ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 3**

УДК 621.391.1 : 519.725

© 2022 г. **И.Ю. Могильных, Ф.И. Соловьева**

О ВЕСОВОМ СПЕКТРЕ КЛАССА КОДОВ С ПАРАМЕТРАМИ КОДОВ РИДА – МАЛЛЕРА[1]

Приведен новый метод построения дважды экспоненциального класса двоичных кодов с параметрами кодов Рида – Маллера. Исследованы весовой спектр и дистанционная инвариантность предложенных кодов. В построенном классе кодов с параметрами кода Рида – Маллера показано существование кодов с тем же весовым распределением, что и у кода Рида – Маллера, а также кодов с весовым распределением, отличным от него. Установлено, что все коды с параметрами кода Рида – Маллера, полученные конструкцией Васильева – Пулатова, отличные от расширенных совершенных кодов, либо эквивалентны оригинальным кодам Рида – Маллера, либо имеют отличное от них распределение расстояний.

Ключевые слова: код Рида – Маллера, код с параметрами кода Рида – Маллера, весовой спектр, дистанционная инвариантность, обобщенная конструкция Пулатова, свитчинговая конструкция.

DOI: 10.31857/S0555292322030032, **EDN:** EAAOCA

§ 1. Введение

Двоичный линейный *код Рида – Маллера порядка* r, $0 \leqslant r \leqslant m$, обозначаемый через $RM(r,m)$, определяется как совокупность векторов длины 2^m для любого $m \geqslant 1$, отвечающих булевым функциям от m переменных степени не более чем r. Код $RM(r,m)$ имеет мощность 2^k, $k = \sum\limits_{i=0}^{r} \binom{m}{i}$, и *кодовое расстояние* 2^{m-r}. Коды Рида – Маллера обладают рядом хороших свойств. Известно, что код $RM(m-r-1,m)$ является дуальным к коду $RM(r,m)$. Код $RM(m-2,m)$ – расширенный двоичный код Хэмминга, а $RM(1,m)$ – расширенный двоичный код Адамара длины $n = 2^m$, $m \geqslant 2$. Для любых допустимых r и m код $RM(r,m)$ обладает базисом, состоящим из кодовых слов минимального веса (см. [1]). Напомним, что код Рида – Маллера $RM(r+1,m+1)$ представим широко известной в литературе конструкцией Плоткина:

$$\{(x+y\,|\,x) :\ x \in RM(r+1,m),\ y \in RM(r,m)\} \tag{1}$$

(см., например, [1]).

Задача описания весового спектра классических двоичных кодов Рида – Маллера все еще остается открытой, несмотря на значительные усилия и полученные результаты ряда исследователей (см. [2], а также недавние работы [3, 4]).

[1] Исследование выполнено за счет гранта Российского научного фонда № 22-21-00135, https://rscf.ru/project/22-21-00135/

Коды Рида – Маллера обладают хорошими процедурами кодирования и декодирования и в течение многих десятилетий активно используются как на практике, так и в теоретических исследованиях в области теории кодирования и криптографии. Кроме того, в теории блок-схем представляют интерес 3-схемы, получаемые из совокупностей кодовых слов фиксированного веса. Каждая такая схема обладает нетривиальными комбинаторно-алгебраическими свойствами.

В 2009 г. в [5] были предложены полярные схемы, имеющие те же самые параметры, что и схемы кодов Рида – Маллера, но не изоморфные им. Этот результат опроверг широко известную гипотезу Хамады для схем, выдвинутую в 1973 г. в работе [6]. Расширение двоичного кода, натянутого на блоки полярной схемы, полученной из проективной геометрии $PG(2s, 2)$, является кодом, допускающим мажоритарное декодирование и имеет параметры кода Рида – Маллера $RM(s, 2s + 1)$, будучи не эквивалентным ему [7]. В работе [8] показано, что некоторые из этих кодов обладают исключительным свойством иметь то же самое весовое распределение, что и упомянутые коды Рида – Маллера.

Широкие классы двоичных нелинейных кодов с параметрами кодов Рида – Маллера были предложены рядом авторов (см. [9] и список литературы в работе [10], а также [11]). Среди них упомянем конструкции и исследование нетривиальных свойств $\mathbb{Z}_4$-линейных кодов Рида – Маллера (см. [10, 12–14]).

В настоящей статье приведено обобщение свитчинговой конструкции Пулатова [9] для кодов с параметрами классических двоичных кодов Рида – Маллера. Метод построения Пулатова является обобщением широко известной конструкции Васильева для совершенных кодов [15]. Следует отметить, что свитчинговый подход оказался плодотворным для решения многих проблем для совершенных q-ичных кодов, $q \geqslant 2$ (см. [16]).

В данной статье для предложенного нового класса кодов исследованы такие важные инварианты и свойства как весовой спектр и дистанционная инвариантность. Найдены условия, при которых код имеет тот же самый весовой спектр, что и код $RM(r, m)$, а также условия, при которых полученный код является дистанционно инвариантным. Доказано, что дистанционно инвариантные коды из предложенного класса кодов с тем же самым весовым спектром, что и у классического кода Рида – Маллера, но не эквивалентные ему, крайне редки. В частности показано, что таких кодов нет среди оригинальных кодов Пулатова.

§ 2. Конструкция

Основные определения и понятия см. в [1]. Всюду далее через d обозначено кодовое расстояние, а через $w(x)$ – вес вектора x. *Весовой спектр* кода C – это упорядоченный набор W_C, где $W_{C,i}$ равно числу кодовых слов кода C веса i. Двоичный код C называется *дистанционно инвариантным*, если выполняется $W_{C+x} = W_{C+y}$ для любых кодовых слов x и y из C. Вектор $y = (y_1, \ldots, y_n)$ называется *предшествующим* вектору $x = (x_1, \ldots, x_n)$, что записывается в виде $y \preceq x$, если $y_i \leqslant x_i$ для всякого $i = 1, \ldots, n$.

Далее потребуется следующий известный факт.

Утверждение 1. *Для любых векторов z, y справедливо $w(y+z \,|\, z) \geqslant w(y)$, где равенство достижимо в том и только том случае, когда $z \preceq y$.*

Напомним свитчинговую конструкцию Пулатова [9] для кодов с параметрами классических кодов Рида – Маллера.

Пусть e_i – двоичный вектор длины 2^m с 1 лишь в i-й координатной позиции. Пусть $\lambda\colon RM(r, m) \to \{0, 1\}$ – произвольная функция. Тогда множество

$$\big\{(x + y + e_1\lambda(y) \mid x + e_1\lambda(y)) :\ x \in RM(r + 1, m),\ y \in RM(r, m)\big\} \tag{2}$$

является расширенным двоичным кодом Пулатова, имеющим те же параметры, что и код Рида – Маллера $RM(r+1, m+1)$. Полагая функцию λ тождественно равной нулю, получим представление кода $RM(r+1, m+1)$ посредством конструкции Плоткина (1).

Рассмотрим следующее обобщение метода построения Пулатова. Обозначим через $\mathcal{T}$ совокупность представителей (лидеров) смежных классов кода $RM(r+1, m)$ в пространстве $\mathbb{F}^{2^m}$, взятых по одному вектору из каждого смежного класса. Пусть $\lambda\colon RM(r, m) \to \mathcal{T}$ – произвольная функция. Через $RM^{\lambda}(r+1, m+1)$ обозначим следующий код:

$$\big\{(x + y + \lambda(y) \,|\, x + \lambda(y)) : \, x \in RM(r+1, m), \, y \in RM(r, m)\big\}. \tag{3}$$

Для произвольного фиксированного кодового слова y из кода $RM(r, m)$ рассмотрим подкод

$$R_y^{\lambda} = \big\{(x + y + \lambda(y) \,|\, x + \lambda(y)) : \, x \in RM(r+1, m)\big\} \tag{4}$$

кода $RM^{\lambda}(r+1, m+1)$. Таким образом, последний представляет собой следующее объединение подкодов R_y^{λ}:

$$RM^{\lambda}(r+1, m+1) = \bigcup_{y \in RM(r,m)} R_y^{\lambda}. \tag{5}$$

Если λ – тождественно нулевая функция, то через R_y будем обозначать множество

$$\{(x + y \,|\, x) : \, x \in RM(r+1, m)\}.$$

Отсюда с учетом (1) имеем следующее представление классического кода Рида – Маллера:

$$RM(r+1, m+1) = \bigcup_{y \in RM(r,m)} R_y. \tag{6}$$

Для любого $y \in RM(r, m)$ минимальное расстояние подкода R_y^{λ} совпадает с минимальным расстоянием $d = 2^{m-r}$ кода $RM(r, m)$, так как по определению R_y^{λ} (см. (4)) его минимальное расстояние равно минимальному весу ненулевого вектора $(x \,|\, x)$, $x \in RM(r+1, m)$, т.е. $2 \times 2^{m-(r+1)} = 2^{m-r}$. Для различных y, y' из кода $RM(r, m)$ и для любых векторов x, $x' \in RM(r+1, m)$ согласно утверждению 1 справедливо

$$w\big(x + y + \lambda(y) + x' + y' + \lambda(y') \,|\, x + \lambda(y) + x' + \lambda(y')\big) \geqslant w(y + y'),$$

и в свою очередь, вес вектора $y + y'$ не меньше d. Отсюда минимальное расстояние кода $RM^{\lambda}(r+1, m+1)$ равно d. Следовательно, справедлива

Теорема 1. *Для любой функции $\lambda\colon RM(r, m) \to \mathcal{T}$ код $RM^{\lambda}(r+1, m+1)$ имеет ту же самую длину, мощность и минимальное расстояние, что и код Рида – Маллера $RM(r+1, m+1)$.*

Замечание 1. Заметим, что теорема 1 верна также в случае, когда вместо кодов $RM(r, m)$ и $RM(r+1, m)$ рассматриваются произвольные линейные коды C и D, а также для кодов над некоторыми другими метриками, в частности, над метрикой Ли. Полученные ниже весовые свойства этой конструкции кодов Рида – Маллера существенно опираются на результат Касами и Токуры [2] о несуществовании кодовых слов оригинального кода Рида – Маллера, имеющих веса между d и $3d/2$. По этой причине приводимые ниже результаты излагаются лишь для кодов Рида – Маллера.

Следствие 1. *Пусть λ и λ' – функции из $RM(r,m)$ в $\mathcal{T}$, такие что существует y из $RM(r,m)$, для которого $\lambda(y) \neq \lambda'(y)$. Тогда коды $RM^{\lambda}(r+1,m+1)$ и $RM^{\lambda'}(r+1,m+1)$ различны. В частности, имеется*

$$|RM(m-r-2,m)|^{|RM(r,m)|}$$

попарно различных кодов, полученных согласно конструкции (3).

Доказательство. Предположим, что $RM^{\lambda}(r+1,m+1) = RM^{\lambda'}(r+1,m+1)$. Для кодового слова y из $RM(r,m)$, удовлетворяющего условию следствия, и некоторого кодового слова $y' \in RM(r,m)$ рассмотрим кодовые слова

$$(x+y+\lambda(y)\,|\,x+\lambda(y)) \quad \text{и} \quad (x'+y'+\lambda'(y')\,|\,x'+\lambda'(y'))$$

кодов $RM^{\lambda}(r+1,m+1)$ и $RM^{\lambda'}(r+1,m+1)$ соответственно. Если эти векторы совпадают, то

$$\lambda(y)+\lambda'(y') = x+x',$$
$$x+y+\lambda(y) = x'+y'+\lambda'(y').$$

Поскольку x и x' принадлежат коду $RM(r+1,m)$, из первого условия имеем

$$\lambda(y)+\lambda'(y') = x+x' \in RM(r+1,m).$$

Объединяя это со вторым равенством, получаем $y = y'$, и значит, $\lambda(y)+\lambda'(y) \in \in RM(r+1,m)$. Отсюда, так как функции λ и λ' принимают значения в $\mathcal{T}$, получаем, что $\lambda(y) = \lambda'(y)$, противоречие.

Так как код $RM(m-r-2,m)$ дуален коду $RM(r+1,m)$, то размер множества $\mathcal{T}$ равен

$$|\mathbb{F}^{2^m}/RM(r+1,m)| = |RM(m-r-2,m)|.$$

Отсюда с учетом числа различных функций λ, действующих из кода $RM(r,m)$ в множество $\mathcal{T}$, следует требуемая нижняя оценка числа кодов. ▲

§ 3. Основные результаты

В данном параграфе ограничимся случаем, когда функция λ такова, что $y \in \in RM(r,m)$ и $w(\lambda(y)) < d/4$. Всюду далее $d = 2^{m-r}$ – минимальное расстояние кодов $RM(r,m)$ и $RM^{\lambda}(r+1,m+1)$.

3.1. Нижняя граница весового спектра кода $RM^{\lambda}(r+1,m+1)$. В этом пункте коснемся весового спектра кода (5), в частности, исследуем число кодовых слов небольшого веса, меньшего $3d/2$.

Утверждение 2. *Пусть x – кодовое слово кода $RM(r+1,m)$, а y – кодовое слово кода $RM(r,m)$, такое что $w(y) > d$, где $d = 2^{m-r}$. Тогда для любого вектора $u \in \mathbb{F}^{2^m}$ выполняется*

$$w(y+u+x\,|\,u+x) \geqslant w(y) \geqslant 3d/2.$$

Доказательство. Неравенство $w(y+u+x\,|\,u+x) \geqslant w(y)$ справедливо согласно утверждению 1. Распределение небольших, т.е. близких к минимальному, весов в коде Рида – Маллера известно (см. [2]). В частности, вес, следующий за минимальным весом в коде $RM(r,m)$, равен $3d/2$. Значит, так как $w(y) > d$, то $w(y) \geqslant 3d/2$, и утверждение доказано. ▲

Рассматривая достаточно небольшие веса вектора $\lambda(y)$, из следующей леммы получим, что кодовые слова $(x+y+\lambda(y)\,|\,x+\lambda(y))$ кода $RM^{\lambda}(r+1,m+1)$ минимального веса могут возникнуть только вследствие минимальности веса вектора $(x+y\,|\,x)$, либо в случае, когда он нулевой.

Лемма 1. *Пусть* $\lambda\colon RM(r,m)\to\mathcal{T}$ *– произвольная функция, удовлетворяющая условиям* $\lambda(\mathbf{0})=\mathbf{0}$ *и* $w(\lambda(y))<d/4$ *для любого* $y\in RM(r,m)$, *где* $d=2^{m-r}$.

1. *Если* $y\in RM(r,m)$ *таков, что* $w(y)=d$ *и для некоторого* $x\in RM(r+1,m)$ *выполнено*

$$w(x+y+\lambda(y)\,|\,x+\lambda(y))=d,$$

то $w(x+y\,|\,x)=d$;

2. *Для любого* $y\in RM(r,m)$ *имеем* $W_{R_y^{\lambda},d}\leqslant W_{R_y,d}$. *Кроме того, справедливо*

$$W_{RM^{\lambda}(r+1,m+1),d}\leqslant W_{RM(r+1,m+1),d}.$$

Доказательство. 1. Предположим противное, т.е. $w(x+y\,|\,x)>d$. Заметим, что по утверждению 1 имеет место

$$w(x+y\,|\,x)\geqslant w(y)=d.$$

Тогда по теореме Касами и Токуры [2] кодовое слово $(x+y\,|\,x)$ кода $RM(r+1,m+1)$ имеет вес не менее $3d/2$. Тогда, поскольку $w(\lambda(y))<d/4$, то вес вектора $(x+y+\lambda(y)\,|\,x+\lambda(y))$ не может быть равен d, противоречие с условием.

2. Напомним, что

$$R_y^{\lambda}=\big\{(x+y+\lambda(y)\,|\,x+\lambda(y))\colon\ x\in RM(r+1,m)\big\}$$

и

$$R_y=\big\{(x+y\,|\,x)\colon\ x\in RM(r+1,m)\big\}.$$

Согласно (5) код $RM^{\lambda}(r+1,m+1)$ равен $\bigcup\limits_{y\in RM(r,m)}R_y^{\lambda}$, в то время как код Рида–Маллера $RM(r+1,m+1)$ равен $\bigcup\limits_{y\in RM(r,m)}R_y$ (см. (6)). Для каждого $y\in RM(r,m)$ сравним число векторов веса d в подкодах R_y^{λ} и R_y.

Если $y=\mathbf{0}$, то поскольку $\lambda(\mathbf{0})=\mathbf{0}$, имеем $R_{\mathbf{0}}^{\lambda}=R_{\mathbf{0}}$ и $W_{R_y^{\lambda},d}=W_{R_y,d}$.

Если $w(y)=d$, то из первого утверждения настоящей леммы следует, что существует инъективное отображение из множества векторов кода R_y^{λ}, имеющих вес d, в множество векторов из R_y веса d посредством сдвига на вектор $(\lambda(y)\,|\,\lambda(y))$. Следовательно, $W_{R_y^{\lambda},d}\leqslant W_{R_y,d}$.

Всякий вектор из R_y равен $(x+y+\lambda(y)\,|\,x+\lambda(y))$ для некоторого $x\in RM(r+1,m)$. Если $w(y)>d$, то полагая $u=\lambda(y)$ в утверждении 2, убеждаемся, что

$$w(x+y+\lambda(y)\,|\,x+\lambda(y))\geqslant 3d/2,$$

и векторов веса d в R_y^{λ} не существует. ▲

Далее рассмотрим случай, который позволяет получить коды с весовым спектром, отличным от спектра кода $RM(r+1,m+1)$.

Лемма 2. *Пусть* $\lambda\colon RM(r,m)\to\mathcal{T}$ *– произвольная функция, удовлетворяющая условиям* $\lambda(\mathbf{0})=\mathbf{0}$ *и* $w(\lambda(y))<d/4$ *для любого* $y\in RM(r,m)$, *где* $d=2^{m-r}$. *Если найдется кодовое слово* z *в* $RM(r,m)$, *такое что* $w(z)=d$ *и* $\lambda(z)\not\preceq z$, *то*

$$W_{R_z^{\lambda},d}=0\quad\text{и}\quad W_{RM^{\lambda}(r+1,m+1),d}<W_{RM(r+1,m+1),d}.$$

Доказательство. Предположим противное: пусть в $RM^{\lambda}(r+1,m+1)$ существует кодовое слово $(x+z+\lambda(z)\,|\,x+\lambda(z))$ веса d. Тогда по лемме 1, учитывая, что z – вектор веса d, вектор $(x+z\,|\,x)$ имеет вес d. Отсюда $x \preceq z$ согласно утверждению 1. Из утверждения 1, примененного к вектору $(x+z+\lambda(z)\,|\,x+\lambda(z))$, вытекает, что $x+\lambda(z) \preceq z$. Следовательно, $x \preceq z$, $x+\lambda(z) \preceq z$, а по условию $\lambda(z) \not\preceq z$. Так как одновременно все эти три свойства не выполняются, получаем противоречие. ▲

Следующее утверждение описывает "хороший случай" в том смысле, что весовые спектры кодов $RM^{\lambda}(r+1,m+1)$ и $RM(r+1,m+1)$ совпадают.

Утверждение 3. *Справедливо следующее.*

1. *Пусть* $\lambda\colon RM(r,m) \to \mathcal{T}$ *– произвольная функция, удовлетворяющая условию* $\lambda(y) \preceq y$ *для любого* $y \in RM(r,m)$. *Тогда*

$$W_{RM^{\lambda}(r+1,m+1)} = W_{RM(r+1,m+1)}.$$

2. *Для всякого* $0 \leqslant r < m$ *существует не менее*

$$\sum_{i=1}^{\frac{|RM(r,m)|}{2}-1} C^{i}_{|RM(r,m)|} \sum_{j=1}^{2^{m-r-2}-1} C^{j}_{2^{m-r}}$$

различных кодов $RM^{\lambda}(r+1,m+1)$ *с тем же весовым распределением, что и у кода* $RM(r+1,m+1)$, *и не эквивалентных ему.*

Доказательство. 1. Без ограничения общности предположим, что векторы y, x и $\lambda(y)$ имеют вид

$$y = (1,\dots,1\,|\,0,\dots,0),$$
$$x = (x_1,\dots,x_s\,|\,x_{s+1},\dots,x_n),$$
$$\lambda(y) = (1,\dots,1,0,\dots,0\,|\,0,\dots,0),$$

где $w(y)=s$ и $w(\lambda(y))=\ell<s$.

Рассмотрим векторы $(x+y+\lambda(y)\,|\,x+\lambda(y))$ и $(x+y\,|\,x)$. Очевидно, что конкатенация векторов

$$(y+x+\lambda(y)) = (x_1,\dots,x_\ell,x_{\ell+1}+1,\dots,x_s+1\,|\,x_{s+1},\dots,x_n),$$
$$(x+\lambda(y)) = (x_1+1,\dots,x_\ell+1,x_{\ell+1},\dots,x_s\,|\,x_{s+1},\dots,x_n)$$

может быть получена из конкатенации векторов

$$y+x = (x_1+1,\dots,x_s+1\,|\,x_{s+1},\dots,x_n),$$
$$x = (x_1,\dots,x_s\,|\,x_{s+1},\dots,x_n)$$

посредством некоторой подстановки. Следовательно, вектор $(x+y+\lambda(y)\,|\,x+\lambda(y))$ получается перестановкой из вектора $(x+y\,|\,x)$, и

$$W_{RM^{\lambda}(r+1,m+1)} = W_{RM(r+1,m+1)}.$$

2. Рассмотрим не тождественно нулевые функции λ, принимающие нулевые значения на хотя бы $\frac{|RM(r,m)|}{2}+1$ векторах из $RM(r,m)$, один из которых нулевой, и для всех $y \in RM(r,m)$ выполняется $\lambda(y) \preceq y$, где $w(\lambda(y)) < d/4$. Так как для всякой такой функции λ код $RM^{\lambda}(r+1,m+1)$ содержит нулевой вектор и имеет больше половины общих кодовых слов с линейным кодом $RM(r+1,m+1)$, то код $RM^{\lambda}(r+1,m+1)$ не линеен, и следовательно, не эквивалентен коду $RM(r+1,m+1)$. Согласно первому пункту данного утверждения всякий такой код имеет то же весовое распределение, что и $RM(r+1,m+1)$. Значения рассматриваемой функции λ

всегда принадлежат шару радиуса $d/4-1$ и, в свою очередь, множеству лидеров классов смежности линейного кода $RM(r+1,m)$ в $\mathbb{F}^{2^m}$. В силу утверждения 1 получаем, что все такие коды попарно различны. Из того, что каждое кодовое слово кода $RM(r,m)$ имеет вес не менее $d=2^{m-r}$, число возможностей выбрать ненулевой вектор $\lambda(y)$, $\lambda(y)\preceq y$, в шаре радиуса $d/4-1$ с центром в кодовом слове y веса не менее 2^{m-r} равно

$$\sum_{j=1}^{2^{m-r-2}-1} C_{2^{m-r}}^{j}.$$

Отсюда, предварительно выбирая множество кодовых слов из кода $RM(r,m)$, на которых значения функций λ ненулевые, получаем требуемую нижнюю оценку числа таких кодов. ▲

Замечание 2. Случай $r=m-2$ является исключительным. Для всякой функции λ код $RM^{\lambda}(m-2,m)$ является расширенным совершенным кодом, и следовательно, дистанционно инвариантным.

3.2. Дистанционная инвариантность, случай двузначных функций. В этом пункте рассмотрим двузначные функции λ, полагая ненулевое значение функции вектором, имеющим относительно небольшой вес. Покажем, что при этом ограничении на функцию λ не существует дистанционно инвариантных кодов, полученных конструкцией (3) и имеющих то же весовое распределение, что и коды Рида – Маллера, но отличных от них. Как следствие, будет построено большое количество линейных кодов с весовым распределением, отличным от весового распределения кода Рида – Маллера.

Напомним, что базис линейного кода, состоящий из кодовых слов минимального веса, называется *базисом минимального веса*.

Лемма 3. *Для любых* r,m, *таких что* $0\leqslant r\leqslant m$, $1\leqslant m$ *и* $i\in\{1,\dots,2^m\}$, *код*

$$\{u:\ u\in RM(r,m),\ u_i=0\}$$

имеет базис минимального веса.

Доказательство. Доказательство проведем по индукции. Легко убедиться, что для малых m лемма верна.

Пусть для всех $r\leqslant m-1$ и любых i, не превосходящих 2^{m-1}, коды

$$\{x:\ x\in RM(r,m-1),\ x_i=0\}$$

имеют базисы минимального веса.

Согласно конструкции Плоткина (1) выполняется

$$RM(r,m)=\big\{(x+y\,|\,x):\ x\in RM(r,m-1),\ y\in RM(r-1,m-1)\big\}.$$

Из данной конструкции, подставляя $x+y$ вместо x, без ограничения общности можно считать, что $i\geqslant 2^{m-1}+1$. Убедимся, что код

$$\big\{(x+y\,|\,x):\ x\in RM(r,m-1),\ x_i=0,\ y\in RM(r-1,m-1)\big\} \tag{7}$$

имеет базис минимального веса. Напомним, что минимальное расстояние кода $RM(r-1,m-1)$ равно 2^{m-r} и что он имеет базис минимального веса. По предположению индукции код

$$\big\{(x\,|\,x):\ x\in RM(r,m-1),\ x_i=0\big\}$$

также имеет минимальное расстояние 2^{m-r} и обладает базисом минимального веса. Следовательно, код (7) тоже обладает базисом минимального веса. ▲

Утверждение 4. *Пусть для любого $i \in \{1,\dots,2^m\}$ функция λ такова, что $\lambda(y) = y_i e_i$ для каждого $y \in RM(r,m)$. Тогда код $RM^\lambda(r+1,m+1)$ совпадает с кодом $RM(r+1,m+1)$ с точностью до перестановки координатных позиций.*

Доказательство. Зафиксируем произвольный элемент $i \in \{1,\dots,2^m\}$. Так как $\lambda(y) = y_i e_i$ для каждого кодового слова y кода $RM(r,m)$, то $\lambda(y) \preceq y$. Докажем, что транспозиция $\pi = (i, 2^m + i)$ позволяет получить

$$\pi(RM^\lambda(r+1,m+1)) = RM(r+1,m+1).$$

Пусть y – произвольное кодовое слово в $RM(r,m)$, такое что $y_i = 0$. Тогда $\lambda(y) = \mathbf{0}$, и в силу того, что

$$\pi(x+y\,|\,x) = (x+y\,|\,x) \in RM(r+1,m+1),$$

утверждение справедливо.

Если y – кодовое слово кода $RM(r,m)$, такое что $y_i = 1$, то $\lambda(y) = e_i$. Следовательно,

$$\begin{aligned}&\pi(x+y+\lambda(y)\,|\,x+\lambda(y)) = \pi(x+y+e_i\,|\,x+e_i) = \\ &= \pi(x+e_i\,|\,x+e_i) + \pi(y\,|\,\mathbf{0}) = (x+e_i\,|\,x+e_i) + (y+e_i\,|\,e_i) = \\ &= (x+y\,|\,x) \in RM(r+1,m+1). \quad ▲\end{aligned}$$

Теорема 2. *Пусть r, m таковы, что $0 \leqslant r \leqslant m$ и $1 \leqslant m$, $d = 2^{m-r}$, и пусть u – любой вектор из $\mathbb{F}^{2^m}$, такой что $w(u) < d/4$. Пусть λ – произвольная функция из кода $RM(r,m)$ в множество $\{\mathbf{0}, u\}$, где $\lambda(\mathbf{0}) = \mathbf{0}$. Тогда код $RM^\lambda(r+1,m+1)$ является дистанционно инвариантным, и*

$$W_{RM^\lambda(r+1,m+1)} = W_{RM(r+1,m+1)}$$

в том и только том случае, когда с точностью до перестановки координатных позиций он является кодом Рида – Маллера $RM(r+1,m+1)$.

Доказательство. Достаточность очевидна.

Докажем необходимость. Пусть i таково, что $u_i = 1$. Код $RM(r,m)$ равен объединению линейного подкода

$$\{y :\ y \in RM(r,m),\ y_i = 0\}$$

и его смежного класса

$$\{y :\ y \in RM(r,m),\ y_i = 1\}.$$

Обозначим эти подкоды через $RM_0(r,m)$ и $RM_1(r,m)$ соответственно. Рассмотрим значения функции λ на подкоде $RM_0(r,m)$.

Пусть код $RM^\lambda(r+1,m+1)$ дистанционно инвариантен и имеет тот же весовой спектр, что и у кода $RM(r+1,m+1)$. В первую очередь покажем, что λ – тождественно нулевая функция на $RM_0(r,m)$. Предположим противное. Поскольку $\lambda(\mathbf{0}) = \mathbf{0}$ и λ принимает значение u на некотором кодовом слове из $RM_0(r,m)$, то по лемме 3 найдется последовательность кодовых слов $y^1,\dots,y^t$ в коде $RM_0(r,m)$, удовлетворяющих условиям $y^1 = \mathbf{0}$, $\lambda(\mathbf{0}) = \mathbf{0}$, $\lambda(y^t) = u$, таких что для любого $j \in \{1,\dots,t-1\}$ выполняется $d(y^j, y^{j+1}) = d$. Следовательно, в этой последовательности найдутся два вектора из кода $RM_0(r,m)$ (обозначим их через $\widetilde{y}$ и $\overline{y}$) на расстоянии d друг от друга, удовлетворяющие условиям $\lambda(\widetilde{y}) = \mathbf{0}$, $\lambda(\overline{y}) = u$.

Так как $\lambda(\widetilde{y}) = \mathbf{0}$, то вектор $(\widetilde{y}\,|\,\mathbf{0})$ является кодовым словом кода $RM^{\lambda}(r+1, m+1)$. Покажем, что

$$W_{RM^{\lambda}(r+1,m+1)+(\widetilde{y}|\mathbf{0}),d} < W_{RM(r+1,m+1),d}.$$

Для любого $y \in RM(r,m)$ рассмотрим функцию λ', такую что

$$\lambda'(y) = \lambda(y + \widetilde{y}).$$

Согласно определению функции λ' нетрудно видеть, что

$$RM^{\lambda}(r+1, m+1) + (\widetilde{y}\,|\,\mathbf{0}) = RM^{\lambda'}(r+1, m+1).$$

По выбору векторы $\overline{y}$ и $\widetilde{y}$ в коде $RM_0(r,m)$ находятся на расстоянии d друг от друга, а вектор $\overline{y} + \widetilde{y}$ имеет вес d и принадлежит коду $RM_0(r,m)$. Более того, по определению функции λ' имеем

$$\lambda'(\overline{y} + \widetilde{y}) = \lambda(\overline{y} + \widetilde{y} + \widetilde{y}) = \lambda(\overline{y}) = u.$$

Заметим, что i-я координатная позиция кодовых слов кода $RM_0(r,m)$ нулевая, в то время как i-я координатная позиция вектора u равна 1. Отсюда $u \not\leq \overline{y} + \widetilde{y}$.

Применяя лемму 2 к функции λ' и вектору $z = \overline{y} + \widetilde{y}$ веса d, получим

$$W_{RM^{\lambda'}(r+1,m+1),d} = W_{RM^{\lambda}(r+1,m+1)+(\widetilde{y}|\mathbf{0}),d} < W_{RM(r+1,m+1),d}.$$

Следовательно, в случае, когда функция λ имеет ненулевые значения на коде $RM_0(r,m)$, код $RM^{\lambda}(r+1, m+1)$ не может быть дистанционно инвариантным и одновременно иметь весовой спектр, как у кода Рида – Маллера.

Теперь покажем, что λ принимает одинаковые значения на подкоде $RM_1(r,m)$. Предположим противное. Тогда, аналогично вышеприведенным рассуждениям, найдутся два вектора $\widetilde{y}$ и $\overline{y}$ из подкода $RM_1(r,m)$ на расстоянии d друг от друга, такие что $\lambda(\widetilde{y}) = 0$ и $\lambda(\overline{y}) = u$. Введем функцию λ', такую что $\lambda'(y) = \lambda(y + \widetilde{y})$. Заметим, что

$$RM^{\lambda}(r+1, m+1) + (\widetilde{y}\,|\,\mathbf{0}) = RM^{\lambda'}(r+1, m+1).$$

Так как вектор $z = \overline{y} + \widetilde{y}$ имеет вес d и его i-я позиция равна 0, то $\lambda(z) = u \not\leq \overline{y} + \widetilde{y}$, и по лемме 2 получаем, что

$$W_{RM^{\lambda'}(r+1,m+1),d} = W_{RM^{\lambda}(r+1,m+1)+(\widetilde{y}|\mathbf{0}),d} < W_{RM(r+1,m+1),d},$$

противоречие.

Таким образом, функция λ на $RM_1(r,m)$ либо тождественно нулевая, либо является константой, равной u. В последнем случае функция λ тождественно нулевая только на коде $\{y \in RM(r,m),\ y_i = 0\}$. Если предположить, что вес вектора u больше 1, то повторяя доказательство, приведенное выше, для любого i', $u_{i'} = 1$, $i' \neq i$, получим, что λ принимает нулевое значение только на $\{y \in RM(r,m),\ y_{i'} = 0\}$, противоречие.

Следовательно, если код $RM^{\lambda}(r+1, m+1)$ дистанционно инвариантен и имеет весовой спектр, как у кода Рида – Маллера $RM(r+1, m+1)$, то либо λ – тождественно нулевая функция, либо найдется $i \in \{1, \ldots, 2^m\}$, такое что $\lambda(y) = y_i e_i$ для произвольного $y \in RM(r,m)$. В первом случае код $RM^{\lambda}(r+1, m+1)$ совпадает с кодом $RM(r+1, m+1)$, а во втором случае согласно утверждению 4 код $RM^{\lambda}(r+1, m+1)$ эквивалентен коду $RM(r+1, m+1)$. ▲

Функцию $\lambda\colon RM(r,m) \to \mathcal{T}$ назовем *линейной*, если для любых y, $y' \in RM(r,m)$ выполнено

$$\lambda(y+y') + \lambda(y') + \lambda(y) \in RM(r+1,m).$$

Несложно видеть, что для рассматриваемых кодов имеет место следующее

Утверждение 5. *Пусть* $\lambda\colon RM(r,m) \to \mathcal{T}$ *– произвольная линейная функция. Тогда код* $RM^\lambda(r+1,m+1)$ *линеен.*

Следствие 2. *При* $r \leqslant m$ *всякий дистанционно инвариантный код с параметрами кода Рида – Маллера* $RM(r,m)$*, получаемый конструкцией Пулатова* (2) *и имеющий то же весовое распределение, что и код Рида – Маллера* $RM(r,m)$*, совпадает с ним с точностью до перестановки.*

Доказательство. Заметим, что при $r \leqslant m-3$ конструкция Пулатова является частным случаем рассматриваемой конструкции при функции λ, принимающей значения в множество, состоящее из двух фиксированных векторов веса 0 и 1. Отсюда в силу теоремы 2 получаем требуемое. При $r \geqslant m-2$ утверждение также выполнено в силу дистанционной инвариантности любого кода с параметрами расширенного кода Хэмминга или кода, состоящего из всех векторов четного веса. ▲

Широкий класс дистанционно инвариантных кодов можно получить, используя линейные функции в предложенной выше конструкции. Однако в случае, когда функция принимает только два значения достаточно малого веса, весовой спектр полученных кодов не совпадает с таковым для классического кода Рида – Маллера, либо приводит к коду Рида – Маллера с точностью до перестановки координатных позиций (см. теорему 2).

Следствие 3. *При* $r \leqslant m-3$ *существует по крайней мере*

$$(|RM(r,m)|-1)\left(-1+\sum_{i=0}^{d/4-1}\binom{2^m}{i}\right)-2^m+1$$

попарно различных линейных кодов $RM^\lambda(r+1,m+1)$ *с параметрами кодов Рида – Маллера* $RM(r+1,m+1)$*, таких что*

$$W_{RM^\lambda(r+1,m+1),d} < W_{RM(r+1,m+1),d}.$$

Доказательство. Рассмотрим произвольную не тождественно нулевую линейную функцию

$$\lambda\colon RM(r,m) \to \{\mathbf{0}, u\}, \quad w(u) < d/4.$$

Число выборов вектора u равно

$$-1+\sum_{i=0}^{d/4-1}\binom{2^m}{i}.$$

Отсюда получаем, что количество таких функций равно этому числу способов выбрать вектор u, умноженному на число способов задать значение функции λ, равному вектору u на непустом множестве базисных векторов кода $RM(r,m)$. Из полученных функций мы исключаем 2^m-1 функций вида $\lambda(y) = y_i e_i$, $i \in \{1,\ldots,2^m\}$, так как в силу утверждения 5 коды, соответствующие им, эквивалентны оригинальным кодам Рида – Маллера. В силу доказательства теоремы 2 все остальные коды $RM^\lambda(r+1,m+1)$ удовлетворяют неравенству

$$W_{RM^\lambda(r+1,m+1),d} < W_{RM(r+1,m+1),d}. \quad ▲$$

Следующий результат был получен с помощью компьютера на основе вышеизложенных ограничений на весовое распределение кодов $RM^{\lambda}(2,5)$.

Утверждение 6. *Всякий линейный код* $RM^{\lambda}(2,5)$ *либо эквивалентен коду* $RM(2,5)$, *либо удовлетворяет условию*

$$W_{RM^{\lambda}(2,5),8} < W_{RM(2,5),8}.$$

§ 4. Заключение

В статье предложена новая конструкция двоичных кодов с параметрами кодов Рида – Маллера. Из утверждения 3 вытекает существование богатого множества кодов с теми же самыми параметрами и весовым спектром, что и у кодов Рида – Маллера. Результаты § 3 позволяют сделать вывод, что достаточно трудно обнаружить дистанционно инвариантные коды с числом кодовых слов минимального веса, как у кода Рида – Маллера, но не эквивалентных ему.

Авторы выражают благодарность С.В. Августиновичу и В.Н. Потапову, обратившим внимание авторов на задачу описания весового спектра кодов с параметрами кодов Рида – Маллера.

СПИСОК ЛИТЕРАТУРЫ

1. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. *Kasami T., Tokura N.* On the Weight Structure of Reed–Muller Codes // IEEE Trans. Inform. Theory. 1970. V. 16. № 6. P. 752–759. https://doi.org/10.1109/TIT.1970.1054545
3. *Abbe E., Shpilka A., Ye M.* Reed–Muller Codes: Theory and Algorithms // IEEE Trans. Inform. Theory. 2021. V. 67. № 6. Part 1. P. 3251–3277. https://doi.org/10.1109/TIT.2020.3004749
4. *Kaufman T., Lovett S., Porat E.* Weight Distribution and List-Decoding Size of Reed–Muller Codes // IEEE Trans. Inform. Theory. 2012. V. 58. № 5. P. 2689–2696. https://doi.org/10.1109/TIT.2012.2184841
5. *Jungnickel D., Tonchev V.D.* Polarities, Quasi-symmetric Designs, and Hamada's Conjecture // Des. Codes Cryptogr. 2009. V. 51. № 2. P. 131–140. https://doi.org/10.1007/s10623-008-9249-8
6. *Hamada N.* On the p-Rank of the Incidence Matrix of a Balanced or Partially Balanced Incomplete Block Design and Its Application to Error-Correcting Codes // Hiroshima Math. J. 1973. V. 3. № 1. P. 153–226. https://doi.org/10.32917/hmj/1206137446
7. *Clark D., Tonchev V.D.* A New Class of Majority-Logic Decodable Codes Derived from Polarity Designs // Adv. Math. Commun. 2013. V. 7. № 2. P. 175–186. https://doi.org/10.3934/amc.2013.7.175
8. *Harada M., Novak E., Tonchev V.* The Weight Distribution of the Self-dual [128, 64] Polarity Design Code // Adv. Math. Commun. 2016. V. 10. № 3. P. 643–648. https://doi.org/10.3934/amc.2016032
9. *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.
10. *Соловьева Ф.И.* О пересечении кодов типа Рида – Маллера // Пробл. передачи информ. 2021. Т. 57. № 4. С. 63–73. https://doi.org/10.31857/S0555292321040057
11. *Соловьева Ф.И.* О построении кодов типа Рида – Маллера и исследовании их свойств // Тр. МФТИ. 2022. Т. 14. № 2. С. 110–123. https://www.elibrary.ru/ygvlwy
12. *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
13. *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

14. *Solov'eva F.I.* Minimum Weight Bases for Quaternary Reed–Muller Codes // Сиб. электрон. матем. изв. 2021. Т. 18. № 2. С. 1358–1366. https://doi.org/10.33048/semi.2021.18.103
15. *Васильев Ю.Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. Т. 8. М.: Физматлит, 1962. С. 337–339.
16. *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

Могильных Иван Юрьевич
Институт математики им. С.Л. Соболева
СО РАН, Новосибирск
ivmog@math.nsc.ru
Соловьева Фаина Ивановна
(15.08.1952 – 09.08.2022)

Поступила в редакцию
01.04.2022
После доработки
16.06.2022
Принята к публикации
18.06.2022