Идеалы групповых колец, связанные с кодами Рида—Маллера

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 — одно 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. Этот метод даёт достаточно наглядное построение указанных кодов, а также вводит понятие базисных кодов Рида—Маллера. Известно, что базисные коды Рида—Маллера $\mathcal{M}_\pi(m,k)$ над простыми полями совпадают со степенями радикала $\mathfrak{R}_S$ соответствующей групповой алгебры, а над непростыми полями таких совпадений, кроме тривиальных случаев, нет. В данной работе исследованы идеалы $\mathfrak{R}_S\mathcal{M}_\pi(m,k)$, которые возникают при изучении включений между базисными кодами и степенями радикала.

Abstract

I. N. Tumaykin, Group ring ideals related to Reed–Muller codes, Fundamentalnaya i prikladnaya matematika, vol. 21 (2016), no. 1, pp. 211—215.

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. It is known that basic Reed–Muller codes $\mathcal{M}_\pi(m,k)$ over a prime field are powers of the radical $\mathfrak{R}_S$ of a corresponding group algebra and over a nonprime field there are no such equalities, except for trivial ones. In this paper, we consider the ideals $\mathfrak{R}_S\mathcal{M}_\pi(m,k)$ that arise while studying the inclusions of the basic codes and radical powers.

1. Введение

Известно, что при $\lambda = 1$ базисные коды Рида—Маллера $\mathcal{M}_\pi(m,k)$ совпадают со степенями радикала $\mathfrak{R}_S$ [2], а при $\lambda \neq 1$ подобных совпадений базисных кодов, кроме тривиальных случаев, нет [1]. Рассмотрим включения вида $\mathcal{M}_\pi(m,k) \subset \mathfrak{R}_S^\alpha$. Наиболее важен случай, описываемый следующими соотношениями:

Фундаментальная и прикладная математика, 2016, том 21, № 1, с. 211—215.

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

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

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

Выполнение условий (1)—(3) равносильно выполнению равенства

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

(см. [1]). Таким образом, возникает связь между идеалами $\mathfrak{R}_S\mathcal{M}_\pi(m,k)$ и строением графа включений базисных кодов Рида—Маллера и степеней радикала. В этой работе исследованы условия совпадения идеалов $\mathfrak{R}_S\mathcal{M}_\pi(m,k)$.

2. Базисные коды Рида—Маллера

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 $m \geqslant 1$, $l = \lambda m$, $\pi = p^\lambda$, $\lambda \geqslant 1$. Пусть группа $(H,\cdot)$ изоморфна аддитивной группе поля Q. Рассмотрим групповую алгебру $S = QH$. Радикал S обозначим $\mathfrak{R}_S$.

Пусть $\varphi\colon (H,\cdot) \to (Q,+)$ — указанный выше изоморфизм. Рассмотрим следующие элементы:

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

Определение 2.1. Назовём π-весом числа i сумму цифр в его π-ичном представлении и обозначим это $\omega_\pi(i)$. Заметим, что $\omega_\pi(i) \in \overline{0,(\pi-1)m}$ при $i \in \overline{0,q-1}$. Аналогично вводится p-вес.

Определение 2.2 [2]. Для всякого $k \in \overline{0,(\pi-1)m}$ определим базисный код Рида—Маллера порядка k над полем Q равенством

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

Утверждение 2.1 [2]. *$\mathcal{M}_\pi(m,k)$ является идеалом в S и линейным кодом над Q с кодовыми параметрами $[q, M_\pi(m,k), d_\pi(m,k)]$, где $M_\pi(m,k)$ — размерность идеала $\mathcal{M}_\pi(m,k)$, которая равна числу расстановок $r \leqslant k$ шаров по m лункам так, что в каждой лунке меньше π шаров*:

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

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

Дальнейшие результаты опираются на следующие известные факты.

Лемма 2.1 [2]. *Для любых* $s,t \in \overline{0,q-1}$ *имеют место следующие соотношения*:

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

Лемма 2.2 [1]. *Для любого* $k \in \overline{0,m(\pi-1)-1}$ *имеет место включение* $\mathfrak{R}_S \mathcal{M}_\pi(m,k+1) \subseteq \mathcal{M}_\pi(m,k)$.

Введём необходимые определения.

Определение 2.3 [1]. π-записью числа t назовём его π-ичное представление, обозначим это $[t]_\pi$. Аналогично вводится p-запись. Для $t \in \overline{0,q-1}$ отождествим $[t]_\pi$ и соответствующий элемент $\{0,\dots,\pi-1\}^m$. Аналогично отождествим $[t]_p$ и соответствующий элемент $\{0,\dots,p-1\}^l$. Элементы, составляющие $[t]_\pi$, назовём π-координатами. Аналогично вводятся p-координаты.

Определение 2.4 [1]. Для $t \in \overline{0,q-1}$ введём понятие λ-группы. Для этого разобьём $[t]_p$ на m групп, каждая из которых состоит из λ подряд идущих p-координат. Каждую полученную группу назовём λ-группой. Легко убедиться, что между λ-группами и π-координатами существует взаимно-однозначное отображение. На множестве λ-групп введём отношение порядка, совпадающее с упорядочиванием по старшинству соответствующих π-координат.

Определение 2.5 [1]. Для $t \in \overline{0,q-1}$, $i \in \overline{0,\lambda-1}$ введём понятие i-слоя. Для этого каждой p-координате внутри каждой λ-группы t присвоим номер от 0 до $\lambda-1$ в соответствии с упорядочиванием по старшинству p-координат внутри данной λ-группы как элементов $[t]_p$. Упорядоченный набор p-координат с номерами i назовём i-слоем. Несложно понять, что между элементами i-слоя и π-координатами существует взаимно-однозначное отображение. На элементах i-слоя введём отношение порядка, совпадающее с упорядочиванием по старшинству соответствующих π-координат.

Определение 2.6 [1]. Числа t', в 0-слое которых все p-координаты равны $p-1$, и соответствующие им элементы $u_{t'}$ назовём особыми.

Определение 2.7 [1]. Определим на множестве целых неотрицательных чисел отношение порядка $\preceq_p$: положим $x \preceq_p y$, если каждая p-координата x не превосходит соответствующей p-координаты y. Естественно положить $x \prec_p y$, если $x \preceq_p y$ и $x \neq y$.

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

Лемма 3.1. *Пусть $\lambda \neq l$. Тогда для всех $k \in \overline{0, m(\pi-1)-1}$ существует u_t такое, что $u_t \in \mathfrak{R}_S\mathcal{M}_\pi(m,k+1)$ и $\omega_\pi(t)=k$.*

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

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

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

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

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

Согласно равенству

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

можно изменить элементы в указанных λ-группах следующим образом:

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

Обозначим полученное число t'. Легко убедиться в том, что $\omega_\pi(t')=$ $=\omega_\pi(t)=k$ и t' не является особым, что приводит к противоречию. Лемма доказана. □

Теорема 3.1. *Пусть $\lambda\neq l$. Тогда для всех $k\in\overline{0,m(\pi-1)}$ идеалы $\mathfrak{R}_S\mathcal{M}_\pi(m,k)$ попарно различны.*

Доказательство. Легко убедиться, что для всех $k\in\overline{1,m(\pi-1)}$ утверждение теоремы вытекает из лемм 2.2 и 3.1. При $k=0$ имеем $\mathfrak{R}_S\mathcal{M}_\pi(m,0)=\{0\}$, что завершает доказательство. □

Рассмотрим теперь случай $\lambda=l$.

Лемма 3.2. *Пусть $\lambda = l$. Пусть $k \in \overline{0, m(\pi-1)-1}$. Элемент u_t, такой что $u_t \in \mathfrak{R}_S\mathcal{M}_\pi(m, k+1)$ и $\omega_\pi(t) = k$, существует тогда и только тогда, когда $k \not\equiv_p p-1$.*

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

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

Наоборот, пусть существует элемент $u_t \in \mathfrak{R}_S\mathcal{M}_\pi(m, k+1)$, такой что $\omega_\pi(t) = k$. Согласно [1] это возможно только тогда, когда выполнено равенство $u_s u_{t'} = cu_t$, где $u_s \in \mathfrak{R}_S$, $u_{t'} \in \mathcal{M}_\pi(m, k+1)$ и $t \prec_p t'$. Ясно, что $t' = t+1$. Предположим, что $k \equiv_p p-1$. Тогда $t' = t+1 = \omega_\pi(t)+1 = k+1 \equiv_p 0$. Отсюда вытекает, что младшая p-координата t' равна 0, а младшая p-координата t равна $p-1$, что противоречит условию $t \prec_p t'$. Лемма доказана. □

Лемма 3.3. *В условиях предыдущей леммы равенство $\mathfrak{R}_S\mathcal{M}_\pi(m, k+1) = \mathfrak{R}_S\mathcal{M}_\pi(m,k)$ имеет место тогда и только тогда, когда $k \equiv_p p-1$.*

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

Из лемм 2.2, 3.2 и 3.3 вытекает следующая теорема.

Теорема 3.2. *Пусть $\lambda = l$ и $i, j \in \overline{0, m(\pi-1)}$, $i < j$. Тогда равенство $\mathfrak{R}_S\mathcal{M}_\pi(m,i) = \mathfrak{R}_S\mathcal{M}_\pi(m,j)$ имеет место тогда и только тогда, когда $j = i+1$ и $i \equiv_p p-1$.*

Литература

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

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