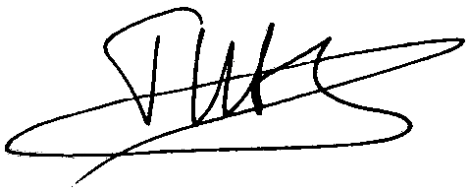
ФГБОУ ВО «МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ имени М.В. ЛОМОНОСОВА»

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи



Тумайкин Илья Николаевич

Коды Рида–Маллера как групповые коды

Специальность 01.01.06 — «математическая логика, алгебра и теория чисел»

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата физико-математических наук

Москва — 2017

Работа выполнена на кафедре высшей алгебры механико-математического факультета ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова».

Научный руководитель: Марков Виктор Тимофеевич,
кандидат физико-математических наук,
доцент.

Официальные оппоненты: Кожухов Игорь Борисович,
доктор физико-математических наук,
профессор, ФГАОУ ВО «Национальный исследовательский университет «МИЭТ»,
профессор кафедры высшей математики №1.

Лебедев Анатолий Николаевич,
кандидат физико-математических наук,
старший научный сотрудник,
ФГБОУ ВО «МГТУ имени Н.Э. Баумана»,
доцент кафедры Информационной безопасности.

Ведущая организация: ФГБОУ ВО «Тульский государственный педагогический университет имени Л.Н. Толстого».

Защита диссертации состоится 23 июня 2017 года в 16 часов 45 минут на заседании диссертационного совета Д 501.001.84 на базе ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова» по адресу: Российская Федерация, 119234, Москва, ГСП-1, Ленинские горы, д. 1, ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», механико-математический факультет, аудитория 14–08.

С диссертацией можно ознакомиться в Фундаментальной библиотеке ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова» по адресу: Российская Федерация, Москва, Ломоносовский проспект, д. 27, сектор А, этаж 8, и на следующих сайтах в сети Интернет:

`http://istina.msu.ru/dissertations/51743906/`
`http://mech.math.msu.su/~snark/index.cgi`

Автореферат разослан 23 мая 2017 года.

Учёный секретарь
диссертационного совета Д 501.001.84
на базе МГУ имени М.В. Ломоносова,
член-корреспондент РАН — Шафаревич Андрей Игоревич

Общая характеристика работы

Диссертация посвящена исследованию алгебраической структуры кодов Рида–Маллера. Данные коды рассматриваются как групповые коды, т.е. как идеалы групповой алгебры некоторой группы. В диссертации изучены совпадения кодов Рида–Маллера со степенями радикала соответствующей групповой алгебры в случае непростого поля, и получены необходимые и достаточные условия, при которых есть включения между кодами Рида–Маллера и степенями радикала.

Актуальность темы

Код с исправлением ошибок — это способ представления информации, обеспечивающий её надёжную передачу по каналу связи с помехами. Теория помехоустойчивого кодирования — обширная и постоянно развивающаяся область математики, включающая в себя разделы алгебры, комбинаторики, теории вероятностей, геометрии и теории чисел. Фундаментальная проблема теории кодирования состоит в эффективном обнаружении искажений, возникших при передаче данных, и восстановлении исходного сообщения. Первые работы, посвящённые проблемам помехоустойчивой передачи информации, были опубликованы К.Э. Шенноном в 1948 году. В настоящее время вопросы, связанные с надёжным обменом информацией, являются как никогда актуальными, что связано, прежде всего, с развитием компьютерных и телекоммуникационных технологий.

В основе помехоустойчивого кодирования лежит следующий принцип: перед передачей сообщения к нему добавляют полученную с помощью некоторого алгоритма избыточную информацию, которая позволяет принимающей стороне обнаружить и устранить возникшие искажения. Процессы добавления избыточной информации и последующего восстановления исходного сообщения называют кодированием и декодированием, соответственно. С каждым кодом связаны перечисленные ниже базовые понятия.

- **Множество сообщений.** Данное множество определяется алфавитом и длиной сообщения. В самом простом и практически важном случае алфавит — это множество $\{0, 1\}$. В общем случае алфавит, как правило, состоит из элементов конечного поля $\mathbb{F}_q$. Сообщения являются словами одинаковой длины k в выбранном алфавите.

- **Множество кодовых слов.** В результате кодирования сообщения получается новое слово в том же алфавите, которое называется кодовым словом. Кодовые слова являются словами одинаковой длины n в выбранном ранее алфавите. Множество всех кодовых слов обычно отождествляют с кодом. Число n называют длиной кода.

- **Алгоритмы кодирования и декодирования.** Алгоритм кодирования определяется функцией, действующей из множества сообщений в множество кодовых слов. Алгоритм декодирования — функцией, действующей из множества кодовых слов в множество сообщений.

На сегодняшний день разработано и изучено большое количество различных семейств кодов. Одним из таких семейств являются коды Рида–Маллера, которые носят имена своих авторов: американских математиков Ирвинга Рида и Дэвида Маллера. Коды Рида–Маллера были созданы в 1954 году и с тех пор представляют интерес как простые в реализации и надёжные коды. Данные коды и алгоритмы их кодирования и декодирования подробно исследованы. Однако, отдельные вопросы о структуре их множества кодовых слов всё ещё остаются открытыми.

Известно, что коды Рида–Маллера допускают несколько эквивалентных определений: с помощью булевых функций [1], с помощью конечных геометрий [2], с помощью идеалов кольца многочленов [2], с помощью идеалов групповой алгебры [3]. Данная диссертация опирается на теоретико-кольцевой метод изучения кодов Рида–Маллера [4], предложенный в 2012 году группой учёных: Коусело, Гонсалес, Марков, Мартинес, Нечаев. В основе этого метода лежит понятие базисного кода Рида–Маллера.

Замечание. Далее будем называть коды Рида–Маллера обычными кодами Рида–Маллера, чтобы отличать их от базисных кодов Рида–Маллера.

Алгебраическая структура обычных кодов Рида–Маллера над простым полем хорошо изучена: классический результат, впервые полученный Берманом [5] и позже обобщённый Шарпен [6], гласит, что в данном случае обычные коды Рида–Маллера совпадают со степенями радикала соответствующей групповой алгебры. Однако, вопрос о совпадении обычных кодов Рида–Маллера и степеней радикала в случае непростого поля оставался без подробного рассмотрения в известных автору диссертации работах. Вопрос об условиях, описывающих теоретико-множественные включения между обычными кодами Рида–Маллера и степенями радикала, оставался полностью неисследованным.

Цель работы

Цель данной работы — доказать отсутствие нетривиальных совпадений обычных кодов Рида–Маллера над непростым полем со степенями радикала соответствующей групповой алгебры, найти необходимые и достаточные условия теоретико-множественных включений между обычными кодами Рида–Маллера и степенями радикала этой алгебры.

---

[1] MacWilliams F.J., Sloane N.J.A. The Theory of Error-Correcting Codes. Amsterdam: North Holland, 1977.

[2] Assmus E.F. Jr., Key J.D. Polynomial codes and finite geometries // Handbook of Coding Theory. Amsterdam: Elsevier, 1998. Vol. 2. P. 1269–1343.

[3] Landrock P., Manz O. Classical codes as ideals in group algebras // Designs, Codes and Cryptography. 1992. Vol. 2, № 3. P. 273–285.

[4] Коусело Е., Гонсалес С., Марков В.Т., Мартинес К., Нечаев А.А. Представления кодов Рида–Соломона и Рида–Маллера идеалами // Алгебра и логика. 2012. Т. 51, № 3. С. 297–320.

[5] Берман С.Д. К теории групповых кодов // Кибернетика. 1967. Т. 3, № 1. С. 31–39.

[6] Charpin P. Une généralisation de la construction de Berman des codes de Reed et Muller p-aires // Communications in Algebra. 1988. Vol. 16, № 11. P. 2231–2246.

Научная новизна

Результаты данной диссертации являются новыми, получены автором самостоятельно и заключаются в следующем:

1. Исследованы совпадения базисных кодов Рида–Маллера со степенями радикала соответствующей групповой алгебры. Доказано отсутствие нетривиальных совпадений в случае непростого подполя.

2. Получены необходимые и достаточные условия, при которых есть включения между базисными кодами Рида–Маллера и степенями радикала соответствующей групповой алгебры. Дано теоретико-кольцевое, теоретико-множественное и числовое описание полученных условий.

3. На основе развитых в данной работе методов получены аналоги вышеперечисленных результатов для обычных кодов Рида–Маллера:

   - Доказано отсутствие нетривиальных совпадений обычных кодов Рида–Маллера со степенями радикала соответствующей групповой алгебры в случае непростого поля.
   - Получены необходимые и достаточные условия, при которых есть включения между обычными кодами Рида–Маллера и степенями радикала соответствующей групповой алгебры. Дано теоретико-кольцевое, теоретико-множественное и числовое описание полученных условий.

Методы исследования

В диссертации используются методы теории колец, методы теории чисел, методы теории базисных кодов Рида–Маллера. Предварительные результаты были получены с помощью методов компьютерного моделирования, которые кратко описаны в приложении.

Теоретическая и практическая ценность

Работа имеет теоретический характер. Вместе с тем, полученные результаты применимы в практических задачах теории кодирования и вносят вклад в теорию обычных и базисных кодов Рида–Маллера.

Апробация диссертации

Результаты диссертации освещались автором на семинарах кафедры высшей алгебры механико-математического факультета МГУ:

- научно-исследовательский семинар по алгебре;
- семинар “Кольца и модули”.

Публикации

Основные результаты диссертации опубликованы в работах [1], [2], [3], из них первые две — в журналах из перечня ВАК. Список публикаций приведён в конце автореферата.

Структура диссертации

Диссертация состоит из введения, шести разделов, заключения, списка литературы и приложения. Библиография содержит 13 наименований. Текст диссертации изложен на 52 страницах.

Краткое содержание работы

Раздел 1 носит вспомогательный характер: приводятся необходимые определения и формулировки базовых фактов, которые используются в данной научной работе. Перечислим ключевые из них.

Пусть A — конечное коммутативное кольцо с единицей, G — группа порядка n с единицей e. Зафиксируем некоторую нумерацию элементов группы G такую, что $G = \{g_1, \ldots, g_n\}$ и $e = g_1$. Рассмотрим групповое кольцо AG. Тогда любое подмножество $I \subseteq AG$ определяет код $\mathcal{K}(I)$ длины n в алфавите A равенством

$$\mathcal{K}(I) = \left\{ (a_1, \ldots, a_n) \in A^n : \sum_{i=1}^{n} a_i g_i \in I \right\}.$$

Если I — идеал AG, то код $\mathcal{K}(I)$ называется групповым кодом в кольце AG. Далее будем отождествлять идеал I и соответствующий ему групповой код $\mathcal{K}(I)$. Отметим, что AG также является групповой алгеброй над кольцом A.

Пусть p — простое число и $q = p^l$, $l \geqslant 1$. Рассмотрим поле $Q = \mathbb{F}_q$ характеристики p и порядка q. Пусть $q = \pi^m$, где $m > 1$, $l = \lambda m$, $\pi = p^\lambda$, $\lambda \geqslant 1$. Рассмотрим поле $P = \mathbb{F}_\pi$ характеристики p и порядка π. Пусть группа $(H, \cdot)$ изоморфна аддитивной группе поля Q. Рассмотрим групповую алгебру $S = QH$ и групповую алгебру $R = PH$. Радикалы алгебр S и R обозначим $\mathfrak{R}_S$ и $\mathfrak{R}_R$, соответственно. Пусть $\phi : (H, \cdot) \to (Q, +)$ — указанный выше изоморфизм.

Рассмотрим следующие элементы:

$$u_i = \sum_{h \in H} (\phi(h))^i h \in S, \ i \in \overline{0, q-1}.$$

π-весом числа i назовём сумму цифр в его π-ичном представлении и обозначим $\omega_\pi(i)$. Заметим, что $\omega_\pi(i) \in \overline{0, m(\pi-1)}$ при $i \in \overline{0, q-1}$. Аналогично вводится p-вес.

Определение. Для всех $k \in \overline{0, m(\pi-1)}$ определим базисный код Рида–Маллера порядка k над полем Q равенством

$$\mathcal{M}_\pi(m,k) = \sum_{\substack{i\in\overline{0,q-1}\\ 0\leqslant\omega_\pi(i)\leqslant k}} Qu_i.$$

Определение. Пусть $\mathrm{tr} = \mathrm{tr}_P^Q$ — функция следа из поля Q в поле P. Определим функцию следа $\mathrm{Tr} = \mathrm{Tr}_R^S$ из алгебры S в алгебру R равенством

$$\mathrm{Tr}\left(\sum_{h\in H}\alpha_h h\right) = \sum_{h\in H}\mathrm{tr}(\alpha_h)h,\ \ \alpha_h \in Q.$$

Утверждение. *Обозначим* $\mathcal{RM}_\pi(m,k) = \mathrm{Tr}(\mathcal{M}_\pi(m,k))$. *Тогда код* $\mathcal{RM}_\pi(m,k)$ *является кодом Рида–Маллера порядка* k *над полем* P.

Раздел 2 описывает совпадения базисных кодов Рида–Маллера со степенями радикала соответствующей групповой алгебры. Кратко изложен известный случай простого подполя и подробно исследован случай непростого подполя. Доказана теорема 2.1, которая показывает, что в случае непростого подполя есть только тривиальные совпадения.

Известно, что при $\lambda = 1$ базисные коды Рида–Маллера — это степени радикала $\mathfrak{R}_S$ [7].

Утверждение 2.1. *Пусть* $j \in \overline{0, l(p-1)}$, *тогда выполнено равенство*

$$\mathcal{M}_p(l,j) = {\mathfrak{R}_S}^{l(p-1)-j}.$$

Совпадения базисных кодов со степенями радикала существуют и в случае произвольного непростого подполя Q. Все они являются тривиальными и описываются следующим утверждением.

Утверждение 2.2. *Пусть* $\lambda \neq 1$, *тогда выполнены равенства*

$$\begin{aligned}\mathcal{M}_\pi(m,0) &= \mathcal{M}_p(l,0),\\ \mathcal{M}_\pi(m,m(\pi-1)-1) &= \mathcal{M}_p(l,l(p-1)-1),\\ \mathcal{M}_\pi(m,m(\pi-1)) &= \mathcal{M}_p(l,l(p-1)).\end{aligned}$$

Основным результатом этого раздела является

Теорема 2.1. *Пусть* $\lambda \neq 1$. *Пусть* $k \in \overline{1, m(\pi-1)-2}$ *и* $j \in \overline{1, l(p-1)-2}$. *Тогда имеет место соотношение*

$$\mathcal{M}_\pi(m,k) \neq \mathcal{M}_p(l,j).$$

Данная теорема показывает, что при $\lambda \neq 1$ есть только перечисленные выше тривиальные совпадения между базисными кодами и степенями радикала $\mathfrak{R}_S$.

[7] Коусело Е., Гонсалес С., Марков В.Т., Мартинес К., Нечаев А.А. Представления кодов Рида–Соломона и Рида–Маллера идеалами // Алгебра и логика. 2012. Т. 51, № 3. С. 297–320.

Раздел 3 посвящён изучению теоретико-множественных включений между базисными кодами Рида–Маллера и степенями радикала. Последовательно рассмотрен сначала случай включения базисных кодов в степени радикала, затем — включения степеней радикала в базисные коды. В обоих случаях получены необходимые и достаточные условия указанных включений.

Рассмотрим граф включений базисных кодов Рида–Маллера и степеней радикала $\mathfrak{R}_S$, т.е. ориентированный граф, в котором вершины соответствуют указанным идеалам, и между двумя идеалами проходит дуга, когда один из них есть подмножество другого; при этом начало такой дуги — вершина, соответствующая надмножеству, а конец — вершина, соответствующая подмножеству. Далее рассматриваются графы после проведения транзитивной редукции, т.е. после удаления всех рёбер, не влияющих на связность между любыми двумя вершинами.

Рассмотрим следующую ситуацию: в вершину, соответствующую идеалу $\mathcal{M}_\pi(m,k)$, входят два направленных ребра. Первое выходит из вершины, соответствующей $\mathcal{M}_\pi(m,k+1)$, а второе выходит из вершины, соответствующей $\mathcal{M}_p(l,l(p-1)-\alpha)=\mathfrak{R}_S{}^\alpha$ для некоторого α. Данный случай описывается следующими условиями:

$$\mathcal{M}_\pi(m,k)\subset\mathfrak{R}_S{}^\alpha, \tag{1}$$

$$\mathcal{M}_\pi(m,k)\nsubseteq\mathfrak{R}_S{}^{\alpha+1}, \tag{2}$$

$$\mathcal{M}_\pi(m,k+1)\nsubseteq\mathfrak{R}_S{}^\alpha. \tag{3}$$

Теоремы 3.1 и 3.2 определяют теоретико-кольцевой критерий указанных включений.

Теорема 3.1. *Пусть для некоторого* $k\in\overline{1,m(\pi-1)-2}$ *выполнено равенство*

$$\mathfrak{R}_S\mathcal{M}_\pi(m,k+1)=\mathcal{M}_\pi(m,k), \tag{4}$$

тогда существует и притом единственное $\alpha\in\overline{1,l(p-1)-1}$ *такое, что имеют место соотношения* (1), (2), (3).

Теорема 3.2. *Пусть* $\alpha\in\overline{1,l(p-1)-1}$ *и* $k\in\overline{1,m(\pi-1)-2}$. *Пусть имеют место соотношения* (1), (2), (3), *тогда выполнено равенство* (4).

Получены также теоретико-множественные и числовые критерии данных включений.

Определение. Определим множества P_j и Π_k равенствами

$$\mathrm{P}_j=\{t\in\mathbb{Z}:0\leqslant\omega_p(t)\leqslant j\},\ \Pi_k=\{t\in\mathbb{Z}:0\leqslant\omega_\pi(t)\leqslant k\}.$$

Утверждение 3.9. *Пусть* $\alpha\in\overline{1,l(p-1)-1}$ *и* $k\in\overline{1,m(\pi-1)-2}$. *Соотношения* (1), (2), (3) *имеют место тогда и только тогда, когда* k *— максимальное среди чисел* k', *для которых* $j=l(p-1)-\alpha$ *является наименьшим таким, что* $\Pi_{k'}\subset\mathrm{P}_j$.

Определим отображение $\psi:\mathbb{N}\to\mathbb{N}$ равенством $\psi(t)=(t+1)p+m(p-1)-1$ и положим $\psi^0=\mathrm{Id}$.

Теорема 3.5. *Пусть* $\alpha \in \overline{1, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-2}$. *Соотношения* (1), (2), (3) *имеют место тогда и только тогда, когда*

$$k = \psi^{\theta}(\tau),$$

где θ *и* τ *— частное и остаток от деления* $j = l(p-1)-\alpha$ *на* $m(p-1)$, *т.е.* $j = \theta m(p-1)+\tau$, *где* $0 \leqslant \tau < m(p-1)$.

Рассмотрим другую ситуацию: в вершину, соответствующую идеалу $\mathcal{M}_p(l, l(p-1)-\alpha) = \mathfrak{R}_S{}^{\alpha}$, входят два направленных ребра. Первое выходит из вершины, соответствующей $\mathfrak{R}_S{}^{\alpha-1}$, а второе выходит из вершины, соответствующей $\mathcal{M}_\pi(m,k)$ для некоторого k. Данный случай описывается следующими условиями:

$$\mathfrak{R}_S{}^{\alpha} \subset \mathcal{M}_\pi(m,k), \tag{5}$$

$$\mathfrak{R}_S{}^{\alpha} \nsubseteq \mathcal{M}_\pi(m,k-1), \tag{6}$$

$$\mathfrak{R}_S{}^{\alpha-1} \nsubseteq \mathcal{M}_\pi(m,k). \tag{7}$$

Для этого типа включений получены теоретико-множественные и числовые критерии.

Утверждение 3.10. *Пусть* $\alpha \in \overline{2, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-1}$. *Число* k *является минимальным таким, что для* $j = l(p-1)-\alpha$ *имеет место включение* $\mathrm{P}_j \subset \Pi_k$, *тогда и только тогда, когда имеют место соотношения* (5), (6), (7).

Теорема 3.6. *Пусть* $\alpha \in \overline{2, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-1}$. *Соотношения* (5), (6), (7) *имеют место тогда и только тогда, когда выполнено равенство*

$$k = \sum_{i=0}^{\theta-1} m(p-1)p^{\lambda-1-i} + \tau p^{\lambda-\theta-1},$$

где θ *и* τ *— частное и остаток от деления* $j = l(p-1)-\alpha$ *на* $m(p-1)$, *т.е.* $j = \theta m(p-1)+\tau$, *где* $0 \leqslant \tau < m(p-1)$.

Отметим, что полученные в данном разделе результаты дают необходимые и достаточные условия, при которых две произвольные вершины, соответствующие идеалам $\mathcal{M}_\pi(m,k)$ и $\mathcal{M}_p(l,j)$, соединены дугой в графе включений.

В **разделе 4** подробнее исследованы произведения радикала и базисных кодов, которые определяют упомянутые выше теоретико-кольцевые критерии включения базисных кодов в степени радикала.

Результаты данного раздела показывают, что в случае $\lambda \neq l$ равенство $\mathfrak{R}_S\mathcal{M}_\pi(m,i) = \mathcal{M}_\pi(m,j)$ может выполняться только при условии $i = j+1$. Однако, в случае $\lambda = l$ равенство $\mathfrak{R}_S\mathcal{M}_\pi(m,i) = \mathcal{M}_\pi(m,j)$ может выполняться при других условиях: $j+1 \not\equiv_p p-1$ и $i = j+1$, либо $j+1 \equiv_p p-1$ и $i = j+1$ или $i = j+2$.

В **разделе 5** построены базисы специального вида для обычных кодов Рида–Маллера. Данные базисы состоят из образов базисных элементов базисных кодов Рида–Маллера под

действием отображения Tr и являются связующим звеном при рассмотрении базисных и обычных кодов в совокупности.

Раздел 6 посвящён доказательству результатов для обычных кодов Рида–Маллера аналогичных результатам, полученным для базисных кодов в разделах 2 и 3. Существенную роль здесь играют базисы, рассмотренные в предыдущем разделе.

В **подразделе 6.1** доказывается важное вспомогательное утверждение, которое многократно используется в разделе 6.

Утверждение 6.1. *Пусть* $k \in \overline{0, q-1}$*, тогда выполнено равенство*

$$\mathfrak{R}_R \mathcal{RM}_\pi(m,k) = \mathrm{Tr}(\mathfrak{R}_S \mathcal{M}_\pi(m,k)).$$

В **подразделе 6.2** исследованы совпадения обычных кодов Рида–Маллера со степенями радикала в случае непростого поля, т.е. в случае $\lambda \neq 1$.

Известно, что при $\lambda = 1$ обычные коды Рида–Маллера — это степени радикала $\mathfrak{R}_R$ [8,9,10].

Утверждение 6.2. *Пусть* $j \in \overline{0, l(p-1)}$*, тогда выполнено равенство*

$$\mathcal{RM}_p(l,j) = {\mathfrak{R}_R}^{l(p-1)-j}.$$

Совпадения кодов Рида–Маллера со степенями радикала существуют и в случае произвольного непростого подполя Q. Все они являются тривиальными и описываются следующим утверждением.

Утверждение 6.3. *Пусть* $\lambda \neq 1$*, тогда выполнены равенства*

$$\begin{gathered}\mathcal{RM}_\pi(m,0) = \mathcal{RM}_p(l,0),\\ \mathcal{RM}_\pi(m, m(\pi-1)-1) = \mathcal{RM}_p(l, l(p-1)-1),\\ \mathcal{RM}_\pi(m, m(\pi-1)) = \mathcal{RM}_p(l, l(p-1)).\end{gathered}$$

Получена теорема 6.1, которая утверждает, что, подобно базисным кодам, при $\lambda \neq 1$ других совпадений обычных кодов Рида–Маллера со степенями радикала нет.

Теорема 6.1. *Пусть* $\lambda \neq 1$*. Пусть* $k \in \overline{1, m(\pi-1)-2}$ *и* $j \in \overline{1, l(p-1)-2}$*. Тогда имеет место соотношение*

$$\mathcal{RM}_\pi(m,k) \neq \mathcal{RM}_p(l,j).$$

Как было отмечено ранее, совпадению кодов Рида–Маллера со степенями радикала в случае $\lambda \neq 1$ обычно уделяется мало внимания. В работе Ландрока и Манца [10] результат

[8] Берман С.Д. К теории групповых кодов // Кибернетика. 1967. Т. 3, № 1. С. 31–39.

[9] Charpin P. Une généralisation de la construction de Berman des codes de Reed et Muller p-aires // Communications in Algebra. 1988. Vol. 16, № 11. P. 2231–2246.

[10] Landrock P., Manz O. Classical codes as ideals in group algebras // Designs, Codes and Cryptography. 1992. Vol. 2, № 3. P. 273–285.

аналогичный теореме 6.1 упомянут без доказательства. Автору не удалось найти доказательств указанной теоремы и в других источниках. Можно сказать, что данная теорема не является абсолютно новым результатом, однако удовлетворительное доказательство оставалось до сих пор неизвестным.

В **подразделе 6.3** изучены теоретико-множественные включения между обычными кодами Рида–Маллера и степенями радикала, и получены необходимые и достаточные условия этих включений.

Подобно случаю базисных кодов, рассмотрим граф включений кодов Рида–Маллера и степеней радикала $\mathfrak{R}_R$, т.е. ориентированный граф, в котором вершины соответствуют указанным идеалам, и между двумя идеалами проходит дуга, когда один из них есть подмножество другого; при этом начало такой дуги — вершина, соответствующая надмножеству, а конец — вершина, соответствующая подмножеству.

Рассмотрим следующую ситуацию: в вершину, соответствующую идеалу $\mathcal{RM}_\pi(m,k)$, входят два направленных ребра. Первое выходит из вершины, соответствующей $\mathcal{RM}_\pi(m,k+1)$, а второе выходит из вершины, соответствующей $\mathcal{RM}_p(l,l(p-1)-\alpha)={\mathfrak{R}_R}^\alpha$ для некоторого α. Данный случай описывается следующими условиями:

$$\mathcal{RM}_\pi(m,k)\subset {\mathfrak{R}_R}^\alpha, \tag{8}$$

$$\mathcal{RM}_\pi(m,k)\nsubseteq {\mathfrak{R}_R}^{\alpha+1}, \tag{9}$$

$$\mathcal{RM}_\pi(m,k+1)\nsubseteq {\mathfrak{R}_R}^\alpha. \tag{10}$$

Теоремы 6.2 и 6.3 определяют теоретико-кольцевой критерий указанных включений.

Теорема 6.2. *Пусть для некоторого* $k\in\overline{1,m(\pi-1)-2}$ *выполнено равенство*

$$\mathfrak{R}_R\mathcal{RM}_\pi(m,k+1)=\mathcal{RM}_\pi(m,k), \tag{11}$$

тогда существует и притом единственное $\alpha\in\overline{1,l(p-1)-1}$ *такое, что имеют место соотношения* (8), (9), (10).

Теорема 6.3. *Пусть* $\alpha\in\overline{1,l(p-1)-1}$ *и* $k\in\overline{1,m(\pi-1)-2}$. *Пусть имеют место соотношения* (8), (9), (10), *тогда выполнено равенство* (11).

Получены также теоретико-множественные и числовые критерии данных включений.

Утверждение 6.7. *Пусть* $\alpha\in\overline{1,l(p-1)-1}$ *и* $k\in\overline{1,m(\pi-1)-2}$. *Число* k *есть максимальное среди чисел* k', *для которых* $j=l(p-1)-\alpha$ *является наименьшим таким, что* $\Pi_{k'}\subset \mathrm{P}_j$, *тогда и только тогда, когда имеют место соотношения* (8), (9), (10).

Теорема 6.5. *Пусть* $\alpha\in\overline{1,l(p-1)-1}$ *и* $k\in\overline{1,m(\pi-1)-2}$. *Соотношения* (8), (9), (10) *имеют место тогда и только тогда, когда*

$$k=\psi^\theta(\tau),$$

где θ *и* τ *— частное и остаток от деления* $j = l(p-1)-\alpha$ *на* $m(p-1)$, *т.е.* $j = \theta m(p-1)+\tau$, *где* $0 \leqslant \tau < m(p-1)$.

Рассмотрим другую ситуацию: в вершину, соответствующую идеалу $\mathcal{RM}_p(l, l(p-1)-\alpha) = {\mathfrak{R}_R}^{\alpha}$, входят два направленных ребра. Первое выходит из вершины, соответствующей ${\mathfrak{R}_R}^{\alpha-1}$, а второе выходит из вершины, соответствующей $\mathcal{RM}_\pi(m,k)$ для некоторого k. Данный случай описывается следующими условиями:

$$ {\mathfrak{R}_R}^{\alpha} \subset \mathcal{RM}_\pi(m,k), \tag{12} $$

$$ {\mathfrak{R}_R}^{\alpha} \nsubseteq \mathcal{RM}_\pi(m,k-1), \tag{13} $$

$$ {\mathfrak{R}_R}^{\alpha-1} \nsubseteq \mathcal{RM}_\pi(m,k). \tag{14} $$

Для этого типа включений доказаны теоретико-множественные и числовые критерии.

Утверждение 6.8. *Пусть* $\alpha \in \overline{2, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-1}$. *Число* k *является минимальным таким, что для* $j = l(p-1)-\alpha$ *имеет место включение* $\mathrm{P}_j \subset \Pi_k$, *тогда и только тогда, когда имеют место соотношения* (12), (13), (14).

Теорема 6.6. *Пусть* $\alpha \in \overline{2, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-1}$. *Соотношения* (12), (13), (14) *имеют место тогда и только тогда, когда выполнено равенство*

$$ k = \sum_{i=0}^{\theta-1} m(p-1)p^{\lambda-1-i} + \tau p^{\lambda-\theta-1}, $$

где θ *и* τ *— частное и остаток от деления* $j = l(p-1)-\alpha$ *на* $m(p-1)$, *т.е.* $j = \theta m(p-1)+\tau$, *где* $0 \leqslant \tau < m(p-1)$.

Заключение

В данной диссертационной работе исследованы совпадения и теоретико-множественные включения между базисными кодами Рида–Маллера и степенями радикала соответствующей групповой алгебры. Доказано отсутствие нетривиальных совпадений в случае непростого подполя. Получены необходимые и достаточные условия, при которых есть включения между базисными кодами и степенями радикала. Дано теоретико-кольцевое, теоретико-множественное и числовое описание указанных условий. Доказанные в работе результаты согласуются с результатами компьютерного моделирования.

Разработаны методы переноса отдельных классов результатов для базисных кодов Рида–Маллера на случай обычных кодов Рида–Маллера. Для этого построены специальные базисы обычных кодов Рида–Маллера, отличающиеся новыми свойствами.

На основе данных методов исследованы совпадения и теоретико-множественные включения между обычными кодами Рида–Маллера и степенями радикала, и для них доказаны аналоги полученных в работе результатов для базисных кодов Рида–Маллера: доказано отсутствие нетривиальных совпадений между обычными кодами Рида–Маллера и степенями

радикала в случае непростого поля, и получены необходимые и достаточные условия, при которых есть включения между обычными кодами Рида–Маллера и степенями радикала соответствующей групповой алгебры.

Представленные результаты и методы, имея самостоятельную научную значимость, дают возможность дальнейшего исследования обычных и базисных кодов Рида–Маллера, например, для оценки параметров указанных кодов в случае непростого поля на основе известных результатов в случае простого поля.

Благодарности

Автор выражает глубокую благодарность за постановку задач, руководство работой и поддержку своему научному руководителю Виктору Тимофеевичу Маркову.

Работы автора по теме диссертации

[1] Тумайкин И.Н. Базисные коды Рида–Маллера и их связь со степенями радикала групповой алгебры над непростым полем // Вестник Московского университета. Серия 1, Математика. Механика. 2013. № 6. С. 46–49.

[2] Тумайкин И.Н. Базисные коды Рида–Маллера как групповые коды // Фундаментальная и прикладная математика. 2013. Т. 18, № 4. С. 137–154.

[3] Тумайкин И.Н. Коды Рида–Маллера как групповые коды // деп. в ВИНИТИ РАН 01.03.2017, № 23–В2017. 29 с.