ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 4**

УДК 621.391.1 : 519.725

© 2021 г. **Ф.И. Соловьева**

О ПЕРЕСЕЧЕНИИ КОДОВ ТИПА РИДА – МАЛЛЕРА[1]

Двоичный код с параметрами и основными свойствами классического кода Рида – Маллера $RM_{r,m}$ порядка r будем называть кодом типа Рида – Маллера порядка r и обозначать через $LRM_{r,m}$. Класс таких кодов содержит семейство кодов, полученных конструкцией Пулатова, а также классические линейные и $\mathbb{Z}_4$-линейные коды Рида – Маллера. Исследуется проблема пересечения кодов типа Рида – Маллера. Доказано, что для любого четного k в интервале $0 \leqslant k \leqslant 2^{2^{\sum_{i=0}^{r-1}\binom{m-1}{i}}}$ существуют коды $LRM_{r,m}$ порядка r длины 2^m, пересечение которых равно k. Доказано также, что существуют два кода типа Рида – Маллера порядка r длины 2^m, пересечение которых равно $2k_1k_2$, где $1 \leqslant k_s \leqslant |RM_{r-1,m-1}|$, $s \in \{1,2\}$, для любой допустимой длины, начиная с 16.

Ключевые слова: код Рида – Маллера, код типа Рида – Маллера, задача о пересечении кодов, коды Пулатова, компоненты кода Рида – Маллера, i-компонента, свитчинг, свитчинговая конструкция кодов.

DOI: 10.31857/S0555292321040057

§ 1. Введение

Векторное пространство размерности n над полем Галуа $GF(2)$, снабженное метрикой Хэмминга, будем обозначать через $\mathbb{F}^n$. Основные определения см. в [1].

Напомним определение и основные свойства классического двоичного линейного кода *Рида – Маллера порядка* r, который будем обозначать через $RM_{r,m}$, а его выколотый код – через $RM^*_{r,m}$. Код Рида – Маллера определяется для любых $1 \leqslant m$, $0 \leqslant r \leqslant m$, как совокупность всех векторов длины 2^m, отвечающих булевым функциям степени не более r от m переменных. Код $RM_{r,m}$ имеет следующие параметры: длина кода равна $n = 2^m$, мощность 2^k, где $k = \sum\limits_{i=0}^{r}\binom{m}{i}$, кодовое расстояние 2^{m-r}. Код $RM_{r,m}$ *антиподален*, т.е. для любого кодового слова x вектор $\bar{x} = x + \mathbf{1}^n$ также принадлежит коду, здесь и далее $\mathbf{1}^n$ – вектор длины n, состоящий из единичных координат, а знаком $+$ обозначено сложение по модулю 2. Код $RM_{r,m}$ является дуальным к коду $RM_{m-1-r,m}$, $0 \leqslant r \leqslant m$, и кроме того, $RM_{r-1,m} \subset RM_{r,m}$. Коды $RM_{m-2,m}$ и $RM_{1,m}$ являются расширенными кодами Хэмминга и Адамара соответственно. Код Рида – Маллера $RM_{r,m}$ порождается множеством своих кодовых слов минимального веса (см. [1, § 13.5]).

Двоичный антиподальный код с параметрами классического кода Рида – Маллера $RM_{r,m}$ порядка r назовем *кодом типа Рида – Маллера* порядка r и будем обозначать через $LRM_{r,m}$. Этот код не обязательно линеен. Класс данных кодов совпадает с обширным классом расширенных совершенных кодов при $r = m-2$. По определению все коды $RM_{r,m}$ являются кодами $LRM_{r,m}$. При $r \in \{0, m-1, m\}$ код $LRM_{r,m}$

[1] Работа выполнена в рамках государственного задания ИМ СО РАН (проект № 0314-2019-0016).

совпадает с кодом $RM_{r,m}$. Несколько конструкций кодов $LRM_{r,m}$ любых порядков, т.е. содержащих не только совершенные расширенные коды и коды Адамара, были предложены в работах [2–4]. Заметим, что, как и код $RM_{r,m}$ длины $n = 2^m$, код типа Рида – Маллера с теми же параметрами, полученный конструкцией Пулатова [3] из кодов Рида – Маллера длины $n = 2^{m-1}$ с нелинейной функцией λ (см. определение кода в § 2), образует ортогональный массив силы $2^r - 1$. Класс кодов типа Рида – Маллера содержит важный класс $\mathbb{Z}_4$-линейных кодов Рида – Маллера (см. их конструкции в работах [5, 6]). Групповые коды над кольцом $\mathbb{Z}_4$, являющиеся прообразами этих $\mathbb{Z}_4$-линейных кодов Рида – Маллера под действием отображения Грэя, имеют базисы минимального веса (см. [7]).

В настоящей работе исследуется следующий вопрос: каков размер пересечения двух кодов $LRM_{r,m}$? Аналогичная проблема ранее, в 1994 г., была выдвинута в [8] для совершенных кодов.

Исследованиям проблемы пересечения совершенных q-ичных кодов и двоичных кодов Адамара посвящено достаточно много статей (см. обзор [9] и библиографию в нем). Полное решение проблемы пересечения двоичных кодов Хэмминга найдено в работе [10]. В статье [11] решена проблема пересечения для всех q-ичных линейных кодов, $q \geqslant 2$, включая двоичные коды Рида – Маллера. Согласно [11] для некоторой подстановки π длины 2^m код Рида – Маллера $RM_{r,m}$ порядка r удовлетворяет условию $|RM_{r,m} \cap \pi(RM_{r,m})| \geqslant 2$, где минимальное значение 2 достижимо только при $r \leqslant [(m-1)/2]$. В [10] показано, что для каждого $m \geqslant 3$ существуют два нелинейных совершенных двоичных кода длины $2^m - 1$, пересекающихся по двум кодовым словам. В работе [12] доказано, что для любых чисел k_1 и k_2, таких что $1 \leqslant k_s \leqslant 2^{(n+1)/2-\log(n+1)}$, $s = 1, 2$, найдутся совершенные двоичные коды C_1 и C_2 длины $n = 2^m - 1$, $m \geqslant 4$, удовлетворяющие $|C_1 \cap C_2| = 2k_1k_2$. В [13] показано, что для любого четного числа k в интервале $0 \leqslant k \leqslant 2^{n+1-2\log(n+1)}$ существуют совершенные двоичные коды C_1 и C_2 длины $n = 2^m - 1$, $m \geqslant 4$, такие что $\eta(C_1, C_2) = k$. Следует отметить, что совокупности чисел пересечений, полученных в [12] и [13], не покрывают друг друга. В работе [14] исследовались пересечения кодов Адамара. В [15] полностью решена проблема пересечения аддитивных ($\mathbb{Z}_4$- и $\mathbb{Z}_2\mathbb{Z}_4$-линейных), расширенных и нерасширенных совершенных кодов. Аналогичный результат был получен для аддитивных ($\mathbb{Z}_4$- и $\mathbb{Z}_2\mathbb{Z}_4$-линейных) кодов Адамара (дуальных кодов к $\mathbb{Z}_4$- и $\mathbb{Z}_2\mathbb{Z}_4$-линейным совершенным кодам соответственно) в работе [16].

Очевидно, что мощность пересечения расширений кодов C_1 и C_2 посредством общей проверки на четность остается такой же, как и для исходных кодов, причем верно также и обратное.

В данной работе доказано (см. теорему 2), что для любого четного k в интервале $0 \leqslant k \leqslant 2^{2\sum_{i=0}^{r-1}\binom{m-1}{i}}$ существуют $LRM_{r,m}$ коды C и C' с длинами 2^m, пересечение которых равно k. Доказано также (см. теорему 3), что существуют два кода $LRM_{r,m}$ порядка r, имеющих длину по крайней мере 16 и пересекающихся по $2k_1k_2$ кодовым словам, где $1 \leqslant k_s \leqslant |RM_{r-1,m-1}|$, $s \in \{1, 2\}$. Отметим, что полученные результаты обобщают результаты работ [8, 11–13]. Кроме того, значение 2 также достижимо среди указанных множеств чисел пересечений кодов типа Рида – Маллера, и как и в случае совершенных кодов, совокупности чисел пересечений, представленных в этих теоремах, не покрывают друг друга. Для получения данных результатов потребовалось изучить свойства i-компонент кода Рида – Маллера и использовать свитчинговую конструкцию Пулатова [3] для построения кодов типа Рида – Маллера.

§ 2. Необходимые определения и понятия

В этом параграфе рассмотрим необходимые определения и понятия и напомним конструкцию Пулатова [3] для кодов типа Рида – Маллера.

Число η для кодов C_1 и C_2 назовем *числом пересечения* этих кодов. Обозначим выколотый код типа Рида – Маллера порядка r через $LRM^*_{r,m}$. Приведем конструкцию Пулатова. Пусть $LRM^*_{r,m-1}$ и $LRM^*_{r-1,m-1}$ – два выколотых кода типа Рида – Маллера порядков r и $r-1$ длины $2^{m-1}-1$, мощностей 2^{k_r} и $2^{k_{r-1}}$, с кодовыми расстояниями $2^{m-r-1}-1$ и $2^{m-r}-1$ соответственно, где $k_r = \sum\limits_{i=0}^{r} \binom{m-1}{i}$ и $k_{r-1} = \sum\limits_{i=0}^{r-1} \binom{m-1}{i}$. Пусть λ – произвольная функция, действующая на множестве кодовых слов кода $LRM^*_{r-1,m-1}$ со значениями в множестве $\{0,1\}$. Для любых r и $m \geqslant 2$, $0 < r < m$, код, полученный итеративной конструкцией Пулатова

$$\{(x+y, x, |x| + \lambda(y)) : \ x \in LRM^*_{r,m-1}, \ y \in LRM^*_{r-1,m-1}\}, \tag{1}$$

является выколотым кодом типа Рида – Маллера длины $n = 2^m - 1$ с числом кодовых слов 2^k, где $k = \sum\limits_{i=0}^{r} \binom{m}{i}$, и кодовым расстоянием, равным $2^{m-r}-1$.

Если $LRM^*_{r,m-1} = RM^*_{r,m-1}$, $LRM^*_{r-1,m-1} = RM^*_{r-1,m-1}$ и $\lambda \equiv 0$, то код, полученный конструкцией Пулатова, является выколотым линейным кодом Рида – Маллера $RM^*_{r,m}$ порядка r. Конструкция Пулатова (1) для выколотых кодов типа Рида – Маллера является обобщением известной свитчинговой конструкции Васильева для совершенных двоичных кодов [17], а для расширенного случая – известной конструкции Плоткина [1].

Пусть C – произвольный код длины n с кодовым расстоянием d, $d \geqslant 3$. Для $i \in \{1, \ldots, n\}$ через $G_i(C)$ обозначим граф с множеством кодовых слов кода C в качестве множества вершин и с множеством ребер $\{(x,y) : \ d(x,y) = d, \ x_i \neq y_i\}$. Компонента связности K графа $G_i(C)$ называется *i-компонентой* кода C. При этом говорят, что код $C' = (C \setminus K) \cup (K + e_i)$ получен из кода C методом *свитчинга i-компоненты K*. Здесь и далее e_i обозначает вектор веса один пространства $\mathbb{F}^n$, имеющий единицу только в i-й координатной позиции. Код C' имеет те же параметры, что и код C: длину, мощность и кодовое расстояние. Метод свитчинга i-компонент оказался весьма эффективным для построения и исследования свойств совершенных кодов и позволил решить ряд проблем, стоящих для совершенных q-ичных кодов, $q \geqslant 2$ (см. обзоры в работах [9, 18]).

Рассмотрим конструкцию Пулатова (1) в случае, когда $LRM^*_{r,m-1}$ и $LRM^*_{r-1,m-1}$ – выколотые линейные коды Рида – Маллера $RM^*_{r,m-1}$ и $RM^*_{r-1,m-1}$ соответственно, а λ – произвольная функция из множества кодовых слов кода $RM^*_{r-1,m-1}$ в множество $\{0,1\}$:

$$LRM^*_{r,m} = \{(x+y, x, |x| + \lambda(y)) : \ x \in RM^*_{r,m-1}, \ y \in RM^*_{r-1,m-1}\}. \tag{2}$$

Через $\mathbf{0}^n$ обозначим вектор длины n, состоящий из нулевых координат.

Согласно [3] множество

$$R_n = \{(x, x, |x|) : \ x \in RM^*_{r,m-1}\}$$

является n-компонентой кодов $LRM^*_{r,m}$ и $RM^*_{r,m}$, где $n = 2^m - 1$. Легко видеть, что код (2) может быть представлен в виде

$$LRM^*_{r,m} = \left(RM^*_{r,m} \Big\setminus \bigcup_{y \in RM^*_{r-1,m-1}, \, \lambda(y)=1} R^y_n \right) \cup \bigcup_{y \in RM^*_{r-1,m-1}, \, \lambda(y)=1} (R^y_n + e_n), \tag{3}$$

где $R^y_n = R_n + (y, \mathbf{0}^{2^{m-1}})$, $y \in RM^*_{r-1,m-1}$. Код (3) задан свитчинговой конструкцией, так как получен из кода $RM^*_{r,m}$ свитчингами n-компонент R^y_n и $R^y_n + e_n$ для каждого y, удовлетворяющего $\lambda(y) = 1$.

Теорема 1. *Для любых r и m, $2 \leqslant m$, $0 \leqslant r < m$, существуют два выколотых кода типа Рида – Маллера порядка r длины $2^m - 1$ (а также их расширения длины 2^m посредством общей проверки на четность), имеющих пересечение η, где*

$$\eta \in \left\{ |RM^*_{r,m-1}|, 2|RM^*_{r,m-1}|, \ldots, (|RM^*_{r-1,m-1}| - 1)|RM^*_{r,m-1}| \right\}.$$

Доказательство. Для получения требуемых чисел пересечений выколотых кодов типа Рида – Маллера рассмотрим следующие пары кодов длины $2^m - 1$: выколотый код Рида – Маллера порядка r и выколотые коды типа Рида – Маллера порядка r, определенные в (3). Пусть A – произвольное подмножество кодовых слов кода $RM^*_{r-1,m-1}$ и $\lambda(y) = 1$ в случае $y \in A$. Поскольку по определению R^y_n выполняется $|R^y_n| = |RM^*_{r,m-1}|$, то легко видеть, что коды

$$RM^*_{r,m} \quad \text{и} \quad \left(RM^*_{r,m} \setminus \bigcup_{y \in A} R^y_n \right) \cup \bigcup_{y \in A} (R^y_n + e_n)$$

пересекаются по

$$(|RM^*_{r-1,m-1}| - |A|)|RM^*_{r,m-1}|$$

кодовым словам. Выбирая подмножество A в коде $RM^*_{r-1,m-1}$ произвольным образом, т.е. варьируя число кодовых слов y в $RM^*_{r-1,m-1}$, удовлетворяющих $\lambda(y) = 1$, из конструкции (3) немедленно получаем, что следующие числа пересечений η являются достижимыми для выколотых кодов типа Рида – Маллера:

$$\eta \in \left\{ |RM^*_{r,m-1}|, 2|R^*_{r,m-1}|, \ldots, (|RM^*_{r-1,m-1}| - 1)|RM^*_{r,m-1}| \right\}.$$

Заметим, что $(|RM^*_{r-1,m-1}| - 1)|RM^*_{r,m-1}| = |RM^*_{r,m}| - |RM^*_{r,m-1}|$.

Такое же множество чисел пересечений получаем и для расширенных кодов $LRM_{r,m}$. ▲

Отметим, что аналогичный результат был получен для совершенных кодов в работе [8].

§ 3. Пересечение кодов типа Рида – Маллера

В данном параграфе будут получены два существенно более богатых класса чисел пересечений для кодов типа Рида – Маллера, чем те, которые дает прямой свитчинговый метод, описанный в теореме 1. Для достижения этой цели построим два кода типа Рида – Маллера специального вида, используя конструкцию Пулатова (1) для расширенного случая.

Прежде чем привести описание кодов, рассмотрим три вспомогательных леммы, одна из которых взята из работы [13]. Пусть π – циклическая подстановка длины $n/2$, здесь и всюду далее $n = 2^m$. Пусть φ обозначает отображение $x \mapsto x + \pi(x)$ из $\mathbb{F}^{n/2}$ в себя, и пусть $\mathbb{F}^{n/2} = \mathbb{F}^{n/2}_0 \cup \mathbb{F}^{n/2}_1$, где $\mathbb{F}^{n/2}_0$ и $\mathbb{F}^{n/2}_1$ – множества всех векторов четного и нечетного весов в $\mathbb{F}^{n/2}$ соответственно. Обозначим через $\ker(\varphi)$ ядро отображения φ, а через $\dim(\ker(\varphi))$ – его размерность. Для полноты изложения приведем с доказательством лемму из [13] о свойствах отображения φ, которые потребуются нам в дальнейшем.

Лемма 1. *Отображение φ линейно и обладает следующими свойствами*:

1. $\dim(\ker(\varphi)) = 1$;
2. $\varphi(\mathbb{F}^{n/2}) = \mathbb{F}^{n/2}_0$;
3. $\varphi(\mathbb{F}^{n/2}) = V \cup (z + V)$, *где* $V = \varphi(\mathbb{F}^{n/2}_0)$, $z = \varphi(u)$ *для некоторого* $u \in \mathbb{F}^{n/2}_1$ *и* $z + V = \varphi(\mathbb{F}^{n/2}_1)$.

Доказательство. 1. Очевидно, что φ – линейное отображение, и так как $x = \pi(x)$ только при $x \in \{\mathbf{0}^{n/2}, \mathbf{1}^{n/2}\}$, то размерность ядра этого отображения равна 1.

2. Поскольку $w(x) = w(\pi(x))$ для любого $x \in \mathbb{F}^{n/2}$, то справедливо $\varphi(\mathbb{F}^{n/2}) = \mathbb{F}_0^{n/2}$, и размерность $\varphi(\mathbb{F}^{n/2})$, очевидно, равна $\frac{n}{2} - \dim(\ker(\varphi)) = \frac{n}{2} - 1$.

Аналогично $\dim(\varphi(\mathbb{F}_0^{n/2})) = \dim(\varphi(\mathbb{F}^{n/2})) - \dim(\ker(\varphi)) = \frac{n}{2} - 2$.

3. Так как $V = \varphi(\mathbb{F}_0^{n/2})$ – подпространство пространства $\varphi(\mathbb{F}^{n/2})$, то $\varphi(\mathbb{F}^{n/2}) = V \cup (z+V)$, где $z+V$ – класс смежности подпространства V с лидером z. Поскольку $z + V \subset \varphi(\mathbb{F}^{n/2})$, то найдется вектор u в $\mathbb{F}_1^{n/2}$, такой что $z = \varphi(u)$. ▲

Лемма 2. *Для любого кодового слова y из кода $RM_{r-1,m}$, $0 \leqslant r \leqslant m-1$, $4 \leqslant m$, $n = 2^m$, существуют ровно два различных кодовых слова $u, \bar{u} \in RM_{r,m}$, удовлетворяющих $y = u + \pi(u)$ и $y = \bar{u} + \pi(\bar{u})$, где $\bar{u} = u + \mathbf{1}^n$.*

Доказательство. Заметим, что в силу леммы 1 размерность ядра отображения φ равна единице. Отсюда, если существует одно решение для y, т.е. найдется некоторый u, такой что $y = u + \pi(u)$, то решений ровно два, так как антиподальный к u вектор $\bar{u} = u + \mathbf{1}^n$ также удовлетворяет $y = \bar{u} + \pi(\bar{u})$. Поэтому достаточно ограничиться в лемме доказательством существования одного вектора u.

Доказательство проведем индукцией по $m \geqslant 3$. При $m = 3$ имеем вложение кодов Рида–Маллера $RM_{0,3} \subset RM_{1,3} \subset RM_{2,3}$. Непосредственной проверкой для любого кодового слова y кода $RM_{1,3}$, который является расширенным кодом Хэмминга длины 8, легко найти два кодовых слова u и $\bar{u}$ из $RM_{2,3}$, удовлетворяющих $y = u + \pi(u)$ и $y = \bar{u} + \pi(\bar{u})$. Для этого достаточно решить для любого $y = (y_1, \ldots, y_8) \in RM_{1,3}$ систему линейных уравнений $u_i + u_{(i+1) \bmod 8} = y_i$, $i = 1, 2, \ldots, 8$. Положим $u_1 = 0$. Легко проверить, что в этом случае система имеет единственное решение u, $u \in RM_{2,3}$, что дает представление $y = u + \pi(u)$. Второе решение также получаем однозначно, полагая $u_1 = 1$, т.е. имеем $y = \bar{u} + \pi(\bar{u})$. Для наглядности приведем для каждого вектора y^i, $y^i \in RM_{1,3}$, соответствующий вектор u^i, $u^i \in RM_{2,3}$, $i = 1, \ldots, 16$:

$$
\begin{aligned}
y^1 &= (0,0,0,0,0,0,0,0), & u^1 &= (0,0,0,0,0,0,0,0);\\
y^2 &= (1,1,1,1,0,0,0,0), & u^2 &= (0,1,0,1,1,1,1,1);\\
y^3 &= (1,1,0,0,1,1,0,0), & u^3 &= (0,1,1,1,0,1,1,1);\\
y^4 &= (1,0,1,0,1,0,1,0), & u^4 &= (0,0,1,1,0,0,1,1);\\
y^5 &= (1,1,0,0,0,0,1,1), & u^5 &= (0,1,1,1,1,1,0,1);\\
y^6 &= (1,0,1,0,0,1,0,1), & u^6 &= (0,0,1,1,1,0,0,1);\\
y^7 &= (1,0,0,1,1,0,0,1), & u^7 &= (0,0,0,1,0,0,0,1);\\
y^8 &= (1,0,0,1,0,1,1,0), & u^8 &= (0,0,0,1,1,0,1,1);\\
y^9 &= (1,1,1,1,1,1,1,1), & u^9 &= (0,1,0,1,0,1,0,1);\\
y^{10} &= (0,0,0,0,1,1,1,1), & u^{10} &= (0,0,0,0,1,0,1,0);\\
y^{11} &= (0,0,1,1,0,0,1,1), & u^{11} &= (0,0,1,0,0,0,1,0);\\
y^{12} &= (0,1,0,1,0,1,0,1), & u^{12} &= (0,1,1,0,0,1,1,0);\\
y^{13} &= (0,0,1,1,1,1,0,0), & u^{13} &= (0,0,1,0,1,0,0,0);\\
y^{14} &= (0,1,0,1,1,0,1,0), & u^{14} &= (0,1,1,0,1,1,0,0);\\
y^{15} &= (0,1,1,0,0,1,1,0), & u^{15} &= (0,1,0,0,0,1,0,0);\\
y^{16} &= (0,1,1,0,1,0,0,1), & u^{16} &= (0,1,0,0,1,1,1,0).
\end{aligned}
$$

Для кода $RM_{0,3}$ выполняется $\mathbf{1}^8 = u + \pi(u)$, где вектор $u = (0,1,0,1,0,1,0,1)$ принадлежит $RM_{1,3}$.

Пусть при $m-1$ лемма верна, т.е. для каждого кодового слова x произвольного кода Рида – Маллера длины 2^{m-1} порядка не более $m-2$ существует $u \in RM_{r,m-1}$, удовлетворяющий $x = u + \pi(u)$. Докажем справедливость леммы для m и любого $0 \leqslant r \leqslant m-1$.

Согласно конструкции Плоткина для линейных кодов Рида – Маллера имеем

$$RM_{r,m} = \{(x+y, x) :\ x \in RM_{r,m-1},\ y \in RM_{r-1,m-1}\}. \tag{4}$$

По предположению индукции для кодовых слов кодов $RM_{r,m-1}$ и $RM_{r-1,m-1}$ выполняется утверждение леммы.

Обозначим через Π подстановку на 2^m координатных позициях, являющуюся циклическим сдвигом на одну координатную позицию вправо.

Рассмотрим произвольный вектор $(x+y, x)$ кода $RM_{r,m}$. Возможны следующие случаи.

Случай 1. Пусть $x \neq \mathbf{0}^{n/2}$, $x \in RM_{r,m-1}$, $y = \mathbf{0}^{n/2}$, $y \in RM_{r-1,m-1}$, где $n = 2^m$. В этом случае согласно (4) имеем $(x,x) \in RM_{r,m}$ для любого x из $RM_{r,m-1}$. По предположению индукции для вектора x найдется вектор u, такой что $x = u + \pi(u)$. Отсюда

$$(x,x) = (u + \pi(u), u + \pi(u)) = (u,u) + (\pi(u), \pi(u)) = (u,u) + \Pi((u,u)). \tag{5}$$

Случай 2. Пусть $x = \mathbf{0}^{n/2}$, $x \in RM_{r,m-1}$, а $y \neq \mathbf{0}^{n/2}$, $y \in RM_{r-1,m-1}$. По предположению индукции для вектора y найдется вектор $u \in RM_{r,m-1}$, такой что $y = u + \pi(u)$.

Рассмотрим подслучай, когда последняя координата вектора u равна 0. Тогда первая координата вектора $\pi(u)$ равна 0. Следовательно,

$$\begin{aligned}(y, \mathbf{0}^{n/2}) &= (u + \pi(u), \mathbf{0}^{n/2}) = (u, \mathbf{0}^{n/2}) + (\pi(u), \mathbf{0}^{n/2}) = \\ &= (u, \mathbf{0}^{n/2}) + \Pi((u, \mathbf{0}^{n/2})),\end{aligned} \tag{6}$$

где $(u, \mathbf{0}^{n/2}) \in RM_{r,m}$.

Если последняя координата вектора u равна 1, то первая координата вектора $\pi(u)$ кода $\pi(RM_{r,m-1})$ равна 1. В этом случае воспользуемся антиподальностью кода $\pi(RM_{r,m-1})$, согласно которой вектор $\pi(u) + \mathbf{1}^{n/2}$ принадлежит коду $\pi(RM_{r,m-1})$, и следовательно, $(u, \mathbf{1}^{n/2}) \in RM_{r,m}$. Отсюда

$$\begin{aligned}(y, \mathbf{0}^{n/2}) &= (u + \pi(u), \mathbf{1}^{n/2} + \pi(\mathbf{1}^{n/2})) = (u, \mathbf{1}^{n/2}) + (\pi(u), \pi(\mathbf{1}^{n/2})) = \\ &= (u, \mathbf{1}^{n/2}) + \Pi((u, \mathbf{1}^{n/2})).\end{aligned} \tag{7}$$

Случай 3. Пусть $x \neq \mathbf{0}^{n/2}$, где $x \in RM_{r,m-1}$ и $y \neq \mathbf{0}^{n/2}$, $y \in RM_{r-1,m-1}$. По предположению индукции для кодовых слов x и y найдутся два вектора u и v, соответственно, удовлетворяющих $x = u + \pi(u)$ и $y = v + \pi(v)$. Отсюда

$$\begin{aligned}(x+y, x) &= (u + \pi(u) + v + \pi(v), u + \pi(u)) = \\ &= [(u,u) + (\pi(u), \pi(u))] + [(v, \mathbf{0}^{n/2}) + (\pi(v), \mathbf{0}^{n/2})].\end{aligned}$$

Таким образом здесь, как и в случае 1, для вектора (x,x) справедливо (5). Для вектора $(y, \mathbf{0}^{n/2})$ аналогично случаю 2 имеем (6) при $v_{n/2} = 0$, а при $v_{n/2} = 1$ справедливо (7). Отсюда при $v_{n/2} = 0$ вытекает требуемое, а именно:

$$(x+y, x) = (u + v, u) + \Pi((u+v, u)).$$

При $v_{n/2} = 1$ с учетом антиподальности кода Рида – Маллера $RM_{r,m-1}$ имеем

$$(x+y,x) = (u,u) + \Pi((u,u)) + (y, \mathbf{0}^{n/2}) =$$
$$= (u,u) + \Pi((u,u)) + (v, \mathbf{1}^{n/2}) + \Pi((v, \mathbf{1}^{n/2})) =$$
$$= (u+v, u+\mathbf{1}^{n/2}) + \Pi((u+v, u+\mathbf{1}^{n/2})). \quad \blacktriangle$$

Пусть $RM_{r-1,m-1} = P_0 \cup P_1$, где P_0 и P_1 – подкоды кода $RM_{r-1,m-1}$ с одинаковыми и различными первыми двумя координатными позициями соответственно. Пусть ν – транспозиция первых двух координатных позиций векторов из $\mathbb{F}^{n/2}$. Тогда

$$\nu(RM_{r-1,m-1}) = P_0 \cup \nu(P_1),$$

так как $\nu(P_0) = P_0$.

Рассмотрим вектор

$$z = (1,0,1,0,\ldots,1,0) \tag{8}$$

длины $n/2$ с чередующимися координатами, равными 1 и 0. Этот вектор принадлежит коду Адамара $RM_{1,m-1}$, заданному порождающей матрицей, столбцы которой представлены в лексикографическом порядке, и следовательно, принадлежит любому коду Рида – Маллера ненулевого порядка, содержащему этот код Адамара. В частности, $z \in RM_{r-1,m-1}$, и следовательно, вектор z может быть взят в качестве представителя класса смежности P_1 по подкоду P_0, т.е. $P_1 = z + P_0$. Значит, вектор

$$\nu(z) = (0,1,1,0,\ldots,1,0) \in \nu(P_1) \tag{9}$$

может быть взят в качестве представителя класса смежности $\nu(P_1)$ по подкоду P_0, т.е. $\nu(P_1) = \nu(z) + P_0$.

Лемма 3. *Пусть y и y' – произвольные кодовые слова кодов P_0 и $\nu(P_1)$ либо P_1 и $\nu(P_1)$ соответственно. Тогда существуют ровно два различных вектора u и $\bar{u} = u + \mathbf{1}^{n/2}$, удовлетворяющих $y + y' = u + \pi(u)$ и $y + y' = \bar{u} + \pi(\bar{u})$. Более того, оба вектора u и $\bar{u}$ имеют нечетный вес.*

Доказательство. Случай 1. Пусть $y \in P_0$ и $y' \in \nu(P_1)$. Поскольку $\mathbf{0}^{n/2} \in P_0$, достаточно рассмотреть доказательство для $\nu(z) = (0,1,1,0,\ldots,1,0)$ – представителя класса смежности $\nu(P_1)$, поскольку для P_0 справедлива лемма 2. Решая систему линейных уравнений $\nu(z_i) = u_i + u_{i+1}$, $i = 1,2,\ldots,n/2$, полагая $u_1 = 0$, однозначно находим $u = (u_1,\ldots,u_{n/2})$ и $\pi(u)$:

$$u = (0,1,0,0,1,1,\ldots,1,1,0,0), \quad \pi(u) = (0,0,1,0,0,1,1,\ldots,1,1,0),$$

где u и $\pi(u)$ – векторы нечетного веса. Аналогично ищем $\bar{u}$, полагая в этом случае $\bar{u}_1 = 1$:

$$\bar{u} = (1,0,1,1,0,0,\ldots,1,1), \quad \pi(\bar{u}) = (1,1,0,1,1,0,\ldots,0,1),$$

где u и $\pi(u)$ – векторы нечетного веса.

Случай 2. Рассмотрим $y \in P_1$ и $y' \in \nu(P_1)$. Векторы $y \in P_1$ и $y' \in \nu(P_1)$ представимы в виде $y = \widetilde{y} + z$ и $y' = y'' + \nu(z)$ соответственно, где z и $\nu(z)$ определены выше в (8) и (9). Здесь $\widetilde{y}, y'' \in P_0$. Тогда

$$y + y' = \widetilde{y} + y'' + \nu(z) + z,$$

где $\widetilde{y} + y'' \in P_0$. Отсюда с учетом случая 1 данной леммы имеем $\widetilde{y} + y'' + \nu(z) = u + \pi(u)$, где u – вектор нечетного веса. В силу того, что вектор $z \in P_1 \subset RM_{1,m-1}$, по лемме 2

справедливо $z = u' + \pi(u')$, где $u' \in RM_{2,m-1}$, в частности, u' имеет четный вес. Следовательно, для $y + y'$ верно требуемое. ▲

Определим коды $D_\lambda(RM_{r-1,m-1})$ и $D_{\lambda'}(\nu(RM_{r-1,m-1}))$ длины n, используя конструкцию Пулатова для расширенных кодов типа Рида – Маллера.

Первый код имеет вид

$$D_\lambda(RM_{r-1,m-1}) = D_0 \cup D_1,$$
$$D_0 = \bigcup_{y \in RM_{r-1,m-1},\ \lambda(y)=0} \{(x+y, x) :\ x \in RM_{r,m-1},\ y \in RM_{r-1,m-1}\},$$
$$D_1 = \bigcup_{y \in RM_{r-1,m-1},\ \lambda(y)=1} \{(x+y+e_i, x+e_i) :\ x \in RM_{r,m-1},\ y \in RM_{r-1,m-1}\},$$

где λ – произвольная функция, действующая из множества кодовых слов кода $RM_{r-1,m-1}$ в множество $\{0,1\}$, а i – произвольный элемент множества $\{1, 2, \ldots, n/2\}$.

Код $D_{\lambda'}(\nu(RM_{r-1,m-1})) = D'_0 \cup D'_1$ определим, используя подстановки π, ν и произвольную функцию λ', действующую из кода $\nu(RM_{r-1,m-1})$ в множество $\{0,1\}$:

$$D'_0 = \bigcup_{\substack{y \in \nu(RM_{r-1,m-1}),\\ \lambda'(y)=0}} \{(x+y, \pi(x)) :\ x \in RM_{r,m-1},\ y \in \nu(RM_{r-1,m-1})\},$$
$$D'_1 = \bigcup_{\substack{y \in \nu(RM_{r-1,m-1}),\\ \lambda'(y)=1}} \{(x+y+e_i, \pi(x+e_i)) :\ x \in RM_{r,m-1},\ y \in \nu(RM_{r-1,m-1})\},$$

здесь i – то же самое число, что и для кода $D_\lambda(RM_{r-1,m-1})$.

Используя отображение φ, свойства которого описаны в лемме 1, и подстановку ν, введем следующие обозначения:

$$N_0 = |RM_{r-1,m-1} \cap \varphi(RM_{r,m-1})|, \quad N_1 = |RM_{r-1,m-1} \cap \varphi(\mathbb{F}_1^{n/2})|,$$
$$M_0 = |\nu(RM_{r-1,m-1}) \cap \varphi(RM_{r,m-1})|, \quad M_1 = |\nu(RM_{r-1,m-1}) \cap \varphi(\mathbb{F}_1^{n/2})|.$$

Кроме того, далее нам потребуются связанные с сужениями функций λ и λ' на введенные подкоды кодов $RM_{r-1,m-1}$ и $\nu(RM_{r-1,m-1})$ следующие числа:

$$\mu_0 = \big|\{y \in RM_{r-1,m-1} \cap \varphi(RM_{r,m-1}) :\ \lambda(y) = 0\}\big|,$$
$$\mu_1 = \big|\{y \in RM_{r-1,m-1} \cap \varphi(\mathbb{F}_1^{n/2}) :\ \lambda(y) = 0\}\big|,$$
$$\gamma_0 = \big|\{y \in \nu(RM_{r-1,m-1}) \cap \varphi(RM_{r,m-1}) :\ \lambda'(y) = 0\}\big|,$$
$$\gamma_1 = \big|\{y \in \nu(RM_{r-1,m-1}) \cap \varphi(\mathbb{F}_1^{n/2}) :\ \lambda'(y) = 0\}\big|.$$

Лемма 4. *Число векторов, лежащих в пересечении кодов $D_\lambda(RM_{r-1,m-1})$ и $D_{\lambda'}(\nu(RM_{r-1,m-1}))$, равно*

$$2\big(\mu_0\gamma_0 + \mu_1\gamma_1 + (N_0 - \mu_0)(M_1 - \gamma_1) + (N_1 - \mu_1)(M_0 - \gamma_0)\big),$$

где $m \geqslant 4$.

Доказательство. Рассмотрим произвольные кодовые слова этих кодов. В силу определения обоих кодов для совпадения этих кодовых слов имеются только следующие две возможности. Если $(x+y, x) \in D_\lambda(RM_{r-1,m-1})$ и $(x'+y', \pi(x')) \in \in D_{\lambda'}(\nu(RM_{r-1,m-1}))$, где x, x' – векторы четного веса, то

$$(x+y, x) = (x'+y', \pi(x')). \tag{10}$$

Если $(x+y+e_i, x+e_i) \in D_\lambda(RM_{r-1,m-1})$ и $(x'+y'+e_i, \pi(x'+e_i)) \in D_{\lambda'}(\nu(RM_{r-1,m-1}))$, где векторы $x+e_i, x'+e_i$ имеют нечетный вес, то справедливо

$$(x+y+e_i, x+e_i) = (x'+y'+e_i, \pi(x'+e_i)), \tag{11}$$

где $x, x' \in RM_{r,m-1}$, $y \in RM_{r-1,m-1}$ и $y' \in \nu(RM_{r-1,m-1})$. В первом случае имеем $\lambda(y) = \lambda'(y') = 0$, во втором случае $\lambda(y) = \lambda'(y') = 1$.

Рассмотрим первый случай. В этой ситуации имеем $x = \pi(x')$, и значит,

$$y + y' = x + x' = x' + \pi(x') = \varphi(x').$$

Следовательно, равенство (10) эквивалентно системе линейных уравнений

$$\begin{cases} x = x' + y + y', \\ \varphi(x') = y + y'. \end{cases} \tag{12}$$

Возможны следующие подслучаи.

а) Пусть $y, y' \in P_0$ либо $y \in P_1$, а $y' \in P_0$, где множества P_0 и P_1 определены выше, $RM_{r-1,m-1} = P_0 \cup P_1$. Тогда в обоих ситуациях имеем $y + y' \in RM_{r-1,m-1}$, и по лемме 2 для вектора $y + y' \in P_0$ существуют два кодовых слова кода $RM_{r,m-1}$, удовлетворяющих второму уравнению в (12), т.е. $\varphi(x') = y + y'$. Следовательно, система уравнений (12) имеет ровно два различных решения относительно x, x' при фиксированном кодовом слове $y + y'$ из $RM_{r-1,m-1}$.

б) Пусть $y \in P_0$, $y' \in \nu(P_1)$ либо $y \in P_1$, а $y' \in \nu(P_1)$, где подстановка ν определена выше (является транспозицией первых двух координат кодовых слов кода $RM_{r-1,m-1}$), $\nu(RM_{r-1,m-1}) = P_0 \cup \nu(P_1)$. Тогда по лемме 3 для фиксированного вектора $y + y'$ найдутся ровно два решения u, таких что $\varphi(u) = y + y'$, причем оба вектора имеют нечетный вес. Но поскольку $y + y' = x + x'$, где $x + x' \in RM_{r,m-1}$, и в частности, этот вектор имеет четный вес, то система уравнений (12) не имеет решений относительно $x, x' \in RM_{r,m-1}$.

Во втором случае, т.е. при $\lambda(y) = \lambda'(y') = 1$, имеем $x + e_i = \pi(x' + e_i)$, следовательно,

$$y + y' = x + x' = x' + e_i + x + e_i = x' + e_i + \pi(x' + e_i) = \varphi(x' + e_i).$$

С учетом этого равенство (11) эквивалентно системе линейных уравнений

$$\begin{cases} x = x' + y + y', \\ \varphi(x' + e_i) = y + y'. \end{cases} \tag{13}$$

Аналогично рассуждениям, проведенным в первом случае, имеется два различных решения системы (13) относительно $x + e_i, x' + e_i$ в случае $y + y' \in \nu(P_1)$ и нет решений в противном случае. ▲

Лемма 5. *Для кодов $D_\lambda(RM_{r-1,m-1})$ и $D_{\lambda'}(\nu(RM_{r-1,m-1}))$, $m \geqslant 4$, справедливо*

$$N_0 = |RM_{r-1,m-1}|, \quad N_1 = 0, \quad M_0 = M_1 = \frac{1}{2}|RM_{r-1,m-1}|.$$

Доказательство. Из леммы 2 вытекает, что $RM_{r-1,m-1} \subset \varphi(RM_{r,m-1})$, значит, $N_0 = |RM_{r-1,m-1}|$, и как следствие, получаем $N_1 = 0$.

Докажем, что $M_0 = M_1 = \frac{1}{2}|RM_{r-1,m-1}|$. С этой целью рассмотрим векторы $u = (0,1,0,0,1,1,\ldots,1,1,0,0)$ и $\pi(u) = (0,0,1,0,0,1,1,\ldots,1,1,0)$, полученные в доказательстве леммы 3, а также их сумму $\varphi(u) = u + \pi(u) = (0,1,1,0,\ldots,1,0)$. Вектор $u + \pi(u)$ равен вектору $\nu(z)$ из леммы 3, т.е. представителю класса смежности $\nu(P_1)$, поскольку $\nu^{-1}(u + \pi(u)) = (1,0,1,0,\ldots,1,0) = z \in RM_{1,m-1} \subset RM_{r-1,m-1}$ для

любого $1 < r \leqslant m-1$. Так как вектор u имеет нечетный вес, то по лемме 3 выполняется $\nu(RM_{r-1,m-1}) \cap \varphi(\mathbb{F}_1^{n/2}) = \nu(P_1)$. Отсюда $M_1 = \frac{1}{2}|\nu(RM_{r-1,m-1})|$, и поскольку $|\nu(RM_{r-1,m-1})| = |RM_{r-1,m-1}|$, то $M_0 = M_1 = \frac{1}{2}|RM_{r-1,m-1}|$. ▲

Теорема 2. *Для любого четного k в интервале*

$$0 \leqslant k \leqslant 2^{2\sum\limits_{i=0}^{r-1}\binom{m-1}{i}}$$

существуют два кода типа Рида – Маллера порядка r длины 2^m, $m \geqslant 4$, пересечение которых равно k.

Доказательство. Для кодов типа Рида – Маллера $C = D_\lambda(RM_{r-1,m-1})$ и $C' = D_{\lambda'}(\nu(RM_{r-1,m-1}))$, имеющих порядок r и длину $n = 2^m$, из лемм 4 и 5 получаем следующую формулу для числа их пересечения η:

$$\eta(C, C') = 2\Big(\mu_0\gamma_0 + (|RM_{r-1,m-1}| - \mu_0)\Big(\frac{1}{2}|RM_{r-1,m-1}| - \gamma_1\Big)\Big).$$

Варьируя значения функций λ и λ' произвольным образом, т.е. выбирая числа μ_0, γ_i произвольным образом в пределах

$$0 \leqslant \mu_0 \leqslant |RM_{r-1,m-1}|, \quad 0 \leqslant \gamma_i \leqslant \frac{1}{2}|\nu(RM_{r-1,m-1}|, \quad i = 1, 2,$$

с учетом $|\nu(RM_{r-1,m-1})| = |RM_{r-1,m-1}|$ получаем требуемое. ▲

Полагая код C' равным $D_{\lambda'}(RM_{r-1,m-1})$ и оставляя код $C = D_\lambda(RM_{r-1,m-1})$ без изменения, согласно лемме 5 имеем

$$N_0 = M_0 = |RM_{r-1,m-1}|, \quad N_1 = M_1 = 0,$$

т.е. в этом случае выполняется $\mu_1 = \gamma_1 = 0$. Отсюда и из леммы 4 вытекает

Теорема 3. *Для любых чисел k_1 и k_2, удовлетворяющих условиям*

$$1 \leqslant k_s \leqslant 2^{\sum\limits_{i=0}^{r-1}\binom{m-1}{i}}, \quad s \in \{1, 2\},$$

существуют два кода типа Рида – Маллера порядка r длины 2^m, $m \geqslant 4$, пересечение которых равно $2k_1k_2$.

Нетрудно убедиться в том, что множества чисел пересечений кодов типа Рида – Маллера порядка r длины 2^m, полученных в теоремах 2 и 3, не покрывают друг друга.

Автор выражает свою признательность И.Ю. Могильных за плодотворные дискуссии и рецензенту за ряд полезных замечаний, позволивших улучшить изложение настоящей статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. *Liu C.L., Ong B.G., Ruth G.R.* A Construction Scheme for Linear and Non-linear Codes // Discrete Math. 1973. V. 4. № 2. P. 171–184. https://doi.org/10.1016/0012-365X(73)90080-0
3. *Пулатов А.К.* Нижняя оценка сложности схемной реализации для одного класса кодов // Дискретный анализ. Вып. 25. Новосибирск: Ин-т матем. СО АН СССР, 1974. С. 56–61.

4. *Соловьева Ф.И.* О двоичных негрупповых кодах // Методы дискретного анализа в изучении булевых функций и графов. Вып. 37. Новосибирск: Ин-т матем. СО АН СССР, 1981. С. 65–76.
5. *Соловьева Ф.И.* О $\mathbb{Z}_4$-линейных кодах с параметрами кодов Рида – Маллера // Пробл. передачи информ. 2007. Т. 43. № 1. С. 32–38. http://mi.mathnet.ru/ppi4
6. *Pujol J., Rifà J., Solov'eva F.I.* Construction of $\mathbb{Z}_4$-Linear Reed–Muller Codes // IEEE Trans. Inform. Theory. 2009. V. 55. № 1. P. 99–104. https://doi.org/10.1109/TIT.2008.2008143
7. *Solov'eva F.I.* Minimum Weight Bases for Quaternary Reed–Muller Codes // Сиб. электрон. матем. изв. 2021. V. 18. № 2. P. 1358–1366. https://doi.org/10.33048/semi.2021.18.103
8. *Etzion T., Vardy A.* Perfect Binary Codes: Constructions, Properties and Enumeration // IEEE Trans. Inform. Theory. 1994. V.40. № 3. P. 754–763. https://doi.org/10.1109/18.335887
9. *Соловьева Ф.И.* Обзор по совершенным кодам // Математические вопросы кибернетики. Вып. 18. М.: Физматлит, 2013. С. 5–34.
10. *Etzion T., Vardy A.* On Perfect Codes and Tilings: Problems and Solutions // SIAM J. Discrete Math. 1998. V. 11. № 2. P. 205–223. https://doi.org/10.1137/S0895480196309171
11. *Bar-Yahalom E., Etzion T.* Intersection of Isomorphic Linear Codes // J. Combin. Theory. Ser. A. 1997. V. 80. № 2. P. 247–256. https://doi.org/10.1006/jcta.1997.2805
12. *Avgustinovich S.V., Heden O., Solov'eva F.I.* On Intersections of Perfect Binary Codes // Bayreuth. Math. Schr. 2005. № 71. P. 1–6.
13. *Avgustinovich S.V., Heden O., Solov'eva F.I.* On Intersection Problem for Perfect Binary Codes // Des. Codes Cryptogr. 2006. V. 39. № 3. P. 317–322. https://doi.org/10.1007/s10623-005-4982-8
14. *Phelps K.T., Villanueva M.* Intersection of Hadamard Codes // IEEE Trans. Inform. Theory. 2007. V. 53. № 5. P. 1924–1928. https://doi.org/10.1109/TIT.2007.894687
15. *Rifá J., Solov'eva F.I., Villanueva M.* On the Intersection of $\mathbb{Z}_2\mathbb{Z}_4$-Additive Perfect Codes // IEEE Trans. Inform. Theory. 2008. V. 54. № 3. P. 1346–1356. https://doi.org/10.1109/TIT.2007.915917
16. *Rifá J., Solov'eva F.I., Villanueva M.* On the Intersection of $\mathbb{Z}_2\mathbb{Z}_4$-Additive Hadamard Codes // IEEE Trans. Inform. Theory. 2009. V. 55. № 4. P. 1766–1774. https://doi.org/10.1109/TIT.2009.2013037
17. *Васильев Ю.Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. Т. 8. М.: Физматлит, 1962. С. 337–339.
18. *Solov'eva F.I.* Switchings and Perfect Codes // Numbers, Information and Complexity. Boston: Springer, 2000. P. 311–324. https://doi.org/10.1007/978-1-4757-6048-4_25

Соловьева Фаина Ивановна
Институт математики им. С.Л. Соболева
СО РАН, Новосибирск
sol@math.nsc.ru

Поступила в редакцию
25.06.2021
После доработки
10.11.2021
Принята к публикации
10.11.2021