Строение кодов Рида—Маллера над непростым полем

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

УДК 512.715

Ключевые слова: коды Рида—Маллера.

Аннотация

Известно, что коды Рида—Маллера над простым полем совпадают со степенями радикала соответствующей групповой алгебры. Вопрос о совпадении кодов Рида—Маллера и степеней радикала в случае непростого поля оставался без подробного рассмотрения. Вопрос об условиях, описывающих теоретико-множественные включения между кодами Рида—Маллера и степенями радикала, оставался полностью неисследованным. В данной работе доказано отсутствие нетривиальных совпадений кодов Рида—Маллера над непростым полем со степенями радикала соответствующей групповой алгебры и получены необходимые и достаточные условия теоретико-множественных включений между кодами Рида—Маллера и степенями радикала этой алгебры.

Abstract

I. N. Tumaykin, The structure of Reed–Muller codes over a nonprime field, Fundamentalnaya i prikladnaya matematika, vol. 23 (2020), no. 3, pp. 231—258.

It is well known that Reed–Muller codes over a prime field are radical powers of a corresponding group algebra. The case of a nonprime field is less studied in terms of equalities and inclusions between Reed–Muller codes and radical powers. In this paper, we prove that Reed–Muller codes in the case of a nonprime field of arbitrary characteristic are distinct from radical powers and provide necessary and sufficient conditions for inclusions between these codes and the powers of the radical.

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 $\phi\colon (H, \cdot) \to (Q, +)$ — указанный выше изоморфизм.

Фундаментальная и прикладная математика, 2020, том 23, № 3, с. 231—258.
© 2020 *Национальный Открытый Университет «ИНТУИТ»*

Рассмотрим следующие элементы:

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

Определение 1.1. Назовём π-весом числа i сумму цифр в его π-ичном представлении и обозначим π-вес $\omega_\pi(i)$. 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

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

Множество $\mathcal{M}_\pi(m,k)$ является идеалом в S и определяет линейный код $\mathcal{K}$ длины q в алфавите Q следующим образом:

$$\mathcal{K} = \left\{(x_1, x_2, \ldots, x_q) \in Q\colon \sum_{i=1}^{q} x_i h_i \in \mathcal{M}_\pi(m,k)\right\},$$

где $H = \{h_1, \ldots, h_q\}$ — некоторое упорядочение элементов группы H.

Замечание 1.1. Известно, что $\mathcal{M}_\pi\big(m(\pi-1)\big) = S$ и $\mathcal{M}_\pi(m, m(\pi-1)-1) = \mathfrak{R}_S$ [2]. Непосредственно из определения следует, что $\mathcal{M}_\pi(m,0) = Qu_0$.

Утверждение 1.1 [2]. *Множество* $\{u_i\colon i \in \overline{0,q-1},\ 0 \leqslant \omega_\pi(i) \leqslant k\}$ *— базис* $\mathcal{M}_\pi(m,k)$.

Определение 1.3 [5]. Функцию следа tr_P^Q из поля Q в поле P определим равенством

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

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

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

Утверждение 1.2 [2]. $\mathrm{Tr}\colon S \to R$ *— 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 1.3 [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.

Замечание 1.2. Далее будем называть коды Рида—Маллера обычными кодами Рида—Маллера, чтобы отличать их от базисных кодов Рида—Маллера.

Большая часть дальнейших результатов опирается на следующие известные факты.

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

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

$$u_s u_t = c_\delta u_\delta, \quad \text{где} \quad c_\delta = -(-1)^{t-\delta}\binom{t}{\delta} = -(-1)^{s-\delta}\binom{s}{\delta},$$

$$\text{если} \quad s + t = q - 1 + \delta < 2(q-1);$$

$$u_{q-1}u_{q-1} = -u_0 - u_{q-1}.$$

Замечание 1.3. Отметим, что $c_\delta \in \mathbb{F}_p$.

Теорема 1.1 (Люка [6]). *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* $m_i < n_i$, *то* $\binom{m}{n} \equiv 0 \bmod p$.

Лемма 1.2 [3]. *Пусть* $k \in \overline{0, m(\pi-1)-1}$. *Тогда имеет место включение*

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

Лемма 1.3 [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* $c_\delta \in {\mathbb{F}_p}^*$.

1.1. Совпадения и включения между базисными кодами Рида—Маллера и степенями радикала $\mathfrak{R}_S$

Все полученные в данной работе результаты для обычных кодов Рида—Маллера основаны на приведённых ниже известных результатах для базисных кодов.

Совпадения базисных кодов со степенями радикала $\mathfrak{R}_S$ в случае простого подполя описываются следующим утверждением.

Утверждение 1.4 [2]. *Пусть* $j \in \overline{0, l(p-1)}$. *Тогда выполнено равенство*

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

Напомним, что при $\lambda \neq 1$ есть только тривиальные совпадения базисных кодов Рида—Маллера и степеней радикала $\mathfrak{R}_S$.

Утверждение 1.5 [3]. *Пусть* $\lambda \neq 1$. *Тогда выполнены равенства*

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

Теорема 1.2 [3]. *Пусть* $\lambda \neq 1$, $k \in \overline{1, m(\pi-1)-2}$ *и* $j \in \overline{1, l(p-1)-2}$. *Тогда имеет место соотношение*

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

Определение 1.6. Определим множества P_j и Π_k равенствами

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

Следствие 1.2 [3]. *Пусть* $\lambda \neq 1$, $k \in \overline{1, m(\pi-1)-2}$ *и* $j \in \overline{1, l(p-1)-2}$. *Тогда имеет место соотношение*

$$\Pi_k \neq \mathrm{P}_j.$$

Поскольку в случае $\lambda \neq 1$ нет нетривиальных совпадений базисных кодов со степенями радикала, естественно рассмотреть теоретико-множественные включения между ними.

Утверждение 1.6 [3]. *Пусть* $j \in \overline{2, l(p-1)}$. *Тогда имеет место включение*

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

Утверждение 1.7 [3]. *Пусть* $j \in \overline{1, l(p-1)}$. *Тогда имеет место включение*

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

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 1.4 и 1.5 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.

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

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

$$\mathcal{M}_\pi(m,k) \not\subseteq {\mathfrak{R}_S}^{\alpha+1}, \tag{2}$$

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

Данный случай описывается следующими известными фактами.

Теорема 1.3 [3]. *Пусть для некоторого* $k \in \overline{1, m(\pi-1)-2}$ *выполнено равенство*

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

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

Теорема 1.4 [3]. *Пусть* $\alpha \in \overline{1, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-2}$ *такие, что имеют место соотношения* (1)—(3)*. Тогда выполнено равенство* (4)*.*

Утверждение 1.8 [3]. *Пусть* $\alpha \in \overline{1, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-2}$*. Тогда соотношения* (1)—(3) *имеют место тогда и только тогда, когда* k *— максимальное среди чисел* k'*, для которых* $j = l(p-1)-\alpha$ *является наименьшим таким, что* $\Pi_{k'} \subset \mathrm{P}_j$*.*

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

Теорема 1.5 [3]. *Пусть* $\alpha \in \overline{1, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-2}$*. Соотношения* (1)—(3) *имеют место тогда и только тогда, когда*

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

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

Отметим также граничные случай равенства (4) при $k = 0$.

Утверждение 1.9 [3]. $\mathfrak{R}_S \mathcal{M}_\pi(m, 1) = \mathcal{M}_\pi(m, 0)$.

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

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

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

$${\mathfrak{R}_S}^{\alpha-1} \not\subset \mathcal{M}_\pi(m, k). \tag{7}$$

Данный случай описывается следующими известными фактами.

Утверждение 1.10 [3]. *Пусть* $\alpha \in \overline{2, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-1}$*. Число* k *является минимальным таким, что для* $j = l(p-1)-\alpha$ *имеет место включение* $\mathrm{P}_j \subset \Pi_k$*, тогда и только тогда, когда имеют место соотношения* (5)—(7)*.*

Теорема 1.6 [3]. *Пусть* $\alpha \in \overline{2, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-1}$*. Соотношения* (5)—(7) *имеют место тогда и только тогда, когда выполнено равенство*

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

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

2. Базисы кодов Рида—Маллера

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 $\mathcal{RM}_\pi(m,k)$. Введём необходимые определения.

Определение 2.1. π-записью числа t назовём его π-ичное представление, обозначим π-запись через $[t]_\pi$. 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.

2.1. Элементы $\mathrm{Tr}(u_i)$

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

Определение 2.2. Пусть $S_\pi\colon \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0}$ — циклический сдвиг π-записи числа t на одну позицию влево: если $[t]_\pi = [t_n, t_{n-1}, \dots, t_1, t_0]$, то $S_\pi(t) = \tilde{t}$, где $[\tilde{t}]_\pi = [t_{n-1}, \dots, t_1, t_0, t_n]$.

Лемма 2.1. *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 $[t]_\pi = [t_{m-1}, t_{m-2}, \dots, t_1, t_0]$. Тогда

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

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 $[\tilde{t}]_\pi = [t_{m-2}, \dots, t_1, t_0, t_{m-1}]$. 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 2.1. Пусть $t \in \overline{0,q-1}$. Несложно понять, что $S_\pi^m(t) = t$.

Далее будем рассматривать только ограничение S_π на $\{0,1,\dots,q-1\}$, 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 2.2. *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

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

Положим

$$\tilde{t} = t\pi^k - t_{m-1}\pi^{k-1}(q-1) - t_{m-2}\pi^{k-2}(q-1) - \ldots - t_{m-k}(q-1).$$

Легко видеть, что $\tilde{t} = S_\pi^k(t)$. Дальнейшие рассуждения повторяют доказательство леммы 2.1. □

Определение 2.3. Рассмотрим действие группы $\langle S_\pi \rangle_m$ на $\{0, 1, \ldots, q-1\}$. Напомним, что орбита числа t определена равенством

$$\operatorname{Orb}(t) = \{S_\pi^k(t) \colon k \in \overline{1, m}\},$$

а стабилизатор числа t определён равенством

$$\operatorname{St}(t) = \{S_\pi^k \in \langle S_\pi \rangle_m \colon S_\pi^k(t) = t\}.$$

Замечание 2.2. Отметим, что $|\operatorname{Orb}(t)| \cdot |\operatorname{St}(t)| = m$.

Лемма 2.3. *Пусть* $t \in \overline{0, q-1}$ *и* $k \in \overline{0, m}$. *Тогда* $\omega_\pi(t) = \omega_\pi\big(S_\pi^k(t)\big)$ *и* $\omega_p(t) = \omega_p\big(S_\pi^k(t)\big)$.

Доказательство непосредственно вытекает из определения S_π.

Лемма 2.4. *Пусть* $t \in \overline{0, q-1}$. *Тогда* π*-запись* t *непериодическая тогда и только тогда, когда* $|\operatorname{Orb}(t)| = m$.

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

В самом деле, если $\operatorname{St}(t) = \langle S_\pi^k \rangle$. 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, то $S_\pi^k \in \operatorname{St}(t)$, и для всех $k' \in \overline{1, k-1}$ имеем $S_\pi^{k'}(t) \neq t$, т. е. $\operatorname{St}(t) = \langle S_\pi^k \rangle$. Лемма доказана. □

Лемма 2.5. *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 $|\operatorname{Orb}(t)| = k$.*

Доказательство. Из доказательства предыдущей леммы вытекает, что период π-записи t равен k тогда и только тогда, когда $\operatorname{St}(t) = \langle S_\pi^k \rangle$. Последнее равенство равносильно тому, что число различных левых смежных классов по $\operatorname{St}(t)$ равно k. Поскольку элементы $\operatorname{Orb}(t)$ находятся в биективном соответствии с левыми смежными классами по стабилизатору t, имеем $|\operatorname{Orb}(t)| = k$, что завершает доказательство. □

Замечание 2.3. Присвоим непериодической π-записи t период m. Тогда период π-записи t всегда совпадает с $|\operatorname{Orb}(t)|$.

Определение 2.4. Рассмотрим произвольный элемент $a \in S$:

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

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

Следствие 2.1. *Пусть $a, b \in S$ и $\xi \in Q$. Тогда $\mathcal{P}_{a+b} = \mathcal{P}_a + \mathcal{P}_b$ и $\mathcal{P}_{\xi \cdot a} = \xi \cdot \mathcal{P}_a$.*

Утверждение непосредственно вытекает из определения $\mathcal{P}_a$.

Следствие 2.2. *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. В частности, $\operatorname{tr} = \operatorname{tr}_P^Q$ — функция следа из поля Q в поле P, являющееся подполем Q, задаётся многочленом

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

Лемма 2.6. *Пусть $a = u_i$, где $i \in \overline{0, q-1}$. Тогда $\mathcal{P}_a(x) = x^i$.*

Доказательство. По определению имеем

$$\mathcal{P}_a(x) = \mathcal{P}_{u_i}(x) = \pi_{u_i}\big(\phi^{-1}(x)\big) = \Big(\phi\big(\phi^{-1}(x)\big)\Big)^i = x^i. \qquad \square$$

Лемма 2.7. *Пусть $a = \operatorname{Tr}(u_i)$, где $i \in \overline{0, q-1}$. Тогда $\mathcal{P}_a(x) = \operatorname{tr}(x^i)$.*

Доказательство. По определению имеем

$$\mathcal{P}_a(x) = \mathcal{P}_{\operatorname{Tr}(u_i)}(x) = \pi_{\operatorname{Tr}(u_i)}\big(\phi^{-1}(x)\big) = \operatorname{tr}\Big(\Big(\phi\big(\phi^{-1}(x)\big)\Big)^i\Big) = \operatorname{tr}(x^i). \qquad \square$$

Лемма 2.8. *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 [5]. 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 $i \neq 0$, то по лемме 2.2 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 2.9. *Пусть $a = \mathrm{Tr}(u_i)$, где $i \in \overline{0, q-1}$. Тогда*

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

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

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

получаем

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

Замечание 2.4. 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 2.3. *Пусть $a = \mathrm{Tr}(u_i)$, где $i \in \overline{0, q-1}$. Тогда выполнено равенство*

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

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

Следствие 2.4. *Пусть $a = \mathrm{Tr}(u_i)$, где $i \in \overline{0, q-1}$. Тогда $a = 0$ тогда и только тогда, когда p делит $|\,\mathrm{St}(i)|$.*

Доказательство. По следствию 2.2 равенство $a = 0$ эквивалентно тому, что $\mathcal{P}_a \equiv 0$. В силу предыдущего следствия данное условие равносильно тому, что $|\,\mathrm{St}(i)|$ кратно p. □

Утверждение 2.1. *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 $|\,\mathrm{St}(i)|$ и $|\,\mathrm{St}(j)|$ делят p. Условие $a = b \neq 0$ равносильно тому, что $|\,\mathrm{St}(i)|$ и $|\,\mathrm{St}(j)|$ не делят p и $i = S_\pi^k(j)$, где $k \in \overline{1, m}$.*

Доказательство. По предыдущему следствию достаточно рассмотреть только случай $a = b \neq 0$. Условие $a = b$ равносильно тому, что $\mathcal{P}_a = \mathcal{P}_b$. По следствию 2.3 множество различных степеней мономов, входящих в $\mathcal{P}_a$, совпадает с множеством $\mathrm{Orb}(i)$, а множество различных степеней мономов, входящих в $\mathcal{P}_b$, совпадает с множеством $\mathrm{Orb}(j)$. Отсюда вытекает, что условие $\mathcal{P}_a = \mathcal{P}_b$ эквивалентно тому, что $\mathrm{Orb}(i) = \mathrm{Orb}(j)$. Последнее равенство равносильно тому, что $i = S_\pi^k(j)$, где $k \in \overline{1, m}$. □

2.2. Элементы $\mathrm{Tr}(\xi u_i)$

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

Определение 2.5. Пусть $j \mid i$. Обозначим через tr_j^i функцию следа из поля $\mathbb{F}_{\pi^i}$ в поле $\mathbb{F}_{\pi^j}$:

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

Замечание 2.5. В предыдущих обозначениях имеем $\mathrm{tr} = \mathrm{tr}_1^m$.

Напомним основные свойства функции tr_j^i.

Теорема 2.1 [5].

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.

Теорема 2.2 [5]. *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 2.10. *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

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

Утверждение 2.2. *Пусть $\xi \in Q$. Пусть $a = \mathrm{Tr}(\xi u_i)$, где $i \in \overline{0, q-1}$. Пусть* $|\mathrm{Orb}(i)| = r$. *Тогда выполнено равенство*

$$\mathcal{P}_a(x) = \mathrm{tr}_r^m(\xi) \cdot x^i + \big(\mathrm{tr}_r^m(\xi)\big)^\pi \cdot x^{i\pi} + \ldots + \big(\mathrm{tr}_r^m(\xi)\big)^{\pi^{r-1}} \cdot x^{i\pi^{r-1}}. \qquad (8)$$

Доказательство. Из замечаний 2.2 и 2.3 следует, что r — период π-записи i и $r \mid m$. Пусть $k = m/r$. Тогда по леммам 2.2, 2.4, 2.5 имеют место соотношения

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

Тогда согласно леммам 2.2 и 2.8 справедливы равенства

$$
\begin{aligned}
&x^i = x^{i\pi^r} = x^{i\pi^{2r}} = \ldots = x^{i\pi^{(k-1)r}},\\
&x^{i\pi} = x^{i\pi^{r+1}} = x^{i\pi^{2r+1}} = \ldots = x^{i\pi^{(k-1)r+1}},\\
&\quad\vdots\\
&x^{i\pi^{r-1}} = x^{i\pi^{r+(r-1)}} = x^{i\pi^{2r+(r-1)}} = \ldots = x^{i\pi^{(k-1)r+(r-1)}}.
\end{aligned}
$$

Отсюда вытекает следующая цепочка равенств:

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

Замечание 2.6. Отметим, что в (8) все мономы имеют различные степени и множество этих степеней совпадает с $\operatorname{Orb}(i)$.

Следствие 2.5. *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

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

Следствие 2.6. *В условиях предыдущего утверждения имеем* $a \neq 0$ *при* $\operatorname{tr}(\xi) \neq 0$.

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

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

Отсюда получаем $\mathcal{P}_a \not\equiv 0$. Значит, согласно следствию 2.2 имеем $a \neq 0$. □

Утверждение 2.3. *Пусть $\xi, \chi \in Q$. Положим $a = \mathrm{Tr}(\xi u_i)$, $b = \mathrm{Tr}(\chi u_i)$, где $i \in \overline{0, q-1}$. Пусть $|\mathrm{Orb}(i)| = r$. 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 2.2 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 2.7. *Пусть $\xi \in Q$. Положим $a = \mathrm{Tr}(\xi u_i)$, где $i \in \overline{0, q-1}$. Пусть $|\mathrm{Orb}(i)| = r$. Тогда $a = 0$ тогда и только тогда, когда $\mathrm{tr}_r^m(\xi) = 0$.*

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

Теорема 2.3. *Пусть $\xi, \chi \in Q$. Положим $a = \mathrm{Tr}(\xi u_i)$, $b = \mathrm{Tr}(\chi u_j)$, где $i, j \in \overline{0, q-1}$. Пусть $|\mathrm{Orb}(i)| = r_1$, $|\mathrm{Orb}(j)| = r_2$. 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 $\mathrm{tr}_{r_1}^m(\xi) \neq 0$, $\mathrm{tr}_{r_2}^m(\chi) \neq 0$, $r_1 = r_2 = r$, $i = S_\pi^k(j)$, $\mathrm{tr}_r^m(\xi) = \big(\mathrm{tr}_r^m(\chi)\big)^{\pi^k}$, где $k \in \overline{1, m}$.*

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

По замечанию 2.6 последнее равенство влечёт $\mathrm{Orb}(i) = \mathrm{Orb}(j)$, 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. $\mathrm{tr}_r^m(\xi) = \big(\mathrm{tr}_r^m(\chi)\big)^{\pi^k}$.

Наоборот, пусть $r_1 = r_2 = r$, $i = S_\pi^k(j)$ и $\mathrm{tr}_r^m(\xi) = \big(\mathrm{tr}_r^m(\chi)\big)^{\pi^k}$. Тогда по следствию 2.5 заключаем, что $\mathcal{P}_a = \mathcal{P}_b$. Теорема доказана. □

2.3. 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 2.11. *Пусть $a = u_i$, $b = u_j$, где $i, j \in \overline{0, q-1}$. Тогда*

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

Доказательство. Согласно определению имеем

$$u_i = \sum_{h\in H} \phi(h)^i h.$$

Аналогично для u_j. Тогда имеет место цепочка равенств

$$u_i \cdot u_j = \sum_{h\in H}\sum_{g\in H} \phi(g)^i \phi(h)^j gh = \sum_{h\in H}\Big(\sum_{g\in H} \phi(g)^i \phi(g^{-1}h)^j\Big)h =$$
$$= \sum_{h\in H}\Big(\sum_{g\in H} \phi(g)^i \big(\phi(h)-\phi(g)\big)^j\Big)h = \sum_{h\in H}\Big(\sum_{c\in Q} c^i(\phi(h)-c)^j\Big)h,$$

где последнее равенство справедливо, поскольку 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 2.12. *Пусть $a = \mathrm{Tr}(u_i)$, $b = \mathrm{Tr}(u_j)$, где $i,j \in \overline{0,q-1}$. Тогда*

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

Доказательство. По определению имеем

$$\mathrm{Tr}(u_i) = \sum_{h\in H} \mathrm{tr}(\phi(h)^i)h.$$

Аналогично для $\mathrm{Tr}(u_j)$. Тогда имеет место цепочка равенств

$$\mathrm{Tr}(u_i)\cdot\mathrm{Tr}(u_j) = \sum_{h\in H}\sum_{g\in H} \mathrm{tr}(\phi(g)^i)\mathrm{tr}(\phi(h)^j)gh =$$
$$= \sum_{h\in H}\Big(\sum_{g\in H} \mathrm{tr}(\phi(g)^i)\mathrm{tr}(\phi(g^{-1}h)^j)\Big)h =$$
$$= \sum_{h\in H}\Big(\sum_{g\in H} \mathrm{tr}(\phi(g)^i)\mathrm{tr}\Big(\big(\phi(h)-\phi(g)\big)^j\Big)\Big)h =$$
$$= \sum_{h\in H}\Big(\sum_{c\in Q} \mathrm{tr}(c^i)\mathrm{tr}\big((\phi(h)-c)^j\big)\Big)h,$$

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

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

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

Лемма 2.13. *Пусть $i \in \overline{0,q-1}$, $k \in \overline{0,m}$. Пусть $f \in Q[x]$. Тогда многочлены $f^{i\pi^k}$ и $f^{S^k_\pi(i)}$ определяют одну и ту же функцию, действующую из поля Q в себя.*

Доказательство. По лемме 2.8 мономы $x^{i\pi^k}$ и $x^{S_\pi^k(i)}$ определяют одну и ту же функцию. Значит, выполнено равенство функций

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

Лемма 2.14. *Пусть $f \in Q[x]$. Тогда многочлены f^q и f определяют одну и ту же функцию, действующую из поля Q в себя.*

Доказательство. Мономы x^q и x задают одну и ту же функцию. Значит, выполнено равенство функций

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

Лемма 2.15. *Пусть $a = \mathrm{Tr}(u_i)$, $b = \mathrm{Tr}(u_j)$, где $i, j \in \overline{0, q-1}$. Тогда*

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

Доказательство. Согласно лемме 2.12 получаем

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

Пусть $a_{s,t} = c^{i\pi^{s-1}} (x-c)^{j\pi^{t-1}}$. Тогда имеем

$$\mathcal{P}_{a\cdot b} = \sum_{c\in Q} \sum_{s=1}^{m} \sum_{t=1}^{m} a_{s,t}.$$

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

$$\sum_{s=1}^{m} \sum_{t=1}^{m} a_{s,t} = \sum_{k=0}^{m-1} M_k.$$

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 $M_k = \mathrm{tr}\big(c^i(x-c)^{j\pi^k}\big)$. В самом деле, имеем

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

По предыдущей лемме получаем

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

Отсюда вытекает, что

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

Из вышесказанного заключаем, что

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

Следствие 2.8. *Пусть* $a = \mathrm{Tr}(u_i)$, $b = \mathrm{Tr}(u_j)$, *где* $i, j \in \overline{0, q-1}$. *Тогда*

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

Доказательство. Согласно лемме 2.13 получаем

$$\mathrm{tr}\big(c^i(x-c)^{j\pi^k}\big) = \mathrm{tr}\Big(c^i(x-c)^{S_\pi^k(j)}\Big).$$

что завершает доказательство. $\square$

Утверждение 2.4. *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 2.6 и 2.11 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

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

$$= \sum_{k=0}^{m-1} \operatorname{tr}(c_{\delta_k} \cdot x^{\delta_k}) = \sum_{k=0}^{m-1} c_{\delta_k} \cdot \operatorname{tr}(x^{\delta_k}) = \sum_{k=0}^{m-1} c_{\delta_k} \cdot \mathcal{P}_{\operatorname{Tr}(u_{\delta_k})},$$

что завершает доказательство. □

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

Лемма 2.16. *Пусть* $a = \operatorname{Tr}(\xi u_i)$, $b = \operatorname{Tr}(\chi u_j)$, *где* $\xi, \chi \in Q$ *и* $i, j \in \overline{0, q-1}$. *Тогда*

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

Доказательство. Согласно определению имеем

$$\operatorname{Tr}(\xi u_i) = \sum_{h\in H} \operatorname{tr}(\xi \phi(h)^i) h.$$

Аналогично для $\operatorname{Tr}(\chi u_j)$. Дальнейшие рассуждения повторяют доказательство леммы 2.12. □

Лемма 2.17. *Пусть* $a = \operatorname{Tr}(\xi u_i)$, $b = \operatorname{Tr}(\chi u_j)$, *где* $\xi, \chi \in Q$, $i, j \in \overline{0, q-1}$. *Тогда*

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

Доказательство. Положим $a_{s,t} = (\xi c^i)^{\pi^{s-1}} (\chi (x-c)^j)^{\pi^{t-1}}$. Тогда имеем

$$\mathcal{P}_{a\cdot b} = \sum_{c\in Q} \sum_{s=1}^{m} \sum_{t=1}^{m} a_{s,t}.$$

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 2.15, получаем

$$\sum_{s=1}^{m} \sum_{t=1}^{m} a_{s,t} = \sum_{k=0}^{m-1} M_k.$$

Заметим, что $M_k = \mathrm{tr}\big(\xi c^i \chi^{\pi^k}(x-c)^{j\pi^k}\big)$. В самом деле, по лемме 2.14 имеет место цепочка равенств

$$
\begin{aligned}
M_k &= \sum_{s=1}^{m-k} a_{s,s+k} + \sum_{s=m-k+1}^{m} a_{s,s+k-m} = \\
&= \Big(\xi c^i (\chi(x-c)^j)^{\pi^k} + (\xi c^i)^{\pi} (\chi(x-c)^j)^{\pi^{k+1}} + \ldots + (\xi c^i)^{\pi^{m-k-1}} (\chi(x-c)^j)^{\pi^{m-1}}\Big) + \\
&+ \Big((\xi c^i)^{\pi^{m-k}} (\chi(x-c)^j) + \\
&+ (\xi c^i)^{\pi^{m-k+1}} (\chi(x-c)^j)^{\pi} + \ldots + (\xi c^i)^{\pi^{m-1}} (\chi(x-c)^j)^{\pi^{k-1}}\Big) = \\
&= \Big(\xi c^i (\chi(x-c)^j)^{\pi^k} + (\xi c^i)^{\pi} (\chi(x-c)^j)^{\pi^{k+1}} + \ldots + (\xi c^i)^{\pi^{m-k-1}} (\chi(x-c)^j)^{\pi^{m-1}}\Big) + \\
&+ \Big((\xi c^i)^{\pi^{m-k}} (\chi(x-c)^j)^{\pi^m} + \\
&+ (\xi c^i)^{\pi^{m-k+1}} (\chi(x-c)^j)^{\pi^{m+1}} + \ldots + (\xi c^i)^{\pi^{m-1}} (\chi(x-c)^j)^{\pi^{m+k-1}}\Big) = \\
&= \mathrm{tr}\big(\xi c^i \chi^{\pi^k}(x-c)^{j\pi^k}\big).
\end{aligned}
$$

По лемме 2.13 имеем

$$\mathrm{tr}\big(\xi c^i \chi^{\pi^k}(x-c)^{j\pi^k}\big) = \mathrm{tr}\big(\xi c^i \chi^{\pi^k}(x-c)^{S_\pi^k(j)}\big).$$

Отсюда получаем

$$
\begin{aligned}
\mathcal{P}_{a\cdot b} &= \sum_{c\in Q}\sum_{s=1}^{m}\sum_{t=1}^{m} a_{s,t} = \sum_{c\in Q}\sum_{k=0}^{m-1} M_k = \sum_{k=0}^{m-1}\sum_{c\in Q} M_k = \\
&= \sum_{k=0}^{m-1}\sum_{c\in Q} \mathrm{tr}\big(\xi c^i \chi^{\pi^k}(x-c)^{j\pi^k}\big) = \sum_{k=0}^{m-1}\sum_{c\in Q} \mathrm{tr}\big(\xi c^i \chi^{\pi^k}(x-c)^{S_\pi^k(j)}\big). \quad \square
\end{aligned}
$$

Теорема 2.4. *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*

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

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

$$(\xi u_i)\cdot\big(\chi^{\pi^k} u_{S_\pi^k(j)}\big) = c_{\delta_k}\xi\chi^{\pi^k} u_{\delta_k},$$

где c_{δ_k} определяется в соответствии с условием. Отсюда по леммам 2.6 и 2.11 заключаем, что

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

По предыдущей лемме получаем

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

что завершает доказательство. □

Теорема 2.5. *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*

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

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 обмена местами i и j, ξ и χ. □

2.4. Базисы кодов Рида—Маллера

Лемма 2.18. *Пусть* $t\in\overline{0,q-1}$, $\chi\in Q$ *и* $s\in\operatorname{Orb}(t)$. *Тогда существует* $\xi\in Q$, *такой что* $\operatorname{Tr}(\chi u_s) = \operatorname{Tr}(\xi u_t)$.

Доказательство. Если выполнено равенство $\operatorname{Tr}(\chi u_s)=0$, то утверждение очевидно. Рассмотрим случай $\operatorname{Tr}(\chi u_s)\neq 0$. Пусть $|\operatorname{Orb}(t)| = r$. Тогда согласно теореме 2.3 для искомого ξ должно выполняться равенство $\operatorname{tr}_r^m(\xi) = \bigl(\operatorname{tr}_r^m(\chi)\bigr)^{\pi^k}$, где $k\in\overline{1,m}$. Поскольку tr_r^m является сюръективным отображением [5], указанный элемент ξ существует. Лемма доказана. □

Следствие 2.9. *При* $t\in\overline{0,q-1}$ *выполнено равенство*

$$\operatorname{Tr}\Biggl(\sum_{s\in\operatorname{Orb}(t)}Qu_s\Biggr) = \operatorname{Tr}(Qu_t).$$

Определение 2.6. Произвольный набор представителей всевозможных орбит элементов Π_k под действием группы $\langle S_\pi\rangle_m$ обозначим $I_\pi(m,k)$.

По определению имеем

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

Отсюда согласно предыдущему следствию получаем

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

Утверждение 2.5. *Пусть* $t \in \overline{0,q-1}$, $|\mathrm{Orb}(t)| = r$. *Пусть* $\alpha'_1,\dots,\alpha'_r$ — *базис* $\mathbb{F}_{\pi^r}$ *над* P, *а* $\alpha_1,\dots,\alpha_r \in Q$ *такие, что* $\alpha'_1 = \mathrm{tr}_r^m(\alpha_1),\dots,\alpha'_r = \mathrm{tr}_r^m(\alpha_r)$. *Тогда* $\mathrm{Tr}(\alpha_1 u_t),\dots,\mathrm{Tr}(\alpha_r u_t)$ — *базис* $\mathrm{Tr}(Qu_t)$ *над* P.

Доказательство. В силу того что tr_r^m — сюръективное отображение, указанные элементы $\alpha_1,\dots,\alpha_r$ существуют. Рассмотрим произвольный элемент $\mathrm{Tr}(\xi u_t)$. Пусть $p_1,\dots,p_r \in P$ — коэффициенты разложения $\mathrm{tr}_r^m(\xi)$ по базису $\alpha'_1,\dots,\alpha'_r$, т. е. $\mathrm{tr}_r^m(\xi) = p_1\alpha'_1 + \ldots + p_r\alpha'_r$. Согласно следствию 2.5 имеет место цепочка равенств

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

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

Покажем, что данные элементы линейно независимы. Пусть $p_1,\dots,p_r \in P$ такие, что $p_1\mathrm{Tr}(\alpha_1 u_t) + \ldots + p_r\mathrm{Tr}(\alpha_r u_t) = 0$. Легко видеть, что тогда имеем $\mathrm{Tr}\big((p_1\alpha_1+\ldots+p_r\alpha_r)u_t\big) = 0$. По следствию 2.7 последнее равенство равносильно тому, что $\mathrm{tr}_r^m(p_1\alpha_1 + \ldots + p_r\alpha_r) = 0$. Отсюда получаем

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

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

Таким образом, для каждого $t \in I_\pi(m,k)$ элементы $\mathrm{Tr}(\alpha_{t,1}u_t),\dots,\mathrm{Tr}(\alpha_{t,r_t}u_t)$ образуют базис $\mathrm{Tr}(Qu_t)$ над P, где $r_t = |\mathrm{Orb}(t)|$. В силу теоремы 2.3 полученные базисы не содержат общих элементов.

Определение 2.7. Для всех $k \in \overline{0,m(\pi-1)}$ определим множество $\mathrm{B}_\pi(m,k)$ равенством

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

Теорема 2.6. $\mathrm{B}_\pi(m,k)$ *является базисом* $\mathcal{RM}_\pi(m,k)$ *над* P.

Доказательство. По предыдущему утверждению указанные элементы порождают идеал $\mathcal{RM}_\pi(m,k)$. Покажем, что они линейно независимы. Пусть $I_\pi(m,k) = \{t_1,\dots,t_n\}$. Пусть

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

где $r_i = |\operatorname{Orb}(t_i)|$, — такие элементы, что

$$\sum_{i=1}^{n} p_{t_i,1}\operatorname{Tr}(\alpha_{t_i,1}u_{t_i}) + \ldots + p_{t_i,r_i}\operatorname{Tr}(\alpha_{t_i,r_i}u_{t_i}) = 0. \tag{9}$$

Положим

$$T_i = p_{t_i,1}\operatorname{Tr}(\alpha_{t_i,1}u_{t_i}) + \ldots + p_{t_i,r_i}\operatorname{Tr}(\alpha_{t_i,r_i}u_{t_i}).$$

Равенство (9) равносильно тому, что

$$\sum_{i=1}^{n} \mathcal{P}_{T_i} \equiv 0.$$

По замечанию 2.6 степени ненулевых мономов, входящих в $\mathcal{P}_{T_i}$, являются элементами множества $\operatorname{Orb}(t_i)$. Отсюда заключаем, что равенство (9) 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 $\operatorname{Tr}(\alpha_{t,1}u_t), \ldots, \operatorname{Tr}(\alpha_{t,r_t}u_t)$ линейно независимы над P. Следовательно, условие $\mathcal{P}_{T_i} \equiv 0$ равносильно тому, что $p_{t_i,1} = \ldots = p_{t_i,r_i} = 0$. Таким образом, получаем

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

что завершает доказательство. □

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

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

Подобно случаю базисных кодов покажем, что при $\lambda \neq 1$ нет нетривиальных совпадений обычных кодов Рида—Маллера $\mathcal{RM}_\pi(m,k)$ и степеней радикала $\mathfrak{R}_R$, и исследуем граф включений указанных идеалов.

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

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

$$\mathfrak{R}_R\mathcal{RM}_\pi(m,k) = \operatorname{Tr}\big(\mathfrak{R}_S\mathcal{M}_\pi(m,k)\big). \tag{10}$$

Лемма 3.1 [2]. *Пусть $\alpha \in \overline{0,l(p-1)}$. Тогда выполнено равенство*

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

Следовательно, равенство (10) равносильно тому, что

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

Лемма 3.2. *Пусть $k \in \overline{0,q-1}$. Тогда имеет место включение*

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

Доказательство. Рассмотрим $u_s \in \mathfrak{R}_S$, $u_t \in \mathcal{M}_\pi(m,k)$ и $\xi,\chi \in Q$. По теореме 2.4 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 $\mathrm{Tr}\big(\mathfrak{R}_S\mathcal{M}_\pi(m,k)\big)$. В самом деле, по лемме 2.3 получаем, что $u_{S_\pi^i(t)} \in \mathcal{M}_\pi(m,k)$, где $i \in \overline{0,m-1}$. По лемме 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 $c_{\delta_i}\mathrm{Tr}(\xi\chi^{\pi^i}u_{\delta_i}) \in \mathrm{Tr}\big(\mathfrak{R}_S\mathcal{M}_\pi(m,k)\big)$, что завершает доказательство. □

Лемма 3.3. *Пусть $k \in \overline{0,q-1}$, тогда имеет место включение*

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

Доказательство. Рассмотрим произвольный элемент $u_\delta \in \mathfrak{R}_S\mathcal{M}_\pi(m,k)$. Согласно лемме 1.3 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 2.5 имеем

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

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

$$\begin{aligned}
\sum_{j=1}^{m}\mathrm{Tr}(\xi_j u_s)\mathrm{Tr}(\chi_j u_t) &= \sum_{j=1}^{m}\mathrm{Tr}(c_\delta\xi_j\chi_j u_\delta) + \sum_{j=1}^{m}\sum_{i=1}^{m-1}\mathrm{Tr}\big(c_{\tilde{\delta}_i}{\xi_j}^{\pi^i}\chi_j u_{\tilde{\delta}_i}\big) = \\
&= \mathrm{Tr}\Big(\sum_{j=1}^{m} c_\delta\xi_j\chi_j u_\delta\Big) + \sum_{i=1}^{m-1}\mathrm{Tr}\Big(\sum_{j=1}^{m} c_{\tilde{\delta}_i}{\xi_j}^{\pi^i}\chi_j u_{\tilde{\delta}_i}\Big) = \\
&= \mathrm{Tr}\Big(c_\delta\Big(\sum_{j=1}^{m}\xi_j\chi_j\Big)u_\delta\Big) + \sum_{i=1}^{m-1}\mathrm{Tr}\Big(c_{\tilde{\delta}_i}\Big(\sum_{j=1}^{m}{\xi_j}^{\pi^i}\chi_j\Big)u_{\tilde{\delta}_i}\Big). \qquad (11)
\end{aligned}$$

Рассмотрим следующую систему линейных уравнений относительно неизвестных χ_j:

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

где $\xi \in Q$. Легко видеть, что если данная система уравнений имеет решение, то равенство (11) можно переписать следующим образом:

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

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 $\mathrm{Tr}(\mathfrak{R}_S)\mathrm{Tr}\bigl(\mathcal{M}_\pi(m,k)\bigr)$. Отсюда заключаем, что имеет место включение $\mathrm{Tr}(\mathfrak{R}_S)\mathrm{Tr}\bigl(\mathcal{M}_\pi(m,k)\bigr) \supseteq \mathrm{Tr}\bigl(\mathfrak{R}_S\mathcal{M}_\pi(m,k)\bigr)$.

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 [7]. Так как степень Q над P равна $[Q : P] = m$ [5], можно выбрать элементы $\xi_1, \ldots, \xi_m$ линейно независимыми над P. Тогда получаем $\det A \neq 0$, т. е. $\mathrm{rk}\, A = m$.

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 $\mathrm{rk}\,\tilde{A} = m$. В самом деле, пусть $\tilde{A}_1, \tilde{A}_2, \ldots, \tilde{A}_m$ — система строк матрицы $\tilde{A}$. Предположим, что $\lambda_1\tilde{A}_1 + \ldots + \lambda_m\tilde{A}_m = 0$, где $\lambda_1, \ldots, \lambda_m \in Q$. Если

$\xi \neq 0$, то, рассматривая последний столбец матрицы $\tilde{A}$, получаем, что $\lambda_1 = 0$. Отсюда вытекает, что $\lambda_2\tilde{A}_2 + \ldots + \lambda_m\tilde{A}_m = 0$. Пусть $A_1, A_2, \ldots, A_m$ — система строк матрицы A. Тогда $A_2, \ldots, A_m$ — укороченная система строк $\tilde{A}_2, \ldots, \tilde{A}_m$. Так как $\operatorname{rk} A = m$, 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 $\lambda_1 = \lambda_2 = \ldots = \lambda_m = 0$, т. е. $\operatorname{rk}\tilde{A} = m$. Если $\xi = 0$, то $A_1, \ldots, A_m$ — 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 3.2 и 3.3 вытекает следующее утверждение.

Утверждение 3.1. *Пусть $k \in \overline{0, q-1}$. Тогда выполнено равенство*

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

Следствие 3.1. *Если выполнено равенство* (4)*, то выполнено равенство*

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

Доказательство. Пусть выполнено равенство (4). Тогда, применяя к обеим частям данного равенства функцию Tr, по предыдущему утверждению получаем, что

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

3.2. Совпадения кодов Рида—Маллера со степенями радикала $\mathfrak{R}_R$

Известно, что при $\lambda = 1$ обычные коды Рида—Маллера являются степенями радикала $\mathfrak{R}_R$ [1, 4]. Цель данного подраздела — показать, что при $\lambda \neq 1$ подобных совпадений, кроме тривиальных случаев, нет.

Совпадения обычных кодов Рида—Маллера со степенями радикала $\mathfrak{R}_R$ в случае простого подполя описываются следующим утверждением.

Утверждение 3.2 [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 3.3. *Пусть $\lambda \neq 1$. Тогда выполнены равенства*

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

Доказательство. Утверждение непосредственно вытекает из утверждения 1.5. □

Докажем аналог теоремы 1.2.

Лемма 3.4. *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 $\mathrm{Tr}(\xi u_t) \in \mathcal{RM}_\pi(m,k)$. По следствиям 2.5 и 2.7 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 2.6 получаем, что степени мономов, входящих в $\mathcal{P}_{\mathrm{Tr}(\alpha_i u_j)}$, являются элементами множества $\mathrm{Orb}(j)$. Отсюда по определению $\mathrm{B}_\pi(m,k)$ заключаем, что $t \in \bigcup\limits_{j \in I_\pi(m,k)} \mathrm{Orb}(j) = \Pi_k$. Лемма доказана. □

Следствие 3.2. *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. Утверждение непосредственно вытекает из предыдущей леммы при $\lambda = 1$. □

Следствие 3.3. *Пусть* $k \in \overline{0,m(\pi-1)}$, $j \in \overline{0,l(p-1)}$. *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 3.1. 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 3.1. *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. По следствию 3.3 заключаем, что равенство $\mathcal{RM}_\pi(m,k) = \mathcal{RM}_p(l,j)$ равносильно тому, что $\Pi_k = \mathrm{P}_j$. Согласно следствию 1.2 заключаем, что последнее невозможно. Теорема доказана. □

3.3. 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 3.5. *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 1.2 имеем $\mathfrak{R}_S\mathcal{M}_\pi(m,k+1) \subseteq \mathcal{M}_\pi(m,k)$. Применяя к обеим частям данного включения функцию Tr, по утверждению 3.1 получаем $\mathfrak{R}_R\mathcal{RM}_\pi(m,k+1) \subseteq \mathcal{RM}_\pi(m,k)$, что завершает доказательство. □

Утверждение 3.4. *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 1.1 и 1.6 при указанных значениях j имеет место включение $\mathrm{P}_{l(p-1)-j} \subset \Pi_{m(\pi-1)-j}$, что завершает доказательство. □

Утверждение 3.5. *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 1.1 и 1.7 при указанных значениях j имеет место включение $\mathrm{P}_j \supset \Pi_j$, что завершает доказательство. □

3.3.1. 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 идеалу $\mathcal{RM}_\pi(m,k+1)$, 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:

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

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

$$\mathcal{RM}_\pi(m,k+1) \not\subset \mathfrak{R}_R^\alpha. \tag{14}$$

Теорема 3.2. *Пусть для некоторого* $k \in \overline{1, m(\pi-1)-2}$ *выполнено равенство*

$$\mathfrak{R}_R\mathcal{RM}_\pi(m,k+1) = \mathcal{RM}_\pi(m,k). \tag{15}$$

Тогда существует и притом единственное $\alpha \in \overline{1, l(p-1)-1}$, *такое что имеют место соотношения* (12)—(14).

Доказательство. Доказательство повторяет доказательство теоремы 1.3, с заменой всюду $\mathcal{M}_\pi(m,k)$ на $\mathcal{RM}_\pi(m,k)$ и $\mathfrak{R}_S$ на $\mathfrak{R}_R$. □

Утверждение 3.6.

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

Доказательство. Утверждение непосредственно вытекает из утверждений 1.9 и 3.1. □

Теорема 3.3. *Пусть* $\alpha \in \overline{1, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-2}$ *такие, что имеют место соотношения* (12)—(14). *Тогда выполнено равенство* (15).

Доказательство. Доказательство повторяет доказательство теоремы 1.4 с заменой всюду $\mathcal{M}_\pi(m,k)$ на $\mathcal{RM}_\pi(m,k)$ и $\mathfrak{R}_S$ на $\mathfrak{R}_R$. □

Теорема 3.4. *Пусть* $\lambda \neq l$. *Тогда количество* $k \in \overline{0, m(\pi-1)-1}$, *таких что выполнено равенство* (15), *равно* $l(p-1)$.

Доказательство. Известно, что количество $k \in \overline{0, m(\pi-1)-1}$, таких что выполнено равенство (4), равно $l(p-1)$ [3]. Отсюда по следствию 3.1 заключаем, что количество $k \in \overline{0, m(\pi-1)-1}$, таких что выполнено равенство (15), 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 3.2 существует, и притом единственное, α, такое что имеют место соотношения (12)—(14). Несложно понять, что различным значениям k соответствуют различные α. Отсюда следует, что количество k, таких что выполнено равенство (15), не превосходит $l(p-1)$. Теорема доказана. □

Следствие 3.4. *Пусть* $k \in m(\pi-1)-1$. *Тогда равенство* (4) *выполнено тогда и только тогда, когда выполнено равенство* (15).

Утверждение 3.7. *Пусть* $\alpha \in \overline{1, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-2}$. *Число* k *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* (12)—(14).

Доказательство. Рассмотрим множество чисел k', для которых $j = l(p-1)-\alpha$ является наименьшим таким, что $\Pi_{k'} \subset \mathrm{P}_j$. По утверждению 3.2 и следствию 3.3 данное условие равносильно тому, что для k', α имеют место соотношения (12) и (13). Согласно утверждению 3.5 указанное множество непусто. Пусть k максимальное среди k'. Легко видеть, что данное условие эквивалентно тому, что для k, α имеют место соотношения (12)—(14). □

Теорема 3.5. *Пусть* $\alpha \in \overline{1, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-2}$. *Соотношения* (12)—(14) *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 1.8 и 3.7 соотношения (12)—(14) имеют место тогда и только тогда, когда имеют место соотношения (1)—(3). Дальнейшие рассуждения повторяют доказательство теоремы 1.5. □

3.3.2. 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:

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

$$\mathfrak{R}_R^{\alpha} \not\subseteq \mathcal{RM}_{\pi}(m,k-1), \tag{17}$$

$$\mathfrak{R}_R^{\alpha-1} \not\subset \mathcal{RM}_{\pi}(m,k). \tag{18}$$

Утверждение 3.8. *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* (16)—(18).

Доказательство. Рассмотрим множество таких чисел k', что для $j = l(p-1)-\alpha$ имеет место включение $\mathrm{P}_j \subset \Pi_{k'}$. В силу утверждения 3.2 и следствия 3.3 данное условие равносильно тому, что для k', α имеет место соотношение (16). Согласно утверждению 3.4 указанное множество непусто. Пусть k — минимальное среди k'. Легко видеть, что данное условие эквивалентно тому, что для k, α имеют место соотношения (16) и (17). Рассуждая тем же образом, что и при доказательстве утверждения 1.10, заключаем, что для k, α также имеет место соотношение (18), что завершает доказательство. □

Теорема 3.6. *Пусть* $\alpha \in \overline{2, l(p-1)-1}$ *и* $k \in \overline{1, m(\pi-1)-1}$. *Соотношения* (16)—(18) *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 1.10 и 3.8 соотношения (16)—(18) имеют место тогда и только тогда, когда имеют место соотношения (5)—(7). Дальнейшие рассуждения повторяют доказательство теоремы 1.6. □

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 $\mathcal{RM}_p(l,j) \supset \supset \mathcal{RM}_{\pi}(m,k)$ описывается с помощью теорем 3.2 и 3.3 и утверждения 3.7, случай $\mathcal{RM}_{\pi}(m,k) \supset \mathcal{RM}_p(l,j)$ — с помощью утверждения 3.8. Теоремы 3.5 и 3.6 дают числовое описание указанных включений.

Литература

[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] Тумайкин И. Н. Базисные коды Рида—Маллера как групповые коды // Фундамент. и прикл. матем. — 2013. — Т. 18, вып. 4. — С. 137—154.

[4] Charpin P. Une généralisation de la construction de Berman des codes de Reed et Muller p-aires // Commun. Algebra. — 1988. — Vol. 16, no. 11. — P. 2231—2246.

[5] Lidl R., Niederreiter H. Finite Fields. — Cambridge: Cambridge Univ. Press, 1997. — (Encycl. Math. Its Appl.; Vol. 20).

[6] MacWilliams F. J., Sloane N. J. The Theory of Error-Correcting Codes. — Elsevier, 1988. — (North-Holland Math. Lib.; Vol. 16).

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