ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 3**

УДК 621.391 : 519.725

© 2021 г. **А.М. Романов**

О СОВЕРШЕННЫХ КОДАХ И КОДАХ РИДА – МАЛЛЕРА НАД КОНЕЧНЫМИ ПОЛЯМИ[1]

Рассматриваются коды с исправлением ошибок над конечным полем с q элементами (q-ичные коды). Изучается связь q-ичных совершенных кодов с исправлением одной ошибки и q-ичных кодов Рида – Маллера. При $q \geqslant 3$ найдены параметры аффинных кодов Рида – Маллера порядка $(q-1)m-2$. Показано, что аффинные коды Рида – Маллера порядка $(q-1)m-2$ являются квазисовершенными кодами. Предложена конструкция, которая позволяет строить q-ичные совершенные коды, исправляющие одну ошибку, из кодов с параметрами аффинных кодов Рида – Маллера. Модификация этой конструкции позволяет строить q-ичные квазисовершенные коды с параметрами аффинных кодов Рида – Маллера.

Ключевые слова: код Рида – Маллера, аффинный код Рида – Маллера, проективный код Рида – Маллера, код Хэмминга, совершенный код, квазисовершенный код, МДР-код, конечное поле.

DOI: 10.31857/S0555292321030013

§ 1. Введение

В данной статье рассматриваются аффинные и проективные коды Рида – Маллера и совершенные коды с исправлением одной ошибки (1-совершенные коды). Все эти коды определяются над конечным полем $\mathbb{F}_q$ и являются q-ичными кодами. В статье изучается связь между q-ичными кодами Рида – Маллера и q-ичными 1-совершенными кодами.

Классические коды Рида – Маллера являются двоичными кодами и определяются над конечным полем $\mathbb{F}_2$ (см. [1, гл. 13]). Без преувеличения можно сказать, что коды Рида – Маллера являются наиболее известным и изученным классом двоичных кодов с исправлением ошибок. Аффинные коды Рида – Маллера были открыты в работе [2] и были названы авторами этой работы обобщенными кодами Рида – Маллера. Аффинные коды Рида – Маллера являются прямым обобщением двоичных кодов Рида – Маллера и определяются над любым конечным полем $\mathbb{F}_q$. В данной статье при $q \geqslant 3$ найдены параметры аффинных кодов Рида – Маллера порядка $(q-1)m-2$.

Значительно позднее были открыты так называемые проективные коды Рида – Маллера [3]. Из работ [3, 4] следует, что при $q \geqslant 3$ проективный код Рида – Маллера порядка $(q-1)m-1$ является q-ичным кодом Хэмминга длины $n = (q^{m+1}-1)/(q-1)$.

Группы автоморфизмов аффинных кодов Рида – Маллера известны [5]. Исследование групп автоморфизмов проективных кодов Рида – Маллера предложено в [6].

[1] Работа выполнена при поддержке программы фундаментальных научных исследований СО РАН № I.5.1., проект № 0314-2019-0017.

Хорошо известна связь между расширенными двоичными кодами Хэмминга и кодами Рида – Маллера. Известно, что расширенный двоичный код Хэмминга длины 2^m является кодом Рида – Маллера длины 2^m и порядка $m-2$. Также известно, что код Рида – Маллера порядка $m-2$ (двоичный расширенный код Хэмминга) можно построить с помощью $(\boldsymbol{u}\,|\,\boldsymbol{u}+\boldsymbol{v})$-конструкции [1, с. 76]. Вертикальная черта $(\cdot\,|\,\cdot)$ обозначает конкатенацию. Следует заметить, что с помощью $(\boldsymbol{u}\,|\,\boldsymbol{u}+\boldsymbol{v})$-конструкции можно построить код Рида – Маллера любого порядка [7, с. 34].

Одним из наиболее простых и распространенных методов построения нелинейных двоичных 1-совершенных кодов является комбинаторное обобщение $(\boldsymbol{u}\,|\,\boldsymbol{u}+\boldsymbol{v})$-конструкции (см., например, [8]). При этом этот метод позволяет строить как нелинейные двоичные 1-совершенные коды, так и расширенные нелинейные двоичные 1-совершенные коды. В [9] Фелпс представил комбинаторную конструкцию расширенных двоичных 1-совершенных кодов. В [10] он предложил многомерное обобщение двоичной комбинаторной конструкции из [9] также на двоичный случай. Работы Фелпса [9, 10] являются классическими работами по теории нелинейных совершенных кодов. В [8] дано обобщение двоичной комбинаторной $(\boldsymbol{u}\,|\,\boldsymbol{u}+\boldsymbol{v})$-конструкции на q-ичный случай. В настоящей статье предложена конструкция, обобщающая конструкции из [8, 10] и позволяющая строить q-ичные 1-совершенные коды из q-ичных кодов с параметрами аффинных кодов Рида – Маллера порядка $(q-1)m-2$. Модификация этой конструкции позволяет строить q-ичные квазисовершенные коды с параметрами аффинных кодов Рида – Маллера порядка $(q-1)m-2$. Приведены также нижние оценки для числа неэквивалентных q-ичных 1-совершенных кодов и для числа неэквивалентных q-ичных квазисовершенных кодов с параметрами аффинных кодов Рида – Маллера порядка $(q-1)m-2$.

Методы построения кодов из [8–10] и метод, предлагаемый в настоящей статье, являются примерами конструкции обобщенных каскадных кодов [11].

Из результатов настоящей статьи следует, что аффинные коды Рида – Маллера порядка $(q-1)m-2$ играют такую же роль в теории q-ичных 1-совершенных кодов, что и расширенные двоичные коды Хэмминга в теории двоичных 1-совершенных кодов.

Аффинные коды Рида – Маллера порядка $(q-1)m-2$, так же как и расширенные двоичные коды Хэмминга, являются линейными квазисовершенными кодами, и следовательно, равномерно упакованными и полностью регулярными кодами.

Известно, что коды, имеющие параметры расширенных двоичных кодов Хэмминга, являются квазисовершенными, равномерно упакованными и полностью регулярными [12].

В § 2 приведены необходимые определения и обозначения. В § 3 дано определение аффинных кодов Рида – Маллера и найдены параметры аффинных кодов Рида – Маллера длины q^m и порядка $(q-1)m-2$. В § 4 дано определение проективных кодов Рида – Маллера и показано, что при $q \geqslant 3$ код Хэмминга длины $n=(q^{m+1}-1)/(q-1)$ является проективным кодом Рида – Маллера порядка $(q-1)m-1$. В § 5 приведены конструкции 1-совершенных кодов и кодов с параметрами аффинных кодов Рида – Маллера.

§ 2. Определения и обозначения

Пусть $\mathbb{F}_q^n$ – векторное пространство размерности n над конечным полем $\mathbb{F}_q$, где q – степень простого числа. Произвольное подмножество $\mathcal{C} \subseteq \mathbb{F}_q^n$ называется *q-ичным кодом с исправлением ошибок* (кратко – q-ичным кодом). *Длина* кода $\mathcal{C} \subseteq \mathbb{F}_q^n$ равна размерности пространства $\mathbb{F}_q^n$. Мы предполагаем, что нулевой вектор $\mathbf{0}$ всегда принадлежит коду, если не указано иное. Код называется *линейным*, если он образует линейное подпространство над $\mathbb{F}_q$. В противном случае код называется *нелинейным*. Векторы, принадлежащие пространству $\mathbb{F}_q^n$, будем рассматривать как слова длины n

над алфавитом $\mathbb{F}_q$. Слова, принадлежащие коду $\mathcal{C} \subseteq \mathbb{F}_q^n$, будем называть *кодовыми словами*.

Расстояние Хэмминга $d(\boldsymbol{x}, \boldsymbol{y})$ между двумя векторами $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$ равно числу ненулевых координатных позиций в векторе $\boldsymbol{x} - \boldsymbol{y}$. *Вес* вектора $\boldsymbol{x} \in \mathbb{F}_q^n$ равен $d(\boldsymbol{x}, \boldsymbol{0})$. *Минимальное расстояние* кода $\mathcal{C}$ равно наименьшему расстоянию Хэмминга между двумя различными кодовыми словами из $\mathcal{C}$ и обозначается через $d(\mathcal{C})$. Линейный q-ичный код длины n и размерности $\dim(\mathcal{C}) = k$ с минимальным расстоянием d называется $[n, k, d]_q$-кодом. Нелинейный q-ичный код длины n с M кодовыми словами и минимальным расстоянием d называется $(n, M, d)_q$-кодом.

Для кода с параметрами $(n, M, d)_q$ справедливо неравенство

$$M \leqslant q^{n-d+1}. \tag{1}$$

Неравенство (1) называется *границей Синглтона*. Коды, достигающие границы Синглтона, называются *разделимыми кодами с максимальным расстоянием*, или кратко МДР-кодами. В данной статье будут рассматриваться МДР-коды только с минимальным расстоянием 2.

Для кода с параметрами $(n, M, d)_q$ справедливо также неравенство

$$q^n \geqslant M \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} (q-1)^i \binom{n}{i}, \tag{2}$$

где $\lfloor \cdot \rfloor$ обозначает целую часть числа. Неравенство (2) называется *границей сферической упаковки*. Коды, достигающие границы сферической упаковки, называются *совершенными кодами*. Совершенные q-ичные коды с минимальным расстоянием 3 (т.е. коды, исправляющие одну ошибку) называются q-ичными 1-*совершенными* кодами. Линейные q-ичные 1-совершенные коды называются q-ичными *кодами Хэмминга* и обозначаются через $\mathcal{H}_q(m)$. Коды Хэмминга имеют следующие параметры:

1. Длина q-ичного кода Хэмминга $\mathcal{H}_q(m)$ равна $n = \dfrac{q^m - 1}{q - 1}$, где $m \geqslant 2$;
2. Размерность q-ичного кода Хэмминга $\mathcal{H}_q(m)$ равна $n - m$;
3. Минимальное расстояние q-ичного кода Хэмминга $\mathcal{H}_q(m)$ равно 3.

Параметры нелинейных q-ичных 1-совершенных кодов длины n совпадают с параметрами q-ичного кода Хэмминга длины n.

Коды $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$ называются *различными*, если $\mathcal{C}_1 \neq \mathcal{C}_2$. Два кода $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$ называются *эквивалентными*, если существует вектор $\boldsymbol{v} \in \mathbb{F}_q^n$ и мономиальная матрица M размера $n \times n$ над полем $\mathbb{F}_q$, такие что

$$\mathcal{C}_2 = \{(\boldsymbol{v} + \boldsymbol{c}M) \mid \boldsymbol{c} \in \mathcal{C}_1\}.$$

Известно, что существует единственный с точностью до эквивалентности q-ичный код Хэмминга длины n (см. [7, теорема 1.8.2]).

Определим *радиус упаковки* $e(\mathcal{C})$ кода $\mathcal{C} \subseteq \mathbb{F}_q^n$. Положим $e(\mathcal{C}) = \lfloor (d-1)/2 \rfloor$, где d – минимальное расстояние кода $\mathcal{C}$. Определим также *радиус покрытия* $\rho(\mathcal{C})$ кода $\mathcal{C}$. Положим

$$\rho(\mathcal{C}) = \max_{\boldsymbol{x} \in \mathbb{F}_q^n} \min_{\boldsymbol{c} \in \mathcal{C}} d(\boldsymbol{x}, \boldsymbol{c}).$$

Код $\mathcal{C}$ является совершенным тогда и только тогда, когда $\rho(\mathcal{C}) = e(\mathcal{C})$. Код $\mathcal{C}$ называется *квазисовершенным*, если $\rho(\mathcal{C}) = e(\mathcal{C}) + 1$ (см. [1, с. 19]).

Далее определим функцию $p\colon \mathbb{F}_q^n \to \mathbb{F}_q$. Если $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$, то

$$p(\boldsymbol{x}) = \sum_{i=1}^{n} x_i.$$

Функция $p(\boldsymbol{x})$ называется *функцией четности*. Пусть q-ичный код $\mathcal{C}$ имеет параметры $(n, M, d)_q$. Тогда определим *расширенный* код $\widehat{\mathcal{C}}$. Положим

$$\widehat{\mathcal{C}} = \big\{\boldsymbol{x} = (x_1, x_2, \ldots, x_n, x_{n+1}) \in \mathbb{F}_q^{n+1} \mid (x_1, x_2, \ldots, x_n) \in \mathcal{C} \text{ и } p(\boldsymbol{x}) = 0\big\}.$$

Расширенный код $\widehat{\mathcal{C}}$ имеет параметры $(n+1, M, \widehat{d})_q$, где $\widehat{d} = d$ или $d+1$ [7, с. 14]. Говорят, что код $\widehat{\mathcal{C}}$ получен из кода $\mathcal{C}$ добавлением общей проверки на четность.

Вектор $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ называется *четным*, если $p(\boldsymbol{x}) = \sum\limits_{i=1}^{n} x_i = 0$. Код называется *четным*, если он имеет только четные кодовые слова. Четный код длины n является подкодом линейного МДР-кода с параметрами $[n, n-1, 2]_q$.

Все не определенные в данной статье понятия можно найти в [1, 7].

§ 3. Аффинные коды Рида – Маллера

Рассмотрим алгебру $\mathbb{F}_q[X_1, X_2, \ldots, X_m]$ многочленов от m переменных над полем $\mathbb{F}_q$. Через $\deg(f)$ обозначим полную степень многочлена f из $\mathbb{F}_q[X_1, X_2, \ldots, X_m]$. Пусть $n = q^m$, и пусть точки $P_1, P_2, \ldots, P_n$ аффинного пространства $AG(m, q)$ размерности m над полем $\mathbb{F}_q$ некоторым образом упорядочены. Пусть r – целое число, такое что $0 \leqslant r \leqslant (q-1)m$. Тогда аффинным (или обобщенным [2]) кодом Рида – Маллера порядка r над полем $\mathbb{F}_q$ называется подпространство

$$RM_q(r, m) = \big\{(f(P_1), f(P_2), \ldots, f(P_n)) \mid f \in \mathbb{F}_q[X_1, X_2, \ldots, X_m],\ \deg(f) \leqslant r\big\}.$$

Аффинные коды Рида – Маллера $RM_q(r, m)$ порядка r над полем $\mathbb{F}_q$ имеют следующие параметры (см. [2; 13, теорема 5.5]):

1. Длина кода $RM_q(r, m)$ равна q^m;
2. Размерность кода $RM_q(r, m)$ равна

$$\sum_{k=0}^{m} (-1)^k \binom{m}{k} \binom{m + r - kq}{r - kq}; \tag{3}$$

3. Минимальное расстояние кода $RM_q(r, m)$ равно

$$(q-b)q^{m-a-1}, \tag{4}$$

где $r = (q-1)a + b$ и $0 \leqslant b < q-1$.

При $q = 2$ и $0 \leqslant r \leqslant m$ аффинный код Рида – Маллера порядка r является классическим кодом Рида – Маллера порядка r (см. [13, пример 5.4]).

Утверждение 1. *При $q \geqslant 3$ аффинный код Рида – Маллера над полем $\mathbb{F}_q$ длины $n = q^m$ и порядка $(q-1)m - 2$ имеет размерность $n - m - 1$ и минимальное расстояние* 3.

Доказательство. Если код $\mathcal{C}$ принадлежит классу аффинных кодов Рида – Маллера, то и дуальный код $\mathcal{C}^{\perp}$ также принадлежит этому классу [14]. Допустим, что длина кода $\mathcal{C}$ равна n. Тогда

$$\dim(\mathcal{C}) + \dim(\mathcal{C}^{\perp}) = n. \tag{5}$$

Из [13, теорема 5.8] следует, что при $r < (q-1)m$

$$RM_q(r,m)^{\perp} = RM_q((q-1)m-1-r,m).$$

Следовательно, порядок кода, дуального к коду $RM_q((q-1)m-2,m)$, равен 1. В силу формул (3) и (5) размерность аффинного кода Рида – Маллера $RM_q((q-1)m-2,m)$ равна $n-m-1$.

Теперь покажем, что минимальное расстояние кода $RM_q((q-1)m-2,m)$ равно 3. Поскольку

$$r = (q-1)m-2 = (q-1)a+b \quad \text{и} \quad 0 \leqslant b < q-1,$$

то при $q \geqslant 3$ имеем $a = m-1$ и $b = q-3$. Следовательно, в силу формулы (4) код $RM_q((q-1)m-2,m)$ имеет минимальное расстояние 3. ▲

Аффинный код Рида – Маллера порядка $(q-1)m-1$ является линейным q-ичным МДР-кодом длины q^m с минимальным расстоянием 2. Очевидно, что если $r < v$, то $RM_q(r,m) \subset RM_q(v,m)$. Следовательно, код $RM_q((q-1)m-2,m)$ является подкодом линейного МДР-кода длины q^m с минимальным расстоянием 2, т.е. четным кодом.

Утверждение 2. *Аффинный код Рида – Маллера $RM_q((q-1)m-2,m)$ является квазисовершенным кодом.*

Доказательство. Аффинный код Рида – Маллера 1-го порядка является линейным двухвесовым кодом [14]. Согласно [15, теорема 5.10] код, дуальный к линейному двухвесовому коду, имеет радиус покрытия 2. Следовательно, аффинные коды Рида – Маллера порядка $(q-1)m-2$ являются квазисовершенными. ▲

В силу [16, теорема 3.11] линейные квазисовершенные коды являются равномерно упакованными. Равномерно упакованные коды достигают границы Джонсона и являются оптимальными кодами [16, теорема 1.3]. Известно также, что равномерно упакованный код полностью регулярен [17].

§ 4. Проективные коды Рида – Маллера

Пусть r – целое число, такое что $1 \leqslant r \leqslant (q-1)m$. Рассмотрим множество $\mathbb{S}_r$ однородных многочленов полной степени r над полем $\mathbb{F}_q$ от переменных $X_0, X_1, \ldots, X_m$. Пусть $n = \dfrac{q^{m+1}-1}{q-1}$, и пусть точки $P_0, P_1, \ldots, P_{n-1}$ проективного пространства $PG(m,q)$ размерности m над полем $\mathbb{F}_q$ некоторым образом упорядочены. Точки проективного пространства $PG(m,q)$ задаются так, чтобы крайняя левая ненулевая координата была равна единице. Тогда проективный код Рида – Маллера порядка r над полем $\mathbb{F}_q$ состоит из слов

$$PRM_q(r,m) = \big\{(f(P_0), f(P_1), \ldots, f(P_{n-1})) \mid f \in \mathbb{S}_r \cup \{\mathbf{0}\}\big\}.$$

Длина проективного кода Рида – Маллера $PRM_q(r,m)$ равна $n = \dfrac{q^{m+1}-1}{q-1}$. Известны и другие параметры проективных кодов Рида – Маллера [3, 4].

Утверждение 3. *При $q \geqslant 3$ проективный код Рида – Маллера над полем $\mathbb{F}_q$ длины $n = \dfrac{q^{m+1}-1}{q-1}$ и порядка $(q-1)m-1$ является кодом Хэмминга $\mathcal{H}_q(m+1)$.*

Доказательство. Проективный q-ичный код Рида – Маллера первого порядка является q-ичным симплексным кодом [3]. Известно, что q-ичный симплексный код дуален q-ичному коду Хэмминга [7, с. 30].

Пусть $\mu = (q-1)m - \nu$. Тогда в [4] доказано, что

$$PRM_q(\nu, m)^{\perp} = PRM_q(\mu, m) \quad \text{при} \quad \nu \neq 0 \mod (q-1),$$
$$PRM_q(\nu, m)^{\perp} = \overline{PRM_q(\mu, m)} \quad \text{при} \quad \nu = 0 \mod (q-1),$$

где код $\overline{PRM_q(\mu, m)}$ порождается проективным кодом Рида – Маллера $PRM_q(\mu, m)$ и вектором, состоящим из единиц. Таким образом, мы получаем, что при $q \geqslant 3$ код Хэмминга длины $n = \dfrac{q^{m+1}-1}{q-1}$ является проективным кодом Рида – Маллера порядка $(q-1)m - 1$. ▲

При $q = 2$, $m \geqslant 2$ проективный код Рида – Маллера $PRM_2(m-1, m)$ является четной половиной двоичного кода Хэмминга $\mathcal{H}_2(m+1)$ и является полностью регулярным кодом [12].

§ 5. Конструкции кодов

В этом параграфе представлена конструкция q-ичных 1-совершенных кодов. Эта конструкция основана на разбиениях и является обобщением конструкций из [8,10]. Модификация этой конструкции позволяет строить квазисовершенные коды с параметрами аффинных кодов Рида – Маллера. Приведены также нижние оценки для числа неэквивалентных q-ичных 1-совершенных кодов и для числа неэквивалентных q-ичных квазисовершенных кодов с параметрами аффинных кодов Рида – Маллера.

1. Пусть $\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_{(q-1)n}$ – разбиение пространства $\mathbb{F}_q^n$ на q-ичные 1-совершенные коды длины $n = \dfrac{q^{s_1}-1}{q-1}$, где $s_1 \geqslant 2$.
2. Пусть пространство $\mathbb{F}_q^{(q-1)n+1}$ разбито на смежные классы, образованные аффинным кодом Рида – Маллера $RM_q((q-1)s_1 - 1, s_1)$ порядка $(q-1)s_1 - 1$. Поскольку $n = \dfrac{q^{s_1}-1}{q-1}$, то $(q-1)n + 1 = q^{s_1}$.
3. Пусть $\mathcal{C}_0^k, \mathcal{C}_1^k, \ldots, \mathcal{C}_{(q-1)n}^k$ – разбиение k-го смежного класса на коды с параметрами аффинных кодов Рида – Маллера $RM_q((q-1)s_1 - 2, s_1)$ порядка $(q-1)s_1 - 2$, коды могут быть как линейные, так и нелинейные, $0 \leqslant k \leqslant q-1$.
4. Пусть $\mathcal{R}$ является q-ичным 1-совершенным кодом длины $m = \dfrac{q^{s_2}-1}{q-1}$, где $s_2 \geqslant 2$. Для каждого кодового слова $\boldsymbol{r} \in \mathcal{R}$ определим m-арную квазигруппу $q_{\boldsymbol{r}}$ порядка $(q-1)n + 1$. Квазигруппа определяется на множестве $\{0, 1, \ldots, (q-1)n\}$. Квазигруппу $q_{\boldsymbol{r}}$ можно рассматривать как код длины $m+1$ с минимальным расстоянием 2 над алфавитом из $(q-1)n + 1$ элементов.

Тогда образуем q-ичный код $\mathcal{H}$. Положим

$$\mathcal{H} = \Big\{ (\boldsymbol{u} \,|\, \boldsymbol{v}_1 \,|\, \boldsymbol{v}_2 \,|\, \ldots \,|\, \boldsymbol{v}_m) \mid \boldsymbol{u} \in \mathcal{B}_{j_0},\ \boldsymbol{v}_i \in \mathcal{C}_{j_i}^{r_i} \text{ при } 1 \leqslant i \leqslant m,$$
$$\boldsymbol{r} = (r_1, r_2, \ldots, r_m) \in \mathcal{R},\ j_0 = q_{\boldsymbol{r}}(j_1, j_2, \ldots, j_m),$$
$$j_i \in \{0, 1, \ldots, (q-1)n\} \text{ при } i = 0, 1, \ldots, m \Big\}. \tag{6}$$

Поясним обозначение $\mathcal{C}_j^{r_i}$. Для этого рассмотрим i-ю компоненту r_i кодового слова $\boldsymbol{r} = (r_1, r_2, \ldots, r_m) \in \mathcal{R}$. По определению $r_i \in \mathbb{F}_q$. Пусть α – примитивный элемент конечного поля $\mathbb{F}_q$. Если $r_i \neq 0$, то $r_i = \alpha^k$, где $k \in \{1, \ldots, q-1\}$. Тогда обозначение $\mathcal{C}_j^{r_i}$ следует понимать как $\mathcal{C}_j^k$, при этом $0 \leqslant j \leqslant (q-1)n$. Если $r_i = 0$, то $\mathcal{C}_j^{r_i} = \mathcal{C}_j^0$ и $\mathcal{C}_j^{r_i}$ является элементом разбиения 0-го смежного класса.

Теорема 1. *Построенный выше код $\mathcal{H}$ является q-ичным 1-совершенным кодом длины $(q-1)nm+n+m$.*

Доказательство. Поскольку $\boldsymbol{u} \in \mathcal{B}_{j_0} \subseteq \mathbb{F}_q^n$ и $\boldsymbol{v}_i \in \mathcal{C}_{j_i}^{r_i} \subseteq \mathbb{F}_q^{(q+1)n+1}$, то

$$n + \big((q+1)n+1\big)m = (q+1)nm + n + m,$$

и поскольку $n = \dfrac{q^{s_1}-1}{q-1}$ и $m = \dfrac{q^{s_2}-1}{q-1}$, то

$$(q-1)nm + n + m = \frac{q^{s_1+s_2}-1}{q-1}.$$

Следовательно, код $\mathcal{H}$ имеет корректную длину.

Далее покажем, что код $\mathcal{H}$ содержит корректное число кодовых слов и его минимальное расстояние равно 3.

Поскольку разбиение $\mathcal{C}_0^k, \mathcal{C}_1^k, \ldots, \mathcal{C}_{(q-1)n}^k$ k-го смежного класса, образованного кодом $RM_q((q-1)s_1-1, s_1)$, содержит $(q-1)n+1$ элементов и размерность кода $RM_q((q-1)s_1-1, s_1)$ равна

$$q^{s_1-1} = (q-1)\frac{q^{s_1}-1}{q-1} = (q-1)n,$$

то

$$|\mathcal{C}_{j_i}^{r_i}|((q-1)n+1) = q^{(q-1)n}.$$

По определению $|\mathcal{B}_{j_0}| = q^{n-s_1}$ для каждого $j_0 \in \{0, 1, \ldots, (q-1)n\}$. Следовательно, для каждого $\boldsymbol{r} \in \mathcal{R}$ мы можем построить

$$|\mathcal{B}_{j_0}||\mathcal{C}_{j_i}^{r_i}|^m((q-1)n+1)^m = q^{n-s_1}q^{(q-1)nm} = q^{(q-1)nm+n-s_1}$$

кодовых слов. Поскольку мощность q-ичного 1-совершенного кода $|\mathcal{R}| = q^{m-s_2}$, то

$$|\mathcal{H}| = q^{(q-1)nm+n+m-(s_1+s_2)}.$$

Следовательно, код $\mathcal{H}$ содержит корректное число кодовых слов.

Теперь покажем, что минимальное расстояние кода $\mathcal{H}$ равно 3. Предположим, что векторы $\boldsymbol{x} = (\boldsymbol{x}_0 \,|\, \boldsymbol{x}_1 \,|\, \ldots \,|\, \boldsymbol{x}_m)$ и $\boldsymbol{y} = (\boldsymbol{y}_0 \,|\, \boldsymbol{y}_1 \,|\, \ldots \,|\, \boldsymbol{y}_m)$ принадлежат коду $\mathcal{H}$. Тогда

$$d(\boldsymbol{x}, \boldsymbol{y}) \geqslant \sum_{i=0}^{m} d(\boldsymbol{x}_i, \boldsymbol{y}_i),$$

где векторы $\boldsymbol{x}_0, \boldsymbol{y}_0$ имеют длину n, а при $1 \leqslant i \leqslant m$ векторы $\boldsymbol{x}_i, \boldsymbol{y}_i$ имеют длину $(q-1)n+1$. Пусть $r_i = p(\boldsymbol{x}_i)$ и $r_i' = p(\boldsymbol{y}_i)$, $i = 1, 2, \ldots, m$, где $p(\boldsymbol{x})$ – функция четности. Тогда векторы $\boldsymbol{r} = (r_1, r_2, \ldots, r_m)$ и $\boldsymbol{r}' = (r_1', r_2', \ldots, r_m')$ принадлежат коду $\mathcal{R}$.

Если $d(\boldsymbol{x}_i, \boldsymbol{y}_i) = 0$ для всех значений i, то $\boldsymbol{r} = \boldsymbol{r}'$. Если $r_i \neq r_i'$, то $d(\boldsymbol{x}_i, \boldsymbol{y}_i) \geqslant 1$. Следовательно, если $d(\boldsymbol{r}, \boldsymbol{r}') \geqslant 3$, то $d(\boldsymbol{x}_i, \boldsymbol{y}_i) \geqslant 1$ как минимум для трех значений i. Таким образом,

$$\sum_{i=0}^{m} d(\boldsymbol{x}_i, \boldsymbol{y}_i) \geqslant 3 \quad \text{при } \boldsymbol{r} \neq \boldsymbol{r}'.$$

Если $\boldsymbol{r} = \boldsymbol{r}'$, то $p(\boldsymbol{x}_i) = p(\boldsymbol{y}_i)$ и $d(\boldsymbol{x}_i, \boldsymbol{y}_i) \geqslant 2$ при $\boldsymbol{x}_i \neq \boldsymbol{y}_i$, $i = 1, 2, \ldots, m$, и $d(\boldsymbol{x}_0, \boldsymbol{y}_0) \geqslant 1$ при $\boldsymbol{x}_0 \neq \boldsymbol{y}_0$. Допустим, что $\boldsymbol{x}_0 \in \mathcal{B}_{j_0}$, $\boldsymbol{y}_0 \in \mathcal{B}_{k_0}$, $\boldsymbol{x}_i \in \mathcal{C}_{j_i}^{r_i}$ и $\boldsymbol{y}_i \in \mathcal{C}_{k_i}^{r_i}$,

где $i = 1, 2, \ldots, m$. Тогда равенство $d(\boldsymbol{x}_i, \boldsymbol{y}_i) = 0$ означает, что $j_i = k_i$, $i = 0, 1, \ldots, m$. Поскольку $\boldsymbol{j} = (j_0, j_1, \ldots, j_m)$ и $\boldsymbol{k} = (k_0, k_1, \ldots, k_m)$ могут совпадать только в $m-1$ позициях, то мы получаем, что хотя бы для одного значения $i \in \{0, 1, \ldots, m\}$ справедливо неравенство $d(\boldsymbol{x}_i, \boldsymbol{y}_i) \geqslant 2$, а для некоторого другого значения i справедливо неравенство $d(\boldsymbol{x}_i, \boldsymbol{y}_i) \geqslant 1$. Таким образом, $d(\boldsymbol{x}, \boldsymbol{y}) \geqslant 3$ за исключением случая, когда $\boldsymbol{j} = \boldsymbol{k}$. Однако в этом случае, если $\boldsymbol{x}_i \neq \boldsymbol{y}_i$, то в силу утверждения 1 справедливо неравенство $d(\boldsymbol{x}_i, \boldsymbol{y}_i) \geqslant 3$, и следовательно, $d(\boldsymbol{x}, \boldsymbol{y}) \geqslant 3$. ▲

При $m = 1$ конструкция (6) сводится к комбинаторной конструкции q-ичных 1-совершенных кодов [8].

Теорема 2. *Число неэквивалентных q-ичных 1-совершенных кодов длины $(q^{s_1+s_2}-1)/(q-1)$ превосходит*

$$q^{s_1 q^{s_1}(q^{s_1}-1)(q^{s_2-1}-2)q^{q^{s_2-1}-s_2-1}-(s_1+s_2+2)q^{s_1+s_2}+(s_1+s_2+1)},$$

где величина $(q^{s_1+s_2}-1)/(q-1)$ является достаточно большой.

Доказательство. Обозначим через $Q(m, (q-1)n+1)$ множество всех m-арных квазигрупп порядка $(q-1)n+1$. Множество $Q(m, (q-1)n+1)$ можно также рассматривать как множество $((q-1)n+1)$-ичных кодов с параметрами

$$\big(m+1, ((q-1)n+1)^m, 2\big)_{(q-1)n+1}.$$

В [10] показано, что при достаточно больших n справедливо неравенство

$$|Q(m, (q-1)n+1)| \geqslant ((q-1)n+1)^{\left[((q-1)n+1)^2-((q-1)n+1)\right](m-1)}. \tag{7}$$

Далее рассмотрим вышеописанную конструкцию 1-совершенных кодов. Поскольку для каждого кодового слова $\boldsymbol{r} \in \mathcal{R}$ мы можем выбрать любую m-арную квазигруппу $q_{\boldsymbol{r}} \in Q(m, (q-1)n+1)$, то исходя из одного фиксированного разбиения пространства $\mathbb{F}_q^n$ на коды $\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_{(q-1)n}$ и одного фиксированного разбиения пространства $\mathbb{F}_q^{(q-1)n+1}$ на коды $\mathcal{C}_0^k, \mathcal{C}_1^k, \ldots, \mathcal{C}_{(q-1)n}^k$ мы можем построить

$$|Q(m, (q-1)n+1)|^{|\mathcal{R}|} \tag{8}$$

различных q-ичных 1-совершенных кодов длины $(q^{s_1+s_2}-1)/(q-1)$.

Так как $(q-1)n+1 = q^{s_1}$ и $(q-1)m+1 = q^{s_2}$, то в силу формулы (7) получаем, что

$$|Q(m, (q-1)n+1)|^{|\mathcal{R}|} \geqslant \left(\left(q^{s_1}\right)^{\left[(q^{s_1})^2-q^{s_1}\right]\left(q^{s_2-1}-2\right)}\right)^{|\mathcal{R}|}.$$

Поскольку $\mathcal{R}$ является q-ичным 1-совершенным кодом длины $(q^{s_2}-1)/(q-1)$, то

$$|\mathcal{R}| = q^{\frac{q^{s_2}-1}{q-1}-s_2},$$

и так как

$$q^{q^{s_2-1}-s_2-1} < q^{\frac{q^{s_2}-1}{q-1}-s_2},$$

то

$$|Q(m, (q-1)n+1)|^{|\mathcal{R}|} \geqslant \left(q^{s_1}\right)^{\left[(q^{s_1})^2-q^{s_1}\right]\left(q^{s_2-1}-2\right)q^{q^{s_2-1}-s_2-1}}. \tag{9}$$

Множество различных q-ичных 1-совершенных кодов длины $(q^{s_1+s_2}-1)/(q-1)$ разбивается на классы эквивалентности. Произвольный класс эквивалентности в

этом разбиении содержит не более чем

$$(q-1)^{\frac{q^{s_1+s_2-1}}{q-1}}\left(\frac{q^{s_1+s_2}-1}{q-1}\right)!\,q^{\frac{q^{s_1+s_2-1}}{q-1}}$$

различных q-ичных 1-совершенных кодов длины $(q^{s_1+s_2}-1)/(q-1)$, где

$$(q-1)^{\frac{q^{s_1+s_2-1}}{q-1}}\left(\frac{q^{s_1+s_2}-1}{q-1}\right)!$$

– число мономиальных матриц размера $\dfrac{q^{s_1+s_2}-1}{q-1}\times\dfrac{q^{s_1+s_2}-1}{q-1}$ над полем $\mathbb{F}_q$, а

$$q^{\frac{q^{s_1+s_2-1}}{q-1}}$$

– число векторов в пространстве $\mathbb{F}_q^{\frac{q^{s_1+s_2-1}}{q-1}}$. Если коды из множества различных q-ичных 1-совершенных кодов длины $(q^{s_1+s_2}-1)/(q-1)$ содержат нулевой вектор $\mathbf{0}$, то произвольный класс эквивалентности содержит не более чем

$$(q-1)^{\frac{q^{s_1+s_2-1}}{q-1}}\left(\frac{q^{s_1+s_2}-1}{q-1}\right)!\,q^{\frac{q^{s_1+s_2-1}}{q-1}-(s_1+s_2)}$$

различных q-ичных 1-совершенных кодов длины $(q^{s_1+s_2}-1)/(q-1)$, где

$$q^{\frac{q^{s_1+s_2-1}}{q-1}-(s_1+s_2)}$$

– число слов в q-ичном 1-совершенном коде длины $(q^{s_1+s_2}-1)/(q-1)$.

В [10] показано, что неравенство (7) справедливо и для квазигрупп q, таких что $q(0,0,\ldots,0)=0$. Поскольку мы предполагаем, что нулевой вектор $\mathbf{0}$ всегда принадлежит коду, то коды $\mathcal{B}_0$, $\mathcal{C}_0^0$ и $\mathcal{R}$ содержат вектор $\mathbf{0}$. Следовательно, мы можем предполагать, что q-ичные 1-совершенные коды длины $(q^{s_1+s_2}-1)/(q-1)$, построенные вышеописанным методом, также содержат вектор $\mathbf{0}$.

Справедливость теоремы 2 вытекает из неравенства (9) и следующих неравенств:

$$q^{\frac{q^{s_1+s_2-1}}{q-1}-(s_1+s_2)}\leqslant q^{q^{s_1+s_2}-(s_1+s_2+1)},$$

$$(q-1)^{\frac{q^{s_1+s_2-1}}{q-1}}\left(\frac{q^{s_1+s_2}-1}{q-1}\right)!\,q^{q^{s_1+s_2}-(s_1+s_2+1)}\leqslant$$

$$\leqslant(q-1)^{q^{s_1+s_2}}(q^{s_1+s_2})!\cdot q^{q^{s_1+s_2}-(s_1+s_2+1)},$$

$$(q-1)^{q^{s_1+s_2}}(q^{s_1+s_2})!\,q^{q^{s_1+s_2}-(s_1+s_2+1)}\leqslant q^{q^{s_1+s_2}+(s_1+s_2)q^{s_1+s_2}+q^{s_1+s_2}-(s_1+s_2+1)}.\quad\blacktriangle$$

Следствие 1. *Число неэквивалентных q-ичных 1-совершенных кодов длины $n=(q^s-1)/(q-1)$ превосходит $q^{q^{cn}}$, где константа $c<1$, а s – достаточно большое натуральное число.*

В [10] Фелпс предложил конструкцию расширенных двоичных 1-совершенных кодов, т.е. кодов с параметрами расширенных двоичных кодов Хэмминга (кодов Рида – Маллера). Далее мы представим модификацию конструкции (6), которая позволяет строить коды с параметрами аффинных кодов Рида – Маллера и является прямым обобщением конструкции Фелпса [10] на q-ичный случай.

1. Пусть пространство $\mathbb{F}_q^{(q-1)n+1}$ разбито на смежные классы, образованные аффинным кодом Рида – Маллера $RM_q((q-1)s_1-1,s_1)$ порядка $(q-1)s_1-1$. При этом $n=\dfrac{q^{s_1}-1}{q-1}$, $(q-1)n+1=q^{s_1}$ и $s_1\geqslant 2$.

2. Пусть $\mathcal{C}_0^k, \mathcal{C}_1^k, \ldots, \mathcal{C}_{(q-1)n}^k$ – разбиение k-го смежного класса на квазисовершенные коды с параметрами аффинных кодов Рида – Маллера порядка $(q-1)s_1-2$, коды могут быть как линейные, так и нелинейные, $0 \leqslant k \leqslant q-1$.
3. Пусть $\mathcal{R}$ – четный квазисовершенный код с параметрами аффинного кода Рида – Маллера $RM_q((q-1)s_2-2, s_2)$ порядка $(q-1)s_2-2$, $s_2 \geqslant 2$.
4. Пусть $m = \dfrac{q^{s_2}-1}{q-1}$. Для каждого кодового слова $\boldsymbol{r} \in \mathcal{R}$ определим $(q-1)m$-арную квазигруппу $q_{\boldsymbol{r}}$ порядка $(q-1)n+1$. Квазигруппа определяется на множестве индексов $\{0,1,\ldots,(q-1)n\}$. В этом случае квазигруппу $q_{\boldsymbol{r}}$ можно рассматривать как код длины $(q-1)m+1$ с минимальным расстоянием 2 над алфавитом, состоящим из $(q-1)n+1$ элементов.

Тогда образуем q-ичный код $\mathcal{P}$. Положим

$$\mathcal{P} = \Big\{(\boldsymbol{c}_0 \,|\, \boldsymbol{c}_1 \,|\, \boldsymbol{c}_2 \,|\, \ldots \,|\, \boldsymbol{c}_{(q-1)m}) \mid \boldsymbol{c}_i \in \mathcal{C}_{j_i}^{r_i},$$
$$\boldsymbol{r} = (r_0, r_1, \ldots, r_{(q-1)m}) \in \mathcal{R},\ j_0 = q_{\boldsymbol{r}}(j_1, j_2, \ldots, j_{(q-1)m}),$$
$$j_i \in \{0,1,\ldots,(q-1)n\},\ i = 0,1,\ldots,(q-1)m\Big\}. \tag{10}$$

Теорема 3. *Построенный выше код $\mathcal{P}$ является q-ичным квазисовершенным кодом с параметрами аффинного кода Рида – Маллера порядка $(q-1)(s_1+s_2)-2$.*

Доказательство. При $q=2$ теорема 3 доказана в [10]. Докажем теорему 3 при $q \geqslant 3$.

В силу утверждений 1, 2 аффинный код Рида – Маллера $RM_q((q-1)(s_1+s_2)-2, s_1+s_2)$ порядка $(q-1)(s_1+s_2)-2$ имеет следующие параметры:

1. Длина кода Рида – Маллера $RM_q((q-1)(s_1+s_2)-2, s_1+s_2)$ равна $q^{s_1+s_2}$;
2. Число кодовых слов в коде $RM_q((q-1)(s_1+s_2)-2, s_1+s_2)$ равно $q^{q^{s_1+s_2}-(s_1+s_2)-1}$;
3. Минимальное расстояние $d(RM_q((q-1)(s_1+s_2)-2, s_1+s_2)) = 3$;
4. Радиус покрытия $\rho(RM_q((q-1)(s_1+s_2)-2, s_1+s_2)) = 2$.

Покажем, что код $\mathcal{P}$ имеет такие же параметры.

Поскольку $(q-1)n+1 = q^{s_1}$ и $(q-1)m+1 = q^{s_2}$, то

$$((q-1)n+1)((q-1)m+1) = q^{s_1+s_2}.$$

Следовательно, длина кода $\mathcal{P}$ равна $q^{s_1+s_2}$.

Поскольку размерность аффинного кода Рида – Маллера $RM_q((q-1)s_1-1, s_1)$ порядка $(q-1)s_1-1$ равна $q^{s_1-1} = (q-1)n$ и каждый смежный класс, образованный этим кодом, разбивается на $(q-1)n+1$ подкодов $\mathcal{C}_{j_i}^{r_i}$, то получаем, что

$$|\mathcal{C}_{j_i}^{r_i}|((q-1)n+1) = q^{(q-1)n}.$$

Так как $|\mathcal{C}_{j_i}^{r_i}| = q^{(q-1)n-s_1}$ при $j_i \in \{0,1,\ldots,(q-1)n\}$, $i = 0,1,\ldots,(q-1)m$, то для каждого $\boldsymbol{r} \in \mathcal{R}$ мы можем построить

$$|\mathcal{C}_{j_0}^{r_0}||\mathcal{C}_{j_i}^{r_i}|^{(q-1)m}((q-1)n+1)^{(q-1)m} = q^{(q-1)n(q-1)m+(q-1)n-s_1}$$

кодовых слов.

Поскольку $|\mathcal{R}| = q^{(q-1)m-s_2}$, то

$$|\mathcal{P}| = q^{(q-1)n(q-1)m+(q-1)n+(q-1)m+1-(s_1+s_2)-1} = q^{((q-1)n+1)((q-1)m+1)-(s_1+s_2)-1}.$$

Следовательно,

$$|\mathcal{P}| = q^{q^{s_1+s_2}-(s_1+s_2)-1}.$$

Далее мы покажем, что минимальное расстояние кода $\mathcal{P}$ равно 3. Пусть векторы $\boldsymbol{x} = (\boldsymbol{x}_0 \,|\, \boldsymbol{x}_1 \,|\, \ldots \,|\, \boldsymbol{x}_{(q-1)m})$ и $\boldsymbol{y} = (\boldsymbol{y}_0 \,|\, \boldsymbol{y}_1 \,|\, \ldots \,|\, \boldsymbol{y}_{(q-1)m})$ принадлежат $\mathcal{P}$. Тогда

$$d(\boldsymbol{x}, \boldsymbol{y}) \geqslant \sum_{i=0}^{(q-1)m} d(\boldsymbol{x}_i, \boldsymbol{y}_i),$$

где векторы $\boldsymbol{x}_i, \boldsymbol{y}_i$ имеют длину $(q-1)n+1$ при $0 \leqslant i \leqslant (q-1)m$. Пусть $r_i = p(\boldsymbol{x}_i)$ и $r'_i = p(\boldsymbol{y}_i)$, где $p(\boldsymbol{x})$ – функция четности и $i = 1, 2, \ldots, (q-1)m$. Тогда векторы $\boldsymbol{r} = (r_1, r_2, \ldots, r_{(q-1)m})$ и $\boldsymbol{r}' = (r'_1, r'_2, \ldots, r'_{(q-1)m})$ принадлежат коду $\mathcal{R}$. Если $d(\boldsymbol{x}_i, \boldsymbol{y}_i) = 0$, то $\boldsymbol{r} = \boldsymbol{r}'$. Если $r_i \neq r'_i$, то $d(\boldsymbol{x}_i, \boldsymbol{y}_i) \geqslant 1$. Поэтому если $d(\boldsymbol{r}, \boldsymbol{r}') \geqslant 3$, то $d(\boldsymbol{x}_i, \boldsymbol{y}_i) \geqslant 1$ для трех значений i.

Таким образом,

$$\sum_{i=0}^{(q-1)m} d(\boldsymbol{x}_i, \boldsymbol{y}_i) \geqslant 3 \quad \text{при } \boldsymbol{r} \neq \boldsymbol{r}'.$$

Если $\boldsymbol{r} = \boldsymbol{r}'$, то $p(\boldsymbol{x}_i) = p(\boldsymbol{y}_i)$ и $d(\boldsymbol{x}_i, \boldsymbol{y}_i) \geqslant 2$ при $\boldsymbol{x}_i \neq \boldsymbol{y}_i$. Допустим,что $\boldsymbol{x}_0 \in \mathcal{C}_{j_0}$, $\boldsymbol{y}_0 \in \mathcal{C}_{k_0}$, $\boldsymbol{x}_i \in \mathcal{C}^{r_i}_{j_i}$ и $\boldsymbol{x}_i \in \mathcal{C}^{r_i}_{k_i}$, где $i = 1, 2, \ldots, (q-1)m$. Тогда равенство $d(\boldsymbol{x}_i, \boldsymbol{y}_i) = 0$ означает, что $j_i = k_i$ для всех $i = 0, 1, \ldots, (q-1)m$. Поскольку $\boldsymbol{j} = (j_0, j_1, \ldots, j_{(q-1)m})$ и $\boldsymbol{k} = (k_0, k_1, \ldots, k_{(q-1)m})$ могут совпадать только в $(q-1)m-1$ позициях, то $d(\boldsymbol{x}_i, \boldsymbol{y}_i) \geqslant 2$ по крайней мере для двух значений i. Следовательно, $d(\boldsymbol{x}, \boldsymbol{y}) \geqslant 3$ за исключением случая, когда $\boldsymbol{j} = \boldsymbol{k}$. Однако в этом случае, если $\boldsymbol{x}_i \neq \boldsymbol{y}_i$, то в силу утверждения 1 имеем $d(\boldsymbol{x}_i, \boldsymbol{y}_i) \geqslant 3$, и следовательно, $d(\boldsymbol{x}, \boldsymbol{y}) \geqslant 3$.

Остается показать, что радиус покрытия кода $\mathcal{P}$ равен 2. В векторном пространстве размерности $q^{s_1+s_2} = ((q-1)n+1)((q-1)m+1)$ над полем $\mathbb{F}_q$ рассмотрим произвольный вектор $\boldsymbol{x} = (\boldsymbol{x}_0 \,|\, \boldsymbol{x}_1 \,|\, \ldots \,|\, \boldsymbol{x}_{(q-1)m})$. Код $\mathcal{R}$ – квазисовершенный код с параметрами аффинного кода Рида – Маллера порядка $(q-1)s_2-2$. Следовательно, радиус покрытия кода $\mathcal{R}$ равен 2 и существует кодовое слово $(\boldsymbol{c}_0 \,|\, \boldsymbol{c}_1 \,|\, \boldsymbol{c}_2 \,|\, \ldots \,|\, \boldsymbol{c}_{(q-1)m}) \in \mathcal{P}$, такое что

$$d\Big((p(\boldsymbol{x}_0) \,|\, p(\boldsymbol{x}_1) \,|\, \ldots \,|\, p(\boldsymbol{x}_{(q-1)m})), \big(p(\boldsymbol{c}_0) \,|\, p(\boldsymbol{c}_1) \,|\, p(\boldsymbol{c}_2) \,|\, \ldots \,|\, p(\boldsymbol{c}_{(q-1)m})\big)\Big) \leqslant 2.$$

Без ограничения общности мы можем полагать, что кодовое слово $(\boldsymbol{c}_0 \,|\, \boldsymbol{c}_1 \,|\, \boldsymbol{c}_2 \,|\, \ldots \,|\, \boldsymbol{c}_{(q-1)m})$ является нулевым, а вектор $\boldsymbol{x}$ таков, что $\boldsymbol{x}_2 = \boldsymbol{0}, \ldots, \boldsymbol{x}_{(q-1)m} = \boldsymbol{0}$. Тогда вектор $\boldsymbol{x} = \big(\boldsymbol{x}_0 \,|\, \boldsymbol{x}_1 \,|\, \ldots \,|\, \boldsymbol{x}_{(q-1)m}\big)$ принадлежит линейному подпространству

$$\Big\{\big(\boldsymbol{y}_0 \,|\, \boldsymbol{y}_1 \,|\, \boldsymbol{c}_2 \,|\, \ldots \,|\, \boldsymbol{c}_{(q-1)m}\big) \mid \boldsymbol{y}_0, \boldsymbol{y}_1 \in \mathbb{F}_q^{(q-1)n+1},\ \boldsymbol{c}_i = \boldsymbol{0},\ i = 2, 3, \ldots, (q-1)m\Big\}. \quad (11)$$

Если $\boldsymbol{y}_1 = \boldsymbol{0}$, то по построению кода $\mathcal{P}$ подпространство

$$\Big\{\big(\boldsymbol{y}_0 \,|\, \boldsymbol{0} \,|\, \boldsymbol{c}_2 \,|\, \ldots \,|\, \boldsymbol{c}_{(q-1)m}\big) \mid \boldsymbol{y}_0 \in \mathbb{F}_q^{(q-1)n+1},\ \boldsymbol{c}_i = \boldsymbol{0},\ i = 2, 3, \ldots, (q-1)m\Big\}$$

содержит код с параметрами кода $RM_q((q-1)s_1-2, s_1)$, радиус покрытия которого равен 2 (утверждение 2). Если $p(\boldsymbol{y}_1) = \boldsymbol{0}$ и вектор $\boldsymbol{y}_1$ является фиксированным,

тогда аналогичное утверждение справедливо и для всех линейных многообразий

$$\Big\{\big(\boldsymbol{y}_0 \,|\, \boldsymbol{y}_1 \,|\, \boldsymbol{c}_2 \,|\, \ldots \,|\, \boldsymbol{c}_{(q-1)m}\big) \mid \boldsymbol{y}_0, \boldsymbol{y}_1 \in \mathbb{F}_q^{(q-1)n+1},\ p(\boldsymbol{y}_1) = \boldsymbol{0},\ \boldsymbol{c}_i = \boldsymbol{0},\ i = 2, 3, \ldots, (q-1)m\Big\}.$$

Поскольку радиус покрытия аффинного кода Рида – Маллера $RM_q((q-1)s_1 - 1, s_1)$ порядка $(q-1)s_1 - 1$ равен 1, то по построению кода $\mathcal{P}$ для любого вектора из множества

$$\Big\{\big(\boldsymbol{y}_0 \,|\, \boldsymbol{y}_1 \,|\, \boldsymbol{c}_2 \,|\, \ldots \,|\, \boldsymbol{c}_{(q-1)m}\big) \mid \boldsymbol{y}_0, \boldsymbol{y}_1 \in \mathbb{F}_q^{(q-1)n+1},\ p(\boldsymbol{y}_1) \neq \boldsymbol{0},\ \boldsymbol{c}_i = \boldsymbol{0},\ i = 2, 3, \ldots, (q-1)m\Big\}$$

в подпространстве (11) существует кодовое слово из $\mathcal{P}$ на расстоянии не более 2. ▲

Утверждение 4. *Построенный выше код $\mathcal{P}$ является четным.*

Доказательство. Поскольку

$$p(\boldsymbol{x}) = p(p(\boldsymbol{x}_0), p(\boldsymbol{x}_1), \ldots, p(\boldsymbol{x}_{(q-1)m})) = p(r_0, r_1, \ldots, r_{(q-1)m}) = p(\boldsymbol{r})$$

и $p(\boldsymbol{r}) = 0$ для всех $\boldsymbol{r} \in \mathcal{R}$, то $p(\boldsymbol{x}) = 0$ для всех $\boldsymbol{x} \in \mathcal{P}$. ▲

Теорема 4. *Число неэквивалентных q-ичных четных квазисовершенных кодов с параметрами аффинного кода Рида – Маллера порядка $(q-1)(s_1+s_2)-2$ и длины $q^{s_1+s_2}$ превосходит*

$$q^{s_1 q^{s_1}(q^{s_1}-1)(q^{s_2}-2)q^{q^{s_2}-s_2-1}-(s_1+s_2+2)q^{s_1+s_2}+(s_1+s_2+1)},$$

где число $q^{s_1+s_2}$ является достаточно большим.

Доказательство. Рассмотрим множество $Q((q-1)m, (q-1)n+1)$ всех $(q-1)m$-арных квазигрупп порядка $(q-1)n+1$. Множество $Q((q-1)m, (q-1)n+1)$ можно также рассматривать как множество $((q-1)n+1)$-ичных кодов с параметрами

$$\Big((q-1)m+1, ((q-1)n+1)^{(q-1)m}, 2\Big)_{(q-1)n+1}.$$

В [10] показано, что при достаточно больших n справедливо неравенство

$$|Q((q-1)m, (q-1)n+1)| \geqslant ((q-1)n+1)^{\left[((q-1)n+1)^2-((q-1)n+1)\right]((q-1)m-1)}. \qquad (12)$$

Далее рассмотрим вышеописанную конструкцию квазисовершенных кодов. Поскольку для каждого кодового слова $\boldsymbol{r} \in \mathcal{R}$ мы можем выбрать любую квазигруппу $q_{\boldsymbol{r}} \in Q((q-1)m, (q-1)n+1)$, то исходя из одного фиксированного разбиения пространства $\mathbb{F}_q^{(q-1)n+1}$ на коды $\mathcal{C}_0^k, \mathcal{C}_1^k, \ldots, \mathcal{C}_{(q-1)n}^k$ мы можем построить более чем

$$|Q((q-1)m, (q-1)n+1)|^{|\mathcal{R}|}$$

различных q-ичных четных квазисовершенных кодов с параметрами аффинного кода Рида – Маллера порядка $(q-1)(s_1+s_2)-2$ и длины $q^{s_1+s_2}$.

Так как $(q-1)n+1 = q^{s_1}$ и $(q-1)m+1 = q^{s_2}$, то в силу формулы (12) получаем, что

$$|Q((q-1)m, (q-1)n+1)|^{|\mathcal{R}|} \geqslant \left(\left(q^{s_1}\right)^{\left[(q^{s_1})^2-q^{s_1}\right](q^{s_2}-2)}\right)^{|\mathcal{R}|}.$$

Из утверждения (1) следует, что $|\mathcal{R}| = q^{q^{s_2}-s_2-1}$. Следовательно,

$$|Q((q-1)m,(q-1)n+1)|^{|\mathcal{R}|} \geqslant \left(q^{s_1}\right)^{\left[(q^{s_1})^2-q^{s_1}\right](q^{s_2}-2)q^{q^{s_2}-s_2-1}}. \tag{13}$$

Множество различных q-ичных четных квазисовершенных кодов с параметрами аффинного кода Рида – Маллера порядка $(q-1)(s_1+s_2)-2$ и длины $q^{s_1+s_2}$ разбивается на классы эквивалентности. Справедливость теоремы 4 следует из формулы (13) и того факта, что произвольный класс эквивалентности в этом разбиении содержит не более чем

$$\left((q-1)^{q^{s_1+s_2}}(q^{s_1+s_2})!\right)\left(q^{q^{s_1+s_2}-(s_1+s_2+1)}\right) \leqslant q^{q^{s_1+s_2}+(s_1+s_2)q^{s_1+s_2}+q^{s_1+s_2}-(s_1+s_2+1)}$$

различных q-ичных четных квазисовершенных кодов с параметрами аффинного кода Рида – Маллера порядка $(q-1)(s_1+s_2)-2$ и длины $q^{s_1+s_2}$. ▲

Следствие 2. *Число неэквивалентных q-ичных четных квазисовершенных кодов с параметрами аффинного кода Рида – Маллера порядка $(q-1)s-2$ и длины $n=q^s$ превосходит $q^{q^{cn}}$, где константа $c<1$, а s – достаточно большое натуральное число.*

При $q=2,3$ существует единственный q-ичный код с параметрами аффинного кода Рида – Маллера $RM_q((q-1)s_1-1,s_1)$ [18, с. 224]. (Аффинный код Рида – Маллера $RM_q((q-1)s_1-1,s_1)$ является линейным q-ичным МДР-кодом с параметрами $[q^{s_1},q^{s_1}-1,2]_q$.)

Некоторая модификация конструкции (10) позволяет строить коды с параметрами аффинных кодов Рида – Маллера $RM_q((q-1)s_1-1,s_1)$.

Допустим, что код $\mathcal{R}$ является элементом разбиения кода $RM_q((q-1)s_2-1,s_2)$ на подкоды, имеющие параметры кода $RM_q((q-1)s_2-2,s_2)$. Такое разбиение содержит q^{s_2} элементов, поскольку код $RM_q((q-1)s_2-1,s_2)$ имеет параметры $[q^{s_2},q^{s_2}-1,2]_q$, а код $RM_q((q-1)s_2-1,s_2)$ в силу утверждения 1 имеет параметры $[q^{s_2},q^{s_2}-s_2-1,3]_q$. Разбиение кода $RM_q((q-1)s_1-1,s_1)$ на подкоды с параметрами кода $RM_q((q-1)s_1-2,s_1)$ содержит q^{s_1} элементов. Следовательно, каждый элемент разбиения кода $RM_q((q-1)s_2-1,s_2)$ на подкоды, имеющие параметры кода $RM_q((q-1)s_2-2,s_2)$, позволяет построить q^{s_1} попарно непересекающихся кодов с параметрами аффинного кода Рида – Маллера порядка $(q-1)(s_1+s_2)-2$. Следовательно, мы можем построить $q^{s_1+s_2}$ попарно непересекающихся кодов с параметрами аффинного кода Рида – Маллера порядка $(q-1)(s_1+s_2)-2$.

Таким образом, если код $\mathcal{R}$ является элементом разбиения аффинного кода Рида – Маллера $RM_q((q-1)s_2-1,s_2)$ на подкоды, имеющие параметры аффинного кода Рида – Маллера $RM_q((q-1)s_2-2,s_2)$, то и код $\mathcal{P}$ является элементом разбиения кода с параметрами аффинного кода Рида – Маллера $RM_q((q-1)(s_1+s_2)-1,s_1+s_2)$ на подкоды с параметрами аффинного кода Рида – Маллера порядка $(q-1)(s_1+s_2)-2$.

Автор искренне признателен рецензенту за полезные замечания и предложения, которые позволили существенно улучшить первоначальный вариант статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. *Kasami T., Lin S., Peterson W.* New Generalizations of the Reed–Muller Codes. I: Primitive Codes // IEEE Trans. Inform. Theory. 1968. V. 14. № 2. P. 189–199. https://doi.org/10.1109/TIT.1968.1054127
3. *Lachaud G.* The Parameters of Projective Reed–Müller Codes // Discrete Math. 1990. V. 81. № 2. P. 217–221. https://doi.org/10.1016/0012-365X(90)90155-B

4. *Sørensen A.B.* Projective Reed–Muller Codes // IEEE Trans. Inform. Theory. 1991. V. 37. № 6. P. 1567–1576. https://doi.org/10.1109/18.104317
5. *Berger T., Charpin P.* The Automorphism Group of Generalized Reed–Muller Codes // Discrete Math. 1993. V. 117. № 1–3. P. 1–17. https://doi.org/10.1016/0012-365X(93)90321-J
6. *Berger T.P.* Automorphism Groups of Homogeneous and Projective Reed–Muller Codes // IEEE Trans. Inform. Theory. 2002. V. 48. № 5. P. 1035–1045. https://doi.org/10.1109/18.995540
7. *Huffman W.C., Pless V.* Fundamentals of Error-Correcting Codes. Cambridge: Cambridge Univ. Press, 2003.
8. *Romanov A.M.* On Non-Full-Rank Perfect Codes over Finite Fields // Des. Codes Cryptogr. 2019. V. 87. № 5. P. 995–1003. https://doi.org/10.1007/s10623-018-0506-1
9. *Phelps K.T.* A Combinatorial Construction of Perfect Codes // SIAM J. Algebr. Discrete Methods. 1983. V. 4. № 3. P. 398–403. https://doi.org/10.1137/0604040
10. *Phelps K.T.* A General Product Construction for Error Correcting Codes // SIAM J. Algebr. Discrete Methods. 1984. V. 5. № 2. P. 224–228. https://doi.org/10.1137/0605023
11. *Зиновьев В.А.* Обобщенные каскадные коды // Пробл. передачи информ. 1976. Т. 12. № 1. С. 5–15. http://mi.mathnet.ru/ppi1670
12. *Боржес Ж., Рифа Ж., Зиновьев В.А.* О полностью регулярных кодах // Пробл. передачи информ. 2019. Т. 55. № 1. С. 3–50. https://doi.org/10.1134/S0134347519010017
13. *Assmus E.F., Key J.D.* Polynomial Codes and Finite Geometries // Handbook of Coding Theory. V. II. Amsterdam: Elsevier, 1998. P. 1269–1344.
14. *Delsarte P., Goethals J.-M., MacWilliams F.J.* On Generalized Reed–Muller Codes and Their Relatives // Inform. Control. 1970. V. 16. № 5. P. 403–442. https://doi.org/10.1016/S0019-9958(70)90214-7
15. *Delsarte P.* An Algebraic Approach to the Association Schemes of Coding Theory // Philips Res. Rep. Suppl. 1973. № 10.
16. *van Tilborg H.C.A.* Uniformly Packed Codes. PhD Thesis. Technische Hogeschool Eindhoven, Nederland, 1976.
17. *Goethals J.-M., van Tilborg H.C.A.* Uniformly Packed Codes // Philips Res. Rep. 1975. V. 30. P. 9–36.
18. *Laywine C.F., Mullen G.L.* Discrete Mathematics Using Latin Squares. New York: Wiley, 1998.

Романов Александр Михайлович
Институт математики им. С.Л. Соболева СО РАН,
Новосибирск
rom@math.nsc.ru

Поступила в редакцию
30.06.2020
После доработки
12.04.2021
Принята к публикации
04.06.2021