На правах рукописи

Беспалов Евгений Андреевич

Методы алгебраической теории графов в исследовании МДР кодов

01.01.09 — дискретная математика и
математическая кибернетика

Автореферат
диссертации на соискание ученой степени
кандидата физико-математических наук

Новосибирск
2018

Работа выполнена в Федеральном государственном автономном образовательном учреждении высшего образования «Новосибирский национальный исследовательский государственный университет».

Научный руководитель:
Кротов Денис Станиславович, доктор физико-математических наук.

Официальные оппоненты:

Кабанов Владислав Владимирович, доктор физико-математических наук, профессор, главный научный сотрудник, Институт математики и механики им. Н. Н. Красовского Уральского отделения Российской академии наук (ИММ УрО РАН).

Воробьев Илья Викторович, кандидат физико-математических наук, научный сотрудник, Сколковский институт науки и технологий, Центр Сколтеха по научным и инженерным технологиям для задач с большими массивами данных.

Ведущая организация:
Уральский федеральный государственный университет имени первого Президента России Б. Н. Ельцина.

Защита состоится 23 января 2019 г. в 16 ч. 00 мин. на заседании диссертационного совета Д 003.015.01 при Федеральном государственном бюджетном учреждении науки Институте математики им. С. Л. Соболева Сибирского отделения Российской академии наук по адресу: 630090, г. Новосибирск, пр. Академика Коптюга, 4.

С диссертацией можно ознакомиться в библиотеке и на сайте Федерального государственного бюджетного учреждения науки Института математики им. С. Л. Соболева Сибирского отделения Российской академии наук, http://math.nsc.ru.

Автореферат разослан "___" _____ 2018 г.

Ученый секретарь
диссертационного совета
Д 003.015.01, д.ф.-м.н. Ю. В. Шамардин

Общая характеристика работы

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 [1] и независимо Тиетвайнен [2] 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 [3], 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 1964 году им было показано [4], 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 годы n-арные квазигруппы интенсивно изучались В. Д. Белоусовым и его научной школой [5] [6]. В настоящее время изучение квазигрупп вызывает ин-

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

[2] Tietäväinen, A. On the nonexistence of perfect codes over finite fields // SIAM J. Appl. Math. — 1973. — V.24, №1. — P.123 – 132.

[3] Golay M. J. E. Notes on digital coding // Proc. IRE. — 1949. — V.37, №6. — P.657.

[4] Singleton R. Maximum distance q-nary code // IEEE Trans. Inf. Theory. — 1964. — V.10, №2. — P.116-118.

[5] Белоусов В. Д. n-Арные квазигруппы // Кишинев : Штиинца. — 1972.

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

терес в связи с их приложениями в теории кодирования [7] [8] и криптографии [9]. 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. Латинские квадраты имеют множество применений [10].

В общем случае вопрос существования и классификации МДР кодов в графах 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 [11] с помощью компьютерных вычислений классифицировали все такие системы для $q \leq 9$. Т. Л. Алдерсон [12] показал, что коды с параметрами $(6, 4^3, 4)_4$ и $(5, 4^3, 3)$ единственны с точностью до эквивалентности. Существует ряд работ по классификации МДР кодов при $q = 5, 7, 8$ [13] [14] [15]. 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 [16] [17] [18], в работах 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 [19] [20] [21].

n-Арная квазигруппа называется *разделимой*, если ее можно представить в

---

[7] Heden O., Krotov D. S. On the structure of non-full-rank perfect q-ary codes // Adv. Math. Commun. — 2011. — V.5, №2. — P.149-156.

[8] Phelps K. T. A general product construction for error correcting codes // SIAM J. Algebraic Discrete Methods. — 1984. — V.5, №2. — P.224-28.

[9] Shcherbacov V. A. Quasigroups in cryptology // Comput. Sci. J. Mold. — 2009. — V.17, №2. — P.193-228.

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

[11] Egan J., Wanless I. Enumeration of MOLS of small order // Mathematics of Computation. — 2016. — V.85, №298. — P.799-824.

[12] Alderson T. L. (6, 3)-MDS codes over an alphabet of size 4 // Des. Codes Cryptography. — 2006. — V.38, №1. — P.11-40.

[13] Kokkala J. I., Krotov D. S., Östergård, P. R. J. On the classification of MDS codes // IEEE Trans. Inf. Theory. — 2015. — V.61, №12. — P.6485-6492.

[14] Kokkala J. I., Östergård, P. R. J. Further results on the classification of MDS codes // Adv. Math. Commun. — 2016. — V.10, №3. — P.489-498.

[15] Kokkala J. I., Östergård, P. R. J. Classification of Graeco–Latin cubes // J. Comb. Des. — 2015. — V.23, №12. — P.509-521.

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

[17] Ball S. On sets of vectors of a finite vector space in which every subset of basis size is a basis // J. Eur. Math. Soc. — 2012. — V.14, №3. — P.733-748.

[18] 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. — V.65, №1-2. — P.5-14.

[19] Mullen G. L., Weber R. E. Latin cubes of order ≤ 5 // Discrete Math. — 1980. — V.32, №3. — P.291-297.

[20] Hulpke A., Kaski P., Östergård, P. R. J. The number of Latin squares of order 11 // Math. Comp. — 2011. — V.80, №274. — P.1197-1219.

[21] McKay B. D., Wanless I. M. A census of small Latin hypercubes // SIAM J. Discrete Math. — 2008. — V.22, №2. — P.719-736.

виде бесповторной суперпозиции двух квазигрупп меньшей арности, т.е.

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

где g — m-арная квазигруппа, h — $(n-m+1)$-арная квазигруппа, σ — некоторая перестановка и $m\in\{2,\dots,n-1\}$. В противном случае n-арная квазигруппа называется *неразделимой*. Вопрос, при каких n и q существуют неразделимые n-арные квазигруппы, ставился еще В. Д. Белоусовым [22]. Эта задача исследовалась многими авторами и была окончательно решена в работе Д. С. Кротова, В. Н. Потапова и П. В. Соколовой [23], 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 [24]. Единственный нетривиальный порядок с точки зрения характеризации квазигрупп, для которого полностью охарактеризованы все n-арные квазигруппы, — это $q=4$. Д. С. Кротов и В. Н. Потапов [25] доказали, что любая n-арная квазигруппа порядка 4 разделима либо полулинейна. Также для n-арных квазигрупп порядка 4 была найдена асимптотика числа таких квазигрупп, при этом было показано, что класс полулинейных квазигрупп асимптотически более мощный, чем класс разделимых квазигрупп [26]. Тем самым вызывает интерес задача исследования и описания неразделимых n-арных квазигрупп порядка $q>4$.

Так как n-арная квазигруппа $f(x_1,\dots,x_n)$ обратима в каждой позиции, существует n-арная квазигруппа $f^i(x_1,\dots,x_{i-1},x_0,x_{i+1},\dots,x_n)$, обратная ей в i-й позиции, для любого i от 1 до n. Таким образом, уравнения $x_0=f(x_1,\dots,x_n)$ и $x_i=f^i(x_1,\dots,x_{i-1},x_0,x_{i+1},\dots,x_n)$ 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* $C_{i_1,\dots,i_k}$ и *сечение* $C^{a_1,\dots,a_k}_{i_1,\dots,i_k}$ следующим образом:

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

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

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

[22] Белоусов В. Д. n-Арные квазигруппы // Кишинев : Штиинца, 1972.

[23] Krotov D. S., Potapov V. N., Sokolova P. V. On reconstructing reducible n-ary quasigroups and switching subquasigroups // Quasigroups Relat. Syst. — 2008. — V.16, №1. — P.55-67.

[24] Finizio N. J., Lewis J. T. Enumeration of maximal codes // Congr. Numerantium. — 1994. — V.102. — P.139-145.

[25] Krotov D. S., Potapov V. N. n-Ary quasigroups of order 4 // SIAM J. Discrete Math. — 2009. — V.23, №2. — P.561-570.

[26] Потапов В. Н., Кротов Д. С. Асимптотика числа n-квазигрупп порядка 4 // Сиб. мат. ж. — 2006. — Т.47, №4. — P.873-887.

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

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 принадлежит уже охарактеризованному множеству.

Существует 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 [27]. 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. Было доказано, что если f — неразделимая n-арная квазигруппа порядка 4, у которой имеется неразделимый $(n-1)$-арный ретракт, то квазигруппа f — полулинейна [28]. После для всех четных n были построены критические n-арные квазигруппы порядка 4 [29], в связи с чем пришлось доказывать гипотезу отдельно для критических квазигрупп, пользуясь более слабым признаком разделимости и индукционным шагом длины 2 [30].

Возникает вопрос: для каких q существуют критические квазигруппы? Д. С. Кротовым [31] был предложен метод, позволяющий строить критические ква-

[27] Krotov D. S., Potapov V. N. On connection between reducibility of an n-ary quasigroup and that of its retracts // Discrete Math. — 2011. — V.311, №1. — P.58-66.

[28] Потапов В. Н., Кротов Д. С. Асимптотика числа n-квазигрупп порядка 4 // Сиб. мат. ж. — 2006. — Т.47, №4. — P.873-887.

[29] Krotov D. S. On irreducible n-ary quasigroups with reducible retracts // Eur. J. Comb. — 2008. — V.29, №2. — P.507-513.

[30] Krotov D. S., Potapov V. N. n-Ary quasigroups of order 4 // SIAM J. Discrete Math. — 2009. — V.23, №2. — P.561-570.

[31] Кротов Д. С. О связи свитчинговой разделимости графа и его подграфов // Дискрет. анализ и исслед. операций. — 2010. — Т.17, №2. — P.46-56.

зигруппы порядка 4, используя схожее понятие свитчинговой разделимости по модулю 2 для графов. Позже 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 [II].

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 $f : V \to \{0,\dots,k-1\}$. 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 [32] [33] [34] [35].

Ф. Дельсарт [36] 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 $[s_{0,1}, s_{1,2}, \dots, s_{\rho-1,\rho}, s_{1,0}, \dots, s_{\rho,\rho-1}] = [b_0, \dots, b_{p-1}, c_1, \dots, c_\rho]$ 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 [37] [38], а гипотеза

[32] Фон-Дер-Флаасс Д. Г. Совершенные 2-раскраски гиперкуба // Сиб. мат. ж. — 2007. — Т.48, №4. — P.923-930.

[33] Axenovich M. A. On multiple coverings of the infinite rectangular grid with balls of constant radius // Discrete Math. — 2003. — V.268, №1-3. — P. 31–48.

[34] 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. — P.3-19.

[35] Gavrilyuk A. L., Goryainov S. V. On perfect 2-colorings of Johnson graphs J(v, 3) // J. Comb. Des. — 2013. — V.21, №2. — P.232-252.

[36] Delsarte P. An Algebraic Approach to Association Schemes of Coding Theory // Adv. Math. Commun. — 1973. — V.10 of Philips Res. Rep., Supplement.

[37] Chihara L. On the zeros of the Askey–Wilson polynomials, with applications to coding theory // SIAM J. Math. Anal. — 1987. — V.18, №1. — P.191-207.

[38] Martin W. J., Zhu X. J. Anticodes for the Grassman and bilinear forms graphs // Des. Codes Cryptography.

Дельсарта [39] 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 обзор Э. ван Дама, Дж. Кулена и Х. Танаки [40]. 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 [41]. 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 [42], 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 $2m+n = \frac{4^l-1}{3}$ [43]. Дж. Кулен и А. Мунемаса [44] построили совершенный код в графе $D(1,3)$ и совершенный код в графе $D(2,1)$, а Д. С. Кротов [45] построил совершенные коды для асимптотически двух третей значений (m,n), удовлетворяющих $2m+n = \frac{4^l-1}{3}$. В графах Дуба $D(m,n)$ для кода C с расстоянием d можно установить границу на мощность кода, аналогичную границе Синглтона

— 1995. — V.6, №1. — P.73-79.

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

[40]van Dam E. R., Koolen J. H., Tanaka H. Distance-regular graphs // The Electronic Journal of Combinatorics. — 2016. — V.Dynamic Surveys, №DS22. — P.1-156.

[41]Shrikhande S. The uniqueness of the L2 association scheme // The Annals of Mathematical Statistics. — 1959. — V.30, №3. — P.781-798.

[42]Egawa Y. Characterization of H(n, q) by the parameters // Journal of Combinatorial Theory, Series A. — 1981. — V.31, №2. — P.108-125.

[43]Koolen J. H., Munemasa A. Tight 2-designs and perfect 1-codes in Doob graphs // J. Stat. Plann. Inference. — 2000. — V.86, №2. — P.505-513.

[44]Koolen J. H., Munemasa A. Tight 2-designs and perfect 1-codes in Doob graphs // J. Stat. Plann. Inference. — 2000. — V.86, №2. — P.505-513.

[45]Krotov D. S. Perfect codes in Doob graphs // Des. Codes Cryptography. — 2016. — V.80, №1. — P.91-102.

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 существуют МДР коды в графах Дуба, и задача характеризации всех МДР кодов в графах Дуба. Задача описания МДР кодов с кодовым расстоянием 2 рассмотрена отдельно [46]. 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:

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

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

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

является собственной функцией с минимальным собственным значением $-2m-n$. С другой стороны, если g — 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. например обзор Д. С. Кротова [47]. В свете этого вызывает интерес

[46] Krotov D. S., Bespalov E. A. Distance-2 MDS codes and latin colorings in the Doob graphs // Graphs and Combinatorics. — 2018. — V.34, №5. — P.1001-1017.

[47] 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.

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 [48], графах Джонсона [49], графах Пэйли [50].

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]. Большинство результатов, выносимых на защиту, получено автором лично, остальные результаты получены в неразделимом соавторстве с научным руководителем.

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, снабжены подробными доказательствами 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 наименьшей мощностью носителя для минимального собственного значения и второго по величине собственного значения.

Структура и объем диссертации. Диссертация состоит из введения, трех глав, заключения и списка литературы. Текст работы изложен на 88 станицах.

[48] Valyuzhenich A. A. Minimum supports of eigenfunctions of Hamming graphs // Discrete Mathematics. — 2017. — V.340, №5. — P.1064-1068.

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

[50] Goryainov S., Kabanov V., Shalaginov L., Valyuzhenich A. On eigenfunctions and maximal cliques of Paley graphs of square order // Finite Fields and Their Applications. — 2018. — V.52 — P.361-369.

Содержание работы

Первая глава посвящена свитчинговой разделимости графов по модулю q.

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 $V \backslash W$. 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.

В данной главе целью является описание всех таких графов G, которые обладают следующим свойством: сам граф G неразделим, и при удалении любой его вершины всегда получается разделимый подграф графа G. Графы с таким свойством назовем *критическими*.

Перед тем как сформулировать основной результат первой главы определим для четного q семейство графов $G_{n,\gamma}$, $\gamma \in \{0, 1, \ldots, q-1\}$, $n = 2k+1 \geq 5$. Множество вершин графа — $\{a_0, a_1, \ldots, a_k, b_1, \ldots, b_k\}$, вершина a_0 изолированна, а веса остальных ребер определим 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.

Граф $G_{n,0}$ изображен на рис. 1.

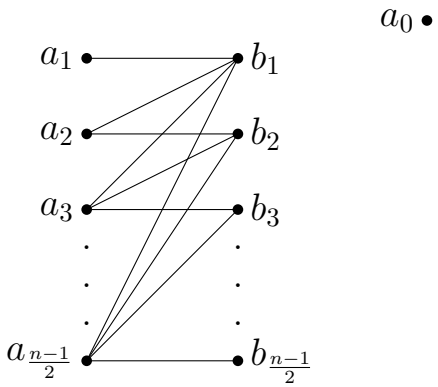

Рис. 1: Граф $G_{n,0}$

Основным результатом главы является следующая теорема, характеризующая все критические графы.

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

Отдельно доказано, что графы из данного семейства действительно являются критическими.

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

Тем самым 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.

Вторая глава посвящена МДР кодам в графах Дуба с кодовым расстоянием $d \geq 3$.

В начале нам потребуется несколько определений.

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 $\{1, 2, 3\}$. Пусть m и n — неотрицательные целые числа. Через $D(m, n) = \mathrm{Sh}^m \times K^n$ обозначим граф, являющийся прямым произведением m копий графа Шрикханде и n копий полного графа K_4. Если $m > 0$, то такой граф называется *графом*

Дуба, тогда как $D(0,n)$ — граф Хэмминга $H(n,4)$.

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

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

МДР кодом с параметрами $((m,n),4^k,d)$ назовем код в графе $D(m,n)$ мощности 4^k с кодовым расстоянием $d = 2m+n-k+1$. Через $L_{m,n,k}$ обозначим количество кодов с данными параметрами с точностью до эквивалентности (два кода считаются эквивалентными если один переходит в другой под действием некоторого автоморфизма графа Дуба).

Основным результатом второй главы является характеризация всех таких кодов с кодовым расстоянием $d \ge 3$, приведенная в следующей теореме.

Теорема 2. *Число $L_{m,n,k}$ неэквивалентных МДР кодов мощности 4^k в графах Дуба $D(m,n)$, $2m+n-2 \ge k \ge 1$ (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 $4 \le 2m+n \le 6$ и $3 \le d \le 4$ 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 разбито на несколько случаев, в зависимости от параметров МДР кода.

В приложении к главе 2 в явном виде приведены все, с точностью до эквивалентности, МДР коды с расстоянием $2 < d < 2m+n$.

Третья глава посвящена минимальным носителям собственных функций в графах Дуба.

Приведем необходимые определения. Множество вершин графа G обозначим через ${}_{\mathrm{v}}G$. 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

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

Определим на графе Шрикханде 2 семейства функций.

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

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

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

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

Эти функции являются собственными, и небольшим перебором доказано, что эти функции описывают все собственные функции графа Шрикханде с минимальным возможным носителем и собственными значениями 2 и -2, а именно:

Лемма 2. *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 $c \in \mathbb{R}$.*

Лемма 3. *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 $c \in \mathbb{R}$.*

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 $x \in {}_{\mathrm{v}}D(m,0)$, $y \in {}_{\mathrm{v}}D(0,n)$, $x' \in {}_{\mathrm{v}}D(m',0)$, $y' \in {}_{\mathrm{v}}D(0,n')$. Отметим, что произведение $f = gh$ двух функций $g \in V_i^{m,n}$ и $h \in V_j^{m',n'}$ есть функция из $V_{i+j}^{m+m',n+n'}$

А. А. Валюженичем [51] была решена задача описания собственных функций со вторым по величине собственным значением и наименьшей мощностью но-

[51] Valyuzhenich A. A. Minimum supports of eigenfunctions of Hamming graphs // Discrete Mathematics. — 2017. — V.340, №5. — P.1064-1068.

сителя для графов Хэмминга $H(n,q)$, в частности для графов вида $D(0,n)$. Это описание используется в качестве базы индукции для описания собственных функций со вторым по величине собственным значением и наименьшей мощностью носителя в графах Дуба $D(m,n)$.

Определим два семейства функций.

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

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

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

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

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

Теперь можно сформулировать основные результаты третьей 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 некоторого $i \in \{1,\dots,m\}$, некоторых $a \in {}_{\mathrm{v}}\mathrm{Sh}$, $c \in \mathbb{R}$, и $g_j = I^{1,0}$, при $j \neq i$, $j = 1,\dots,m$*

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

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 $g_i = u_{a_i,s_i,1}$, $h_j = r_{k_j,l_j,1}$, $a_i \in {}_{\mathrm{v}}\mathrm{Sh}$, $s_i \in \{01,10,11\}$, $k_j,l_j \in \{0,1,2,3\}$, $k_j \neq l_j$, $i = 1,\dots,m$, $j = 1,\dots,n$, $c \in \mathbb{R}$.*

Таким образом, 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.

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.

Публикации автора по теме диссертации

[I] E. A. Bespalov. On switching nonseparable graphs with switching separable subgraphs // Сиб. электрон. матем. изв. — 2014. — V.11. — C.988–998.

[II] Е. А. Беспалов, Д. С. Кротов. Об одном признаке свитчинговой разделимости графов по модулю q // Сиб. матем. журн. — 2016. — V.57, №1. — С. 10–24. (Перевод: E. A. Bespalov, D. S. Krotov. On one test for the switching separability of graphs modulo q // Siberian Math. J. — 2016. — V.57 №1. — P. 7–17.)

[III] Е. А. Беспалов, Д. С. Кротов. МДР-коды в графах Дуба // Пробл. передачи информ. — 2017. — V.53, №2. — С. 40–59. (Перевод: E. A. Bespalov, D. S. Krotov. MDS codes in Doob graphs // Problems Inform. Transmission. — 2017. — V.53, №2. — P. 136–154.)

[IV] E. A. Bespalov. On the minimum supports of some eigenfunctions in the Doob graphs // Сиб. электрон. матем. изв. — 2018. — V.15. — С. 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. — С.10-12.