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

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи
УДК 512.715

Тумайкин Илья Николаевич

Коды Рида–Маллера как групповые коды

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

Диссертация на соискание учёной степени
кандидата физико-математических наук

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

Москва — 2017

Содержание

Введение

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. Прежде чем переходить к формулировке основной проблемы, введём необходимые понятия.

Известно, что коды Рида–Маллера допускают несколько эквивалентных определений: с помощью булевых функций [8], с помощью конечных геометрий [4], с помощью идеалов в кольце многочленов [4], с помощью идеалов групповой алгебры [7]. Данная диссертация опирается на теоретико-кольцевой метод изучения кодов Рида–Маллера [2], 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.

Перейдём к построению обычных кодов Рида–Маллера. Пусть A — конечное коммутативное кольцо с единицей, G — группа порядка n с единицей e. Зафиксируем некоторое упорядочивание элементов группы G такое, что $G = \{e = g_1, \ldots, g_n\}$. 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.

Положим $A = \mathbb{F}_q$ — конечное поле характеристики p и порядка $q = p^l$, $G = H$ — элементарная абелева группа, изоморфная аддитивной группе поля $\mathbb{F}_q$, и пусть ϕ — соответствующий изоморфизм. Рассмотрим $\mathbb{F}_\pi$ — подполе порядка $\pi = p^\lambda$ в поле $\mathbb{F}_q$. Пусть $\omega_\pi(i)$ — сумма цифр в π-ичном представлении числа i. Тогда базисный код Рида–Маллера порядка k — это групповой код $\mathcal{M}_\pi(k)$ длины q в алфавите $\mathbb{F}_q$, где идеал $\mathcal{M}_\pi(k)$ определён равенством

$$\mathcal{M}_\pi(k) = \sum_{i \in \overline{0,q-1}:\ 0 \leqslant \omega_\pi(i) \leqslant k} \mathbb{F}_q \left(\sum_{h \in H} (\phi(h))^i h \right).$$

Рассмотрим tr — функцию следа из поля $\mathbb{F}_q$ в подполе $\mathbb{F}_\pi$. Определим отображение Tr:

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

Тогда $\mathrm{Tr}(\mathcal{M}_\pi(k))$ является идеалом $\mathbb{F}_\pi H$, а групповой код $\mathrm{Tr}(\mathcal{M}_\pi(k))$ длины q в алфавите $\mathbb{F}_\pi$ — это обычный код Рида–Маллера порядка k [2].

Алгебраическая структура обычных кодов Рида–Маллера над простым полем хорошо изучена: классический результат, впервые полученный Берманом [1] и позже обобщённый Шарпен [5], гласит, что в данном случае обычные коды Рида–Маллера совпадают со степенями радикала указанной выше 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.

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 данной работы опубликованы в [11], [12], [13].

Структура диссертации

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

Краткое содержание диссертации по разделам

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

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 три таких тривиальных совпадения.

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.

В первом случае теоретико-кольцевые критерии описаны в теоремах 3.1 и 3.2, теоретико-множественные критерии — в утверждении 3.9, числовые критерии — в теореме 3.5. Во втором случае теоретико-множественные критерии описаны в утверждении 3.10, числовые критерии — в теореме 3.6.

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

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. Основным результатом раздела является теорема 5.4, а непосредственная конструкция указанных базисов содержится в предшествующих данной теореме утверждениях.

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 6.2 исследованы совпадения обычных кодов Рида–Маллера со степенями радикала в случае непростого поля. Доказана теорема 6.1, которая показывает, что, подобно базисным кодам, в случае непростого поля есть только три таких тривиальных совпадения.

В подразделе 6.3 изучены теоретико-множественные включения между обычными кодами Рида–Маллера и степенями радикала и получены необходимые и достаточные условия этих включений. В случае включения кодов в степени радикала теоретико-кольцевые критерии описаны в теоремах 6.2 и 6.3, теоретико-множественные критерии — в утверждении 6.7, числовые критерии — в теореме 6.5. В случае включения степеней радикала в обычные коды теоретико-множественные критерии описаны в утверждении 6.8, числовые критерии — в теореме 6.6. Отметим, что теоретико-множественные и числовые критерии одинаковы для базисных и обычных кодов Рида–Маллера.

Благодарности

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

1 Предварительные сведения и результаты

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:

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

Определение 1.1. 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 1.2 ([2])**.** Для всех $k \in \overline{0, m(\pi-1)}$ определим базисный код Рида–Маллера порядка k над полем Q равенством

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

Утверждение 1.1 ([2])**.** *$\mathcal{M}_\pi(m, k)$ является идеалом в S и линейным кодом над Q с кодовыми параметрами $[q, M_\pi(m, k), d_\pi(m, k)]$, где $M_\pi(m, k)$ — размерность идеала $\mathcal{M}_\pi(m, k)$, которая равна числу расстановок $r \leqslant k$ шаров по m лункам так, что в каждой лунке меньше π шаров:*

$$M_\pi(m, k) = \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{m + k - \pi j}{k - \pi j} = \sum_{r=0}^{k} \left(\sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{m - 1 + r - \pi j}{m - 1} \right);$$

$d_\pi(m, k) = (\rho + 1)\pi^\varkappa$, где $\varkappa$ и ρ — частное и остаток от деления $m(\pi-1) - k$ на $(\pi - 1)$, т.е. $m(\pi-1) - k = \varkappa(\pi-1) + \rho$, где $0 \leqslant \rho < \pi - 1$.

Замечание 1.1. Известно, что $\mathcal{M}_\pi(m, m(\pi-1)) = S$ и $\mathcal{M}_\pi(m, m(\pi-1) - 1) = \mathfrak{R}_S$ [2]. Непосредственно из определения следует, что $\mathcal{M}_\pi(m, 0) = Q u_0$.

Утверждение 1.2 ([2])**.** *Множество $\{u_i : i \in \overline{0, q-1}, 0 \leqslant \omega_\pi(i) \leqslant k\}$ — базис $\mathcal{M}_\pi(m, k)$.*

Определение 1.3 ([3, 10])**.** Функцию следа tr_P^Q из поля Q в поле P определим равенством

$$\mathrm{tr}_P^Q(\alpha) = \alpha + \alpha^\pi + \alpha^{\pi^2} + \cdots + \alpha^{\pi^{m-1}},\ \alpha \in Q.$$

Определение 1.4 ([2])**.** 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 1.3 ([2])**.** $\mathrm{Tr} : S \to R$ *— эпиморфизм модулей, и образ любого ненулевого идеала в* S *является ненулевым идеалом в* R*.*

Определение 1.5 ([2])**.** Обозначим $\mathcal{RM}_\pi(m,k) = \mathrm{Tr}(\mathcal{M}_\pi(m,k))$.

Утверждение 1.4 ([2])**.** $\mathcal{RM}_\pi(m,k)$ *является идеалом в* R *и линейным кодом над* P *с кодовыми параметрами* $[q, M_\pi(m,k), d_\pi(m,k)]$*. Код* $\mathcal{RM}_\pi(m,k)$ *является кодом Рида–Маллера порядка* k *над полем* P*.*

Значительная часть дальнейших результатов опирается на следующие известные факты.

Лемма 1.1 ([2])**.** *Для любых* $s, t \in \overline{0, q-1}$ *имеют место соотношения:*

$$\begin{gathered} u_s u_t = 0,\ \textit{если } s+t \leqslant q-2; \\ u_s u_t = c_\delta u_\delta,\ \textit{где } c_\delta = -(-1)^{t-\delta}\binom{t}{\delta} = -(-1)^{s-\delta}\binom{s}{\delta}, \\ \textit{если } s+t = q-1+\delta < 2(q-1); \\ u_{q-1}u_{q-1} = -u_0 - u_{q-1}. \end{gathered}$$

Замечание 1.2. Отметим, что $c_\delta \in \mathbb{F}_p$.

Теорема 1.1 (Люка [8])**.** *Пусть* m, n *— целые неотрицательные числа, пусть* p *— простое число. Пусть* $[m]_p = [m_s, \ldots, m_0]$ *и* $[n]_p = [n_s, \ldots, n_0]$ *— p-ичные представления* m *и* n*, соответственно. Тогда*

$$\binom{m}{n} \equiv \prod_{i=0}^{s}\binom{m_i}{n_i} \bmod p.$$

Следствие 1.1. *Если в условиях предыдущей теоремы для некоторого* $i \in \overline{0, s}$ *выполнено* $m_i < n_i$*, тогда* $\binom{m}{n} \equiv 0 \bmod p$*.*

2 Совпадения базисных кодов Рида–Маллера со степенями радикала $\mathfrak{R}_S$

Известно, что при $\lambda = 1$ коды Рида–Маллера являются степенями радикала $\mathfrak{R}_R$ [1, 5], а базисные коды Рида–Маллера при этом совпадают со степенями радикала $\mathfrak{R}_S$ [2]. Цель данного раздела — показать, что при $\lambda \neq 1$ подобных совпадений базисных кодов, кроме тривиальных случаев, нет.

Лемма 2.1 ([6]). *Количество различных ненулевых степеней $\mathfrak{R}_S$ равно $l(p-1)$.*

Лемма 2.2. *Для всех целых $p \geqslant 2$ выполнено неравенство*

$$l(p-1) \leqslant m(\pi-1), \tag{1}$$

причём равенство достигается только при $\lambda = 1$.

Доказательство. Случай $\lambda = 1$ очевиден. Пусть $\lambda > 1$, тогда неравенство (1) можно переписать в виде $\lambda < \frac{p^\lambda - 1}{p-1}$. Сокращая в правой части, получаем $\lambda < 1 + p + \cdots + p^{\lambda-1}$. Число слагаемых справа равно λ, что завершает доказательство. □

Из лемм 2.1 и 2.2 вытекает, что в общем случае все базисные коды не могут совпадать со степенями радикала. В самом деле, согласно неравенству (1) заключаем, что для любого подполя P поля Q, кроме простого, количество базисных кодов Рида–Маллера больше количества степеней радикала.

Совпадения базисных кодов со степенями радикала в случае простого подполя описываются следующим утверждением.

Утверждение 2.1 ([2]). *Пусть $j \in \overline{0, l(p-1)}$, тогда выполнено равенство*

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

Замечание 2.1. В предыдущем утверждении мы рассматриваем также нулевую степень радикала, которую естественно положить равной S.

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*

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

Доказательство. Непосредственно следует из замечания 1.1 и утверждения 2.1. □

Покажем, что при $\lambda \neq 1$ других совпадений базисных кодов со степенями радикала нет. Введём необходимые определения.

Определение 2.1. π-записью числа t назовём его π-ичное представление и обозначим $[t]_\pi$. Аналогично вводится p-запись. Для $t \in \overline{0, q-1}$ отождествим $[t]_\pi$ и соответствующий элемент $\{0, \dots, \pi-1\}^m$. Аналогично отождествим $[t]_p$ и соответствующий элемент $\{0, \dots, p-1\}^l$. Элементы, составляющие $[t]_\pi$, назовём π-координатами. Аналогично вводятся p-координаты.

Определение 2.2. Для $t \in \overline{0, q-1}$ введём понятие λ-группы. Для этого разобьём $[t]_p$ на m групп, каждая из которых состоит из λ подряд идущих p-координат. Каждую полученную группу назовём λ-группой. Легко видеть, что между λ-группами и π-координатами существует взаимно-однозначное отображение. На множестве λ-групп введём отношение порядка, совпадающее с упорядочиванием по старшинству соответствующих π-координат.

Определение 2.3. Для $t \in \overline{0, q-1}$, $i \in \overline{0, \lambda-1}$ введём понятие i-слоя. Для этого каждой p-координате внутри каждой λ-группы t присвоим номер от 0 до $(\lambda-1)$ в соответствии с упорядочиванием по старшинству p-координат внутри данной λ-группы как элементов $[t]_p$. Упорядоченный набор p-координат с номерами i назовём i-слоем. Несложно понять, что между элементами i-слоя и π-координатами существует взаимно-однозначное отображение. На элементах i-слоя введём отношение порядка, совпадающее с упорядочиванием по старшинству соответствующих π-координат. Если значение i не требует уточнения, будем называть i-слой просто слоем.

Определение 2.4. Весом i-слоя назовём сумму его элементов.

Замечание 2.2. Пусть $t \in \overline{0, q-1}$ и $i \in \overline{0, \lambda-1}$, тогда

$$[t]_\pi = [\beta_{m-1}, \dots, \beta_0], \text{ где } \beta_j = \alpha_{\lambda-1,j} p^{\lambda-1} + \dots + \alpha_{i,j} p^i + \dots + \alpha_{0,j};$$
$$[t]_p = [\underbrace{\alpha_{\lambda-1,m-1}, \dots, \alpha_{i,m-1}, \dots, \alpha_{0,m-1}}_{\lambda\text{-группа}}, \dots, \underbrace{\alpha_{\lambda-1,0}, \dots, \alpha_{i,0}, \dots, \alpha_{0,0}}_{\lambda\text{-группа}}];$$
$$i\text{-слой} = [\alpha_{i,m-1}, \alpha_{i,m-2}, \dots, \alpha_{i,0}].$$

Определение 2.5. Определим множества P_j и Π_k равенствами

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

Лемма 2.3. *Пусть $j \in \overline{0, l(p-1)}$. Пусть*

$$t = \sum_{i=0}^{\theta-1} m(p-1) p^{\lambda-1-i} + \tau p^{\lambda-\theta-1}, \tag{2}$$

где θ и τ — частное и остаток от деления j на $m(p-1)$, т.е. $j = \theta m(p-1) + \tau$, где $0 \leqslant \tau < m(p-1)$. Тогда t имеет максимальный π-вес среди элементов P_j.

Доказательство. Построим число t максимального π-веса среди элементов P_j. Для этого необходимо предварительно найти число максимального π-веса среди чисел фиксированного p-веса. Покажем как должен быть распределён p-вес в p-записи искомого числа. Сначала рассмотрим отдельную λ-группу и максимизируем её π-вес. Несложно понять, что следует распределить наибольший p-вес в самые старшие разряды, поскольку при этом получается наибольшее значение соответствующей данной λ-группе π-координаты. Теперь максимизируем π-вес всех λ-групп в совокупности: сначала распределим максимально допустимый p-вес в самый старший разряд каждой из λ-групп, затем распределим максимально допустимый p-вес в следующий самый старший разряд каждой из λ-групп и т.д. Ясно, что построение p-записи происходит от старшего i-слоя к младшему. Легко видеть, что распределение p-веса в пределах одного i-слоя не имеет значения в силу того, что элементы одного слоя дают одинаковый вклад в результирующий π-вес. Для определённости p-вес в пределах одного слоя будем распределять от старшей p-координаты к младшей.

Таким образом, нашли число максимального π-веса среди чисел фиксированного p-веса. В самом деле, рассмотрим два числа a и b одинакового p-веса: a — произвольное, а b получено по указанной выше процедуре. Если веса соответствующих i-слоёв a и b совпадают, то у этих чисел одинаковый π-вес. Пусть a и b отличаются весом некоторых i-слоёв, тогда рассмотрим старший среди таких слоёв. Заметим, что вес данного i-слоя a меньше веса того же слоя b, поскольку последний по построению b имеет максимально допустимый вес. Отсюда вытекает, что в a значение какого-то разряда в этом i-слое уменьшилось в пользу какого-то разряда в более младшем слое a, т.е. результирующий π-вес a тоже уменьшился по сравнению с b. Следовательно, π-вес b больше π-веса a.

Легко видеть, что чем больший p-вес зафиксирован в начале, тем больший π-вес имеет построенное число. Значит, число t, которое имеет максимальный π-вес среди элементов P_j, удовлетворяет следующим условиям: во-первых, получено по указанной выше процедуре с точностью до перераспределения p-веса внутри некоторых i-слоёв, во-вторых, имеет p-вес равный j. Без ограничения общности можно считать, что p-запись t имеет распределение p-веса полностью совпадающее с вышеизложенной процедурой.

Заметим, что полностью заполненный слой имеет вес $m(p-1)$. Несложно понять, что в p-записи t будут полностью заполнены все слои от $(\lambda-1)$-слоя до $(\lambda-\theta)$-слоя, а $(\lambda-\theta-1)$-слой имеет вес τ, где θ и τ — частное и остаток от деления j на $m(p-1)$. Таким образом, значение t можно вычислить по формуле (2), что завершает доказательство. □

Следствие 2.1. *В условиях предыдущей леммы имеем* $\omega_p(t) = j$.

Лемма 2.4. *Пусть* $p \neq 2$. *Пусть* $j \in \overline{2, l(p-1)-2}$. *Пусть* t *определено согласно* (2). *Тогда в некоторой* λ*-группе* t *разность между старшей и младшей* p*-координатой не меньше* 2.

Доказательство. Пусть $[t]_p = [\alpha_{\lambda-1,m-1}, \ldots, \alpha_{0,m-1}, \ldots, \alpha_{\lambda-1,0}, \ldots, \alpha_{0,0}]$. Поскольку $j \geqslant 2$, по построению t имеем $\alpha_{\lambda-1,m-1} \geqslant 2$. Если $\alpha_{0,m-1} = 0$, то старшая λ-группа t является искомой. Пусть $\alpha_{0,m-1} > 0$, тогда согласно построению t получаем

$$\alpha_{\lambda-1,m-1} = \alpha_{\lambda-1,m-2} = \cdots = \alpha_{\lambda-1,0} = (p-1).$$

Заметим, что в данном случае $\alpha_{0,0} < (p-2)$. В самом деле, если $\alpha_{0,0} \geqslant (p-2)$, тогда по построению t имеем $t \geqslant (q-2)$, т.е. $\omega_p(t) = j \geqslant l(p-1)-1$, что противоречит условию. Отсюда заключаем, что при $\alpha_{0,m-1} > 0$ младшая λ-группа t является искомой. Лемма доказана. $\square$

Лемма 2.5. *Пусть $p = 2$. Пусть $j \in \overline{2, l(p-1)-2}$. Пусть t определено согласно* (2). *Тогда хотя бы в двух λ-группах t разность между старшей и младшей p-координатой равна* 1.

Доказательство. Пусть $[t]_p = [\alpha_{\lambda-1,m-1}, \ldots, \alpha_{0,m-1}, \ldots, \alpha_{\lambda-1,0}, \ldots, \alpha_{0,0}]$. Поскольку $j \geqslant 2$, по построению t имеем $\alpha_{\lambda-1,m-1} = \alpha_{\lambda-1,m-2} = 1$. Если $\alpha_{0,m-1} = 0$, то $\alpha_{0,m-2} = 0$ и две самые старшие λ-группы t являются искомыми. Пусть $\alpha_{0,m-1} > 0$, тогда согласно построению t получаем

$$\alpha_{\lambda-1,m-1} = \alpha_{\lambda-1,m-2} = \cdots = \alpha_{\lambda-1,0} = 1.$$

Заметим, что в данном случае $\alpha_{1,0} = \alpha_{0,0} = 0$. В самом деле, если это не так, тогда по построению t имеем $\omega_p(t) = j \geqslant l(p-1)-1$, что противоречит условию. Отсюда заключаем, что при $\alpha_{0,m-1} > 0$ две самые младшие λ-группы t являются искомыми. Лемма доказана. $\square$

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*

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

Доказательство. Рассуждая от противного, предположим, что существуют k, j такие, что имеет место равенство $\mathcal{M}_\pi(m,k) = \mathcal{M}_p(l,j)$. Согласно утверждению 1.2 данное равенство эквивалентно тому, что базисы из элементов u_i указанных идеалов совпадают, что, в свою очередь, равносильно тому, что $\mathrm{P}_j = \Pi_k$. Покажем, что в этом случае существует число $\tilde{t}$, принадлежащее Π_k, но не принадлежащее P_j, что приводит к противоречию.

Пусть сначала $j = 1$. В силу равенств $\omega_p(p^{\lambda-1}) = 1$ и $\omega_\pi(p^{\lambda-1}) = p^{\lambda-1}$ имеем $k \geqslant p^{\lambda-1}$. Положим $\tilde{t} = p^\lambda + 1$. Легко видеть, что $\omega_p(\tilde{t}) = 2$ и $\omega_\pi(\tilde{t}) = 2 \leqslant p^{\lambda-1} \leqslant k$. Таким образом, получено число $\tilde{t}$ такое, что $\tilde{t} \in \Pi_k$ и $\tilde{t} \notin \mathrm{P}_j$.

Пусть теперь $j > 1$. Пусть t определено согласно (2), тогда имеем $\omega_p(t) = j$ и $\omega_\pi(t) = k$. По леммам 2.4 и 2.5 без ограничения общности можно считать, что в младшей λ-группе t разность между старшей и младшей p-координатой не меньше 2 при $p \neq 2$ и равна 1 при $p = 2$. Положим $t' = t + 1$. Тогда в силу лемм 2.4 и 2.5 в некоторой λ-группе t' разность между старшей и младшей p-координатой не меньше 1. Несложно понять, что $\omega_p(t') = j + 1$ и $\omega_\pi(t') = k + 1$.

Рассмотрим следующее преобразование t': внутри каждой λ-группы поменяем местами p-координаты, стоящие на симметричных относительно середины данной λ-группы местах, т.е. переставим первую и последнюю позиции, вторую и предпоследнюю и т.д. Полученное число обозначим $\tilde{t}$.

Легко видеть, что $\omega_p(\tilde{t}) = \omega_p(t') = j + 1$. Заметим, что $\omega_\pi(\tilde{t}) < \omega_\pi(t') = k + 1$. В самом деле, по построению t' если две p-координаты одной λ-группы находятся на симметричных относительно середины данной λ-группы местах, то значение старшей из них не меньше значения младшей. Значит, при указанном преобразовании общий вклад этих p-координат в

π-вес не увеличится. Однако, в некоторой λ-группе t' разность между старшей и младшей p-координатой не меньше 1. Отсюда следует, что при рассмотренном выше преобразовании общий вклад этих p-координат в π-вес уменьшится. Таким образом, получено число $\tilde{t}$ такое, что $\tilde{t} \in \Pi_k$ и $\tilde{t} \notin \mathrm{P}_j$. Теорема доказана. □

Замечание 2.3. Аналогичный результат для $M_\pi(m,k)$ и $M_p(l,j)$ неверен: при $p=2$, $l=9$, $\lambda=3$ имеем $M_8(3,2)=M_2(9,1)$ и $M_8(3,18)=M_2(9,7)$, при $p=3$, $l=6$, $\lambda=3$ имеем $M_{27}(2,6)=M_3(6,2)$ и $M_{27}(2,45)=M_3(6,9)$.

Замечание 2.4. Несложно понять, что $\omega_\pi(t')-\omega_\pi(\tilde{t}) \geqslant p^{\lambda-1}-1$, причём равенство достигается только при $\omega_\pi(t')=l(p-1)-1$.

В работах, посвящённых кодам Рида–Маллера, основное внимание, как правило, уделено совпадению данных кодов со степенями радикала при $\lambda=1$, а случай $\lambda \neq 1$ рассматривается менее детально. Согласно теореме 2.1 при $\lambda \neq 1$ нет нетривиальных совпадений между базисными кодами Рида–Маллера и степенями радикала $\mathfrak{R}_S$. В разделе 6 получен аналог данной теоремы для обычных кодов Рида–Маллера. Далее, если не указано дополнительно, будем считать, что $\lambda \neq 1$.

3 Строение графа включений базисных кодов и степеней радикала

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. В данном графе есть два маршрута: маршрут, соответствующий включениям идеалов $\mathcal{M}_\pi(m,k)$ между собой, и маршрут, соответствующий включениям степеней радикала $\mathfrak{R}_S$ между собой. Согласно утверждениям 2.1 и 2.2 данные маршруты имеют три общие вершины, соответствующие тривиальным совпадениям. Отметим, что первый маршрут значительно длиннее второго. Далее рассматриваются графы после проведения транзитивной редукции, т.е. после удаления всех рёбер, не влияющих на связность между любыми двумя вершинами.

Естественно возникает вопрос: есть ли какие-то включения, кроме включений внутри указанных маршрутов? В данном разделе мы покажем, что такие включения существуют, и дадим их числовое описание.

Докажем результат, обобщающий [2, лемму 5.1].

Лемма 3.1. *Пусть* $k \in \overline{0, m(\pi-1)-1}$, *тогда имеет место включение*

$$\mathfrak{R}_S \mathcal{M}_\pi(m, k+1) \subseteq \mathcal{M}_\pi(m,k).$$

Доказательство. Пусть $u_s \in \mathfrak{R}_S$ и $u_t \in \mathcal{M}_\pi(m,k+1)$. Покажем, что тогда $u_s u_t \in \mathcal{M}_\pi(m,k)$. Отметим, что $s < q-1$. Согласно лемме 1.1 получаем либо $u_s u_t = 0 \in \mathcal{M}_\pi(m,k)$, либо $u_s u_t = c_\delta u_\delta$, $c_\delta \in {\mathbb{F}_p}^*$. Из теоремы Люка следует, что в последнем случае p-координаты t и δ, которые мы обозначим t_i и δ_i, удовлетворяют неравенствам

$$\delta_0 \leqslant t_0, \delta_1 \leqslant t_1, \ldots, \delta_{l-1} \leqslant t_{l-1}.$$

Значит, π-координаты t и δ удовлетворяют тем же неравенствам. По лемме 1.1 имеем $\delta < t$. Отсюда заключаем, что $\omega_\pi(\delta) < \omega_\pi(t) \leqslant k+1$, т.е. $c_\delta u_\delta \in \mathcal{M}_\pi(m,k)$. □

Утверждение 3.1. *Пусть* $j \in \overline{2, l(p-1)}$, *тогда имеет место включение*

$$\mathcal{M}_p(l, l(p-1)-j) \subset \mathcal{M}_\pi(m, m(\pi-1)-j).$$

Доказательство. Согласно утверждению 2.2 имеем

$$\mathcal{M}_p(l, l(p-1)-1) = \mathfrak{R}_S = \mathfrak{R}_S \mathcal{M}_\pi(m, m(\pi-1)) = \mathcal{M}_\pi(m, m(\pi-1)-1).$$

Применяя лемму 3.1, получаем

$$\mathcal{M}_p(l, l(p-1)-2) = \mathfrak{R}_S{}^2 = \mathfrak{R}_S\mathcal{M}_\pi(m, m(\pi-1)-1) \subseteq \mathcal{M}_\pi(m, m(\pi-1)-2).$$

Применяя эту лемму снова, получаем

$$\mathcal{M}_p(l, l(p-1)-3) = \mathfrak{R}_S{}^3 \subseteq \mathfrak{R}_S\mathcal{M}_\pi(m, m(\pi-1)-2) \subseteq \mathcal{M}_\pi(m, m(\pi-1)-3).$$

Повторяя аналогичные рассуждения, заключаем, что $\mathcal{M}_p(l, l(p-1)-j) \subseteq \mathcal{M}_\pi(m, m(\pi-1)-j)$. По теореме 2.1 данное включение строгое при $j \in \overline{2, l(p-1)-1}$. В силу утверждения 2.2 и леммы 2.2 данное включение строгое при $j = l(p-1)$. □

Лемма 3.2. *Для любого целого неотрицательного t выполнено неравенство $\omega_p(t) \leqslant \omega_\pi(t)$.*

Доказательство. Несложно понять, что достаточно рассмотреть только одну π-координату t и соответствующую ей λ-группу, т.е. можно считать, что $t \in \overline{0, \pi-1}$. Пусть $[t]_p = [t_{\lambda-1}, \ldots, t_0]$, тогда получаем

$$\omega_p(t) = t_0 + t_1 + t_2 + \cdots + t_{\lambda-1} \leqslant t_0 + t_1 p + t_2 p^2 + \cdots + t_{\lambda-1} p^{\lambda-1} = \omega_\pi(t).$$

□

Утверждение 3.2. *Пусть $j \in \overline{1, l(p-1)}$, тогда имеет место включение*

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

Доказательство. Пусть $u_t \in \mathcal{M}_\pi(m, j)$. Тогда по предыдущей лемме имеем $\omega_p(t) \leqslant \omega_\pi(t) \leqslant j$. Отсюда вытекает, что $u_t \in \mathcal{M}_p(l, j)$, т.е. $\mathcal{M}_p(l, j) \supseteq \mathcal{M}_\pi(m, j)$. Согласно теореме 2.1 данное включение строгое при $j \in \overline{1, l(p-1)-2}$. В силу утверждения 2.2 и леммы 2.2 данное включение строгое при $j = l(p-1)-1$ и $j = l(p-1)$. □

Доказанные выше утверждения дают часть информации о строении графа включений, но недостаточно, чтобы полностью описать его. Наша цель — найти необходимые и достаточные условия, при которых две вершины, соответствующие идеалам $\mathcal{M}_\pi(m, k)$ и $\mathcal{M}_p(l, l(p-1)-j) = \mathfrak{R}_S{}^j$, соединены дугой.

3.1 Включения вида $\mathfrak{R}_S{}^\alpha \supset \mathcal{M}_\pi(m, k)$

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:

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

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

$$\mathcal{M}_\pi(m,k+1) \nsubseteq {\mathfrak{R}_S}^\alpha. \tag{5}$$

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

$$\mathfrak{R}_S \mathcal{M}_\pi(m,k+1) = \mathcal{M}_\pi(m,k), \tag{6}$$

тогда существует и притом единственное $\alpha \in \overline{1, l(p-1)-1}$ *такое, что имеют место соотношения* (3), (4), (5).

Доказательство. Пусть для некоторого $k \in \overline{1, m(\pi-1)-2}$ выполнено равенство (6). Рассмотрим $\alpha \in \overline{1, l(p-1)-1}$ такое, что имеют место соотношения (3) и (4). Ясно, что указанное α существует и притом единственное. Предположим, что соотношение (5) неверно. Тогда имеем $\mathcal{M}_\pi(m,k+1) \subset {\mathfrak{R}_S}^\alpha$. Умножая обе части этого включения на $\mathfrak{R}_S$, получаем $\mathfrak{R}_S \mathcal{M}_\pi(m,k+1) \subseteq {\mathfrak{R}_S}^{\alpha+1}$. Отсюда следует, что $\mathcal{M}_\pi(m,k) \subseteq {\mathfrak{R}_S}^{\alpha+1}$, что противоречит (4). Таким образом, имеет место соотношение (5). Теорема доказана. □

Остановимся подробнее на граничных случаях равенства (6). Ранее было показано, что оно выполнено при $k = m(\pi-1)-1$. Докажем аналогичное утверждение при $k = 0$.

Утверждение 3.3.

$$\mathfrak{R}_S \mathcal{M}_\pi(m,1) = \mathcal{M}_\pi(m,0).$$

Доказательство. По лемме 3.1 имеем $\mathfrak{R}_S \mathcal{M}_\pi(m,1) \subseteq \mathcal{M}_\pi(m,0)$. Ясно, что $\mathcal{M}_\pi(m,0) = Qu_0$. Из леммы 1.1 получаем $u_{q-2}u_1 = u_0$, что завершает доказательство. □

Отметим, что граничные случаи равенства (6) соответствуют тривиальным совпадениям базисных кодов с ненулевыми степенями радикала.

Утверждение 3.4.

При $p \neq 2$ *имеем* $\mathfrak{R}_S \mathcal{M}_\pi(m,2) = \mathcal{M}_\pi(m,1)$.

При $p = 2, \lambda \neq l$ *имеем* $\mathfrak{R}_S \mathcal{M}_\pi(m,2) = \mathcal{M}_\pi(m,1)$.

При $p = 2, \lambda = l$ *имеем* $\mathfrak{R}_S \mathcal{M}_\pi(m,2) = \mathcal{M}_\pi(m,0)$.

Доказательство. Докажем первое утверждение. По лемме 3.1 получаем $\mathfrak{R}_S \mathcal{M}_\pi(m,2) \subseteq \mathcal{M}_\pi(m,1)$. Пусть δ такое, что $u_\delta \in \mathcal{M}_\pi(m,1)$, т.е. $\delta = \pi^i$, $i \in \overline{0, m-1}$. Тогда для $s = q-1-\pi^i$, $t = \delta + \pi^i$ имеем $u_s \in \mathfrak{R}_S$, $u_t \in \mathcal{M}_\pi(m,2)$. Значит, $u_s u_t = c_\delta u_\delta$, где согласно теореме Люка $c_\delta = \binom{t}{\delta} = \binom{2\pi^i}{\pi^i} \equiv_p \binom{2}{1} = 2$.

Теперь докажем второе утверждение. Снова рассмотрим δ такое, что $u_\delta \in \mathcal{M}_\pi(m,1)$. Пусть сначала $\delta = 1$. Тогда для $s = q-1-\pi$, $t = 1+\pi$ имеем $u_s \in \mathfrak{R}_S$, $u_t \in \mathcal{M}_\pi(m,2)$. Значит,

$u_s u_t = c_\delta u_\delta$, где $c_\delta = -\binom{t}{\delta} = -\binom{1+\pi}{1} = -(1+\pi) \equiv_2 1$. Пусть теперь $\delta = \pi^i$, $i \in \overline{1, m-1}$. Тогда положим $s = q-2$, $t = \delta + 1$. Значит, $u_s u_t = c_\delta u_\delta$, где $c_\delta = -\binom{t}{\delta} = -\binom{\delta+1}{1} = -(\delta+1) \equiv_2 1$.

Докажем третье утверждение. Согласно определению имеем $\mathcal{M}_\pi(m,2) = \mathcal{M}_\pi(m,1) + Qu_2$. Таким образом, достаточно показать, что $\mathfrak{R}_S(Qu_2) \subseteq \mathcal{M}_\pi(m,0)$. Данное включение следует из равенств $u_{q-3}u_2 = u_0$ и $u_{q-2}u_2 = 2 \cdot u_1 = 0$. □

На примере предыдущего утверждения видно, что случай $\lambda = l$ потребует отдельного рассмотрения. Докажем теперь обращение теоремы 3.1.

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* (3), (4), (5), *тогда выполнено равенство* (6).

Доказательство. Для каждого $\alpha \in \overline{1, l(p-1)-1}$ существует и притом единственное $k \in \overline{1, m(\pi-1)-2}$ такое, что имеют место соотношения (3), (4), (5). В самом деле, согласно утверждениям 2.1 и 3.2 множество чисел k, удовлетворяющих условиям (3) и (4) при фиксированном α, непусто. Выбрав в указанном множестве максимальный элемент, получим k такое, что имеют место соотношения (3), (4), (5).

Как показано далее, количество $k \in \overline{0, m(\pi-1)-1}$, для которых выполнено равенство (6), равно количеству различных ненулевых степеней $\mathfrak{R}_S$. Откинув граничные случаи $k = 0$ и $k = m(\pi-1)-1$, получаем, что для каждого из оставшихся k по теореме 3.1 имеют место соотношения (3), (4), (5). Поскольку количество равенств совпадает с количеством степеней радикала, и k определяется однозначно для данного α, заключаем, что выполнено обращение теоремы 3.1. Теорема доказана. □

Теорема 3.3. *Пусть $\lambda \neq l$, тогда количество $k \in \overline{0, m(\pi-1)-1}$ таких, что выполнено равенство* (6), *равно $l(p-1)$.*

Доказательство. Доказательство проведём полной индукцией по l. Докажем шаг индукции. Пусть для всех чисел меньших l теорема верна, и пусть λ — делитель l такой, что $\lambda \neq l$.

Рассмотрим произвольный элемент $u \in \mathfrak{R}_S\mathcal{M}_\pi(m, k+1)$. Тогда

$$u = \sum_{u_t \in \mathcal{M}_\pi(m,k+1)} \left(\sum_{u_s \in \mathfrak{R}_S} \alpha_s u_s \right) \alpha_t u_t = \sum_{\substack{u_t \in \mathcal{M}_\pi(m,k+1) \\ u_s \in \mathfrak{R}_S}} \alpha_{s,t} u_s u_t,$$

где $\alpha_s, \alpha_t, \alpha_{s,t} \in Q$. По утверждению 1.2 элементы $u_t \in \mathcal{M}_\pi(m,k)$ образуют базис $\mathcal{M}_\pi(m,k)$. В силу лемм 1.1 и 3.1 каждое ненулевое произведение $u_s u_t$ имеет вид $c_\delta u_\delta$, где $u_\delta \in \mathcal{M}_\pi(m,k)$. Указанные элементы u_δ образуют базис $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1)$, поскольку они являются элементами базиса $\mathcal{M}_\pi(m,k)$ и $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1) \subseteq \mathcal{M}_\pi(m,k)$. Следовательно, доказаны

Лемма 3.3. *Пусть $u_\delta \in \mathfrak{R}_S\mathcal{M}_\pi(m,k+1)$, тогда существуют $u_s \in \mathfrak{R}_S$, $u_t \in \mathcal{M}_\pi(m,k)$ такие, что $u_s u_t = c_\delta u_\delta$, где $c_\delta \in {\mathbb{F}_p}^*$.*

Лемма 3.4. *Включение $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1) \subset \mathcal{M}_\pi(m,k)$ равносильно тому, что существует $u_{t'} \in \mathcal{M}_\pi(m,k)$ такой, что для любых $u_t \in \mathcal{M}_\pi(m,k+1)$, $u_s \in \mathfrak{R}_S$ имеем $u_{t'} \notin (Qu_s u_t)$.*

Пусть $u_{t'} \in \mathcal{M}_\pi(m,k)$. Пусть i-я p-координата в 0-слое t' не равна $(p-1)$, где $i \in \overline{0,m-1}$. Положим $t = t' + \pi^i$. Заметим, что при данном сложении нет переноса разрядов в p-записи. По условию имеем $\omega_\pi(t') \leqslant k$, откуда $\omega_\pi(t) = \omega_\pi(t') + 1 \leqslant k+1$ и $u_t \in \mathcal{M}_\pi(m,k+1)$. Положим $s = q - 1 - \pi^i$, тогда $s \leqslant q-2$ и $u_s \in \mathfrak{R}_S$. Отсюда вытекает, что $u_s u_t = c u_{t'}$, $c = \pm\binom{t}{t'}$. По построению каждая p-координата t' не превосходит соответствующей p-координаты t. По теореме Люка заключаем, что $c \not\equiv_p 0$. Значит, на роль t' в предыдущей лемме подходят только числа, в 0-слое которых все p-координаты равны $(p-1)$.

Определение 3.1. Числа $t' \in \overline{0,q-1}$, в 0-слое которых все p-координаты равны $(p-1)$, и соответствующие им элементы $u_{t'}$ назовём особыми.

Из вышесказанного вытекает

Лемма 3.5. *Включение $\mathfrak{R}_S \mathcal{M}_\pi(m,k+1) \subset \mathcal{M}_\pi(m,k)$ равносильно тому, что существует особый элемент $u_{t'} \in \mathcal{M}_\pi(m,k)$ такой, что для любых $u_t \in \mathcal{M}_\pi(m,k+1)$, $u_s \in \mathfrak{R}_S$ имеем $u_{t'} \notin (Q u_s u_t)$.*

Рассмотрим наименьшее особое число t'_0. Все p-координаты в его 0-слое равны $(p-1)$, а остальные p-координаты равны 0. Очевидно, что $\omega_p(t'_0) = \omega_\pi(t'_0) = m(p-1)$. Отсюда следует, что для всех $k \in \overline{0, m(p-1)-1}$ в $\mathcal{M}_\pi(m,k)$ нет особых элементов, т.е. доказано

Утверждение 3.5. *Пусть $k \in \overline{0, m(p-1)-1}$, тогда выполнено равенство* (6).

С помощью предыдущего утверждения находим $m(p-1)$ требуемых значений k. Осталось найти ещё $l(p-1) - m(p-1) = \lambda m(p-1) - m(p-1) = m(\lambda-1)(p-1)$ значений.

Определение 3.2. Будем обозначать $x \preceq_p y$, если каждая p-координата x не превосходит соответствующей p-координаты y. Будем обозначать $x \prec_p y$, если $x \preceq_p y$ и $x \neq y$.

Заметим, что особый $u_{t'}$ может быть получен с помощью умножения на элемент $\mathfrak{R}_S$ только из особого u_t такого, что $t' \prec_p t$. В самом деле, пусть t' — произвольное особое число и $u_s u_t = c u_{t'}$, где $u_s \in \mathfrak{R}_S$, $c = \pm\binom{t}{t'}$. Согласно теореме Люка соотношение $c \not\equiv_p 0$ имеет место только при условии, что каждая p-координата t не меньше соответствующей p-координаты t', т.е. $t' \preceq_p t$. Ясно, что тогда t — тоже особое число. Из леммы 1.1 вытекает, что $t' < t$, откуда $t' \prec_p t$. Таким образом, доказано

Утверждение 3.6. *Равенство* (6) *равносильно тому, что для любого особого t' такого, что $\omega_\pi(t') \leqslant k$, существует особое число t такое, что $\omega_\pi(t) \leqslant k+1$ и $t' \prec_p t$.*

Рассмотрим произвольное особое число t и применим к нему следующее преобразование: исключим из p-записи t все p-координаты, принадлежащие 0-слою. Обозначим указанное преобразование σ. Образом σ являются всевозможные числа с p-записью длины $\tilde{l} = l - m = m(\lambda-1)$. Несложно понять, что σ биективно, и λ-группы t находятся во взаимно-однозначном соответствии с $(\lambda-1)$-группами $\sigma(t)$. Положим $\tilde{\lambda} = \lambda - 1$, тогда $\tilde{l} = m\tilde{\lambda}$ и $\tilde{\pi} = p^{\tilde{\lambda}} = p^{\lambda-1}$. Легко видеть, что $\omega_p(t) = \omega_p(\sigma(t)) + m(p-1)$ и $\omega_\pi(t) = \omega_{\tilde{\pi}}(\sigma(t))p + m(p-1)$.

По предположению индукции для $\tilde{l}$ и любого его делителя, отличного от $\tilde{l}$, существует $\tilde{l}(p-1)$ чисел $\tilde{k} \in \overline{0, m(\tilde{\pi}-1)-1}$ таких, что выполнено равенство

$$\mathfrak{R}_{\tilde{S}} \mathcal{M}_{\tilde{\pi}}(m, \tilde{k}+1) = \mathcal{M}_{\tilde{\pi}}(m, \tilde{k}). \tag{7}$$

По условию имеем $\lambda \neq l$, откуда следует, что $m \neq 1$, значит $\tilde{l} = m\tilde{\lambda} \neq \tilde{\lambda}$. Таким образом, предположение индукции можно применить к $\tilde{l}$, выбрав в качестве делителя $\tilde{\lambda}$.

Утверждение 3.7. *Пусть p — простое число, l — натуральное число, λ — делитель l такой, что $\lambda \geqslant 2$. Положим $\tilde{\lambda} = \lambda - 1$, $\tilde{\pi} = p^{\tilde{\lambda}}$, $\tilde{l} = m\tilde{\lambda}$, $m = l/\lambda$. Аналогично S определим $\tilde{S} = \tilde{Q}\tilde{H}$. Радикал $\tilde{S}$ обозначим $\mathfrak{R}_{\tilde{S}}$. Пусть для некоторого $\tilde{k} \in \overline{0, m(\tilde{\pi}-1)-1}$ выполнено равенство (7), тогда при $k+1 = (\tilde{k}+1)p + m(p-1)$ выполнено равенство (6).*

Замечание 3.1. Некоторая избыточность при формулировке этого утверждения связана с его универсальностью, т.к. мы не налагаем никаких условий на λ, лишь бы только $\tilde{\lambda}$ было положительным.

Замечание 3.2. Данное утверждение позволяет поднимать значения $\tilde{k} \in \overline{0, m(\tilde{\pi}-1)-1}$ до значений $k \in \overline{0, m(\pi-1)-1}$ с сохранением равенства (6).

Доказательство. Проверим, что соблюдены верхние границы для k. В самом деле, имеем

$$k = (\tilde{k}+1)p + m(p-1) - 1 \leqslant m(\tilde{\pi}-1)p + m(p-1) - 1 = m\pi - mp + mp - m - 1 = m(\pi-1) - 1.$$

Покажем, что для указанного k выполнены условия утверждения 3.6. Рассмотрим особое число t' такое, что $\omega_\pi(t') \leqslant k$, и соответствующее ему $\sigma(t')$. Заметим, что

$$\omega_{\tilde{\pi}}(\sigma(t')) = (\omega_\pi(t') - m(p-1))/p \leqslant (k - m(p-1))/p = \tilde{k} + (p-1)/p < \tilde{k} + 1,$$

т.е. $u_{\sigma(t')} \in \mathcal{M}_{\tilde{\pi}}(m, \tilde{k})$. По условию выполнено равенство (7). Значит, для $\sigma(t')$ существует число $\tilde{t}$ такое, что $\omega_{\tilde{\pi}}(\tilde{t}) \leqslant \tilde{k}+1$ и $u_{\tilde{s}} u_{\tilde{t}} = \tilde{c} u_{\sigma(t')}$, где $u_{\tilde{s}} \in \mathfrak{R}_{\tilde{S}}$, $\tilde{c} = \pm\binom{\tilde{t}}{\sigma(t')} \neq 0$. Поскольку отображение σ биективно, имеем $\tilde{t} = \sigma(t)$ для некоторого t. Легко видеть, что

$$\omega_\pi(t) = \omega_{\tilde{\pi}}(\sigma(t))p + m(p-1) \leqslant (\tilde{k}+1)p + m(p-1) = k+1,$$

т.е. $u_t \in \mathcal{M}_\pi(m, k+1)$. По теореме Люка имеем $\sigma(t') \prec_p \sigma(t)$, откуда следует, что $t' \prec_p t$. Таким образом, в силу утверждения 3.6 заключаем, что выполнено равенство (6). □

Вернёмся к доказательству теоремы 3.3. С помощью предыдущего утверждения находим $\tilde{l}(p-1) = m\tilde{\lambda}(p-1) = m(\lambda-1)(p-1)$ недостающих значений k. Шаг индукции доказан.

Осталось проверить базу индукции. Шаг индукции позволяет сводить случай (p, l, λ) к случаю $(p, l-m, \lambda-1)$, причём $\lambda - 1 = \tilde{\lambda} \neq m\tilde{\lambda} = \tilde{l} = l - m$ при $\lambda \neq l$. Значит, достаточно рассмотреть только случай $(p, l, 1)$, т.е. случай простого подполя, когда базисные коды совпадают со степенями радикала. Легко видеть, что в этом случае равенство (6) выполнено

при всех $k \in \overline{0, l(p-1)-1}$. Таким образом, получены $l(p-1)$ необходимых значений k, что завершает доказательство теоремы. □

Докажем теперь аналог теоремы 3.3 для случая $\lambda = l$.

Теорема 3.4. *Пусть $\lambda = l$, тогда количество $k \in \overline{0, m(\pi-1)-1}$ таких, что выполнено равенство (6), равно $l(p-1)$.*

Доказательство. Доказательство проведём полной индукцией по l. Шаг индукции доказывается точно так же, как в предыдущей теореме.

Осталось проверить базу индукции. Шаг индукции позволяет сводить случай (p, l, λ) к случаю $(p, l-m, \lambda-1)$, причём $\lambda - 1 = \tilde{\lambda} = m\tilde{\lambda} = \tilde{l} = l - m$ при $\lambda = l$. Значит, достаточно рассмотреть только случай $(p, 1, 1)$, т.е. случай простого подполя, когда базисные коды совпадают со степенями радикала. Легко видеть, что при этом $\mathrm{Tr} = \mathrm{Id}$ — тождественное отображение, и равенство (6) выполнено при всех $k \in \overline{0, (p-1)-1}$. Таким образом, получены $(p-1)$ необходимых значений k в случае $(p, 1, 1)$, что завершает доказательство. □

Утверждение 3.8. *Пусть $\lambda = l = 2$, $i \in \overline{0, p-1}$, тогда выполнено равенство*

$$\mathfrak{R}_S \mathcal{M}_\pi(1, (p-1) + ip) = \mathcal{M}_\pi(1, (p-1) + ip - 1).$$

Доказательство. Доказательство проведём индукцией по i. Проверим базу индукции. Требуемое равенство при $i = 0$ является частным случаем утверждения 3.5 при $k = p - 2$.

Теперь докажем шаг индукции. Пусть при $j = i - 1$ выполнено равенство

$$\mathfrak{R}_S \mathcal{M}_\pi(1, (p-1) + jp) = \mathcal{M}_\pi(1, (p-1) + jp - 1).$$

Покажем, что оно выполнено при $j = i$. Рассмотрим $t = (p-1) + (i-1)p$. Легко видеть, что $\omega_\pi(t) = t$ и $u_t \in \mathcal{M}_\pi(1, (p-1) + (i-1)p)$. Ясно, что t — наименьшее особое число такое, что $u_t \notin \mathcal{M}_\pi(1, (p-1) + (i-1)p - 1)$. Заметим, что $u_t \in \mathcal{M}_\pi(1, (p-1) + ip - 1)$, поскольку $\omega_\pi(t) = (p-1) + (i-1)p < (p-1) + ip - 1$. Положим $t' = t + p = (p-1) + ip$. Тогда $\omega_\pi(t') = t'$, $u_{t'} \in \mathcal{M}_\pi(1, (p-1)+ip)$ и t' — наименьшее особое число такое, что $t \prec_p t'$. Пользуясь предположением индукции, получаем, что при $j = i$ выполнены условия утверждения 3.6, что завершает доказательство. □

Замечание 3.3. С помощью предыдущего утверждения находим p значений k таких, что выполнено равенство (6), из утверждения 3.5 находим ещё $(p-1)$ таких значений k, но эти два набора значений имеют единственный одинаковый элемент $k = p - 2$. Отсюда общее число различных значений k равно $p + (p-1) - 1 = 2(p-1)$. Значит, в теореме 3.4 можно свести доказательство базы индукции к случаю $(p, 2, 2)$.

Утверждение 3.9. *Пусть $\alpha \in \overline{1, l(p-1)-1}$ и $k \in \overline{1, m(\pi-1)-2}$. Соотношения (3), (4), (5) имеют место тогда и только тогда, когда k — максимальное среди чисел k', для которых $j = l(p-1) - \alpha$ является наименьшим таким, что $\Pi_{k'} \subset \mathrm{P}_j$.*

Доказательство. Рассмотрим множество чисел k', для которых $j = l(p-1) - \alpha$ является наименьшим таким, что $\Pi_{k'} \subset \mathrm{P}_j$. В силу утверждений 1.2 и 2.1 данное условие равносильно тому, что для k', α имеют место соотношения (3) и (4). Согласно утверждению 3.2 указанное множество непусто. Пусть k — максимальное среди k'. Легко видеть, что данное условие эквивалентно тому, что для k, α имеют место соотношения (3), (4), (5). □

Пусть $\psi : \mathbb{N} \to \mathbb{N}$ — операция поднятия из утверждения 3.7, т.е. $\psi(t) = (t+1)p + m(p-1) - 1$. Естественно положить $\psi^0 = \mathrm{Id}$.

Теорема 3.5. *Пусть* $\alpha \in \overline{1, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-2}$. *Соотношения* (3), (4), (5) *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* $0 \leqslant \tau < m(p-1)$.

Доказательство. Согласно теоремам 3.1 и 3.2 соотношения (3), (4), (5) имеют место тогда и только тогда, когда выполнено равенство (6). Из доказательств теорем 3.3 и 3.4 следует, что значения k, для которых выполнено равенство (6), получаются двумя способами: часть значений, которые мы назовём нижними, получается из утверждения 3.5; другая часть значений, которые мы назовём верхними, получается из утверждения 3.7. Ясно, что любое нижнее значение меньше любого верхнего.

Очевидно, что ψ строго возрастает. Значит, первые $m(p-1)$ верхних значений k в случае (p, l, λ) получены поднятием нижних значений в случае $(p, l-m, \lambda-1)$, следующие $m(p-1)$ верхних значений в случае (p, l, λ) получены поднятием первых $m(p-1)$ верхних значений в случае $(p, l-m, \lambda-1)$, которые, в свою очередь, получены поднятием нижних значений в случае $(p, l-2m, \lambda-2)$. Повторяя аналогичные рассуждения, заключаем, что θ-я группа из $m(p-1)$ верхних значений в случае (p, l, λ) получена θ-кратным поднятием нижних значений в случае $(p, l-\theta m, \lambda-\theta)$. Поскольку ψ строго возрастает, τ-е нижнее значение в случае $(p, l-\theta m, \lambda-\theta)$ перейдёт в τ-е верхнее значение внутри θ-й группы из $m(p-1)$ верхних значений в случае (p, l, λ), где $\tau \in \overline{0, m(p-1)-1}$. Таким образом, j-е значение k получено θ-кратным поднятием τ-го нижнего значения в случае $(p, l-\theta m, \lambda-\theta)$, где θ и τ — частное и остаток от деления j на $m(p-1)$. Теорема доказана. □

3.2 Включения вида $\mathcal{M}_\pi(m,k) \supset {\mathfrak{R}_S}^\alpha$

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:

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

$$\mathfrak{R}_S{}^{\alpha} \nsubseteq \mathcal{M}_{\pi}(m,k-1), \tag{9}$$

$$\mathfrak{R}_S{}^{\alpha-1} \nsubseteq \mathcal{M}_{\pi}(m,k). \tag{10}$$

Лемма 3.6. *Пусть* $j \in \overline{0, l(p-1)-1}$. *Пусть* t *определено согласно* (2). *Тогда младшая* p*-координата* t *не превосходит* $(p-2)$.

Доказательство. Предположим, что младшая p-координата t равна $(p-1)$. По построению t отсюда вытекает, что все p-координаты t равны $(p-1)$. Таким образом, имеем $\omega_p(t) = l(p-1)$. Согласно следствию 2.1 получаем $j = l(p-1)$, что противоречит условию. Лемма доказана. □

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* (8), (9), (10).

Доказательство. Рассмотрим множество чисел k' таких, что для $j = l(p-1)-\alpha$ имеет место включение $\mathrm{P}_j \subset \Pi_{k'}$. В силу утверждений 1.2 и 2.1 данное условие равносильно тому, что для k', α имеет место соотношение (8). Согласно утверждению 3.1 указанное множество непусто. Пусть k — минимальное среди k'. Легко видеть, что данное условие эквивалентно тому, что для k, α имеют место соотношения (8) и (9).

Покажем, что если k — минимальное среди указанных k', то для k, α имеет место соотношение (10). В самом деле, согласно лемме 2.3 существует число t такое, что $\omega_p(t) = j$ и $\omega_\pi(t) = k$. Положим $t' = t + 1$. В силу леммы 3.6 получаем $\omega_p(t') = j + 1$ и $\omega_\pi(t') = k + 1$. Отсюда заключаем, что $\mathrm{P}_{j+1} \nsubseteq \Pi_k$. Таким образом, имеет место соотношение (10). □

Теорема 3.6. *Пусть* $\alpha \in \overline{2, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-1}$. *Соотношения* (8), (9), (10) *имеют место тогда и только тогда, когда выполнено равенство*

$$k = \sum_{i=0}^{\theta-1} m(p-1)p^{\lambda-1-i} + \tau p^{\lambda-\theta-1}, \tag{11}$$

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* $0 \leqslant \tau < m(p-1)$.

Доказательство. По предыдущему утверждению соотношения (8), (9), (10) имеют место тогда и только тогда, когда k является минимальным таким, что для $j = l(p-1) - \alpha$ имеет место включение $\mathrm{P}_j \subset \Pi_k$. Согласно лемме 2.3 данное k можно вычислить по формуле (11). Теорема доказана. □

Подводя итог раздела 3, отметим, что полученные результаты дают необходимые и достаточные условия, при которых две вершины, соответствующие идеалам $\mathcal{M}_\pi(m,k)$ и $\mathcal{M}_p(l,j)$,

соединены дугой в графе включений. Случай $\mathcal{M}_p(l,j) \supset \mathcal{M}_\pi(m,k)$ описывается с помощью теорем 3.1 и 3.2 и утверждения 3.9. Случай $\mathcal{M}_\pi(m,k) \supset \mathcal{M}_p(l,j)$ описывается с помощью утверждения 3.10. Теоремы 3.5 и 3.6 дают числовое описание указанных включений.

4 Совпадения идеалов $\mathfrak{R}_S\mathcal{M}_\pi(m,k)$

Цель данного раздела — исследовать совпадения идеалов $\mathfrak{R}_S\mathcal{M}_\pi(m,k)$ между собой.

Лемма 4.1. *Пусть $\lambda \neq l$. Тогда для всех $k \in \overline{0, m(\pi-1)-1}$ существует u_t такой, что $u_t \in \mathfrak{R}_S\mathcal{M}_\pi(m,k+1)$ и $\omega_\pi(t) = k$.*

Доказательство. Если выполнено равенство $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1) = \mathcal{M}_\pi(m,k)$, то утверждение очевидно. Рассмотрим случай $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1) \subset \mathcal{M}_\pi(m,k)$, и пусть $u_t \in \mathcal{M}_\pi(m,k)$ такой, что $\omega_\pi(t) = k$.

Пусть t — не особое число, тогда i-я p-координата в 0-слое t отлична от $(p-1)$, где $i \in \overline{0, m-1}$. Положим $t' = t + \pi^i$, тогда $\omega_\pi(t') = k+1$ и $u_{t'} \in \mathcal{M}_\pi(m,k+1)$. Положим $s = q-1-\pi^i$, тогда $s \leqslant q-2$ и $u_s \in \mathfrak{R}_S$. Отсюда следует, что $u_s u_{t'} = cu_t$, и по теореме Люка имеем $c = \pm\binom{t'}{t} \not\equiv_p 0$. Таким образом, получаем $u_t \in \mathfrak{R}_S\mathcal{M}_\pi(m,k+1)$.

Предположим, что все числа t такие, что $\omega_\pi(t) = k$, являются особыми. Покажем, что это невозможно. Рассмотрим произвольное особое число t такое, что $\omega_\pi(t) = k$. Поскольку $\lambda \neq l$, имеем $m = l/\lambda \geqslant 2$. Значит, количество λ-групп t не меньше 2. Согласно условию $k \leqslant m(\pi-1)-1$ заключаем, что в некоторой λ-группе t есть p-координата меньше $(p-1)$. Рассмотрим данную λ-группу и любую из $(m-1)$ оставшихся:

$$(\underbrace{*,\ldots,*,p-1}_{\lambda})(\underbrace{*,\ldots,*,\alpha,\overbrace{p-1,\ldots,p-1}^{s}}_{\lambda}),$$

где $s \in \overline{1, \lambda-1}$ и α — самая младшая из p-координат указанной λ-группы, отличных от $(p-1)$.

Согласно равенству

$$(p-1) + \alpha p^s + (p-1)p^{s-1} + \cdots + (p-1)p + (p-1) = (p-2) + (\alpha+1)p^s + 0,$$

можно изменить элементы в указанных λ-группах следующим образом:

$$(\underbrace{*,\ldots,*,p-2}_{\lambda})(\underbrace{*,\ldots,*,\alpha+1,\overbrace{0,\ldots,0}^{s}}_{\lambda}).$$

Обозначим полученное число t'. Легко видеть, что $\omega_\pi(t') = \omega_\pi(t) = k$ и t' — не особое, что приводит к противоречию. Лемма доказана. □

Утверждение 4.1. *Пусть $\lambda \neq l$. Тогда для всех $k \in \overline{0, m(\pi-1)}$ идеалы $\mathfrak{R}_S\mathcal{M}_\pi(m,k)$ попарно различны.*

Доказательство. Легко видеть, что для всех $k \in \overline{1, m(\pi-1)}$ данное утверждение следует из лемм 3.1 и 4.1. При $k = 0$ получаем $\mathfrak{R}_S\mathcal{M}_\pi(m,0) = \{0\}$, что завершает доказательство. □

Рассмотрим теперь случай $\lambda = l$.

Лемма 4.2. *Пусть $\lambda = l$. Тогда для $k \in \overline{0, m(\pi-1)-1}$ существует u_t такой, что $u_t \in \mathfrak{R}_S\mathcal{M}_\pi(m, k+1)$ и $\omega_\pi(t) = k$, тогда и только тогда, когда $k \not\equiv_p p-1$.*

Доказательство. Пусть $u_t \in \mathcal{M}_\pi(m,k)$ такой, что $\omega_\pi(t) = k$. Поскольку $\lambda = l$, то $m = 1$. Отсюда вытекает, что p-запись t состоит из единственной λ-группы и $\omega_\pi(t) = t = k$.

Пусть $k \not\equiv_p p-1$, тогда t — не особое число. Положим $t' = t+1$, тогда $\omega_\pi(t') = t' = k+1$ и $u_{t'} \in \mathcal{M}_\pi(m, k+1)$. Отсюда следует, что $u_{q-2}u_{t'} = cu_t$, и по теореме Люка имеем $c = \pm\binom{t'}{t} \not\equiv_p 0$. Таким образом, $u_t \in \mathfrak{R}_S\mathcal{M}_\pi(m, k+1)$.

Наоборот, пусть существует элемент $u_t \in \mathfrak{R}_S\mathcal{M}_\pi(m, k+1)$ такой, что $\omega_\pi(t) = k$. Согласно лемме 3.3 существуют $u_s \in \mathfrak{R}_S$, $u_{t'} \in \mathcal{M}_\pi(m, k+1)$ такие, что $u_s u_{t'} = cu_t$, где $c \neq 0$. Отсюда по теореме Люка следует, что $t \prec_p t'$. Ясно, что $t' = t+1$. Предположим, что $k \equiv_p p-1$. Тогда $t' = t+1 = \omega_\pi(t)+1 = k+1 \equiv_p 0$. Отсюда вытекает, что младшая p-координата t' равна 0, а младшая p-координата t равна $(p-1)$, что противоречит условию $t \prec_p t'$. Значит, имеем $k \not\equiv_p p-1$, что завершает доказательство. □

Лемма 4.3. *В условиях предыдущей леммы равенство $\mathfrak{R}_S\mathcal{M}_\pi(m, k+1) = \mathfrak{R}_S\mathcal{M}_\pi(m,k)$ выполнено тогда и только тогда, когда $k \equiv_p p-1$.*

Доказательство. Согласно предыдущей лемме достаточно показать, что при $k \equiv_p p-1$ произведения вида $u_s u_{k+1}$, где $u_s \in \mathfrak{R}_S$, принадлежат $\mathfrak{R}_S\mathcal{M}_\pi(m,k)$. Пусть $u_s u_{k+1} = cu_\delta$, $c = \pm\binom{k+1}{\delta} \not\equiv_p 0$. По теореме Люка имеем $\delta \prec_p k+1$. Поскольку $k+1 \equiv_p 0$, получаем $k+1-\delta \geqslant p$. Положим $t = \delta+1$. Тогда $\omega_\pi(t) = \delta+1 \leqslant k+2-p \leqslant k$ и $u_t \in \mathcal{M}_\pi(m,k)$. Легко видеть, что $u_{q-2}u_t = cu_\delta$, $c = \pm 1$. Отсюда следует, что $u_s u_{k+1} \in \mathfrak{R}_S\mathcal{M}_\pi(m,k)$. Лемма доказана. □

Утверждение 4.2. *Пусть $\lambda = l$. Пусть $i, j \in \overline{0, m(\pi-1)}$ и $i < j$. Равенство $\mathfrak{R}_S\mathcal{M}_\pi(m,i) = \mathfrak{R}_S\mathcal{M}_\pi(m,j)$ выполнено тогда и только тогда, когда $j = i+1$ и $i \equiv_p p-1$.*

Доказательство. Непосредственно вытекает из лемм 3.1, 4.2, 4.3. □

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 $i = j+1$. В самом деле, в силу леммы 4.1 существует u_t такой, что $u_t \in \mathfrak{R}_S\mathcal{M}_\pi(m, j+2)$ и $u_t \in \mathcal{M}_\pi(m, j+1)\backslash\mathcal{M}_\pi(m,j)$, т.е. $i \leqslant j+1$. По лемме 3.1 имеем $\mathfrak{R}_S\mathcal{M}_\pi(m,j) \subseteq \mathcal{M}_\pi(m, j-1)$, т.е. $i \geqslant j+1$. Отсюда заключаем, что $i = j+1$.

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 самом деле, при $j+1 \not\equiv_p p-1$ в силу леммы 4.2, рассуждая тем же образом, что и в случае $\lambda \neq l$, получаем $i = j+1$. Если $j+1 \equiv_p p-1$, тогда $j+2 \not\equiv_p p-1$. По лемме 4.2 существует u_t такой, что $u_t \in \mathfrak{R}_S\mathcal{M}_\pi(m, j+3)$ и $u_t \in \mathcal{M}_\pi(m, j+2)\backslash\mathcal{M}_\pi(m, j+1)$, т.е. $i \leqslant j+2$. По лемме 3.1 имеем $\mathfrak{R}_S\mathcal{M}_\pi(m,j) \subseteq \mathcal{M}_\pi(m, j-1)$, т.е. $i \geqslant j+1$. Согласно лемме 4.3 получаем $\mathfrak{R}_S\mathcal{M}_\pi(m, j+2) = \mathfrak{R}_S\mathcal{M}_\pi(m, j+1)$. Отсюда заключаем, что $i = j+1$ или $i = j+2$.

5 Базисы кодов Рида–Маллера

Напомним, что коды Рида–Маллера являются идеалами $\mathcal{RM}_\pi(m,k)$, где $\mathcal{RM}_\pi(m,k) = \mathrm{Tr}(\mathcal{M}_\pi(m,k))$, а идеалы $\mathcal{M}_\pi(m,k)$ порождены базисом из элементов u_i. Цель данного раздела — построить специальные базисы кодов Рида–Маллера, которые тесно связаны с базисами соответствующих базисных кодов Рида–Маллера. Это позволит в дальнейшем переносить результаты для идеалов $\mathcal{M}_\pi(m,k)$ на случай идеалов $\mathcal{RM}_\pi(m,k)$.

5.1 Элементы $\mathrm{Tr}(u_i)$

Начнём с подробного исследования элементов $\mathrm{Tr}(u_i)$.

Определение 5.1. Пусть $S_\pi : \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0}$ — циклический сдвиг π-записи числа t на одну позицию влево: если $[t]_\pi = [t_n, t_{n-1}, \ldots, t_1, t_0]$, тогда $S_\pi(t) = \tilde{t}$, где $\left[\tilde{t}\right]_\pi = [t_{n-1}, \ldots, t_1, t_0, t_n]$.

Лемма 5.1. *Пусть $s, t \in \overline{1, q-1}$. Тогда следующие условия эквивалентны:*

$$s \equiv t\pi \bmod (q-1),$$
$$s = S_\pi(t).$$

Доказательство. Пусть $[t]_\pi = [t_{m-1}, t_{m-2}, \ldots, t_1, t_0]$. Тогда

$$[t\pi]_\pi = [\underbrace{t_{m-1}, t_{m-2}, \ldots, t_1, t_0, 0}_{m+1}].$$

Положим $\tilde{t} = t\pi - t_{m-1}(q-1)$. Тогда

$$\tilde{t} = t\pi - t_{m-1}(\pi^m - 1) = t\pi - t_{m-1}\pi^m + t_{m-1}.$$

Отсюда получаем $\left[\tilde{t}\right]_\pi = [t_{m-2}, \ldots, t_1, t_0, t_{m-1}]$. Легко видеть, что $\tilde{t} = S_\pi(t)$. Пусть $s = S_\pi(t)$. Тогда $s = \tilde{t} = t\pi - t_{m-1}(q-1) \equiv t\pi \bmod (q-1)$.

Пусть $s \equiv t\pi \bmod (q-1)$. Тогда $s \equiv t\pi - t_{m-1}(q-1) \bmod (q-1)$, т.е. $s \equiv \tilde{t} \bmod (q-1)$. По условию имеем $s \in \overline{1, q-1}$, по построению $\tilde{t}$ имеем $\tilde{t} \in \overline{1, q-1}$. Таким образом, из соотношения $s \equiv \tilde{t} \bmod (q-1)$ вытекает, что $s = \tilde{t}$. Лемма доказана. □

Замечание 5.1. Пусть $t \in \overline{0, q-1}$. Несложно понять, что ${S_\pi}^m(t) = t$.

Далее будем рассматривать только ограничение S_π на $\{0, 1, \ldots, q-1\}$, которое также обозначим S_π. Естественно положить ${S_\pi}^0 = \mathrm{Id}$. Ясно, что $\{{S_\pi}^1, \ldots, {S_\pi}^{m-1}, {S_\pi}^m\}$ является циклической группой порядка m относительно операции композиции. Обозначим указанную группу $\langle S_\pi \rangle_m$.

Лемма 5.2. *Пусть $s, t \in \overline{1, q-1}$ и $k \in \overline{0, m}$. Тогда следующие условия эквивалентны:*

$$s \equiv t\pi^k \bmod (q-1),$$
$$s = {S_\pi}^k(t).$$

Доказательство. Пусть $[t]_\pi = [t_{m-1}, t_{m-2}, \ldots, t_1, t_0]$. Тогда

$$\left[t\pi^k\right]_\pi = [\underbrace{t_{m-1}, t_{m-2}, \ldots, t_1, t_0}_{m}, \underbrace{0, \ldots, 0}_{k}].$$

Положим $\tilde{t} = t\pi^k - t_{m-1}\pi^{k-1}(q-1) - t_{m-2}\pi^{k-2}(q-1) - \cdots - t_{m-k}(q-1)$. Легко видеть, что $\tilde{t} = {S_\pi}^k(t)$. Дальнейшие рассуждения повторяют доказательство леммы 5.1. □

Определение 5.2. Рассмотрим действие группы $\langle S_\pi \rangle_m$ на $\{0, 1, \ldots, q-1\}$. Напомним, что орбита числа t определена равенством

$$Orb(t) = \left\{ {S_\pi}^k(t) : k \in \overline{1, m} \right\},$$

а стабилизатор числа t определён равенством

$$St(t) = \left\{ {S_\pi}^k \in \langle S_\pi \rangle_m : {S_\pi}^k(t) = t \right\}.$$

Замечание 5.2. Отметим, что $|Orb(t)| \cdot |St(t)| = m$.

Лемма 5.3. *Пусть $t \in \overline{0, q-1}$ и $k \in \overline{0, m}$. Тогда $\omega_\pi(t) = \omega_\pi({S_\pi}^k(t))$ и $\omega_p(t) = \omega_p({S_\pi}^k(t))$.*

Доказательство. Непосредственно вытекает из определения S_π. □

Лемма 5.4. *Пусть $t \in \overline{0, q-1}$. Тогда π-запись t непериодическая тогда и только тогда, когда $|Orb(t)| = m$.*

Доказательство. По предыдущему замечанию условие $|Orb(t)| \neq m$ равносильно тому, что $|St(t)| > 1$. Последнее неравенство эквивалентно тому, что существует $k \in \overline{1, m-1}$ такое, что ${S_\pi}^k(t) = t$. Ясно, что $St(t)$ — подгруппа в $\langle S_\pi \rangle_m$. Отсюда следует, что $St(t)$ — циклическая группа, как подгруппа циклической группы. Без ограничения общности можно считать, что $St(t) = \langle {S_\pi}^k \rangle$. Это равносильно тому, что период π-записи t равен k.

В самом деле, если $St(t) = \langle {S_\pi}^k \rangle$, тогда для всех $k' \in \overline{1, k-1}$ имеем ${S_\pi}^{k'}(t) \neq t$. Пусть $[t]_\pi = [t_{m-1}, \ldots, t_1, t_0]$, тогда выполнены равенства

$$t_0 = t_k, t_1 = t_{k+1}, \ldots, t_{k-1} = t_{k+(k-1)},$$

т.е. период π-записи t равен k.

Наоборот, если период π-записи t равен k, тогда ${S_\pi}^k \in St(t)$, и для всех $k' \in \overline{1, k-1}$ имеем ${S_\pi}^{k'}(t) \neq t$, т.е. $St(t) = \langle {S_\pi}^k \rangle$. Лемма доказана. □

Лемма 5.5. *Пусть $t \in \overline{0, q-1}$. Тогда π-запись t периодическая с периодом $k \in \overline{1, m-1}$ тогда и только тогда, когда $|Orb(t)| = k$.*

Доказательство. Из доказательства предыдущей леммы вытекает, что период π-записи t равен k тогда и только тогда, когда $St(t) = \langle {S_\pi}^k \rangle$. Последнее равенство равносильно тому, что число различных левых смежных классов по $St(t)$ равно k. Поскольку элементы $Orb(t)$

находятся в биективном соответствии с левыми смежными классами по стабилизатору t, имеем $|Orb(t)| = k$, что завершает доказательство. □

Замечание 5.3. Присвоим непериодической π-записи t период m. Тогда период π-записи t всегда совпадает с $|Orb(t)|$.

Определение 5.3. Рассмотрим произвольный элемент $a \in S$:

$$a = \sum_{h \in H} a_h h,\ a_h \in Q.$$

Пусть $\pi_a : H \to Q$ — проекция на h-ю координату a, т.е. $\pi_a(h) = a_h$. Согласно определению имеем $\phi : (H, \cdot) \to (Q, +)$ — изоморфизм. Определим отображение $\mathcal{P}_a : Q \to Q$ равенством $\mathcal{P}_a = \pi_a \circ \phi^{-1}$, т.е. $\mathcal{P}_a(x) = \pi_a\left(\phi^{-1}(x)\right)$.

Следствие 5.1. *Пусть $a, b \in S$ и $\xi \in Q$. Тогда $\mathcal{P}_{a+b} = \mathcal{P}_a + \mathcal{P}_b$ и $\mathcal{P}_{\xi \cdot a} = \xi \cdot \mathcal{P}_a$.*

Доказательство. Непосредственно вытекает из определения $\mathcal{P}_a$. □

Следствие 5.2. *Пусть $a, b \in S$. Тогда $a = b$ тогда и только тогда, когда $\mathcal{P}_a = \mathcal{P}_b$.*

Доказательство. Условие $a = b$ равносильно тому, что $\pi_a = \pi_b$. Поскольку ϕ — изоморфизм, последнее равенство эквивалентно тому, что $\mathcal{P}_a = \mathcal{P}_b$. □

Множество функций, действующих из поля Q в себя, совпадает с множеством многочленов над Q от одной переменной, степень которых меньше q [10]. В частности, $\mathrm{tr} = \mathrm{tr}_P^Q$ — функция следа из поля Q в поле P, являющееся подполем Q, задаётся многочленом

$$\mathrm{tr}(x) = x + x^{\pi} + x^{\pi^2} + \cdots + x^{\pi^{m-1}}.$$

Лемма 5.6. *Пусть $a = u_i$, где $i \in \overline{0, q-1}$. Тогда $\mathcal{P}_a(x) = x^i$.*

Доказательство. По определению имеем

$$\mathcal{P}_a(x) = \mathcal{P}_{u_i}(x) = \pi_{u_i}\left(\phi^{-1}(x)\right) = \left(\phi\left(\phi^{-1}(x)\right)\right)^i = x^i.$$

□

Лемма 5.7. *Пусть $a = \mathrm{Tr}(u_i)$, где $i \in \overline{0, q-1}$. Тогда $\mathcal{P}_a(x) = \mathrm{tr}(x^i)$.*

Доказательство. По определению имеем

$$\mathcal{P}_a(x) = \mathcal{P}_{\mathrm{Tr}(u_i)}(x) = \pi_{\mathrm{Tr}(u_i)}\left(\phi^{-1}(x)\right) = \mathrm{tr}\left(\left(\phi\left(\phi^{-1}(x)\right)\right)^i\right) = \mathrm{tr}(x^i).$$

□

Лемма 5.8. *Пусть $i \in \overline{0, q-1}$, $k \in \overline{0, m}$. Тогда мономы $x^{i\pi^k}$ и $x^{S_\pi{}^k(i)}$ определяют одну и ту же функцию, действующую из поля Q в себя.*

Доказательство. Известно, что многочлены над Q, сравнимые по модулю двучлена $x^q - x$, определяют одну и ту же функцию, действующую из поля Q в себя [10]. В частности, это означает, что мономы $x^{q+\alpha}$ и $x^{1+\alpha}$ задают одну и ту же функцию при всех целых неотрицательных α. Заметим, что при этом $q + \alpha \equiv 1 + \alpha \bmod (q-1)$. Заменяя $x^{q+\alpha}$ на $x^{1+\alpha}$ в мономе $x^{i\pi^k}$, можно добиться того, что его степень станет меньше q. Если $i \neq 0$, тогда по лемме 5.2 заключаем, что моном $x^{i\pi^k}$ в результате указанных замен перейдёт в $x^{S_\pi{}^k(i)}$. Отметим, что в этом случае мономов нулевой степени ни до, ни после замен нет. Если $i = 0$, то легко видеть, что $x^{i\pi^k} = x^{S_\pi{}^k(i)} = x^0 = 1$. Лемма доказана. □

Лемма 5.9. *Пусть* $a = \mathrm{Tr}(u_i)$, *где* $i \in \overline{0, q-1}$. *Тогда* $\mathcal{P}_a(x) = \sum\limits_{k=1}^{m} x^{S_\pi{}^k(i)}$.

Доказательство. Отметим, что $x^{S_\pi{}^m(i)} = x^{S_\pi{}^0(i)} = x^i$. Применяя результаты предыдущей леммы к равенству

$$\mathcal{P}_a(x) = \mathrm{tr}(x^i) = x^i + x^{i\pi} + x^{i\pi^2} + \cdots + x^{i\pi^{m-1}},$$

получаем

$$\mathcal{P}_a(x) = x^{S_\pi{}^m(i)} + x^{S_\pi{}^1(i)} + x^{S_\pi{}^2(i)} + \cdots + x^{S_\pi{}^{m-1}(i)} = \sum_{k=1}^{m} x^{S_\pi{}^k(i)}.$$

□

Замечание 5.4. Далее, рассматривая $\mathcal{P}_{\mathrm{Tr}(u_i)}$ как многочлен, будем отождествлять мономы $x^{i\pi^k}$ и $x^{S_\pi{}^k(i)}$ и будем считать, что $\deg\left(\mathcal{P}_{\mathrm{Tr}(u_i)}\right) < q$.

Следствие 5.3. *Пусть* $a = \mathrm{Tr}(u_i)$, *где* $i \in \overline{0, q-1}$. *Тогда выполнено равенство*

$$\mathcal{P}_a(x) = |St(i)| \cdot \sum_{k \in Orb(i)} x^k.$$

Доказательство. Согласно предыдущей лемме множество различных степеней мономов, входящих в $\mathcal{P}_a$, совпадает с $Orb(i)$, а количество мономов одной степени равно $|St(i)|$. □

Следствие 5.4. *Пусть* $a = \mathrm{Tr}(u_i)$, *где* $i \in \overline{0, q-1}$. *Тогда* $a = 0$ *тогда и только тогда, когда* p *делит* $|St(i)|$.

Доказательство. По следствию 5.2 равенство $a = 0$ эквивалентно тому, что $\mathcal{P}_a \equiv 0$. В силу предыдущего следствия данное условие равносильно тому, что $|St(i)|$ кратно p. □

Утверждение 5.1. *Пусть* $a = \mathrm{Tr}(u_i)$, $b = \mathrm{Tr}(u_j)$, *где* $i, j \in \overline{0, q-1}$. *Условие* $a = b = 0$ *равносильно тому, что* $|St(i)|$ *и* $|St(j)|$ *делят* p. *Условие* $a = b \neq 0$ *равносильно тому, что* $|St(i)|$ *и* $|St(j)|$ *не делят* p, *и* $i = S_\pi{}^k(j)$, *где* $k \in \overline{1, m}$.

Доказательство. В силу предыдущего следствия достаточно рассмотреть только случай $a = b \neq 0$. Условие $a = b$ равносильно тому, что $\mathcal{P}_a = \mathcal{P}_b$. По следствию 5.3 множество различных степеней мономов, входящих в $\mathcal{P}_a$, совпадает с множеством $Orb(i)$, а множество различных степеней мономов, входящих в $\mathcal{P}_b$, совпадает с множеством $Orb(j)$. Отсюда вытекает, что условие $\mathcal{P}_a = \mathcal{P}_b$ эквивалентно тому, что $Orb(i) = Orb(j)$. Последнее равенство равносильно тому, что $i = S_\pi{}^k(j)$, где $k \in \overline{1, m}$. □

5.2 Элементы $\mathrm{Tr}(\xi u_i)$

Перейдём теперь к исследованию элементов $\mathrm{Tr}(\xi u_i)$, где $\xi \in Q$.

Определение 5.4. Пусть $j \mid i$. Обозначим через tr_j^i функцию следа из поля $\mathbb{F}_{\pi^i}$ в поле $\mathbb{F}_{\pi^j}$:

$$\mathrm{tr}_j^i(x) = x + x^{\pi^j} + x^{\pi^{2j}} + \cdots + x^{\pi^{i-j}}.$$

Замечание 5.5. В предыдущих обозначениях имеем $\mathrm{tr} = \mathrm{tr}_1^m$.

Напомним основные свойства функции tr_j^i.

Лемма 5.10 ([3])**.**

Выполнено равенство $\mathrm{tr}_j^i(x_1 + x_2) = \mathrm{tr}_j^i(x_1) + \mathrm{tr}_j^i(x_2)$.

При всех $\xi \in \mathbb{F}_{\pi^j}$ *выполнено равенство* $\mathrm{tr}_j^i(\xi \cdot x) = \xi \cdot \mathrm{tr}_j^i(x)$.

Выполнено равенство $\mathrm{tr}_j^i(x^{\pi^j}) = \mathrm{tr}_j^i(x)$.

При $j \mid k \mid i$ *выполнено равенство* $\mathrm{tr}_j^i = \mathrm{tr}_j^k \circ \mathrm{tr}_k^i$.

Дальнейшие результаты опираются на следующий известный факт.

Лемма 5.11 ([3])**.** *Для любых элементов x, y конечного поля характеристики p и любого натурального n выполнено равенство* $(x+y)^{p^n} = x^{p^n} + y^{p^n}$.

Лемма 5.12. *Пусть $\xi \in Q$. Пусть $a = \mathrm{Tr}(\xi u_i)$, где $i \in \overline{0, q-1}$. Тогда $\mathcal{P}_a(x) = \mathrm{tr}(\xi x^i)$.*

Доказательство. По определению имеем

$$\mathcal{P}_a(x) = \mathcal{P}_{\mathrm{Tr}(\xi u_i)}(x) = \pi_{\mathrm{Tr}(\xi u_i)}\left(\phi^{-1}(x)\right) = \mathrm{tr}\left(\xi\left(\phi\left(\phi^{-1}(x)\right)\right)^i\right) = \mathrm{tr}(\xi x^i).$$

□

Утверждение 5.2. *Пусть $\xi \in Q$. Пусть $a = \mathrm{Tr}(\xi u_i)$, где $i \in \overline{0, q-1}$. Пусть $|Orb(i)| = r$. Тогда выполнено равенство*

$$\mathcal{P}_a(x) = \mathrm{tr}_r^m(\xi) \cdot x^i + (\mathrm{tr}_r^m(\xi))^{\pi} \cdot x^{i\pi} + \cdots + (\mathrm{tr}_r^m(\xi))^{\pi^{r-1}} \cdot x^{i\pi^{r-1}}. \tag{12}$$

Доказательство. Из замечаний 5.2 и 5.3 следует, что r — период π-записи i и $r \mid m$. Пусть $k = m/r$, тогда по леммам 5.2, 5.4, 5.5 имеют место соотношения:

$$\begin{aligned} i = i\pi^0 \equiv i\pi^r \equiv i\pi^{2r} \equiv \ldots \equiv i\pi^{(k-1)r} \bmod (q-1),\\ i\pi^1 \equiv i\pi^{r+1} \equiv i\pi^{2r+1} \equiv \ldots \equiv i\pi^{(k-1)r+1} \bmod (q-1),\\ \vdots \\ i\pi^{r-1} \equiv i\pi^{r+(r-1)} \equiv i\pi^{2r+(r-1)} \equiv \ldots \equiv i\pi^{(k-1)r+(r-1)} \bmod (q-1). \end{aligned}$$

Тогда согласно леммам 5.2 и 5.8 справедливы равенства:

$$\begin{gathered} x^i = x^{i\pi^r} = x^{i\pi^{2r}} = \cdots = x^{i\pi^{(k-1)r}}, \\ x^{i\pi} = x^{i\pi^{r+1}} = x^{i\pi^{2r+1}} = \cdots = x^{i\pi^{(k-1)r+1}}, \\ \vdots \\ x^{i\pi^{r-1}} = x^{i\pi^{r+(r-1)}} = x^{i\pi^{2r+(r-1)}} = \cdots = x^{i\pi^{(k-1)r+(r-1)}}. \end{gathered}$$

Отсюда вытекает следующая цепочка равенств:

$$\begin{gathered} \mathcal{P}_a(x) = \operatorname{tr}(\xi x^i) = \xi x^i + \xi^{\pi} x^{i\pi} + \cdots + \xi^{\pi^{m-1}} x^{i\pi^{m-1}} = \\ = \left(\xi x^i + \xi^{\pi^r} x^{i\pi^r} + \xi^{\pi^{2r}} x^{i\pi^{2r}} + \cdots + \xi^{\pi^{(k-1)r}} x^{i\pi^{(k-1)r}}\right) + \\ + \left(\xi^{\pi} x^{i\pi} + \xi^{\pi^{r+1}} x^{i\pi^{r+1}} + \xi^{\pi^{2r+1}} x^{i\pi^{2r+1}} + \cdots + \xi^{\pi^{(k-1)r+1}} x^{i\pi^{(k-1)r+1}}\right) + \\ + \cdots + \left(\xi^{\pi^{r-1}} x^{i\pi^{r-1}} + \xi^{\pi^{r+(r-1)}} x^{i\pi^{r+(r-1)}} + \cdots + \xi^{\pi^{(k-1)r+(r-1)}} x^{i\pi^{(k-1)r+(r-1)}}\right) = \\ = \left(\xi + \xi^{\pi^r} + \cdots + \xi^{\pi^{(k-1)r}}\right) \cdot x^i + \left(\xi^{\pi} + \xi^{\pi^{r+1}} + \cdots + \xi^{\pi^{(k-1)r+1}}\right) \cdot x^{i\pi} + \\ + \cdots + \left(\xi^{\pi^{r-1}} + \xi^{\pi^{r+(r-1)}} + \cdots + \xi^{\pi^{(k-1)r+(r-1)}}\right) \cdot x^{i\pi^{r-1}} = \\ = \left(\xi + \xi^{\pi^r} + \cdots + \xi^{\pi^{(k-1)r}}\right) \cdot x^i + \left(\xi + \xi^{\pi^r} + \cdots + \xi^{\pi^{(k-1)r}}\right)^{\pi} \cdot x^{i\pi} + \\ + \cdots + \left(\xi + \xi^{\pi^r} + \cdots + \xi^{\pi^{(k-1)r}}\right)^{\pi^{r-1}} \cdot x^{i\pi^{r-1}} = \\ = \operatorname{tr}_r^m(\xi) \cdot x^i + (\operatorname{tr}_r^m(\xi))^{\pi} \cdot x^{i\pi} + \cdots + (\operatorname{tr}_r^m(\xi))^{\pi^{r-1}} \cdot x^{i\pi^{r-1}}. \end{gathered}$$

□

Замечание 5.6. Отметим, что в (12) все мономы имеют различные степени, и множество этих степеней совпадает с $Orb(i)$.

Следствие 5.5. *В условиях предыдущего утверждения имеем* $\mathcal{P}_a(x) = \operatorname{tr}_1^r(\operatorname{tr}_r^m(\xi) \cdot x^i)$.

Доказательство. Из предыдущего утверждения получаем

$$\begin{gathered} \mathcal{P}_a(x) = \operatorname{tr}_r^m(\xi) \cdot x^i + (\operatorname{tr}_r^m(\xi))^{\pi} \cdot x^{i\pi} + \cdots + (\operatorname{tr}_r^m(\xi))^{\pi^{r-1}} \cdot x^{i\pi^{r-1}} = \\ = \operatorname{tr}_r^m(\xi) \cdot x^i + \left(\operatorname{tr}_r^m(\xi) \cdot x^i\right)^{\pi} + \cdots + \left(\operatorname{tr}_r^m(\xi) \cdot x^i\right)^{\pi^{r-1}} = \operatorname{tr}_1^r(\operatorname{tr}_r^m(\xi) \cdot x^i). \end{gathered}$$

□

Следствие 5.6. *В условиях предыдущего утверждения имеем* $a \neq 0$ *при* $\operatorname{tr}(\xi) \neq 0$.

Доказательство. Рассмотрим $\mathcal{P}_a(1_Q)$:

$$\mathcal{P}_a(1_Q) = \operatorname{tr}_1^r(\operatorname{tr}_r^m(\xi) \cdot 1_Q) = \operatorname{tr}_1^r(\operatorname{tr}_r^m(\xi)) = \operatorname{tr}_1^m(\xi) = \operatorname{tr}(\xi) \neq 0.$$

Отсюда получаем $\mathcal{P}_a \not\equiv 0$. Значит, в силу следствия 5.2 имеем $a \neq 0$. □

Утверждение 5.3. *Пусть* $\xi, \chi \in Q$. *Пусть* $a = \mathrm{Tr}(\xi u_i)$, $b = \mathrm{Tr}(\chi u_i)$, *где* $i \in \overline{0, q-1}$. *Пусть* $|Orb(i)| = r$. *Тогда* $a = b$ *тогда и только тогда, когда* $\mathrm{tr}_r^m(\xi) = \mathrm{tr}_r^m(\chi)$.

Доказательство. Условие $a = b$ равносильно тому, что $\mathcal{P}_a = \mathcal{P}_b$. В силу утверждения 5.2 последнее равенство эквивалентно тому, что у $\mathcal{P}_a$ и $\mathcal{P}_b$ одинаковый коэффициент при x^i, т.е. $\mathrm{tr}_r^m(\xi) = \mathrm{tr}_r^m(\chi)$. □

Следствие 5.7. *Пусть* $\xi \in Q$. *Пусть* $a = \mathrm{Tr}(\xi u_i)$, *где* $i \in \overline{0, q-1}$. *Пусть* $|Orb(i)| = r$. *Тогда* $a = 0$ *тогда и только тогда, когда* $\mathrm{tr}_r^m(\xi) = 0$.

Доказательство. Воспользуемся предыдущим утверждением для $\chi = 0$. □

Теорема 5.1. *Пусть* $\xi, \chi \in Q$. *Пусть* $a = \mathrm{Tr}(\xi u_i)$, $b = \mathrm{Tr}(\chi u_j)$, *где* $i, j \in \overline{0, q-1}$. *Пусть* $|Orb(i)| = r_1$, $|Orb(j)| = r_2$. *Условие* $a = b = 0$ *равносильно тому, что* $\mathrm{tr}_{r_1}^m(\xi) = \mathrm{tr}_{r_2}^m(\chi) = 0$. *Условие* $a = b \neq 0$ *равносильно тому, что* $\mathrm{tr}_{r_1}^m(\xi) \neq 0$, $\mathrm{tr}_{r_2}^m(\chi) \neq 0$, $r_1 = r_2 = r$, $i = {S_\pi}^k(j)$, $\mathrm{tr}_r^m(\xi) = \left(\mathrm{tr}_r^m(\chi)\right)^{\pi^k}$, *где* $k \in \overline{1, m}$.

Доказательство. Согласно предыдущему следствию достаточно рассмотреть только случай $a = b \neq 0$. Условие $a = b$ равносильно тому, что $\mathcal{P}_a = \mathcal{P}_b$.

В силу замечания 5.6 последнее равенство влечёт $Orb(i) = Orb(j)$, т.е. $r_1 = r_2 = r$, $i = {S_\pi}^k(j)$, где $k \in \overline{1, m}$. Отсюда вытекает, что коэффициент при x^i в $\mathcal{P}_a$ равен коэффициенту при $x^{j\pi^k}$ в $\mathcal{P}_b$, т.е. $\mathrm{tr}_r^m(\xi) = \left(\mathrm{tr}_r^m(\chi)\right)^{\pi^k}$.

Наоборот, пусть $r_1 = r_2 = r$, $i = {S_\pi}^k(j)$ и $\mathrm{tr}_r^m(\xi) = \left(\mathrm{tr}_r^m(\chi)\right)^{\pi^k}$, тогда по следствию 5.5 заключаем, что $\mathcal{P}_a = \mathcal{P}_b$. Теорема доказана. □

5.3 Произведения вида $\mathrm{Tr}(\xi u_i) \cdot \mathrm{Tr}(\chi u_j)$

Докажем аналог леммы 1.1 для произведения элементов $\mathrm{Tr}(\xi u_i)$ и $\mathrm{Tr}(\chi u_j)$, где $\xi, \chi \in Q$. Начнём с подробного исследования произведения элементов $\mathrm{Tr}(u_i)$ и $\mathrm{Tr}(u_j)$.

Лемма 5.13. *Пусть* $a = u_i$, $b = u_j$, *где* $i, j \in \overline{0, q-1}$. *Тогда* $\mathcal{P}_{a \cdot b} = \sum\limits_{c \in Q} c^i (x - c)^j$.

Доказательство. Согласно определению имеем $u_i = \sum\limits_{h \in H} \phi(h)^i h$. Аналогично для u_j. Тогда имеет место цепочка равенств:

$$u_i \cdot u_j = \sum_{h \in H} \sum_{g \in H} \phi(g)^i \phi(h)^j gh = \sum_{h \in H} \left(\sum_{g \in H} \phi(g)^i \phi\left(g^{-1}h\right)^j \right) h =$$

$$= \sum_{h \in H} \left(\sum_{g \in H} \phi(g)^i (\phi(h) - \phi(g))^j \right) h = \sum_{h \in H} \left(\sum_{c \in Q} c^i (\phi(h) - c)^j \right) h,$$

где последнее равенство справедливо в силу того, что ϕ — изоморфизм между $(H, \cdot)$ и $(Q, +)$. Легко видеть, что

$$\pi_{a \cdot b}(h) = \sum_{c \in Q} c^i (\phi(h) - c)^j.$$

Отсюда по определению $\mathcal{P}_{a \cdot b}$ получаем требуемое равенство. Лемма доказана. □

Лемма 5.14. *Пусть $a = Tr(u_i)$, $b = Tr(u_j)$, где $i, j \in \overline{0, q-1}$. Тогда*

$$\mathcal{P}_{a\cdot b} = \sum_{c\in Q} \operatorname{tr}\left(c^i\right) \operatorname{tr}\left((x-c)^j\right).$$

Доказательство. По определению имеем $\mathrm{Tr}(u_i) = \sum\limits_{h\in H} \operatorname{tr}\left(\phi(h)^i\right) h$. Аналогично для $\mathrm{Tr}(u_j)$. Тогда имеет место цепочка равенств:

$$\mathrm{Tr}(u_i)\cdot \mathrm{Tr}(u_j) = \sum_{h\in H}\sum_{g\in H} \operatorname{tr}\left(\phi(g)^i\right) \operatorname{tr}\left(\phi(h)^j\right) gh = \sum_{h\in H}\left(\sum_{g\in H} \operatorname{tr}\left(\phi(g)^i\right) \operatorname{tr}\left(\phi\left(g^{-1}h\right)^j\right)\right) h =$$

$$= \sum_{h\in H}\left(\sum_{g\in H} \operatorname{tr}\left(\phi(g)^i\right) \operatorname{tr}\left((\phi(h)-\phi(g))^j\right)\right) h = \sum_{h\in H}\left(\sum_{c\in Q} \operatorname{tr}(c^i)\operatorname{tr}\left((\phi(h)-c)^j\right)\right) h,$$

где последнее равенство справедливо в силу того, что ϕ — изоморфизм между $(H,\cdot)$ и $(Q,+)$. Легко видеть, что

$$\pi_{a\cdot b}(h) = \sum_{c\in Q} \operatorname{tr}\left(c^i\right) \operatorname{tr}\left((\phi(h)-c)^j\right).$$

Отсюда по определению $\mathcal{P}_{a\cdot b}$ получаем требуемое равенство. Лемма доказана. □

Лемма 5.15. *Пусть $i \in \overline{0, q-1}$, $k \in \overline{0, m}$. Пусть $f \in Q[x]$. Тогда многочлены $f^{i\pi^k}$ и $f^{S_\pi{}^k(i)}$ определяют одну и ту же функцию, действующую из поля Q в себя.*

Доказательство. По лемме 5.8 мономы $x^{i\pi^k}$ и $x^{S_\pi{}^k(i)}$ определяют одну и ту же функцию. Значит, выполнено равенство функций:

$$f^{i\pi^k} = x^{i\pi^k} \circ f = x^{S_\pi{}^k(i)} \circ f = f^{S_\pi{}^k(i)}.$$

□

Лемма 5.16. *Пусть $f \in Q[x]$. Тогда многочлены f^q и f определяют одну и ту же функцию, действующую из поля Q в себя.*

Доказательство. Известно, что многочлены над Q, сравнимые по модулю двучлена $x^q - x$, определяют одну и ту же функцию, действующую из поля Q в себя [10]. В частности, мономы x^q и x задают одну и ту же функцию. Значит, выполнено равенство функций:

$$f^q = x^q \circ f = x \circ f = f.$$

□

Лемма 5.17. *Пусть $a = Tr(u_i)$, $b = Tr(u_j)$, где $i, j \in \overline{0, q-1}$. Тогда*

$$\mathcal{P}_{a\cdot b} = \sum_{k=0}^{m-1}\sum_{c\in Q} \operatorname{tr}\left(c^i (x-c)^{j\pi^k}\right).$$

Доказательство. Согласно лемме 5.14 получаем

$$\mathcal{P}_{a\cdot b} = \sum_{c\in Q} \operatorname{tr}\left(c^i\right) \operatorname{tr}\left((x-c)^j\right) =$$
$$= \sum_{c\in Q} \left(c^i + c^{i\pi} + \cdots + c^{i\pi^{m-1}}\right)\left((x-c)^j + (x-c)^{j\pi} + \cdots + (x-c)^{j\pi^{m-1}}\right).$$

Пусть $a_{s,t} = c^{i\pi^{s-1}}(x-c)^{j\pi^{t-1}}$. Тогда имеем $\mathcal{P}_{a\cdot b} = \sum\limits_{c\in Q}\sum\limits_{s=1}^{m}\sum\limits_{t=1}^{m} a_{s,t}$. Положим

$$M_k = \sum_{s=1}^{m-k} a_{s,s+k} + \sum_{s=m-k+1}^{m} a_{s,s+k-m}.$$

Несложно понять, что $\sum\limits_{s=1}^{m}\sum\limits_{t=1}^{m} a_{s,t} = \sum\limits_{k=0}^{m-1} M_k$. В самом деле, имеет место цепочка равенств:

$$\sum_{k=0}^{m-1} M_k = \sum_{k=0}^{m-1}\sum_{s=1}^{m-k} a_{s,s+k} + \sum_{k=0}^{m-1}\sum_{s=m-k+1}^{m} a_{s,s+k-m} = \sum_{\substack{s,t\in\overline{1,m}\\ s\leqslant t}} a_{s,t} + \sum_{\substack{s,t\in\overline{1,m}\\ s>t}} a_{s,t} = \sum_{s=1}^{m}\sum_{t=1}^{m} a_{s,t}.$$

Заметим, что $M_k = \operatorname{tr}\left(c^i(x-c)^{j\pi^k}\right)$. В самом деле, имеем

$$M_k = \sum_{s=1}^{m-k} a_{s,s+k} + \sum_{s=m-k+1}^{m} a_{s,s+k-m} =$$
$$= \left(c^i(x-c)^{j\pi^k} + c^{i\pi}(x-c)^{j\pi^{k+1}} + \cdots + c^{i\pi^{m-k-1}}(x-c)^{j\pi^{m-1}}\right) +$$
$$+ \left(c^{i\pi^{m-k}}(x-c)^{j} + c^{i\pi^{m-k+1}}(x-c)^{j\pi} + \cdots + c^{i\pi^{m-1}}(x-c)^{j\pi^{k-1}}\right).$$

В силу предыдущей леммы получаем

$$\left(c^{i\pi^{m-k}}(x-c)^{j} + c^{i\pi^{m-k+1}}(x-c)^{j\pi} + \cdots + c^{i\pi^{m-1}}(x-c)^{j\pi^{k-1}}\right) =$$
$$= \left(c^{i\pi^{m-k}}(x-c)^{j\pi^m} + c^{i\pi^{m-k+1}}(x-c)^{j\pi^{m+1}} + \cdots + c^{i\pi^{m-1}}(x-c)^{j\pi^{m+k-1}}\right).$$

Отсюда вытекает, что

$$M_k = \left(c^i(x-c)^{j\pi^k} + c^{i\pi}(x-c)^{j\pi^{k+1}} + \cdots + c^{i\pi^{m-k-1}}(x-c)^{j\pi^{m-1}}\right) +$$
$$+ \left(c^{i\pi^{m-k}}(x-c)^{j\pi^m} + c^{i\pi^{m-k+1}}(x-c)^{j\pi^{m+1}} + \cdots + c^{i\pi^{m-1}}(x-c)^{j\pi^{m+k-1}}\right) = \operatorname{tr}\left(c^i(x-c)^{j\pi^k}\right).$$

Из вышесказанного заключаем, что

$$\mathcal{P}_{a\cdot b} = \sum_{c\in Q}\sum_{s=1}^{m}\sum_{t=1}^{m} a_{s,t} = \sum_{c\in Q}\sum_{k=0}^{m-1} M_k = \sum_{k=0}^{m-1}\sum_{c\in Q} M_k = \sum_{k=0}^{m-1}\sum_{c\in Q} \operatorname{tr}\left(c^i(x-c)^{j\pi^k}\right).$$

□

Следствие 5.8. *Пусть* $a = Tr(u_i)$, $b = Tr(u_j)$, *где* $i, j \in \overline{0, q-1}$. *Тогда*

$$\mathcal{P}_{a\cdot b} = \sum_{k=0}^{m-1} \sum_{c\in Q} \operatorname{tr}\left(c^i (x-c)^{S_\pi{}^k(j)}\right).$$

Доказательство. Согласно лемме 5.15 получаем $\operatorname{tr}\left(c^i (x-c)^{j\pi^k}\right) = \operatorname{tr}\left(c^i (x-c)^{S_\pi{}^k(j)}\right)$, что завершает доказательство. □

Утверждение 5.4. *Пусть* $a = \mathrm{Tr}(u_i)$, $b = \mathrm{Tr}(u_j)$, *где* $i, j \in \overline{0, q-1}$ *и* i, j *не равны* $(q-1)$ *одновременно. Тогда*

$$\mathrm{Tr}(u_i) \cdot \mathrm{Tr}(u_j) = \sum_{k=0}^{m-1} c_{\delta_k} \cdot \mathrm{Tr}(u_{\delta_k}),$$

где $\delta_k = i + S_\pi{}^k(j) - (q-1)$, $c_{\delta_k} = 0$ *при* $\delta_k < 0$ *и* c_{δ_k} *определяется по лемме 1.1 при* $\delta_k \geqslant 0$.

Доказательство. По лемме 1.1 имеем $u_i u_{S_\pi{}^k(j)} = c_{\delta_k} u_{\delta_k}$, где c_{δ_k} определяется в соответствии с условием. Отсюда по леммам 5.6 и 5.13 заключаем, что

$$\mathcal{P}_{u_i u_{S_\pi{}^k(j)}} = \sum_{c\in Q} c^i (x-c)^{S_\pi{}^k(j)} = c_{\delta_k} \cdot x^{\delta_k} = \mathcal{P}_{c_{\delta_k} u_{\delta_k}}.$$

Из предыдущего следствия получаем

$$\begin{aligned}\mathcal{P}_{a\cdot b} &= \sum_{k=0}^{m-1} \sum_{c\in Q} \operatorname{tr}\left(c^i (x-c)^{S_\pi{}^k(j)}\right) = \sum_{k=0}^{m-1} \operatorname{tr}\left(\sum_{c\in Q} c^i (x-c)^{S_\pi{}^k(j)}\right) = \\ &= \sum_{k=0}^{m-1} \operatorname{tr}\left(c_{\delta_k} \cdot x^{\delta_k}\right) = \sum_{k=0}^{m-1} c_{\delta_k} \cdot \operatorname{tr}(x^{\delta_k}) = \sum_{k=0}^{m-1} c_{\delta_k} \cdot \mathcal{P}_{\mathrm{Tr}(u_{\delta_k})},\end{aligned}$$

что завершает доказательство. □

Перейдём теперь к исследованию произведения элементов $\mathrm{Tr}(\xi u_i)$ и $\mathrm{Tr}(\chi u_j)$, где $\xi, \chi \in Q$.

Лемма 5.18. *Пусть* $a = \mathrm{Tr}(\xi u_i)$, $b = \mathrm{Tr}(\chi u_j)$, *где* $\xi, \chi \in Q$ *и* $i, j \in \overline{0, q-1}$. *Тогда*

$$\mathcal{P}_{a\cdot b} = \sum_{c\in Q} \operatorname{tr}\left(\xi c^i\right) \operatorname{tr}\left(\chi (x-c)^j\right).$$

Доказательство. Согласно определению имеем $\mathrm{Tr}(\xi u_i) = \sum\limits_{h\in H} \operatorname{tr}\left(\xi \phi(h)^i\right) h$. Аналогично для $\mathrm{Tr}(\chi u_j)$. Дальнейшие рассуждения повторяют доказательство леммы 5.14. □

Лемма 5.19. *Пусть* $a = \mathrm{Tr}(\xi u_i)$, $b = \mathrm{Tr}(\chi u_j)$, *где* $\xi, \chi \in Q$, $i, j \in \overline{0, q-1}$. *Тогда*

$$\mathcal{P}_{a\cdot b} = \sum_{k=0}^{m-1} \sum_{c\in Q} \operatorname{tr}\left(\xi c^i \chi^{\pi^k} (x-c)^{S_\pi{}^k(j)}\right).$$

Доказательство. Положим $a_{s,t} = (\xi c^i)^{\pi^{s-1}} (\chi (x-c)^j)^{\pi^{t-1}}$. Тогда имеем $\mathcal{P}_{a\cdot b} = \sum\limits_{c\in Q} \sum\limits_{s=1}^{m} \sum\limits_{t=1}^{m} a_{s,t}$. Пусть

$$M_k = \sum_{s=1}^{m-k} a_{s,s+k} + \sum_{s=m-k+1}^{m} a_{s,s+k-m}.$$

Рассуждая тем же образом, что и в доказательстве леммы 5.17, получаем $\sum\limits_{s=1}^{m} \sum\limits_{t=1}^{m} a_{s,t} = \sum\limits_{k=0}^{m-1} M_k$.

Заметим, что $M_k = \operatorname{tr}\left(\xi c^i \chi^{\pi^k} (x-c)^{j\pi^k}\right)$. В самом деле, в силу леммы 5.16 имеет место цепочка равенств:

$$\begin{gathered}
M_k = \sum_{s=1}^{m-k} a_{s,s+k} + \sum_{s=m-k+1}^{m} a_{s,s+k-m} = \\
= \left(\xi c^i (\chi (x-c)^j)^{\pi^k} + (\xi c^i)^{\pi} (\chi (x-c)^j)^{\pi^{k+1}} + \cdots + (\xi c^i)^{\pi^{m-k-1}} (\chi (x-c)^j)^{\pi^{m-1}}\right) + \\
+ \left((\xi c^i)^{\pi^{m-k}} (\chi (x-c)^j) + (\xi c^i)^{\pi^{m-k+1}} (\chi (x-c)^j)^{\pi} + \cdots + (\xi c^i)^{\pi^{m-1}} (\chi (x-c)^j)^{\pi^{k-1}}\right) = \\
= \left(\xi c^i (\chi (x-c)^j)^{\pi^k} + (\xi c^i)^{\pi} (\chi (x-c)^j)^{\pi^{k+1}} + \cdots + (\xi c^i)^{\pi^{m-k-1}} (\chi (x-c)^j)^{\pi^{m-1}}\right) + \\
+ \left((\xi c^i)^{\pi^{m-k}} (\chi (x-c)^j)^{\pi^m} + (\xi c^i)^{\pi^{m-k+1}} (\chi (x-c)^j)^{\pi^{m+1}} + \cdots + (\xi c^i)^{\pi^{m-1}} (\chi (x-c)^j)^{\pi^{m+k-1}}\right) = \\
= \operatorname{tr}\left(\xi c^i \chi^{\pi^k} (x-c)^{j\pi^k}\right).
\end{gathered}$$

По лемме 5.15 имеем $\operatorname{tr}\left(\xi c^i \chi^{\pi^k} (x-c)^{j\pi^k}\right) = \operatorname{tr}\left(\xi c^i \chi^{\pi^k} (x-c)^{S_{\pi^k}(j)}\right)$. Отсюда получаем

$$\begin{gathered}
\mathcal{P}_{a\cdot b} = \sum_{c\in Q} \sum_{s=1}^{m} \sum_{t=1}^{m} a_{s,t} = \sum_{c\in Q} \sum_{k=0}^{m-1} M_k = \sum_{k=0}^{m-1} \sum_{c\in Q} M_k = \\
= \sum_{k=0}^{m-1} \sum_{c\in Q} \operatorname{tr}\left(\xi c^i \chi^{\pi^k} (x-c)^{j\pi^k}\right) = \sum_{k=0}^{m-1} \sum_{c\in Q} \operatorname{tr}\left(\xi c^i \chi^{\pi^k} (x-c)^{S_{\pi^k}(j)}\right).
\end{gathered}$$

□

Теорема 5.2. *Пусть* $a = \operatorname{Tr}(\xi u_i)$, $b = \operatorname{Tr}(\chi u_j)$, *где* $\xi, \chi \in Q$, $i, j \in \overline{0, q-1}$ *и* i, j *не равны* $(q-1)$ *одновременно. Тогда*

$$\operatorname{Tr}(\xi u_i) \cdot \operatorname{Tr}(\chi u_j) = \sum_{k=0}^{m-1} c_{\delta_k} \cdot \operatorname{Tr}(\xi \chi^{\pi^k} u_{\delta_k}),$$

где $\delta_k = i + S_{\pi}{}^k(j) - (q-1)$, $c_{\delta_k} = 0$ *при* $\delta_k < 0$ *и* c_{δ_k} *определяется по лемме 1.1 при* $\delta_k \geqslant 0$.

Доказательство. По лемме 1.1 имеем $(\xi u_i) \cdot \left(\chi^{\pi^k} u_{S_{\pi^k}(j)}\right) = c_{\delta_k} \xi \chi^{\pi^k} u_{\delta_k}$, где c_{δ_k} определяется в соответствии с условием. Отсюда по леммам 5.6 и 5.13 заключаем, что

$$\mathcal{P}_{(\xi u_i)\cdot\left(\chi^{\pi^k} u_{S_{\pi^k}(j)}\right)} = \sum_{c\in Q} \xi c^i \chi^{\pi^k} (x-c)^{S_{\pi^k}(j)} = c_{\delta_k} \xi \chi^{\pi^k} \cdot x^{\delta_k} = \mathcal{P}_{c_{\delta_k} \xi \chi^{\pi^k} u_{\delta_k}}.$$

В силу предыдущей леммы получаем

$$\mathcal{P}_{a\cdot b} = \sum_{k=0}^{m-1} \sum_{c\in Q} \mathrm{tr}\left(\xi c^i \chi^{\pi^k} (x-c)^{S_\pi{}^k(j)}\right) = \sum_{k=0}^{m-1} \mathrm{tr}\left(\sum_{c\in Q} \xi c^i \chi^{\pi^k} (x-c)^{S_\pi{}^k(j)}\right) =$$
$$= \sum_{k=0}^{m-1} \mathrm{tr}\left(c_{\delta_k}\cdot \xi\chi^{\pi^k} x^{\delta_k}\right) = \sum_{k=0}^{m-1} c_{\delta_k}\cdot \mathrm{tr}(\xi\chi^{\pi^k} x^{\delta_k}) = \sum_{k=0}^{m-1} c_{\delta_k}\cdot \mathcal{P}_{\mathrm{Tr}(\xi\chi^{\pi^k} u_{\delta_k})},$$

что завершает доказательство. □

Теорема 5.3. *Пусть* $a = \mathrm{Tr}(\xi u_i)$, $b = \mathrm{Tr}(\chi u_j)$, *где* $\xi, \chi \in Q$, $i, j \in \overline{0, q-1}$ *и* i, j *не равны* $(q-1)$ *одновременно. Тогда*

$$\mathrm{Tr}(\xi u_i)\cdot \mathrm{Tr}(\chi u_j) = \sum_{k=0}^{m-1} c_{\tilde{\delta_k}}\cdot \mathrm{Tr}(\xi^{\pi^k}\chi u_{\tilde{\delta_k}}),$$

где $\tilde{\delta_k} = S_\pi{}^k(i) + j - (q-1)$, $c_{\tilde{\delta_k}} = 0$ *при* $\tilde{\delta_k} < 0$ *и* $c_{\tilde{\delta_k}}$ *определяется по лемме 1.1 при* $\tilde{\delta_k} \geqslant 0$.

Доказательство. Непосредственно вытекает из предыдущей теоремы после замены местами i и j, ξ и χ. □

5.4 Базисы кодов Рида–Маллера

Лемма 5.20. *Пусть* $t \in \overline{0, q-1}$ *и* $\chi \in Q$. *Пусть* $s \in Orb(t)$. *Тогда существует* $\xi \in Q$ *такой, что* $\mathrm{Tr}(\chi u_s) = \mathrm{Tr}(\xi u_t)$.

Доказательство. Если выполнено равенство $\mathrm{Tr}(\chi u_s) = 0$, то утверждение очевидно. Рассмотрим случай $\mathrm{Tr}(\chi u_s) \neq 0$. Пусть $|Orb(t)| = r$. Тогда согласно теореме 5.1 для искомого ξ должно выполняться равенство $\mathrm{tr}_r^m(\xi) = (\mathrm{tr}_r^m(\chi))^{\pi^k}$, где $k \in \overline{1, m}$. Поскольку tr_r^m является сюръективным отображением [3], указанный элемент ξ существует. Лемма доказана. □

Следствие 5.9. *Пусть* $t \in \overline{0, q-1}$. *Тогда выполнено равенство* $\mathrm{Tr}\left(\sum\limits_{s\in Orb(t)} Qu_s\right) = \mathrm{Tr}(Qu_t)$.

Определение 5.5. Произвольный набор представителей всевозможных орбит элементов Π_k под действием группы $\langle S_\pi\rangle_m$ обозначим $I_\pi(m,k)$.

По определению имеем

$$\mathcal{M}_\pi(m,k) = \sum_{t\in I_\pi(m,k)} \left(\sum_{s\in Orb(t)} Qu_s\right).$$

Отсюда согласно предыдущему следствию получаем

$$\mathcal{RM}_\pi(m,k) = \mathrm{Tr}\left(\sum_{t\in I_\pi(m,k)} \left(\sum_{s\in Orb(t)} Qu_s\right)\right) = \sum_{t\in I_\pi(m,k)} \mathrm{Tr}\left(\sum_{s\in Orb(t)} Qu_s\right) = \sum_{t\in I_\pi(m,k)} \mathrm{Tr}(Qu_t).$$

Утверждение 5.5. *Пусть* $t \in \overline{0, q-1}$, $|Orb(t)| = r$. *Пусть* $\alpha'_1, \ldots, \alpha'_r$ — *базис* $\mathbb{F}_{\pi^r}$ *над* P. *Пусть* $\alpha_1, \ldots, \alpha_r \in Q$ *такие, что* $\alpha'_1 = \mathrm{tr}_r^m(\alpha_1), \ldots, \alpha'_r = \mathrm{tr}_r^m(\alpha_r)$. *Тогда* $\mathrm{Tr}(\alpha_1 u_t), \ldots, \mathrm{Tr}(\alpha_r u_t)$ — *базис* $\mathrm{Tr}(Qu_t)$ *над* P.

Доказательство. В силу того, что tr_r^m — сюръективное отображение, указанные элементы $\alpha_1, \ldots, \alpha_r$ существуют. Рассмотрим произвольный элемент $\mathrm{Tr}(\xi u_t)$. Пусть $p_1, \ldots, p_r \in P$ — коэффициенты разложения $\mathrm{tr}_r^m(\xi)$ по базису $\alpha'_1, \ldots, \alpha'_r$, т.е. $\mathrm{tr}_r^m(\xi) = p_1\alpha'_1 + \cdots + p_r\alpha'_r$. Согласно следствию 5.5 имеет место цепочка равенств:

$$\begin{gathered}\mathcal{P}_{\mathrm{Tr}(\xi u_t)} = \mathrm{tr}_1^r(\mathrm{tr}_r^m(\xi) \cdot x^t) = \mathrm{tr}_1^r((p_1\alpha'_1 + \cdots + p_r\alpha'_r) \cdot x^t) = \mathrm{tr}_1^r(p_1\alpha'_1 x^t) + \cdots + \mathrm{tr}_1^r(p_r\alpha'_r x^t) = \\ = p_1\mathrm{tr}_1^r(\alpha'_1 x^t) + \cdots + p_r\mathrm{tr}_1^r(\alpha'_r x^t) = p_1\mathrm{tr}_1^r(\mathrm{tr}_r^m(\alpha_1)x^t) + \cdots + p_r\mathrm{tr}_1^r(\mathrm{tr}_r^m(\alpha_r)x^t) = \\ = p_1\mathcal{P}_{\mathrm{Tr}(\alpha_1 u_t)} + \cdots + p_r\mathcal{P}_{\mathrm{Tr}(\alpha_r u_t)}.\end{gathered}$$

Отсюда заключаем, что элементы $\mathrm{Tr}(\alpha_1 u_t), \ldots, \mathrm{Tr}(\alpha_r u_t)$ порождают $\mathrm{Tr}(Qu_t)$.

Покажем, что данные элементы линейно независимы. Пусть $p_1, \ldots, p_r \in P$ такие, что $p_1\mathrm{Tr}(\alpha_1 u_t) + \cdots + p_r\mathrm{Tr}(\alpha_r u_t) = 0$. Легко видеть, что тогда имеем $\mathrm{Tr}((p_1\alpha_1 + \cdots + p_r\alpha_r)u_t) = 0$. По следствию 5.7 последнее равенство равносильно тому, что $\mathrm{tr}_r^m(p_1\alpha_1 + \cdots + p_r\alpha_r) = 0$. Отсюда получаем

$$\begin{gathered}0 = \mathrm{tr}_r^m(p_1\alpha_1 + \cdots + p_r\alpha_r) = \mathrm{tr}_r^m(p_1\alpha_1) + \cdots + \mathrm{tr}_r^m(p_r\alpha_r) = \\ = p_1\mathrm{tr}_r^m(\alpha_1) + \cdots + p_r\mathrm{tr}_r^m(\alpha_r) = p_1\alpha'_1 + \cdots + p_r\alpha'_r.\end{gathered}$$

Поскольку $\alpha'_1, \ldots, \alpha'_r$ — базис, имеем $p_1 = \cdots = p_r = 0$, что завершает доказательство. □

Таким образом, для каждого $t \in I_\pi(m, k)$ элементы $\mathrm{Tr}(\alpha_{t,1}u_t), \ldots, \mathrm{Tr}(\alpha_{t,r_t}u_t)$ образуют базис $\mathrm{Tr}(Qu_t)$ над P, где $r_t = |Orb(t)|$. В силу теоремы 5.1 полученные базисы не содержат общих элементов.

Определение 5.6. Для всех $k \in \overline{0, m(\pi-1)}$ определим множество $\mathrm{B}_\pi(m, k)$ равенством

$$\mathrm{B}_\pi(m, k) = \bigsqcup_{t \in I_\pi(m,k)} \{\mathrm{Tr}(\alpha_{t,1}u_t), \ldots, \mathrm{Tr}(\alpha_{t,r_t}u_t)\}.$$

Теорема 5.4. $\mathrm{B}_\pi(m, k)$ *является базисом* $\mathcal{RM}_\pi(m, k)$ *над* P.

Доказательство. В силу предыдущего утверждения указанные элементы порождают идеал $\mathcal{RM}_\pi(m, k)$. Покажем, что они линейно независимы. Пусть $I_\pi(m, k) = \{t_1, \ldots, t_n\}$. Пусть элементы

$$p_{t_1,1}, \ldots, p_{t_1,r_1}, \ldots, p_{t_n,1}, \ldots, p_{t_n,r_n} \in P$$

где $r_i = |Orb(t_i)|$, такие, что

$$\sum_{i=1}^{n} p_{t_i,1}\mathrm{Tr}(\alpha_{t_i,1}u_{t_i}) + \cdots + p_{t_i,r_i}\mathrm{Tr}(\alpha_{t_i,r_i}u_{t_i}) = 0. \tag{13}$$

Положим $T_i = p_{t_i,1}\mathrm{Tr}(\alpha_{t_i,1}u_{t_i}) + \cdots + p_{t_i,r_i}\mathrm{Tr}(\alpha_{t_i,r_i}u_{t_i})$. Равенство (13) равносильно тому, что $\sum\limits_{i=1}^{n} \mathcal{P}_{T_i} \equiv 0$. В силу замечания 5.6 степени ненулевых мономов, входящих в $\mathcal{P}_{T_i}$, являются элементами множества $Orb(t_i)$. Отсюда заключаем, что равенство (13) эквивалентно тому, что $\mathcal{P}_{T_i} \equiv 0$ при всех $i \in \overline{1,n}$, поскольку различные элементы $I_\pi(m,k)$ имеют непересекающиеся орбиты. По построению, элементы $\mathrm{Tr}(\alpha_{t,1}u_t), \ldots, \mathrm{Tr}(\alpha_{t,r_t}u_t)$ линейно независимы над P. Следовательно, условие $\mathcal{P}_{T_i} \equiv 0$ равносильно тому, что $p_{t_i,1} = \cdots = p_{t_i,r_i} = 0$. Таким образом, получаем

$$p_{t_1,1} = \cdots = p_{t_1,r_1} = \cdots = p_{t_n,1} = \cdots = p_{t_n,r_n} = 0,$$

что завершает доказательство. □

Следствие 5.10. *Пусть $k \in \overline{0, m(\pi-1)}$. Тогда выполнено равенство*

$$\dim_Q \mathcal{M}_\pi(m,k) = \dim_P \mathcal{RM}_\pi(m,k).$$

Доказательство. В силу предыдущей теоремы и утверждения 1.2 получаем

$$\dim_Q \mathcal{M}_\pi(m,k) = \sum_{t \in I_\pi(m,k)} |Orb(t)| = \dim_P \mathcal{RM}_\pi(m,k).$$

□

Замечание 5.7. Предыдущее следствие является известным фактом [2]. Однако, в отличие от доказательства, представленного в [2], предложенное здесь доказательство не использует предварительных результатов о строении кодов Рида–Маллера.

Отметим, что построенный базис $\mathrm{B}_\pi(m,k)$ определён неоднозначно: во-первых, множество $I_\pi(m,k)$ можно выбрать несколькими способами, во-вторых, набор элементов $\alpha_{t,1}, \ldots, \alpha_{t,r_t}$ для каждого $t \in I_\pi(m,k)$ также можно выбрать несколькими способами.

6 Перенос результатов для идеалов $\mathcal{M}_\pi(m,k)$ на случай идеалов $\mathcal{RM}_\pi(m,k)$

Цель данного раздела — доказать для идеалов $\mathcal{RM}_\pi(m,k)$ и $\mathcal{RM}_p(l,j)$ аналоги основных утверждений из разделов 2 и 3. Подобно случаю базисных кодов, покажем, что при $\lambda \neq 1$ нет нетривиальных совпадений кодов Рида–Маллера $\mathcal{RM}_\pi(m,k)$ и степеней радикала $\mathfrak{R}_R$, и исследуем граф включений указанных идеалов.

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

Докажем вспомогательное утверждение, которое неоднократно будет использовано далее. Покажем, что для всех $k \in \overline{0,q-1}$ выполнено равенство

$$\mathfrak{R}_R\mathcal{RM}_\pi(m,k) = \mathrm{Tr}(\mathfrak{R}_S\mathcal{M}_\pi(m,k)). \tag{14}$$

Лемма 6.1 ([2]). *Пусть $\alpha \in \overline{0,l(p-1)}$, тогда выполнено равенство*

$$\mathrm{Tr}({\mathfrak{R}_S}^\alpha) = {\mathfrak{R}_R}^\alpha.$$

Следовательно, равенство (14) равносильно тому, что

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

Лемма 6.2. *Пусть $k \in \overline{0,q-1}$, тогда имеет место включение*

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

Доказательство. Рассмотрим $u_s \in \mathfrak{R}_S$, $u_t \in \mathcal{M}_\pi(m,k)$ и $\xi,\chi \in Q$. По теореме 5.2 имеем

$$\mathrm{Tr}(\xi u_s)\cdot\mathrm{Tr}(\chi u_t) = \sum_{i=0}^{m-1} c_{\delta_i}\cdot\mathrm{Tr}(\xi\chi^{\pi^i}u_{\delta_i}),$$

где $\delta_i = s + {S_\pi}^i(t) - (q-1)$, $c_{\delta_i} = 0$ при $\delta_i < 0$ и c_{δ_i} определяется по лемме 1.1 при $\delta_i \geqslant 0$. Заметим, что каждое слагаемое $c_{\delta_i}\mathrm{Tr}(\xi\chi^{\pi^i}u_{\delta_i})$ принадлежит $\mathrm{Tr}(\mathfrak{R}_S\mathcal{M}_\pi(m,k))$. В самом деле, по лемме 5.3 получаем $u_{{S_\pi}^i(t)} \in \mathcal{M}_\pi(m,k)$, где $i \in \overline{0,m-1}$. В силу леммы 1.1 заключаем, что $c_{\delta_i}\xi\chi^{\pi^i}u_{\delta_i} \in \mathfrak{R}_S\mathcal{M}_\pi(m,k)$. Значит, имеем $c_{\delta_i}\mathrm{Tr}(\xi\chi^{\pi^i}u_{\delta_i}) \in \mathrm{Tr}(\mathfrak{R}_S\mathcal{M}_\pi(m,k))$, что завершает доказательство. □

Лемма 6.3. *Пусть $k \in \overline{0,q-1}$, тогда имеет место включение*

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

Доказательство. Рассмотрим произвольный элемент $u_\delta \in \mathfrak{R}_S\mathcal{M}_\pi(m,k)$. Согласно лемме 3.3 существуют $u_s \in \mathfrak{R}_S$, $u_t \in \mathcal{M}_\pi(m,k)$ такие, что $u_s u_t = c_\delta u_\delta$, $c_\delta \neq 0$, и все такие элементы u_δ

образуют базис $\mathfrak{R}_S\mathcal{M}_\pi(m,k)$. Пусть $\xi_j, \chi_j \in Q$, где $j \in \overline{1,m}$. Тогда по теореме 5.3 имеем

$$\mathrm{Tr}(\xi_j u_s)\mathrm{Tr}(\chi_j u_t) = \mathrm{Tr}(c_\delta \xi_j \chi_j u_\delta) + \sum_{i=1}^{m-1} \mathrm{Tr}(c_{\tilde{\delta}_i} {\xi_j}^{\pi^i} \chi_j u_{\tilde{\delta}_i}),$$

где $\tilde{\delta}_i = {S_\pi}^i(s) + t - (q-1)$, $c_{\tilde{\delta}_i} = 0$ при $\tilde{\delta}_i < 0$ и $c_{\tilde{\delta}_i}$ определяется по лемме 1.1 при $\tilde{\delta}_i \geqslant 0$. Отсюда вытекает цепочка равенств:

$$\begin{aligned}\sum_{j=1}^{m} \mathrm{Tr}(\xi_j u_s)\mathrm{Tr}(\chi_j u_t) &= \sum_{j=1}^{m} \mathrm{Tr}(c_\delta \xi_j \chi_j u_\delta) + \sum_{j=1}^{m}\sum_{i=1}^{m-1} \mathrm{Tr}(c_{\tilde{\delta}_i} {\xi_j}^{\pi^i} \chi_j u_{\tilde{\delta}_i}) = \\ &= \mathrm{Tr}\left(\sum_{j=1}^{m} c_\delta \xi_j \chi_j u_\delta\right) + \sum_{i=1}^{m-1} \mathrm{Tr}\left(\sum_{j=1}^{m} c_{\tilde{\delta}_i} {\xi_j}^{\pi^i} \chi_j u_{\tilde{\delta}_i}\right) = \\ &= \mathrm{Tr}\left(c_\delta \left(\sum_{j=1}^{m} \xi_j \chi_j\right) u_\delta\right) + \sum_{i=1}^{m-1} \mathrm{Tr}\left(c_{\tilde{\delta}_i} \left(\sum_{j=1}^{m} {\xi_j}^{\pi^i} \chi_j\right) u_{\tilde{\delta}_i}\right).\end{aligned} \tag{15}$$

Рассмотрим следующую систему линейных уравнений относительно неизвестных χ_j:

$$\begin{cases} \xi_1\chi_1 + \cdots + \xi_m\chi_m = \xi \\ {\xi_1}^{\pi}\chi_1 + \cdots + {\xi_m}^{\pi}\chi_m = 0 \\ {\xi_1}^{\pi^2}\chi_1 + \cdots + {\xi_m}^{\pi^2}\chi_m = 0 \\ \vdots \\ {\xi_1}^{\pi^{m-1}}\chi_1 + \cdots + {\xi_m}^{\pi^{m-1}}\chi_m = 0, \end{cases}$$

где $\xi \in Q$. Легко видеть, что если данная система уравнений имеет решение, то равенство (15) можно переписать следующим образом:

$$\sum_{j=1}^{m} \mathrm{Tr}(\xi_j u_s)\mathrm{Tr}(\chi_j u_t) = \mathrm{Tr}\left(c_\delta \left(\sum_{j=1}^{m} \xi_j \chi_j\right) u_\delta\right) + \sum_{i=1}^{m-1} \mathrm{Tr}\left(c_{\tilde{\delta}_i} \left(\sum_{j=1}^{m} {\xi_j}^{\pi^i} \chi_j\right) u_{\tilde{\delta}_i}\right) = \mathrm{Tr}\left(c_\delta \xi u_\delta\right).$$

Поскольку ξ можно выбрать произвольно, получено представление произвольного элемента $\mathrm{Tr}(\xi u_\delta)$, где $\xi \in Q$, $u_\delta \in \mathfrak{R}_S\mathcal{M}_\pi(m,k)$, в виде элемента идеала $\mathrm{Tr}(\mathfrak{R}_S)\mathrm{Tr}(\mathcal{M}_\pi(m,k))$. Отсюда заключаем, что имеет место включение $\mathrm{Tr}(\mathfrak{R}_S)\mathrm{Tr}(\mathcal{M}_\pi(m,k)) \supseteq \mathrm{Tr}(\mathfrak{R}_S\mathcal{M}_\pi(m,k))$.

Покажем, что рассмотренная система уравнений имеет решение. Матрица коэффициентов данной системы имеет вид:

$$A_{m\times m} = \begin{pmatrix} \xi_1 & \xi_2 & \cdots & \xi_m \\ {\xi_1}^{\pi} & {\xi_2}^{\pi} & \cdots & {\xi_m}^{\pi} \\ {\xi_1}^{\pi^2} & {\xi_2}^{\pi^2} & \cdots & {\xi_m}^{\pi^2} \\ \vdots & \vdots & \ddots & \vdots \\ {\xi_1}^{\pi^{m-1}} & {\xi_2}^{\pi^{m-1}} & \cdots & {\xi_m}^{\pi^{m-1}} \end{pmatrix}$$

Заметим, что A — транспонированная матрица Мура. Как известно, её определитель

нулевой тогда и только тогда, когда элементы $\xi_1, \ldots, \xi_m$ линейно зависимы над P [9]. В силу того, что степень Q над P равна $[Q : P] = m$ [3], можно выбрать элементы $\xi_1, \ldots, \xi_m$ линейно независимыми над P. Тогда получаем $\det A \neq 0$, т.е. $\operatorname{rk} A = m$.

Рассмотрим теперь расширенную матрицу указанной системы уравнений:

$$\tilde{A} = \begin{pmatrix} \xi_1 & \xi_2 & \cdots & \xi_m & \xi \\ {\xi_1}^{\pi} & {\xi_2}^{\pi} & \cdots & {\xi_m}^{\pi} & 0 \\ {\xi_1}^{\pi^2} & {\xi_2}^{\pi^2} & \cdots & {\xi_m}^{\pi^2} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ {\xi_1}^{\pi^{m-1}} & {\xi_2}^{\pi^{m-1}} & \cdots & {\xi_m}^{\pi^{m-1}} & 0 \end{pmatrix}$$

Заметим, что $\operatorname{rk} \tilde{A} = m$. В самом деле, пусть $\tilde{A}_1, \tilde{A}_2, \ldots, \tilde{A}_m$ — система строк матрицы $\tilde{A}$. Предположим, что $\lambda_1 \tilde{A}_1 + \cdots + \lambda_m \tilde{A}_m = 0$, где $\lambda_1, \ldots, \lambda_m \in Q$. Если $\xi \neq 0$, тогда, рассматривая последний столбец матрицы $\tilde{A}$, получаем $\lambda_1 = 0$. Отсюда вытекает, что $\lambda_2 \tilde{A}_2 + \cdots + \lambda_m \tilde{A}_m = 0$. Пусть $A_1, A_2, \ldots, A_m$ — система строк матрицы A, тогда $A_2, \ldots, A_m$ — укороченная система строк $\tilde{A}_2, \ldots, \tilde{A}_m$. В силу того, что $\operatorname{rk} A = m$, заключаем, что строки $A_2, \ldots, A_m$ линейно независимы над Q. Значит, строки $\tilde{A}_2, \ldots, \tilde{A}_m$ линейно независимы над Q. Следовательно, получаем $\lambda_1 = \lambda_2 = \cdots = \lambda_m = 0$, т.е. $\operatorname{rk} \tilde{A} = m$. Если $\xi = 0$, тогда $A_1, \ldots, A_m$ — укороченная система строк $\tilde{A}_1, \ldots, \tilde{A}_m$. Поскольку $\operatorname{rk} A = m$, имеем $\operatorname{rk} \tilde{A} = m$.

По теореме Кронекера–Капелли из равенства $\operatorname{rk} A = \operatorname{rk} \tilde{A} = m$ следует, что рассмотренная выше система уравнений имеет решение. Лемма доказана. □

Из лемм 6.2 и 6.3 вытекает

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

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

Следствие 6.1. *Если выполнено равенство* (6)*, тогда выполнено равенство*

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

Доказательство. Пусть выполнено равенство (6). Тогда, применяя к обеим частям данного равенства функцию Tr, в силу предыдущего утверждения получаем

$$\mathfrak{R}_R \mathcal{RM}_\pi(m, k+1) = \operatorname{Tr}(\mathfrak{R}_S \mathcal{M}_\pi(m, k+1)) = \operatorname{Tr}(\mathcal{M}_\pi(m, k)) = \mathcal{RM}_\pi(m, k).$$

□

6.2 Совпадения кодов Рида–Маллера со степенями радикала $\mathfrak{R}_R$

Далее под степенями радикала будем понимать степени радикала $\mathfrak{R}_R$. Покажем, что при $\lambda \neq 1$ нет нетривиальных совпадений между кодами Рида–Маллера и степенями радикала $\mathfrak{R}_R$.

Совпадения кодов Рида–Маллера со степенями радикала в случае простого подполя описываются следующим утверждением.

Утверждение 6.2 ([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*

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

Доказательство. Непосредственно вытекает из утверждения 2.2. □

Докажем аналог теоремы 2.1.

Лемма 6.4. *Пусть $t \in \overline{0,q-1}$ и $k \in \overline{0,m(\pi-1)}$. Пусть $\xi \in Q$. Пусть $\mathrm{Tr}(\xi u_t) \neq 0$. Тогда $\mathrm{Tr}(\xi u_t) \in \mathcal{RM}_\pi(m,k)$ тогда и только тогда, когда $t \in \Pi_k$.*

Доказательство. Пусть $t \in \Pi_k$, тогда $u_t \in \mathcal{M}_\pi(m,k)$. Значит, имеем $\mathrm{Tr}(\xi u_t) \in \mathcal{RM}_\pi(m,k)$ для любого $\xi \in Q$.

Наоборот, пусть $\mathrm{Tr}(\xi u_t) \in \mathcal{RM}_\pi(m,k)$. В силу следствий 5.5 и 5.7 заключаем, что моном x^t входит в многочлен $\mathcal{P}_{\mathrm{Tr}(\xi u_t)}$ с ненулевым коэффициентом. Пусть $\mathrm{B}_\pi(m,k)$ — базис $\mathcal{RM}_\pi(m,k)$. Тогда $\mathrm{Tr}(\xi u_t)$ является линейной комбинацией элементов $\mathrm{Tr}(\alpha_i u_j) \in \mathrm{B}_\pi(m,k)$. Отсюда имеем

$$\mathcal{P}_{\mathrm{Tr}(\xi u_t)} = \sum_{\mathrm{Tr}(\alpha_i u_j) \in \mathrm{B}_\pi(m,k)} p_{i,j} \cdot \mathcal{P}_{\mathrm{Tr}(\alpha_i u_j)},$$

где $p_{i,j} \in P$. Согласно замечанию 5.6 получаем, что степени мономов, входящих в $\mathcal{P}_{\mathrm{Tr}(\alpha_i u_j)}$, являются элементами множества $Orb(j)$. Отсюда в силу определения $\mathrm{B}_\pi(m,k)$ заключаем, что $t \in \bigcup\limits_{j \in I_\pi(m,k)} Orb(j) = \Pi_k$. Лемма доказана. □

Следствие 6.2. *Пусть $t \in \overline{0,q-1}$ и $j \in \overline{0,l(p-1)}$. Пусть $\xi \in Q$. Пусть $\mathrm{Tr}(\xi u_t) \neq 0$. Тогда $\mathrm{Tr}(\xi u_t) \in \mathcal{RM}_p(l,j)$ тогда и только тогда, когда $t \in \mathrm{P}_j$.*

Доказательство. Непосредственно вытекает из предыдущей леммы при $\lambda = 1$. □

Следствие 6.3. *Пусть $k \in \overline{0,m(\pi-1)}$ и $j \in \overline{0,l(p-1)}$. Включение $\mathcal{RM}_\pi(m,k) \subseteq \mathcal{RM}_p(l,j)$ равносильно тому, что $\Pi_k \subseteq \mathrm{P}_j$. Включение $\mathcal{RM}_\pi(m,k) \supseteq \mathcal{RM}_p(l,j)$ равносильно тому, что $\Pi_k \supseteq \mathrm{P}_j$.*

Замечание 6.1. Легко видеть, что все утверждения о базисных кодах Рида–Маллера, которые можно сформулировать только относительно множеств Π_k и P_j, имеют аналоги для обычных кодов Рида–Маллера.

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*

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

Доказательство. В силу следствия 6.3 заключаем, что равенство $\mathcal{RM}_\pi(m,k) = \mathcal{RM}_p(l,j)$ равносильно тому, что $\Pi_k = \mathrm{P}_j$. При доказательстве теоремы 2.1 было показано, что последнее невозможно. Теорема доказана. □

6.3 Строение графа включений кодов Рида–Маллера и степеней радикала

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.

Лемма 6.5. *Пусть* $k \in \overline{0, m(\pi-1)-1}$, *тогда имеет место включение*

$$\mathfrak{R}_R\mathcal{RM}_\pi(m,k+1) \subseteq \mathcal{RM}_\pi(m,k).$$

Доказательство. По лемме 3.1 имеем $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1) \subseteq \mathcal{M}_\pi(m,k)$. Применяя к обеим частям данного включения функцию Tr, в силу утверждения 6.1 получаем $\mathfrak{R}_R\mathcal{RM}_\pi(m,k+1) \subseteq \mathcal{RM}_\pi(m,k)$, что завершает доказательство. □

Утверждение 6.4. *Пусть* $j \in \overline{2, l(p-1)}$, *тогда имеет место включение*

$$\mathcal{RM}_p(l, l(p-1)-j) \subset \mathcal{RM}_\pi(m, m(\pi-1)-j).$$

Доказательство. Согласно утверждениям 1.2 и 3.1 при указанных значениях j имеет место включение $\mathrm{P}_{l(p-1)-j} \subset \Pi_{m(\pi-1)-j}$, что завершает доказательство. □

Утверждение 6.5. *Пусть* $j \in \overline{1, l(p-1)}$, *тогда имеет место включение*

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

Доказательство. Согласно утверждениям 1.2 и 3.2 при указанных значениях j имеет место включение $\mathrm{P}_j \supset \Pi_j$, что завершает доказательство. □

6.3.1 Включения вида $\mathfrak{R}_R{}^{\alpha} \supset \mathcal{RM}_{\pi}(m,k)$

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:

$$\mathcal{RM}_{\pi}(m,k) \subset \mathfrak{R}_R{}^{\alpha}, \tag{16}$$

$$\mathcal{RM}_{\pi}(m,k) \nsubseteq \mathfrak{R}_R{}^{\alpha+1}, \tag{17}$$

$$\mathcal{RM}_{\pi}(m,k+1) \nsubseteq \mathfrak{R}_R{}^{\alpha}. \tag{18}$$

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

$$\mathfrak{R}_R\mathcal{RM}_{\pi}(m,k+1) = \mathcal{RM}_{\pi}(m,k), \tag{19}$$

тогда существует и притом единственное $\alpha \in \overline{1, l(p-1)-1}$ *такое, что имеют место соотношения* (16), (17), (18).

Доказательство. Доказательство повторяет доказательство теоремы 3.1, заменяя $\mathcal{M}_{\pi}(m,k)$ на $\mathcal{RM}_{\pi}(m,k)$ и $\mathfrak{R}_S$ на $\mathfrak{R}_R$. □

Утверждение 6.6.

$$\mathfrak{R}_R\mathcal{RM}_{\pi}(m,1) = \mathcal{RM}_{\pi}(m,0).$$

Доказательство. Непосредственно вытекает из утверждений 3.3 и 6.1. □

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* (16), (17), (18), *тогда выполнено равенство* (19).

Доказательство. Доказательство повторяет доказательство теоремы 3.2, заменяя $\mathcal{M}_{\pi}(m,k)$ на $\mathcal{RM}_{\pi}(m,k)$ и $\mathfrak{R}_S$ на $\mathfrak{R}_R$. □

Теорема 6.4. *Количество* $k \in \overline{0, m(\pi-1)-1}$ *таких, что выполнено равенство* (19), *равно* $l(p-1)$.

Доказательство. Согласно теоремам 3.3 и 3.4 количество $k \in \overline{0, m(\pi-1)-1}$ таких, что выполнено равенство (6), равно $l(p-1)$. Отсюда по следствию 6.1 заключаем, что количество $k \in \overline{0, m(\pi-1)-1}$ таких, что выполнено равенство (19), не меньше $l(p-1)$.

Откинув граничные случаи $k = 0$ и $k = m(\pi-1)-1$, получаем, что для каждого из оставшихся k по теореме 6.2 существует и притом единственное α такое, что имеют место соотношения (16), (17), (18). Несложно понять, что различным значениям k соответствуют различные α. Отсюда следует, что количество k таких, что выполнено равенство (19), не превосходит $l(p-1)$. Теорема доказана. □

Следствие 6.4. *Пусть* $k \in m(\pi-1)-1$. *Тогда равенство* (6) *выполнено тогда и только тогда, когда выполнено равенство* (19).

Замечание 6.2. Легко видеть, что все утверждения о базисных кодах Рида–Маллера, которые можно сформулировать только относительно равенства (6), имеют аналоги для обычных кодов Рида–Маллера.

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* (16), (17), (18).

Доказательство. Рассмотрим множество чисел k', для которых $j = l(p-1)-\alpha$ является наименьшим таким, что $\Pi_{k'} \subset \mathrm{P}_j$. В силу утверждения 6.2 и следствия 6.3 данное условие равносильно тому, что для k', α имеют место соотношения (16) и (17). Согласно утверждению 6.5 указанное множество непусто. Пусть k — максимальное среди k'. Легко видеть, что данное условие эквивалентно тому, что для k, α имеют место соотношения (16), (17), (18). □

Теорема 6.5. *Пусть* $\alpha \in \overline{1, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-2}$. *Соотношения* (16), (17), (18) *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* $0 \leqslant \tau < m(p-1)$.

Доказательство. В силу утверждений 3.9 и 6.7 соотношения (16), (17), (18) имеют место тогда и только тогда, когда имеют место соотношения (3), (4), (5). Дальнейшие рассуждения повторяют доказательство теоремы 3.5. □

6.3.2 Включения вида $\mathcal{RM}_{\pi}(m,k) \supset {\mathfrak{R}_R}^{\alpha}$

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:

$${\mathfrak{R}_R}^{\alpha} \subset \mathcal{RM}_{\pi}(m,k), \tag{20}$$

$${\mathfrak{R}_R}^{\alpha} \nsubseteq \mathcal{RM}_{\pi}(m,k-1), \tag{21}$$

$${\mathfrak{R}_R}^{\alpha-1} \nsubseteq \mathcal{RM}_{\pi}(m,k). \tag{22}$$

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* (20), (21), (22).

Доказательство. Рассмотрим множество чисел k' таких, что для $j = l(p-1)-\alpha$ имеет место включение $\mathrm{P}_j \subset \Pi_{k'}$. В силу утверждения 6.2 и следствия 6.3 данное условие равносильно тому, что для k', α имеет место соотношение (20). Согласно утверждению 6.4 указанное

множество непусто. Пусть k — минимальное среди k'. Легко видеть, что данное условие эквивалентно тому, что для k, α имеют место соотношения (20) и (21). Рассуждая тем же образом, что и при доказательстве утверждения 3.10, заключаем, что для k, α также имеет место соотношение (22), что завершает доказательство. □

Теорема 6.6. *Пусть* $\alpha \in \overline{2, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-1}$. *Соотношения* (20), (21), (22) *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* $0 \leqslant \tau < m(p-1)$.

Доказательство. В силу утверждений 3.10 и 6.8 соотношения (20), (21), (22) имеют место тогда и только тогда, когда имеют место соотношения (8), (9), (10). Дальнейшие рассуждения повторяют доказательство теоремы 3.6. □

Подводя итог раздела 6, отметим, что полученные результаты дают необходимые и достаточные условия, при которых вершины, соответствующие идеалам $\mathcal{RM}_\pi(m,k)$ и $\mathcal{RM}_p(l,j)$, соединены дугой в графе включений. Случай $\mathcal{RM}_p(l,j) \supset \mathcal{RM}_\pi(m,k)$ описывается с помощью теорем 6.2 и 6.3 и утверждения 6.7. Случай $\mathcal{RM}_\pi(m,k) \supset \mathcal{RM}_p(l,j)$ — с помощью утверждения 6.8. Теоремы 6.5 и 6.6 дают числовое описание указанных включений.

Доказана теорема 6.1, которая является аналогом теоремы 2.1 для обычных кодов Рида–Маллера. Как было отмечено ранее, совпадению кодов Рида–Маллера со степенями радикала в случае $\lambda \neq 1$ обычно уделяется мало внимания. В [7] аналогичный результат упомянут без доказательства. Автору не удалось найти доказательств указанной теоремы и в других источниках. Можно сказать, что теорема 6.1 не является абсолютно новым результатом, однако удовлетворительное доказательство оставалось до сих пор неизвестным.

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.

Список литературы

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

[2] 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.

[3] Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988.

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

[5] 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.

[6] Jennings S.A. The structure of the group ring of a p-group over a modular field // Trans. Amer. Math. Soc. 1941. Vol. 50, № 1. P. 175–185.

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

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

[9] Moore E.H. A two-fold generalization of Fermat's theorem // Bull. Amer. Math. Soc. 1896. Vol. 2, № 7. P. 189–199.

[10] Roman S. Field Theory. New York: Springer, 2006.

Работы автора по теме диссертации

[11] 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.

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

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

Приложение: графы включений базисных кодов Рида–Маллера и степеней радикала

Частные случаи основных результатов разделов 2, 3, 4 были сначала смоделированы и получены с помощью системы компьютерной алгебры GAP. Для построения графов включений базисных кодов Рида–Маллера и степеней радикала автором была написана программа на языке C. Исходный код данных программ доступен в Интернете по адресу `https://github.com/Coacher/rmc-inclusion`. Приведём здесь некоторые из полученных графов.

(a) $p = 2, l = 4, \lambda = 4$. (b) $p = 2, l = 6, \lambda = 2$.

Рис. 1: Графы включений при небольших значениях параметров.

При увеличении значений параметров количество вершин в графе также возрастает. Особенно быстро растёт количество идеалов $\mathcal{M}_\pi(m,k)$. Количество степеней радикала растёт медленнее. Полезны следующие упрощения: будем изображать только те из вершин $\mathcal{M}_\pi(m,k)$, которые связаны хотя бы одним ребром с некоторой степенью радикала, и группировать отдельно вершины, соответствующие степеням радикала и базисным кодам.

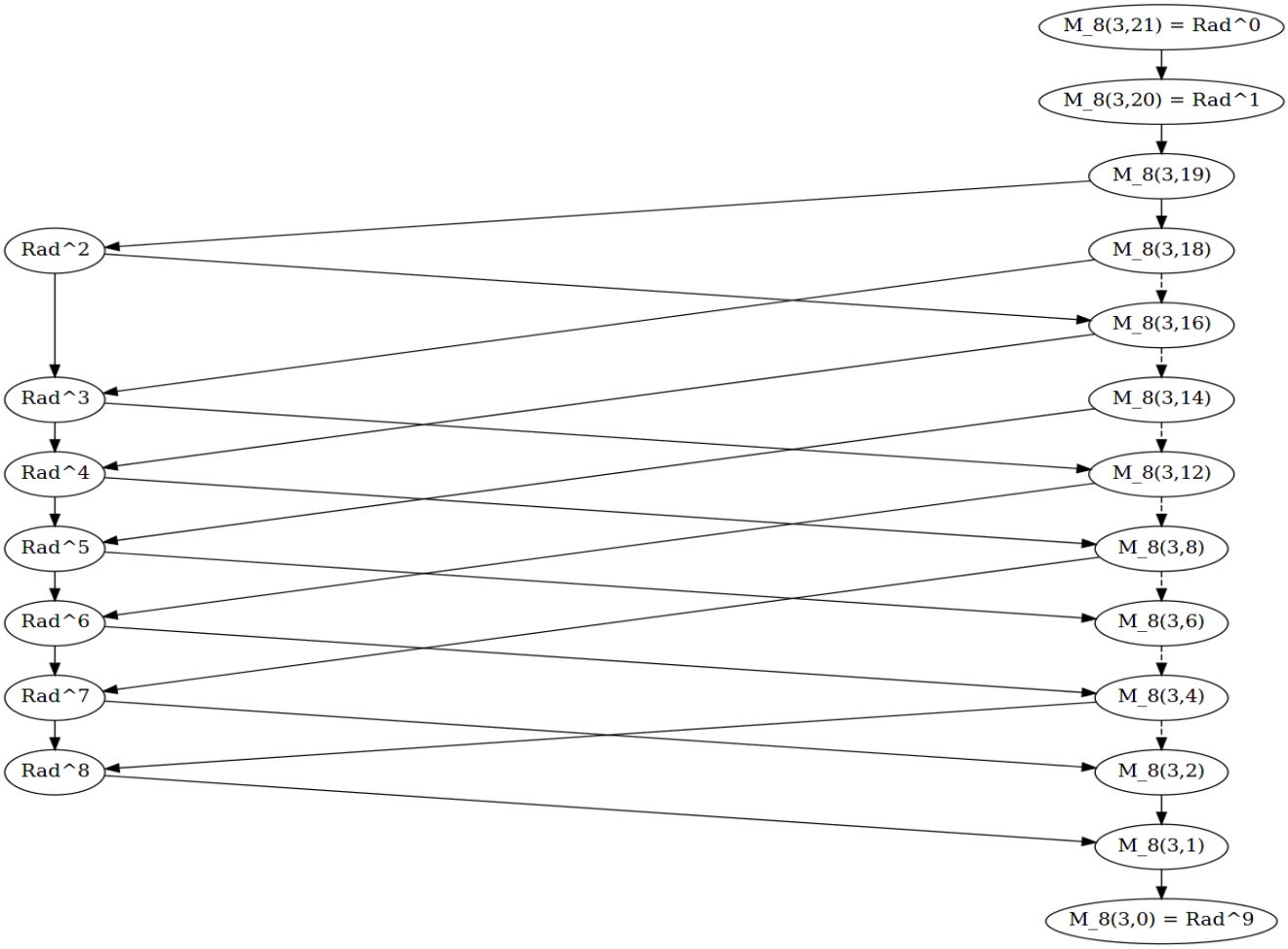

Рис. 2: Упрощённый граф включений для $p = 2, l = 9, \lambda = 3$.