ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НОВОСИБИРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

На правах рукописи

Беспалов Евгений Андреевич

Методы алгебраической теории графов в исследовании МДР кодов

01.01.09 — дискретная математика и
математическая кибернетика

Диссертация на соискание ученой степени кандидата
физико-математических наук

Научный руководитель —
д.ф.-м.н.
Д. С. Кротов

Новосибирск 2018

Оглавление

Введение

Актуальность темы. Тема исследования данной работы лежит на стыке алгебраической комбинаторики, теории кодирования и теории графов.

При исследовании комбинаторных объектов в графах, как правило, решаются такие задачи, как вопрос существования объектов с данными параметрами, нахождение и улучшение нижних и верхних оценок на число таких объектов, описание всех объектов с заданными параметрами и построение объектов с дополнительными свойствами.

Пусть дан некоторый граф G (простой неориентированный граф без петель и кратных ребер). *Кодом* в графе называется произвольное подмножество множества вершин графа. Вершины подмножества будем называть *кодовыми*, а *кодовым расстоянием* — минимальное расстояние между двумя различными кодовыми вершинами. Код, состоящий из одной вершины либо всех вершин графа, назовем *тривиальным*. Остальные коды назовем *нетривиальными*. Возникает естественная задача нахождения кодов в заданном графе с фиксированным расстоянием и наибольшей возможной мощностью.

Можно с уверенностью сказать, что наиболее важным графом в теории кодирования является граф Хэмминга. Граф Хэмминга можно определить следующим образом: рассмотрим метрическое пространство E_q^n с носителем, состоящим из слов длины n в алфавите $\{0, \ldots, q-1\}$, т.е. множество $\{0, \ldots, q-1\}^n$, где расстояние между двумя словами равно количеству позиций, в которых данные слова различаются. Данному метрическому пространству соответствует граф Хэмминга $H(n, q)$, в котором вершины — это слова длины n, и две

вершины смежны тогда и только тогда, когда расстояние между ними равно 1. В случае, когда $q = p^n$ — степень простого числа, множество слов E_q^n можно представить как векторное пространство над полем $GF(q)$. Если некоторый код C является линейным подпространством, то он называется *линейным*. В связи с этим при исследовании кодов в графах Хэмминга особое внимание уделяется именно этому случаю.

Существует ряд известных оценок на мощность кода в графе Хэмминга: граница Хэмминга, граница Синглтона, граница Варшамова-Гилберта и т.д. Рассмотрим две важные границы.

Начнем с границы Хэмминга. Пусть в графе $H(n, q)$ дан код C с кодовым расстоянием $d = 2\rho + 1$. Ричард Хэмминг установил, что

$$|C| \leq \frac{q^n}{1 + (q-1)C_n^1 + \ldots + (q-1)^\rho C_n^\rho}.$$

Если мощность кода достигает этой границы, то он называется *ρ-совершенным* или просто *совершенным* кодом с расстоянием $d = 2\rho+1$. В 1973 году Зиновьев, Леонтьев [58] и независимо Тиетвайнен [42] установили, что в случае, когда $q = p^n$ — степень простого числа, любой нетривиальный совершенный код в графе Хэмминга $H(n, q)$ должен иметь те же параметры (т. е. длину, мощность и кодовое расстояние), что и один из кодов Хэмминга, либо один из двух кодов Голея [18], либо код с повторением. В случае, когда q не равно степени простого числа, вопрос существования совершенных кодов остается открытым.

Второй важной границей является граница Синглтона, названная в честь Ричарда Синглтона. В [40] показано, что если в графе $H(n, q)$ дан код C с кодовым расстоянием d, то мощность $|C| \leq q^{n-d+1}$. Код, в котором достигается граница Синглтона, называется *МДР кодом* (в англоязычной литературе maximum distance separable code или сокращенно MDS code). Параметры такого кода обозначим через $(n, q^k, d)_q$. Одним из известных примеров МДР кодов являются коды Рида-Соломона.

МДР коды связаны с одним известным классом алгебраических объектов. Пусть Σ — конечное множество, состоящее из q элементов. *n-Арной квазигруппой* порядка q называется функция $f : \Sigma^n \to \Sigma$ такая, что в уравнении $x_0 = f(x_1, \ldots, x_n)$ по значениям любых n переменных из $x_0, \ldots, x_n$ однозначно восстанавливается значение оставшейся переменной (строго говоря n-арной квазигруппой считается пара (Σ, f), но мы будем пользоваться общепринятым упрощением терминологии). В качестве примера n-арной квазигруппы можно привести функцию

$$g(x_1, \ldots, x_n) = x_1 + \ldots + x_n \mod q.$$

Также удобно представлять квазигруппу как предикат $Q < x_0, x_1, \ldots, x_n >$, истинный на всех наборах значений, удовлетворяющих уравнению $f(x_1, \ldots, x_n) = x_0$. Множество вершин, соответствующее такому предикату, является МДР кодом с расстоянием 2 в графе $H(n+1, q)$. Более того, если C — МДР код в графе $H(n, q)$ с расстоянием d, то кодовые слова кода C можно представить в виде

$$\{(x_1, \ldots, x_{n-d+1}, f_1(x_1, \ldots, x_{n-d+1}), \ldots, f_{d-1}(x_1, \ldots, x_{n-d+1})) : x_j \in \{0, \ldots, q-1\}\},$$

где $f_i(x_1, \ldots, x_{n-d+1})$ — $(n-d+1)$-арная квазигруппа для любого $i = 1, \ldots, d-1$.

В 1960-е n-арные квазигруппы интенсивно изучались В. Д. Белоусовым и его научной школой (см. например [48], [47]). В настоящее время изучение квазигрупп вызывает интерес в связи с их приложениями в теории кодирования [60], [19], [36] и криптографии [37], [53]. С другой стороны, n-арные квазигруппы также известны в комбинаторике как латинские гиперкубы (многомерные обобщения латинских квадратов), а $(n, q^k, d)_q$ МДР код можно представить как систему ортогональных латинских гиперкубов. О применении латинских квадратов см. например [13].

В общем случае вопрос существования и классификации МДР кодов в гра-

фах Хэмминга остается открытым, однако существуют результаты для небольших значений q. Если $k = 2$, то $(d + 1, 4^2, d)_q$ МДР код можно представить как систему ортогональных латинских квадратов порядка q. Ян Уонлесс и Дж. Иган [14] с помощью компьютерных вычислений классифицировали все такие системы для $q \leq 9$. Т. Л. Алдерсон [2] показал, что коды с параметрами $(6, 4^3, 4)_4$ и $(5, 4^3, 3)$ единственны с точностью до эквивалентности. О классификации МДР кодов при $q = 5, 7, 8$ см. [22], [24], [23]. Также стоит отметить известную гипотезу о том, что если существует линейный (n, q^k, d) МДР код при $2 < d < n$, то $n \leq q + 1$, за исключением случая, когда q — степень 2 и $k = 3$ либо $k = q - 1$. Тогда $n \leq q + 2$. Существенное продвижение в доказательстве получено С. Болом и Дж. Де Бойлем в работах [5], [6], [7], в которых гипотеза была доказана для простых q, а в случае, когда $q = p^n$ — степень простого числа, гипотеза доказана для всех $k \leq 2p - 2$. Также в ряде работ получены результаты по классификации латинских гиперкубов с малыми n и q [34], [57], [21], [20], [33].

n-Арная квазигруппа называется *разделимой*, если ее можно представить в виде бесповторной суперпозиции двух квазигрупп меньшей арности, т.е.

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

где g — m-арная квазигруппа, h — $(n-m+1)$-арная квазигруппа, σ — некоторая перестановка и $m \in \{2, \ldots, n-1\}$. В противном случае n-арная квазигруппа называется *неразделимой*. Вопрос при каких n и q существуют неразделимые n-арные квазигруппы ставился еще В. Д. Белоусовым [47]. Эта задача исследовалась во многих работах ([48], [49], [52], [54], [55], [65], [1]) и была окончательно решена в работе [31], где были построены неразделимые n-арные квазигруппы порядка q для всех $q \geq 4$ и $n \geq 3$.

При $q = 3$ существует единственная с точностью до изотопии (перестановки элементов носителя квазигруппы независимо в каждой координате) n-арная квазигруппа [16]. Единственный нетривиальный порядок с точки зрения харак-

теризации квазигрупп, для которого полностью охарактеризованы все n-арные квазигруппы, — это $q = 4$. Д. С. Кротов и В. Н. Потапов [29] доказали, что любая n-арная квазигруппа порядка 4 разделима либо полулинейна. Также в работе [62] была найдена асимптотика числа n-арных квазигрупп порядка 4, при этом было показано, что класс полулинейных квазигрупп асимптотически более мощный, чем класс разделимых квазигрупп. Тем самым вызывает интерес задача исследования и описания неразделимых n-арных квазигрупп порядка $q > 4$.

Так как n-арная квазигруппа $f(x_1, \ldots, x_n)$ обратима в каждой позиции, то для любого i от 1 до n существует n-арная квазигруппа $f^i(x_1, \ldots, x_{i-1}, x_0, x_{i+1}, \ldots, x_n$ обратная ей в i-й позиции. Таким образом, уравнения $x_0 = f(x_1, \ldots, x_n)$ и $x_i = f^i(x_1, \ldots, x_{i-1}, x_0, x_{i+1}, \ldots, x_n)$ эквивалентны. Если в n-арной квазигруппе f или в одном из ее обращений f^i вместо некоторых k переменных подставить константы, то полученную $(n-k)$-арную квазигруппу назовем $(n-k)$-*арным* ретрактом.

Для произвольного кода C в графе Хэмминга $H(n, q)$ определим *проекцию* $C_{i_1,\ldots,i_k}$ и *сечение* $C^{a_1,\ldots,a_k}_{i_1,\ldots,i_k}$ следующим образом:

$C_{i_1,\ldots,i_k} = \{x_1, \ldots, x_{i_1-1}, x_{i_1+1}, \ldots, x_{i_k-1}, x_{i_k+1}, \ldots, x_n) :$

$$\exists(a_1, \ldots, a_k)(x_1, \ldots, x_{i_1-1}, a_1, x_{i_1+1} \ldots, x_{i_k-1}, a_{i_k} x_{i_k+1}, \ldots, x_n) \in C\}.$$

$C^{a_1,\ldots,a_k}_{i_1,\ldots,i_k} = \{x_1, \ldots, x_{i_1-1}, x_{i_1+1} \ldots, x_{i_k-1}, x_{i_k+1}, \ldots, x_n) :$

$$(x_1, \ldots, x_{i_1-1}, a_1, x_{i_1+1} \ldots, x_{i_k-1}, a_{i_k} x_{i_k+1}, \ldots, x_n) \in C\}.$$

У МДР кодов есть одно замечательное свойство: проекция или сечение МДР кода также является МДР кодом. Это дает возможность при описании квазигрупп и МДР кодов использовать индукцию, постепенно увеличивая диаметр графа и пользуясь тем, что некоторая проекция или некоторое сечение МДР кода либо некоторый ретракт квазигруппы принадлежат уже охарактеризован-

ному множеству.

В статье [30] был доказан признак разделимости квазигрупп, использующий разделимость ретрактов, а именно: если в n-арной квазигруппе, $n \geq 4$, все $(n-1)$-арные и $(n-2)$-арные ретракты разделимы, то и сама квазигруппа разделима. Более того, в той же работе данный признак был усилен для простых значений q, а именно: если в n-арной квазигруппе f простого порядка q все $(n-1)$-арные ретракты разделимы, то и сама квазигруппа f разделима. Возникает вопрос: для каких еще порядков квазигруппы верен усиленный признак разделимости? Квазигруппу, для которой этот признак не верен (т.е. такую n-арную квазигруппу, которая неразделима, но у которой все $(n-1)$-арные ретракты разделимы), назовем *критической*, . Допустим, для некоторого q мы хотим охарактеризовать все неразделимые квазигруппы порядка q из некоторого класса, в котором не существует критических квазигрупп. Предположим, мы сформулировали некоторую гипотезу о строении произвольной неразделимой n-арной квазигруппы и хотим ее доказать. Тогда фиксацией некоторой переменной из исходной квазигруппы получается неразделимый $(n-1)$-арный ретракт, для которого утверждение гипотезы верно.

Подобные рассуждения применялись при характеризации квазигрупп порядка 4. Была сформулирована гипотеза о том, что каждая n-арная квазигруппа разделима или полулинейна. В статье [62] было доказано, что если f — неразделимая n-арная квазигруппа порядка 4, у которой имеется неразделимый $(n-1)$-арный ретракт, то квазигруппа f — полулинейна. А в статье [26] для всех четных n были построены критические n-арные квазигруппы порядка 4, в связи с чем в работе [29] пришлось доказывать гипотезу отдельно для критических квазигрупп, пользуясь более слабым признаком разделимости и индукционным шагом длины 2.

Возникает вопрос: для каких q существуют критические квазигруппы? В работе [61] Д. С. Кротовым был предложен метод, позволяющий строить критические квазигруппы порядка 4, используя схожее понятие свитчинговой раз-

делимости по модулю 2 для графов. Позже в статье [II] им был обобщен этот метод, а именно, для произвольного простого значения q описана конструкция, которая позволяет построить критическую квазигруппу порядка q^2 по графу, который также является критическим в терминах свитчинговой разделимости по модулю q.

Изложим вкратце суть данного метода. Будем рассматривать неориентированные графы с ребрами, помеченными элементами из множества $\{1, \ldots, q-1\}$, $q \geq 2$. Такой граф можно представить парой (V, E), где V — множество вершин, а $E : V^2 \to \{0, 1, \ldots, q-1\}$, причем $E(v, v) = 0$ для любой вершины $v \in V$ и для любых различных u, v условие $E(u, v) = 0$ означает отсутствие ребра.. Результатом сложения двух графов (V, E_1) и (V, E_2) на одном и том же множестве вершин будет граф (V, E), где $E(u, w) = E_1(u, w) + E_2(u, w) \mod q$ для любых вершин u, w из V. Граф называется *аддитивным*, если его вершины можно пометить элементами из $\{0, 1, \ldots, q-1\}$ так, что вес пары (u, w) определяется как сумма меток вершин u и w для любых вершин u и w. Свитчингом графа G называется результат сложения этого графа с некоторым аддитивным графом. Множество вершин W назовем отделимым, если в некотором свитчинге между вершинами из множеств W и $V \backslash W$ все ребра имеют вес 0, а граф называется свитчингово разделимым, если у него есть отделимое множество U такое, что $2 \leq |U| \leq n-2$. Для свитчинговой разделимости графов можно поставить аналогичный вопрос, как и для разделимости n-арных квазигрупп: для каких q существует неразделимый граф такой, что удаление любой вершины приводит к разделимому графу? Такие графы назовем критическими.

Опишем теперь построение критических квазигрупп по критическим графам. Пусть q — простое число. Частичной функцией назовем функцию $f^{[a]} : \Sigma_a \to Z_q$, где $\Sigma_a = \{(x_1, \ldots, x_n, x_0) : x_1 + \ldots + x_n + x_0 = a\}$. Функцию $f^{[a]}$ назовем расширением всюду определенной функции $f : Z_q^n \to Z_q$, если $f^{[a]}(x_1, \ldots, x_n, x_0) = f(x_1, \ldots, x_n)$, где $x_0 = a - \sum_1^n x_i$. Пусть $C = \{c_1, \ldots, c_k\}$, где $c_1 < \ldots < c_k$. Обозначим $x_C = (x_{c_1}, \ldots, x_{c_k})$. Расширенную функцию $f^{[a]}$

назовем W-разделимой, если $f(x_1, \ldots, x_n, x_0) = f'(x_W) + f''(x_U)$, где $U = \{0, 1, \ldots, n\} \backslash W$. Если для некоторого множества аргументов W такого, что $2 \leq |W| \leq n-1$, функция $f^{[a]}$ — W-разделима, то $f^{[a]}$ назовем разделимой. Частичную функцию $f^{[a]}$ от $n+1$ переменной назовем квадратичной, если существует квадратичная всюду определенная функция от $n+1$ переменной, совпадающая с $f^{[a]}$ на области определения Σ_a. Пусть дан граф $G(V, E)$, где $V = \{0, 1, \ldots, n\}$, $E : V^2 \to \{0, 1, \ldots, q-1\}$. Графу G можно сопоставить квадратичный многочлен, у которого коэффициент при $x_i x_j$ равен весу ребра (i, j). Рассмотрим множество пар $\Sigma = \{[a, b] : a, b \in Z_q\}$. Для произвольной функции $f : Z_q^n \to Z_q$ и константы $a \in Z_q$ на носителе Σ определим квазигруппу Q_f порядка q^2 следующим образом:

$$Q_{f,a}([x_1, y_1], \ldots, [x_n, y_n]) = [-\sum_1^n x_i + a][-\sum_1^n y_i + f(x_1, \ldots, x_n)].$$

В статье [II] Д. С. Кротовым было доказано, что n-арная квазигруппа $Q_{f,a}$ разделима тогда и только тогда, когда разделима частичная функция $f^{[0]}$, а квадратичная частичная функция разделима тогда и только тогда, когда разделим граф, построенный по соответствующему квадратичному многочлену. Более того, квазигруппа $Q_{f,a}$ является критической тогда и только тогда, когда соответствующий граф также является критическим.

С теорией кодирования связан еще один комбинаторной объект. Совершенной раскраской в k цветов графа G с матрицей параметров $(s_{ij})_{k \times k}$ называется такая раскраска вершин графа, что любая вершина цвета i смежна ровно с s_{ij} вершинами цвета j. Раскраску графа $G(V, E)$ в k цветов удобно представлять как функцию $f : V \to \{0, \ldots, k-1\}$. Совершенный код с расстоянием 3 в графе $H(n, q)$ эквивалентен совершенной раскраске в 2 цвета с матрицей параметров $\begin{bmatrix} 0 & n(q-1) \\ 1 & n(q-1)-1 \end{bmatrix}$, а МДР код в графе $H(n, q)$ с расстоянием 2 эквивалентен совершенной раскраске в 2 цвета с матрицей параметров $\begin{bmatrix} 0 & n(q-1) \\ n & n(q-2) \end{bmatrix}$. Совершенные раскраски исследовались во многих графах, приведем лишь малую часть

работ: [64], [51], [3], [63], [46], [4], [17].

В [12] Ф. Дельсарт ввел понятие полностью регулярного кода, обобщающее понятие совершенного кода. Множество вершин C графа G называется полностью регулярным кодом радиуса ρ, если дистанционное разбиение вершин по отношению к C является совершенной раскраской в $\rho+1$ цвет. Такая совершенная раскраска имеет трехдиагональную матрицу параметров, некоторую (s_{ij}), а множество значений $[s_{0,1}, s_{1,2}, \ldots, s_{\rho-1,\rho}, s_{1,0}, \ldots, s_{\rho,\rho-1}] = [b_0, \ldots, b_{p-1}, c_1, \ldots, c_\rho]$ называется массивом пересечений. В этих терминах можно определить дистанционно регулярные графы. Связный граф G называется *дистанционно-регулярным*, если любая его вершина является полностью регулярным кодом, и массив пересечений не зависит от выбора вершины.

Различные коды, совершенные раскраски и другие комбинаторные объекты исследуются и в графах, отличных от графа Хэмминга. Наибольший интерес вызывают дистанционно-регулярные графы ввиду возможности использования аппарата алгебраической теории графов. Например, вопрос существования совершенных кодов изучался в графах Грассмана, графах Джонсона и графах билинейных форм. Известно, что в графах Грассмана и в графах билинейных форм не существует нетривиальных совершенных кодов [10], [32], а гипотеза Дельсарта [56] о несуществовании нетривиальных совершенных кодов в графах Джонсона до сих пор не доказана и не опровергнута. О полностью регулярных кодах в дистанционно-регулярных графах см. например в [44]. Одной из немногих известных серий дистанционно-регулярных графов сколь угодно большого диаметра являются графы Дуба. Известно, что для всех q, отличных от 4, единственный сильно регулярный граф с параметрами $(q^2, 2(q-1), q-2, 2)$ — это граф Хэмминга $H(2, q)$ (граф G называется *сильно регулярным* с параметрами (v, k, λ, μ), если G — регулярный граф степени k на v вершинах, и любая пара смежных вершин имеет λ общих соседей, а любая пара несмежных вершин имеет μ общих соседей). Единственный граф с такими параметрами, неизоморфный графу Хэмминга, был найден в случае $q = 4$ в 1959 году Ш.

Шрикханде [39]. Причем $q = 4$ — это также единственный случай, когда граф Хэмминга $H(n, q)$ не определяется как дистанционно-регулярный граф с данным массивом пересечений. Другой пример дистанционно-регулярного графа с тем же массивом пересечений, что и граф Хэмминга $H(N, 4)$, — это граф Дуба $D(m, n)$, где $N = 2m + n$. Причем графы Дуба — это единственное исключение [15], т.е. если граф G — дистанционно-регулярный, имеющий тот же массив пересечений, что и граф Хэмминга $H(N, 4)$, но неизоморфный ему, то тогда G — граф Дуба. Обозначим через $D(m, n)$ граф, являющийся декартовым произведением m копий графа Шрикханде и n копий полного графа K_4. Тогда при $m > 0$ граф $D(m, n)$ называется графом Дуба. Некоторые коды уже изучались в графах Дуба. Известно, что нетривиальный ρ-совершенный код в графе Дуба $D(m, n)$ (в графах Дуба код называется ρ-совершенным, если вершины графа можно разбить на непересекающиеся шары радиуса ρ с центрами в кодовых вершинах) может существовать, только если $\rho = 1$ и диаметр можно представить в виде $2m+n = \frac{4^l-1}{3}$ (см. например [25]). В [25] Дж. Кулен и А. Мунемаса построили совершенный код в графе $D(1, 3)$ и совершенный код в графе $D(2, 1)$, а в работе [27] Д. С. Кротов построил совершенные коды для асимптотически двух третей значений (m, n), удовлетворяющих $2m + n = \frac{4^l-1}{3}$. Также в работах [27], [38] изучаются совершенные коды в графах Дуба, линейные над кольцом Галуа $GR(4^2)$ либо аддитивные. В графах Дуба $D(m, n)$ для кода C с расстоянием d можно установить границу на мощность кода, аналогичную границе Синглтона для графов Хэмминга, а именно: $|C| \leq 4^{2m+n-d+1}$, что в точности совпадает с границей на мощность кода с расстоянием d в графе Хэмминга $H(2m + n, 4)$. По аналогии назовем код, мощность которого достигает данной границы, *МДР кодом*. Возникает вопрос, при каких параметрах существует МДР коды в графах Дуба, и задача характеризации всех МДР кодов в графах Дуба. Задача описания МДР кодов с кодовым расстоянием 2 рассмотрена отдельно в работе [28], в которой была обобщена на графы Дуба характеризация МДР кодов с расстоянием 2 в графах Хэмминга $H(n, 4)$, полученная в [29]. Данная работа не

включена в диссертацию, так как основные результаты принадлежат соавтору.

Многие комбинаторные объекты в графах связаны с собственными функциями, заданными на этих графах. Например, совершенные раскраски. Пусть $f : V \to \{0, 1\}$ — совершенная раскраска некоторого графа $G(V, E)$ с матрицей параметров $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Совершенной раскраске f соответствует собственная функция g с собственным значением $(a - c)$, определенная следующим образом:

$$g(x) = \begin{cases} b, & g(x) = 0, \\ -c, & g(x) = 1. \end{cases}$$

В частности, если C — МДР код с расстоянием 2 в графе Дуба $D(m, n)$, то функция f, определенная следующим образом:

$$f(x) = \begin{cases} 3, & x \in C, \\ -1, & \text{иначе}, \end{cases}$$

является собственной функцией с минимальным собственным значением $-2m-n$. С другой стороны, если f — собственная функция графа $D(m, n)$ с собственным значением $-2m-n$ и множеством значений $\{3, -1\}$, то множество вершин, на которых значение функции равно 3, является МДР кодом с расстоянием 2.

Изучение некоторых комбинаторных конфигураций зачастую приводит к рассмотрению разности двух конфигураций из одного и того же класса. Для двух совершенных раскрасок с одной и той же матрицей параметров $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ такую разность можно представить как разность соответствующих собственных функций. Эта разность — собственная функция со значениями из множества $\{(b+c), -(b+c), 0\}$. Рассмотрение разности может быть полезно при построении новых объектов с теми же самыми параметрами либо при нахождении границы на число таких объектов. Для некоторых других комбинаторных конфигураций такая разность принадлежит к числу объектов, известных как трейды, которые

также в ряде случаев связаны с $\{0, \pm 1\}$ собственными функциями. Подробнее о трейдах см. в [59]. В свете этого вызывает интерес задача нахождения собственных функций с минимальным возможным носителем. В настоящий момент известны некоторые оценки и точные значения для минимальной возможной величины носителей собственных функций в графах Хэмминга [43], [50], графах Джонсона [45], графах Пэйли [35], кубических дистанционно-регулярных графах [41].

Публикации. По теме диссертации автором опубликовано 5 работ, в том числе 4 статьи из списка ВАК (работы [I], [II], [III], [IV]) и одна работа в трудах конференции [V].

Апробация работы. Результаты работы докладывались на Десятой молодежной научной школе по дискретной математике и ее приложениям (Москва, 2015). Также результаты докладывались на совместном русско-японском семинаре «The First Russian-Japanese mini-workshop on Algebraic combinatorics» (Новосибирск, 2016). Кроме того, результаты неоднократно докладывались на семинарах «Теория кодирования», «Квазигруппы и смежные вопросы», «Дискретный анализ» Института математики им. С. Л. Соболева СО РАН.

Научная новизна. Основные результаты диссертации являются новыми и состоят в следующем:

1. Получена характеризация всех свитчингово неразделимых графов таких, что удаление любой вершины графа приводит к свитчингово разделимому графу. Как следствие, верен аналогичный результат для МДР кодов, построенных на основе графов.

2. Описаны все МДР коды в графах Дуба с кодовым расстоянием $d \geq 3$. Показано, что число классов эквивалентности МДР кодов с расстоянием, равным диаметру графа, растет как полином третьей степени, и существует 10 классов эквивалентности МДР кодов с меньшим расстоянием.

3. Получена характеризация всех собственных функций графа Дуба с наи-

меньшей мощностью носителя для минимального собственного значения и второго по величине собственного значения.

Первая глава посвящена свитчинговой разделимости графов по модулю q (далее просто разделимости). Все необходимые определения приведены в параграфе 1.1. Целью в данной главе является описание всех таких неразделимых графов, что удаление любой вершины приводит к разделимому графу (назовем такие графы критическими). В параграфе 1.1 сформулированы и доказаны несколько необходимых утверждений о разделимых графах, а также о связи разделимости графа с разделимостью его подграфов. Также в следствии 4 доказан признак разделимости графов, а именно то, что если в графе G порядка n все подграфы порядков $n-1$ и $n-2$ разделимы, то и сам граф G разделим. Доказательство признака разбито на предложения 1 и 2.

В параграфе 1.2 для четных q и нечетных n определен класс графов $G_{n,\gamma}$, где $\gamma \in \{0, \ldots, q-1\}$. Основной результат сформулирован в теореме 1, в которой утверждается, что любой неразделимый граф порядка $n \geq 6$ такой, что при удалении любой его вершины получается разделимый граф, изоморфен некоторому свитчингу графа $G_{n,\gamma}$. В предложении 3 отдельно рассмотрен случай $n = 5$. В предложении 4 доказано, что граф $G_{n,\gamma}$ — критический.

Вторая глава посвящена МДР кодам в графах Дуба. В параграфе 2.1 приведены необходимые определения, а также ряд утверждений, используемых при доказательстве основного результата. Основной результат приведен в теореме 2, где найдено число всех с точностью до эквивалентности МДР кодов в графе Дуба $D(m, n)$ с кодовым расстоянием $d = 2m+n-k+1$ для всех m, n и $d \geq 3$. Это число обозначено через $L_{m,n,k}$. Доказательство разбито на предложения 5-11. В приложении в явном виде приведены все с точностью до эквивалентности МДР коды в графах Дуба с кодовым расстоянием $2 < d < 2m + n$.

Третья глава посвящена минимальным носителям собственных функций графов Дуба. В главе рассматриваются собственные функции графов Дуба со

вторым по величине и минимальным собственным значениями. В параграфе 3.1 приведены все необходимые определения. Определение графа Дуба приведено в главе 2. Основные результаты сформулированы в теоремах 3 и 4. Доказательство теоремы 3 проводится по индукции, в качестве базы используя аналогичный результат из [43] для собственных функций в графах Хэмминга со вторым по величине собственным значением. Для шага индукции используются следствие 8 и лемма 30.

Автор выражает глубокую благодарность и признательность своему научному руководителю Кротову Денису Станиславовичу за интересные постановки задач, постоянное внимание и всестороннюю поддержку. Также автор благодарит участников семинара «Теория кодирования» за полезные замечания и внимание к работе.

Глава 1

Свитчинговая разделимость графов

1.1. Определения и вспомогательные утверждения

Будем рассматривать неориентированные графы, ребра которых помечены элементами из множества $\{1, \ldots, q-1\}$, $q \geq 2$ — натуральное, которые будем называть *весом* ребра (вес можно также трактовать как кратность). Метку 0 будем ассоциировать с отсутствием ребра, то есть пару несмежных вершин будем считать ребром веса 0 (что тем не менее не позволяет считать эти вершины соседними). Таким образом, реберно помеченный граф удобно представлять парой (V, E), где V — множество вершин, а $E : V^2 \to \{0, 1, \ldots, q-1\}$ — симметричное отображение, равное нулю везде на диагонали $\{(v, v) | v \in V\}$. Под *подграфом* графа $G = (V, E)$ будем подразумевать подграф $G_W = (W, I)$, порожденный множеством вершин $W \subset V$ и унаследовавший от G веса ребер: $I(v, w) = E(v, w)$, для любых $v, w \in W$. Результатом сложения двух графов G_1 и G_2 с общим множеством вершин будет граф G на том же множестве вершин, определенный следующим образом: вес любого ребра графа G равен сумме по модулю q весов соответствующих ребер в графах G_1 и G_2. Граф будем называть *аддитивным*, если каждую его вершину можно пометить числами от 0 до

$q-1$ таким образом, что вес каждого ребра будет равен сумме по модулю q меток двух вершин ребра. Далее определим *свитчинг* графа G, как результат сложения графа G с некотором аддитивным графом на том же множестве вершин. Множество вершин W графа G назовем *отделимым*, если некоторый свитчинг графа G не содержит ребер (ненулевого веса) между W и $V\backslash W$ (отметим, что при этом множество $V\backslash W$ также будет отделимым). Легко видеть, что любое множество вершин мощности 0, 1, $n-1$ или n в графе порядка n является отделимым. Любые другие отделимые множества назовем *нетривиальными*. Граф $G=(V,E)$ назовем *свитчингово разделимым* (далее в тексте — просто *разделимым*), если существует нетривиальное отделимое множество его вершин.

Лемма 1. *Множество аддитивных графов замкнуто относительно сложения.*

Доказательство. Утверждение следует прямо из определения: в качестве метки каждой вершины результирующего графа можно взять сумму меток этой вершины в графах-слагаемых. ▲

Таким образом, отношение "граф G — свитчинг графа H" является отношением эквивалентности. Если какое-то множество отделимо в графе (или в некотором подграфе), то оно отделимо и в каждом его свитчинге (в соответствующем подграфе), поэтому в вопросах разделимости мы без потери общности можем рассматривать наиболее удобный свитчинг данного графа. В частности, мы всегда можем считать некоторую одну данную вершину изолированной. Далее под словами "изолируем вершину o" будем подразумевать рассмотрение без потери общности свитчинга исходного графа, у которого вершина o изолирована.

Лемма 2. *Множество вершин W графа $G=(V,E)$ отделимо тогда и только тогда, когда существуют $W_0,\ldots,W_{q-1}$, $V_0,\ldots,V_{q-1}$ такие, что $W=W_0\cup W_1\cup\ldots\cup W_{q-1}$, $V\backslash W=V_0\cup V_1\cup\ldots\cup V_{q-1}$ и любое ребро, соединяющее вершины из множеств W_i и V_j имеет вес $i+j$.*

Доказательство. Сопоставив каждой вершине из W_i или V_i метку $q-i$, мы породим некоторый аддитивный граф. Очевидно, что его сумма с исходным графом не имеет ребер, соединяющих W и $V\backslash W$. ▲

Следствие 1. *Пусть множество вершин W графа $G=(V,E)$, имеющее изолированную вершину, отделимо. Тогда любая вершина из W соединена со всеми вершинами из $V\backslash W$ ребрами одного веса.*

Доказательство. Допустим, в разбиении множества $V\backslash W$ из леммы 2 есть хотя бы два непустых множества. Но тогда вершины из разных множеств будут соединены с изолированной вершиной ребрами разных весов, что неверно. Поэтому разбиение множества $V\backslash W$ состоит не более чем из одного непустого элемента, и любая вершина из W соединена со всеми вершинами из $V\backslash W$ ребрами одного и того же веса. ▲

Следствие 2. *Пусть любая вершина из множества $V\backslash W$ соединена со всеми вершинами W ребрами одного и того же веса. Тогда W отделимо.*

Доказательство. Обозначим $W_0=W$, $W_1=\ldots=W_{q-1}=\emptyset$. Множество вершин из $V\backslash W$, соединенных с вершинами из W ребрами веса i обозначим через V_i. Тогда по лемме 2 множество W отделимо. ▲

Следствие 3. *Пусть граф G разделим и имеет изолированую вершину o. Тогда для любых $i,j\in\{0,1,\ldots,q-1\}$ если в графе G поменять веса i и j местами, то получившийся граф также будет разделим.*

Доказательство. Пусть W — нетривиальное отделимое множество, не содержащее вершину o. По следствию 1 любая вершина из $V\backslash W$ соединена со всеми вершинами из W ребрами одного и того же веса. Но если поменять местами веса i и j в графе G, то полученный граф будет разделим по следствию 2. ▲

Лемма 3. *Пусть D — разделимый граф порядка больше 4 и d — некоторая его вершина. Граф $D\backslash\{d\}$ неразделим тогда и только тогда, когда вершина d в графе D принадлежит единственному нетривиальному отделимому множеству*

вершин $W = \{d, e\}$, *для некоторой вершины* e.

Доказательство. Пусть $D = (V, E)$ — разделимый граф, $|V| \geq 5$, $D\backslash\{d\}$ — его неразделимый подграф и W — нетривиальное отделимое множество, содержащее d. Сначала предположим, что $|W\backslash\{d\}| \geq 2$. Тогда $W\backslash\{d\}$ и $V\backslash W\backslash\{d\}$ содержат по крайней мере по две вершины и по лемме 2 граф $D\backslash\{d\}$ разделим, противоречие. Предположим теперь, что у нас есть два отделимых множества $\{d, e\}$ и $\{d, b\}$. Изолируем вершину d. Тогда по следствию 1 вершина e будет соединена со всеми остальными вершинами (за исключением вершины d) ребрами одинакового веса. Аналогично с вершиной b. Но тогда, если удалить вершину d, множество $\{e, b\}$ будет отделимо по следствию 2, что противоречит неразделимости $D\backslash\{d\}$.

Пусть теперь $W = \{d, e\}$ — единственное нетривиальное отделимое множество, содержащее d. Изолируем вершину e. Тогда по следствию 1 вершина d соединена со всеми вершинами из $D\backslash\{d, e\}$ ребрами одного веса. Предположим от противного, что граф $D\backslash\{d\}$ разделим; обозначим через U его нетривиальное отделимое множество, не содержащее вершину e. Так как вершина d соединена со всеми вершинами U ребрами одного веса, то по следствию 2 множество U отделимо в D. Поскольку $V\backslash U$ содержит d и не совпадает с W, получаем противоречие с единственностью W. ▲

Лемма 4. *Любой разделимый граф порядка* $n \geq 5$ *имеет либо* 0, *либо* 2 *неразделимых подграфа порядка* $n - 1$.

Доказательство. Пусть граф G имеет неразделимый подграф $G\backslash\{a\}$ для некоторой вершины a. Тогда по лемме 3 отделимым множеством графа G будет пара $\{a, b\}$ для некоторой вершины b. Считая без потери общности, что $G\backslash\{a, b\}$ содержит изолированную вершину, мы видим по следствию 1, что граф $G\backslash\{b\}$ изоморфен графу $G\backslash\{a\}$ и, следовательно, также неразделим. Удаление же из графа G любой вершины c, отличной от a и b, приводит к разделимому подграфу, поскольку $\{a, b\}$ остается отделимым в $G\backslash\{c\}$. ▲

Предложение 1. *Пусть в графе G порядка $n \geq 5$ каждый подграф порядка* 4 *или* 5 *разделим. Тогда граф G разделим.*

Доказательство. Без потери общности мы можем считать, что граф содержит изолированную вершину o. По следствию 1 в графе $G\backslash\{o\}$ не существует трех вершин таких, что веса ребер между этими вершинами попарно различны. Выберем в этом графе три вершины a, b, c, соединенные между собой ребрами двух различных весов (если таких не существует, то в подграфе $G\backslash\{o\}$ все ребра одного веса, и граф G разделим): $E(a,b) = i \neq E(a,c) = E(b,c) = j$. Определим три множества U, V, W:

U — множество вершин, соединенных с вершинами a и b ребрами веса i;

V — множество вершин, соединенных с вершинами a и b ребрами одинакового веса, отличного от i;

W — множество вершин, соединенных с вершинами a и b ребрами разного веса.

Для произвольных вершин v из V и w из W рассмотрим подграф, порождаемый множеством вершин $\{o, a, b, v, w\}$. Пусть ребра $\{v, a\}$ и $\{v, b\}$ имеют вес $l \neq i$. Одно из ребер $\{w, a\}$ и $\{w, b\}$ имеет вес i, скажем $\{w, a\}$. Тогда ребро $\{w, b\}$ будет иметь вес $k \neq i$. По условию леммы рассматриваемый подграф на пяти вершинах разделим, а значит, имеет отделимую пару вершин. Как легко убедиться, применяя следствие 1, такой парой может быть только $\{o, v\}$ или $\{w, b\}$, см. рис. 1.1. В обоих случаях ребро $\{v, w\}$ должно иметь вес l. В силу произвольности вершин v и w получаем, что любая вершина v из V соединена со всеми вершинами из $W \cup \{a, b\}$ ребрами одного веса, который обозначим через l_v.

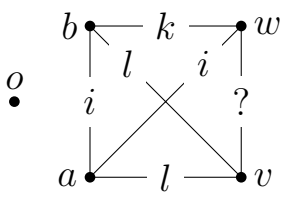


Рис. 1.1: $k \neq i$, $l \neq i$

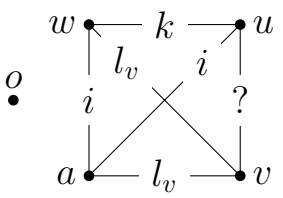


Рис. 1.2: $k \neq i$, $l_v \neq i$

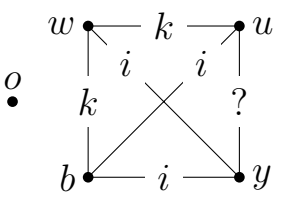


Рис. 1.3: $k \neq i$

Далее, множество U разделим на два U_1 и U_2 следующим образом: U_1 — множество вершин, которые соединены со всеми вершинами из $W \cup \{a, b\}$ ребрами веса i; U_2 — остальные вершины. Заметим, что если U_2 пусто, то из доказанного уже следует отделимость множества $V \cup U_1 \cup \{o\}$.

Рассмотрим произвольную вершину u из U_2. По определению множества U_2 найдется вершина w из W такая, что $E(u, w) \neq i$. Без потери общности мы можем считать, что $E(w, a) = i \neq E(w, b)$. Для произвольной вершины v из V рассмотрим подграф, порожденный пятеркой $\{o, a, u, w, v\}$, см. рис. 1.2. Отделимой парой в этом подграфе может быть только $\{o, v\}$ или $\{u, w\}$. В обоих случаях $E(v, u) = l_v$.

При тех же условиях на u и v рассмотрим произвольную вершину y из U_1. В графе, порожденном пятеркой $\{o, b, u, w, y\}$, см. рис. 1.3, отделимой парой может быть только $\{o, y\}$ или $\{u, b\}$. В обоих случаях $E(y, u) = i$.

Таким образом, каждая вершина v из V соединена со всеми вершинами из $\{a, b\} \cup W \cup U_2$ ребрами веса l_v, а каждая вершина из U_1 соединена со всеми вершинами из $\{a, b\} \cup W \cup U_2$ ребрами веса i. По следствию 2 множество $V \cup U_1 \cup \{o\}$ отделимо и граф G разделим. ▲

Предложение 2. *Пусть G_K — неразделимый подграф порядка χ, $4 \leq \chi < n - 2$, графа G порядка n. И пусть все подграфы графа G порядков $\chi + 1$ и $\chi+2$, содержащие G_K в качестве подграфа, разделимы. Тогда граф G разделим.*

Доказательство. Рассмотрим произвольную вершину a из $V \backslash K$. Граф $G_{K \cup \{a\}}$ разделим, в то время как граф G_K неразделим. По лемме 3 в графе $G_{K \cup \{a\}}$ будет только одно (с точностью до дополнения) нетривиальное отделимое множество вершин $\{a, c\}$, для некоторой c из K. Изолируем вершину c. Тогда по следствию 1 вершина a соединена со всеми вершинами из $K \backslash \{c\}$ ребрами одинакового веса. Для доказательства разделимости графа G нам необходимо найти нетривиальное отделимое множество. Для этого в множестве $V \backslash K$ выделим подмножество A вершин, которые соединены со всеми вершинами множе-

ства $K\backslash\{c\}$ ребрами одинакового веса, в частности $a \in A$. В оставшейся части доказательства мы покажем, что множество $A \cup \{c\}$ отделимо в G. Остаток $V\backslash K\backslash A$ обозначим через B.

(*) *Для произвольной вершины d из $V\backslash(K\cup\{a\})$ докажем, что либо $d \in A$, либо вершина a соединена с d ребром того же веса, что и с вершинами из* $K\backslash\{c\}$. Рассмотрим граф $G_{K\cup\{a,d\}}$. По условию он разделим, поэтому вершина d лежит в некотором нетривиальном отделимом в $G_{K\cup\{a,d\}}$ множестве W. Величина $m = |W \cap K|$ может принимать 3 значения: 0, 1 или $\chi - 1$ (иначе $W\backslash\{a, d\}$ — нетривиальное отделимое множество в G_K, что противоречит неразделимости этого графа). Рассмотрим эти случаи.

- $m = 0$. В этом случае $\{a, d\}$ отделимо в графе $G_{K\cup\{a,d\}}$. По следствию 1 любая вершина из K соединена с этой парой вершин ребрами одного и того же веса. Следовательно, вершина d соединена со всеми вершинами множества $K\backslash\{c\}$ так же, как и вершина a, то есть ребрами одинакового веса. Имеем $d \in A$.

- $m = 1$. В этом случае W содержит некоторую вершину e из K.

  Если a принадлежит W, то $e = c$, иначе в графе $G_{K\cup\{a\}}$ будет больше одного отделимого множества, что противоречит лемме 3 (отметим, что для применения этой леммы мы используем условие $\chi \geq 4$). Таким образом, $W = \{a, c, d\}$, и легко видеть, что $d \in A$.

  Если a не принадлежит W, то $W = \{d, e\}$. Если $e = c$, то очевидно, что $d \in A$. Если $e \in K\backslash\{c\}$, то $E(a, d) = E(a, e)$, то есть вершина a соединена с d ребром того же веса, что и с вершинами из $K\backslash\{c\}$.

- $m = \chi-1$. Отделимое дополнение до W в графе $G_{K\cup\{a,d\}}$ есть пара $\{a, e\}$, для некоторого e из K. Как и в предыдущем случае, мы видим, что $e = c$. Следовательно, a соединена с d ребром того же веса, что и со всеми вершинами из $K\backslash\{c\}$.

Утверждение (*) доказано.

Покажем теперь, что каждая вершина из A соединена со всеми вершинами из B ребрами одинакового веса. Для вершины a это верно по утверждению (*). Но любая другая вершина f из A соединена со всеми вершинами графа $K\backslash\{c\}$ ребрами одинакового веса и образует с вершиной c отделимое множество в графе $K \cup \{f\}$. Поэтому для нее мы можем повторить те же рассуждения, что и для вершины a. А так как любая вершина g из B по построению не соединена со всеми вершинами графа $K\backslash\{c\}$ ребрами одинакового веса, то вершина f соединена с вершиной g так же (то есть ребром того же веса), как и с вершинами графа $K\backslash\{c\}$. Поэтому по следствию 2 множество $A \cup \{c\}$ является отделимым в графе G, и граф G разделим. ▲

Следствие 4. *Если все подграфы порядков $n-1$ и $n-2$ графа G порядка n разделимы, то и сам граф G разделим.*

Доказательство. Пусть χ — максимальный порядок собственного неразделимого подграфа. По условию $\chi < n-2$. Если $\chi = 3$, то граф G разделим по предложению 1. Если $\chi > 3$, то граф G разделим по предложению 2. ▲

Чтобы сформулировать основную теорему, при четном q определим семейство графов $G_{n,\gamma}$, $\gamma \in \{0, \ldots, q-1\}$, $n = 2k+1 \geq 5$. Множество вершин графа — $\{a_0, a_1, \ldots, a_k, b_1, \ldots, b_k\}$, вершина a_0 изолирована, веса остальных ребер определяются следующим образом:

- для любых l, m от 1 до k ребро $\{a_l, b_m\}$ имеет вес γ, если $l < m$, и вес $\gamma + q/2 \bmod q$, если $l \geq m$;
- для любых различных l, m от 1 до k ребра $\{a_l, a_m\}$ и $\{b_l, b_m\}$ имеют вес γ.

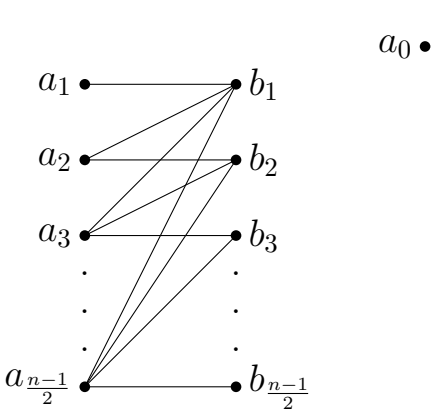


Рис. 1.4: Граф $G_{n,0}$

1.2. Основной результат

Теорема 1. *Если при удалении любой вершины из графа G порядка $n \geq 6$ всегда получается разделимый подграф графа G, то либо граф G разделим, либо q четно, n нечетно, и граф G изоморфен некоторому свитчингу графа $G_{n,\gamma}$, $\gamma \in \{0, \ldots, q-1\}$.*

Доказательство. Пусть граф G имеет порядок n произвольной четности. Попробуем охарактеризовать все неразделимые графы G порядка n, у которых все подграфы порядка $n-1$ разделимы. Итак, пусть дан граф G порядка $n \geq 6$, обладающий свойствами:

(i) G — неразделимый граф.

(ii) Для любой вершины a из G граф $G\backslash\{a\}$ разделимый.

Будем говорить, что пара вершин графа G обладает свойством $\{x, y\}_*$, если существует вершина z такая, что $\{x, y\}$ — единственное (с точностью до дополнения) нетривиальное отделимое множество в графе $G\backslash\{z\}$. Если такая вершина z известна, будем также обозначать это свойство через $\{x, y\}_z$. По лемме 3 ($D = G\backslash\{z\}$) из свойства $\{x, y\}_z$ следует, что графы $G\backslash\{z, x\}$ и $G\backslash\{z, y\}$ неразделимы.

Пусть P — множество всех пар $\{x, y\}$, обладающих свойством $\{x, y\}_*$. Его можно построить, рассмотрев все подграфы порядка $n-1$: если некоторая пара

вершин является единственным отделимым множеством в одном из них, то эта пара принадлежит P.

Рассмотрим несколько свойств множества P и входящих в него пар.

(iii) *Множество P не пусто.* Это следует из следствия 4 и свойств (i) и (ii).

(iv) *Если для некоторой пары вершин $\{a, b\}$ выполняются соотношения $\{a, b\}_{c_1}$ и $\{a, b\}_{c_2}$, то $c_1 = c_2$.* Действительно, пусть $\{a, b\}$ — отделимое множество в графах $G\backslash\{c_1\}$ и $G\backslash\{c_2\}$. Изолируем некоторую вершину o, отличную от a, b, c_1, c_2. Все вершины графа $G\backslash\{c_1\}$ соединены с парой $\{a, b\}$ ребрами одинакового веса по следствию 1; то же верно для графа $G\backslash\{c_2\}$. По следствию 2 пара $\{a, b\}$ отделима в графе G, что противоречит свойству (i).

(v) *Любая вершина a графа G встречается ровно в двух парах множества P, либо не встречается совсем.* Действительно, из соотношения $\{a, b\}_c$ следует неразделимость графа $G\backslash\{a, c\}$. С другой стороны, из неразделимости графа $G\backslash\{a, c\}$ по лемме 3 следует $\{a, b\}_c$ для некоторого b, поскольку граф $G\backslash\{c\}$ разделим (свойство (i)). По лемме 4 в графе $G\backslash\{a\}$ ровно 2 неразделимых подграфа: $G\backslash\{a, c\}$ и $G\backslash\{a, c'\}$ для некоторых c и c'. Отсюда следует, что $\{a, b\}_c$ и $\{a, b'\}_{c'}$ для некоторых b и b', и другой пары из P, содержащей a, нет.

(vi) *Если $\{a, b\}_c$, то $\{c, d\}_a$ и $\{c, e\}_b$ для некоторых d и e, причем $a \neq e \neq d \neq b$.* Действительно, граф $G\backslash\{a, c\}$ неразделим, а граф $G\backslash\{a\}$ разделим, следовательно, для некоторой вершины d пара $\{c, d\}$ — единственное отделимое множество в графе $G\backslash\{a\}$. Причем $d \neq b$, иначе все вершины множества $V\backslash\{a, b, c\}$ (считая одну из них изолированной) соединены с парами вершин $\{a, b\}$ и $\{b, c\}$ ребрами одинакового веса и, следовательно, множество $\{a, b, c\}$ отделимо, что противоречит свойству (i). Аналогично, в графе $G\backslash\{b\}$ отделимое множество $\{c, e\}$ для некоторой вершины e, отличной от a. Из (iv) следует, что $e \neq d$.

Перебирая пары из P приведенным ниже алгоритмом, построим два множества вершин A, B. Выберем произвольную пару вершин $\{a_0, a_1\}$ из P. Изолируем вершину a_0, поместим a_1 в A. Вершину b_1 такую, что $\{a_0, a_1\}_{b_1}$, поместим

в множество B. Тогда, согласно (vi), в графе $G\backslash\{a_1\}$ единственным отделимым множеством будет $\{b_1, b_2\}$, для некоторой вершины b_2. Помещаем вершину b_2 в множество B. Далее, в графе $G\backslash\{b_2\}$ отделимым множеством будет пара $\{a_1, a_2\}$ для некоторой вершины a_2, которую включим в A. Дальше продолжаем аналогично, до тех пор, пока не окажется, что очередная вершина уже была рассмотрена ранее, то есть принадлежит $\{a_0\} \cup A \cup B$. Так как каждая рассматриваемая вершина содержится ровно в двух парах из P, этой вершиной может быть только a_0, то есть, для некоторого k верно либо $\{a_{k-1}, a_0\}_{b_k}$ (в этом случае также выполнено $\{b_k, b_1\}_{a_0}$, согласно (v)), либо $\{b_k, a_0\}_{a_k}$ (и $\{a_k, b_1\}_{a_0}$).

Покажем, что первый из этих двух случаев приводит к противоречию. Выполнены следующие соотношения: $\{b_2, b_3\}_{a_2}$, ..., $\{b_{k-1}, b_k\}_{a_{k-1}}$, следовательно, ребра $\{b_1, b_2\}$, ..., $\{b_1, b_k\}$ имеют одинаковый вес. Аналогично, ребра $\{b_k, b_{k-1}\}$, ..., $\{b_k, b_1\}$ имеют один, тот же самый, вес. В графе $G\backslash\{a_0\}$ отделимым множеством будет пара $\{b_1, b_k\}$. Поскольку $E(b_1, b) = E(b_k, b)$ при $b = b_2$, то такое же равенство верно для любого b из $V\backslash\{a_0, b_1, b_k\}$. Следовательно, пара $\{b_1, b_k\}$ отделима в G, что противоречит свойству (i).

Рассмотрим второй случай. Докажем, что множество $\{a_0\} \cup A \cup B$ содержит все вершины графа G. Предположим, что это не так. Возьмем произвольную вершину a не из $\{a_0\} \cup A \cup B$. Выполнены следующие соотношения: $\{b_1, b_2\}_{a_1}$, ..., $\{b_{k-1}, b_k\}_{a_{k-1}}$, следовательно, ребра $\{a, b_1\}$, ..., $\{a, b_k\}$ имеют одинаковый вес. Аналогично, из соотношений $\{a_1, a_2\}_{b_2}$, ..., $\{a_{k-1}, a_k\}_{b_k}$, ребра $\{a, a_1\}$, ..., $\{a, a_k\}$ имеют один вес. Из соотношений $\{a_0, a_1\}_{b_1}$ и $\{b_k, a_0\}_{a_k}$ получаем, что $E(a_1, a) = E(a_1, b_k) = E(b_k, a)$ Получается, что вершина a соединена со всеми вершинами множества $A \cup B$ ребрами одинакового веса. В силу произвольности вершины a, это верно для всех остальных вершин, не лежащих в $A \cup B \cup a_0$. А следовательно, все эти вершины вместе с вершиной a_0 по следствию 2 образуют отделимое множество в графе G, что противоречит его неразделимости.

Итак, $n = 2k+1$ нечетно, множество вершин состоит из изолированной вершины a_0 и подмножеств $A = \{a_1, \ldots, a_k\}$ и $B = \{b_1, \ldots, b_k\}$. Вершины связаны

следующими соотношениями:

$$\{a_0, a_1\}_{b_1} \dots \{a_{k-1}, a_k\}_{b_k}, \{a_k, b_1\}_{a_0}, \{b_1, b_2\}_{a_1} \dots \{b_{k-1}, b_k\}_{a_{k-1}}, \{b_k, a_0\}_{a_k}.$$

Установим серию равенств для весов между ребрами графа. Для любого $i \in \{1, \dots, k\}$ верно следующее:

$$E(a_i, a_j) = E(a_i, a_{j+1}), \quad \forall j \in \{i+1, \dots, k-1\}; \tag{1.1}$$

$$E(a_i, a_l) = E(a_i, a_{l-1}), \quad \forall l \in \{2, \dots, i-1\}; \tag{1.2}$$

$$E(b_i, b_j) = E(b_i, b_{j+1}), \quad \forall j \in \{i+1, \dots, k-1\}; \tag{1.3}$$

$$E(b_i, b_l) = E(b_i, b_{l-1}), \quad \forall l \in \{2, \dots, i-1\}; \tag{1.4}$$

$$E(a_i, b_j) = E(a_i, b_{j+1}), \quad \forall j \in \{i+1, \dots, k-1\}; \tag{1.5}$$

$$E(a_i, b_l) = E(a_i, b_{l-1}), \quad \forall l \in \{2, \dots, i\}; \tag{1.6}$$

$$E(b_i, a_j) = E(b_i, a_{j+1}), \quad \forall j \in \{i, \dots, k-1\}; \tag{1.7}$$

$$E(b_i, a_l) = E(b_i, a_{l-1}), \quad \forall l \in \{2, \dots, i-1\}; \tag{1.8}$$

$$E(a_1, a_k) = E(a_1, b_k) \neq E(a_1, b_1); \tag{1.9}$$

$$E(b_k, a_1) = E(b_k, b_1) \neq E(b_k, a_k). \tag{1.10}$$

Действительно, соотношения (1.1), (1.2), (1.7), (1.8) следуют из $\{a_{m-1}, a_m\}_{b_m}$, $m \in \{2, \dots, k\}$: в графе $G \backslash \{b_m\}$ дополнение до отделимой пары $\{a_{m-1}, a_m\}$ содержит изолированную вершину a_0, а значит, по следствию 1, для любой вершины c этого дополнения верно $E(c, a_{m-1}) = E(c, a_m)$. Аналогично, соотношения (1.3)–(1.6) следуют из $\{b_{m-1}, b_m\}_{a_{m-1}}$. Соотношение (1.9) (аналогично (1.10)) следует по следствию 1 из $\{a_0, a_1\}_{b_1}$ (соответственно $\{b_k, a_0\}_{a_k}$), поскольку в графе $G \backslash \{b_1\}$ пара $\{a_0, a_1\}$ отделимая, но в графе G она уже не отделима.

Из равенств (1.1) и (1.2) (соответственно, (1.3) и (1.4)) легко заключить, что все ребра, соединяющие вершины из множества A (B) между собой, имеют один и тот же вес, скажем α (соответственно, β). Из равенств (1.5) и (1.8) следует,

что все ребра $\{a_i, b_j\}$, где $1 \le i < j \le k$, имеют один и тот же вес, скажем γ. Аналогично, из (1.6) и (1.7) вытекает, что все ребра $\{a_i, b_j\}$, где $1 \le j \le i \le k$, имеют один и тот же вес, скажем δ. Более того из (1.9) и (1.10) мы видим, что $\alpha = \gamma = \beta \ne \delta$.

Остается показать, что $\delta = \gamma + q/2$. В графе $G\backslash\{a_0\}$ отделима пара $\{a_k, b_1\}$. По лемме 2 и в соответствии с ее обозначениями, $\{a_k\} = W_a$, $\{b_1\} = W_b$, $A\backslash\{a_k\} = V_{a'}$, $B\backslash\{b_1\} = V_{b'}$, причем $a + a' = b + b' = \gamma$ и $a + b' = b + a' = \delta$. Отсюда видно, что $2\gamma = 2\delta$. Поскольку $\gamma \ne \delta$, имеем $\delta = \gamma + q/2$, где q четно. ▲

Рассмотрим отдельно случай $n = 5$.

Предложение 3. *Если при удалении любой вершины из графа G порядка 5 всегда получается разделимый подграф графа G, то либо граф G разделим, либо q четно и граф G изоморфен некоторому свитчингу графа $G_{5,\gamma}$, $\gamma \in \{0, \ldots, q-1\}$.*

Доказательство. Обозначим вершины графа G через o, a_1, a_2, a_3, a_4. Изолируем вершину o. Верно следующее свойство.

(*) *Для любого $i \in \{1, 2, 3, 4\}$ веса ребер в графе $G\backslash\{o, a_i\}$ не могут быть попарно различны.* Это следует из разделимости графа $G\backslash\{a_i\}$.

Рассмотрим случай, когда $E(a_1, a_2) = E(a_2, a_3) = E(a_3, a_1) = \alpha$. Тогда $E(a_1, a_4) = \beta \ne \alpha$, иначе множество $\{o, a_1\}$ отделимо в G. Вес $E(a_2, a_4)$ не может быть равен α, иначе множество $\{o, a_2\}$ отделимо в G. Аналогично, $E(a_3, a_4) \ne \alpha$. Тогда $E(a_2, a_4) = E(a_3, a_4) = \beta$ по свойству (*). Но тогда множество $\{o, a_4\}$ отделимо в G.

Пусть $E(a_1, a_2) = E(a_1, a_3) = \alpha$, $E(a_2, a_3) = \beta$, $\alpha \ne \beta$. $E(a_1, a_4) \ne \alpha$, иначе множество $\{o, a_1\}$ отделимо в G. Допустим, $E(a_1, a_4) = \gamma \ne \beta$. Если $E(a_4, a_2) = E(a_4, a_3)$, то множество $\{o, a_1, a_4\}$ отделимо в G. Тогда веса $E(a_4, a_2)$, $E(a_4, a_3)$ различны и по свойству (*) отличны от β. Но тогда в графе $G\backslash\{o, a_1\}$ не выполняется свойство (*). Следовательно, $E(a_1, a_4) = \beta$. Также

$E(a_2, a_4) \neq E(a_3, a_4)$, иначе множество $\{o, a_1, a_4\}$ отделимо в G. По свойству (*) один из весов $E(a_2, a_4)$, $E(a_3, a_4)$ равен α, скажем $E(a_2, a_4)$, а другой β.

Рассмотрим граф $G\backslash\{o\}$. По условию он разделим. Изолируем в этом графе вершину a_1 (прибавим аддитивный граф с метками 0, $-\alpha$, $-\alpha$ и $-\beta$). В получившимся графе веса ребер $\{a_2, a_3\}$, $\{a_2, a_4\}$ и $\{a_3, a_4\}$ равны $\beta - 2\alpha$, $-\beta$ и $-\alpha$, соответственно. Так как граф разделим, то среди этих трех весов не более двух различных. Так как по условию $\alpha \neq \beta$, то $\beta - 2\alpha = -\beta$, а следовательно, $\beta = \alpha + q/2$, где q четно. ▲

Для полноты картины остается показать, что сам граф $G_{n,\gamma}$ действительно является исключением.

Предложение 4. *Граф $G_{n,\gamma}$ ($n \geq 5$ нечетно, q четно) неразделим и все его подграфы порядка $n-1$ разделимы.*

Доказательство. Предположим от противного, что $G_{n,\gamma} = (V, E)$ разделим. Пусть W — нетривиальное отделимое множество, содержащее a_0. Вершины a_k и b_1 не могут одновременно принадлежать $V\backslash W$ (иначе, согласно следствию 1 в W не может быть никакой вершины, кроме a_0). Если $a_k \in W$, то либо $\{a_1, \ldots, a_{k-1}\}$, либо $\{b_1, \ldots, b_k\}$ полностью содержится в W (иначе имеем противоречие со следствием 1). В первом случае $V\backslash W$ содержит некоторые b_i, b_j, $i < j$, и вершина a_i из W противоречит следствию 1. Во втором случае $V\backslash W$ содержит некоторые a_i, a_j, $i < j$, и вершина b_j из W противоречит следствию 1. Случай $b_1 \in W$ аналогичен. Полученное противоречие доказывает неразделимость графа $G_{n,\gamma}$.

Остается заметить, что пара $\{a_k, b_1\}$ отделима в $G\backslash\{a_0\}$, пара $\{b_i, b_{i+1}\}$ отделима в $G\backslash\{a_i\}$, $i = 1, \ldots, k-1$, пара $\{b_k, a_0\}$ отделима в $G\backslash\{a_k\}$, пара $\{a_{i-1}, a_i\}$ отделима в $G\backslash\{b_i\}$, $i = 1, \ldots, k$. ▲

Таким образом, получена характеризация всех свитчингово неразделимых графов по модулю q таких, что удаление любой вершины графа приводит к свитчингово разделимому графу по модулю q. Такие графы существуют толь-

ко при четных q, и, следовательно, по ним нельзя построить неразделимые n-арные квазигруппы порядка q^2, где q — простое, у которых любой $(n-1)$-арный ретракт разделим. Возникает гипотеза, что при данных порядках квазигрупп с такими свойствами не существует.

Глава 2

МДР коды в графах Дуба

2.1. Определения и вспомогательные утверждения

Граф Шрикханде Sh — это граф Кэли над группой $\mathbb{Z}_4^2$ с порождающим множеством $\{01, 03, 10, 30, 11, 33\}$ (вершины графа — элементы группы $\mathbb{Z}_4^2$, которые мы обозначим 00, 01, 02, ..., 33; две вершины смежны тогда и только тогда, когда их разность принадлежит порождающему множеству). Полный граф $K = K_4$ — граф Кэли над группой $\mathbb{Z}_4$ с порождающим множеством $\{1, 2, 3\}$. *Расстоянием* между двумя вершинами в связном графе называется длина кратчайшего пути между этими вершинами. *Окрестностью* вершины называется множество вершин на расстоянии 1 от нее.

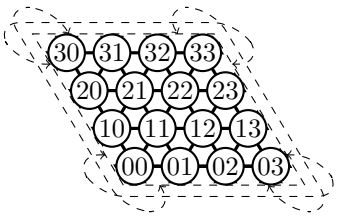


Рис. 2.1: Граф Шрикханде, изображенный на торе

Пусть m и n — неотрицательные целые числа. Через $D(m, n) = \mathrm{Sh}^m \times K^n$ обозначим граф, являющийся декартовым произведением m копий графа Шрикханде и n копий полного графа K_4. Если $m > 0$, то такой граф назы-

вается *графом Дуба*, тогда как $D(0,n)$ — граф Хэмминга $H(n,4)$. Граф Дуба — дистанционно-регулярный с тем же массивом пересечений, что и граф Хэмминга $H(2m+n,4)$ (напомним, что связный граф диаметра d называется *дистанционно-регулярным* с массивом пересечений $\{a_{ij}\}_{i,j=0}^{d}$, если для любых двух вершин x и y на расстоянии i друг от друга окрестность вершины y содержит ровно a_{ij} вершин на расстоянии j от x).

Множество вершин графа G обозначим через ${}_{\mathrm{v}}G$. Вершины графа $D(m,n)$ мы будем обозначать через $(s_1,\ldots,s_m;h_1,\ldots,h_n)$, где $s_i \in \mathbb{Z}_4^2$, $h_i \in \mathbb{Z}_4$. Для произвольных вершин $a,b \in {}_{\mathrm{v}}D(m,n)$ обозначим через $d(a,b)$ расстояние между вершинами a,b в графе $D(m,n)$. Так как $D(m,n)$ декартово произведение графов Sh и K, то для двух вершин $c=(s_1,\ldots,s_m;h_1,\ldots,h_n)$ и $c'=(s'_1,\ldots,s'_m;h'_1,\ldots,h'_n)$ из ${}_{\mathrm{v}}D(m,n)$ расстояние

$$d(c,c')=\sum_{i=1}^{m} d(s_i,s'_i)+\sum_{j=1}^{n} d(h_j,h'_j).$$

Кодом назовем произвольное подмножество вершин графа $D(m,n)$. Вершины, принадлежащие коду, будем называть *кодовыми*. *Кодовое расстояние* равно минимальному расстоянию между различными кодовыми вершинами.

Пусть дан набор координат $(i_1,\ldots,i_v;j_1,\ldots,j_w)$, где $1 \le i_1 < \ldots < i_v \le m$; $1 \le j_1 < \ldots < j_w \le n$.

Для кода C определим *проекцию* $C_{i_1,\ldots,i_v;j_1,\ldots,j_w}$ и *сечение* $C^{a_1,\ldots,a_v;b_1,\ldots,b_w}_{i_1,\ldots,i_v;j_1,\ldots,j_w}$, где $a_i \in {}_{\mathrm{v}}\mathrm{Sh}$ для $i=1,\ldots,v$ и $b_j \in {}_{\mathrm{v}}K$ для $j=1,\ldots,w$.

Для начала определим:

$$C_{i;}=\{(s_1,\ldots,s_{i-1},s_{i+1},\ldots,s_m;h_1,\ldots,h_n):\ \text{существует вершина } x \in {}_{\mathrm{v}}\mathrm{Sh}$$

$$\text{такая, что } (s_1,\ldots,s_{i-1},x,s_{i+1},\ldots,s_m;h_1,\ldots,h_n) \in C\},\ i \in \{1,\ldots,m\}.$$

$$C_{;j}=\{(s_1,\ldots,s_m;h_1,\ldots,h_{j-1},h_{j+1},\ldots,h_n):\ \text{существует вершина } y \in {}_{\mathrm{v}}K$$

такая, что $(s_1, \ldots, s_m; h_1, \ldots, h_{j-1}, y, h_{j+1}, \ldots, h_n) \in C\}, j \in \{1, \ldots, n\}$.

Тогда проекцию $C_{i_1,\ldots,i_v;j_1,\ldots,j_w}$ можно определить рекурсивно по правилам:

$$C_{i_1,\ldots,i_v;j_1,\ldots,j_w} = (C_{i_1,\ldots,i_v;j_2,\ldots,j_w})_{;j_1} \text{ и } C_{i_1,\ldots,i_w;} = (C_{i_2,\ldots,i_w;})_{i_1;}.$$

Хотя формально отображение $C \to C_{i_1,\ldots,i_v;j_1,\ldots,j_w}$ не обязательно является биекцией и мощность проекции может оказаться меньше мощности исходного кода, в дальнейших рассуждениях такая ситуация не встречается.

Также определим:

$C^{a;}_{i;} = \{(s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_m; h_1, \ldots, h_n) :$

$$(s_1, \ldots, s_{i-1}, a, s_{i+1}, \ldots, s_m; h_1, \ldots, h_n) \in C\}, i \in \{1, \ldots, m\}.$$

$C^{;b}_{;j} = \{(s_1, \ldots, s_m; h_1, \ldots, h_{j-1}, h_{j+1}, \ldots, h_n) :$

$$(s_1, \ldots, s_m; h_1, \ldots, h_{j-1}, b, h_{j+1}, \ldots, h_n) \in C\}, j \in \{1, \ldots, n\}.$$

Тогда сечение $C^{a_1,\ldots,a_v;b_1,\ldots,b_w}_{i_1,\ldots,i_v;j_1,\ldots,j_w}$ можно определить рекурсивно по следующим правилам:

$$C^{a_1,\ldots,a_v;b_1,\ldots,b_w}_{i_1,\ldots,i_v;j_1,\ldots,j_w} = (C^{a_1,\ldots,a_v;b_2,\ldots,b_w}_{i_1,\ldots,i_v;j_2,\ldots,j_w})^{;b_1}_{;j_1} \text{ и } C^{a_1,\ldots,a_v;}_{i_1,\ldots,i_v;} = (C^{a_2,\ldots,a_v;}_{i_2,\ldots,i_v;})^{a_1;}_{i_1;}.$$

Существует следующая граница на мощность кода в графе Дуба (аналогичная границе Синглтона для графов Хэмминга, доказательство также аналогично).

Лемма 5. *Пусть C — код в графе $D(m, n)$ с кодовым расстоянием d. Тогда $|C| \leq 4^{2m+n-d+1}$.*

Доказательство. Если $n > 0$ либо d нечетно, то зафиксируем некоторый набор координат $(i_1, \ldots, i_k; j_1, \ldots, j_l)$ такой, что $2k + l = d - 1$. Тогда

$C_{i_1,\ldots,i_k;j_1,\ldots,j_l}$ — код с кодовым расстоянием не менее 1, откуда следует, что мощность кода C не превосходит количества вершин в графе Дуба $D(m-k, n-l)$, т.е. $4^{2(m-k)+(n-l)} = 4^{2m+n-d+1}$. Если же $n = 0$ и d четно, то зафиксируем некоторый набор координат $(i_1, \ldots, i_k;)$ такой, что $2k = d-2$. Тогда $C_{i_1,\ldots,i_k;}$ — код с кодовым расстоянием не менее 2, т.е. независимое множество графа Дуба $D(m-k, 0)$. Число независимости графа Шрикханде равно 4, следовательно, число независимости графа Дуба $D(m-k, 0)$ не превосходит (на самом деле в точности равно) $4^{2(m-k)-1} = 4^{2m-d+1}$. ▲

МДР кодом с параметрами $((m, n), 4^k, d)$ назовем код в графе $D(m, n)$ мощности 4^k с кодовым расстоянием $d = 2m + n - k + 1$.

Два множества вершин (кода) C и C' графа Дуба $D(m, n)$ назовем *эквивалентными*, если существует набор автоморфизмов $\theta_1, \ldots, \theta_m$ графа Sh, набор перестановок $\sigma_1, \ldots, \sigma_n$ из Sym_4 и перестановки координат $\tau_1 \in \mathrm{Sym}_m$ и $\tau_2 \in \mathrm{Sym}_n$ такие, что

$$C' = \{(\theta_1(s_{\tau_1(1)}), \ldots, \theta_m(s_{\tau_1(m)}); \sigma_1(h_{\tau_2(1)}), \ldots, \sigma_n(h_{\tau_2(n)})) : \\ (s_1, \ldots, s_m; h_1, \ldots, h_n) \in C\}$$

Число различных МДР кодов с параметрами $((m, n), 4^k, d)$ с точностью до эквивалентности обозначим через $L_{m,n,k}$.

Граф $G = (V, E)$ называется *сильно регулярным* с параметрами (v, k, λ, μ), если G — регулярный граф степени k на v вершинах, и любая пара смежных вершин имеет λ общих соседей, а любая пара несмежных вершин имеет μ общих соседей. Графы Sh и K^2 — сильно регулярные с параметрами $(16, 6, 2, 2)$.

В графе Шрикханде любая пара различных вершин a и b имеет ровно 2 общих соседа. Обозначим их через $u(a, b)$ и $w(a, b)$. Напомним, что вершины графа Шрикханде — это элементы группы $\mathbb{Z}_4^2$. Обозначим множества $A = \{01, 03, 10, 30, 11, 33\}$, $B = \{02, 20, 22\}$, $C = \{12, 32, 13, 31, 21, 23\}$. Элементы из A и C имеют порядок 4, элементы из B имеют порядок 2.

Лемма 6. *Пусть a и b — несмежные вершины графа Шрикханде. Тогда если*

порядок элемента $(a-b)$ *равен* 2*, то вершины* $u(a,b)$ *и* $w(a,b)$ *несмежны. Если порядок элемента* $(a-b)$ *равен* 4*, то вершины* $u(a,b)$ *и* $w(a,b)$ *смежны.*

Доказательство. Пусть элемент $(a-b)$ принадлежит множеству B. Допустим $a = b + 02$. Тогда $u(a,b) = a + 01$, $w(a,b) = a + 03$, и эти вершины несмежны. Если $a = b + 20$ либо $a = b + 22$, то аналогично.

Пусть теперь элемент $(a-b)$ принадлежит C. Рассмотрим окрестность вершины $u(a,b)$. Тогда $a = u(a,b) + s_1$, $b = u(a,b) + s_2$, где $s_1, s_2 \in A$, $s_1 \neq s_2$, вершины s_1 и s_2 несмежны, и $(s_1 - s_2) \in C$. Нетрудно убедиться, что тогда найдется вершина $s \in A$, смежная с вершинами s_1 и s_2. Тогда $w(a,b) = u(a,b) + s$, и вершины $u(a,b)$ и $w(a,b)$ смежны. ▲

Лемма 7. *Для любой пары вершин* a*,* b *графа Шрикханде и любого автоморфизма графа Шрикханде* τ *порядок элемента* $(a-b)$ *равен порядку элемента* $(\tau(a) - \tau(b))$.

Доказательство. Если вершины a и b смежны, то вершины $\tau(a)$ и $\tau(b)$ также смежны, следовательно, $(a-b) \in A$ и $(\tau(a) - \tau(b)) \in A$.

Пусть a и b несмежны. Предположим, что элементы $(a-b)$ и $(\tau(a) - \tau(b))$ имеют разный порядок. Вершины $\tau(u(a,b))$, $\tau(w(a,b))$ будут общими соседями для вершин $\tau(a)$ и $\tau(b)$. Тогда из леммы 6 следует, что вершины $u(a,b)$ и $w(a,b)$ смежны тогда и только тогда, когда $\tau(u(a,b))$ и $\tau(w(a,b))$ несмежны. Противоречие с тем, что τ — автоморфизм. ▲

Множество из 4 попарно несмежных вершин в графе Sh или K^2 назовем *кокликой.*

Лемма 8. *В графе Шрикханде ровно* 2 *коклики с точностью до эквивалентности:* $\{00, 02, 20, 22\}$ *(рис. 2.2(а)) и* $\{00, 02, 21, 23\}$ *(рис. 2.2(б)). Каждая вершина графа Шрикханде принадлежит ровно четырем различным кокликам.*

Доказательство. Пусть U – коклика в графе Шрикханде. Без потери общности считаем, что U содержит вершину 00. Покажем, что она совпадает с одной из следующих коклик:

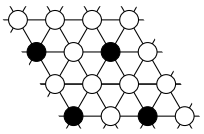
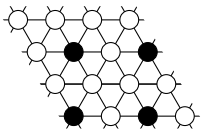
(а)  (б) 

Рис. 2.2: Все коклики в Sh с точностью до эквивалентности

$A = \{00, 02, 20, 22\}$, $B = \{00, 02, 21, 23\}$,

$C = \{00, 20, 12, 32\}$, $D = \{00, 22, 13, 31\}$.

Действительно, коклике U принадлежит хотя бы одна из вершин множества $\{02, 20, 22\}$, иначе U содержит 3 вершины из множеств $\{12, 13, 23\}$ и $\{21, 31, 32\}$, а так как в каждом из этих множеств все вершины попарно смежны, то мы получим противоречие. Допустим, U содержит вершину 02. Тогда оставшиеся две вершины принадлежат множеству $\{20, 21, 22, 23\}$, и это будут либо вершины 20, 22, либо 21, 23, то есть $U = A$ либо $U = B$. Рассмотрев случай, когда U содержит 20, получим, что $U = A$ либо $U = C$, а в случае, когда U содержит 22, получим, что $U = A$ либо $U = D$.

Коклики C и D эквивалентны B (в качестве соответствующих автоморфизмов графа Sh можно взять $\tau(ab) = ba$ и $\tau(ab) = (b - a)b$ соответственно). Коклики A и B неэквивалентны по лемме 7. ▲

Коклику, эквивалентную $\{00, 02, 20, 22\}$, назовем *линейной*, эквивалентную $\{00, 02, 21, 23\}$ — *полулинейной*. Эти коклики изображены на рис. 2.2.

Замечание 1. На самом деле, обе рассмотренные выше коклики являются линейными множествами (подмодулями модуля $\mathbb{Z}_4^2$) над кольцом $\mathbb{Z}_4$, поскольку они замкнуты относительно сложения и умножения на константу. Однако, первое множество линейно также и над кольцом Галуа $\mathrm{GR}(4^2)$, которое естественным образом ассоциируется с графом Шрикханде в вопросах, связанных с теорией кодирования, см. напр. [27].

Два разбиения вершин (в дальнейшем просто разбиения) графа Шрикханде на непересекающиеся коклики называются *эквивалентными*, если существует автоморфизм графа Шрикханде такой, что каждая коклика из одного разбиения при автоморфизме переходит в коклику из второго разбиения.

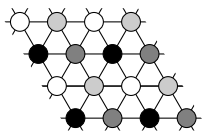
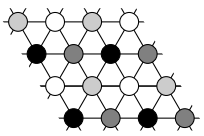
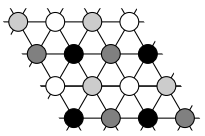
(а)  (б)  (в) 

Рис. 2.3: Все разбиения графа Sh на непересекающиеся коклики с точностью до эквивалентности

Лемма 9. *В графе Шрикханде ровно* 3 *разбиения вершин на непересекающиеся коклики с точностью до эквивалентности (рис. 2.3).*

Доказательство. Пусть имеется некоторое разбиение на коклики F. Если все коклики из разбиения F линейные, то такое разбиение единственно. Иначе, без ограничения общности можно считать, что F содержит $\{00, 02, 21, 23\}$. Тогда вершина 01 может содержаться только в коклике $\{01, 03, 20, 22\}$. Оставшиеся вершины $\{10, 11, 12, 13, 30, 31, 32, 33\}$ разбиваются двумя способами: либо на две линейные, либо на две полулинейные коклики. Таким образом любое разбиение эквивалентно одному из трех разбиений: на 4 линейные коклики, на 2 линейные и 2 полулинейные и на 4 полулинейные. ▲

Все, с точностью до эквивалентности, разбиения графа Шрикханде на непересекающиеся коклики изображены на рис. 2.3.

Лемма 10. *Пусть $G = (V, E)$ — граф Шрикханде либо граф K^2, и $U = \{u_0, u_1, u_2, u_3\}$ — произвольная коклика в G. Тогда любая вершина из $V \backslash U$ смежна ровно с двумя вершинами из U.*

Доказательство. Степень любой вершины графа G равна 6. Следовательно, количество ребер таких, что один из концов ребра принадлежит U равно 24. Мощность $|V \backslash U|$ равна 12. Предположим, утверждение леммы неверно. Тогда существует вершина $u \in V \backslash U$, смежная с 3 либо 4 вершинами из U.

Рассмотрим окрестность вершины u. Докажем, что в этой окрестности не существует 3 или 4 попарно несмежных вершин, принадлежащих некоторой коклике. Это докажет лемму.

Если G — граф K^2, то окрестность вершины u индуцирует объединение двух непересекающихся полных графов на 3 вершинах. Очевидно, что в этой

окрестности нельзя выбрать 3 либо 4 попарно несмежных вершины.

Если G — граф Шрикханде, то окрестность вершины u индуцирует цикл на 6 вершинах. Обозначим вершины цикла через a_1, a_2, a_3, a_4, a_5, a_6, где вершины a_i и a_{i-1} смежны для $i = 2, 3, 4, 5, 6$, а также смежны вершины a_1 и a_6. Очевидно, что в этой окрестности нельзя выбрать 4 попарно несмежных вершины. Предположим, что 3 вершины из окрестности принадлежат некоторой коклике. Тогда это либо вершины a_1, a_3, a_5, либо a_2, a_4, a_6. Без потери общности будем считать, что это вершины a_1, a_3, a_5. Обозначим через W множество вершин, состоящее из вершины u и вершин из ее окрестности. Каждая вершина a_i, где $i = 1, 2, 3, 4, 5, 6$, смежна ровно с 3 вершинами из W, а следовательно и с 3 вершинами из $V\backslash W$. Легко увидеть, что оба общих соседа вершин a_1, a_3 принадлежат множеству W (вершины u и a_2). То же верно для вершин a_3, a_5, и для вершин a_1, a_5. Следовательно, есть ровно 9 вершин из $V\backslash W$ смежных с одной из вершин a_1, a_3, a_5. Но мощность $|V\backslash W| = 9$, следовательно, множество $\{a_1, a_3, a_5\}$ не может содержаться в какой-либо коклике. Лемма доказана. ▲

Лемма 11. *Пусть C — $((m, n), 4^k, 2m + n - k + 1)$ МДР код. Если $2v + w = 2m+n-k$, то в $C_{i_1,\ldots,i_v;j_1,\ldots,j_w}$ каждая вершина графа $D(m-v, n-w)$ встречается ровно один раз.*

Доказательство. Если прообраз некоторой вершины из $C_{i_1,\ldots,i_v;j_1,\ldots,j_w}$ при проекции состоит из двух или более вершин кода C, то расстояние между ними будет не больше $2m + n - k$, что противоречит кодовому расстоянию кода C. С другой стороны, число 4^k кодовых вершин равно количеству вершин в графе $D(m - v, n - w)$. ▲

Из леммы 11 следует, что если в $((m, n), 4^k, d)$ МДР коде мы зафиксируем такой набор координат $(i_1, \ldots, i_v; j_1, \ldots, j_w)$, что $2v + w = k$, то значения в любой другой координате можно представить в виде функции, определенной на всем множестве вершин графа $D(v, w)$.

Лемма 12. *Пусть C — $((m, n), 4^k, d)$ МДР код. Тогда:*

1. *Множество* $C_{i_1,\ldots,i_v;j_1,\ldots,j_w}$ — $((m-v,n-w),4^k,d-2v-w)$ *МДР код при* $2v+w<d$;

2. *Множество* $C^{a_1,\ldots,a_v;b_1,\ldots,b_w}_{i_1,\ldots,i_v;j_1,\ldots,j_w}$ — $((m-v,n-w),4^{k-2v-w},d)$ *МДР код при* $2v+w<k$.

Доказательство.

1. Докажем утверждение для проекции $C_{i_1,\ldots,i_v;j_1,\ldots,j_w}$. Мощность проекции равна 4^k. Кодовое расстояние не меньше, чем $d-2v-w$. С другой стороны, по лемме 5 кодовое расстояние не может быть больше, чем $d-2v-w$.

2. Докажем утверждение для сечения $C^{a_1,\ldots,a_v;b_1,\ldots,b_w}_{i_1,\ldots,i_v;j_1,\ldots,j_w}$. Кодовое расстояние равно d, следовательно, по лемме 5 имеем $|C^{a_1,\ldots,a_v;b_1,\ldots,b_w}_{i_1,\ldots,i_v;j_1,\ldots,j_w}| \leq \frac{|C|}{4^{2v+w}}$. С другой стороны, для набора $(i_1,\ldots,i_v;j_1,\ldots,j_w)$ есть 4^{2v+w} различных сечений. Сумма мощностей всех таких сечений равна 4^k. Следовательно, мощность каждого из них равна 4^{k-2v-w}.

▲

Лемма 13. *Пусть даны два графа* $G_1(V,E_1)$ *и* $G_2(V,E_2)$*, каждый из которых является либо графом* Sh*, либо графом* K^2*, и* $E_1\cap E_2=\emptyset$*. Тогда граф* $G_3=(V,E_3=\overline{E_1\cup E_2})$ — *объединение* 4 *непересекающихся графов* K_4.

Доказательство. Графы G_1 и G_2 — сильно регулярные с параметрами $(16,6,2,2)$. Их дополнения $\overline{G_1}$ и $\overline{G_2}$ — сильно регулярные графы с параметрами $(16,9,4,6)$.

Определим для каждой вершины a из V значения $S'(a)$, $S''(a)$, $N'(a)$, $N''(a)$ и $N(a)$. Обозначим через V_a^1, V_a^2 и V_a^3 множества вершин из окрестности вершины a в графах G_1, G_2 и G_3 соответственно. Тогда

$$S'(a)=|E_3\cap(V_a^1\times V_a^1)|,$$

$$S''(a) = |E_3 \cap (V_a^2 \times V_a^2)|,$$

$$N'(a) = |(E_3 \cup E_1) \cap (V_a^3 \times V_a^3)|,$$

$$N''(a) = |(E_3 \cup E_2) \cap (V_a^3 \times V_a^3)|,$$

$$N(a) = |E_3 \cap (V_a^3 \times V_a^3)|.$$

Так как G_3 — регулярный граф степени 3, то $N'(a) \leq 3$, $N''(a) \leq 3$ и $N(a) \leq 3$.

Для произвольной вершины a рассмотрим граф, индуцированный окрестностью этой вершины в графе $\overline{G_2}$, — граф $(V_a^1 \cup V_a^3, (E_1 \cup E_3) \cap ((V_a^1 \cup V_a^3) \times (V_a^1 \cup V_a^3))$. Это регулярный граф степени 4 (действительно, если взять любую вершину b из окрестности a в графе $\overline{G_2}$, то у нее с вершиной a будет ровно $\lambda = 4$ общих соседа), у него 18 ребер.

С другой стороны, число ребер равно $(S'(a) + 6)$ (ребра, соединяющие вершины из V_a^1) $+(3 \cdot 4 - N'(a))$ (ребра, у которых хотя бы один из концов лежит в V_a^3). Поэтому $18 = S'(a) + 6 + 12 - N'(a)$, и $S'(a) = N'(a)$.

Посчитаем сумму $\sum_{b \in V} S'(b)$. Так как граф G_1 сильно регулярный с параметрами $(16, 6, 2, 2)$, то каждая пара вершин, соединенная ребром из E_3, содержится в окрестности ровно двух вершин в графе G_1, а следовательно, каждое ребро из E_3 будет посчитано ровно два раза. Следовательно, $\sum_{b \in V} S'(b) = 48$.

А следовательно, $\sum_{b \in V} N'(b) = 48$, а так как для любой вершины a выполняется $N'(a) \leq 3$, то $N'(a) = 3$ для любой вершины a.

Аналогично, рассмотрев граф, индуцированный окрестностью произвольной вершины a в графе $\overline{G_1}$, т.е. граф $(V_a^2 \cup V_a^3, (E_2 \cup E_3) \cap ((V_a^2 \cup V_a^3) \times (V_a^2 \cup V_a^3))$, можно доказать, что $S''(a) = N''(a) = 3$ для любой вершины $a \in V$.

Но из того, что $N'(a) = N''(a) = 3$, следует, что $N(a) = 3$, откуда следует утверждение леммы. ▲

В разделе 2.3 нам понадобится следующее вспомогательное утверждение.

Лемма 14. *Для любого натурального m число S_m четверок (a, b, c, d) целых неотрицательных чисел, удовлетворяющих соотношениям $a + b + c + d = m$ и $b \le c \le d$, вычисляется по формуле*

$$S_m = m^3/36 + 7m^2/24 + 11m/12 + 1 - (m \bmod 2)/8 - (m \bmod 3)/9.$$

В частности, $S_0 = 1$, $S_1 = 2$, $S_2 = 4$, $S_3 = 7$, $S_4 = 11$, $S_5 = 16$, $S_6 = 23$.

Доказательство. Будем рассматривать только такие четверки (a, b, c, d), что a, b, c, d — целые неотрицательные числа и $a + b + c + d = m$.

Представим S_m в виде $S_m = M_m + N_m + K_m$, где

M_m — число таких четверок (a, b, c, d), что $b = c = d$;

N_m — число таких четверок (a, b, c, d), что либо $b = c < d$, либо $b < c = d$;

K_m — число таких четверок (a, b, c, d), что $b < c < d$.

Посчитаем M_m. По значению b значение a восстанавливается однозначно. Так как b не превосходит $\lfloor m/3 \rfloor$, имеем $M_m = \lfloor m/3 \rfloor + 1$.

Посчитаем N_m. Для начала найдем число L_m таких четверок (a, b, c, d), что $b \ne c = d$. Для фиксированного числа c число четверок (a, b, c, c) равно $m - 2c + 1$. Число c пробегает значения от 0 до $\lfloor m/2 \rfloor$. Поэтому

$$\begin{aligned} L_m &= \Big(\sum_{i=0}^{\lfloor m/2 \rfloor} (m - 2i + 1)) - M_m \\ &= (((m+1) + (m - 2\lfloor m/2 \rfloor + 1))/2)(\lfloor (m+2)/2) \rfloor) - M_m \\ &= \lfloor (m+3)/2 \rfloor \lfloor (m+2)/2 \rfloor - M_m. \end{aligned}$$

Здесь мы использовали равенство $(m+1-\lfloor m/2 \rfloor) = \lfloor (m+3)/2 \rfloor$. В его верности легко убедиться, рассмотрев случаи $m = 2k$ и $m = 2k + 1$. Число четверок

(a, b, c, d) таких, что $b = c \neq d$, очевидно, также равно L_m. Так как при подсчете N_m из двух четверок (a, b, b, c) и (a, c, b, b), где $b \neq c$, мы выбираем ровно одну, то $N_m = (L_m + L_m)/2 = L_m$. Таким образом,

$$N_m = (\lfloor m/2 \rfloor + 1)(\lfloor (m+1)/2 \rfloor + 1) - M_m.$$

Посчитаем K_m. Для начала найдем число таких четверок (a, b, c, d), что числа b, c, d попарно различны. Это число вычисляется как $(m+3)(m+2)(m+1)/6$ (число всевозможных представлений числа m в виде суммы неотрицательных a, b, c, d) минус $3L_m$ (число четверок таких, что среди b, c, d ровно два различных числа) минус M_m (число четверок таких, что числа b, c, d совпадают). Так как по условию $b < c < d$, то чтобы получить K_m, это число нужно поделить на 6 (чтобы упорядочить числа b, c, d). Таким образом,

$$K_m = ((m+3)(m+2)(m+1)/6 - 3L_m - M_m)/6.$$

Подставив выражения для M_m, N_m, K_m, получаем

$$S_m = (m+3)(m+2)(m+1)/36 + (\lfloor m/2 \rfloor + 1)(\lfloor (m+1)/2 \rfloor + 1)/2 + (\lfloor m/3 \rfloor + 1)/3. \tag{2.1}$$

Используем следующие тождества:

$$\lfloor m/2 \rfloor + \lfloor (m+1)/2 \rfloor = m,$$

$$\lfloor m/2 \rfloor \lfloor (m+1)/2 \rfloor = m^2/4 - (m \bmod 2)/4,$$

$$\lfloor m/3 \rfloor = m/3 - (m \bmod 3)/3.$$

В верности первых двух легко убедиться, рассмотрев случаи $m = 2k$, $m = 2k+1$, а в верности третьего — рассмотрев случаи $m = 3k$, $m = 3k+1$, $m = 3k+2$. Применив эти тождества к (2.1), получим утверждение леммы. ▲

2.2. Основная теорема.

Сформулируем основную теорему.

Теорема 2. *Число $L_{m,n,k}$ неэквивалентных МДР кодов мощности 4^k в графах Дуба $D(m,n)$, $2m+n-2 \geq k \geq 1$ (то есть с расстоянием от 3 до $2m+n$, включительно), характеризуется следующими утверждениями.*

1. $L_{m,n,1} = m^3/36 + 7m^2/24 + 11m/12 + 1 - (m \bmod 2)/8 - (m \bmod 3)/9$.
2. *При $4 \leq 2m+n \leq 6$ и $3 \leq d \leq 4$ значения $L_{m,n,2m+n-d+1}$ представлены в таблице:*

(m,n)	$(2,0)$	$(1,2)$	$(2,1)$	$(1,3)$	$(2,2)$	$(1,4)$	$(3,0)$
$d=3$	2	1	2	1	0	0	0
$d=4$	4	2	2	1	1	0	0

3. *Если $2m+n=6$, то $L_{m,n,2} = 0$.*
4. *Если $2m+n > 6$ и $2 < d < 2m+n$, то $L_{m,n,2m+n-d+1} = 0$.*

Доказательство разобьем на несколько частей.

2.3. $((m,n), 4^1, 2m+n)$ МДР коды

Предложение 5. *Число $L_{m,n,1}$ неэквивалентных МДР кодов с расстоянием $2m+n$ в графе дуба $D(m,n)$ вычисляется по формуле*

$$L_{m,n,1} = m^3/36 + 7m^2/24 + 11m/12 + 1 - (m \bmod 2)/8 - (m \bmod 3)/9.$$

Для начала докажем две следующие леммы:

Лемма 15. *Для любого $n \geq 0$ выполняется $L_{m,n,1} = L_{m,0,1}$.*

Доказательство. Пусть даны два $((m,n),4^1,2m+n)$ МДР кода C и C'. Легко увидеть, что эти коды эквивалентны тогда и только тогда, когда эквивалентны проекции $C_{1,\dots,n}$ и $C'_{1,\dots,n}$. Из этого следует утверждение леммы. ▲

Лемма 16. *Пусть $U=\{u_0,u_1,u_2,u_3\}$ — коклика в* Sh. *Тогда*

1. *Если U — линейная, то существует автоморфизм τ графа* Sh *такой, что:*

   $\tau(u_0)=00$, $\tau(u_1)=02$, $\tau(u_2)=20$, $\tau(u_3)=22$;

2. *Если U — полулинейная, то выполняется ровно одно из следующих утверждений:*

   1) существует автоморфизм τ графа Sh *такой, что*

   $\tau(u_0)=00$, $\tau(u_1)=02$, $\tau(u_2)=21$, $\tau(u_3)=23$;

   2) существует автоморфизм τ графа Sh *такой, что*

   $\tau(u_0)=00$, $\tau(u_1)=21$, $\tau(u_2)=02$, $\tau(u_3)=23$;

   3) существует автоморфизм τ графа Sh *такой, что*

   $\tau(u_0)=00$, $\tau(u_1)=21$, $\tau(u_2)=23$, $\tau(u_3)=02$.

Доказательство.

1. Пусть U — линейная. Тогда вершину u_0 можно перевести в вершину 00 автоморфизмом $\theta(s)=s-u_0$. Тогда множество $\{u_1,u_2,u_3\}$ перейдет во множество $\{02,20,22\}$, а все различные перестановки элементов множества $\{02,20,22\}$ дают, например, автоморфизмы $\tau_1(ab)=ab$, $\tau_2(ab)=ba$, $\tau_3(ab)=a(a-b)$, $\tau_4(ab)=(b-a)b$, $\tau_5(ab)=(a-b)a$, $\tau_6(ab)=b(b-a)$.

2. Пусть U — полулинейная. Для начала докажем то, что хотя бы одно из утверждений верно. U некоторым автоморфизмом σ можно перевести во множество $\{00,02,21,23\}$. Тогда вершину $\sigma(u_0)$ можно перевести в вершину 00 автоморфизмом $\theta(s)=s-\sigma(u_0)$. Тогда, так как $\sigma(u_0)$ принадлежит $\{00,02,21,23\}$, то легко убедиться, что элемент $(-\sigma(u_0))$ также принадлежит этому множеству и θ переводит $\{00,02,21,23\}$ в себя.

Поменять местами вершины 21 и 23 можно, например, автоморфизмом $\delta(ab) = (-a)(-b)$. То, что верно ровно одно из утверждений, следует из леммы 7.

▲

Доказательство предложения 5. Из леммы 15 следует, что достаточно рассматривать только МДР коды, в параметрах которых $n = 0$.

Пусть C — $((m, 0), 4^1, 2m)$ МДР код. После некоторого упорядочивания обозначим его вершины через $c^i = (s_1^i, \ldots, s_m^i)$, где $i = 0, 1, 2, 3$. Также обозначим $A_i = \{s_i^0, s_i^1, s_i^2, s_i^3\}$, $i = 1, \ldots, m$. Из кодового расстояния следует, что A_i — коклика для каждого i.

Назовем $((m, 0), 4^1, 2m)$ МДР код C *приведенным*, если для некоторых l, j, t таких, что $l \leq j \leq t$, выполнено:

$s_i^0 = 00$, $s_i^1 = 02$, $s_i^2 = 21$, $s_i^3 = 23$, $i = 1, \ldots, l$;

$s_i^0 = 00$, $s_i^1 = 21$, $s_i^2 = 02$, $s_i^3 = 23$, $i = l + 1, \ldots, l + j$;

$s_i^0 = 00$, $s_i^1 = 21$, $s_i^2 = 23$, $s_i^3 = 02$, $i = l + j + 1, \ldots, l + j + t$;

$s_i^0 = 00$, $s_i^1 = 02$, $s_i^2 = 20$, $s_i^3 = 22$, $i = l + j + t + 1, \ldots, m$.

Так как для любой такой тройки (l, j, t) приведенный код определяется единственным образом, обозначим этот код через $C^{l,j,t}$.

Обозначим через T_m число различных приведенных $((m, 0), 4^1, 2m)$ МДР кодов. Это число равно количеству таких четверок $(m - l - j - t, l, j, t)$, что $l \leq j \leq t$. Тогда по лемме 14 имеем $T_m = m^3/36 + 7m^2/24 + 11m/12 + 1 - (m \bmod 2)/8 - (m \bmod 3)/9$.

Для $((m, 0), 4^1, 2m)$ МДР кода C определим четверку чисел $(a, b, c, d)_C$, где $b \leq c \leq d$.

Значение a — число линейных коклик во множестве $\{A_i : i = 1, \ldots, m\}$. Пусть $N_i(C)$ — число элементов порядка 2 во множестве $\{(s_j^0 - s_j^i) : j = 1, \ldots, m\}$, $i = 1, 2, 3$. Пусть $M_i(C) = N_i(C) - a$. Упорядочив значения $M_1(C)$, $M_2(C)$, $M_3(C)$, мы получим значения b, c, d.

Докажем, что четверка $(a, b, c, d)_C$ не зависит от упорядочивания вершин кода. Для значения a это тривиально. Достаточно доказать, что если поменять местами кодовые вершины c^1, c^2, c^3, либо поменять местами вершины c^0 и c^1, то значения b, c, d не изменятся. Если поменять местами кодовые вершины c^1, c^2, c^3, то изменится только порядок $N_1(C)$, $N_2(C)$, $N_3(C)$, следовательно, значения b, c, d не изменятся. Определим $N'_i(C)$ — количество элементов порядка 2 во множестве $\{(s^1_j - s^i_j : j = 1, \ldots, m)\}$, $i = 0, 2, 3$. Очевидно, что $N_1(C) = N'_0(C)$. Также $N_2(C) = N'_3(C)$. Действительно, так как для любого $j = 1, \ldots, m$ множество $\{s^0_j, s^1_j, s^2_j, s^3_j\}$ является кокликой, порядок элемента $(s^1_j - s^3_j)$ равен порядку элемента $(s^0_j - s^2_j)$ (достаточно проверить это для коклик $\{00, 02, 20, 22\}$ и $\{00, 02, 21, 23\}$). Аналогично $N_3(C) = N'_2(C)$. Следовательно, если поменять местами вершины c^0 и c^1, то значения b, c, d не изменятся.

Если два $((m, 0), 4^1, 2m)$ МДР кода C и C' эквивалентны, то соответствующие им четверки $(a, b, c, d)_C$ и $(a, b, c, d)_{C'}$ совпадают. Действительно, очевидно, что перестановка координат в коде C не меняет $(a, b, c, d)_C$. Также по лемме 7 набор автоморфизмов графа Шрикханде не меняет $(a, b, c, d)_C$.

Для приведенного кода $D = C^{l,j,t}$ четверка $(a, b, c, d)_D$ равна $(m - l - j - t, l, j, t)$. Тогда, если тройки чисел (l_1, j_1, t_1) и (l_2, j_2, t_2) не совпадают, то коды C^{l_1,j_1,t_1} и C^{l_2,j_2,t_2} не эквивалентны. Тогда все приведенные коды попарно неэквивалентны, следовательно, $T_m \leq L_{m,n,1}$.

Докажем, что произвольный $((m, 0), 4^1, 2m)$ МДР код C эквивалентен некоторому приведенному коду. Этому коду соответствует четверка $(a, b, c, d)_C$. Тогда можно взять перестановку координат π такую, что для кода C', полученного из кода C при помощи перестановки координат π, выполнено:

элемент $(s^0_j - s^1_j)$ имеет порядок 2, $j = 1, \ldots, b$;

элемент $(s^0_j - s^2_j)$ имеет порядок 2, $j = b + 1, \ldots, b + c$;

элемент $(s^0_j - s^3_j)$ имеет порядок 2, $j = b + c + 1, \ldots, b + c + d$;

множество $\{s^0_j, s^1_j, s^2_j, s^3_j\}$ — линейная коклика, $j = b + c + d + 1, \ldots, m$.

Тогда по лемме 16 существует набор автоморфизмов $\tau_1, \ldots, \tau_m$ графа Шрик-

ханде, переводящий код C' в приведенный код $C^{b,c,d}$. Отсюда следует, что $L_{m,n,1} \leq T_m$. Тогда $L_{m,n,1} = T_m$, что доказывает предложение. ▲

2.4. $((m,n),4^2,2m+n-1)$ МДР коды

Предложение 6. *(1) Числа $L_{2,0,2}$ и $L_{1,2,2}$ МДР кодов с расстоянием 3 в графах Дуба диаметра 4 равны $L_{2,0,2} = 2$, $L_{1,2,2} = 1$.*

(2) Числа $L_{2,1,2}$ и $L_{1,3,2}$ МДР кодов с расстоянием 4 в графах Дуба диаметра 5 равны $L_{2,1,2} = 2$, $L_{1,3,2} = 1$.

Доказательство. Рассмотрим МДР коды с параметрами $((2,0),4^2,3)$ и $((1,2),4^2,3)$. Пусть C — один из таких кодов. Представим кодовые слова в виде $(a, f(a))$, где $a \in {}_v\mathrm{Sh}$, а $f(a) \in {}_v\mathrm{Sh}$ в случае $((2,0),4^2,3)$ МДР кода, $f(a) \in {}_vK^2$ в случае $((1,2),4^2,3)$ МДР кода. Из кодового расстояния следует, что отображение f является биекцией.

Для кода C определим разбиение L^C графа Шрикханде на коклики.

Для начала определим графы $G_1(V_1,E_1)$, $G_2(V_f,E_2)$ и $G_f(V_1,E_f)$, где $V_1 = {}_v\mathrm{Sh}$, $V_f = \{f(a) : a \in V_1\}$ и

$$E_1 = \{(a_1,a_2) : d(a_1,a_2) = 1, a_1, a_2 \in V_1\},$$

$$E_2 = \{(f(a_1),f(a_2)) : d(f(a_1),f(a_2)) = 1, f(a_1), f(a_2) \in V_f\},$$

$$E_f = \{(a_1,a_2) : d(f(a_1),f(a_2)) = 1, a_1, a_2 \in V_1\}.$$

Очевидно, G_1 — граф Шрикханде, G_2 —граф Шрикханде либо граф K^2. Граф G_f изоморфен графу G_2, следовательно, также является графом Шрикханде либо графом K^2.

Множества ребер E_1 и E_f не пересекаются (если некоторое ребро (a,b) лежит в пересечении, то между кодовыми вершинами $(a,f(a))$ и $(b,f(b))$ расстояние равно 2).

Из леммы 13 следует, что существует единственное разбиение $V_1 = L_0 \cup L_1 \cup L_2 \cup L_3$ такое, что : $|L_i| = 4$ для каждого $i = 0, 1, 2, 3$, и вершины a и b графа $G_3 = (V_1, \overline{E_1 \cup E_f})$ смежны тогда и только тогда, когда a и b принадлежат одному и тому же множеству L_i для некоторого $i = 0, 1, 2, 3$. Множества вершин L_0, L_1, L_2, L_3 будут попарно непересекающимися кокликами в графах G_1 и G_f. Тогда определим $L^C = \{L_0, L_1, L_2, L_3\}$.

Для каждой вершины a графа Шрикханде обозначим через $L^C(a)$ ту коклику разбиения, которой она принадлежит.

Из построения следует:

Лемма 17. *Пусть C — МДР код с параметрами $((2,0), 4^2, 3)$ либо $((1,2), 4^2, 3)$. Тогда расстояние между двумя различными кодовыми вершинами $(a, f(a))$ и $(b, f(b))$ равно 4 тогда и только тогда, когда $b \in L^C(a)$, и равно 3 иначе.*

Также определим $R_i = \{f(a) : a \in L_i\}$. По лемме 17 R_i является кокликой в графе G_2 для каждого $i = 0, 1, 2, 3$. Для каждой вершины a обозначим через $R^C(a)$ то множество из этого разбиения, которому оно принадлежит. По определению вершина $a \in L^C(b)$ тогда и только тогда, когда вершина $f(a) \in R^C(f(b))$.

Пусть L — разбиение графа Шрикханде на коклики. Тогда если вершины a и b принадлежат одной коклике, то обозначим это через aLb, и обозначим $a\overline{L}b$ иначе.

Для разбиения L единственным образом можно определить граф $G_L = (V, E_L)$, где $V = \text{vSh}$ и

$$E_L = \{(a, b) : d(a, b) = 2, a\overline{L}b\}.$$

Пусть $L^C = L$ для некоторого кода C. Тогда f — такое отображение, что $d(f(a), f(b)) = 1$ тогда и только тогда, когда $(a, b) \in E_L$. Отсюда следует, что если $L^C = L^{C'}$ для некоторого кода C', то $d(f(a), f(b)) = d(f'(a), f'(b))$ для любой пары вершин из Sh, следовательно, коды C и C' эквивалентны. Также если разбиения L^C и $L^{C'}$ эквивалентны, то и коды C и C' эквивалентны.

Действительно, так как разбиения эквивалентны, то код C' эквивалентен некоторому коду C'' такому, что $L^{C''} = L^C$. Тогда коды C и C'' эквивалентны, а следовательно, коды C и C' также эквивалентны. Тогда если для некоторого разбиения L найти такой код C, что для отображения f из V_1 в V_f множество $E_L = \{(a, b) : d(f(a), f(b))\}$, то любой другой код C' такой, что разбиение $L^{C'}$ эквивалентно разбиению L^C, эквивалентен C.

В графе Шрикханде существует три неэквивалентных разбиения на клики. Эти разбиения изображены на рис. 2.3.

Если L — разбиение (а), то G_L — граф Шрикханде. При этом разбиение $\{R_i : i = 0, 1, 2, 3\}$, где $R_i = \{f(a) : a \in L_i\}$, является также разбиением (а).

Если L — разбиение (б), то G_L — граф Шрикханде. При этом разбиение $\{R_i : i = 0, 1, 2, 3\}$, где $R_i = \{f(a) : a \in L_i\}$, является разбиением (б). Тогда МДР коды, соответствующие разбиениям (а) и (б), неэквивалентны.

Если L — разбиение (в), то G_L — граф K^2.

Таким образом мы получаем, что неэквивалентных $((2, 0), 4^2, 3)$ МДР кодов ровно 2, а $((1, 2), 4^2, 3)$ МДР код единственный с точностью до эквивалентности. Это доказывает пункт 1 предложения 6.

Пусть теперь C — МДР код с параметрами $((2, 1), 4^2, 4)$ (с параметрами $((1, 3), 4^2, 4)$). Обозначим его вершины через $(a, f(a), g(a))$, где $a \in \mathrm{Sh}$, $f(a) \in {}_v\mathrm{Sh}$ ($f(a) \in {}_vK^2$) , $g(a) \in {}_vK$. Проекция $D = C_{;1}$ — МДР код с параметрами $((2, 0), 4^2, 3)$ (для $((1, 3), 4^2, 4)$ МДР кода $D = C_{;3}$ — $((1, 2), 4^2, 3)$ МДР код). Из леммы 17 следует, что если b не принадлежит $L^D(a)$, то из кодового расстояния получаем, что $g(a) \neq g(b)$. Так как для каждого $i = 0, 1, 2, 3$ выполнено $|C^{;i}_{;1}| = 4$ ($|C^{;i}_{;3}| = 4$), то $g(a) = g(b)$ тогда и только тогда, когда $a \in L^D(b)$, и по заданному коду $C_{;1}$ код C восстанавливается однозначно с точностью до перестановки из Sym_4. Отсюда следует, что $L_{2,1,2} = L_{2,0,2}$ и $L_{1,3,2} = L_{1,2,2}$. ▲

Также из построения следует:

Лемма 18. *Пусть C — МДР код с параметрами $((2, 1), 4^2, 4)$ либо $((1, 3), 4^2, 4)$.*

Тогда расстояние между любыми двумя различными кодовыми вершинами равно 4.

2.5. $((m,n),4^3,2m+n-2)$ МДР коды

2.5.1. МДР коды с параметрами $((2,1),4^3,3)$ и $((1,3),4^3,3)$

Предложение 7. $L_{2,1,3}=2$, $L_{1,3,3}=1$.

В данном разделе рассмотрим МДР коды с параметрами $((2,1),4^3,3)$ и $((1,3),4^3,3)$. Пусть C — один из таких кодов. Представим кодовые вершины в виде $(f_k(a),a,k)$, где $k\in {}_{\mathrm{v}}K$, $f_k(a)\in {}_{\mathrm{v}}\mathrm{Sh}$ и a — в первом случае вершина графа Шрикханде, во втором вершина графа K^2.

Обозначим через D_i сечение $C^{;i}_{;1}$ ($D_i=C^{;i}_{;3}$ в случае $((1,3),4^3,3)$ МДР кода).

Для начала докажем следующую лемму.

Лемма 19. *Пусть C — МДР код с параметрами $((2,1),4^3,3)$ либо $((1,3),4^3,3)$. Тогда*

(i) *для любой вершины a и любых различных $i,j\in\{0,1,2,3\}$ выполняется $d(f_i(a),f_j(a))=2$;*

(ii) *для любой вершины a и для любого $i=1,2,3$*

$$\{f_k(a):\ k=0,1,2,3\}=L^{D_0}(f_0(a))=L^{D_i}(f_i(a));$$

(iii) *для любой вершины a и для любого $i=1,2,3$*

$$R^{D_i}(a)=R^{D_0}(a);$$

(iv) *для любого $i=1,2,3$ и любой пары вершин a и b*

$$d(f_0(a),f_0(b))=d(f_i(a),f_i(b)).$$

Доказательство.

(i) Так как расстояние между соответствующими вершинами $(f_i(a), a, i)$ и $(f_j(a), a, j)$ кода C не меньше трех, то расстояние между вершинами $f_i(a)$ и $f_j(a)$ равно 2.

(ii) По лемме 11 найдется b такое, что $(f_1(a), b, 0) \in C$ (т.е. $f_0(b) = f_1(a)$).

Так как расстояние между вершинами $(f_1(a), a, 1)$ и $(f_1(a), b, 0)$ из C не меньше 3, расстояние между a и b равно 2. Тогда из (i) следует, что расстояние между вершинами $(f_0(a), a, 0)$ и $(f_1(a), b, 0)$ равно 4. Следовательно, по лемме 17 $f_1(a) \in L^{D_0}(f_0(a))$. Аналогично получаем $f_2(a) \in L^{D_0}(f_0(a))$ и $f_3(a) \in L^{D_0}(f_0(a))$, кроме того, тривиально $f_0(a) \in L^{D_0}(f_0(a))$. В итоге имеем $\{f_k(a) : k = 0, 1, 2, 3\} = L^{D_0}(f_0(a))$, оставшиеся три равенства аналогичны.

(iii) Пусть вершина $b \in R^{D_0}(a)$. Тогда по определению $f_0(b) \in L^{D_0}(f_0(a)) = \{f_0(a), f_1(a), f_2(a), f_3(a)\}$, следовательно, $f_0(b) = f_j(a)$ для некоторого $j = 1, 2, 3$. Тогда $f_i(b) \in \{f_0(b), f_1(b), f_2(b), f_3(b)\} = L^{D_i}(f_0(b)) = L^{D_i}(f_j(a)) = \{f_0(a), f_1(a), f_2(a), f_3(a)\} = L^{D_i}(f_i(a))$ для любого $i = 1, 2, 3$. Тогда $b \in R^{D_i}(a)$ и пункт леммы доказан.

(iv) Пусть $a \neq b$. По лемме 17 расстояние $d((f_i(a), a, i), (f_i(b), b, i))$ равно 4, если $b \in R^{D_i}(a)$, и равно 3 в противном случае. Но согласно (iii) имеем $R^{D_i}(a) = R^{D_0}(a)$, откуда следует, что это расстояние не зависит от i. А значит, и расстояние между $f_i(a)$ и $f_i(b)$ не зависит от i.

▲

Лемма 20. *Пусть $U = \{U_0, U_1, U_2, U_3\}$ — разбиение графа Шрикханде на непересекающиеся коклики. Тогда существует единственный набор из трех автоморфизмов графа Шрикханде τ_1, τ_2, τ_3 такой, что для любого $j = 0, 1, 2, 3$, для любого $i = 1, 2, 3$ и для любой вершины графа Шрикханде s выполнено:*

1) если $s \in U_j$, то $\tau_i(s) \in U_j$;

2) $d(\tau_i(s), s) = 2$;

3) $d(\tau_i(s), \tau_j(s)) = 2$ при $i \neq j$.

Доказательство.

Обозначим $A = \{02, 20, 22\}$, $B = \{12, 32, 21, 23, 13, 31\}$.

Для начала рассмотрим случай, когда U — разбиение (а) из рис. 2.3. Пусть τ — автоморфизм, удовлетворяющий условиям 1 и 2. Тогда для любой вершины $s \in {}_{\mathrm{v}}\mathrm{Sh}$ либо $\tau(s) = s + 02$, либо $\tau(s) = s + 20$, либо $\tau(s) = s + 22$.

Пусть $\tau(a) = a + 02$ для некоторой вершины a. Докажем, что тогда $\tau(s) = s + 02$ для любой вершины $s \in {}_{\mathrm{v}}\mathrm{Sh}$. Вершины $a + 01$ и $a + 03$ принадлежат одной и той же линейной коклике U_i для некоторого $i = 0, 1, 2, 3$. Так как a переходит в вершину $a + 02$, вершины $a + 01$ и $a + 03$ переходят в вершины из U_i, принадлежащие окрестности вершины $a + 02$. По лемме 10 таких вершин ровно 2, и это вершины $a + 01$ и $a + 03$. Тогда $\tau(a + 01) = a + 03$ и $\tau(a + 03) = a + 01$ по условию 2. Так как у вершин $a + 01$ и $a + 03$ ровно 2 общих соседа, множество вершин $\{a, a + 02\}$ переходит во множество $\{a, a + 02\}$, а следовательно, $\tau(a + 02) = a$. Предположим, что $\tau(b) \neq b + 02$ для некоторой вершины $b \in {}_{\mathrm{v}}\mathrm{Sh}$. Пусть $\tau(b) = b + 20$. Тогда, аналогично, $\tau(b + 10) = b + 30$, $\tau(b + 20) = b$, $\tau(b + 30) = b + 10$. Множества вершин $\{a, a + 01, a + 02, a + 03\}$ и $\{b, b + 10, b + 20, b + 30\}$ пересекаются в некоторой вершине c. Тогда $\tau(c) = c + 02$ и $\tau(c) = c + 20$, и мы получаем противоречие. Аналогично, если $\tau(b) = b + 22$.

Аналогично доказывается для любого $x \in A$, что если $\tau(a) = a + x$ для некоторой вершины a, то $\tau(s) = s + x$ для любой вершины $s \in {}_{\mathrm{v}}\mathrm{Sh}$. Тогда набор автоморфизмов $\tau_1(s) = s + 02$, $\tau_2(s) = s + 20$, $\tau_3(s) = s + 22$ является единственным набором, удовлетворяющим условиям 1–3.

Рассмотрим случай, когда U — разбиение (б) или (в) из рис. 2.3.

Пусть a, b, c — различные попарно смежные вершины в Sh. Тогда если вершина d не совпадает с a, b, c и смежна с двумя из этих вершин, скажем с a и b, то по значениям $\tau(a)$, $\tau(b)$, $\tau(c)$ однозначно восстанавливается значение $\tau(d)$.

Это следует из того, что $\tau(c)$ и $\tau(d)$ будут общими соседями вершин $\tau(a)$ и $\tau(b)$, а так как у любой пары вершин в Sh ровно 2 общих соседа, то значение $\tau(d)$ определяется однозначно. Тогда, используя это свойство, нетрудно убедиться, что по значениям $\tau(a)$, $\tau(b)$, $\tau(c)$ однозначно задаются значения $\tau(s)$ для любой вершины $s \in {}_{\mathrm{v}}\mathrm{Sh}$.

Пусть τ — автоморфизм, удовлетворяющий условиям 1 и 2. Докажем, что если $\tau(s) = s + x$, где $x \in B$, для некоторой вершины s, то τ определяется однозначно по разбиению U. Вершины s и $s+x$ имеют 2 общих соседа, скажем вершины a и b. Так как элемент x имеет порядок 4, то по лемме 6 вершины a и b смежны, а следовательно, принадлежат разным кокликам из U, скажем U_i и U_j, где $i \neq j$. По лемме 10 в окрестности вершины $s + x$ есть ровно одна вершина $c \neq a$, принадлежащая U_i, а также ровно одна вершина $d \neq b$, принадлежащая U_j. Тогда $\tau(a) = a$ либо $\tau(a) = c$. Первое неверно по свойству 2. Следовательно, $\tau(a) = c$. Аналогично, $\tau(b) = d$. То есть значения $\tau(a)$ и $\tau(b)$ по U определяются однозначно. Тогда так как вершины a, b, s попарно смежны, то по значениям $\tau(a)$, $\tau(b)$, $\tau(s)$ автоморфизм τ восстанавливается однозначно. Таким образом, если существует автоморфизм τ, удовлетворяющий условиям 1 и 2, такой, что $\tau(s) = s + x$ для некоторой вершины s, где $x \in B$, то такой автоморфизм единственный. В разбиении U найдется полулинейная коклика. Тогда эту коклику можно представить в виде $\{s, s+x, s+y, s+z\}$, где $x, y \in B$, $z \in A$, $s \in {}_{\mathrm{v}}\mathrm{Sh}$. Тогда для набора автоморфизмов τ_1, τ_2, τ_3, удовлетворяющих условиям 1–3, $\tau_1(s) = s + x$, $\tau_2(s) = s + y$, $\tau_3(s) = s + z$. Автоморфизмы τ_1 и τ_2 определяются однозначно. Тогда, так как для любого $i = 0, 1, 2, 3$ и для любой вершины $s \in U_i$ множество $\{s, \tau_1(s), \tau_2(s), \tau_3(s)\}$ равно U_i, то для любой вершины s значение $\tau_3(s)$ определяется однозначно по значениям $\tau_1(s)$ и $\tau_2(s)$. Таким образом, если существует набор автоморфизмов τ_1, τ_2, τ_3, то он единственный.

Осталось привести такой набор автоморфизмов для каждого разбиения.

Пусть $U_0 = \{00, 02, 21, 23\}$, $U_1 = \{01, 03, 22, 20\}$, $U_2 = \{10, 12, 30, 32\}$, $U_3 = \{11, 13, 31, 33\}$. Тогда

$\tau_1(ab) = a(a-b)+21$, $\tau_2(ab) = ab+02$, $\tau_3(ab) = a(a-b)+23$.

Пусть $U_0 = \{00, 02, 21, 23\}$, $U_1 = \{01, 03, 20, 22\}$, $U_2 = \{10, 12, 31, 33\}$, $U_3 = \{11, 13, 30, 32\}$. Тогда

$\tau_1(ab) = ab+02$, $\tau_2(ab) = ab+21$, $\tau_3(ab) = ab+23$.

Пусть $U' = \{U'_0, U'_1, U'_2, U'_3\}$ и $U = \{U_0, U_1, U_2, U_3\}$ эквивалентные разбиения. Тогда существует автоморфизм ϕ, переводящий U в U', и $U'_j = \{\phi(x) : x \in U_j\}$, $j = 0, 1, 2, 3$,

Тогда если набор автоморфизмов τ_1, τ_2, τ_3 удовлетворяет условиям 1–3 для разбиения U, то набор автоморфизмов $\sigma_i(s) = \phi(\tau_i(\phi^{-1}(s)))$, $i = 1, 2, 3$, удовлетворяет условиям 1–3 для разбиения U'.

Действительно, пусть вершина $s \in U'_j$. Тогда $\phi^{-1}(s) \in U_j$, $\tau_i(\phi^{-1}(s)) \in U_j$, $\phi(\tau_i(\phi^{-1}(s))) \in U'_j$, т.е. условие 1 выполняется. Если для некоторого $i = 1, 2, 3$ автоморфизм σ_i не удовлетворяет условию 2, то из условия 1 следует, что $\sigma_i(s) = s$ для некоторой вершины s. Но тогда $\tau_i(\phi^{-1}(s)) = \phi^{-1}(s)$, и мы получаем противоречие. Если не выполняется условие 3, то для некоторых $i \neq j$ и некоторой вершины s имеем $\sigma_i(s) = \sigma_j(s)$, а следовательно, $\tau_i(\phi^{-1}(s)) = \tau_j(\phi^{-1}(s))$, и мы получаем противоречие. ▲

Доказательство предложения 7. Пусть C — МДР код с параметрами $((2,1), 4^3, 3)$ (либо $((1,3), 4^3, 3)$). Сечение $D_0 = C^{;0}_{;1}$ ($D_0 = C^{0;}_{3;}$) является МДР кодом с параметрами $((2,0), 4^2, 3)$ $((1,2), 4^2, 3)$ соответственно). Обозначим через L_0, L_1, L_2, L_3 — разбиение на коклики, определенное следующим образом: вершины a и b принадлежат одному и тому же множеству тогда и только тогда, когда $a \in L^{D_0}(b)$. Так как f_0 — биекция, то для $i = 1, 2, 3$ можно обозначить $\tau_i(s) = f_i(f_0^{-1}(s))$. Из пункта (iv) леммы 19 следует, что τ_i — автоморфизм для любого $i = 1, 2, 3$. По пункту (i) леммы 19 для любой вершины $s = f_0(a)$ графа Шрикханде и для любого $i = 1, 2, 3$ выполнено $d(\tau_i(s), s) = 2$. Также по пункту (i) леммы 19 для любой вершины $s = f_0(a)$ и любых $i \neq j$ выполнено $d(\tau_i(s), \tau_j(s)) = 2$. Из пунктов (ii) и (iii) леммы 19 следует, что для любой вершины $s = f_0(a)$, любого $i = 1, 2, 3$ и любого $j = 0, 1, 2, 3$ выполнено:

если $s \in L_j$, то $\tau_i(s) \in L_j$. Тогда из леммы 20 следует, что если для любой вершины $a \in {}_{\mathrm{v}}\mathrm{Sh}$ известно значение $f_0(a)$, то для любой вершины $a \in {}_{\mathrm{v}}\mathrm{Sh}$ и любого $i = 1, 2, 3$ значение $f_i(a)$ восстанавливается с точностью до перестановки значений i. Из этого следует, что если эквивалентны сечения $C^{;0}_{;1}$ и $C'^{;0}_{;1}$ ($C^{;0}_{;3}$ и $C'^{;0}_{;3}$ для $((1,3),4^3,3)$ МДР кода) МДР кодов C и C' с параметрами $((2,1),4^3,3)$ ($((1,3),4^3,3)$), то коды C и C' эквивалентны.

Так как $((2,0),4^2,3)$ МДР кодов 2 с точностью до эквивалентности, то $L_{2,1,3} = L_{2,0,2} = 2$. Аналогично, $L_{1,3,3} = L_{1,2,2} = 1$. ▲

2.5.2. МДР коды с параметрами $((2,2),4^3,4)$ или $((1,4),4^3,4)$

Предложение 8. $L_{2,2,3} = 1$, $L_{1,4,3} = 0$.

Доказательство. При доказательстве будем рассматривать $((2,2),4^3,4)$ МДР коды. Для $((1,4),4^3,4)$ МДР кодов рассуждения аналогичны. Пусть C — МДР код с параметрами $((2,2),4^3,4)$ (с параметрами $((1,4),4^3,4)$). Обозначим его вершины через $(f_i(a), a, i, g_i(a))$, где $f_i(a) \in {}_{\mathrm{v}}\mathrm{Sh}$, $a \in {}_{\mathrm{v}}\mathrm{Sh}$ ($a \in {}_{\mathrm{v}}K^2$), а i, $g_i(a) \in {}_{\mathrm{v}}K$.

Обозначим $P = C_{;2}$ (для $((1,4),4^3,4)$ МДР кода $P = C_{;4}$). Обозначим $D_i = P^{;i}_{;1}$ ($D_i = P^{;i}_{;3}$ соответственно). По лемме 19 разбиения $\{L^{D_i}(a) : a \in {}_{\mathrm{v}}\mathrm{Sh}\}$ и $\{R^{D_i}(a) : a \in {}_{\mathrm{v}}\mathrm{Sh}\}$ не зависят от i. Обозначим эти разбиения через L и R соответственно, а коклики из этих разбиений через L_i и R_i, $i = 0, 1, 2, 3$. Если вершины a, b принадлежат одной и той же коклике, то обозначим это через $a \overset{L}{\sim} b$ и $a \overset{R}{\sim} b$ соответственно.

Если C — $((2,2),4^3,4)$ МДР код, то P — $((2,1),4^3,3)$ МДР код. Таких кодов 2 с точностью до эквивалентности. В одном случае разбиение L эквивалентно разбиением (а) из рис. 2.3, в другом разбиение L эквивалентно разбиению (б) из рис. 2.3. Если C — МДР код с параметрами $((1,4),4^3,4)$, то P имеет параметры $((1,3),4^3,3)$. Такой код единственен с точностью до эквивалентности, а L эквивалентно разбиению (в) из рис. 2.3.

Докажем, что L — разбиение (a) из рис. 2.3. Из этого будет следовать, что МДР код P определяется однозначно с точностью до эквивалентности, а также то, что $((1,4),4^3,4)$ МДР кодов не существует.

Для начала докажем ряд утверждений:

1. *Для любого* $i = 0,1,2,3$ *выполняется* $L_t = \{f_i(a) : a \in R_t\}$.

По пунктам (ii) и (iii) леммы 19.

2. *Для любой вершины* a *если* $i \neq j$, *то* $d((f_i(a),(f_j(a)) = 2$.

По пункту (i) леммы 19.

3. *Для любых* $i \neq j$ *и для любой вершины* a *выполняется* $g_i(a) \neq g_j(a)$.

Иначе получим противоречие с кодовым расстоянием.

4. *Для любого* $i = 0,1,2,3$ *равенство* $g_i(a) = g_i(b)$ *имеет место тогда и только тогда, когда* $a \overset{R}{\sim} b$.

Рассмотрим сечение $U = C^{;i}_{;1}$ ($C^{;i}_{;3}$). По лемме 18 расстояние между вершинами $(f_i(a), a, g_i(a))$ и $(f_i(b), b, g_i(b))$ равно 4. Получается, что $g_i(a) = g_i(b)$ тогда и только тогда, когда расстояние между $(f_i(a), a)$ и $(f_i(b), b)$ равно 4. По лемме 17 для проекции $U_{;1}$ ($U_{;3}$) последнее эквивалентно соотношению $a \overset{R}{\sim} b$.

5. *Если* $i \neq 0$ *и* $g_0(a) = g_i(b)$, *то* $d(f_0(a), f_0(b)) = d(f_0(a), f_i(b))$.

Из пункта 3 следует, что $g_0(b) \neq g_i(b)$, следовательно, $g_0(a) \neq g_0(b)$. Из пункта 4 следует, что $a \overset{R}{\not\sim} b$. Вершины $(f_0(a), a, g_0(a))$ и $(f_0(b), b, g_0(b))$ принадлежат сечению $C^{;0}_{;1}$ ($C^{;0}_{;3}$), следовательно, по лемме 18 расстояние между ними равно 4, и $d((f_0(a), a), (f_0(b), b)) = 3$. Вершины $(f_0(a), a, 0)$ и $(f_i(b), b, i)$ принадлежат сечению $C^{;g_0(a)}_{;2}$ ($C^{;g_0(a)}_{;4}$), следовательно, по лемме 18 расстояние между ними равно 4, и $d((f_0(a), a), (f_i(b), b)) = 3$. Отсюда следует утверждение.

6. *Пусть* $A = \{a_1, a_2, a_3, a_4\}$ *и* $B = \{b_1, b_2, b_3, b_4\}$ — *непересекающиеся коклики графа Шрикханде, и пусть* τ — *автоморфизм графа Шрикханде такой, что для любой вершины* $s \in B$ *выполняется:* $\tau(s) \in B$, $\tau(s) \neq s$ *и* $d(a_i, b_j) = d(a_i, \tau(b_j))$ *для любых* $i, j = 0,1,2,3$. *Тогда подграф на множестве вершин* $A \cup B$ *является объединением двух непересекающихся циклов на* 4 *вершинах.*

Действительно, подграф на множестве вершин $A \cup B$ двудольный, а из леммы 10 следует, что это регулярный граф степени 2. Тогда это либо цикл C_8 на 8 вершинах, либо объединением двух непересекающихся циклов C_4 на 4 вершинах. Но в цикле C_8 найдется пара вершин из A, имеющая ровно одного общего соседа из B, скажем вершину b. Тогда с одной стороны $\tau(b) = b$, а с другой $\tau(b) \neq b$, и мы получаем противоречие.

7. *Пусть $A = \{A_0, A_1, A_2, A_3\}$ — разбиение графа Шрикханде на коклики и для любых $s \neq t$ подграф на множестве вершин $A_s \cup A_t$ является объединением двух непересекающихся циклов на 4 вершинах. Тогда A — разбиение а) из рис. 2.3.*

Доказывается непосредственной проверкой разбиений а), б) и в) из рис. 2.3.

Докажем, что L — разбиение а) из рис. 2.3. Для произвольных $s \neq t$ рассмотрим множества $\{f_0(a) : a \in R_s\}$ и $\{f_0(b) : b \in R_t\}$. По пункту 1 эти множества равны L_s и L_t соответственно. По пункту 4 для любой вершины a из R_s значение $g_0(a)$ равно некоторому g_1. Аналогично, для любой вершины b из R_t значение $g_0(b)$ равно некоторому $g_2 \neq g_1$. По пункту 3 для вершины $b \in R_t$ существует единственное $i \neq 0$ такое, что $g_i(b) = g_1$. Рассмотрим $\tau(s) = f_i(f_0^{-1}(s))$. Из пункта (iv) леммы 19 следует, что τ является автоморфизмом. Из пунктов 1, 2 и 5 следует, что к L_s, L_t и τ можно применить пункт 6. В силу произвольности s и t из пункта 7 следует, что $\{L_i : i = 0, 1, 2, 3\}$ — разбиение а) из рис. 2.3.

МДР код с параметрами $((2, 2), 4^3, 4)$ приведен в приложении. Обозначим его через C. Как и ранее, вершины кода обозначим через $(f_i(a), a, i, g_i(a))$. Докажем, что он единственен с точностью до эквивалентности.

Пусть C' — $((2, 2), 4^3, 4)$ МДР код. Докажем, что он эквивалентен C.

Действительно, проекции $C_{;2}$ и $C'_{;2}$ эквивалентны. Значения $g_0(a)$ для всех $a \in {}_{\mathrm{v}}\mathrm{Sh}$ по пункту 4 определяются с точностью до перестановки. Тогда код C' перестановкой и набором автоморфизмов можно перевести в код C'' такой, что если обозначить вершины кода через $(f'_i(a), a, i, g'_i(a))$, то для любой вершины $a \in {}_{\mathrm{v}}\mathrm{Sh}$ и любого $i = 0, 1, 2, 3$ выполнено $f_i(a) = f'_i(a)$, $g_0(a) = g'_0(a)$.

Докажем, что для любого $i = 1, 2, 3$ и любой вершины $a \in {}_{\mathrm{v}}\mathrm{Sh}$ выполняется $g_i(a) = g'_i(a)$. Предположим обратное. Пусть существует вершина $a \in {}_{\mathrm{v}}\mathrm{Sh}$ и $l \in \{1, 2, 3\}$ такие, что $g_l(a) \neq g'_l(a)$. Тогда по пункту 3 существует $j \neq l, 0$ такое, что $g'_j(a) = g_l(a)$. Вершина a принадлежит R_s для некоторого $s = 0, 1, 2, 3$. Из пункта 4 следует, что для некоторого t имеем $g_0(c) = g_l(a)$ для всех $c \in R_t$, $t \neq s$. Тогда по лемме 10 существует вершина $b \in R_t$ такая, что $d(f_0(a), f_0(b)) = 1$. Так как $g_0(b) = g_l(a)$, то по пункту 5 выполнено $d(f_0(b), f_l(a)) = d(f_0(b), f_0(a)) = 1$. Так как $g'_0(b) = g'_j(a)$, то по пункту 5 выполнено $d(f_0(b), f_j(a)) = d(f_0(b), f_0(a)) = 1$. Тогда вершина $f_0(b)$ смежна с вершинами $f_0(a)$, $f_l(a)$, $f_j(a)$, то есть вершина $f_0(b)$ смежна с тремя вершинами из коклики L_s, и мы получаем противоречие по лемме 10.

Тогда код C'' совпадает с C, а следовательно C' эквивалентен C. ▲

2.5.3. МДР коды с параметрами $((3, 0), 4^3, 4)$

Рассмотрим МДР коды с параметрами $((3, 0), 4^3, 4)$. Пусть C — один из таких кодов. Для любой вершины $a \in {}_{\mathrm{v}}\mathrm{Sh}$ сечение $C^{a;}_{1;}$ является МДР кодом с параметрами $((2, 0), 4^1, 4)$. Тогда множество кодовых вершин можно представить в виде $\{(a, f_i(a), g_i(a)) : i = 0, 1, 2, 3, a \in {}_{\mathrm{v}}\mathrm{Sh}\}$. Также обозначим $F(a) = \{f_i(a) : i = 0, 1, 2, 3\}$, $G(a) = \{g_i(a) : i = 0, 1, 2, 3\}$. Из кодового расстояния следует, что эти множества являются кокликами в Sh.

Предложение 9. *Не существует МДР кодов с параметрами* $((3, 0), 4^3, 4)$.

Доказательство. Предположим обратное. Пусть C — $((3, 0), 4^3, 4)$ МДР код. Докажем несколько утверждений.

1. *Расстояние между любыми двумя различными вершинами кода* C *равно либо* 4*, либо* 6.

Пусть a и b вершины графа Шрикханде такие, что $d(a, b) = 1$. Посчитаем

сумму

$$\begin{aligned} S &= \sum_{i,j=0,1,2,3} d((a, f_i(a), g_i(a)), (b, f_j(b), g_j(b))) = \\ &= 16 \cdot d(a,b) + \sum_{i,j=0,1,2,3} d(f_i(a), f_j(b)) + \sum_{i,j=0,1,2,3} d(g_i(a), g_j(b)). \end{aligned}$$

Множества вершин $\{f_i(a) : i = 0,1,2,3\}$ и $\{f_i(b) : i = 0,1,2,3\}$ — непересекающиеся коклики. По лемме 10 каждая вершина из одного множества соединена ровно с двумя вершинами из другого. Тогда

$$\sum_{i,j=0,1,2,3} d(f_i(a), f_j(b)) = 4(1+1+2+2) = 24.$$

Аналогично,

$$\sum_{i,j=0,1,2,3} d(g_i(a), g_j(b)) = 4(1+1+2+2) = 24.$$

Следовательно, $S = 64$. С другой стороны, так как расстояние между двумя различными кодовыми вершинами не меньше 4, то $S \geq 64$, и неравенство достигается только если $d((a, f_i(a), g_i(a)), (b, f_j(b), g_j(b))) = 4$ для любых $i, j = 0,1,2,3$.

2. *Пусть a_0, a_1, a_2, a_3 различные вершины графа Шрикханде такие, что $d(a_2, a_3) = 2$, а все остальные пары вершин смежны. Тогда множества $F(a_0)$, $F(a_1)$, $F(a_2)$, $F(a_3)$ попарно не пересекаются. Аналогично, попарно не пересекаются множества $G(a_0)$, $G(a_1)$, $G(a_2)$, $G(a_3)$.*

Как следует из кодового расстояния, если вершины a и b смежны, то множества $F(a)$ и $F(b)$ не пересекаются. Поэтому остается доказать, что не пересекаются множества $F(a_2)$ и $F(a_3)$. Предположим обратное. Допустим, что для некоторых k и l имеет место $f_k(a_2) = f_l(a_3)$. По лемме 10 во множестве $F(a_0)$ ровно две вершины, некоторые $f_i(a_0)$ и $f_j(a_0)$, такие, что $d(f_k(a_2), f_i(a_0)) =$

$d(f_k(a_2), f_j(a_0)) = 2$, и во множестве $F(a_1)$ ровно две вершины, некоторые $f_s(a_1)$ и $f_t(a_1)$, такие, что $d(f_k(a_2), f_s(a_1)) = d(f_k(a_2), f_t(a_1)) = 2$. Тогда по пункту 1 вершины $g_i(a_0)$, $g_j(a_0)$, $g_s(a_1)$, $g_t(a_1)$ являются общими соседями для вершин $g_k(a_2)$ и $g_l(a_3)$, а так как в графе Шрикханде любые две различные вершины имеют ровно 2 общих соседа, то $g_k(a_2)$ и $g_l(a_3)$ совпадают. Но тогда

$$d((a_2, f_k(a_2), g_k(a_2)), (a_3, f_l(a_3), g_l(a_3))) = 2,$$

и мы получаем противоречие с кодовым расстоянием. Утверждение для множеств G доказывается аналогично.

3. *Множества $F(a)$ и $F(b)$, а также множества $G(a)$ и $G(b)$, совпадают тогда и только тогда, когда a и b принадлежат одной линейной коклике.*

Пусть a, b, c — три попарно смежные вершины. Тогда по пункту 2 для вершины d, смежной с двумя из этих вершин, множество $F(d)$ однозначно восстанавливается по множествам $F(a)$, $F(b)$, $F(c)$.

Тогда если обозначить $A = F(00)$, $B = F(10)$, $C = F(11)$, то для любой другой вершины a множество $F(a)$ восстанавливается однозначно, и легко убедиться, что утверждение для множеств F выполняется.

Аналогично получается утверждение для множеств G.

4. *Для любой вершины a коклики $F(a)$ и $G(a)$ — линейные .*

По пункту 3 для любой вершины a из Sh множества $(C_{3;})^{a;}_{2;}$ и $(C_{2;})^{a;}_{3;}$ будут линейными кокликами. Кодовые вершины кода C можно представить также в виде $(f'_i(a), a, g'_i(a))$, где $i = 0, 1, 2, 3$, $a \in {}_{\mathrm{v}}\mathrm{Sh}$. Тогда, аналогично, можно доказать, что множества $(C_{3;})^{a;}_{1;}$ и $(C_{1;})^{a;}_{3;}$ будут линейными кокликами для всех $a \in {}_{\mathrm{v}}\mathrm{Sh}$. Также кодовые слова можно представить в виде $(f''_i(a), g''_i(a), a)$, $i = 0, 1, 2, 3$, $a \in {}_{\mathrm{v}}\mathrm{Sh}$. Тогда, аналогично, можно доказать, что множества $(C_{1;})^{a;}_{2;}$ и $(C_{2;})^{a;}_{1;}$ будут линейными кокликами для всех $a \in {}_{\mathrm{v}}\mathrm{Sh}$. Так как $F(a) = (C_{3;})^{a;}_{1;}$, $G(a) = (C_{2;})^{a;}_{1;}$, то утверждение доказано.

Пусть a_0, a_1, a_2, a_3 — различные вершины графа Шрикханде такие, что

$d(a_2, a_3) = 2$, а все остальные пары вершин смежны. По пунктам 2 и 4 коклики $F(a_0)$, $F(a_1)$, $F(a_2)$, $F(a_3)$ — линейные и попарно не пересекаются. Тогда множество вершин $\{f_i(a_j) : i, j = 0, 1, 2, 3\}$ образует граф Шрикханде. Для некоторых $i, j = 0, 1, 2, 3$ вершины $f_i(a_2)$ и $f_j(a_3)$ несмежны. Эти вершины имеют 2 общих соседа, некоторые u и v. Очевидно, что u, v не принадлежат $F(a_2)$ и $F(a_3)$. Так как вершины $f_i(a_2)$ и $f_j(a_3)$ принадлежат разным линейным кокликам, то элемент $(f_i(a_2) - f_j(a_3))$ не принадлежит множеству $\{02, 20, 22\}$. Тогда по лемме 6 вершины u и v смежны. Тогда они не могут принадлежать одной и той же коклике, а значит $u = f_k(a_0)$, $v = f_l(a_1)$ для некоторых k, l. Тогда по пункту 1 вершины $g_k(a_0)$, $g_l(a_1)$, $g_i(a_2)$, $g_j(a_3)$ попарно несмежны. Также по пунктам 2 и 4 коклики $G(a_0)$, $G(a_1)$, $G(a_2)$, $G(a_3)$ — линейные и попарно не пересекаются. Также множество вершин $\{g_i(a_j) : i, j = 0, 1, 2, 3\}$ образуют граф Шрикханде. Вершины $g_k(a_0), g_l(a_1), g_i(a_2), g_j(a_3)$ образуют коклику в этом графе. Но в любой коклике существует такая пара вершин a и b, что элемент $(a - b) \in \{02, 20, 22\}$, то есть a и b принадлежат одной линейной коклике, но вершины из множества $\{g_k(a_0), g_l(a_1), g_i(a_2), g_j(a_3)\}$ принадлежат различным линейным кокликам, следовательно, это множество вершин не может быть кокликой. Это противоречие доказывает предложение. ▲

2.6. Параметры, при которых МДР кодов не существует

Предложение 10. *При $2m + n = 6$ не существует $((m, n), 4^2, 5)$ МДР кодов.*

Доказательство. Допустим такой код существует. Обозначим вершины кода через $(a, f(a), g(a))$, где $a \in {}_{\mathrm{v}}\mathrm{Sh}$, а $f(a)$, $g(a)$ — либо вершина графа Sh, либо вершина графа K^2. Определим на множестве вершин $V = {}_{\mathrm{v}}\mathrm{Sh}$ графы $G_1 = (V, E_1)$, $G_2 = (V, E_2)$, $G_3 = (V, E_3)$, где:

$E_1 = \{(a, b) : a, b \in V, d(a, b) = 1\}$;

$E_2 = \{(a,b) : a,b \in V, d(f(a),f(b)) = 1\}$;

$E_3 = \{(a,b) : a,b \in V, d(g(a),g(b)) = 1\}$.

Множества ребер E_1, E_2, E_3 попарно не пересекаются (иначе получим противоречие с кодовым расстоянием). Каждый из графов G_1, G_2, G_3 является либо графом Шрикханде, либо графом K^2.

Тогда $|E_1 \cup E_2 \cup E_3| = 144$, но в графе на 16 вершинах не больше 120 ребер, и мы получаем противоречие. ▲

Лемма 21. *При $2m+n > 5$ не существует $((m,n), 4^2, 2m+n-1)$ МДР кодов.*

Доказательство. Предположим обратное. Пусть $2m+n > 5$ и C — $((m,n), 4^2, 2m+n-1)$ МДР код. Зафиксируем некоторый набор координат $(i_1, \ldots, i_v; j_1, \ldots, j_w)$ такой, что $2v+w = 2m+n-6$. Тогда по лемме 12 проекция $C_{i_1,\ldots,i_v;j_1,\ldots,j_w}$ является $((m-v, n-w), 4^2, 2(m-v)+(n-w)-1)$ МДР кодом, и так как $2(m-v)+(n-w) = 6$, то применив предложение 10, мы получим противоречие. ▲

Лемма 22. *Если $2m+n \geq 6$, то не существует $((m,n), 4^{2m+n-2}, 3)$ МДР кодов.*

Доказательство. Предположим обратное. Пусть C — $((m,n), 4^{2m+n-2}, 3)$ МДР код. Для произвольной вершины $a \in {}_{\mathrm{v}}D(m,n)$ обозначим шар радиуса 1 с центром в этой вершине через $B_1(a) = \{b \in {}_{\mathrm{v}}D(m,n) : d(a,b) \leq 1\}$. Тогда для любой вершины a мощность $|B_1(a)| = 3(2m+n)+1$. Из кодового расстояния следует, что для любых двух различных кодовых вершин a, b множества $B_1(a)$ и $B_1(b)$ не пересекаются. Тогда из неравенства

$$4^{2m+n-2}(3(2m+n)+1) \leq 4^{2m+n}$$

получаем, что $2m+n \leq 5$. ▲

Лемма 23. *Если $2m+n > 6$, то не существует $((m,n), 4^{2m+n-3}, 4)$ МДР кодов.*

Доказательство. Предположим обратное. Пусть $2m+n > 6$ и C — $((m,n), 4^{2m+n-3}, 4)$ МДР код. Если $n > 0$, то проекция $C_{;1}$ — МДР код с па-

раметрами $((m, n-1), 4^{2m+n-3}, 3)$, и утверждение верно по лемме 22. Пусть $n = 0$. Пусть $(a_1, \ldots, a_m)$ — некоторая вершина кода C. Рассмотрим сечение $C^{a_1,\ldots,a_{m-3};}_{1,\ldots,m-3;}$. Это $((3,0), 4^3, 4)$ МДР код, и мы получаем противоречие по предложению 9. ▲

Предложение 11. *Если $2m + n > 6$ и $2 < d < 2m + n$, то не существует $((m, n), 4^k, d)$ МДР кодов.*

Доказательство. Предположим обратное. Пусть $2m + n > 6$ и C — $((m, n), 4^k, d)$ МДР код. Если $d = 3$ либо $d = 4$, то утверждение верно по леммам 22 и 23 соответственно.

Пусть $d > 5$.

Для начала рассмотрим случай, когда $n = 0$ и k — нечетно. В этом случае d четно и $d \leq 2m - 2$. Зафиксируем некоторый набор координат $(i_1, \ldots, i_v;)$ такой, что $2v = d - 4$. Тогда $C_{i_1,\ldots,i_v;}$ является $((m - v, 0), 4^k, 4)$ МДР кодом и $2(m-v) \geq 6$. Если $2(m-v) = 6$, то мы получаем противоречие по предложению 9. Если $2(m - v) > 6$, то мы получаем противоречие по лемме 23.

Если $n > 0$ либо k — четно, то мы можем зафиксировать такой набор координат $(i_1, \ldots, i_v; j_1, \ldots, j_w)$, что $2v + w = k - 2$. Тогда по лемме 12 сечение $C^{00,\ldots,00;0,\ldots,0}_{i_1,\ldots,i_v;j_1,\ldots,j_w}$ — МДР код с параметрами $((m - v, n - w), 4^2, d)$. Так как $d = 2m + n - k + 1 = 2(m - v) + (n - w) - 1$, то по лемме 21 выполняется $2(m - v) + (n - w) \leq 5$, и $d \leq 4$, и мы получаем противоречие с $d > 5$. ▲

2.7. Приложение

В данном приложении приведены все МДР коды при $4 \leq 2m + n \leq 6$ и $d = 3$, 4 с точностью до эквивалентности.

Для компактности мы обозначим вершины графа Шрикханде следующим образом:

$A = 00, B = 01, C = 02, D = 03, E = 10, F = 11, G = 12, H = 13, I = 20, J = 21, K = 22, L = 23, M = 30, N = 31, O = 32, P = 33$

параметры	код
$((2,0),4^2,3)$	AA, CC, II, KK, BL, DJ, JD, LB, EG, MO, GE, OM, FN, HP, NF, PH
$((2,0),4^2,3)$	AA, CC, IL, KJ, BK, DI, JB, LD, EO, GM, NE, PG, FH, HF, MN, OP
$((1,2),4^2,3)$	A00, C12, J23, L31, B21, D33, K10, I02, E11, G03, N30, P22, F32, H20, O01, M13
$((2,1),4^2,4)$	AA0, CC0, II0, KK0, BL1, DJ1, JD1, LB1, EG2, MO2, GE2, OM2, FN3, HP3, NF3, PH3
$((2,1),4^2,4)$	AA0, CC0, IL0, KJ0, BK1, DI1, JB1, LD1, EO2, GM2, NE2, PG2, FH3, HF3, MN3, OP3
$((1,3),4^2,4)$	A000, C120, J230, L310, B211, D331, K101, I021, E112, G032, N302, P222, F323, H203, O013, M133
$((2,1),4^3,3)$	AA0, CA1, IA2, KA3, CC0, AC1, KC2, IC3, II0, KI1, AI2, CI3, KK0, IK1, CK2, AK3, LB0, JB1, DB2, BB3, JD0, LD1, BD2, DD3, DJ0, BJ1, LJ2, JJ3, BL0, DL1, JL2, LL3, GE0, EE1, OE2, ME3, OM0, MM1, GM2, EM3, EG0, GG1, MG2, OG3, MO0, OO1, EO2, GO3, NF0, PF1, FF2, HF3, PH0, NH1, HH2, FH3, FN0, HN1, NN2, PN3, HP0, FP1, PP2, NP3

параметры	код
$((2,1),4^3,3)$	AA0, CA1, JA2, LA3, CC0, AC1, LC2, JC3, LI0, JI1, AI2, CI3, JK0, LK1, CK2, AK3, KB0, IB1, BB2, DB3, ID0, KD1, DD2, BD3, BJ0, DJ1, IJ2, KJ3, DL0, BL1, KL2, IL3, OE0, ME1, GE2, EE3, MG0, OG1, EG2, GG3, EN0, GN1, ON2, MN3, GP0, EP1, MP2, OP3 HF0, FF1, PF2, NF3, FH0, HH1, NH2, PH3, NM0, PM1, HM2, FM3, PO0, NO1, FO2, HO3
$((1,3),4^3,3)$	A000, C001, J002, L003, C120, A121, L122, J123, J230, L231, C232, A233, L310, J311, A312, C313, B210, D211, K212, I213, D330, B331, I332, K333, K100, I101, D102, B103, I020, K021, B022, D023, E110, G111, N112, P113, G030, E031, P032, N033, N300, P301, G302, E303, P220, N221, E222, G223, F320, H321, O322, M323, H200, F201, M202, O203, O010, M011, H012, F013, M130, O131, F132, H133
$((2,2),4^3,4)$	AA00, CA11, IA22, KA33, CC00, AC11, KC22, IC33, II00, KI11, AI22, CI33, KK00, IK11, CK22, AK33, LB01, JB10, DB23, BB32, JD01, LD10, BD23, DD32, DJ01, BJ10, LJ23, JJ32, BL01, DL10, JL23, LL32, GE02, EE13, OE20, ME31, OM02, MM13, GM20, EM31 EG02, GG13, MG20, OG31, MO02, OO13, EO20, GO31, NF03, PF12, FF21, HF30, PH03, NH12, HH21, FH30, FN03, HN12, NN21, PN30, HP03, FP12, PP21, NP30

Глава 3

Минимальные носители собственных функций в графах Дуба

3.1. Определения и вспомогательные утверждения

Функция $f : {}_{\mathrm{v}}D(m,n) \to \mathbb{R}$ называется *собственной функцией* графа $D(m,n)$ с собственным значением λ, если $f \not\equiv 0$ и $Af = \lambda f$, где A — матрица смежности графа $D(m,n)$. У матрицы смежности графа $D(m,n)$ следующие собственные значения:

$$\lambda_i = 6m + 3n - 4i, i = 0, 1, \ldots, 2m + n.$$

Обозначим соответствующие собственные подпространства через

$$V_i^{m,n} = \{f : {}_{\mathrm{v}}D(m,n) \to \mathbb{R} \mid \sum_{\substack{d(x,y)=1 \\ y \in {}_{\mathrm{v}}D(m,n)}} f(y) = \lambda_i f(x),\ \forall x \in {}_{\mathrm{v}}D(m,n)\}.$$

Носителем функции $f : {}_{\mathrm{v}}D(m,n) \to \mathbb{R}$ назовем множество

$$S(f) = \{x \in {}_{\mathrm{v}}D(m,n) : f(x) \neq 0\}.$$

Лемма 24. *Пусть* $f \in V_1^{1,0}$. *Тогда*

1. $\sum\limits_{a \in \mathrm{vSh}} f(a) = 0$;
2. $f(a) + f(a+02) + f(a+20) + f(a+22) = 0$ *для любой вершины* $a \in \mathrm{vSh}$;
3. $f(a) + f(a+2s) = f(a+s) + f(a+3s)$ *для любой вершины* $a \in \mathrm{vSh}$, *для любого* $s \in \{01, 10, 11\}$.

Доказательство. При доказательстве каждого пункта мы воспользуемся тем, что $\lambda_1 = 2$, и для функции f и любой вершины $x \in \mathrm{vSh}$ выполняется

$$2f(x) = \sum_{\substack{d(x,y)=1 \\ y \in \mathrm{vSh}}} f(y).$$

1. Так как граф Шрикханде — регулярный граф степени 6, то

$$2 \sum_{a \in \mathrm{vSh}} f(a) = 6 \sum_{a \in \mathrm{vSh}} f(a),$$

откуда следует утверждение.

2. Без потери общности можно считать, что $a = 00$. Тогда

$$2(f(00) + f(02) + f(20) + f(22)) = 2 \sum_{\substack{b \in \mathrm{vSh} \\ b \neq 00,02,20,22}} f(b) =$$

$$= -2(f(00) + f(02) + f(20) + f(22)),$$

откуда следует утверждение. Последнее равенство следует из пункта 1.

3. Без потери общности можно считать, что $a = 00$, $s = 01$. Обозначим $\Sigma_1 = f(10) + f(12) + f(30) + f(32)$, $\Sigma_2 = f(11) + f(13) + f(31) + f(33)$. Тогда

$$2(f(00) + f(02)) = 2f(01) + 2f(03) + \Sigma_1 + \Sigma_2,$$

и утверждение следует из пункта 2. ▲

Для $c \in \mathbb{R}$ и $a \in {}_{\mathrm{v}}\mathrm{Sh}$ определим следующую функцию на ${}_{\mathrm{v}}D(1,0)$:

$$f_{a,c}(x) = \begin{cases} c, & x \in \{a+31, a+32, a+21\}, \\ -c, & x \in \{a+23, a+12, a+13\}, \\ 0, & \text{иначе.} \end{cases}$$

Функция $f_{03,1}$ изображена на рис. 3.1.

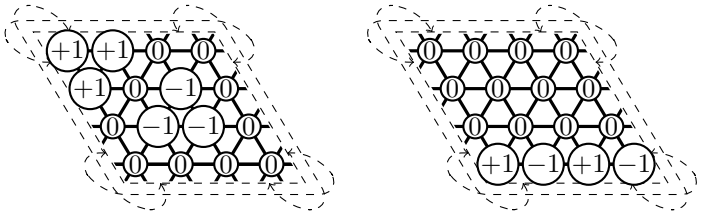


Рис. 3.1: Собственные функции графа Шрикханде с собственными значениями 2 и -2 и минимальными носителями.

Лемма 25. *Пусть f — собственная функция графа Шрикханде с собственным значением 2. Тогда $|S(f)| \geq 6$. Более того, если $|S(f)| = 6$, то $f = f_{a,c}$ для некоторой вершины $a \in {}_{\mathrm{v}}\mathrm{Sh}$ и некоторого $c \in \mathbb{R}$.*

Доказательство. По пункту 1 леммы 24 f принимает положительные и отрицательные значения. Пусть на некоторой вершине x функция f принимает максимальное значение $w = f(x) > 0$, а на вершине y — минимальное значение $u = f(y) < 0$. Тогда либо окрестность вершины x содержит 2 вершины со значением w и 4 вершины со значением 0, либо не менее 3 вершин с положительным значением. Аналогично, либо окрестность вершины y содержит 2 вершины со значением u и 4 вершины со значением 0, либо не менее 3 вершин с отрицательным значением. Отсюда, $|S(f)| \geq 6$, и, более того, если $|S(f)| = 6$, то носитель f состоит из трех попарно смежных вершин со значением w и трех попарно смежных вершин со значением $u = -w$, и при этом нет пары смежных вершин z, t таких, что $f(z) = -f(t) = w$. Также, если $|S(f)| = 6$, то для некоторой вершины b множество $\{b, b+01, b+02, b+03\}$ содержит хотя бы 3

вершины со значением 0. Из пункта 3 леммы 24 следует, что на всех вершинах из множества $\{b, b+01, b+02, b+03\}$ функция принимает значение 0. Аналогично, для некоторой вершины $d = b + s$, где $s \in \{00, 01, 02, 03\}$, функция f принимает значение 0 на вершинах d, $d+10$, $d+20$, $d+30$. Отсюда, учитывая все вышесказанное, нетрудно убедиться, что $f = \pm f_{d,w}$. То, что функция $f_{d,w}$ — собственная с собственным значением 2, проверяется непосредственно. ▲

Для $c \in \mathbb{R}$, $a \in {}_{\mathrm{v}}\mathrm{Sh}$, $s \in \{01, 10, 11\}$ определим следующую функцию на ${}_{\mathrm{v}}D(1,0)$:

$$u_{a,s,c}(x) = \begin{cases} c, & x \in \{a, a+2s\} \\ -c, & x \in \{a+s, a+3s\} \\ 0, & \text{иначе} \end{cases}$$

Функция $u_{00,01,1}$ изображена на рис. 3.1.

Лемма 26. *Пусть h — собственная функция графа Шрикханде с собственным значением -2. Тогда $|S(h)| \geq 4$. Более того, если $|S(h)| = 4$, то $h = u_{a,s,c}$ для некоторых $a \in {}_{\mathrm{v}}\mathrm{Sh}$, $s \in \{01, 10, 11\}$ и $c \in \mathbb{R}$.*

Доказательство. Пусть на некоторой вершине x функция h принимает максимальное по модулю значение $w = f(x)$. Без потери общности можно считать, что $w > 0$. Тогда либо окрестность x содержит не менее 3 вершин с отрицательным значением, либо 2 вершины со значением $-w$ и 4 вершины со значением 0. В первом случае $|S(h)| > 4$ (в самом деле, если $|S(h)| = 4$, то легко убедиться, что найдется вершина y со значением 0 такая, что в ее окрестности есть вершина с отрицательным значением, но нет ни одной вершины с положительным значением). Во втором случае найдется еще хотя бы одна вершина с положительным значением, и если ровно одна, то вершины из носителя образуют цикл на 4 вершинах. Такой цикл в графе Шрикханде имеет вид $\{x, x+s, x+2s, x+3s\}$ для некоторого $s \in \{01, 10, 11\}$. То, что функция $u_{x,s,w}$ — собственная с собственным значением -2, проверяется непосредственно. ▲

Для функций $g : {}_{\mathrm{v}}D(m,n) \to \mathbb{R}$ и $h : {}_{\mathrm{v}}D(m',n') \to \mathbb{R}$ определим *произведение* $f = gh : {}_{\mathrm{v}}D(m+m', n+n') \to \mathbb{R}$ как $f(x,x',y,y') = g(x,y)h(x',y')$, где $x \in {}_{\mathrm{v}}D(m,0)$, $y \in {}_{\mathrm{v}}D(0,n)$, $x' \in {}_{\mathrm{v}}D(m',0)$, $y' \in {}_{\mathrm{v}}D(0,n')$. Тогда следующая лемма следует непосредственно из определения.

Лемма 27. *Пусть $g \in V_i^{m,n}$, $h \in V_j^{m',n'}$. Тогда $f = gh \in V_{i+j}^{m+m',n+n'}$.*

Обозначим через $I^{m,n}$ функцию на ${}_{\mathrm{v}}D(m,n)$, тождественно равную 1.

Следующая лемма хорошо известна в различных формулировках (см. например [9](1.4.6) или [11] (теоремы 2.23, 2.24)), но для полноты мы докажем ее непосредственно.

Лемма 28. *Пусть G и H — графы с собственными значениями $\lambda_1, \dots, \lambda_m$ и $\mu_1, \dots, \mu_n$ соответственно. Пусть $e_{i1}, \dots, e_{is(i)}$ — базис собственного подпространства $V_i(G)$ размерности $s(i)$, отвечающего собственному значению λ_i, и пусть $y_{j1}, \dots, y_{jt(j)}$ — базис собственного подпространства $V_j(H)$ размерности $t(j)$, отвечающего собственному значению μ_j.*

Пусть $F = G \times H$ — декартово произведение графов G и H. Тогда граф F имеет следующие собственные значения:

$$\{\theta_r : \theta_r = \lambda_i + \mu_j; i = 1, \dots, m; j = 1, \dots, n\},$$

а множество функций

$$\{e_{ip}y_{ju} : \text{ для всех } i,j \text{ таких, что } \lambda_i + \mu_j = \theta_r, p = 1, \dots, s(i), u = 1, \dots, t(j)\}$$

образует базис собственного подпространства $V_r(F)$. Размерность собственного подпространства $V_r(F)$ равна $\sum\limits_{\substack{i,j \\ \lambda_i+\mu_j=\theta_r}} s(i)t(j)$.

Доказательство. Для начала докажем, что множество функций

$$\{e_{ij}y_{kl} : i = 1, \dots, m; j = 1, \dots s(i); k = 1, \dots, n; l = 1, \dots, t(k)\}$$

образует базис вещественно-значных функций на графе F. Рассмотрим линейную комбинацию функций из этого множества. Пусть

$$\sum_{i,j} e_{ij} \sum_{k,l} \lambda_{ijkl} \cdot y_{kl} \equiv 0.$$

Определим функцию f_{ij} на H следующим образом: $f_{ij} = \sum\limits_{k,l} \lambda_{ijkl} \cdot y_{kl}$. Так как множество функций e_{ij} образует базис на G, то для любых i, j имеет место $f_{ij} \equiv 0$. Так как функции из множества $\{y_{kl}\}$ линейно независимы, то $\lambda_{ijkl} = 0$ для всех i, j, k, l. Следовательно, любая функция вида $e_{ij}y_{kl}$ такая, что $\lambda_i + \mu_j = \theta_r$, образует базис собственного подпространства $V_r(F)$, откуда следует утверждение леммы. ▲

Следствие 5. *Размерность собственного подпространства $V_i^{m,n}$ равна $C_{2m+n}^i \cdot 3^i$.*

Доказательство. У графа Шрикханде 3 собственных значения: -2, 2, 6 с кратностями 9, 6, 1 соответственно. У графа Хэмминга $H(2,4)$ те же самые собственные значения с теми же кратностями. Тогда по лемме 28 у графа $D(m,n)$ те же самые собственные значения с теми же кратностями, что и у графа Хэмминга $H(2m+n,4)$. В графе Хэмминга $H(N,q)$ собственное значение $\lambda_i = N(q-1) - iq$ имеет кратность $C_N^i(q-1)^i$ ([8], 9.2), откуда следует утверждение следствия. ▲

Следствие 6. *Пусть f — собственная функция графа $D(m,n)$ с максимальным собственным значением $\lambda_0 = 6m+3n$. Тогда $f \equiv c$ для некоторого $c \in \mathbb{R}$, $c \neq 0$.*

Доказательство. Это следует из того, что размерность собственного подпространства $V_0^{m,n}$ равна 1 и из того, что $f \equiv c$ — собственная функция с собственным значением λ_0. ▲

Следствие 7. *Пусть f — собственная функция графа $D(m,n)$ с минимальным собственным значением $\lambda_{2m+n} = -2m-n$. Тогда для любых вершин $a_1, \ldots, a_k \in$ vSh, $b_1, \ldots, b_l \in$ vK_4 и любого набора координат $(i_1, \ldots, i_k; j_1, \ldots, j_l)$ сужение $f|_{x_{i_1}=a_1,\ldots,x_{i_k}=a_k;y_{j_1}=b_1,\ldots,y_{j_l}=b_l}$ — собственная функция графа $D(m-k,n-l)$ с ми-*

нимальным собственным значением $-2(m-k)-(n-l)$.

Доказательство. Из леммы 28 следует, что можно выбрать базис собственного подпространства $V^{m,n}_{2m+n}$ такой, что любая функция e из базиса может быть представлена в виде $e_1 \dots e_m y_1 \dots y_n$, где $e_1, \dots, e_m$ — собственные функции графа Sh с минимальным собственным значением -2, а $y_1, \dots, y_n$ — собственные функции графа K_4 с минимальным собственным значением -1. Сужение $e|_{x_{i_1}=a_1,\dots,x_{i_k}=a_k;y_{j_1}=b_1,\dots,y_{j_l}=b_l}$ — это собственная функция графа $D(m-k, n-l)$ с минимальным собственным значением, откуда следует утверждение следствия. ▲

Следствие 8. *Пусть f — собственная функция графа Дуба $D(m,n)$ с собственным значением $\lambda_1 = 6m+3n-4$. Тогда f представима в виде $f = hI^{1,0} + I^{m-1,n}g$, где $h \in V_1^{m-1,n}$, $g \in V_1^{1,0}$.*

Доказательство. Пусть $e_1, \dots, e_k$ — базис собственного подпространства $V_1^{m-1,n}$, где $k = 6(m-1)+3n$, а $y_1, \dots, y_6$ — базис собственного подпространства $V_1^{1,0}$. Тогда по лемме 28 функции $e_1 I^{1,0}$, …, $e_k I^{1,0}$, $I^{m-1,n}y_1, \dots$, $I^{m-1,n}y_6$ образуют базис собственного подпространства $V_1^{m,n}$. Следовательно, для любой функции f из $V_1^{m,n}$ найдется набор чисел μ_i, $i = 1, \dots, 6m+3n$, такой, что $f = \mu_1 e_1 I^{1,0} + \dots + \mu_k e_k I^{1,0} + \mu_{k+1} I^{m-1,n} y_1 + \dots + \mu_{k+6} I^{m-1,n} y_6$. Тогда $f = hI^{1,0} + I^{m-1,n}g$, где $h = \mu_1 e_1 + \dots + \mu_k e_k$, $g = \mu_{k+1} y_1 + \dots + \mu_{k+6} y_6$. ▲

Лемма 29. *Пусть $F = G \times H$ — декартово произведение графов G и H. Пусть f — собственная функция графа F с собственным значением λ. Пусть для любой вершины $y \in {}_{\mathrm{v}}H$ функция $g_y(z) = f(z,y)$ — собственная функция графа G с собственным значением λ_1 либо $g_y \equiv 0$, и для любой вершины $x \in {}_{\mathrm{v}}G$ функция $h_x(z) = f(x,z)$ — собственная функция графа H с собственным значением λ_2 либо $h_x \equiv 0$, где $\lambda_1 + \lambda_2 = \lambda$. Пусть r — величина минимального возможного носителя собственной функции графа G с собственным значением λ_1, и s — величина минимального возможного носителя собственной функции графа H с собственным значением λ_2.*

Тогда $|S(f)| \geq rs$. *Более того, если* $|S(f)| = rs$, *то* $f = gh$, *где* g — *собственная функция графа* G *с собственным значением* λ_1, h — *собственная функция графа* H *с собственным значением* λ_2, *и* $|S(g)| = r$, $|S(h)| = s$.

Доказательство. Так как $f \not\equiv 0$, то найдутся вершины $x \in {}_{\mathrm{v}}G$, $y \in {}_{\mathrm{v}}H$ такие, что $f(x, y) \neq 0$. Тогда $|S(g_y)| \geq r$. Так как $|S(h_a)| \geq s$ для любой вершины a из $S(g_y)$, то $|S(f)| \geq rs$, и равенство достигается, если $|S(g_y)| = r$, $|S(h_x)| = s$, $S(h_a) = S(h_x)$ для любой вершины a из $S(g_y)$, и для любой вершины b из ${}_{\mathrm{v}}G \backslash S(g_y)$ множество $S(h_b)$ пусто. Более того, $h_a(z) = c_a h_x(z)$ для любой вершины $a \in S(g_y)$ и любой вершины $z \in {}_{\mathrm{v}}H$, где $c_a = g_y(a)/f(x, y)$. Действительно, рассмотрим функцию $p(z) = c_a \cdot h_x(z) - h_a(z)$. Так как $c_a \cdot h_x(y) = h_a(y)$, то $|S(p)| < s$, и, следовательно, $p \equiv 0$. Тогда $f = gh$, где $g(z) = g_y(z)/f(x, y)$, $h(z') = h_x(z')$, $z \in {}_{\mathrm{v}}G$, $z' \in {}_{\mathrm{v}}H$. ▲

Лемма 30. *Пусть функция* $f : {}_{\mathrm{v}}D(1, 0) \to \mathbb{R}$ *может быть представлена в виде* $f = g + h$, *где* $g \in V_1^{1,0}$, $h \in V_0^{1,0}$, *и функции* g, h *не равны тождественно* 0. *Тогда* $|S(f)| \geq 7$.

Доказательство. Пусть функция f удовлетворяет условиям леммы, и $|S(f)| \leq 7$. Следовательно $|f^{-1}(0)| \geq 9$. По условию $h(a) = -c$ для любой вершины $a \in {}_{\mathrm{v}}\mathrm{Sh}$ и для некоторого $c \in \mathbb{R}$, $c \neq 0$. Тогда $|g^{-1}(c)| = |f^{-1}(0)| \geq 9$. Обозначим через $C(b, r)$, множество $\{b, b + r, b + 2r, b + 3r\}$, $b \in {}_{\mathrm{v}}\mathrm{Sh}$, $r \in \{01, 10, 11\}$. Тогда для каждого $s \in \{01, 10, 11\}$ найдется цикл $C(a_s, s)$, для некоторой вершины a_s, содержащий хотя бы 3 вершины из множества $g^{-1}(c)$. Из пункта 3 леммы 24 следует, что все вершины такого цикла будут принадлежать множеству $g^{-1}(c)$. Без потери общности, можно считать, что вершины $00, 01, 02, 03, 10, 20, 30$ принадлежат $g^{-1}(c)$. Тогда множеству $g^{-1}(c)$ принадлежит одна из вершин $21, 32, 31, 13, 12, 23$ (в противном случае вершины $11, 22, 33$ принадлежат $g^{-1}(c)$, и в вершине 00 нарушается условие для собственной функции).

Так как g — собственная функция с собственным значением 2, используя

лемму 24, в каждом из случаев можно однозначно восстановить значения функции g. Все возможные функции изображены на рис. 3.2 ($c = 1$). Для каждой из них носитель соответствующей функции f равен 7, что доказывает лемму. ▲

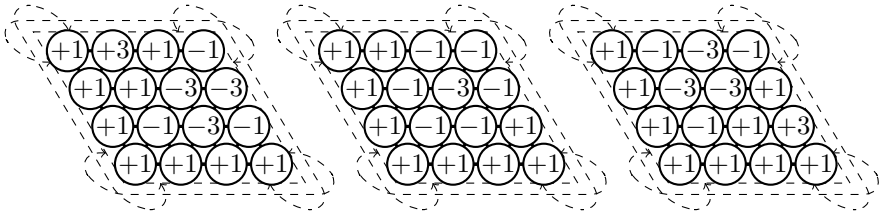


Рис. 3.2: Случаи из доказательства леммы 30

Для $c \in \mathbb{R}$ и $k, l \in \{0, 1, 2, 3\}$ определим следующую функцию на ${}_{\mathrm{v}}D(0, 2)$:

$$h_{k,l,c}(x) = \begin{cases} c, & x \in \{(k+1, l), (k+2, l), (k+3, l)\} \\ -c, & x \in \{(k, l+1), (k, l+2), (k, l+3)\} \\ 0, & \text{иначе} \end{cases}$$

Лемма 31. *[43] Пусть h — собственная функция графа Хэмминга $H(n, 4)$ с собственным значением $\lambda_1 = 3n - 4$ и минимальным возможным носителем. Тогда $|S(h)| = 6 \cdot 4^{n-2}$, и функция представима в виде $h = h_1 \dots h_{n-1}$, где $h_i = h_{k,l,c}$ для некоторых $k, l \in \{0, 1, 2, 3\}$, некоторого $i = 1, \dots, n-1$ и некоторого $c \in \mathbb{R}$, и $h_j = I^{0,1}$ при $j \neq i$, $j = 1, \dots, n-1$.*

Для $c \in \mathbb{R}$ и $k, l \in \{0, 1, 2, 3\}$, $k \neq l$, определим следующую функцию на ${}_{\mathrm{v}}D(0, 1)$:

$$r_{k,l,c}(x) = \begin{cases} c, & x = k \\ -c, & x = l \\ 0, & \text{иначе} \end{cases}$$

Очевидно, что если функция f на ${}_{\mathrm{v}}D(0, 1)$ — собственная функция с минимальным собственным значением -1 и минимальным возможным носителем, то $f = r_{k,l,c}$ для некоторых $c \in \mathbb{R}$ и $k, l \in \{0, 1, 2, 3\}$, $k \neq l$.

3.2. Основные результаты.

Теперь можно сформулировать и доказать основные теоремы данной главы.

Теорема 3. *Пусть f – собственная функция графа $D(m,n)$ с собственным значением $\lambda_1 = 6m + 3n - 4$. Тогда $|S(f)| \geq 6 \cdot 4^{2m+n-2}$. Более того, если $|S(f)| = 6 \cdot 4^{2m+n-2}$, то верно одно из следующих утверждений:*

1. *$f = g_1 \dots g_m I^{0,n}$, где $g_i = f_{a,c}$ для некоторых $i \in \{1, \dots, m\}$, $a \in {}^{\mathrm{v}}\mathrm{Sh}$, $c \in \mathbb{R}$, и $g_j = I^{1,0}$, при $j \neq i$, $j \in \{1, \dots, m\}$*

2. *$f = I^{m,0} h_1 \dots h_{n-1}$, где $h_i = h_{k,l,c}$ для некоторых $i \in \{1, \dots, n-1\}$, $k, l \in \{0, 1, 2, 3\}$, $c \in \mathbb{R}$, и $h_j = I^{0,1}$, при $j \neq i$, $j \in \{1, \dots, n-1\}$.*

Доказательство. Докажем индукцией по m. При $m = 0$ утверждение следует из леммы 31. Пусть f — собственная функция графа $D(m,n)$ с собственным значением λ_1 и минимальным возможным носителем. По следствию 8 функция f может быть представлена в виде $f = hI^{1,0} + I^{m-1,n} g$, где $h \in V_1^{m-1,n}$, $g \in V_1^{1,0}$. Если g тождественно равна 0, то $|S(f)| = 16 \cdot |S(h)|$, следовательно, по индукционному предположению $|S(f)| \geq 6 \cdot 4^{2m+n-2}$, и для h, а следовательно и для f, верно утверждение теоремы. Пусть функция g не равна тождественно 0. Докажем, что тогда функция h тождественна равна 0. Пусть x — произвольная вершина графа $D(m-1,n)$. Обозначим $f_x(y) = f(x,y)$, $x \in {}^{\mathrm{v}}D(m-1,n)$, $y \in {}^{\mathrm{v}}\mathrm{Sh}$. Обозначим $v_x = h(x) I^{1,0}$. Тогда

$$|S(f)| = \sum_{x \in {}^{\mathrm{v}}D(m-1,n)} |S(f_x)| = \sum_{x \in {}^{\mathrm{v}}D(m-1,n)} |S(v_x + g)|.$$

По лемме 30 если $h(x) \neq 0$, то $|S(v_x + g)| \geq 7$. Если $h(x) = 0$, то $|S(v_x + g)| = |S(g)| \geq 6$. Тогда если $h(x) \neq 0$ для некоторой вершины x графа $D(m-1,n)$, то $|S(f)| > 6 \cdot 4^{2m+n-2}$, и мы получаем противоречие с величиной минимального носителя. Значит h тождественна равна 0, и утверждение теоремы следует из леммы 25. ▲

Теорема 4. *Пусть f — собственная функция графа $D(m,n)$ с минимальным собственным значением $\lambda_{2m+n} = -2m - n$. Тогда $|S(f)| \geq 2^{2m+n}$. Более того, если $|S(f)| = 2^{2m+n}$, то $f = c \cdot g_1 \dots g_m h_1 \dots h_n$, где $g_i = u_{a_i,s_i,1}$, $h_j = r_{k_j,l_j,1}$, $a_i \in {}_{\mathrm{v}}\mathrm{Sh}$, $s_i \in \{01, 10, 11\}$, $k_j, l_j \in \{0,1,2,3\}$, $k_j \neq l_j$, $i = 1, \dots, m$, $j = 1, \dots, n$, $c \in \mathbb{R}$.*

Доказательство. По следствию 7 сужение функции f на подграф, являющийся графом Шрикханде, является собственной функцией с собственным значением -2. Также по следствию 7 сужение функции f на подграф, являющийся графом K_4, является собственной функцией с собственным значением -1. Тогда по лемме 29 функция f представима в виде $f = g_1 \dots g_m h_1 \dots h_n$, где g_i — собственная функция графа Шрикханде с собственным значением -2 и минимальной возможной мощностью носителя, а h_j — собственная функция графа K_4 с собственным значением -1 и минимальной возможной мощностью носителя, $i = 1, \dots, m$, $j = 1, \dots, n$. Собственные функции графа Шрикханде с собственным значением -2 и минимальной возможной мощностью носителя охарактеризованы в лемме 26. ▲

Заключение

В диссертации получена характеризация всех свитчингово неразделимых графов по модулю q таких, что удаление любой вершины графа приводит к свитчингово разделимому графу по модулю q. Такие графы существуют только при четных q, и, следовательно, по ним нельзя построить неразделимые n-арные квазигруппы порядка q^2, где q — простое, у которых любой $(n-1)$-арный ретракт разделим. Возникает гипотеза, что при данных порядках квазигрупп с такими свойствами не существует. Было бы интересно узнать, верна ли эта гипотеза и нельзя ли обобщить доказательство, проведенное для графов, на квазигруппы, хотя такое доказательство может оказаться значительно труднее.

Также в диссертации описаны все МДР коды в графах Дуба с кодовым расстоянием $d \geq 3$. Из них 3 с точностью до эквивалентности являются совершенными. Для графов Дуба можно определить множество других известных комбинаторных объектов, таких как совершенные коды, совершенные раскраски, полностью регулярные коды. Одним из направлений дальнейшего исследования может быть изучение любого из этих типов объектов.

Также в диссертации получена характеризация всех собственных функций графа Дуба с наименьшей мощностью носителя для минимального собственного значения и второго по величине собственного значения. При этом для других собственных значений вопрос остается открытым.

Литература

[1] Akivis M. A., Goldberg V. V. Solution of Belousov's problem // Discuss. Math., Gen. Algebra Appl. — 2001. — Vol. 21, no. 1. — P. 93–103. — DOI: 10.7151/dmgaa.1030.

[2] Alderson T. L. $(6, 3)$-MDS codes over an alphabet of size 4 // Des. Codes Cryptography. — 2006. — Vol. 38, no. 1. — P. 11–40. — DOI: 10.1007/s10623-004-5659-4.

[3] Axenovich M. A. On multiple coverings of the infinite rectangular grid with balls of constant radius // Discrete Math. — 2003. — Vol. 268, no. 1-3. — P. 31–48. — DOI: 10.1016/S0012-365X(02)00744-6.

[4] Equitable partitions of latin-square graphs : E-print : 1802.01001 / ArXiv.org ; Executor: Cameron Peter J. Gavrilyuk Alexander L. Bailey, R. A., Sergey V. Goryainov : 2018. — Access mode: https://arxiv.org/pdf/1802.01001.pdf.

[5] Ball S. A proof of the MDS conjecture over prime fields // 3rd International Castle Meeting on Coding Theory and Application / Ed. by Joaquim Borges, Mercè Villanueva. — Bellaterra, Spain : Universitat Autònoma de Barcelona. Servei de Publicacions, 2011. — P. 43–46.

[6] Ball S. On sets of vectors of a finite vector space in which every subset of basis size is a basis // J. Eur. Math. Soc. — 2012. — Vol. 14, no. 3. — P. 733–748. — DOI: 10.4171/JEMS/316.

[7] Ball S., De Beule J. On sets of vectors of a finite vector space in which every subset of basis size is a basis II // Des. Codes Cryptography. — 2012. — Vol. 65, no. 1-2. — P. 5–14. — DOI: 10.1007/s10623-012-9658-6.

[8] Brouwer A. E., Cohen A. M., Neumaier A. Distance-Regular Graphs. — Berlin : Springer-Verlag, 1989. — DOI: 10.1007/978-3-642-74341-2.

[9] Brouwer A. E., Haemers W. H. Spectra of graphs. — New York : Springer-Verlag, 2012.

[10] Chihara L. On the zeros of the Askey–Wilson polynomials, with applications to coding theory // SIAM J. Math. Anal. — 1987. — Vol. 18, no. 1. — P. 191–207. — DOI: 10.1137/0518015.

[11] Cvetković D. M., Doob M., Sachs H. Spectra of Graphs: Theory and Application. — New York, San Francisco, London : Academic Press, 1980.

[12] Delsarte P. An Algebraic Approach to Association Schemes of Coding Theory. — 1973. — Vol. 10 of Philips Res. Rep., Supplement.

[13] Dénes J., Keedwel A. D. Latin Squares and Their Applications. — New York : Academic Press, 1974.

[14] Egan J., Wanless I. Enumeration of MOLS of small order // Mathematics of Computation. — 2016. — Vol. 85, no. 298. — P. 799–824.

[15] Egawa Y. Characterization of H(n, q) by the parameters // Journal of Combinatorial Theory, Series A. — 1981. — Vol. 31, no. 2. — P. 108–125.

[16] Finizio N. J., Lewis J. T. Enumeration of maximal codes // Congr. Numerantium. — 1994. — Vol. 102. — P. 139–145.

[17] Gavrilyuk A. L., Goryainov S. V. On perfect 2-colorings of Johnson graphs J(v, 3) // J. Comb. Des. — 2013. — Vol. 21. — P. 232–252.

[18] Golay M. J. E. Notes on digital coding // Proc. IRE. — 1949. — Vol. 37, no. 6. — P. 657. — DOI: 10.1109/JRPROC.1949.233620.

[19] Heden O., Krotov D. S. On the structure of non-full-rank perfect q-ary codes // Adv. Math. Commun. — 2011. — Vol. 5, no. 2. — P. 149–156. — DOI: 10.3934/amc.2011.5.149.

[20] Hulpke A., Kaski P., Östergård P. R. J. The number of Latin squares of order 11 // Math. Comp. — 80. — Vol. 2011. — P. 1197–1219. — DOI: 10.1090/S0025-5718-2010-02420-2.

[21] Ito T. Creation method of table, creation apparatus, creation program and program storage medium. — 2004. — no. 2004/0243621A1. — http://ip.com/patapp/US20040243621 New date stamp at http://www.freepatentsonline.com/7228311.html http://ip.com/patent/US7228311. Access mode: http://www.freepatentsonline.com/y2004/0243621.html.

[22] Kokkala J. I., Krotov D. S., Östergård P. R. J. On the classification of MDS codes // IEEE Trans. Inf. Theory. — 2015. — December. — Vol. 61, no. 12. — P. 6485–6492. — DOI: 10.1109/TIT.2015.2488659.

[23] Kokkala J. I., Östergård P. R. J. Classification of Graeco–Latin cubes // J. Comb. Des. — 2015. — Vol. 23, no. 12. — P. 509–521. — DOI: 10.1002/jcd.21400.

[24] Kokkala J. I., Östergård P. R. J. Further results on the classification of MDS codes // Adv. Math. Commun. — 2016. — August. — Vol. 10, no. 3. — P. 489–498. — DOI: 10.3934/amc.2016020.

[25] Koolen J. H., Munemasa A. Tight 2-designs and perfect 1-codes in Doob graphs // J. Stat. Plann. Inference. — 2000. — Vol. 86, no. 2. — P. 505–513. — DOI: 10.1016/S0378-3758(99)00126-3.

[26] Krotov D. S. On irreducible n-ary quasigroups with reducible retracts // Eur. J. Comb. — 2008. — Vol. 29, no. 2. — P. 507–513. — DOI: 10.1016/j.ejc.2007.01.005.

[27] Krotov D. S. Perfect codes in Doob graphs // Des. Codes Cryptography. — 2016. — July. — Vol. 80, no. 1. — P. 91–102. — DOI: 10.1007/s10623-015-0066-6.

[28] Krotov D. S., Bespalov E. A. Distance-2 MDS codes and latin colorings in the Doob graphs // Graphs and Combinatorics. — 2018. — Vol. 34, no. 5. — P. 1001–1017. — DOI: 10.1007/s00373-018-1926-4.

[29] Krotov D. S., Potapov V. N. n-Ary quasigroups of order 4 // SIAM J. Discrete Math. — 2009. — Vol. 23, no. 2. — P. 561–570. — DOI: 10.1137/070697331.

[30] Krotov D. S., Potapov V. N. On connection between reducibility of an n-ary quasigroup and that of its retracts // Discrete Math. — 2011. — Vol. 311, no. 1. — P. 58–66. — DOI: 10.1016/j.disc.2010.09.023.

[31] Krotov D. S., Potapov V. N., Sokolova P. V. On reconstructing reducible n-ary quasigroups and switching subquasigroups // Quasigroups Relat. Syst. — 2008. — Vol. 16, no. 1. — P. 55–67. — DOI: 10.17686/sced_rusnauka_2008-1040.

[32] Martin W. J., Zhu X. J. Anticodes for the Grassman and bilinear forms graphs // Des. Codes Cryptography. — 1995. — Vol. 6, no. 1. — P. 73–79. — DOI: 10.1007/BF01390772.

[33] McKay B. D., Wanless I. M. A census of small Latin hypercubes // SIAM J. Discrete Math. — 2008. — Vol. 22, no. 2. — P. 719–736. — DOI: 10.1137/070693874.

[34] Mullen G. L., Weber R. E. Latin cubes of order ≤ 5 // Discrete Math. — 1980. — Vol. 32, no. 3. — P. 291–297. — DOI: 10.1016/0012-365X(80)90267-8.

[35] On eigenfunctions and maximal cliques of Paley graphs of square order / S. Goryainov, V. Kabanov, L. Shalaginov, A. Valyuzhenich // Finite

Fields and Their Applications. — July 2018. — Vol. 52. — P. 361–369. — DOI: 10.1016/j.ffa.2018.05.001.

[36] Phelps K. T. A general product construction for error correcting codes // SIAM J. Algebraic Discrete Methods. — 1984. — Vol. 5, no. 2. — P. 224–228. — DOI: 10.1137/0605023.

[37] Shcherbacov V. A. Quasigroups in cryptology // Comput. Sci. J. Mold. — 2009. — Vol. 17, no. 2. — P. 193–228. — Online http://www.math.md/en/publications/csjm/issues/v17-n2/10088/.

[38] Shi M., Huang D., Krotov D. S. Additive perfect codes in Doob graphs. — 2018. — no. 1806.04834v1. — Access mode: https://arxiv.org/abs/1806.04834v1.

[39] Shrikhande S. The uniqueness of the L2 association scheme // The Annals of Mathematical Statistics. — 1959. — Vol. 30, no. 3. — P. 781–798.

[40] Singleton R. Maximum distance q-nary codes // IEEE Trans. Inf. Theory. — 1964. — Vol. 10, no. 2. — P. 116–118. — DOI: 10.1109/TIT.1964.1053661.

[41] Sotnikova E. V. Eigenfunctions supports of minimum cardinality in cubical distance-regular graphs // Siberian Electronic Mathematical Reports. — 2018. — Vol. 15. — P. 223–245.

[42] Tietäväinen A. On the nonexistence of perfect codes over finite fields // SIAM J. Appl. Math. — 1973. — Vol. 24, no. 1. — P. 88–96. — DOI: 10.1137/0124010.

[43] Valyuzhenich A. A. Minimum supports of eigenfunctions of Hamming graphs // Discrete Mathematics. — 2017. — Vol. 340, no. 5. — P. 1064–1068.

[44] van Dam E. R., Koolen J. H., Tanaka H. Distance-regular graphs // The Electronic Journal of Combinatorics: EJC, Dynamic Surveys. — 2016. — Vol. Dynamic Surveys, no. DS22. — P. 1–156.

[45] Vorob'ev K., Mogilnych I., Valyuzhenich A. Minimum supports of eigenfunctions of Johnson graphs. — 2017. — no. 1706.03987. — Available at http://arxiv.org/abs/math/1706.03987.

[46] Августинович С. В., Могильных И. Ю. Совершенные раскраски графов Джонсона $J(8,3)$ и $J(8,4)$ в два цвета // Diskretn. Anal. Issled. Oper. — 2010. — Т. 17, № 2. — С. 3–19. — Режим доступа: http://mi.mathnet.ru/da602.

[47] Белоусов В. Д. n-Арные квазигруппы. — Кишинев : Штиинца, 1972.

[48] Белоусов В. Д., Сандик М. Д. n-Арные квази-группы и лупы // Сиб. мат. ж. — 1966. — Т. 7, № 1. — С. 31–54.

[49] Борисенко В. В. Неприводимые n-квазигруппы на конечных множествах составного порядка // Квазигруппы и лупы. — Кишинев : Штиинца, 1979. — Т. 51 из Мат. Исслед. — С. 38–42.

[50] Воробьёв К. В., Кротов Д. С. Оценки мощности минимального 1-совершенного битрейда в графе Хэмминга // Дискрет. анализ и исслед. операций. — 2014. — Т. 21, № 6. — С. 3–10. — Режим доступа: http://mi.mathnet.ru/da797.

[51] Воробьёв К. В., Фон-Дер-Флаасс Д. Г. О совершенных 2-раскрасках гиперкуба // Сиб. электрон. мат. изв. — 2010. — Т. 7. — С. 65–75. — Режим доступа: http://mi.mathnet.ru/semr228.

[52] Глухов М. М. О многообразиях (i,j)-приводимых n-квазигрупп // Сети и квазигруппы. — Кишинев : Штиинца, 1976. — Т. 39 из Мат. Исслед. — С. 67–72.

[53] Глухов М. М. О применениях квазигрупп в криптографии // Прикладная дискретная математика. — 2008. — Т. 2, № 2. — С. 28–32. — Режим доступа: http://mi.mathnet.ru/pdm29.

[54] Гольдберг В. В. Об инвариантной характеристике некоторых условий замыкания в тернарных квазигруппах // Сиб. мат. ж. — 1975. — Т. 16, № 1. — С. 29–43.

[55] Гольдберг В. В. О приводимых, групповых и $(2n + 2)$-эдричных $(n + 1)$-тканях многомерных поверхностей // Сиб. мат. ж. — 1976. — Т. 17, № 1. — С. 44–57.

[56] Дельсарт Ф. Алгебраический подход к схемам отношений теории кодирования: Пер. с англ. Библиотека Кибернетического Сборника. — М. : Мир, 1976.

[57] Зиновьев В. А., Зиновьев Д. В. Двоичные расширенные совершенные коды длины 16 ранга 14 // Пробл. передачи инф. — 2006. — Т. 42, № 2. — С. 63–80. — Режим доступа: http://mi.mathnet.ru/ppi45.

[58] Зиновьев В. А., Леонтьев В. К. Несуществование совершенных кодов над полями Галуа // Проблемы управления и теории информации. — 1973. — Т. 2, № 2. — С. 123–132.

[59] Кротов Д. С. Трейды в комбинаторных конфигурациях // XII международный семинар «Дискретная математика и ее приложения» им. академика О.Б. Лупанова. — Москва, 20-25 Июня 2016. — С. 84–96.

[60] Кротов Д. С. Нижние оценки числа m-квазигрупп порядка 4 и числа совершенных двоичных кодов // Дискрет. анализ и исслед. операций. Сер. 1. — 2000. — Т. 7, № 2. — С. 47–53. — Режим доступа: http://mi.mathnet.ru/da261.

[61] Кротов Д. С. О связи свитчинговой разделимости графа и его подграфов // Дискрет. анализ и исслед. операций. — 2010. — Т. 17, № 2. — С. 46–56. — Режим доступа: http://mi.mathnet.ru/da605.

[62] Потапов В. Н., Кротов Д. С. Асимптотика числа n-квазигрупп порядка 4 // Сиб. мат. ж. — 2006. — Т. 47, № 4. — С. 873–887. — Режим доступа: http://mi.mathnet.ru/smj902.

[63] Пузынина С. А. Периодичность совершенных раскрасок бесконечной прямоугольной решетки // Дискрет. анализ и исслед. операций. Сер. 1. — 2004. — Т. 11, № 1. — С. 79–92. — Режим доступа: http://mi.mathnet.ru/da98.

[64] Фон-Дер-Флаасс Д. Г. Совершенные 2-раскраски гиперкуба // Сиб. мат. ж. — 2007. — Т. 48, № 4. — С. 923–930. — Режим доступа: http://mi.mathnet.ru/smj1755.

[65] Френкин Б. Р. О приводимости и сводимости в некоторых классах n-группоидов. II. — Кишинев : Штиинца, 1972. — Т. 7:1(23) из Мат. Исслед. — С. 150–162.

Публикации автора по теме диссертации

[I] E. A. Bespalov, “On switching nonseparable graphs with switching separable subgraphs”, Сиб. электрон. матем. изв., 11 (2014), 988–998

[II] Е. А. Беспалов, Д. С. Кротов, “Об одном признаке свитчинговой разделимости графов по модулю q”, Сиб. матем. журн., 57:1 (2016), 10–24; Siberian Math. J., 57:1 (2016), 7–17

[III] Е. А. Беспалов, Д. С. Кротов, “МДР-коды в графах Дуба”, Пробл. передачи информ., 53:2 (2017), 40–59; Problems Inform. Transmission, 53:2 (2017), 136–154

[IV] E. A. Bespalov, “On the minimum supports of some eigenfunctions in the Doob graphs”, Сиб. электрон. матем. изв., 15 (2018), 258–266

[V] Е. А. Беспалов, “Свитчинговая разделимость графов по модулю q”, Материалы X молодежной школы по дискретной математике и ее приложениям, Москва, 6-8 октября 2015, 10-12.