q}\sqrt{A}$, $\sigma_a = \frac{\sqrt{A}}{q}$ as $a \neq 0$.

Значение $\max_a \sigma_a$ возрастает, если A возрастает. Тогда оптимальному решению исходной проблемы соответствует случай, когда все суммы $\sum_{a \in F_p} (\delta_f^{z,a})^2$ равны. Возьмём $A = \frac{1}{q^n}$. Тогда получаем, что $\min_f(\max_{z \in Q_q^n, a \in Q_q} \delta_f^{z,a}) \ge \frac{1}{q^{\frac{n}{2}+1}}$. Равенство (27) доказывает п.1.

2. Из доказательства п.1 мы видим, что равенство $nl(f) = (q-1)q^n - q^{\frac{n}{2}-1}$ достигается только в случае, когда $\delta_f^{z,a}$ принимает два значения. Кроме того, $\delta_f^{z,a}$ принимает значение $-\frac{q-1}{q^{\frac{n}{2}+1}}$ один раз и $q-1$ раз значение $\frac{1}{q^{\frac{n}{2}+1}}$ для любого $z \in Q_q^n$. Из утверждений 114 и 123 следует, что при любом $z \in Q_q^n$ $\widehat{\xi^f}(z) = -\xi^a$ для некоторого $a \in Q_q$. Тогда f — слабо регулярная бент-функция. Поскольку число $nl(f)$ целое, n должно быть чётным. □

14.4 Разностные множества

Пусть K — конечная абелева группа.

Определение 65. *Множество $D \subseteq K$ называется разностным с параметрами (v, k, λ), если $|K| = v$, $|D| = k$ и для любого ненулевого $a \in K$ существует ровно λ пар элементов $d_1, d_2 \in D$ таких, что $d_1 - d_2 = a$.*

Утверждение 124. *Множество $D \subseteq K$ является разностным с параметрами (v, k, λ), если и только если $\chi_D * \chi_{-D} = \lambda \cdot \mathbf{1} + (k - \lambda)\delta / v^{1/2}$.*

Доказательство. Вычислим свёртку $\sum\limits_{x \in K} \chi_D(x) \cdot \chi_D(-(y - x))$. Пусть $y \neq 0$. По определению в разностном множестве имеется ровно λ таких элементов $x \in D$, что x и $(x - y)$ одновременно принадлежат разностному множеству, так как $y = x - (x - y)$. Значение свёртки в нуле равно $\sum\limits_{x \in K} \chi_D(x) \cdot \chi_D(x) = |D|$. □

Следствие 50 ([71])**.** *Пусть b — булева бент-функция и $\widehat{(-1)^b}(\bar{0}) = 1$. Рассмотрим $B = \{x \in \{0,1\}^n \mid b(x) = 1\}$, $b = \chi_B$. Тогда B есть разностное множество с параметрами $(2^n, 2^{n-1} - 2^{n/2-1}, 2^{n-2} - 2^{n/2-1})$. Верно и обратное: если B разностное множество с указанными параметрами, то χ_B — бент-функция.*

Доказательство. Имеем $|K| = 2^n$ по условию и $|B| = \frac{1}{2}(2^n - 2^{n/2})$ по утверждению 117. Аналогично доказательству утверждения 117 имеем равенства $b * b = \frac{1}{4}(\mathbf{1} - (-1)^b) * (\mathbf{1} - (-1)^b) = \frac{1}{4}(2^n \mathbf{1} + 2^{n/2}\delta - 2 \cdot 2^{n/2}\mathbf{1}) = (2^{n-2} - 2^{n/2-1})\mathbf{1} + 2^{n/2-2}\delta$. Здесь мы воспользовались линейностью свёртки и основным свойством бент-функции (утверждение 112). Из утверждения 124 находим параметры разностного множества λ и k. Аналогичным образом, опираясь на утверждение 112), нетрудно доказать обратное. □

Замечание 20. Если b — булева бент-функция и $\widehat{(-1)^b}(\bar{0}) = -1$, то аналогично можно показать, что её носитель есть разностное множество с параметрами $(2^n, 2^{n-1} + 2^{n/2-1}, 2^{n-2} + 2^{n/2-1})$. Эти и такие как в следствии 50 параметры разностного множества называются параметрами МакФарланда.

Ниже будет показано, что любое разностное множество с параметрами МакФарланда можно преобразовать в матрицу Адамара.

Докажем, что из любого разностного множества можно получить ортогональную матрицу с коэффициентами, принимающими всего два значения $a, b \in \mathbb{R}$. Пусть имеется разностное множество D с параметрами (v, k, λ). Рассмотрим характеристические функции $f_1(x) = \chi_D(x - d_1)$ и $f_2(x) = \chi_D(x - d_2)$ для произвольных $d_1, d_2 \in K$. Из определения разностного множества следует, что функции f_1 и f_2 одновременно равны

1 ровно в λ точках. В силу симметрии они различны в $2(k-\lambda)$ точках и одновременно равны 0 в оставшихся $v-\lambda-2(k-\lambda)$ точках. Пусть a и b удовлетворяют уравнению

$$\lambda a^2 + 2(k-\lambda)ab + (v-\lambda-2(k-\lambda))b^2 = 0.$$

Нетрудно видеть, что ортогональность функций $g_{d_1} = af_1 + b(\mathbf{1} - f_1)$ и $g_{d_2} = af_2 + b(\mathbf{1} - f_2)$ эквивалентна этому равенству. Из определения разностного множества следует, что для любых различных d_1 и d_2 функции g_{d_1} и g_{d_2} ортогональны. Покажем, что $a = 1$ и $b = -1$ для разностных множеств с параметрами МакФарланда. Действительно,

$$\lambda - 2(k-\lambda) + (v-\lambda-2(k-\lambda)) = v - 4(k-\lambda) = 2^n - 4\cdot 2^{n-2} = 0.$$

Запишем вектора значений функций g_d, $d \in K$, в строки матрицы T. Матрица T размера $v \times v$ является ортогональной с точностью до скалярного множителя, так как нормы строк одинаковы. В случае параметров МакФарланда элементы матрицы T принимают значения ± 1. Поэтому матрица T является матрицей Адамара. Это означает, что $(-1)^{\chi_D} * (-1)^{\chi_D}(x) = 0$ при $x \neq \overline{0}$. Тогда из утверждения 116 (или из утверждения 115) имеем

Следствие 51 ([71]). *Пусть B есть разностное множество с параметрами $(2^n, 2^{n-1} \pm 2^{n/2-1}, 2^{n-2} \pm 2^{n/2-1})$. Тогда $b = \chi_B$ — булева бент-функция.*

Из ортогональности матрицы T следует, что пара (a,a) (а также пары (b,a), (a,b) или (b,b)) встречается в любой паре строк (или столбцов) матрицы T одинаковое число раз. По построению $T(x,y) = a\chi_D(x-y) + b(\mathbf{1} - \chi_D)(x-y)$. Заменим в матрице T элементы a на 1 и b на 0, т. е. рассмотрим матрицу $Q_D(x,y) = \chi_D(x-y)$. Теперь каждая из пар $(1,1)$, $(0,1)$, $(1,0)$, $(0,0)$ встречается в любой паре столбцов (строк) одинаковое число раз. Если рассматривать строки матрицы Q_D как характеристические вектора k-блоков v-элементного множества, то мы получим дизайн с параметрами 2-(v,k,λ) мощности v. Дизайны с такими параметрами называют симметричными 2-дизайнами.

Разностное множество $D \subseteq K$ с параметрами $(v,k,1)$ порождает конечную проективную плоскость. Рассмотрим в качестве точек плоскости элементы группы K, а в качестве прямых — смежные классы $D+a$, $a \in G$. Покажем, что произвольные прямые $D+a_1$ и $D+a_2$ пересекаются по одной точке. Действительно, из определения разностного множества следует, что имеется единственная пара $d_1, d_2 \in D$, для которой $a_1 - a_2 = d_2 - d_1$, т. е. $a_1 + d_1 = a_2 + d_2$. Покажем, что для двух произвольных точек $a_1, a_2 \in K$ найдётся прямая $D+b$, которой они принадлежат. Пусть $a_2 - a_1 = d_2 - d_1$ и $b = a_1 - d_1$. Тогда $a_1 \in D+b$ и $a_2 = d_2 + b \in D+b$.

Определение 66. *Частично разностным множеством с параметрами* (v, k, λ, μ) *называется множество* $D \subseteq K$, *если* $|K| = v$, $|D| = k$ *и для любого ненулевого* $a \in D$ *существует ровно* λ *пар элементов* $d_1, d_2 \in D$ *таких, что* $d_1 - d_2 = a$, *а для любого ненулевого* $a \in K \setminus D$ *существует ровно* μ *пар элементов* $d_1, d_2 \in D$ *таких, что* $d_1 - d_2 = a$.

Аналогично утверждению 124 нетрудно доказать, что определение частично разностного множества эквивалентно равенству

$$\chi_D * \chi_{-D} = \lambda \cdot \chi_D + \mu \cdot (\mathbf{1} - \chi_D) + \frac{k-\mu}{v^{1/2}}\delta. \tag{29}$$

Другими словами, если свёрточный квадрат характеристической функции множества есть линейная комбинация характеристической функции множества, постоянной функции и δ-функции, то это множество является частично разностным, параметры которого μ, λ, k определяются из коэффициентов этой линейной комбинации. В дальнейшем будем дополнительно полагать, что $D = -D$ и $0 \notin D$.

Применив к равенству (29) преобразование Фурье, получаем следующее квадратное уравнение для функции $f = \widehat{\chi_D}$

$$f \cdot f = \lambda \cdot f + \mu \cdot (\delta - f) + \frac{k-\mu}{v^{1/2}}\mathbf{1}.$$

Рассматривая это равенство для каждого фиксированного аргумента, заключаем, что функция f может принимать только значения $\frac{\lambda-\mu\pm\Delta}{2}$, где $\Delta = \sqrt{(\lambda-\mu)^2 + 4(k-\mu)/v^{1/2}}$ на ненулевых элементах группы K и $f(0) = k/v^{1/2}$.

Пусть $D^+ = \{x \in K \mid f(x) = \frac{\lambda-\mu+\Delta}{2}\}$.

Утверждение 125 (Дельсарт [69])**.** D^+ *является частично разностным множеством.*

Доказательство. Достаточно проверить выполнение равенства (29) для множества D^+ и некоторых k', λ' и μ'. Нетрудно видеть, что $D^+ = -D^+$, поскольку $D = -D$ и, следовательно, $f(x) = f(-x)$. Из равенства $\widehat{\widehat{f(x)}} = f(-x)$ имеем $\widehat{f} = \chi_D$. Отсюда получаем равенство $\widehat{f} \cdot \widehat{f} = \widehat{f}$ и, применяя преобразование Фурье (утверждение 89) получаем, что $f * f = v^{1/2} f$. По определению множества D^+ справедливо равенство $f = \alpha_1 \chi_{D^+} + \alpha_2 \mathbf{1} + \alpha_3 \delta$ для некоторых коэффициентах $\alpha_1, \alpha_2, \alpha_3$. Подставляя это представление функции f в равенство $f * f = v^{1/2} f$ и учитывая равенства $\chi_{D^+} * \delta = v^{1/2}\chi_{D^+}$ и $\chi_{D^+} * \mathbf{1} = |D^+|\mathbf{1}$, получаем, что свёртка $\chi_{D^+} * \chi_{D^+}$ представима в виде требуемой линейной комбинации. Таким образом, найдутся некоторые коэффициенты μ', λ', k', для которых верно равенство

$$\chi_{D^+} * \chi_{D^+} = \lambda' \cdot \chi_{D^+} + \mu' \cdot (\mathbf{1} - \chi_{D^+}) + \frac{k'-\mu'}{v^{1/2}}\delta.$$

□

14.5 Разностные множества и сильно регулярные графы как совершенные раскраски

Рассмотрим граф Кэли группы K с множеством образующих D, $D = -D$ и $0 \notin D$. Из определения частично разностного множества с параметрами (v, k, λ, μ) следует, что граф $Cay(K, D)$ является сильно регулярным с параметрами (v, k, λ, μ). Действительно, пусть вершины $x, y \in K$ смежны в графе $Cay(K, D)$, т. е. $x + a = y$ и $a \in D$. Тогда по определению частично разностного множества найдутся λ таких пар $d_1, d_2 \in D$, что $a = d_1 - d_2$. Следовательно, найдутся λ вершин $x + d_1 = y + d_2$, которые смежны с вершинами x и y в графе $Cay(K, D)$. Аналогично можно рассмотреть случай когда вершины $x, y \in K$ несмежны. Нетрудно видеть, что верно и обратное: из сильной регулярности графа $Cay(K, D)$ следует, что D — частично разностное множество в группе K.

Как показано в предыдущем разделе, любому разностному множеству D с параметрами (v, k, λ) соответствует симметричный 2-(v, k, λ) дизайн. Если $D = -D$ и $0 \notin D$, то матрица $Q_D(x, y) = \chi_D(x - y)$ является матрицей смежности графа $Cay(K, D)$. Более того, из определений сразу следует, что строки матрицы смежности сильно регулярного графа с параметрами (v, k, λ, λ) образуют симметричный 2-(v, k, λ) дизайн. Верно и обратное: если матрица, строки которой являются характеристическими векторами k-блоков симметричного 2-(v, k, λ) дизайна, симметрична и имеет нули по главной диагонали, то она является матрицей смежности некоторого сильно регулярного графа с параметрами (v, k, λ, λ).

Покажем, что любой сильно регулярный граф можно рассматривать как совершенную раскраску некоторого гиперграфа.

Рассмотрим полный граф K_n. Вершинами гиперграфа Γ_n будем считать все рёбра графа K_n, а его рёбрами — тройки рёбер, составляющие треугольники. Рассмотрим сильно регулярный граф G на тех же n вершинах. Определим раскраску вершин гиперграфа Γ_n следующим образом: $f(e) = 1$, если $e \in E(G)$, и $f(e) = 0$, если $e \notin E(G)$. По определению совершенной раскраски гиперграфа достаточно удостоверится, что для любых двух вершин u и v в графе G, число вершин смежных только с u, смежных только с v, смежных с u и v, а также и несмежных ни с u, ни с v зависит только от того смежны ли вершины u и v. Это условие совпадает с определением сильно регулярного графа. В частности, для сильно регулярного графа с параметрами (n, k, λ, μ) имеем: если вершина u смежна с v, то число вершин смежных с ними двумя равно λ, смежных только с первой или второй из них равно $k - \lambda$, несмежных ни с одной из них равно $n - 2 - 2k + \lambda$.

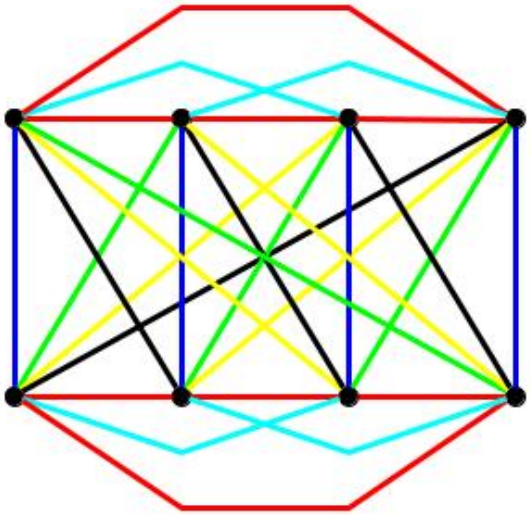
Наоборот, рёбра цвета 1 совершенной 2-раскраски гиперграфа Γ_n порождают сильно регулярный граф, несвязный граф или граф-звезду. Отсутствие взаимной однозначности между совершенными 2-раскрасками

гиперграфа Γ_n и сильно регулярными графами возникает из-за того, что в определении совершенной раскраски гиперграфа не важен порядок вершин в гиперребре.

Рассмотрим ассоциативную схему $\{R_0, R_1, \ldots, R_m\}$ на множестве X из n элементов, здесь R_0 — отношение, содержащее пары вида (x, x). Если ассоциативная схема симметрична, т. е. из $(x, y) \in R_i$ следует $(y, x) \in R_i$ для любого $i \in \{1, \ldots, m\}$, то ассоциативная схема определяет совершенную раскраску графа Γ_n в цвета $\{R_1, \ldots, R_m\}$. Действительно, вершинами графа Γ_n являются пары элементов из X, гиперрёбрами — тройки из пар, образующие треугольник, а условие для совершенной раскраски гиперграфа Γ_n совпадает с пунктом (3) в определении ассоциативной схемы: если $(x, y) \in R_k$, то число таких $z \in X$, что $(x, z) \in R_i$ и $(z, y) \in R_j$, зависит только от i, j, k.

Несмотря на близость определений симметричной ассоциативной схемы и совершенной раскраски графа Γ_n, они не совпадают.

Пример 45. Рассмотрим гиперграф Γ_8 и следующую раскраску его вершин (рёбер графа K_8):



Нетрудно видеть, что раскраска на рисунке выше является совершенной для гиперграфа Γ_8, в котором мы считаем, что две вершины смежны, если соответствующие им рёбра графа K_8 лежат в одном треугольнике. В то же время, эта совершенная раскраска не задаёт ассоциативную схему, так как для рёбер графа K_8 красного цвета правый и левый концы не эквивалентны. А именно, из одного конца красного ребра выходит синее ребро, которое замыкается в треугольник чёрным ребром, а из другого — зелёным ребром. В симметричной ассоциативной схеме концы рёбер должны быть эквивалентными.

14.6 Бент-функции как совершенные раскраски

Далее подробнее рассмотрим абелеву группу $\mathbb{Z}_2^n$. Обозначим через Δ_n 3-униформный гиперграф, вершинами которого являются все элементы группы $\mathbb{Z}_2^n$ кроме 0, и тройка вершин $\{a_1, a_2, a_3\}$ составляет гиперребро если $a_1 + a_2 + a_3 = 0$. Заметим, что равенство $a_1 + a_2 + a_3 = 0$ подразумевает, что все элементы $a_i \neq 0$, $i = 1, 2, 3$ различны. Если D является частично разностным множеством в $\mathbb{Z}_2^n$ с параметрами (v, k, λ, μ), то раскраска χ_D гиперграфа Δ_n является совершенной. Действительно, равенство $a_1 + a_2 + a_3 = 0$ эквивалентно равенству $a_1 = a_2 - a_3$ в $\mathbb{Z}_2^n$. Тогда каждая вершина $a_1 \in D$ содержится в λ гиперрёбрах, состоящих только из элементов множества D, и каждая вершина $a_1 \notin D$ содержится в μ гиперрёбрах, в которых имеется два элемента из множества D. Поскольку каждая пара $a, b \in \mathbb{Z}_2^n \setminus \{0\}$ принадлежит ровно одному гиперребру, можно вычислить число гиперрёбер любого цветового состава, содержащих вершину $a \in D$ или вершину $a \notin D$. Это число зависит только от цвета самой вершины. Следовательно, раскраска χ_D является совершенной по определению. Верно также и обратное утверждение. Пусть D — множество вершин цвета 1. Достаточно заметить, что параметр λ частично разностного множества оказывается равен числу гиперрёбер цветового состава $(1, 1, 1)$, содержащих фиксированную вершину цвета 1, а параметр μ — равен числу гиперрёбер цветового состава $(0, 1, 1)$, содержащих фиксированную вершину цвета 0.

Тогда из утверждения 50 следует

Утверждение 126. *Булевы бент-функции взаимно однозначно соответствуют 2-раскраскам гиперграфа Δ_n с соответствующей матрицей параметров.*

По утверждению 43, совершенная раскраска гиперграфа Δ_n порождает совершенную раскраску его рёберного графа $\mathcal{E}(\Delta_n)$. Поскольку пересечения двух гиперрёбер из Δ_n содержат не более одной вершины, $\mathcal{E}(\Delta_n)$ — простой граф. Заметим, что 2-раскраска χ_D гиперграфа Δ_n порождает 4-раскраску графа $\mathcal{E}(\Delta_n)$, поскольку каждое гиперребро гиперграфа Δ_n состоит из трёх вершин и может содержать 0, 1, 2 or 3 вершин первого цвета. Рассмотрим элементы группы $\mathbb{Z}_2^n$ как элементы векторного пространства $(GF(2))^n$. Гиперребро в Δ_n соответствует 2-мерному подпространству в $(GF(2))^n$. Кроме того, два гиперребра в Δ_n имеют общую вершину тогда и только тогда, когда соответствующие им 2-мерные подпространства пересекаются по 1-мерному подпространству. Граф $\mathcal{E}(\Delta_n)$ является частным случаем графа Грассмана.

Определение 67. *Графом Грассмана $J_q(n, k)$ называется граф, вершинами которого являются k-мерные подпространства векторного пространства $(GF(q))^n$. Две вершины смежны, если соответствующие*

им подпространства пересекаются по $(k-1)$*-мерному подпространству.*

Графы Грассмана являются дистанционно-регулярными (см. [14]).

Рассмотрим граф $J_2(n,2)$, вершинами которого являются 2-мерные подпространства. Пусть $f: Q_2^n \to Q_2$ — булева функция, будем полагать что $f(\bar{0})=1$. Каждое 2-мерное подпространство в $(GF(2))^n$ состоит из 4х элементов булева гиперкуба. Функция f порождает раскраску вершин графа $J_2(n,2)$ в 4 цвета по количеству единиц функции в подпространстве. В этом смысле, любая булева функция есть раскраска графа $J_2(n,2)$.

Теорема 48 ([128]). *Функция* $b: Q_2^n \to Q_2$, $\widehat{(-1)^b}(\bar{0})=1$, $b(\bar{0})=1$, *является бент-функцией тогда и только тогда, когда она является совершенной раскраской графа* $J_2(n,2)$ *с матрицей параметров*

$$\begin{pmatrix} 3(2^{n-3}-2^{(n/2)-2}-1) & 3\cdot 2^{n-2}-3 & 3(2^{n-3}+2^{(n/2)-2}) & 0 \\ 2^{n-2}-2^{(n/2)-1} & 5\cdot 2^{n-3}-2^{(n/2)-2}-5 & 2^{n-1}+2^{(n/2)-1} & 2^{n-3}+2^{(n/2)-2}-1 \\ 2^{n-3}-2^{(n/2)-2} & 2^{n-1}-2^{(n/2)-1}-1 & 5\cdot 2^{n-3}+2^{(n/2)-2}-3 & 2^{n-2}+2^{(n/2)-1}-2 \\ 0 & 3(2^{n-3}-2^{(n/2)-2}) & 3\cdot 2^{n-2} & 3(2^{n-3}+2^{(n/2)-2}-2) \end{pmatrix}.$$

Доказательство. Получим совершенную раскраску из бент-функции. По утверждению 117 имеем $|\mathrm{supp}(b)| = \frac{1}{2}(2^n \pm 2^{n/2})$. Точнее $|\mathrm{supp}(b)| = \frac{1}{2}(2^n + 2^{n/2})$ из условия $\widehat{(-1)^b}(0)=1$. Из определения бент-функции следует, что $|\{x \in Q_2^n : b(x) \oplus b(x+y)=0\}| = |\{x \in Q_2^n : b(x) \oplus b(x+y)=1\}|$ при $y \neq \bar{0}$.

Рассмотрим подпространства, которые пересекаются по $\{\bar{0}, y\}$. Обозначим через $A_{\alpha\beta}$ число пар значений (α,β) среди $(b(x), b(x+y))$, $x \in (GF(2))^n$. Тогда имеем равенства $A_{01}+A_{10}=A_{00}+A_{11}$. Кроме того, $A_{01}+A_{10}+A_{00}+A_{11}=2^n$, $A_{01}=A_{10}$ из симметрии и $A_{10}+A_{11}=|\mathrm{supp}(b)|$, поскольку $b(\bar{0})=1$. Отсюда легко вычислить, что $A_{01}=A_{10}=2^{n-2}$, $A_{11}=2^{n-2}+2^{(n/2)-1}$ и $A_{00}=2^{n-2}-2^{(n/2)-1}$. Следовательно, если известен цветовой состав подпространства, то известен цветовой состав смежных с ним в графе $J_2(n,2)$ подпространств. Например, подпространство 4-го цвета не видит подпространств 1-го цвета; видит $3A_{00}/2$ подпространств 2-го цвета, поскольку каждая пара вершин $(x, x+y)$, где $(b(x), b(x+y)) = (0,0)$, учитывается дважды $(x, x+y)$ и $(x+y, x)$; видит $(3A_{11}-12)/2$ подпространств 4-го цвета, поскольку содержит четыре элемента (включая $\bar{0}$), на которых функция b принимает значение 1, и при фиксации каждой из трёх ненулевых вершин имеем $(A_{11}-4)/2$ смежных подпространства 4-го цвета. Тогда имеем совершенную раскраску с матрицей параметров $\frac{1}{2}\begin{pmatrix} 3A_{00}-6 & 6A_{01}-6 & 3A_{11} & 0 \\ 2A_{00} & 4A_{01}+A_{00}-10 & 2A_{01}+2A_{11} & A_{11}-2 \\ A_{00} & 2A_{01}+2A_{00}-2 & 4A_{10}+A_{11}-6 & 2A_{11}-4 \\ 0 & 3A_{00} & 6A_{01} & 3A_{11}-12 \end{pmatrix}$.

Предположим имеется раскраска графа $J_2(n,2)$ с указанными параметрами. Определим функцию b следующим образом: $b(\bar{0}) = 1$ и во всех вершинах $x \in (GF(2))^n$, входящих в подпространства 4-го цвета, определим $b(x) = 1$. В остальных вершинах определим $b(x) = 0$. Покажем, что так полученная функция b является бент-функцией.

Для каждой вершины $x \in B = \{x \neq \bar{0} : b(x) = 1\}$ обозначим через $M(x)$ число подпространств 4-го цвета, в которые входит эта вершина. Из параметров раскраски (4-й столбец, 1-я строка) следует, что никакая вершина $x \in B$ не содержится в подпространстве 1-го цвета. Кроме того, все три ненулевые вершины подпространства содержатся в B тогда и только тогда, когда это подпространство 4-го цвета, поскольку такое подпространство не может быть смежно с подпространством 1-го цвета, а подпространства других цветов должны быть смежны с подпространствами 1-го цвета. Из параметров раскраски (4-й столбец, 4-я строка) следует, что среднее для чисел $M(x)$ по вершинам $x \in B$ из любого фиксированного подпространства 4-го цвета равно $\frac{A_{11}}{2} - 1$. Предположим найдутся такие x, что $M(x) \neq \frac{A_{11}}{2} - 1$. Выберем такую вершину $x \in B$, что разность $|M(x) - (\frac{A_{11}}{2} - 1)|$ максимальна.

Пусть для этой вершины $M(x) > \frac{A_{11}}{2} - 1$ и отклонение от среднего значения величины $M(x)$ строго максимально. Покажем, что имеется как минимум ещё одна вершина $z \in B$, для которой $M(z) \geq A_{11}/2$. Рассмотрим произвольное подпространство 4-го цвета, содержащее вершину x. Для обеих вершин $z \neq x$ и $x + z$ из этого подпространства имеем $M(z) < \frac{A_{11}}{2} - 1$ и $M(x+z) < \frac{A_{11}}{2} - 1$, поскольку среднее значение величин $M(y)$ по любому подпространству 4-го цвета одинаково и отклонение $M(x)$ от $\frac{A_{11}}{2} - 1$ строго максимально по предположению. Если $M(z) > 1$ (или $M(x+z) > 1$), то имеются как минимум два разных подпространства 4-го цвета, которые содержат z (или $z+x$). И в каждом из них есть вершина $y \in B$ с $M(y) \geq A_{11}/2$. Рассмотрим оставшийся случай $M(z) = M(z+x) = 1$. В этом случае вершина x содержится во всех соседних с подпространством $\{\bar{0}, x, z, x+z\}$ подпространствах 4-го цвета, т. е. $M(x) = \frac{3A_{11}}{2} - 6$. Тогда все подпространства, содержащие x, видят не меньше чем $\frac{3A_{11}}{2} - 6$ подпространств 4-го цвета. Значит из параметров раскраски (см. 4-й столбец) следует, что они являются подпространствами 4-го цвета. Это противоречит наличию в раскраске подпространств 1-го цвета. Поскольку любое подпространство смежно с некоторым подпространством, содержащим вершину x, а подпространства 1-го цвета не смежны с подпространствами 4-го цвета.

Мы показали, найдётся $y \neq x$ такая, что $M(y) \geq A_{11}/2$. Рассмотрим подпространство, содержащее вершины x и y. Оно смежно с $M(x) + M(y) + M(x+y) - 3$ либо с $M(x) + M(y)$ подпространствами 4-го цвета, в зависимости от того $x + y \in B$ или $x + y \notin B$, но в любом из этих случаев количество смежных подпространств 4-го цвета не соответствует

параметрам исходной раскраски. Пришли к противоречию.

Теперь предположим, что разность $|M(x) - (\frac{A_{11}}{2} - 1)|$ максимальна (возможно нестрого) для некоторой вершины $x \in B$ такой, что $M(x) < \frac{A_{11}}{2} - 1$. Рассмотрим произвольное подпространство 4-го цвета, содержащее вершину x. В каждом таком подпространстве имеется вершина $z \in B$, для которой $M(z) > \frac{A_{11}}{2} - 1$, поскольку среднее значение по любому подпространству 4-го цвета одинаково. Рассмотрев подпространства 4-го цвета, содержащие z мы найдём $M(z)$ различных вершин $y, y', \ldots \in B$, для которых $M(y) < \frac{A_{11}}{2} - 1$ и $M(y') < \frac{A_{11}}{2} - 1$. Рассмотрим подпространство $\Omega = \{\bar{0}, x, y, x+y\}$. Оно смежно с $M(x)+M(y)+M(x+y)-3$ либо с $M(x)+M(y)$ подпространствами 4-го цвета, в зависимости от того $x + y \in B$ или $x + y \notin B$. Покажем, что в любом из этих случаев количество смежных подпространств 4-го цвета не соответствует ни 4-му, ни 3-му, ни 1-му цвету в матрице параметров исходной раскраски. Для 4-го цвета подпространство Ω имеет слишком мало смежных подпространств 4-го цвета. В случае 3-го цвета должны быть смежные подпространства 1-го цвета, поэтому $x + y \notin B$, но тогда имеется только $M(x) + M(y)$ смежных подпространств 4-го цвета, т. е. меньше чем соответствующее значение в матрице параметров. Подпространство Ω не может иметь 1-й цвет, поскольку оно смежно с подпространствами 4-го цвета.

Итак, мы получили, что Ω имеет 2-й цвет и, следовательно, A_{00} смежных подпространств 1-го цвета, которые содержат вершину $x + y$. Они не могут содержать вершины x или y, поскольку это противоречило бы несмежности подпространств 1-го и 4-го цвета. Рассмотрим подпространство $\Omega' = \{\bar{0}, x, y', x+y'\}$. Аналогичным образом, получим, что имеется A_{00} подпространств 1-го цвета, которые содержат вершину $x + y'$. Тогда рассмотрим подпространство $\{\bar{0}, x + y, x + y', y + y'\}$. Оно смежно не менее чем с $2A_{00} - 1$ подпространствами 1-го цвета. Из матрицы параметров следует, что таких подпространств не существует. Пришли к противоречию.

Мы доказали, что $M(x) = \frac{A_{11}}{2} - 1$ для любого $x \in B$. Тогда из 4-го столбца матрицы параметров получаем, что в подпространстве i-го цвета содержится $i - 1$ вершина из множества B. Следовательно, функция b является совершенной раскраской гиперграфа Γ_{2^n-1}, рёбрами которого являются тройки ненулевых вершин, входящих в подпространство. Как было замечено выше, эта совершенная раскраска является характеристической функцией частично разностного множества, а в данном случае бент-функцией по следствию 51. □

Нетрудно видеть, что разностное множество с параметрами МакФарланда определяет совершенную раскраску графа $J_2(n, 2)$ с параметрами из теоремы 48. Тогда имеем

Следствие 52. *Характеристическая функция разностного множества с параметрами* $(2^n, 2^{n-1}-2^{n/2-1}, 2^{n-2}-2^{n/2-1})$ *является бент-функцией.*

Нетрудно убедиться, что объединив попарно чётные и нечётные цвета в построенной выше совершенной раскраске графа $J_2(n,2)$, мы получим совершенную раскраску с параметрами $\begin{pmatrix} 3\cdot 2^{n-2}-3 & 3\cdot 2^{n-2}-3 \\ 3\cdot 2^{n-2} & 3\cdot 2^{n-2}-6 \end{pmatrix}$.

Однако, по совершенной 2-раскраске с такими параметрами нельзя восстановить бент-функцию, поскольку добавление аффинной функции не приводит к изменению раскраски.

14.7 Спреды

Пусть $q = p^k$ — степень простого числа. Рассмотрим Q_q^n как векторное пространство на конечным полем $GF(q)$.

Определение 68. *Спредом (spread), точнее k-спредом, в векторном пространстве Q_q^n называется набор линейных подпространств фиксированной размерности k, который однократно покрывает все вектора за исключением нуль-вектора.*

Нетрудно видеть, что определение k-спреда эквивалентно определению 1-фактора в гиперграфе, вершинами которого являются наборы из Q_q^n, а гиперрёбрами — все k-мерные подпространства. В графе Грассмана $J_q(n,k)$ k-мерные подпространства соответствуют вершинам. Нетрудно видеть, что расстояние между двумя k-мерными подпространствами в графе $J_q(n,k)$ равно k минус размерность их пересечения. Поэтому спреды эквиваленты кодам в графах Грассмана с максимально возможным кодовым расстоянием k в $J_q(n,k)$ и максимально возможным для такого расстояния числом вершин $c = \frac{q^n-1}{q^k-1}$. Ясно, что спреды могут существовать только когда число c — целое.

Утверждение 127. *Если $n = kt$, то в Q_q^n имеется k-спред.*

Доказательство. Рассмотрим множество Q_q^n как t-мерное векторное пространство над полем $GF(q^k)$. Пусть A_v — 1-мерное линейное подпространство, содержащее вектор $v \in (GF(q^k))^t$, т. е. множество векторов коллинеарных вектору v и нуль-вектор. Тогда $\{A_v : v \in (GF(q^k))^t\}$ является 1-спредом в $Q_{q^k}^t$.

Ясно, что каждый элемент поля $GF(q^k)$ можно рассматривать как вектор размерности k над полем $GF(q)$. Поэтому вектору $v \in (GF(q^k))^t$ соответствует матрица размера $k \times t$ из элементов поля $GF(q)$. Множество матриц, соответствующих векторам из A_v (при фиксированном v), замкнуто относительно операции сложения на $GF(q)$, поскольку сложение в $GF(q^k)$ — это сложение соответствующих векторов, и относительно операции умножения на скаляр из $GF(q)$, поскольку умножение вектора из $(GF(q))^k$ на скаляр из $GF(q)$ соответсвует умножения элемента

$GF(q^k)$ на элемент подполя $GF(q)$. Следовательно, множество A_v порождает подпространство в $Q_q^n \simeq (GF(q))^{kt}$. Размерность этого подпространства равна k, поскольку $|A_v| = q^k$. По построению, множества A_v и A_u либо совпадают (если v и u коллинеарны), либо пересекаются только по нуль-вектору. Таким образом, требуемый k-спред в Q_q^n построен. $\square$

Определение 69. *Частичным спредом называется набор пересекающихся только по нуль-вектору линейных подпространств фиксированной размерности.*

Утверждение 128 (Диллон, см. [71]). *Пусть $\{V_i : i = 1, \ldots, 2^{n-1}\}$ — частичный n-спред в Q_2^{2n}. Тогда характеристическая функция b множества $B = \cup_{i=1}^{2^{n-1}} \setminus \{\bar{0}\}$ является бент-функцией.*

Доказательство.

$$(-1)^b = 2b - \mathbf{1} = 2\left(\sum_{i=1}^{2^{n-1}} \chi_{V_i} - \delta/2\right) - \mathbf{1},$$

$$\widehat{(-1)^b} = 2\sum_{i=1}^{2^{n-1}} \widehat{\chi_{V_i}} - \widehat{\delta} - \widehat{\mathbf{1}} = 2\sum_{i=1}^{2^{n-1}} \chi_{V_i^\perp} - \mathbf{1} - \delta,$$

поскольку $\widehat{\chi_V} = \frac{|V|}{2^n}\chi_{V^\perp} = \chi_{V^\perp}$ для любого линейного подпространства V размерности n (см. утверждение 42) и $\widehat{\delta} = \mathbf{1}$ (см. раздел 11.4). Для n-мерных подпространств в Q_2^{2n} из $V_i \cap V_j = \{\bar{0}\}$ следует, что и $V_i^\perp \cap V_j^\perp = \{\bar{0}\}$. Поэтому функция $\widehat{(-1)^b}$ принимает только два значения ± 1. Тогда b является бент-функцией по определению. $\square$

Задача 136. Докажите, что расстояние Хэмминга между двумя различными бент-функциями в n-мерном булевом кубе не может быть меньше, чем $2^{n/2}$.

Задача 137. Для произвольной булевой функции $f : Q_2^n \to Q_2$ определим энтропию $H(f)$ равенством $H(f) = -\sum\limits_{x \in Q_2^n} p(x)\log_2 p(x)$, где $p(x) = (\widehat{(-1)f}(x))^2/2^n$. Докажите, что при чётном n максимум энтропии равный $n2^n$ достигается только на бент-функциях.

Задача 138. Докажите, что сужение бент-функции на гиперграни является платовидной функцией.

Задача 139. Докажите, что не существует булевых функций от n переменных, достигающих границы Таранникова при $\mathrm{cor}(f) \le n/2$.

Задача 140. Пусть D — разностное множество с параметрами МакФарланда. Докажите, что ортогональный массив, состоящий из строк двух матриц Q_D и $Q_D \oplus 1$, имеет силу 2.

Задача 141. Докажите, что дополнение к разностному множеству также является разностным множеством.

Задача 142. Пусть M — матрица смежности сильно регулярного графа с параметрами $(v, k, \lambda, \lambda + 2)$. Докажите, что строки матрицы $M + I$ являются характеристическими векторами $(k+1)$-блоков симметричного 2-$(v, k + 1, \lambda + 2)$ дизайна.

Задача 143. Пусть D некоторый дизайн с параметрами 2-(v, k, λ) мощности v. Пусть строки матрицы Q_D являются характеристическими векторами блоков дизайна D. Докажите, что столбцы матрицы D являются характеристическими векторами блоков дизайна с теми же параметрами.

Задача 144. Докажите, что симметричные дизайны с параметрами 2-$(v, k, 1)$ эквивалентны конечным проективным плоскостям.

Задача 145. Докажите аналог утверждения 124 для частично разностных множеств.

Задача 146. Докажите, что характеристическая функция спреда в графе Грассмана $J_2(n, 2)$ является совершенной раскраской с матрицей параметров $\begin{pmatrix} 0 & 3 \cdot 2^{n-1} - 6 \\ 3 & 3 \cdot 2^{n-1} - 9 \end{pmatrix}$.

Задача 147. Пусть $\{V_i : i = 1, \ldots, 2^{n-1}+1\}$ — частичный n-спред в Q_2^{2n}. Докажите, что характеристическая функция множества $B = \cup_{i=1}^{2^{n-1}+1} V_i$ является бент-функцией.

Задача 148. Докажите, что с помощью конструкции Диллона (утверждение 128) можно построить не менее $\binom{a_n}{2^{n-1}}$, где $a_n = \frac{2^{2n}-1}{2^n-1}$, различных бент-функций в Q_2^{2n}.

Задача 149. Докажите, что с помощью конструкции Майораны—МакФарланда (утверждение 121) можно построить не менее $(2^n)!2^{2^n}$, различных бент-функций в Q_2^{2n}.

Задача 150. Пусть имеется разностное множество D с параметрами $(v, k, 1)$. Докажите, что матрица Z размера $v \times v$, строки которой являются характеристическими векторами множеств $a - D$, $a \in K$, не содержит подматриц размера 2×2, состоящих из 4х единиц.

Задача 151. Докажите, что любого простого p найдётся квадратная матрица размера $p(p + 1) + 1$, содержащая $(p + 1)(p(p + 1) + 1)$ единиц, которая не содержит подматриц размера 2×2, состоящих из 4х единиц.

Задача 152. Докажите, что для любого $p \geq 1$ квадратная матрица размера $p(p + 1) + 1$, содержащая более $(p + 1)(p(p + 1) + 1)$ единиц, содержит и подматрицу размера 2×2, состоящую из 4х единиц.

Задача 153. Докажите, что для любого $p \geq 1$ двудольный граф, содержащий в каждой доле по $p(p+1)+1$ вершин и R ребёр содержит цикл длины 4 когда $R > (p+1)(p(p+1)+1)$; а если $R = (p+1)(p(p+1)+1)$ и p — простое, то найдётся такой граф без циклов длины менее 6 (задача Заранкиевича).

Задача 154. Пусть f — совершенная раскраска в два цвета гиперграфа Γ_n, определённого выше на рёбрах полного графа K_n. Докажите, что если рёбра любого из цветов раскраски f порождают регулярный граф G, то граф G является сильно регулярным.

15 Полиномиальное представление булевых функций

15.1 Преобразование Мёбиуса

Два базиса $\{u_1, \ldots, u_n\}$ и $\{v_1, \ldots, v_n\}$ в векторном пространстве над некоторым полем F называют *биортогональными*, если $\langle u_i, v_j \rangle = 0$ при $i \neq j$ и $\langle u_i, v_i \rangle = 1$ для любых $i, j \in \{1, \ldots, n\}$. Пусть U и V — квадратные матрицы, составленные из базисных векторов. Тогда $U^{\mathrm{T}}V = I_n$, то есть $U^{\mathrm{T}} = V^{-1}$.

Рассмотрим некоторое конечное множество T и частичный порядок $\leq$ на нём. Для каждого $z \in T$ определим функцию $\omega_z(x) = 1$ при $x \leq z$ и $\omega_z(x) = 0$ в противном случае. Рассмотрим векторное пространство $\mathbb{V}(T)$ функций $f : T \to F$. Число функций ω_z число совпадает с размерностью $|T|$ пространства $\mathbb{V}(T)$. Рассмотрим матрицу W, строки которой есть вектора значений функций $\{\omega_z\}$. Нетрудно видеть, что если элементы множества T занумерованы по неубыванию, то матрица W является нижней треугольной с единицами по главной диагонали. Следовательно, матрица W не вырождена, и имеется базис ν_y, биортогональный базису $\{\omega_z\}$.

Определение 70. *Умножение матрицы W на вектор $f : T \to F$ называют преобразованием Мёбиуса вектора f, а умножение на матрицу V^{T}, где V составлена из функций $\{\nu_y\}$, — обратным преобразованием Мёбиуса.*

Матрицы W и V^{T} взаимно обратны, т. е. $V^{\mathrm{T}}(Wf) = (V^{\mathrm{T}}W)f = f$. Отсюда следует, что и матрица V^{T} является нижней треугольной с единицами по главной диагонали, а V — верхней треугольной. Таким образом, $Wf(z) = \sum_{x \leq z} \omega_z(x) f(x)$ и $V^{\mathrm{T}}g(y) = \sum_{z \leq y} \nu_z(y) g(z)$, так как $V^{\mathrm{T}}(y, z) = V(z, y) = \nu_z(y)$.

Из того, что матрицы W и V^{T} взаимно обратны и являются нижними треугольными, также следуют равенства

Утверждение 129. $\sum\limits_{x:y\le x\le z}\nu_x(z)=0$ *и* $\sum\limits_{x:y_<x\le z}\nu_y(x)=0$ *для любых* $y\ne z$, $y,z\in T$.

Доказательство.

$$\sum_{x:y_<x\le z}\nu_x(z)=\sum_{x:y\le x\le z}V^{\mathrm{T}}(z,x)=\sum_{x:y\le x\le z}V^{\mathrm{T}}(z,x)W(x,y)=\sum_{x}V^{\mathrm{T}}(z,x)W(x,y)=0.$$

Второе равенство можно вывести аналогично. □

В случае линейного порядка матрица W содержит единицы на всех позициях ниже главной диагонали, а матрица V^{T} имеет только две ненулевые диагонали: главную — из единиц и следующую под ней из -1.

В качестве множества с частичным порядком можно рассмотреть булев гиперкуб с лексикографическим порядком. Тогда базисными векторами ω_z являются характеристические функции граней, содержащие $\bar{0}$ и z. Нетрудно проверить, что биортогональный базис $\{\nu_y\}$ состоит из характеристических функций граней, содержащих $\bar{1}$ и y, умноженных на счётчик чётности. Если поле F имеет характеристику 2, то умножение на счётчик чётности не требуется (см. утверждение 131).

Утверждение 130. *Пусть* $f:Q_2^n\to\mathbb{C}$ *— собственная функция с собственным числом* $\lambda=n-2k$. *Тогда*
1) функция f *определяется суммами своих значений в гранях размерности* $n-k$, *содержащих вершину* $\bar{0}$;
2) функция f *в шаре радиуса* $d\le n-k$ *с центром в вершине* $\bar{0}$ *определяется суммами своих значений в гранях размерности* d, *содержащих вершину* $\bar{0}$.

Доказательство. 1) Рассмотрим следствие 43 тождества Саркара $\sum\limits_{z\in\Gamma^\perp}\widehat{f}(z)=2^{n/2-\dim\Gamma}\sum\limits_{x\in\Gamma}f(x)$ при $\dim\Gamma=n-k$. Из утверждения 84 следует, что $\widehat{f}(z)\ne0$ только, если $\mathrm{wt}(z)=k$. Значит в левой части суммы имеется единственное ненулевое слагаемое, т. е. $\widehat{f}(z)=2^{k-n/2}\sum\limits_{x\in\Gamma}f(x)$. Функцию f можно получить из равенства $f=\widehat{\widehat{f}}$.
2) Вначале покажем, что из сумм $\sum\limits_{x\in\Gamma'}f(x)$ при $\dim\Gamma'=m\le n-k$ можно вычислить суммы $\sum\limits_{x\in\Gamma}f(x)$ при $\dim\Gamma=m-1$. Поскольку любые две из $n-(m-1)$ граней размерности m, включающие грань Γ, пересекаются только по грани Γ, имеем равенство

$$\sum_{\Gamma\subset\Gamma'}\sum_{x\in\Gamma'}f(x)-(n-(m-1))\sum_{x\in\Gamma}f(x)=\sum_{x\in\Gamma}\sum_{y:d(x,y)=1}f(y)-(m-1)\sum_{x\in\Gamma}f(x),$$

в левой и правой части которого вычислена сумма значений функции f по всем граням Γ', $\dim \Gamma' = m$, включающим грань Γ, за вычетом их пересечения, т. е. грани Γ. Поскольку f — собственная функция, имеем равенство $\sum\limits_{y:d(x,y)=1} f(y) = \lambda f(x)$. Тогда из двух предыдущих равенств следует равенство

$$\sum_{\Gamma \subset \Gamma'} \sum_{x \in \Gamma'} f(x) = (n - 2(m-1) + \lambda) \sum_{x \in \Gamma} f(x).$$

Рассмотрим $m \le d \le n - k$. По условию имеем $n - 2(m-1) + \lambda \ge n - 2(n-k-1) + n - 2k = 2$, следовательно сумма значений функции по любой грани размерности меньше d может быть вычислена рекуррентно, если известны суммы её значений в гранях размерности d. Обратное преобразование Мёбиуса вычисляет значения функции из сумм её значений в гранях. □

Заметим, что вместо вершины $\bar{0}$ в качестве пересечения всех граней можно брать любую вершину гиперкуба.

15.2 Степень булевой функции

Далее рассмотрим частный случай преобразования Мёбиуса над $GF(2)$ в булевом кубе с лексикографическим порядком.

Каждая булева функция $f : Q_2^n \to Q_2$ может быть представлена в виде *многочлена Жегалкина* или, другими словами, в *алгебраической нормальной форме*

$$f(x_1, \ldots, x_n) = \bigoplus_{y \in Q_2^n} G[f](y) x_1^{y_1} \cdots x_n^{y_n}, \tag{30}$$

где $x^0 = 1, x^1 = x$, $G[f] : Q_2^n \to Q_2$.

Возможность такого представления следует из того, что операции сложения и умножения над $GF(2)$ вместе с константами $0, 1$ образуют полный базис. В частности, умножение совпадает с конъюнкцией, а дизъюнкция выражается как $x \vee y = x \oplus y \oplus xy$. Булеву функцию можно представить в алгебраической нормальной форме единственным образом, поскольку оператор G переводит булевы функции в булевы функции от того же числа переменных.

Определение 71. *Алгебраической степенью булевой функции f называется максимальная степень монома в её многочлене Жегалкина, т. е.* $\deg f = \max\limits_{G[f](y)=1} \mathrm{wt}(y)$.

Алгебраической степенью множества $C \subset Q_2^n$ будем называть алгебраическую степень его характеристической функции. Введём обозначение $x \le y$ для лексикографического порядка на Q_2^n. Имеем $x \le y$ тогда

и только тогда, когда $\mathrm{supp}(x) \subseteq \mathrm{supp}(y)$. Заметим, что $\{x \in Q_2^n \mid x \leq y\}$ есть грань размерности $\mathrm{wt}(y)$, содержащая вершину $\bar{0}$.

Справедливо следующее

Утверждение 131. *Для любой булевой функции f верны равенства $G[f](y) = \bigoplus\limits_{x \in Q_2^n, x \leq y} f(x)$, т.е. $G[f]$ — преобразование Мёбиуса функции f над $GF(2)$. Кроме того, $G[G[f]] = f$.*

Доказательство. Нетрудно видеть, что при $\mathrm{supp}(y) \not\subseteq \mathrm{supp}(x)$ имеем $x_1^{y_1} \cdots x_n^{y_n} = 0$, а в противном случае $x_1^{y_1} \cdots x_n^{y_n} = 1$. Зафиксируем $z \in Q_2^n$. Покажем, что $\bigoplus\limits_{x \in Q_2^n, x \leq z} x_1^{y_1} \cdots x_n^{y_n} = 1$ только если $z = y$. Действительно, если $y < z$, то в сумме $2^{\mathrm{wt}(z) - \mathrm{wt}(y)}$ единиц, а значит сумма равна 0. А если z и y несравнимы или $z < y$, то все слагаемые равны 0. Суммируя обе части равенства (30) по грани $\{x \in Q_2^n : x \leq z\}$, получаем равенство $\bigoplus\limits_{x \in Q_2^n, x \leq z} f(x) = G[f](z)$.

Зафиксируем $x \in Q_2^n$. В правой части равенства (30) мономы $x_1^{y_1} \cdots x_n^{y_n}$ равны 1 только при $y \leq x$. Поэтому $f(x) = \bigoplus\limits_{y \in Q_2^n, y \leq x} G[f](y)$. Отсюда имеем равенство $G[G[f]] = f$ для любой булевой функции f. □

Будем говорить, что булева функция уравновешена по модулю 2 в грани Γ, если её булева сумма в грани равна 0.

Утверждение 132. *Булева функция $f : Q_2^n \to Q_2$ является уравновешенной по модулю 2 в гранях размерности $m+1$ тогда и только тогда, когда $\deg f \leq m$.*

Доказательство. С одной стороны, мономы степени меньшей, чем размерность грани Γ, имеют в грани Γ чётное число единиц. Поэтому функция уравновешена по модулю 2 в гранях размерности больше чем $\deg f$.

С другой стороны, $\bigoplus\limits_{x \in Q_2^n, x \leq z} x_1^{y_1} \cdots x_n^{y_n} = 1$ если и только если $z = y$. Поэтому если в многочлене Жегалкина есть моном степени k, то найдётся грань размерности k и содержащая $\bar{0}$, сумма по которой равна 1. □

Утверждение 133 ([134])**.** *Если булева функция f имеет чётное число единиц в грани размерности $m = n - \mathrm{cor}(f)$, то $\deg(f) \leq m - 1$; если нечётное, то $\deg(f) = m$ и $G[f](z) = 1$ для любого $z \in Q_2^n$, $\mathrm{wt}(z) = m$.*

Доказательство. По определению корреляционнной иммунности функция f имеет одинаковое число единиц в гранях размерности m. Если это число чётное, то $\deg(f) \leq m-1$ по утверждению 132. Если нечётное, то в гранях размерности $m+1$ оказывается уже чётное число единиц. Более

того, поскольку во всех гранях размерности m нечётное число единиц, то $G[f](z) = \bigoplus\limits_{x \in Q_2^n, x \le z} f(x) = 1$ для любого $z \in Q_2^n$, $\mathrm{wt}(z) = m$. □

Следствие 53 (неравенство Зигенталера)**.**
Для любой булевой функции $f : Q_2^n \to Q_2$ верно $\deg(f) \le n - \mathrm{cor}(f)$ *и неравенство* $\deg(f) \le n - \mathrm{cor}(f) - 1$ *верно для устойчивой функции f, за исключением аффинных функций.*

По утверждению 96 совершенная раскраска в булевом n-мерном кубе с матрицей параметров

$$\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix} \tag{31}$$

является корреляционно-иммунной функцией порядка $\frac{b+c}{2} - 1$. Тогда из утверждения 133 вытекает

Следствие 54. *Пусть $f : Q_2^n \to Q_2$ — совершенная раскраска с матрицей параметров* (31)*. Тогда* $\deg(f) \le n - \frac{b+c}{2} + 1$.

Булевы функции $f : Q_2^n \to Q_2$ можно рассматривать в виде набора значений как элементы булева гиперкуба размерности 2^n. Множество векторов значений булевых функций в гиперкубе Q_2^n алгебраической степени не выше m называется кодом Рида—Маллера типа $\mathcal{R}(m, n)$ в $Q_2^{2^n}$. Код Рида—Маллера является линейным, поскольку степень суммы многочленов не больше степени слагаемых.

Утверждение 134 ([125])**.** *Для любой не тождественно нулевой булевой функции f справедливо неравенство* $|\mathrm{supp}(f)| \ge 2^{n-\deg(f)}$*. Если* $|\mathrm{supp}(f)| = 2^{n-\deg(f)}$*, то множество* $\mathrm{supp}(f)$ *является аффинным подпространством.*

Доказательство. Индукция по n. Если функция f равна 1 в единственной точке, то её сумма по всему гиперкубу нечётна и в многочлене Жегалкина есть слагаемое степени n. Если функция более одного раза принимает значение 1, то не менее одной единицы функции содержится в каждой из двух гиперграней по некоторому направлению. Степень функции, ограниченной на гипергрань, не больше степени исходной функции. По предположению индукции в каждой из гиперграней не менее $2^{(n-1)-\deg(f)}$ единиц функции.

Аффинность булевой функции эквивалентна тому, что пересечение с любой гранью любого направления имеет мощность 2^i или 0. Доказательство случая равенства можно провести по индукции. □

Следствие 55. *Кодовое расстояние кода $\mathcal{R}(m, n)$ равно 2^{n-m}.*

Из тождества Саркара нетрудно вывести следующее

Утверждение 135. *Пусть f — булева функция и для любого $v \in Q_2^n$ имеем $\widehat{(-1)^f}(v) = 2^k m(v)$, где $m(v)$ — целое. Тогда* $\deg(f) \le \frac{n}{2} - k + 1$.

Доказательство. Рассмотрим моном $x_1^{y_1} \cdots x_n^{y_n}$ максимальной степени в многочлене Жегалкина функции f, т. е. $G[f](y) = 1$ и $\mathrm{wt}(y) = \deg(f)$. Тогда $\sum\limits_{x \le y} f(x) \equiv 1 \mod 2$ и $\sum\limits_{x \le y} (-1)^{f(x)} = 2(m'+1)$ и m' — чётное (возможно и отрицательное). Из тождества Саркара (следствие 43) имеем

$$\sum_{v \in Q_2^n, v \le y \oplus 1} \widehat{(-1)^f}(v) = 2^{n/2 - \mathrm{wt}(y)} \sum_{x \le y} (-1)^{f(x)} = (1+m') 2^{n/2 - \deg(f) + 1}. \quad (32)$$

Тогда по условию получаем, что $k \le n/2 - \deg(f) + 1$. □

Отметим, что k в этом утверждении может быть и отрицательным.

Теорема 49. 1. *Если f — бент-функция, то* $\deg(f) \le n/2$ *при* $n \ge 4$.
2. *Если f — устойчивая и $nl(f) = 2^{n-1} - 2^{\mathrm{cor}(f)+1}$, то* $\deg(f) = n - \mathrm{cor}(f) - 1$.
3. *Если f не устойчива и $nl(f) = 2^{n-1} - 2^{\mathrm{cor}(f)}$, то* $\deg(f) = n - \mathrm{cor}(f)$. *Причём* $G[f](y) = 1$ *при* $\mathrm{wt}(y) = n - \mathrm{cor}(f)$.

Доказательство. 1. Имеем $|\widehat{(-1)^f}| = \mathbf{1}$ для любой бент-функции. Из утверждения 135 следует, что $\deg(f) \le \frac{n}{2} + 1$. Уточним эту оценку. В грани размерности $n - \deg(f)$ имеется $2^{n-\deg(f)}$ ($n - \deg(f) > 0$ при $n > 2$) точек, поэтому сумма $\sum\limits_{v \in Q_2^n, v \le y \oplus 1} \widehat{(-1)^f}(v)$ в равенстве (32) чётна. Из равенства (32) следует, что число $2^{n/2-\deg(f)}$ целое.

2. Достаточно доказать, что $\deg(f) \ge n - \mathrm{cor}(f) - 1$ (см. следствие 53). Из тождества Саркара (замечание 18) и утверждения 118 видно, что все ненулевые коэффициенты Адамара—Уолша функции f имеют вид $\pm 2^{2+\mathrm{cor}(f)-\frac{n}{2}}$. По теореме 34 найдётся $y \in Q_2^n$, $\mathrm{wt}(y) = \mathrm{cor}(f)+1$, для которого $|\widehat{(-1)^f(y)}| = 2^{2+\mathrm{cor}(f)-\frac{n}{2}}$. Аналогично равенству (32) имеем

$$\pm 2^{2+\mathrm{cor}(f)-\frac{n}{2}} = \sum_{v \in Q_2^n, v \le y} \widehat{(-1)^f}(v) = 2^{\frac{n}{2}-\mathrm{wt}(y \oplus 1)} \sum_{x \le y \oplus 1} (-1)^{f(x)} = 2^{\mathrm{cor}(f)-\frac{n}{2}+1} \sum_{x \le y \oplus 1} (-1)^{f(x)}.$$

Тогда $\sum\limits_{x \le y \oplus 1} (-1)^{f(x)} = \pm 2$. Последнее равенство возможно только если $\sum\limits_{x \le y \oplus 1} f(x) \equiv 1 \mod 2$. Тогда $\deg f \ge \mathrm{wt}(y \oplus 1) = n - \mathrm{cor}(f) - 1$.

3. Из тождества Саркара (замечание 18) и утверждения 118 видно, что все ненулевые коэффициенты Адамара—Уолша функции f имеют вид $\pm 2^{\mathrm{cor}(f)+1-\frac{n}{2}}$. Поскольку f не устойчива, имеем $|\widehat{(-1)^f}(\bar{0})| = 2^{\mathrm{cor}(f)+1-\frac{n}{2}}$. По теореме 34 имеем $\widehat{(-1)^f}(z) = 0$ для всех z, $0 < \mathrm{wt}(z) \le \mathrm{cor}(f)$. Рассмотрим произвольный y, для которого $\mathrm{wt}(y) = n - \mathrm{cor}(f)$ и

$\mathrm{wt}(y \oplus 1) = \mathrm{cor}(f)$. Тогда из левой части равенства (32) имеем $2^{n/2-\mathrm{wt}(y)} \sum\limits_{x \le y} (-1)^{f(x)} = \widehat{(-1)^f}(\bar{0}) = \pm 2^{\mathrm{cor}(f)+1-\frac{n}{2}}$. Следовательно, $\sum\limits_{x \le y} (-1)^{f(x)} = \pm 2$. Последнее равенство возможно только если $\sum\limits_{x \le y} f(x) \equiv 1 \mod 2$. Тогда $G[f](y) = 1$. □

Утверждение 49 означает что, максимально нелинейная при фиксированной корреляционной иммунности функция не только является платовидной, но и достигает равенства в неравенстве Зигенталера.

15.3 Алгебраическая иммунность

При вскрытии некоторых шифров возникает следующая задача. Известны булева функция $f : Q_2^n \to Q_2$, аффинное преобразование $L : Q_2^n \to Q_2^n$ и выходная последовательность $b_0 = f(x), b_1 = f(L(x)), \ldots, b_i = f(L^i(x)), \ldots$. Нужно найти ключ $x \in Q_2^n$. Сложность системы уравнений зависит от степени функции f. Поэтому, если существует такая булева функция g, что $\deg(g) < \deg(f)$ и $gf = \mathbf{0}$, то можно искать подходящие наборы x как решения более простой системы $g(x)b_0 = 0, \ldots, g(L^i(x))b_i = 0, \ldots$. Для оценки устойчивости функции f относительно такого метода криптоанализа вводится понятие алгебраической иммунности.

Определение 72. *Алгебраической иммунностью булевой функции f называется величина $AI(f) = \min_g\{\deg(g) \mid gf = \mathbf{0}$ или $g(f \oplus \mathbf{1}) = \mathbf{0}, g \neq \mathbf{0}\}$.*

Теорема 50 (Куртуа и Майер [26])**.** *Для любой булевой функции $f : Q_2^n \to Q_2$ найдётся такая булева функция g, $\deg(g) \le \lceil \frac{n}{2} \rceil$, что $\deg(fg) \le \lfloor \frac{n}{2} \rfloor$.*

Доказательство. Пусть A_d — множество всех мономов степени не больше d, $|A_d| = \sum\limits_{i=0}^{d} \binom{n}{i}$. Возьмём $d_1 = \lfloor \frac{n}{2} \rfloor$ и $d_2 = \lceil \frac{n}{2} \rceil$. Рассмотрим набор функций $B = \{fw \mid w \in A_{d_2}\}$. Пусть$B$ — линейно зависимое множество. Тогда $fw_1 \oplus fw_2 \oplus \cdots \oplus fw_k = \mathbf{0}$ для некоторых различных функций $w_1, \ldots, w_k \in A_{d_2}$. Тогда $g = w_1 \oplus w_2 \oplus \cdots \oplus w_k$ искомая функция. В противном случае B — линейно независимое множество и $|B| = |A_{d_2}|$. Имеем $|B| + |A_{d_1}| = \sum\limits_{i=0}^{d_1} \binom{n}{i} + \sum\limits_{i=0}^{d_2} \binom{n}{i} = \sum\limits_{i=0}^{n} \binom{n}{i} + \binom{n}{\lfloor \frac{n}{2} \rfloor} > 2^n$. Поскольку векторное пространство булевых функций над $GF(2)$ имеем размерность 2^n, то множество функций $B \cup A_{d_1}$ линейно зависимое. Тогда найдётся линейная комбинация вида $h \oplus fg = \mathbf{0}$, где h — линейная комбинация мономов из A_{d_1}, а g — линейная комбинация мономов из A_{d_2}. □

Следствие 56. *Для любой булевой функции f в n-мерном булевом кубе верно, что $AI(f) \le \lceil \frac{n}{2} \rceil$.*

Доказательство. Из теоремы 50 следует, что найдётся булева функция g, для которой $\deg(g \oplus fg) \le \lceil \frac{n}{2} \rceil$. Очевидно, что $f(g \oplus fg) = fg \oplus fg = \mathbf{0}$. □

Утверждение 136 ([19]). *Для любой булевой функции f в n-мерном булевом кубе верно, что* $nl(f) \ge \sum_{i=0}^{AI(f)-2} \binom{n}{i}$.

Доказательство. Оценим величину $\mathrm{wt}(f) = |\mathrm{supp}(f)|$. Рассмотрим систему из $|\mathrm{supp}(f)|$ булевых уравнений $\sum_{w \in A_d} a_w w(x) = 0$ относительно неизвестных a_w, где x принимает все значения из $\mathrm{supp}(f)$. Если такая система имеет ненулевое решение (a_w), то $f \cdot (\sum_{w \in A_d} a_w w) = \mathbf{0}$. Выберем d так, что $AI(f) = d + 1$. Тогда система имеет только нулевое решение, следовательно, число уравнений не меньше числа переменных, т. е. $\sum_{i=0}^{AI(f)-1} \binom{n}{i} \le \mathrm{wt}(f)$.

Рассмотрим функцию $f \oplus \ell$, где ℓ — произвольная аффинная функция. Если $(f \oplus \ell)g = \mathbf{0}$ для некоторой функции g, то $fg = g\ell$. Тогда $fg(1 \oplus \ell) = g\ell(1 \oplus \ell) = g\ell \oplus g\ell = \mathbf{0}$. Кроме того, $\deg(g(1 \oplus \ell)) \le \deg(g) + 1$. Следовательно, $AI(f \oplus \ell) \le AI(f) + 1$ и $AI(f) = AI(f \oplus \ell \oplus \ell) \le AI(f \oplus \ell) + 1$.

Тогда имеем $\sum_{i=0}^{AI(f)-2} \binom{n}{i} \le \sum_{i=0}^{AI(f \oplus \ell)-1} \binom{n}{i} \le \mathrm{wt}(f \oplus \ell)$. Из определения нелинейности $nl(f) = \min_\ell \mathrm{wt}(f \oplus \ell)$ получаем требуемое. □

Точные соотношения между алгебраической иммунностью и нелинейностью (расстоянием от функции до аффинных функций или функций ограниченной степени) получены М.С.Лобановым [123].

15.4 Представление линейного кода многочленом

Сдвиг множества $C \subset Q_2^n$ на любой вектор $y \in Q_2^n$ осуществляется преобразованием аргумента $x' = x \oplus y$. Поэтому изометричные преобразования не изменяют степень характеристической функции множества. Из аффинного подпространства C можно получить линейное, прибавив к нему любой, принадлежащий ему вектор.

Любое линейное подпространство C можно задать проверочной матрицей H полного ранга, т. е. $C = \{x \in Q_2^n \mid Hx = \bar{0}\}$, где $H = \{h_{ij}\}$ — матрица размера $k \times n$ и $\mathrm{rank}(C) = n - k$. Пусть $H[x]$ — матрица из столбцов вида $h_j x_j$, где h_j — столбцы матрицы H, $j = 1, \ldots, n$. Например, если $H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$, то $H[x] = \begin{pmatrix} 0 & x_2 & x_3 \\ x_1 & 0 & x_3 \end{pmatrix}$.

Утверждение 137. *Пусть* $C = \{x \in Q_2^n | Hx = \bar{1}\}$, *тогда* $\chi_C = \mathrm{per}_2(H[x])$.

Доказательство. Нетрудно видеть, что $\chi_C(x) = \prod_i(\bigoplus_j h_{ij}x_j)$ — произведение сумм строк матрицы $H[x]$. А это по определению $\mathrm{per}_2(H[x])$. $\square$

Утверждение 138. *Степень характеристической функции линейного кода $C \subset Q_2^n$ равна $n - \mathrm{rank}(C)$.*

Доказательство. Пусть $C = \{x \in Q_2^n \mid Hx = \bar{0}\}$, где $H = \{h_{ij}\}$ — матрица размера $k \times n$, $k = n - \mathrm{rank}(C)$. Рассмотрим множество $C' = \{x \in Q_2^n \mid Hx = \bar{1}\}$. Очевидно, C' — аффинное подпространство, эквивалентное коду C. Нетрудно видеть, что $\chi_{C'}(x) = \prod_i(\bigoplus_j h_{ij}x_j)$ — произведение сумм строк матрицы $H[x]$. Очевидно, $\deg(\chi_{C'}) \leq k$. Рассмотрим невырожденную подматрицу A матрицы H размера $k \times k$. Невырожденность матрицы A означает, что $\det(A) = 1$ (над полем $\mathrm{GF}(2)$). В свою очередь из равенства $\det(A) = 1$ следует, что моном, соответствующий столбцам матрицы A входит в произведение $\prod_i(\bigoplus_j h_{ij}x_j)$ нечётное число раз. $\square$

Следствие 57. *Пусть $C \subset Q_2^n$ — код Хэмминга, $n = 2^t - 1$. Тогда $\deg(\chi_C) = t$.*

Задача 155. Докажите[41], что любую функцию $f : Q_p^n \to Q_p$, p — простое, можно единственным образом представить в виде многочлена над $GF(p)$ степени не выше $n(p-1)$ (каждая переменная в мономе имеет степень не выше $p-1$).

Задача 156. Докажите, что при простом q степень характеристической функции линейного кода $C \subset Q_q^n$ равна $n - \mathrm{rank}(C)$.

Задача 157. Докажите, что для неустойчивой платовидной функции f справедливо следующее свойство: $|\widehat{(-1)^f}(z)| = |\widehat{(-1)^f}(y)|$, если $\mathrm{wt}(y) = \mathrm{wt}(z)$. В частности, $|\widehat{(-1)^f}(z)| = 2^{\mathrm{cor}(f)+1-\frac{n}{2}}$ при $\mathrm{wt}(z) = \mathrm{cor}(f) + 1$.

Задача 158. Докажите, что булева функция $f : Q_2^n \to Q_2$ зависит от переменной x_i линейно (над полем $GF(2)$) тогда и только тогда, когда $\widehat{(-1)^f}(z) = 0$ для всех $z \in Q_2^n$ таких, что $z_i = 0$.

Задача 159. Докажите, что для любого $k \geq 0$ найдётся $n(k)$ такое, что при $n \geq n(k)$ верно следующее. Если $\mathrm{cor}(f) \geq n - k$, то булева функция $f : Q_2^n \to Q_2$ зависит от некоторых переменных линейно.

Задача 160. Докажите, что для любого $k \geq 0$ найдётся $n(k)$ такое, что при $n \geq n(k)$ верно следующее. Если $\widehat{f}(z) = 0$ при $\mathrm{wt}(z) \geq k$, то булева функция $f : Q_2^n \to Q_2$ не зависит от некоторых переменных.

Задача 161. Докажите, что мощность носителя булевой функции степени k от n переменных делится на $2^{\lceil n/k \rceil - 1}$. (Теорема МакЭлиса)

[41] Это утверждение верно для любого конечного поля.

Задача 162. Докажите, что степень характеристической функции 1-совершенного двоичного кода длины n не превышает $\frac{n+1}{2}$. Оцените минимальное расстояние Хэмминга между двумя 1-совершенными кодами.

Задача 163. Оцените минимальное расстояние Хэмминга между двумя платовидными функциями с одинаковыми параметрами.

Задача 164. Докажите, что коды Рида—Маллера $\mathcal{R}(m,n)$ и $\mathcal{R}(k,n)$ дуальны, т. е. $\mathcal{R}(k,n) \subseteq \mathcal{R}(m,n)^{\perp}$, в частности самодуальны, при $k+m<n$.

Задача 165. Докажите, что $\mathcal{R}(1,n)$ — это расширенный код Адамара, а $\mathcal{R}(n-2,n)$ — расширенный код Хэмминга.

Задача 166. Докажите, что если две булевы функции f и g, обе степени не больше r, совпадают в некотором шаре B_r радиуса r, то $f=g$.

16 Замощения и совершенные коды

16.1 Замощения

Определение 73. *Замощением (факторизацией) группы $(Gr,\circ)$ называется пара (C,B) множеств $C \subset Gr$ и $B \subset Gr$ такая, что для любого $x \in Gr$ существует единственная пара элементов $c \in C$ и $b \in B$, для которых $x = c \circ b$, т. е. $Gr = C \circ B$.*

Если $C < Gr$ — подгруппа, то в множество B можно выбрать по одному представителю из каждого фактор-класса Gr/C. Нетрудно видеть, что для конечной группы единственность представления влечёт равенство $|Gr| = |C||B|$.

Если (C,B) — замощение, то и $(C, B\circ a)$ — замощение для любого $a \in Gr$. Поэтому всегда можно полагать что нейтральный элемент группы ε содержится в $C \cap B$. В этом случае очевидно $C \cap B = \{\varepsilon\}$.

Утверждение 139. *Пара (C,B) является замощением группы $(Gr,\circ)$ тогда и только тогда, когда $(C^{-1}\circ C)\cap(B\circ B^{-1}) = \{\varepsilon\}$ и $|Gr| = |C||B|$.*

Доказательство. Равенство $c_1 \circ b_1 = c_2 \circ b_2$ эквивалентно равенству $c_2^{-1} \circ c_1 = b_2 \circ b_1^{-1}$. Таким образом, единственность представления эквивалентна равенству $C^{-1} \circ C \cap B \circ B^{-1} = \{\varepsilon\}$. Представление любого элемента группы в виде $c \circ b$ существует, поскольку все элементы $C \circ B$ различны и их число совпадает с мощностью группы. □

В случае абелевой группы это условие приобретает более симметричный вид $(C-C)\cap(B-B) = \{0\}$.

Пусть A — множество образующих в графе Кэли $G = Cay(Gr, A)$. Рассмотрим единичный шар $B = A \cup \{\varepsilon\}$. Нетрудно видеть, что множество $C \subset Gr$ является 1-совершенным кодом в G тогда и только тогда, когда (C,B) — замощение группы Gr.

Пример 46. Код Хэмминга $C \subset Q_q^n$ и единичный шар $B = \{x \in Q_q^n \mid \mathrm{wt}(x) \leq 1\}$ образуют замощение при $n = \frac{q^t-1}{q-1}$.

Утверждение 140. *Пара (C, B) является замощением абелевой группы K тогда и только тогда, когда $\chi_C * \chi_B = \mathbf{1}$ или, эквивалентно, $\widehat{\chi_C} \cdot \widehat{\chi_B} = \delta/|K|^{1/2} = \mathbf{1}_{\{0\}}$.*

Доказательство. Первое равенство следует из определения замощения, второе — из утверждения 89 и равенства $\widehat{\mathbf{1}} = \delta$. □

В качестве обобщения замощений абелевой группы K можно рассмотреть пары функций (f, g), $f, g : K \to \mathbb{C}$, для которых $f * g = \alpha\mathbf{1}$, для некоторого $\alpha \in \mathbb{C}$. Аналогично утверждению 140 критерием того, что пара (f, g) — обобщённое замощение, является равенство $\mathrm{supp}(\widehat{f}) \cap \mathrm{supp}(\widehat{g}) = \{0\}$.

Замощение группы можно использовать для компактного хранения группы. Для выполнения групповой операции нужна её таблица Кэли, которая имеет размер $|Gr|^2$. Если же имеется замощение (C, B) группы Gr, то достаточно иметь таблицы умножения элементов группы на элементы из C и на элементы из B, т. е. две таблицы размеров $|Gr||C|$ и $|Gr||B|$.

Замощение (C, B) группы $\mathbb{Z}_2^k$ можно использовать для построения 1-совершенных кодов в Q_2^n. Будем рассматривать элементы $\mathbb{Z}_2^k$ как двоичные вектора длины k Пусть $\bar{0} \in C$ и $|C| = n + 1$. Взяв ненулевые элементы C в качестве столбцов, построим матрицу H размера $k \times n$.

Утверждение 141 ([25])**.** *Объединение множеств решений систем уравнений $Hx = b$ над $GF(2)$ по всем $b \in B$ является 1-совершенным кодом в Q_2^n.*

Доказательство. Пусть $x \in Q_2^n$. Докажем, что имеется кодовое слово на расстоянии не более 1 от x. Рассмотрим $z = x_1c^1 + \cdots + x_nc^n \in \mathbb{Z}_2^k$. Поскольку (C, B) — замощение, найдутся $c^t \in C$ и $b \in B$ такие, что $z = c^t + b$. Если $c^t = \bar{0}$, то x — кодовое слово. В противном случае кодовым словом является вектор $x + (0 \ldots 0\underset{i}{1}0 \ldots 0)$.

Докажем, что расстояние между кодовыми словами не меньше чем 3. Пусть $x_1c^1 + \cdots + x_nc^n = b^1$, $y_1c^1 + \cdots + y_nc^n = b^2$, x и y различаются только в позициях i и j. Тогда имеем равенство $c^i + c^j = b^1 + b^2$, что противоречит определению замощения. Если x и y различаются в одной позиции, то получаем аналогичное противоречие из условия $\bar{0} \in C$. □

Понятие замощения можно распространить на вершинно транзитивные графы.

Определение 74. *Замощением вершинно транзитивного графа G называется пара (A, Gr), где $A \subset V(G)$, $Gr < Aut(G)$, причём $V(G) = \bigsqcup_{\varphi \in Gr} \varphi(A)$.*

Ясно, что условия $|Gr||A| = V(G)$ и $\varphi_1(A) \cap \varphi_2(A) = \varnothing$ при $\varphi_1 \neq \varphi_2$, $\varphi_i \in Gr$ являются необходимыми и достаточными условиями замощения.

16.2 Совершенные коды с расстоянием большим, чем 3

Определение 75. *Совершенным кодом с кодовым расстоянием* $2e+1$ *(*e*-совершенным кодом) в графе* G *называется такое множество* $C \subset V(G)$*, что шары* $B(x,e)$ *с центрами в вершинах* $x \in C$ *радиуса* e *образуют разбиение вершин графа, т. е.* $V(G) = \bigsqcup\limits_{x \in C} B(x,e)$.

Совершенный код с расстоянием $2e+1$ в графе Кэли $G = Cay(Gr, A)$ эквивалентен замощению $(C, A^e \cup \{\varepsilon\})$, где $A^e = \{a_1 \circ \cdots \circ a_k |\ a_i \in A, k = 1, \ldots, e\}$, а также 1-совершенному коду в графе $G = Cay(Gr, A^e)$.

В дистанционно-регулярном графе с параметрами $(b_0, \ldots, b_{d-1}, c_1, \ldots, c_d)$ e-совершенный код C порождает совершенную раскраску с матрицей параметров $S_C = \begin{pmatrix} a_0 & b_0 & 0 & 0 & \ldots & 0 \\ c_1 & a_1 & b_1 & 0 & \ldots & 0 \\ 0 & c_2 & a_2 & b_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & 0 & c_e & a_e + b_e \end{pmatrix}$, в которой в первый цвет покрашены вершины коды C, а цвета остальных вершин определяются минимальным расстоянием до кодовой вершины.

Утверждение 142 (условие Ллойда)**.** *Пусть* C *— совершенный код с расстоянием* $2e+1$ *в дистанционно-регулярном графе* G*. Тогда для любого собственного числа* λ *матрицы* S_C*, кроме* $\lambda_0 = \deg G$*, справедливо равенство* $1 + P_1(\lambda) + \cdots + P_e(\lambda) = 0$*, где* $P_t(x)$ *— многочлен определяемый по графу* G *(см. раздел 4.2).*

Доказательство. Пусть f — характеристическая функция кода C. Тогда по определению e-совершенного кода имеем равенство $If + Mf + M_2 f + \cdots + M_e f = \mathbf{1}$, где $M_i = P_i(M)$ — матрица смежности графа G по расстоянию i. Пусть λ_i, $i = 0, \ldots, e$, — собственные числа матрицы параметров S_C. Из следствия 3 имеем, что для подходящих коэффициентов α_i выполнено равенство $f = \sum_i \alpha_i \varphi_i$, где φ_i собственная функция графа G с собственным числом λ_i.

Покажем, что $\alpha_i \neq 0$ для любого $i = 0, \ldots, e$. Из следствия 1 получаем, что для любого собственного числа матрицы S_C некоторую собственную функцию графа с таким собственным числом можно получить как линейную комбинацию характеристических функций цветов. Характеристическая функция цвета, находящегося на расстоянии i от кода, равна $M_i f$. Поэтому все характеристические функции цветов представимы как линейная комбинация тех же собственных функций графа, что и первый цвет. Значит, если $\alpha_i = 0$ для некоторого $i = 0, \ldots, e$, то все

характеристические функции цветов ортогональны соответствующему собственному подпространству матрицы M. Пришли к противоречию.

Таким образом, из утверждения 18 имеем равенство

$$\mathbf{1} = If + Mf + M_2 f + \cdots + M_e f = \sum_{i=0}^{e} \alpha_i (1 + P_1(\lambda_i) + \cdots + P_e(\lambda_i))\varphi_i.$$

Поскольку $\mathbf{1}$ — собственная функция, соответствующая собственному числу λ_0, получаем, что $1 + P_1(\lambda_i) + \cdots + P_e(\lambda_i) = 0$ при $i = 1, \ldots, e$. □

Если дистанционно-регулярный граф является графом Кэли абелевой группы, то условие Ллойда эквивалентно утверждению 140. Действительно, $\mathbf{1} = If + Mf + M_2 f + \cdots + M_e f = \chi_B * f$, где $f = \chi_C$ и B — шар радиуса e с центром в нуле.

Следствие 58. *Матрица S_C не имеет кратных собственных чисел и справедливо равенство* $\det(S_C - xI) = (-1)^{e+1}(\prod_{t=1}^{e} c_t)(x - \lambda_0) \sum_{t=0}^{e} P_t(x)$.

Доказательство. Поскольку матрица $S_C - \lambda I$ трёхдиагональна с положительными побочными диагоналями, её ранг не меньше e. Следовательно, матрица S_C не имеет кратных собственных чисел. Из условия Ллойда следует, что многочлены $\det(S_C - xI)$ и $(x - \lambda_0) \sum_{t=0}^{e} P_t(x)$ имеют одинаковые корни. Из равенства (7) видно, что коэффициент многочлена $P_e(x)$ при старшей степени равен $1/\prod_{t=1}^{e} c_t$. Коэффициент многочлена $\det(S_C - xI)$ при старшей степени равен $(-1)^{e+1}$. □

16.3 Совершенные коды в гиперкубах

Утверждение 143. *Пусть $C \subset Q_q^n$ — совершенный код с расстоянием $2e+1$. Тогда справедливо равенство $(n-\lambda_1)\cdots(n-\lambda_e) = e!q^n/|C|$, где λ_i, $i = 1, \ldots, e$ — все собственные числа матрицы S_C, кроме $\lambda_0 = (q-1)n$.*

Доказательство. Степени вершин n-мерного гиперкуба равны $(q-1)n$, поэтому $(q-1)n$ есть максимальное собственное число матрицы S_C. Для гиберкубов имеем $c_i = i$. Как было замечено в следствии 58 матрица S_C не имеет кратных собственных чисел, поэтому $\det(S_C - xI) = (-1)^{e+1}(x - \lambda_0)\cdots(x - \lambda_e)$. В обеих частях равенства $\det(S_C - xI) = (-1)^{e+1}e!(x - (q-1)n)\sum_{t=0}^{e} P_t(x)$ из следствия 58 сократим сомножитель $(x - (q-1)n)$. Здесь $P_t = P_t[n, q]$ — q-полином Кравчука. Из утверждения 18 следует, что $\sum_{t=0}^{e} P_t(n)$ — мощность шара радиуса e. Поскольку $C \subset Q_q^n$ — совершенный код с расстоянием $2e+1$, то шары радиуса e с центрами в его вершинах являются разбиением гиперкуба, т. е. $|C| \sum_{t=0}^{e} P_t(n) = q^n$. □

Рассмотрим подробнее булев гиперкуб.

Утверждение 144. *Пусть $S_r \subset Q_2^n$ — сфера радиуса r с центром в $\bar{0}$. Для любого фиксированного $r \in \mathbb{N}$ при достаточно больших n верно неравенство $\widehat{\chi_{S_r}}(z) > 0$ для всех таких z, что $\mathrm{wt}(z) < n/2$.*

Доказательство. Пусть $\mathrm{wt}(z) = m$, где переменная m может зависеть от n. Имеем равенства

$$2^{n/2}\widehat{\chi_{S_r}}(z) = \sum_{\mathrm{wt}(x)=r} (-1)^{\langle x,z\rangle} = \sum_{i=0}^{r} (-1)^i \binom{m}{i}\binom{n-m}{r-i}.$$

Если $2mr+m+r \le n$, то $\binom{m}{1}\binom{n-m}{r-1} \le \frac{1}{2}\binom{n-m}{r}$. Поэтому $\sum\limits_{i=0}^{r}(-1)^i\binom{m}{i}\binom{n-m}{r-i} > \frac{1}{2}\binom{n-m}{r}$.

Если $2mr + m + r > n$, то $m \to \infty$ при $n \to \infty$. Применяя равенство $m \cdots (m-i+1) = m^i(1+o(1))$ при $m \to \infty$ и бином Ньютона, получаем

$$\sum_{i=0}^{r}(-1)^i\binom{m}{i}\binom{n-m}{r-i} = \sum_{i=0}^{r}(-1)^i\frac{m^i(n-m)^{r-i}}{i!(r-i)!}(1+o(1)) = \frac{(n-2m)^r(1+o(1))}{r!}.$$

□

Из утверждения 18 следует, что $2^{n/2}\widehat{\chi_{S_r}}(z) = P_r[n,2](\lambda_{\mathrm{wt}(z)})$. Следовательно, при достаточно больших n многочлены Кравчука $P_r[n,2](x)$ неотрицательны при $x = n, n-2, \ldots, 2$ или $x = n, n-2, \ldots, 1$. Можно показать, что они не отрицательны и на всём промежутке $x \in [1,n]$ при $n > n_0(r)$.

Замечание 21. Если r растёт достаточно медленно (в частности $2^{r/2} \le n$) утверждение 144 остаётся верным. Поскольку $\widehat{\chi_{B_r}}(z) > 0$ при $\mathrm{wt}(z) < n/2$ для достаточно больших n, из утверждения 140 следует, что $\widehat{\chi_C}(z) = 0$ при $0 < \mathrm{wt}(z) < n/2$, где C — произвольный r-совершенный код. Таким образом, характеристическая функция χ_C ортогональна собственным подпространствам гиперкуба с положительными собственными числами (кроме n). Как следует из доказательства условия Ллойда, разложение характеристической функции χ_C в линейную комбинацию собственных функций содержит нетривиальные слагаемые, соотвствующие каждому собственному числу матрицы S_C. Поэтому матрица S_C не имеет положительных собственных чисел (кроме n) для достаточно больших n.

В утверждении 2 построены 1-совершенные линейные коды Хэмминга. Кроме того, в гиперкубах Q_q^n нечётной размерности $n = 2s+1$ имеются совершенные коды с максимальным[42] расстоянием s, состоящие из всех вершин вида $(a, \ldots, a)$, $a \in Q_q$.

[42] Одноточечное множество в любом графе формально является совершенным кодом с расстоянием равным (или большим) диаметру графа, но учитывать этот случай при перечислении совершенных кодов не принято.

Теорема 51 (Титвайнен [97], Зиновьев и Леонтьев [117]). *Имеется не более конечного числа таких размерностей n, что в булевом гиперкубе Q_2^n есть e-совершенный код при $1 < e < \frac{n-1}{2}$.*

Доказательство. Из утверждения 18 и формулы для значений собственных чисел характеров в булевом гиперкубе $\lambda_z = n - 2\mathrm{wt}(z)$ нетрудно вычислить, что $P_t[n,2](-n) = P_t(-n) = (-1)^t\binom{n}{t}$ и $P_t(2-n) = (-1)^t\left(\binom{n-1}{t} - \binom{n-1}{t-1}\right)$.

Воспользуемся известным комбинаторным тождеством (см. задачу 27) $2n\sum\limits_{t=0}^{s}(-1)^t\binom{n}{t} = (-1)^s\left((s+1)\binom{n}{s+1} + (n-s)\binom{n}{s}\right)$, чтобы вычислить $e!\sum\limits_{t=0}^{e}P_t(-n)$ и $e!\sum\limits_{t=0}^{e}P_t(2-n)$. При $e \geq 2$ имеем

$$e!\sum_{t=0}^{e}P_t(-n) = (-1)^e(n-1)\cdots(n-e),$$

$$e!\sum_{t=0}^{e}P_t(2-n) = (-1)^e(n-2)\cdots(n-e-1) - (-1)^e e(n-2)\cdots(n-e) =$$

$$= (-1)^e(n-2)\cdots(n-e)(n-2e-1).$$

Предположим, что существует e-совершенный код $C \subset Q_2^n$ и λ_i, $i = 0,\ldots,e$, — собственные числа матрицы S_C. Тогда из следствия 58, учитывая $\lambda_0 = n$, имеем равенство

$$(\lambda_1 - x)\cdots(\lambda_e - x) = (-1)^e e!\sum_{t=0}^{e}P_t(x).$$

Подставляя в него $x = -n$ и $x = 2-n$, получаем равенства

$$(n+\lambda_1)\cdots(n+\lambda_e) = (n-1)\cdots(n-e),$$

$$(n+\lambda_1-2)\cdots(n+\lambda_e-2) = (n-2)\cdots(n-e)(n-2e-1). \qquad (33)$$

Первое равенство не обращается в нуль. Второе равенство может обращаться в нуль, только когда $n = 2e+1$. Определим величину $\delta(n)$ равенством $n = 2^{\delta(n)}m$, где m — нечётное число. Среди идущих подряд целых чисел только каждое второе делится на 2, каждое четвёртое — на 4 и т. д. Поэтому

$$\delta((m+1)\cdots(m+k)) \leq k + \max_{i=1,\ldots,k}\delta(m+i). \qquad (34)$$

Если C — e-совершенный код, то собственные числа матрицы S_C являются собственными числами матрицы смежности булева гиперкуба (см. следствие 1). Поскольку $\lambda_i = n - 2t$ для некоторого $t = 1,\ldots,n$, имеем $\delta(n+\lambda_i) \geq 1$ при $i = 1,\ldots,e$. Кроме того, $\delta((n+\lambda_i)(n+\lambda_i-2)) \geq 3$,

поскольку один из сомножителей делится на 4. Перемножив левые и правые части равенств (33) и применив неравенство (34), получаем

$$3e \le \delta((n+\lambda_1)\cdots(n+\lambda_e)(n+\lambda_1-2)\cdots(n+\lambda_e-2)) =$$

$$= \delta((n-2e-1)(n-1)(n-2)^2\cdots(n-e)^2)) \le \delta(n-2e-1)+2e+\max_{i=1,\ldots,e}\delta(n-i).$$

Отсюда имеем $e \le \max\limits_{i=1,\ldots,e} \delta(n-i) + \delta(n-2e-1)$, т. е. $n \ge 2^{e/2}$.

В матрице S_C при $q=2$ коэффициенты $a_i = 0, i = 0,\ldots,e$ и $b_e = n-e$. Поэтому сумма собственных чисел матрицы S_C равна $\mathrm{tr}(S_C) = n-e$. Таким образом, $\sum\limits_{i=1}^{e} \lambda_i = -e$ и все числа λ_i различны (см. следствие 58). Тогда при $e > 1$ среди них найдётся положительное собственное число. Из последнего неравенства и замечания 21 следует, что для достаточно больших n в булевом n-кубе не могут существовать e-совершенные коды, за исключением случаев $e = 1$ и $e = \frac{n-1}{2}$. □

Таким образом, для нахождения всех возможных параметров e-совершенных кодов в булевых n-кубах достаточно рассмотреть конечное число значений n и e. Необходимыми для существования e-совершенного кода являются следующие условия: мощность шара $\sum\limits_{t=0}^{e}\binom{n}{t}$ делит мощность множества вершин графа (т. е. равна 2^n), собственные числа матрицы S_C являются собственными числами матрицы смежности булева n-куба (целые, той же чётности, что и n) и выполнено равенство из утверждения 143. Перечисленные условия (при $1 < e < \frac{n-1}{2}$) удовлетворены только в случае $n = 23$, $S_C = \begin{pmatrix} 0 & 23 & 0 & 0 \\ 1 & 0 & 22 & 0 \\ 0 & 2 & 0 & 21 \\ 0 & 0 & 3 & 20 \end{pmatrix}$, собственные числа матрицы $\lambda = 23, 7, -1, -9$. М.Голей [42] обнаружил линейный код с такими параметрами. Он является единственным с точностью до изометрии.

В.А.Зиновьев, В.К.Леонтьев, А.Титвайнен доказали[43] теорему 51, а также доказали отсутствие совершенных кодов нетривиальных параметров (за исключением троичного кода Голея $n = 11$, $e = 2$, $q = 3$ [42]) при $q = p^s$, где p — простое. В настоящее время доказано ([118],[106]), что для произвольных q и $2 < e < \frac{n-1}{2}$ не существует e-совершенных кодов в Q_q^n.

Задача 167. Пусть A — множество образующих в графе Кэли $G = Cay(K, A)$ абелевой группы K, $B = A \cup \{0\}$. Докажите, что если (C, B) — замощение группы K, то раскраска $f : V(G) \to B$ каждой вершины $x \in K$ в цвет b, если $x = c + b$, где $c \in C$, $b \in B$, является совершенной.

[43] Наше изложение соответствует книге [66].

Задача 168. Докажите, что если в дистанционно-регулярном графе имеется совершенный код с расстоянием $2e+1$, то для любого собственного числа λ матрицы S_C верно равенство $|A_{e+1}|P_e(\lambda) = |A_e|P_{e+1}(\lambda)$, где A_e — сфера радиуса e.

Задача 169. Докажите равенство $\det(S_C - xI) = (-1)^{e+1}(c_{e+1}P_{e+1}(x) - b_eP_e(x))\prod_{t=1}^{e} c_t$.

Список литературы

[1] N. Alon, F. R. K. Chung, Explicit construction of linear sized tolerant networks, in Proceedings of the First Japan Conference on Graph Theory and Applications, Hakone, 1986, (1988) 15–19.

[2] Noga Alon, Vitali D. Milman, λ_1, isoperimetric inequalities for graphs, and superconcentrators, J. Comb. Theory, Ser. B 38(1) (1985) 73-88.

[3] N. Alon, S. Friedland, The maximum number of perfect matchings in graphs with a given degree sequence, The Electronic Journal of Combinatorics 15 (2008), #13.

[4] D. Angluin, A. Gardiner, Finite common coverings of pairs of regular graphs, J. Combin. Th. Ser. B 30 (1981) 184-187.

[5] S. V. Avgustinovich, I. Yu. Mogil'nykh, "Induced perfect colorings Сиб. электрон. матем. изв., 8 (2011), 310-316

[6] L. Babai, "Spectra of Cayley graphs," J. Combin. Theory Ser. B 27 (1979), no. 2, 180–189.

[7] 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. (JEMS) 14 (2012), no. 3, 733-748.

[8] Bespalov, Evgeny A.; Krotov, Denis S.; Matiushev, Aleksandr A.; Taranenko, Anna A.; Vorob'ev, Konstantin V. Perfect 2-colorings of Hamming graphs. J. Combin. Des. 29 (2021), no. 6, 367-396.

[9] Bespalov, E.On the non-existence of extended 1-perfect codes and MDS codes. J. Comb. Theory, Ser. A 189, Article ID 105607, 11 p. (2022).

[10] Bierbrauer, J. Bounds on orthogonal arrays and resilient functions. J. Combin. Des. 3 (1995), no. 3, 179-183.

[11] Bierbrauer, J. Introduction to coding theory. Taylor & Francis Group, LLC, Second edition 2017.

[12] Bose, R. C. On the construction of balanced incomplete block designs. Ann. Eugenics 9 (1939), 353-399.

[13] 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. Canad. J. Math. 12 1960 189-203.

[14] Brouwer, A. E.; Cohen, A. M.; Neumaier, A. Distance-regular graphs. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 18. Springer-Verlag, Berlin, 1989. xviii+495 pp.

[15] A. E. Brouwer, C. D. Godsil, J. H. Koolen, and W. J. Martin. Width and dual width of subsets in polynomial association schemes. J. Comb. Theory, Ser. A, 102(2):255–271, 2003.

[16] Brouwer, Andries E.; Haemers, Willem H. Spectra of graphs. Universitext. Berlin: Springer (ISBN 978-1-4614-1938-9/hbk; 978-1-4614-1939-6/ebook). xiii, 250 p. (2012)

[17] Bruck R. H., Ryser H. J. The nonexistence of certain finite projective planes. Canad. J. Math. 1 (1949), 88-93.

[18] Camion P., Courteau B., Delsarte P. On r-partition designs in Hamming spaces. Appl. Algebra Engrg. Comm. Comput. 2 (1992), no. 3, 147-162.

[19] Canteaut A. Open problems related to algebraic attacks on stream ciphers // International workshop on coding and cryptography (WCC 2005) (Bergen, March 2005). Berlin: Springer, 2006. P. 1-11. (L ect. Notes in Comp. Sci.; Vol. 3969).

[20] C. Carlet "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.), pp. 257-397, 2010.

[21] C. Carlet. Boolean and vectorial plateaued functions, and APN functions. IEEE Transactions on Information Theory Vol. 61 no. 11, pp. 6272-6289, 2015

[22] C. Carlet and S. Mesnager. Four decades of research on bent functions. Special Jubilee Issue of Designs, Codes and Cryptography, Vol. 78, pp. 5-50, 2016

[23] C. Carlet "Boolean Functions for Cryptography and Coding Theory Monography, Cambridge University Press, 562 pages, 2020.

[24] Chowla S., Ryser H. J. Combinatorial problems. Canad. J. Math. 2 (1950), 93-99.

[25] G. Cohen, S. Litsyn, A. Vardy, and G. Zémor. Tilings of binary spaces. SIAM J. Discrete Math., 9(3), 393–412, 1996. DOI: 10.1137/S0895480195280137

[26] Courtois N., Meier W. Algebraic Attacks on Stream Ciphers with Linear Feedback // Proceedings of Eurocrypt 2003, Lecture Notes in Computer Sciences. 2003. V. 2656. P. 345 - 359.

[27] Delsarte, Philippe, Four fundamental parameters of a code and their combinatorial significance. Information and Control 23 (1973), 407-438.

[28] Delsarte, Philippe; Levenshtein, Vladimir I. Association schemes and coding theory. Information theory: 1948-1998. IEEE Trans. Inform. Theory 44 (1998), no. 6, 2477-2504.

[29] Denes, J.; Keedwell, A. D. Latin squares. New developments in the theory and applications. With contributions by G. B. Belyavskaya, A. E. Brouwer, T. Evans, K. Heinrich, C. C. Lindner and D. A. Preece. With a foreword by Paul Erdos. Annals of Discrete Mathematics, 46. North-Holland Publishing Co., Amsterdam, 1991. xiv+454 pp.

[30] K. Devriendt, P. Van Mieghem, Tighter spectral bounds for the cut size, based on Laplacian eigenvectors, Linear Algebra Appl. 572 (2019) 68–91.

[31] J. T. Ethier and G. L. Mullen, Strong forms of orthogonality for sets of hypercubes, Discrete Math. 312(12-13) (2012), 2050–2061.

[32] Etzion T., Vardy A. Perfect binary codes and tilings: problems and solutions // SIAM J. Discrete Math. 1998. V. 11. N 2. P. 205–223.

[33] Etzion T. Perfect Codes and Related Structures, World Scientific, 2022.

[34] D.G. Fon-Der-Flaass, "A bound on correlation immunity Сиб. электрон. матем. изв., 4 (2007), 133-135

[35] J. Friedman, On the bit extraction problem, in: Proc. 33rd IEEE Symposium on Foundations of Computer Science 1992, pp. 314-319.

[36] S. Glock, D. Kühn, A. Lo, and D. Osthus. The existence of designs via iterative absorption: hypergraph F-designs for arbitrary F. Mem. Amer. Math. Soc. 284 (2023), no. 1406, v+131 pp.

[37] Godsil, C. D. Equitable partitions. Combinatorics, Paul Erdos is eighty, Vol. 1, 173-192, Bolyai Soc. Math. Stud., Janos Bolyai Math. Soc., Budapest, 1993.

[38] Godsil, C. D. Algebraic combinatorics. Chapman and Hall Mathematics Series. Chapman & Hall, New York, 1993. xvi+362 pp.

[39] C. D. Godsil, Tools from linear algebra P. 1705–1748 in Handbook of combinatorics. Vol. 2. Edited by R. L. Graham, M. Grotschel and L. Lovasz. Elsevier Science B.V., Amsterdam; MIT Press, Cambridge, MA, 1995.

[40] Godsil C., Royle G. Algebraic graph theory. Graduate Texts in Mathematics, 207. Springer-Verlag, New York, 2001. xx+439 pp.

[41] C. Godsil and K. Meagher, Erdos-Ko-Rado Theorems: Algebraic Approaches. Cambridge University Press, 2016.

[42] Golay, Marcel J. E. (1949). "Notes on Digital Coding". Proc. IRE. 37: 657.

[43] K. Golubev, Graphical designs and extremal combinatorics, Linear Alg. Appl., 604 (2020), 490-506.

[44] Haemers, W. H. Eigenvalue techniques in design and graph theory. Dissertation, Technische Hogeschool Eindhoven, Eindhoven, 1979. Mathematical Centre Tracts, 121. Mathematisch Centrum, Amsterdam, 1980. v+102 pp. ISBN: 90-6196-194-7

[45] Haemers, W. H. Interlacing Eigenvalues and Graphs, Linear Algebra Appl. 226-228, 593-616 (1995).

[46] Hamming, R. W. Error detecting and error correcting codes. Bell System Tech. J. 29, (1950). 147-160.

[47] H. Hanani, On quadruple systems, Can. J. Math. 12 (1960), 145–157.

[48] Handbook of combinatorial designs / edited by Charles J. Colbourn, Jeffrey H. Dinitz. - 2nd ed. Boca Raton, FL : Chapman & Hall/Taylor & Francis, - Discrete mathematics and its applications. 2007. 984 p

[49] Hoffman, Alan J. On eigenvalues and colorings of graphs. 1970 Graph Theory and its Applications (Proc. Advanced Sem., Math. Research Center, Univ. of Wisconsin, Madison, Wis., 1969) pp. 79-91.

[50] Ji, Lijun; Yin, Jianxing Constructions of new orthogonal arrays and covering arrays of strength three. J. Combin. Theory Ser. A 117 (2010), no. 3, 236-247.

[51] Keevash P. The existence of designs, arXiv preprint arXiv:1401.3665, 2014 - arxiv.org

[52] Keevash P. The existence of designs II, arXiv preprint arXiv:1802.05900, 2018 - arxiv.org

[53] Kelly, Shane. Constructions of intriguing sets of polar spaces from field reduction and derivation. Des. Codes Cryptogr. 43 (2007), no. 1, 1-8.

[54] J. H. Koolen, W. S. Lee, W. J. Martin. Characterizing completely regular codes from an algebraic viewpoint, arXiv preprint arXiv:0911.1828 [math.CO]

[55] Krotov, Denis S. On weight distributions of perfect colorings and completely regular codes. Des. Codes Cryptogr. 61 (2011), no. 3, 315-329.

[56] D.S. Krotov. On the binary codes with parameters of triply-shortened 1-perfect codes, Designs, Codes, and Cryptography Volume 64, Issue 3, September 2012, Pages 275-283

[57] Krotov D. S. On calculation of the interweight distribution of an equitable partition. J. Algebraic Combin. 40 (2014), no. 2, 373-386.

[58] D. S. Krotov, I. Yu. Mogilnykh, V. N. Potapov. To the theory of q-ary Steiner and other-type trades. Discrete Mathematics, 339(3): 1150-1157, 2016.

[59] D. S. Krotov, V. N. Potapov, Completely regular codes and equitable partitions, in: Completely regular codes in distance-regular graphs, eds. Shi, M., Sole, P., Chapman & Hall/CRC, 2025. 1–84.

[60] Shi, M., Sole, P. eds. Completely regular codes in distance-regular graphs, Chapman & Hall/CRC, 2025. 1–84.

[61] Lam C. W. H., Kolesova G., Thiel L. A computer search for finite projective planes of order 9. Discrete Math. 92 (1991), no. 1-3, 187-195.

[62] Lam C. W. H., Thiel L., Swiercz S. The nonexistence of finite projective planes of order 10. Canad. J. Math. 41 (1989), no. 6, 1117-1123.

[63] Leighton F. T. Finite common coverings of graphs. J. Combin. Theory Ser. B. 1982. Vol. 33, No 3. P. 231-238.

[64] Lang S. Algebra, Graduate Texts in Mathematics, vol. 211 (2002) Revised third ed., New York: Springer-Verlag.

[65] V. I. Levenshtein, Universal bounds for codes and designs, Handbook of Coding Theory, V. S. Pless and W. C. Huffman, Eds., Elsevier, 1998, Ch. 6, 499-648.

[66] van Lint, J. H. Introduction to coding theory. Third edition. Graduate Texts in Mathematics, 86. Springer-Verlag, Berlin, 1999. xiv+227 pp.

[67] Lloyd, S. P. Binary block coding. Bell System Tech. J. 36 (1957), 517-535.

[68] Lovasz, L. Combinatorial problems and exercises. Corrected reprint of the 1993 second edition. AMS Chelsea Publishing, Providence, RI, 2007. 642 pp.

[69] S. L. Ma, A survey of partial difference sets, Designs, Codes and Cryptography vol. 4, P.221–261 (1994).

[70] Martin, W. J. Completely regular subsets. Thesis (Ph.D.)-University of Waterloo (Canada). 1992. 165 pp. ISBN: 978-0315-72488-4

[71] Mesnager, S. Bent functions. Fundamentals and results. Springer, [Cham], 2016. xxvi+544 pp.

[72] B. D. McKay, I. M. Wanless. A census of small latin hypercubes, SIAM J. Discrete Math. 22 (2008) 719-736.

[73] I. Yu. Mogilnykh, "Perfect codes from PGL(2,5) in Star graphs Сиб. электрон. матем. изв., 17 (2020), 534-539

[74] R. Montgomery. A proof of the Ryser-Brualdi-Stein conjecture for large even n, https://arxiv.org/pdf/2310.19779.pdf

[75] N. Nisan, M. Szegedy. On the degree of Boolean functions as real polynomials. Special issue on circuit complexity (Barbados, 1992). Comput. Complexity 4 (1994), no. 4, 301-313.

[76] Ostergerd, Patric R. J.; Pottonen, Olli; Phelps, Kevin T. The perfect binary one-error-correcting codes of length 15: Part II-properties. IEEE Trans. Inform. Theory 56 (2010), no. 6, 2571-2582.

[77] O. G. Parshina, M. A. Lisitsyna, "The perfect 2-colorings of infinite circulant graphs with a continuous set of odd distances Sib. Electron. Math. Reports, 17 (2020), 590-603

[78] Preparata, Franco P. A class of optimum nonlinear double-error-correcting codes. Inform. and Control 13, 378-400 (1968).

[79] Potapov, V. N. On perfect 2-colorings of the q-ary n-cube. Discrete Math. 312 (2012), no. 6, 1269-1272.

[80] Rao, R. C. Factorial experiments derivable from combinatorial arrangements of arrays. Suppl. J. Roy. Statist. Soc. 9, (1947). 128-139.

[81] Reiter, H. Stegeman, J. D. Classical harmonic analysis and locally compact groups. Second edition. London Mathematical Society Monographs. New Series, 22. The Clarendon Press, Oxford University Press, New York, 2000. xiv+327 pp.

[82] Rosa, A. Combinatorial designs with applications. Notes. Belianum, Vydavatel'stvo Univerzity Mateja Bela, Banska Bystrica, 2015. v+58 pp.

[83] Roth, R. M. Higher-order MDS codes. IEEE Trans. Inform. Theory 68 (2022), no. 12, 7798-7816.

[84] O. S. Rothaus. "On "Bent" Functions". Journal of Combinatorial Theory, Series A. 20 (3) (1976), 300-305.

[85] V. G. Ryabov, "Approximation of restrictions of q-valued logic functions to linear manifolds by affine analogues", Diskr. Mat., 32:4 (2020), 89-102; Discrete Math. Appl., 31:6 (2021), 409-419

[86] V. G. Ryabov, "Criteria for maximal nonlinearity of a function over a finite field", Diskr. Mat., 33:3 (2021), 79-91; Discrete Math. Appl., 33:2 (2023), 117-126

[87] P. Sarkar, "Spectral domain analysis of correlation immune and resilient Boolean fuctions", *Cryptology ePrint archive*, Report 2000/049, Sept.2000, 14 p.

[88] Shapiro, H. S.; Slotnick, D. L. On the mathematical theory of error-correcting codes. IBM J. Res. Develop. 3 1959 25-34.

[89] Skolem, Th. Some remarks on the triple systems of Steiner. Math. Scand. 6 (1958), 273-280.

[90] Solov'eva F. I. On perfect codes and related topics. Lecture Notes, Pohang University of Science and Technology, 2004

[91] Sotnikova E., Valyuzhenich A. Minimum supports of eigenfunctions of graphs: a survey // The Art of Discrete and Applied Mathematics DOI: https://doi.org/10.26493/2590-9770.1404.61e

[92] R. Michael Tanner, Explicit concentrators from generalized n-gons, SIAM J. Algebraic Discrete Methods 5(3) (1984) 287-293.

[93] T. Tao, "An uncertainty principle for cyclic groups of prime order", *Math. Res. Lett.*, vol.12(1), 2005, pp. 121–127.

[94] Taranenko A.A. Algebraic properties of perfect structures // Linear Algebra and Its Appl. V.607 P.286-306

[95] Taranenko A.A. Perfect colorings of hypergraphs, Linear Multilinear Algebra 73, No. 8, 1566-1590 (2025).

[96] Tarannikov, Y. On resilient Boolean functions with maximal possible nonlinearity. Progress in cryptology-INDOCRYPT 2000 (Calcutta), 19-30, Lecture Notes in Comput. Sci., 1977, Springer, Berlin, 2000.

[97] Tietavainen, A. On the nonexistence of perfect codes over finite fields. SIAM J. Appl. Math. 24 (1973), 88-96.

[98] Vasil'ev, Yu. L. On closely-packed nongroup codes. (Über dicht gepackte Nichtgruppen-Codes.) Probl. Kibern. 8, 337-339 (1962); German translation in Probl. Kybernetik 8, 375-378 (1965).

[99] Wanless, Ian M. Transversals in Latin squares: a survey. Surveys in combinatorics 2011, 403-437, London Math. Soc. Lecture Note Ser., 392, Cambridge Univ. Press, Cambridge, 2011.

[100] I. Wegener, The complexity of Boolean functions. Wiley-Teubner Series in Computer Science. John Wiley & Sons, Ltd., Chichester; B. G. Teubner, Stuttgart, 1987. xii+457.

[101] J. Wellens, "Relationships between the number of inputs and other complexity measures of Boolean functions," Discrete Analysis 19 (2022) 21 pp. arXiv:2005.00566v2

[102] Wilson, R. M. An existence theory for pairwise balanced designs. III. Proof of the existence conjectures. J. Combinatorial Theory Ser. A 18 (1975), 71-79.

[103] С. В. Августинович, "Об одном свойстве совершенных двоичных кодов Дискретн. анализ и исслед. опер., 2:1 (1995), 4-6.

[104] С. В. Августинович, И. Ю. Могильных, "Совершенные раскраски графов Джонсона $J(8,3)$ и $J(8,4)$ в два цвета Дискретн. анализ и исслед. опер., 17:2 (2010), 3-19

[105] Банаи Э., Ито Т. Алгебраическая комбинаторика. Схемы отношений. М.: Мир, 1987.

[106] Л. А. Бассалыго, В. А. Зиновьев, В. К. Леонтьев, Н. И. Фельдман, "Несуществование совершенных кодов для некоторых составных алфавитов Пробл. передачи информ., 11:3 (1975), 3-13;

[107] А. Ю. Васильева, "Локальные и межвесовые спектры вполне регулярных кодов и совершенных раскрасок Пробл. передачи информ., 45:2 (2009), 84-90; Problems Inform. Transmission, 45:2 (2009), 151-157

[108] А. Ю. Васильева, "О реконструктивных множествах вершин в булевом кубе Дискретн. анализ и исслед. опер., 19:1 (2012), 3-16; J. Appl. Industr. Math., 6:3 (2012), 393-402

[109] А. Ю. Васильева, "Восстановление собственных функций q-ичного n-мерного гиперкуба Пробл. передачи информ., 51:3 (2015), 31-40; Problems Inform. Transmission, 51:3 (2015), 231-239

[110] Васильев Ю. Л. О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Физматгиз, 1962. Вып. 8. С. 337-339.

[111] Б. Ю. Вейсфейлер, А. А. Леман, Приведение графа к каноническому виду и возникающая при этом алгебра, НТИ, сер.2, (1968), 9, 12-16.

[112] В. Г. Визинг. Об оценке хроматического класса p-графа // сб. Дискретный анализ. - Новосибирск: Институт математики СО АН СССР, 1964. - Вып. 3. - С. 25-30.

[113] В. Г. Визинг, "Дистрибутивная раскраска вершин графа Дискретн. анализ и исслед. опер., 2:4 (1995), 3-12

[114] С.Г. Влэдуц, Д.Ю. Ногин, М.А. Цфасман, Алгеброгеометрические коды. Основные понятия, МЦНМО, М., 2003

[115] Дельсарт Ф., Алгебраический подход к схемам отношений теории кодирования, Мир, М., 1976

[116] Городилова А.А, Токарева Н.Н., Шушуев Г.И. Криптография и криптоанализ. Сборник задач: учебное пособие., Новосиб. гос. ун-т, Новосибирск, 2014, 325 с.

[117] В. А. Зиновьев, В. К. Леонтьев, "О совершенных кодах Пробл. передачи информ., 8:1 (1972), 26-35

[118] Зиновьев В. А., Леонтьев В. К. Несуществование совершенных кодов над полями Галуа // Проблемы управления и теории информации. - 1973. Т. 2, № 2. - С. 123-132.

[119] Г. И. Ивченко, Ю. И. Медведев, В. А. Миронова, Многочлены Кравчука и их применения в задачах криптографии и тео- рии кодирования, Матем. вопр. криптогр., 2015, том 6, вы- пуск 1, 33-56

[120] Камерон П., ван Линт Дж. Теория графов, теория кодирования и блок-схемы. М.: Наука, 1980.

[121] Т. Е. Киреева, "Совершенные ориентационные раскраски кубических графов Сиб. электрон. матем. изв., 15 (2018), 1353-1360.

[122] М. А. Лисицына, С. В. Августинович, "Совершенные раскраски призмы Сиб. электрон. матем. изв., 13 (2016), 1116-1128.

[123] М. С. Лобанов, "Точные соотношения между нелинейностью и алгебраической иммунностью Дискретн. анализ и исслед. опер., 15:6 (2008), 34-47

[124] Логачёв О.А., Сальников А.А., Смышляев С.В., Ященко В.В., Булевы функции в теории кодирования и криптологии, 2-е изд., МЦНМО, М., 2012, 584 с.

[125] Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А., Теория кодов, исправляющих ошибки, Связь, М., 1979

[126] А. А. Марков. Избранные труды. Том 2. Теория алгорифмов и конструктивная математика, математическая логика, информатика и смежные вопросы. М.: МЦНМО, 2007.

[127] Моррис С., Двойственность Понтрягина и строение локально компактных абелевых групп. М.: Мир, 1980.

[128] В. Н. Потапов, С. В. Августинович, "Комбинаторные дизайны, разностные множества и бент-функции как совершенные раскраски графов и мультиграфов Сиб. матем. журн., 61:5 (2020), 1087-1100

[129] С. А. Пузынина, "Периодичность совершенных раскрасок бесконечной прямоугольной решетки Дискретн. анализ и исслед. опер., сер. 1, 11:1 (2004), 79-92

[130] Ромащенко А.Е., Румянцев А.Ю., Шень А. Заметки по теории кодирования. 2-е изд., испр. и доп. М.: МЦНМО, 2017. 88 с.

[131] Сидельников В.М. Теория кодирования. М.:Физматлит, 2008.

[132] Соловьёва Ф.И., Введение в теорию кодирования, Учеб. пособие, Новосибирск. гос. ун-т, Новосибирск, 2006, 124 с.

[133] Таранников Ю.В. О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Выпуск 11. М.: Физматлит. 2002. С. 91–148.

[134] Таранников Ю.В., Комбинаторные свойства дискретных структур и приложения к криптологии, МЦНМО, М., 2011, 152 с.

[135] Таранников Ю.В., Дискретная математика. Задачник. Учебное пособие для академического бакалавриата. М.: Юрайт, ISBN 978-5-9916-6283-3, 2016, 385 с.

[136] Токарева Н.Н., Симметричная криптография, Краткий курс: учебное пособие, Новосиб. гос. ун-т, Новосибирск, 2012, 234 с.

[137] Д.Г. Фон-Дер-Флаасс, "Совершенные 2-раскраски гиперкуба Сиб. матем. журн., 48:4 (2007), 923-930; Siberian Math. J., 48:4 (2007), 740-745

[138] А. В. Халявин, "Оценка мощности ортогональных массивов большой силы Вестн. Моск. ун-та. Сер. 1. Матем., мех., 2010, № 3, 49-51

[139] Д. Б. Хорошилова, "О параметрах совершенных 2-раскрасок циркулянтных графов Дискретн. анализ и исслед. опер., 18:6 (2011), 82-89

[140] Хэмминг Р. В. Теория кодирования и теория информации: Пер. с англ. - М.: Радио и связь, 1983. - 176 с.

[141] Цветкович Д., Дуб М., Захс Х., Спектры графов: теория и применение, Наук. думка, Киев, 1984