Базисные коды Рида—Маллера как групповые коды

И. Н. ТУМАЙКИН
Московский государственный университет им. М. В. Ломоносова
e-mail: itumaykin@gmail.com

УДК 512.552.7+512.624.95

Ключевые слова: базисные коды Рида—Маллера, коды Рида—Маллера.

Аннотация

Коды Рида—Маллера являются одним из наиболее известных семейств кодов, однако некоторые вопросы об их структуре остаются открытыми до сих пор. Сравнительно недавно был предложен новый теоретико-кольцевой подход к их описанию, дающий достаточно наглядное построение указанных кодов и вводящий понятие базисных кодов Рида—Маллера. Как известно, коды Рида—Маллера над простыми полями совпадают со степенями радикала соответствующей групповой алгебры. В данной работе доказано отсутствие совпадений базисных кодов над непростым полем произвольной характеристики и степеней радикала, откуда следует отсутствие таких совпадений и для обычных кодов. Также получено полное описание графа включений между базисными кодами Рида—Маллера и степенями радикала с использованием простых числовых равенств.

Abstract

I. N. Tumaykin, Basic Reed–Muller codes as group codes, Fundamentalnaya i prikladnaya matematika, vol. 18 (2013), no. 4, pp. 137—154.

Reed—Muller codes are one of the most well-studied families of codes, however, there are still open problems regarding their structure. Recently, a new ring-theoretic approach has emerged that provides a rather intuitive construction of these codes. This approach is centered around the notion of basic Reed—Muller codes. We recall that Reed—Muller codes over a prime field are radical powers of a corresponding group algebra. In this paper, we prove that basic Reed—Muller codes in the case of a nonprime field of arbitrary characteristic are distinct from radical powers. This implies the same result for regular codes. Also we show how to describe the inclusion graph of basic Reed—Muller codes and radical powers via simple arithmetic equations.

1. Введение

Один из первых результатов, связанных с тематикой данной работы, был представлен в [2], где было показано, что над простым полем характеристики 2 коды Рида—Маллера совпадают со степенями радикала некоторой групповой

Фундаментальная и прикладная математика, 2013, том 18, № 4, с. 137—154.

алгебры. Известны обобщения этого факта на случай произвольной характеристики, (см. [1, 5]). Иногда под кодами Рида—Маллера понимаются коды над полями характеристики 2, а для кодов над полями произвольной характеристики вводится понятие обобщённых кодов Рида—Маллера. Мы рассматриваем коды Рида—Маллера как коды над полями произвольной характеристики.

2. Базисные коды Рида—Маллера

Пусть p — простое число и $q = p^l$, $l \geqslant 2$. Рассмотрим поле $Q = \mathbb{F}_q$ характеристики p и порядка q. Пусть группа $(H, \cdot)$ изоморфна аддитивной группе поля $(Q, +)$ и $\varphi\colon (H, \cdot) \to (Q, +)$ — указанный изоморфизм. Пусть также $q = \pi^m$, где $m \geqslant 1$, $l = \lambda m$, $\pi = p^\lambda$, $\lambda \geqslant 1$. Построим модулярную групповую алгебру $S = QH$. Как известно, её радикал имеет вид

$$\mathrm{Rad}(QH) = \mathfrak{R}_S = \left\{ \sum_{h\in H} \alpha_h h \in QH \;\middle|\; \sum_{h\in H} \alpha_h = 0 \right\} = \{a \in QH \mid a^p = 0\}.$$

Для заданного изоморфизма φ рассмотрим следующие элементы:

$$u_i = \sum_{h\in H} \big(\varphi(h)\big)^i h \in QH, \quad \text{где} \quad i \in \overline{0, q-1}.$$

Определение 2.1. π-весом числа i назовём сумму его координат в π-ричном разложении, обозначим π-вес $\omega_\pi(i)$. Заметим, что $\omega_\pi(i) \in \overline{0, (\pi-1)m}$ при $i \in \in \overline{0, q-1}$. Аналогично вводится p-вес.

Определение 2.2. Для всякого $k \in \overline{0, (\pi-1)m}$ определим базисный код Рида—Маллера порядка k над полем Q равенством

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

Замечание 2.1. Отметим, что

$$\mathcal{M}_\pi(m, 0) = Qu_0$$

и

$$\mathcal{M}_\pi\big(m, m(\pi-1)\big) = S.$$

Оба равенства вытекают из определения. Из [3] известно, что

$$\mathcal{M}_\pi(m, m(\pi-1)-1) = \mathrm{Rad}(S).$$

Приведём без доказательства известные факты, которые понадобятся нам в дальнейшем.

Утверждение 2.1 [3]. *$\mathcal{M}_\pi(m, k)$ — идеал в QH с кодовыми параметрами $[q, M_\pi(m, k), d_\pi(m, k)]$, где $M_\pi(m, k)$ — Q-размерность идеала $\mathcal{M}_\pi(m, k)$, которая равна числу таких расстановок $r \leqslant k$ шаров по m лункам, что в каждой*

лунке меньше π шаров:

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

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

Утверждение 2.2 [3]. $\operatorname{Ann}_S\big(\mathcal{M}_\pi(m,k)\big)=\mathcal{M}_\pi(m,m(\pi-1)-1-k)$, *где* $k\in\overline{0,m(\pi-1)-1}$.

3. Совпадения базисных кодов со степенями радикала в случае непростого поля

Напомним, что базисные коды под действием некоторого отображения «след», действующего из алгебры $S=QH$ в её подалгебру $R=PH$, переходят в обыкновенные коды Рида—Маллера над полем P, где $P=\mathbb{F}_\pi$ [3]. Отметим, что P задаётся параметром λ.

Хорошо известно [2, 5], что над простым полем $F=\mathbb{F}_p$ коды Рида—Маллера — это степени радикала групповой алгебры FH. Более того, соответствующие им (относительно отображения «след») базисные коды Рида—Маллера совпадают со степенями радикала QH [3]. Цель данного раздела — показать, что в случае непростого поля, т. е. при $\lambda\neq 1$, совпадений, кроме тривиальных случаев, нет.

Утверждение 3.1 [4]. *Количество различных ненулевых степеней радикала алгебры S равно $l(p-1)$ и*

$$\operatorname{Rad}(QH)^{l(p-1)}=Q\Bigg(\sum_{h\in H}\mathbb{1}_Q h\Bigg).$$

Утверждение 3.2. *Для всех целых $p\geqslant 2$ и $\lambda\geqslant 1$ имеет место неравенство*

$$\lambda(p-1)\leqslant(p^\lambda-1),\tag{1}$$

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

Доказательство. Случай $\lambda=1$ очевиден. Пусть теперь $\lambda>1$. Тогда неравенство (1) можно переписать в виде $\lambda<(p^\lambda-1)/(p-1)$. Производя сокращения в правой части, получаем $\lambda<1+p+\ldots+p^{\lambda-1}$. Число слагаемых справа равно λ, это завершает доказательство. □

Из предыдущего утверждения вытекает, что в общем случае все базисные коды не могут совпадать со степенями радикала. В самом деле, домножая обе части (1) на m, получаем, что $l(p-1) \leqslant m(\pi-1)$, причём равенство достигается лишь в случае $\lambda = 1$. Это значит, что для любого подполя Q, кроме простого, количество базисных кодов Рида—Маллера строго больше количества степеней радикала. Однако некоторые совпадения данных кодов со степенями радикала есть и в случае произвольного непростого подполя Q. Мы назовём эти случаи *тривиальными*.

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

Утверждение 3.3 [3]. $\mathcal{M}_p(l,j) = \mathrm{Rad}(QH)^{l(p-1)-j}$, *где* $0 \leqslant j \leqslant l(p-1)$.

Замечание 3.1. Для удобства в предыдущем утверждении рассматривается также и нулевая степень радикала, которую естественно положить равной QH. Далее везде под степенями радикала мы подразумеваем только положительные степени, если не указано противное.

Запишем утверждение 3.1 в введённых выше обозначениях и объединим его с результатами замечания 2.1 и утверждения 3.3.

Следствие 3.1. *Пусть* λ *— делитель* l *и* $\lambda \neq 1$. *Тогда* $\mathcal{M}_\pi(m,0) = \mathcal{M}_p(l,0)$, $\mathcal{M}_\pi(m, m(\pi-1)-1) = \mathcal{M}_p(l, l(p-1)-1)$ *и* $\mathcal{M}_\pi\big(m, m(\pi-1)\big) = \mathcal{M}_p\big(l, l(p-1)\big) = QH$.

Следующая теорема утверждает, что, кроме указанных выше тривиальных случаев, других совпадений нет.

Теорема 3.1. *Пусть* λ *— делитель* l *и* $\lambda \neq 1$. *Тогда для произвольных* j, k, *таких что* $1 \leqslant j \leqslant l(p-1)-2$ *и* $1 \leqslant k \leqslant m(\pi-1)-2$, *справедливо соотношение*

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

Доказательство. Будем доказывать от противного. Пусть для некоторых k, j выполнено равенство $\mathcal{M}_\pi(m,k) = \mathcal{M}_p(l,j)$. Идеалы $\mathcal{M}_\pi(m,k)$ и $\mathcal{M}_p(l,j)$ определяются как некоторая сумма элементов Qu_s. Значит, это равенство эквивалентно тому, что наборы элементов Qu_s, из которых получен каждый из идеалов, совпадают, так как элементы u_s образуют базис QH. А это в свою очередь эквивалентно совпадению множеств $\{0 \leqslant t \leqslant q-1 \mid \omega_p(t) \leqslant j\}$ и $\{0 \leqslant t \leqslant q-1 \mid \omega_\pi(t) \leqslant k\}$. Покажем, что это невозможно.

Определение 3.1.

$$P_j = \{0 \leqslant t \leqslant q-1 \mid \omega_p(t) \leqslant j\}, \quad \Pi_k = \{0 \leqslant t \leqslant q-1 \mid \omega_\pi(t) \leqslant k\}.$$

Рассмотрим указанное выше число j и соответствующее ему множество P_j. Для него найдётся минимальное k', такое что для всех $t \in P_j$ имеем $\omega_\pi(t) \leqslant k'$, т. е. $P_j \subseteq \Pi_{k'}$. Согласно нашему предположению $k = k'$, так как $P_j = \Pi_k$. Отсюда следует, что для данного j значение k однозначно определено. Мы покажем, что если $P_j \subseteq \Pi_k$, то найдётся число, лежащее в Π_k, но не лежащее в P_j, что противоречит нашему предположению.

Какой максимальный π-вес может быть среди всех чисел фиксированного p-веса? Чтобы ответить на этот вопрос, введём некоторые дополнительные понятия.

Определение 3.2. С каждым t, таким что $0 \leqslant t \leqslant q-1$, мы будем отождествлять два слова, каждое в своём алфавите. Числу t будет соответствовать слово длины l в алфавите из p элементов $\{0,\ldots,p-1\}$, а именно p-ричное разложение t. Также числу t будет соответствовать слово длины m в алфавите из π элементов $\{0,\ldots,\pi-1\}$, а именно π-ричное разложение t. Назовём эти слова соответственно p-записью и π-записью числа t. Элементы p-записи будем называть p-координатами, элементы π-записи — π-координатами.

Определение 3.3. Рассмотрим t, такое что $0 \leqslant t \leqslant q-1$. Разобьём его p-запись на m групп по λ элементов в каждой так, чтобы каждая такая группа соответствовала своей π-координате в π-записи этого числа. Это стандартная конструкция для случаев, когда рассматривается представление числа в двух системах счисления, у которых основание одной есть некоторая степень другой. Каждую такую группу будем называть λ-группой. Будем упорядочивать λ-группы по их позиции внутри p-записи. При этом самую левую группу мы будем называть старшей, а самую правую — младшей. Аналогично упорядочиваем элементы внутри λ-групп.

Определение 3.4. Для данного t, такого что $0 \leqslant t \leqslant q-1$, назовём i-слоем упорядоченный набор, полученный объединением i-х ($i \in \overline{0,\lambda-1}$) p-координат по всем λ-группам, Будем говорить просто о слое, если значение i ясно из контекста. На первом месте в i-слое стоит элемент из самой старшей λ-группы, на втором — из следующей за ней и т. д. Под весом i-слоя будем понимать сумму всех его элементов. Будем упорядочивать i-слои по значению i. При этом $(\lambda-1)$-слой будем называть старшим, а 0-слой — младшим.

Зафиксируем некоторый p-вес. Сначала выясним, как максимизировать π-вес одной λ-группы. Сделать это очень просто: следует заполнить группу так, чтобы как можно больший p-вес приходился на как можно более старшие разряды. Понятно, что при этом получается наибольшее значение соответствующей этой группе π-координаты. Аналогично происходит заполнение всех λ-групп в совокупности: сначала заполняем старший разряд в каждой группе, пока хватает p-веса или пока на старших позициях во всех группах не будут стоять числа $p-1$, потом переходим к следующему самому старшему незанятому разряду и т. д., т. е. заполнение происходит по слоям от старшего к младшему. Порядок заполнения в пределах одного i-слоя в разных λ-группах не имеет значения, так как они все равноправны в смысле вклада в результирующий π-вес. Для определённости в пределах одного слоя будем производить заполнение от самой старшей λ-группы к самой младшей.

Легко понять, что указанная процедура позволяет построить 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 указанной процедурой. Если веса соответствующих i-слоёв a и b совпадают, то у этих чи-

сел одинаковый π-вес. Если же a и b отличаются весом некоторых i-слоёв, то рассмотрим старший среди таких слоёв. Из описания процедуры следует, что вес данного i-слоя a строго меньше веса того же слоя b. Это значит, что в a значение какого-то разряда в этом i-слое уменьшилось в пользу какого-то разряда в более младшем слое a, а значит, результирующий вклад в π-вес тоже уменьшился. Таким образом, b имеет строго больший π-вес, чем a.

Наша процедура устроена так, что чем больший p-вес мы фиксируем, тем больший π-вес получаем в результате. Применительно к P_j это означает, что число с максимальным π-весом среди элементов P_j удовлетворяет следующим условиям: во-первых, оно получено по указанной процедуре с точностью до перестановок весов разрядов внутри i-слоёв, во-вторых, оно имеет p-вес, равный в точности j. Без ограничения общности можем считать, что p-запись этого числа имеет распределение весов, полностью совпадающее с нашей процедурой.

Обозначим это число t. Рассмотрим его $(\lambda-1)$-слой и младший элемент в нём. Если он не равен $p-1$, то все элементы в более младших слоях равны 0 по построению; если же он равен $p-1$, то перейдём к $(\lambda-2)$-слою и его младшему элементу и т. д. В какой-то момент мы либо переберём все слои, либо найдём в каком-то слое младший элемент, не равный $p-1$. Если мы перебрали все слои и такого элемента не встретили, это значит, что $\omega_p(t)=j=l(p-1)$, чего не может быть по условию. Если мы встретили такой элемент впервые только в самом младшем слое, причём все остальные элементы в этом слое равны $p-1$, а сам младший элемент равен $p-2$, это значит, что $\omega_p(t)=j=l(p-1)-1$, чего опять же не может быть по условию теоремы. Значит, в самом младшем слое на самой младшей позиции стоит число, строго меньшее $p-2$.

Рассмотрим $t'=t+1$. Из того, что $\omega_p(t)=j$ и $\omega_\pi(t)=k$, следует, что $\omega_p(t')=j+1$ и $\omega_\pi(t')=k+1$. Заметим, что у t' в самом младшем слое на самой младшей позиции стоит число, строго меньшее $p-1$. К t' применим погрупповое зеркальное отражение: внутри каждой λ-группы поменяем местами значения, стоящие на симметричных относительно середины данной группы позициях, т. е. поменяем местами первую и последнюю позиции, вторую и предпоследнюю и т. д. Полученное таким образом число обозначим $\tilde{t}$.

Заметим, что $\omega_p(\tilde{t})=\omega_p(t')=j+1$ и $\omega_\pi(\tilde{t})<\omega_\pi(t')=k+1$. В самом деле, так как число t построено по указанной выше процедуре, у него в пределах одной λ-группы значение произвольной p-координаты всегда больше значения любой более младшей p-координаты или равно ему, причём равенство возможно лишь в тех случаях, когда обе рассматриваемые p-координаты равны либо 0, либо $p-1$. Значит, если при отражении пара разрядов поменялась местами, то их общий вклад в π-вес уменьшился или остался таким же. Остаться таким же их вклад может лишь в том случае, когда на обеих позициях, которые мы переставили, стоит либо 0, либо $p-1$. На всех p-позициях 0 стоять не может, так как $t'>1$, случай со всеми $p-1$ также невозможен, так как у t' значение как минимум одной p-координаты меньше $p-1$.

Мы построили число $\tilde{t}$, π-вес которого не больше k, но его p-вес равен $j+1$, а значит, равенство $P_j=\Pi_k$ неверно, что завершает доказательство. $\square$

Замечание 3.2. Легко понять, что при операции зеркального отражения, применённой к числу, построенному по нашей процедуре, вклад в π-вес одной λ-группы может уменьшиться не менее чем на $p^{\lambda-1}-1$. Эта граница достигается, когда внутри группы на всех позициях, кроме младшей, стоят $p-1$, а на самой младшей позиции стоит $p-2$.

Следствие 3.2. *Пусть λ — делитель l и $\lambda \neq 1$. Тогда для произвольных j, k, таких что $1 \leqslant j \leqslant l(p-1)-2$ и $1 \leqslant k \leqslant m(\pi-1)-2$, справедливо соотношение*

$$M_\pi(m,k) \neq M_p(l,j).$$

Из следствия вытекает утверждение теоремы 3.1 для обычных кодов Рида—Маллера, так как они имеют такие же кодовые параметры, что и соответствующие им базисные коды [1].

4. Строение графа включений для базисных кодов Рида—Маллера и степеней радикала

Теорема 3.1 утверждает, что нет нетривиальных совпадений между базисными кодами Рида—Маллера и степенями радикала. Рассмотрим граф включений указанных идеалов, т. е. ориентированный граф, в котором вершины соответствуют идеалам и между двумя идеалами проходит дуга тогда и только тогда, когда один из них есть подмножество другого, при этом начало такой дуги — вершина, соответствующая надмножеству, а конец — вершина, соответствующая подмножеству. В этом графе есть два маршрута, соответствующие идеалам $\mathcal{M}_\pi(m,k)$ и $\mathcal{M}_p(l,j)$. Эти маршруты имеют три общие вершины, соответствующие тривиальным совпадениям. Отметим, что первый маршрут значительно длиннее второго. Здесь и далее везде 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 этих маршрутов? В этом разделе мы покажем, что такие включения всегда существуют, и дадим их числовое описание.

Утверждение 4.1 [3]. *Для любых $s,t \in \overline{0,q-1}$ имеют место соотношения*

$$u_s u_t = 0, \quad \text{если} \quad s+t \leqslant q-2;$$

$$u_s u_t = -(-1)^{t-\delta}\binom{t}{\delta}u_\delta = -(-1)^{s-\delta}\binom{s}{\delta}u_\delta, \quad \text{если} \quad s+t = q-1+\delta < 2(q-1);$$

$$u_{q-1}u_{q-1} = -(2u_{q-1}+e) = -u_0 - u_{q-1}.$$

Утверждение 4.1 — известный факт. Докажем результат, обобщающий лемму 5.1 из [3].

Утверждение 4.2. $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1) \subseteq \mathcal{M}_\pi(m,k)$, *где* $0 \leqslant k \leqslant m(\pi-1)$.

Доказательство. Пусть $u_s \in \mathfrak{R}_S$ и $u_t \in \mathcal{M}_\pi(m, k+1)$, т. е. $s \leqslant q-2$ и $\omega_\pi(t) \leqslant k+1$. Покажем, что $u_s u_t \in \mathcal{M}_\pi(m,k)$. Поскольку $\mathcal{M}_\pi(m,k+1)$ — идеал, то либо $u_s u_t = 0 \in \mathcal{M}_\pi(m,k)$, либо $u_s u_t = cu_\delta$, где $c \in \mathbb{F}_p^*$ и c определяется из утверждения 4.1. Из теоремы Люка следует, что при $c \neq 0$ p-координаты t и δ, которые мы обозначим t_i и δ_i, удовлетворяют неравенствам

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

Тогда π-координаты t и δ удовлетворяют тем же неравенствам. Из утверждения 4.1 и того, что $s \leqslant q-2$, заключаем, что $\delta < t$. А это значит, что $\omega_\pi(\delta) < \omega_\pi(t) \leqslant k+1$, т. е. $u_s u_t = cu_\delta \in \mathcal{M}_\pi(m,k)$. □

Легко убедиться, что

$$\mathfrak{R}_S \mathcal{M}_\pi\big(m, m(\pi-1)\big) = \mathfrak{R}_S \cdot (QH) = \mathfrak{R}_S = \mathcal{M}_\pi(m, m(\pi-1)-1).$$

Применяя утверждение 4.2, 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 его ещё раз, получаем

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

Повторно применяя аналогичные рассуждения и принимая во внимание теорему 3.1, получаем следствие.

Следствие 4.1. *$\mathcal{M}_p(l, l(p-1)-j) \subset \mathcal{M}_\pi(m, m(\pi-1)-j)$, где $2 \leqslant j \leqslant l(p-1)$.*

Докажем симметричный аналог следствия 4.1.

Утверждение 4.3. *$\mathcal{M}_p(l,j) \supset \mathcal{M}_\pi(m,j)$, где $1 \leqslant j \leqslant l(p-1)$.*

Доказательство. Доказательство проведём индукцией по j. Положим $j = 1$. Имеем

$$\mathcal{M}_p(l,1) = Qu_0 + Qu_1 + Qu_p + Qu_{p^2} + \ldots + Qu_{p^{l-1}}$$

и

$$\mathcal{M}_\pi(m,1) = Qu_0 + Qu_1 + Qu_{p^\lambda} + Qu_{p^{2\lambda}} + \ldots + Qu_{p^{(m-1)\lambda}}.$$

Тогда $\mathcal{M}_\pi(m,1) \subset \mathcal{M}_p(l,1)$, так как $l = \lambda m$.

Пусть теперь утверждение верно при $j \leqslant k$. Докажем его для $j = k+1$. Рассмотрим произвольное $u_t \in \mathcal{M}_\pi(m, k+1)$, т. е. $\omega_\pi(t) \leqslant k+1$. Для него найдётся число t', такое что $\omega_\pi(t') = k$ и $t = t' + \pi^i$, где $0 \leqslant i \leqslant m-1$. По предположению индукции $\omega_p(t') \leqslant k$, а значит, $\omega_p(t) \leqslant k+1$. В самом деле, из того, что $\pi^i = p^{\lambda i}$, следует, что p-запись t получается из p-записи t' прибавлением 1 к (λi)-й p-координате. Если при этом не произошло переноса разрядов, то $\omega_p(t) = \omega_p(t') + 1 \leqslant k+1$. Иначе $\omega_p(t)$ меньше $\omega_p(t')$ как минимум на $(p-1)-1 = p-2$, т. е. $\omega_p(t) \leqslant \omega_p(t') - (p-2) \leqslant k+1$. □

Замечание 4.1. Утверждение 4.3 сразу получается из утверждения 2.2 и следствия 4.1, если использовать тот факт, что любая групповая алгебра конечной группы — квазифробениусово кольцо.

Доказанные выше утверждения дают информацию о строении графа включений, но их недостаточно, чтобы полностью описать его. Наша цель — найти необходимые и достаточные условия, при которых два идеала $\mathcal{M}_\pi(m,k)$ и $\mathcal{M}_p(l,j)$ соединены дугой.

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

В этом подразделе мы исследуем 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. Отметим, что первая дуга всегда существует. Этот случай описывается следующими соотношениями:

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

$$\mathcal{M}_\pi(m,k)\not\subseteq\mathfrak{R}_S^{\alpha+1}, \tag{3}$$

$$\mathcal{M}_\pi(m,k+1)\not\subseteq\mathfrak{R}_S^\alpha. \tag{4}$$

Теорема 4.1. *Пусть для некоторого k, такого что $1\leqslant k\leqslant m(\pi-1)-2$, выполнено равенство $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1)=\mathcal{M}_\pi(m,k)$. Тогда найдётся α, такое что $2\leqslant\alpha\leqslant l(p-1)-1$ и выполнены соотношения* (2)—(4).

Доказательство. Пусть для некоторого $\alpha\in\overline{1,l(p-1)-1}$ выполнены условия (2) и (3). Очевидно, такое α всегда можно найти, причём единственным образом. Пусть теперь неверно (4), т. е. $\mathcal{M}_\pi(m,k+1)\subseteq\mathfrak{R}_S^\alpha$. Тогда, домножая обе части этого нестрогого включения на $\mathfrak{R}_S$, получаем, что $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1)\subseteq\subseteq\mathfrak{R}_S^{\alpha+1}$. Отсюда следует, что $\mathcal{M}_\pi(m,k)\subseteq\mathfrak{R}_S^{\alpha+1}$. Это противоречит (3), значит, (4) верно. Из (2)—(4) следует, что случай $\alpha=1$ невозможен. Теорема доказана. □

Замечание 4.2. Далее будет доказано обращение теоремы 4.1, но поскольку его доказательство значительно сложнее, сделаем некоторое отступление.

Остановимся подробнее на граничных случаях. Выше было доказано равенство $\mathfrak{R}_S\mathcal{M}_\pi\big(m,m(\pi-1)\big)=\mathcal{M}_\pi(m,m(\pi-1)-1)$. Докажем аналогичное равенство при $k=0$.

Утверждение 4.4.

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

Доказательство. Из утверждения 4.2 следует, что $\mathfrak{R}_S\mathcal{M}_\pi(m,1)\subseteq\mathcal{M}_\pi(m,0)$. Также $\mathcal{M}_\pi(m,0)=Qu_0$. Требуемое утверждение теперь вытекает из равенства $u_1u_{q-2}=cu_0$, где $c=1$. □

Следствие 4.2. *Пусть $\lambda=l$. Тогда*

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

Доказательство. Утверждение сразу следует из определения базисного кода. □

Утверждение 4.5.

1. *При* $p \neq 2$ *имеем* $\mathfrak{R}_S\mathcal{M}_\pi(m,2) = \mathcal{M}_\pi(m,1)$.
2. *При* $p = 2$, $\lambda \neq l$ *имеем* $\mathfrak{R}_S\mathcal{M}_\pi(m,2) = \mathcal{M}_\pi(m,1)$.
3. *При* $p = 2$, $\lambda = l$ *имеем* $\mathfrak{R}_S\mathcal{M}_\pi(m,2) = \mathcal{M}_\pi(m,0)$.

Доказательство. Докажем первое утверждение. Из утверждения 4.2 следует, что $\mathfrak{R}_S\mathcal{M}_\pi(m,2) \subseteq \mathcal{M}_\pi(m,1)$. Рассмотрим δ, такое что $u_\delta \in \mathcal{M}_\pi(m,1)$, т. е. $\delta = \pi^i$, где $0 \leqslant i \leqslant m-1$. Тогда для $s = q-1-\pi^i$, $t = \delta+\pi^i$ имеем, что $u_s \in \mathfrak{R}_S$, $u_t \in \mathcal{M}_\pi(m,2)$. Значит, $u_s u_t = cu_\delta$, где $c = \binom{2\pi^i}{\pi^i}$. По теореме Люка получаем, что $c \equiv_p \binom{2}{1} = 2$, откуда следует первое утверждение.

Теперь докажем второе утверждение. Опять рассмотрим δ, такое что $u_\delta \in \in \mathcal{M}_\pi(m,1)$. Пусть сначала $\delta = \pi^i$, где $1 \leqslant i \leqslant m-1$, т. е. δ — ненулевая степень двойки. Положив $s = q-2$, $t = \delta+1$, имеем, что $u_s \in \mathfrak{R}_S$, $u_t \in \mathcal{M}_\pi(m,2)$. Далее, $u_s u_t = cu_\delta$, где $c = -\binom{s}{\delta}$. Поскольку все 2-координаты s, за исключением самой младшей, равны 1, а у δ самая младшая 2-координата равна 0, как у степени двойки, то по теореме Люка заключаем, что $c \not\equiv_2 0$. Осталось рассмотреть случай $\delta = 1$. Положим $s = q-1-\pi$, $t = 1+\pi$. Тогда

$$c = -\binom{t}{\delta} = -\binom{1+\pi}{1} = -(1+\pi) \not\equiv_2 0.$$

Наконец, докажем третье утверждение. Из следствия 4.2 получаем, что $\mathcal{M}_\pi(m,2) = Qu_2 + \mathcal{M}_\pi(m,1)$. Значит, достаточно показать, что $\mathfrak{R}_S \cdot (Qu_2) \subseteq \subseteq \mathcal{M}_\pi(m,0)$. Это включение следует из равенств $u_{q-3}u_2 = cu_0$, где $c = \binom{2}{0} = 1$, и $u_{q-2}u_2 = cu_1$, где $c = \binom{2}{1} = 2 \equiv_2 0$. □

На примере этого утверждения видно, что случай $\lambda = l$ потребует отдельного рассмотрения. Докажем теперь обращение теоремы 4.1.

Теорема 4.2. *Пусть* λ *— делитель* l *и либо* $\lambda \neq l$, $\lambda \geqslant 1$, *либо* $\lambda = l$, $\lambda \geqslant 2$. *Пусть для некоторых целых* k *и* α, *таких что* $1 \leqslant k \leqslant m(\pi-1)-2$ *и* $2 \leqslant \alpha \leqslant \leqslant l(p-1)-1$, *выполнены соотношения* (2)—(4). *Тогда выполнено равенство* $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1) = \mathcal{M}_\pi(m,k)$.

Доказательство. Как показано ниже, число равенств вида

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

где $0 \leqslant k \leqslant m(\pi-1)-1$, равно числу степеней радикала. Откинув граничные случаи, получим, что для каждого такого равенства есть включение $\mathcal{M}_\pi(m,k)$ в соответствующую степень радикала по теореме 4.1, т. е. выполнены соотношения (2)—(4). Из того, что количество равенств совпадает с количеством степеней, следует, что выполнено и обращение теоремы 4.1, что завершает доказательство. □

Теорема 4.3. *Пусть λ — делитель l, такой что $\lambda \neq l$ и $\lambda \geqslant 1$. Тогда число равенств вида $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1) = \mathcal{M}_\pi(m,k)$, где $0 \leqslant k \leqslant m(\pi-1)-1$, равно $l(p-1)$.*

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

Рассмотрим произвольный элемент $u_{t'} \in \mathfrak{R}_S\mathcal{M}_\pi(m,k+1)$. Тогда

$$u_{t'} = \sum_{u_t \in \mathcal{M}_\pi(m,k+1)} r_t u_t,$$

где

$$r_t = \sum_{u_s \in \mathfrak{R}_S} \alpha_{t,s} u_s, \quad \alpha_{t,s} \in Q,$$

т. е.

$$u_{t'} = \sum \alpha_{t,s} u_s u_t.$$

Очевидно, что элементы $\{u_t \mid u_t \in \mathcal{M}_\pi(m,k+1)\}$ образуют базис $\mathcal{M}_\pi(m,k+1)$, элементы $\{u_t \mid u_t \in \mathcal{M}_\pi(m,k)\}$ образуют базис $\mathcal{M}_\pi(m,k)$ и элементы $\{u_0,\ldots,u_{q-2}\}$ образуют базис $\mathfrak{R}_S$. Из утверждения 4.1 тогда следует, что указанные элементы $u_s u_t$ линейно независимы в $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1)$. А значит, $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1) \subset \mathcal{M}_\pi(m,k)$ равносильно тому, что

$$\begin{aligned}&\text{найдётся } u_{t'} \in \mathcal{M}_\pi(m,k),\\ &\qquad\text{такой что } u_{t'} \notin \mathfrak{R}_S \cdot (Qu_t) \text{ для всех } u_t \in \mathcal{M}_\pi(m,k+1).\end{aligned} \quad (5)$$

Предположим, что у t' хоть одна (λi)-я, где $0 \leqslant i \leqslant m-1$, p-координата отлична от $p-1$. По условию имеем $\omega_\pi(t') \leqslant k$, значит, $\omega_\pi(t) = \omega_\pi(t')+1 \leqslant k+1$. Тогда для $s = q-1-\pi^i$ получаем $cu_{t'} = u_t u_s$, где $c = \pm\binom{t}{t'}$. Поскольку (λi)-я p-координата t' не равна $p-1$, то p-запись t получается из p-записи t' прибавлением 1 к данной p-координате и при этом не происходит переноса разрядов. По теореме Люка получаем, что $c \not\equiv_p 0$, а значит, для данного t' не выполнено (5).

Таким образом, приходим к выводу, что на роль t' в (5) подходят только числа, в p-записи которых элементы на всех (λi)-х, где $0 \leqslant i \leqslant m-1$, позициях равны $p-1$.

Определение 4.1. Числа t' такого вида, а также соответствующие им элементы $u_{t'}$ будем называть *особыми*.

Уточним (5): $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1) \subset \mathcal{M}_\pi(m,k)$ равносильно тому, что

$$\begin{aligned}&\text{найдётся } u_{t'} \in \mathcal{M}_\pi(m,k),\\ &\qquad\text{такой что } u_{t'} \notin \mathfrak{R}_S \cdot (Qu_t) \text{ для всех } u_t \in \mathcal{M}_\pi(m,k+1) \text{ и } t' \text{ особое}.\end{aligned} \quad (6)$$

Рассмотрим наименьшее особое число t'_0. В его p-записи на (λi)-х позициях стоят $p-1$, так как оно особое, а на остальных позициях стоят 0, так как оно наименьшее. Очевидно, что $\omega_p(t'_0) = \omega_\pi(t'_0) = m(p-1)$. Отсюда следует,

что для всех k, таких что $0 \leqslant k < m(p-1)$, равенство $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1) = \mathcal{M}_\pi(m,k)$ выполняется потому, что даже $u_{t'_0}$ не лежит в $\mathcal{M}_\pi(m,k)$, т. е. не выполнено (6). Это даёт нам $m(p-1)$ необходимых равенств. Остаётся найти ещё $l(p-1)-m(p-1) = \lambda m(p-1) - m(p-1) = m(\lambda-1)(p-1)$ равенств.

Введём на числах меньше q следующие отношения порядка.

Определение 4.2. $x \preceq_p y \iff$ никакая p-координата x не превосходит соответствующей p-координаты y.

Определение 4.3. $x \prec_p y \iff x \preceq_p y$ и $x \neq y$.

Заметим, что особое $u_{t'}$ может быть получено умножением на элементы радикала только из некоторого особого u_t, такого что $t' \prec_p t$. В самом деле, пусть t' — произвольное особое число и $cu_{t'} = u_t u_s$, где $u_s \in \mathfrak{R}_S$ и $c = \pm\binom{t}{t'}$. Из теоремы Люка следует, что $c \not\equiv_p 0$ только при условии, что каждая p-координата t не меньше соответствующей p-координаты t'. Значит, $t' \preceq_p t$, откуда следует, что t особое. Из утверждения 4.1 получаем, что $t' < t$, а значит, $t' \prec_p t$. Таким образом, мы доказали следующее утверждение.

Утверждение 4.6. *Равенство $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1) = \mathcal{M}_\pi(m,k)$ равносильно тому, что для всякого особого числа t', такого что $\omega_\pi(t') \leqslant k$, найдётся особое число t, такое что $\omega_\pi(t) \leqslant k+1$ и $t' \prec_p t$.*

Рассмотрим произвольное особое число t и исключим из его p-записи все (λi)-е позиции, где $0 \leqslant i \leqslant m-1$. Получим в результате некое новое число. Обозначим это отображение σ. Очевидно, что оно биективно и его образом являются всевозможные числа с p-записью длины $\tilde{l} = l - m = m(\lambda-1)$. Также при этом отображении λ-группы t естественным образом переходят в $(\lambda-1)$-группы $\sigma(t)$. Введём в рассмотрение $\tilde{\lambda} = \lambda - 1$. Тогда $\tilde{l} = m\tilde{\lambda}$ и $\tilde{\pi} = p^{\tilde{\lambda}} = p^{\lambda-1} = \pi/p$. Отметим также, что $\omega_p(t) = \omega_p\big(\sigma(t)\big) + m(p-1)$ и $\omega_\pi(t) = \omega_{\tilde{\pi}}\big(\sigma(t)\big)p + m(p-1)$.

По предположению индукции для $\tilde{l}$ и любого его делителя, отличного от самого $\tilde{l}$, найдётся $\tilde{l}(p-1)$ равенств вида

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

где $0 \leqslant \tilde{k} \leqslant m(\tilde{\pi}-1)-1$. Из того, что $\lambda \neq l$, следует, что $m \neq 1$, а значит, $\tilde{l} = m\tilde{\lambda} \neq \tilde{\lambda}$. Таким образом, предположение индукции можно применять к $\tilde{l}$, взяв в качестве делителя $\tilde{\lambda}$.

Утверждение 4.7. *Пусть p — произвольное простое число, l — произвольное положительное число и λ — произвольный делитель l, такой что $\lambda \geqslant 2$. Пусть $\tilde{\lambda} = \lambda - 1$, $\tilde{\pi} = p^{\tilde{\lambda}}$ и $\tilde{l} = m\tilde{\lambda}$, где $m = l/\lambda$. Пусть $S = QH$ как определено выше. Определим аналогично $\tilde{S} = \tilde{Q}\tilde{H}$. Пусть выполнено равенство $\mathfrak{R}_{\tilde{S}}\mathcal{M}_{\tilde{\pi}}(m,\tilde{k}+1) = \mathcal{M}_{\tilde{\pi}}(m,\tilde{k})$. Тогда выполнено равенство $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1) = \mathcal{M}_\pi(m,k)$, где $k+1 = (\tilde{k}+1)p + m(p-1)$ и $\tilde{k} \in \overline{0, m(\tilde{\pi}-1)-1}$.*

Замечание 4.3. Некоторая избыточность при формулировке этого утверждения связана, во-первых, с его универсальностью, так как мы не налагаем никаких условий на λ, лишь бы только $\tilde{\lambda}$ было положительным, во-вторых, с его

важностью для нас, так как оно позволяет найти недостающие равенства с помощью простых арифметических вычислений.

Доказательство. Сначала проверим, что верны необходимые верхние границы для k. В самом деле,

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

Покажем, что выполнены условия утверждения 4.6. Рассмотрим произвольное особое число t', такое что $\omega_\pi(t') \leqslant k$, и соответствующее ему $\sigma(t')$. Заметим, что $u_{\sigma(t')} \in \mathcal{M}_{\tilde{\pi}}(m, \tilde{k})$, так как

$$\omega_{\tilde{\pi}}\big(\sigma(t')\big) = \frac{\omega_\pi(t') - m(p-1)}{p} \leqslant \frac{k - m(p-1)}{p} = \tilde{k} + \frac{p-1}{p}.$$

По условию справедливо равенство

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

Значит, для $\sigma(t')$ найдётся число $\tilde{t}$, такое что $\omega_{\tilde{\pi}}(\tilde{t}) \leqslant \tilde{k}+1$ и $\tilde{c}u_{\sigma(t')} = u_{\tilde{t}}u_{\tilde{s}}$, где $u_{\tilde{s}} \in \mathfrak{R}_{\tilde{S}}$ и $\tilde{c} = \pm\binom{\tilde{t}}{\sigma(t')} \not\equiv_p 0$. Отображение σ биективно, значит, $\tilde{t} = \sigma(t)$ для некоторого целого t. Из того, что

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

следует, что $u_t \in \mathcal{M}_\pi(m, k+1)$. Далее, $\sigma(t') \prec_p \sigma(t)$ влечёт $t' \prec_p t$, откуда следует, что $c = \pm\binom{t}{t'} \not\equiv_p 0$ и $t' < t$. Значит, $s = q - 1 + t' - t \leqslant q - 2$. Отсюда получаем, что $cu_{t'} = u_t u_s$, где $u_s \in \mathfrak{R}_S$ и $c \not\equiv_p 0$. Таким образом, из утверждения 4.6 следует, что выполнено равенство $\mathfrak{R}_S\mathcal{M}_\pi(m, k+1) = \mathcal{M}_\pi(m, k)$. □

Только что доказанное утверждение даёт нам ещё $\tilde{l}(p-1) = m\tilde{\lambda}(p-1) = m(\lambda-1)(p-1)$ равенств, т. е. как раз столько, сколько нам не хватает. Значит, мы доказали шаг индукции.

Осталось проверить базу индукции. Заметим, что нигде выше не использовалось то, что $\lambda \neq l$. Шаг индукции позволяет сводить случай (p, l, λ) к случаю $(p, l-m, \lambda-1)$. Из того, что $\lambda \neq l$, следует, что $m \neq 1$. Отсюда получаем, что $l - m = \tilde{l} = m\tilde{\lambda} \neq \tilde{\lambda} = \lambda - 1$. Значит, достаточно рассмотреть лишь случаи $(p, l, 1)$, где p и l произвольные. Заметим, что случай $(p, l, 1)$ — это случай простого подполя, при котором базисные коды совпадают со степенями радикала S, т. е. равенства $\mathfrak{R}_S\mathcal{M}_\pi(m, k+1) = \mathcal{M}_\pi(m, k)$ выполнены при всех возможных k, которые в данном случае удовлетворяют условию $0 \leqslant k \leqslant l(p-1)-1$. Таким образом, в случае $(p, l, 1)$ мы нашли $l(p-1)$ необходимых равенств, что завершает доказательство теоремы. □

В ходе доказательства этой теоремы были также доказаны утверждения, которые представляют самостоятельную ценность и понадобятся нам в дальнейшем. Выделим их отдельно.

Следствие 4.3. *При всех* $k \in \overline{0, m(p-1)-1}$ *верно*

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

Отметим утверждение 4.6, которое позволяет описывать равенства вида $\mathfrak{R}_S\mathcal{M}_\pi(m, k+1) = \mathcal{M}_\pi(m, k)$ с помощью особых чисел. Заметим, что при доказательстве утверждения не использовалось, что $\lambda \neq l$.

Также отметим утверждение 4.7, которое позволяет сводить задачу поиска указанных равенств к более простому случаю. Вместе со следствием 4.3 оно даёт полное и конструктивное описание всех равенств указанного вида. При доказательстве этого утверждения также не используется тот факт, что $\lambda \neq l$.

Докажем теперь аналог теоремы 4.3 для случая $\lambda = l$.

Теорема 4.4. *Пусть* $\lambda = l$ *и* $\lambda \geqslant 2$. *Тогда число равенств вида*

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

где $0 \leqslant k \leqslant m(\pi-1)-1$, *равно* $l(p-1)$.

Доказательство. Доказательство проведём индукцией по l. Шаг индукции доказывается так же, как и в предыдущей теореме. Изменится только база индукции. Шаг индукции позволяет сводить случай (p, l, λ) к случаю $(p, l-m, \lambda-1)$. Из того, что $\lambda = l$, следует, что $m = 1$. Отсюда получаем, что $l - m = \tilde{l} = m\tilde{\lambda} = \tilde{\lambda} = \lambda - 1$. Значит, достаточно рассмотреть лишь случаи $(p, 2, 2)$, где p — произвольное простое число.

Сначала рассмотрим случай $p = l = \lambda = 2$. Нам требуется найти $l(p-1) = 2$ равенства, и оба эти равенства получаются как граничные случаи, т. е.

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

и

$$\mathfrak{R}_S\mathcal{M}_\pi(m, 3) = \mathfrak{R}_S\mathcal{M}_\pi\big(m, m(\pi-1)\big) = \mathcal{M}_\pi(m, m(\pi-1)-1) = \mathcal{M}_\pi(m, 2).$$

Теперь нам понадобится вспомогательное утверждение.

Утверждение 4.8. *Пусть* $l = \lambda = 2$. *Тогда имеют место равенства*

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

где $i \in \overline{1, p-1}$.

Доказательство. Доказательство проведём индукцией по i. Сначала проверим базу индукции.

Пусть $i = 1$, $p \neq 2$ и $\lambda = l = 2$. Рассмотрим наименьшее особое число t'_0. Тогда $u_{t'_0} \in \mathcal{M}_\pi(1, p-1)$ и $u_{t'_0} \notin \mathcal{M}_\pi(1, p-2)$. Рассмотрим все числа t, такие что $t'_0 \prec_p t$, и пусть t_1 — число наименьшего π-веса среди таких t. Тогда t_1 особое, $u_{t_1} \in \mathcal{M}_\pi(1, (p-1)+p)$ и все особые элементы $u_{t''}$, такие что $\omega_\pi(t'') = \omega_\pi(t_1)$, лежат в $\mathcal{M}_\pi(1, (p-1)+p)$. В самом деле, поскольку $\lambda = 2$, то у всех особых чисел в каждой λ-группе нефиксированная только одна p-координата. Рассмотрим p-запись t'_0 и прибавим 1 к любой нефиксированной p-координате, получим p-запись числа t_1. Таким образом, $\omega_\pi(t_1) = \omega_\pi(t'_0)+p = (p-1)+p$, $t'_0 \prec_p t_1$ и t_1 имеет

минимальный π-вес среди всех чисел t, таких что $t'_0 \prec_p t$. Из утверждения 4.6 выводим, что $\mathfrak{R}_S\mathcal{M}_\pi(1,(p-1)+p) = \mathcal{M}_\pi(1,(p-1)+p-1)$.

Пусть теперь равенство $\mathfrak{R}_S\mathcal{M}_\pi(1,(p-1)+jp) = \mathcal{M}_\pi(1,(p-1)+jp-1)$ выполнено для всех $j \in \overline{1,i-1}$. Докажем, что оно верно для $j=i$. Рассмотрим все особые элементы $u_t \in \mathcal{M}_\pi(1,(p-1)+(i-1)p)$, такие что $\omega_\pi(t) = (p-1)+(i-1)p$. Легко понять, что это множество непусто и все такие u_t лежат в $\mathcal{M}_\pi(1,(p-1)+ip-1)$, так как $\omega_\pi(t) = (p-1)+(i-1)p < (p-1)+ip-1$. Заметим также, что у всех соответствующих чисел t есть хотя бы одна p-координата, отличная от $p-1$, так как $i \leqslant p-1$. В самом деле,

$$\omega_\pi(t) = (p-1)+(i-1)p \leqslant (p-1)p-1 < (p-1)(p+1) = p^2-1 = \pi-1 = q-1.$$

Значит, для каждого такого t найдётся число t', такое что $t \prec_p t'$ и $u_{t'} \in \mathcal{M}_\pi(1,(p-1)+ip)$. Чтобы получить искомое t', прибавим 1 к p-координате t, отличной от $p-1$. Заметим, что при этом $\omega_p(t') = \omega_\pi(t)+p = (p-1)+ip$ и $t \prec_p t'$. Таким образом, выполнены условия утверждения 4.6, откуда следует, что выполнено равенство $\mathfrak{R}_S\mathcal{M}_\pi(1,(p-1)+ip) = \mathcal{M}_\pi(1,(p-1)+ip-1)$. □

Замечание 4.4. Хотя в предыдущем утверждении рассмотрен только случай $p \neq 2$ и $\lambda = l = 2$, оно верно для произвольных l. Необходимо потребовать только $p \neq 2$ и $\lambda = 2$. В самом деле, случай $l \neq \lambda$ является следствием утверждения 4.7. Случай $i = 0$ описывается следствием 4.3.

Доказанное только что утверждение даёт нам $p-2$ равенств, ещё $p-1$ равенство получается из следствия 4.3. Всего получается $p-1+p-1 = 2(p-1) = l(p-1)$ равенств, что завершает доказательство теоремы. □

Таким образом, из теорем 4.3 и 4.4 следует теорема 4.2, дающая обращение теоремы 4.1.

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

В этом подразделе мы исследуем второй тип включений, а именно дуги из базисных кодов в степени радикалов. Напомним, что утверждение 3.3 устанавливает биективное соответствие между степенями радикала и идеалами $\mathcal{M}_p(l,j)$. Рассмотрим вершину, соответствующую идеалу $\mathcal{M}_p(l,j)$, в которую входят два направленных ребра: первое выходит из вершины, соответствующей $\mathcal{M}_p(l,j+1)$, а второе выходит из вершины, соответствующей $\mathcal{M}_\pi(m,k)$ для некоторого k. Отметим, что первая дуга всегда существует. Эта ситуация описывается следующими соотношениями:

$$\mathcal{M}_p(l,j) \subset \mathcal{M}_\pi(m,k), \tag{7}$$

$$\mathcal{M}_p(l,j) \not\subseteq \mathcal{M}_\pi(m,k-1), \tag{8}$$

$$\mathcal{M}_p(l,j+1) \not\subseteq \mathcal{M}_\pi(m,k). \tag{9}$$

Теорема 4.5. *Пусть для некоторых целых k и j, таких что $1 \leqslant k \leqslant m(\pi-1)-2$ и $1 \leqslant j \leqslant l(p-1)-2$, выполнены соотношения* (7)—(9).

Тогда

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

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

Доказательство. Рассмотрим множество P_j. Для него существует минимальное число k', такое что $P_j \subset \Pi_{k'}$. Заметим, что для j и k' выполняются соотношения (7)—(9). В самом деле, соотношения (7), (8) выполнены по построению k'. Напомним, что в доказательстве теоремы 3.1 была рассмотрена процедура построения числа максимального π-веса среди всех чисел фиксированного p-веса. Из её описания следует, что найдётся число t, такое что $\omega_p(t) = j$, $\omega_\pi(t) = k'$ и самая младшая p-координата t отлична от $p-1$. Рассмотрим $t' = t+1$. Тогда получаем, что $\omega_p(t') = j+1$ и $\omega_\pi(t') = k'+1$. Значит, $P_{j+1} \not\subset \Pi_{k'}$, т. е. выполнено (9). Наоборот, очевидно, что если для данных k и j выполнены соотношения (7)—(9), то k является минимальным целым, таким что $P_j \subset \Pi_k$. Значение такого k однозначно определяется значением j по следующему алгоритму.

1: $i \leftarrow 0$, $k \leftarrow 0$
2: $\theta \leftarrow [j/m(p-1)]$, $\tau \leftarrow j \bmod m(p-1)$
   ◁ Здесь $m(p-1)$ — p-вес необходимый для заполнения одного i-слоя.
3: if $\theta = 0$ then
4: $\quad k \leftarrow k + \tau p^{\lambda-1-i}$
5: $\quad$ return k
6: else
7: $\quad k \leftarrow k + m(p-1)p^{\lambda-1-i}$
8: $\quad j \leftarrow j - m(p-1)$
9: $\quad i \leftarrow i+1$
10: $\quad$ go to 2
11: end if

Легко убедиться, что этот алгоритм действительно соответствует нашей процедуре. В самом деле, процедура определена следующим образом: сначала происходит заполнение самой старшей позиции во всех λ-группах, что даёт вклад $p^{\lambda-1}$ в π-вес, далее — следующей старшей позиции во всех λ-группах, что даёт вклад $p^{\lambda-1-1}$, и т. д.

Результирующее значение k можно вычислить по формуле:

$$k = \sum_{i=0}^{\theta-1} m(p-1)p^{\lambda-1-i} + \tau p^{\lambda-1-\theta}, \tag{10}$$

где θ и τ — частное и остаток от деления j на $m(p-1)$ соответственно.

Для доказательства в обратную сторону достаточно заметить, что, если данные j и k удовлетворяют (10), то k — наименьшее целое, такое что $P_j \subset \Pi_k$, а это эквивалентно выполнению условий (7)—(9), что завершает доказательство. □

В заключение получим аналогичную формулу для случая, описываемого соотношениями (2)—(4). Зафиксируем целое $j = l(p-1) - \alpha$. Рассмотрим все числа k', такие что данное j есть наименьшее целое, удовлетворяющее условию $\Pi_{k'} \subset P_j$. Среди всех таких k' выберем максимальное k_j. Легко убедиться, что k_j и α удовлетворяют соотношениям (2)—(4). Аналогично несложно показать, что указанные соотношения выполнены для данных k и α тогда и только тогда, когда k — максимальное число среди всех k', таких что $j = l(p-1) - \alpha$ есть наименьшее целое, удовлетворяющее условию $\Pi_{k'} \subset P_j$, т. е. $k = k_j$. Заметим, что если $j_1 \neq j_2$, то $k_{j_1} \neq k_{j_2}$. Более того, если $j_1 > j_2$, то $k_{j_1} > k_{j_2}$.

Выше было доказано, что соотношения (2)—(4) равносильны выполнению равенства

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

Некоторые из этих равенств (мы назовём их *нижними*) получаются из следствия 4.3, а другие (мы назовём их *верхними*) получается поднятием, как описано в утверждении 4.7. Будем считать все указанные равенства упорядоченными по возрастанию k.

Пусть φ — функция, соответствующая операции поднятия из утверждения 4.7, т. е. $\varphi\colon \mathbb{N} \to \mathbb{N}$ и $\varphi(t) = p(t+1) + m(p-1) - 1$. Очевидно, что φ строго возрастает. Значит, первые $m(p-1)$ верхних равенств в (p, l, λ) получаются поднятием нижних в $(p, l-m, \lambda-1)$, следующие $m(p-1)$ верхних равенств в (p, l, λ) получаются поднятием первых $m(p-1)$ верхних в $(p, l-m, \lambda-1)$, которые, в свою очередь, получаются поднятием нижних в $(p, l-2m, \lambda-2)$. Повторяя аналогичные рассуждения, приходим к выводу, что i-я группа из $m(p-1)$ верхних равенств в (p, l, λ) получается i-кратным поднятием нижних равенств в $(p, l-im, \lambda-i)$, где $i \in \overline{1, \lambda-1}$. Заметим, что в случае $i = \lambda - 1$ происходит поднятие из простого подполя, где все равенства являются нижними. Поскольку φ строго возрастает, то n-е нижнее равенство в $(p, l-im, \lambda-i)$ перейдёт в n-е верхнее равенство внутри i-й группы из $m(p-1)$ верхних равенств в (p, l, λ), где $n \in \overline{0, m(p-1)-1}$.

Таким образом, k_j равно k в j-м равенстве $\mathfrak{R}_S \mathcal{M}_\pi(m, k+1) = \mathcal{M}_\pi(m, k)$. В случае $j < m(p-1)$ по следствию 4.3 получаем, что $k_j = j$. В случае $j \geqslant m(p-1)$ j-е равенство получается θ-кратным поднятием τ-го нижнего равенства в $(p, l-\theta m, \lambda-\theta)$, где θ и τ — частное и остаток от деления j на $m(p-1)$ соответственно, т. е. $j = m(p-1)\theta + \tau$, где $0 \leqslant \tau < m(p-1)$. Таким образом, мы доказали следующее утверждение.

Утверждение 4.9. *Пусть k и α — целые числа, такие, что $1 \leqslant k \leqslant m(\pi-1)-2$ и $2 \leqslant \alpha \leqslant l(p-1)-1$. Пусть выполнены соотношения (2)—(4). Тогда $k = \varphi^\theta(\tau)$, где θ и τ — частное и остаток от деления $j = l(p-1) - \alpha$ на $m(p-1)$ соответственно, $\varphi(t) = p(t+1) + m(p-1) - 1$ и $\varphi^0(t) = t$. Верно и обратное.*

Литература

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

[2] Berman S. D. On the theory of group codes // Kibernetika. — 1967. — Vol. 3. — P. 31—39.

[3] Couselo E., Gonzalez S., Markov V., Martinez C., Nechaev A. Ideal representation of Reed—Solomon and Reed—Muller codes // Algebra Logic. — 2012. — Vol. 51, no. 3. — P. 195—212.

[4] Jennings S. A. The structure of the group ring of a p-group over a modular field // Trans. Am. Math. Soc. — 1941. — Vol. 50. — P. 175—185.

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