ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 60 **2024** **Вып. 3**

УДК 621.391 : 519.725

© 2024 г. **А.М. Романов**

О РАНГЕ НЕЛИНЕЙНЫХ КВАЗИСОВЕРШЕННЫХ КОДОВ НАД КОНЕЧНЫМИ ПОЛЯМИ[1]

Рассматриваются нелинейные квазисовершенные коды с радиусом упаковки 1 над конечным полем из q элементов, где q – степень простого числа. Эти коды мы называем нелинейными 1-квазисовершенными q-ичными кодами. Изучаются ранг и размерность ядра нелинейных 1-квазисовершенных q-ичных кодов. Если ранг кода равен его длине, то код называется кодом полного ранга. Пусть m – положительное целое число. Доказывается, что при $n = q^m$ и при достаточно больших m и q существуют нелинейные 1-квазисовершенные q-ичные коды полного ранга длины n. Также для некоторых нелинейных 1-квазисовершенных q-ичных кодов вычисляются размерности ядра.

Ключевые слова: квазисовершенные коды, нелинейные коды, обобщенные коды Рида – Маллера, переключающая конструкция, ранг кода, ядро кода, геометрия Галуа.

DOI: 10.31857/S055529232403001X, **EDN:** OKKCTV

§ 1. Введение

Пусть $\mathbb{F}_q^n$ – векторное пространство размерности n над конечным полем $\mathbb{F}_q$ порядка q, где q – степень простого числа p. Произвольное непустое 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. Векторы, принадлежащие пространству $\mathbb{F}_q^n$, мы 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*. Код называется *линейным*, если он образует линейное подпространство над $\mathbb{F}_q$. В противном случае код называется *нелинейным*.

Для любой пары слов $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ и $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ из $\mathbb{F}_q^n$ определим *расстояние Хэмминга* $d(\boldsymbol{x}, \boldsymbol{y})$. Положим

$$d(\boldsymbol{x}, \boldsymbol{y}) := |\{i \mid x_i \neq y_i\}|.$$

Сферой Хэмминга радиуса r с центром в слове $\boldsymbol{x}$ называется множество

$$B_r(\boldsymbol{x}) := \{\boldsymbol{y} \in \mathbb{F}_q^n \mid d(\boldsymbol{x}, \boldsymbol{y}) \leqslant r\}.$$

Радиус упаковки $e(\mathcal{C})$ кода $\mathcal{C}$ длины n – это максимальное число $e \in \{0, 1, \ldots, n\}$ такое, что

$$B_e(\boldsymbol{u}) \cap B_e(\boldsymbol{v}) = \varnothing \quad \text{для всех} \quad \boldsymbol{u}, \boldsymbol{v} \in \mathcal{C}, \quad \boldsymbol{u} \neq \boldsymbol{v}.$$

[1] Работа выполнена в рамках государственного задания ИМ СО РАН, тема FWNF-2022-0017.

Радиус покрытия $\rho(\mathcal{C})$ кода $\mathcal{C}$ длины n – это минимальное число $\rho \in \{0, 1, \ldots, n\}$ такое, что

$$\bigcup_{\boldsymbol{c}\in\mathcal{C}} B_\rho(\boldsymbol{c}) = \mathbb{F}_q^n.$$

Код $\mathcal{C}$ называется *совершенным*, если $\rho(\mathcal{C}) = e(\mathcal{C})$, и код $\mathcal{C}$ называется *квазисовершенным*, если $\rho(\mathcal{C}) = e(\mathcal{C}) + 1$. Если радиус упаковки совершенного (квазисовершенного) кода равен e, то код называется e-совершенным (e-квазисовершенным).

В [1] установлена тесная связь 1-совершенных кодов и 1-квазисовершенных кодов с параметрами обобщенных кодов Рида – Маллера порядка

$$r = (q-1)m - 2.$$

В [1] показано, что с помощью конкатенации из 1-квазисовершенных кодов с параметрами обобщенных кодов Рида – Маллера порядка $r = (q-1)m - 2$ можно построить дважды экспоненциальное число попарно неэквивалентных 1-совершенных кодов над $\mathbb{F}_q$. В [2] показано, что с помощью переключающей конструкции из обобщенных кодов Рида – Маллера порядка $r = (q-1)m-2$ можно построить дважды экспоненциальное число попарно неэквивалентных 1-квазисовершенных кодов над $\mathbb{F}_q$. В [3] установлена тесная связь 1-совершенных кодов над смешанным алфавитом и кодов с параметрами обобщенных кодов Рида – Маллера порядка $r = (q-1)m - 2$. В [3] показано, что из кодов с параметрами обобщенных кодов Рида – Маллера порядка $r = (q-1)m - 2$ можно построить дважды экспоненциальное число попарно неэквивалентных 1-совершенных кодов над смешанным алфавитом.

Обзоры работ по квазисовершенным кодам можно найти в [4–6].

Рангом кода $\mathcal{C} \subseteq \mathbb{F}_q^n$ называется размерность подпространства, натянутого на $\mathcal{C}$. Ранг кода $\mathcal{C}$ мы будем обозначать через $\operatorname{rank}(\mathcal{C})$. Если код $\mathcal{C}$ является линейным кодом размерности k, то $\operatorname{rank}(\mathcal{C}) = k$. Если код $\mathcal{C}$ является нелинейным кодом длины n и содержит q^k слов, то $k+1 \leqslant \operatorname{rank}(\mathcal{C}) \leqslant n$. Код $\mathcal{C}$ длины n называется кодом *полного ранга*, если $\operatorname{rank}(\mathcal{C}) = n$.

Ядром кода $\mathcal{C} \subseteq \mathbb{F}_q^n$ называется множество

$$\ker(\mathcal{C}) := \left\{\boldsymbol{x} \in \mathbb{F}_q^n \mid \lambda \cdot \boldsymbol{x} + \mathcal{C} = \mathcal{C} \text{ для любого } \lambda \in \mathbb{F}_q\right\}.$$

Легко заметить, что если нулевое слово принадлежит $\mathcal{C}$, то $\ker(\mathcal{C})$ является линейным подкодом кода $\mathcal{C}$, и $\mathcal{C}$ является объединением смежных классов, образованных подпространством $\ker(\mathcal{C})$. Размерность ядра кода $\mathcal{C}$ будем обозначать через $\dim(\ker(\mathcal{C}))$. Если код $\mathcal{C}$ является линейным кодом размерности k, то $\dim(\ker(\mathcal{C})) = k$. Если код $\mathcal{C}$ является нелинейным кодом, который содержит q^k слов и содержит нулевое слово, то

$$0 \leqslant \dim(\ker(\mathcal{C})) \leqslant k-2 \quad \text{при} \quad q = 2,$$
$$0 \leqslant \dim(\ker(\mathcal{C})) \leqslant k-1 \quad \text{при} \quad q \geqslant 3$$

(см. [7]).

Пусть $\mathcal{C}$ и $\mathcal{D}$ – коды длины n над полем $\mathbb{F}_q$. Тогда коды $\mathcal{C}$ и $\mathcal{D}$ называются *эквивалентными*, если существуют n перестановок $\pi_1, \ldots, \pi_n$ из q элементов и перестановка σ, переставляющая n координатных позиций, такие что $(u_1, \ldots, u_n) \in \mathcal{C}$ тогда и только тогда, когда $\sigma(\pi_1(u_1), \ldots, \pi_n(u_n)) \in \mathcal{D}$.

При приведенном выше определении эквивалентности кодов и при $q \geqslant 5$ существуют нелинейные q-ичные коды, содержащие нулевое слово и эквивалентные линейному q-ичному коду [8, 9]. Ниже мы приведем другое определение эквивалентности q-ичных кодов, при котором ранг и размерность ядра кода будут являться его

алгебраическими инвариантами, т.е. эквивалентные коды, содержащие нулевое слово, будут иметь одинаковый ранг и будут содержать ядра одинаковой размерности. Заметим, что помимо алгебраических инвариантов изучаются также комбинаторные инварианты 1-совершенных кодов [9, 10].

Мономиальная матрица – это матрица, имеющая ровно один ненулевой элемент в каждой строке и каждом столбце.

Пусть $\mathcal{C}$ и $\mathcal{D}$ – коды длины n над полем $\mathbb{F}_q$. Тогда $\mathcal{C}$ и $\mathcal{D}$ называются *эквивалентными*, если существуют вектор $\boldsymbol{v} \in \mathbb{F}_q^n$ и мономиальная матрица M размера $n \times n$ над $\mathbb{F}_q$ такие, что

$$\mathcal{D} = \{\boldsymbol{v} + \boldsymbol{c}M \mid \boldsymbol{c} \in \mathcal{C}\}.$$

Вопрос о ранге и размерности ядра является естественным для нелинейных кодов и связан с классификацией кодов. Ранг и размерность ядра изучались, например, для совершенных кодов, кодов Адамара, $\mathbb{Z}_p\mathbb{Z}_{p^2}$-линейных кодов [7,11–14]. В [15] изучались ранг и размерность ядра некоторых подклассов 1-квазисовершенных двоичных кодов.

В данной статье доказано, что при любом $t \in \{1, 2, \ldots, m+1\}$ существуют нелинейные 1-квазисовершенные q-ичные коды длины n и ранга $n-m-1+t$, где $n = q^m$. При этом $m \geqslant 5$ при $q = 3, 4$, $m \geqslant 4$ при $5 \leqslant q \leqslant 19$ и $m \geqslant 3$ при $q \geqslant 23$. В том числе доказано, что при $n = q^m$ существуют нелинейные 1-квазисовершенные q-ичные коды полного ранга длины n. Обобщенные коды Рида – Маллера $RM_q(r, m)$ порядка

$$r = (q-1)m - 2$$

достигают границы Джонсона и являются оптимальными кодами [1]. Ранг обобщенного кода Рида – Маллера $RM_q(r, m)$ порядка $r = (q-1)m-2$ равен $n-m-1$ (см. [1]). Таким образом, в данной статье доказано существование нелинейных 1-квазисовершенных q-ичных кодов всех возможных рангов при длине $n = q^m$, мощности q^{n-m-1} и минимальном расстоянии 3.

В данной статье также при $q \geqslant 3$, $m \geqslant 2$, $n = q^m$ предложена конструкция нелинейных 1-квазисовершенных q-ичных кодов длины n и ранга $n - m$.

Кроме того, в данной статье для некоторых нелинейных 1-квазисовершенных q-ичных кодов вычисляется размерность ядра.

При $q \geqslant 3$, $m \geqslant 2$, $n = q^m$ предложена конструкция нелинейных 1-квазисовершенных q-ичных кодов длины n с ядром размерности $n - [m]_q - 1$, где $[m]_q$ является q-аналогом натурального числа m. По определению

$$[m]_q := 1 + q + \cdots + q^{m-1}.$$

В данной статье рассматривается переключающая (свитчинговая) конструкция, и с помощью этой конструкции обобщенные коды Рида – Маллера $RM_q(r, m)$ порядка $r = (q-1)m - 2$ преобразуются в нелинейные 1-квазисовершенные q-ичные коды различных рангов, а также с помощью этой конструкции обобщенные коды Рида – Маллера $RM_q(r, m)$ порядка $r = (q-1)m - 2$ преобразуются в нелинейные 1-квазисовершенные q-ичные коды с ядром разных размерностей.

В работах [7,11,12,16] переключающие конструкции применялись для построения нелинейных 1-совершенных кодов. В [2] переключающая конструкция впервые получила распространение на 1-квазисовершенные коды и при ее помощи из обобщенных кодов Рида – Маллера порядка $r = (q-1)m - 2$ было построено дважды экспоненциальное число попарно неэквивалентных нелинейных 1-квазисовершенных кодов над $\mathbb{F}_q$.

Заметим, что в двоичном случае обобщенный код Рида – Маллера $RM_q(r, m)$ порядка $r = (q-1)m - 2$ является расширенным кодом Хэмминга. Таким образом,

существование нелинейных 1-квазисовершенных двоичных кодов различных рангов и существование нелинейных 1-квазисовершенных двоичных кодов с ядром разных размерностей следует из работ [7, 11].

В данной статье раскрываются новые аспекты тесной связи 1-совершенных кодов над $\mathbb{F}_q$ и 1-квазисовершенных кодов с параметрами обобщенных кодов Рида – Маллера порядка $r = (q-1)m - 2$. Данная статья является сокращенным вариантом работы [17], в которой можно найти подробные доказательства приводимых далее утверждений.

В §2 приведены некоторые обозначения и основные определения, а также дан краткий обзор известных результатов. В §3 дано описание переключающей конструкции. В §4 показывается существование и приведена конструкция нелинейных 1-квазисовершенных q-ичных кодов различных рангов, а также приведена конструкция нелинейных 1-квазисовершенных q-ичных кодов с ядрами различных размерностей.

§ 2. Предварительные сведения

В этом параграфе мы приводим некоторые обозначения и основные определения, а также даем краткий обзор известных результатов, которые понадобятся нам в дальнейшем.

Через $\dim(L)$ обозначается размерность подпространства $L \subseteq \mathbb{F}_q^n$.

Минимальное расстояние между любыми двумя различными кодовыми словами кода $\mathcal{C}$ называется его *минимальным расстоянием*. Мы будем использовать обозначение $(n, M, d)_q$ для q-ичного кода длины n и мощности M с минимальным расстоянием d. Для линейного q-ичного кода длины n, размерности k с минимальным расстоянием d мы будем использовать обозначение $[n, k, d]_q$. В случае двоичных кодов индекс q может опускается.

Вес слова $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ равен числу ненулевых компонент в $\boldsymbol{x}$ и обозначается через $\mathrm{wt}(\boldsymbol{x})$.

Пусть $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$, и пусть

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

Тогда слово $\boldsymbol{x}$ называется *четным*, если $p(\boldsymbol{x}) = 0$. Код $\mathcal{C} \subseteq \mathbb{F}_q^n$ называется *четным*, если он содержит только четные кодовые слова.

Для произвольного кода $\mathcal{C} \subseteq \mathbb{F}_q^n$ с параметрами $(n, M, d)_q$ определим *расширенный* код $\widehat{\mathcal{C}}$. Положим

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

Расширенный код $\widehat{\mathcal{C}}$ имеет параметры $(n+1, M, \widehat{d})_q$, где $\widehat{d} = d$ или $d+1$.

Через $AG(m, q)$ обозначается аффинное пространство размерности m над $\mathbb{F}_q$. Векторы векторного пространства $\mathbb{F}_q^m$ являются *точками* аффинного пространства $AG(m, q)$. Смежные классы k-мерных линейных подпространств векторного пространства $\mathbb{F}_q^m$ являются k-мерными *аффинными подпространствами* аффинного пространства $AG(m, q)$. *Прямые* – это 1-мерные аффинные подпространства. Например, аффинная плоскость $AG(2, 3)$ содержит 9 точек и 12 прямых. Более подробные сведения по конечной аффинной геометрии можно найти, например, в [18].

Классические коды Рида – Маллера являются двоичными кодами [19, гл. 13]. Обобщение кодов Рида – Маллера на q-ичный случай было предложено в [20].

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

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

Обобщенные коды Рида – Маллера $RM_q(r, m)$ имеют следующие параметры (см. [20; 21, теорема 5.5]):

- длина кода $RM_q(r, m)$ равна q^m;
- размерность кода $RM_q(r, m)$ равна

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

- минимальное расстояние кода $RM_q(r, m)$ равно

$$(q-b)q^{m-a-1}, \tag{2}$$

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

При $q = 2$ и $0 \leqslant r \leqslant m$ обобщенный код Рида – Маллера порядка r является классическим двоичным кодом Рида – Маллера порядка r (см. [21, пример 5.4]).

При $r \leqslant (q-1)m-1$ обобщенный код Рида – Маллера $RM_q(r, m)$ является четным кодом.

Обобщенный код Рида – Маллера $RM_q(r, m)$ порядка $r = (q-1)m - 2$ при $q \geqslant 3$ имеет параметры $[n = q^m, n-m-1, 3]_q$ (см. [1]). В двоичном случае обобщенный код Рида – Маллера $RM_q(r, m)$ порядка $r = (q-1)m - 2$ является расширенным кодом Хэмминга и имеет параметры $[n = 2^m, n-m-1, 4]$. Порядок кода, двойственного обобщенному коду Рида – Маллера $RM_q(r, m)$ порядка $r = (q-1)m - 2$, равен 1 [22]. Обобщенные коды Рида – Маллера $RM_q(r, m)$ порядка $r = (q-1)m - 2$ являются линейными 1-квазисовершенными кодами [1].

§ 3. Переключающая конструкция

В этом параграфе мы опишем переключающую конструкцию, применение которой к обобщенным кодам Рида – Маллера $RM_q((q-1)m-2, m)$ позволит нам доказать существование и в некоторых случаях построить нелинейные 1-квазисовершенные q-ичные коды различных рангов, а также позволит доказать существование и в некоторых случаях построить нелинейные 1-квазисовершенные q-ичные коды с ядрами различных размерностей. Описываемая в этом параграфе переключающая конструкция основана на некоторых идеях из работ [2, 7, 11, 12, 16, 23].

Проверочная матрица H кода $RM_q((q-1)m-2, m)$ представляет собой матрицу размером $(m+1) \times q^m$, содержащую единичный вектор длины $n = q^m$, т.е. вектор, все компоненты которого равны единице, и содержащую все транспонированные векторы из $\mathbb{F}_q^m$ высоты m (см. [22]). Пусть

$$H = \big[\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_n\big],$$

где $\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_n$ – столбцы матрицы H. Пусть точки $P_1, P_2, \ldots, P_n$ аффинного пространства $AG(m, q)$ соответствуют столбцам $\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_n$ проверочной матрицы H, а также координатам $i_1, i_2, \ldots, i_n$ векторного пространства $\mathbb{F}_q^n$, и пусть эти соответствия являются взаимно-однозначными.

Пусть $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$. *Носителем* вектора $\boldsymbol{x}$ называется множество

$$\operatorname{supp}(\boldsymbol{x}) := \{i \mid x_i \neq 0\}.$$

Далее в этом параграфе будем считать, что $q \geqslant 3$. Как было отмечено в § 2, минимальное расстояние кода $RM_q((q-1)m-2, m)$ равно 3. Кодовое слово веса 3 кода $RM_q((q-1)m-2, m)$ будем называть *тройкой*. Пусть $\boldsymbol{c} = (c_1, c_2, \ldots, c_n)$ является тройкой, и пусть $\operatorname{supp}(\boldsymbol{c}) = \{i, j, k\}$. Тогда

- тройка $\boldsymbol{c}$ лежит на прямой ℓ, если $\{P_i, P_j, P_k\} \subseteq \ell$;
- соответствующие столбцы $\boldsymbol{h}_i, \boldsymbol{h}_j, \boldsymbol{h}_k$ линейно зависимы, т.е.

$$c_i\boldsymbol{h}_i + c_j\boldsymbol{h}_j + c_k\boldsymbol{h}_k = \boldsymbol{0}.$$

Поскольку каждая тройка кода $RM_q((q-1)m-2, m)$ принадлежит нулевому пространству проверочной матрицы H кода $RM_q((q-1)m-2, m)$, то непосредственно из определения прямой аффинного пространства $AG(m, q)$ и структуры проверочной матрицы H обобщенного кода Рида – Маллера $RM_q((q-1)m-2, m)$ следует, что любая тройка кода $RM_q((q-1)m-2, m)$ лежит на некоторой прямой аффинного пространства $AG(m, q)$. Очевидно, что число троек в коде $RM_q((q-1)m-2, m)$ кратно числу ненулевых элементов поля $\mathbb{F}_q$.

При $q = 3$ любая прямая аффинного пространства $AG(m, q)$ содержит 3 точки. Следовательно, при $q = 3$ носители троек кода $RM_q((q-1)m-2, m)$ соответствуют прямым аффинного пространства $AG(m, q)$. При $q = 3$ и $m = 2$ обобщенный код Рида – Маллера $RM_q((q-1)m-2, m)$ содержит 24 тройки, носители которых соответствуют 12 прямым аффинной плоскости $AG(2, 3)$.

Пусть $i \in \{1, \ldots, n\}$. Тогда через $\mathcal{R}_i$ обозначим подпространство, натянутое на множество всех троек кода $RM_q((q-1)m-2, m)$, которые имеют 1 в i-й координате. По определению минимальное расстояние линейного кода $\mathcal{R}_i$ равно 3.

Предложение 1. *Пусть $q \geqslant 3$, $m \geqslant 1$ и $n = q^m$. Тогда при любом $i \in \{1, 2, \ldots, n\}$ размерность линейного кода $\mathcal{R}_i$ равна $n - [m]_q - 1$, где $[m]_q$ является q-аналогом натурального числа m.*

Предложение 2. *Пусть $q \geqslant 3$, $m \geqslant 1$. Пусть $\boldsymbol{c}$ – тройка и $\boldsymbol{c} \in \mathcal{R}_i$. Тогда $\boldsymbol{c}$ лежит на прямой, проходящей через точку P_i.*

Код $RM_q((q-1)m-2, m)$ является 1-квазисовершенным кодом с радиусом покрытия $\rho = 2$ (см. [1]). Для заданного кода $RM_q((q-1)m-2, m)$ и $t = 0, 1, 2$ определим множества $RM_q^{(t)}((q-1)m-2, m)$. Положим

$$RM_q^{(t)}((q-1)m-2, m) := \left\{\boldsymbol{x} \in \mathbb{F}_q^n \mid d\big(\boldsymbol{x}, RM_q((q-1)m-2, m)\big) = t\right\}.$$

Множества $RM_q^{(t)}((q-1)m-2, m)$ называются *подкомпонентами* 1-квазисовершенного кода $RM_q((q-1)m-2, m)$.

Предложение 3. *Пусть $q \geqslant 3$, $m \geqslant 2$. Пусть*

$$\boldsymbol{x} \in RM_q^{(2)}((q-1)m-2, m), \quad \operatorname{wt}(\boldsymbol{x}) = 2, \quad \operatorname{supp}(\boldsymbol{x}) = \{j, k\}.$$

Пусть $i \neq j$, $i \neq k$ и точки P_i, P_j, P_k лежат на одной прямой. Тогда существует тройка $\boldsymbol{c} \in \mathcal{R}_i$, такая что $\operatorname{supp}(\boldsymbol{c}) = \{i, j, k\}$ и $d(\boldsymbol{c}, \boldsymbol{x}) = 2$.

Обозначим через $\boldsymbol{e}_i$ вектор длины n, все компоненты которого равны нулю, кроме i-й компоненты, которая равна 1.

Пусть $\boldsymbol{x} \in RM_q((q-1)m-2, m)$, $\lambda \in \mathbb{F}_q \setminus \{0\}$. Пусть $\mathcal{R}_i + \boldsymbol{x} + \lambda \cdot \boldsymbol{e}_i$ является сдвигом смежного класса $\mathcal{R}_i + \boldsymbol{x}$. Тогда замена смежного класса $\mathcal{R}_i + \boldsymbol{x}$ на сдвиг $\mathcal{R}_i + \boldsymbol{x} + \lambda \cdot \boldsymbol{e}_i$ называется *переключением*.

Предложение 4. *Пусть* $q \geqslant 3$, $m \geqslant 2$, $n = q^m$, $\boldsymbol{x} \in RM_q((q-1)m-2, m)$. *Тогда при любом* $i \in \{1, 2, \ldots, n\}$ *и при любом* $\lambda \in \mathbb{F}_q \setminus \{0\}$ *множество*

$$\mathcal{C}' = \big(RM_q((q-1)m-2, m) \setminus (\mathcal{R}_i + \boldsymbol{x})\big) \cup \big(\mathcal{R}_i + \boldsymbol{x} + \lambda \cdot \boldsymbol{e}_i\big)$$

является нелинейным 1*-квазисовершенным кодом с параметрами* $(n, q^{n-m-1}, 3)_q$.

Пусть L_1 и L_2 являются подпространствами пространства $\mathbb{F}_q^n$. Тогда через $L_1 + L_2$ обозначим сумму подпространств L_1 и L_2. По определению

$$L_1 + L_2 := \{\boldsymbol{x} + \boldsymbol{y} \mid \boldsymbol{x} \in L_1,\ \boldsymbol{y} \in L_2\}.$$

При $m = 1$ обобщенные коды Рида – Маллера представляют собой расширенные коды Рида – Соломона [19, с. 289]. При $m = 1$ аффинное пространство $AG(1, q)$ является прямой, и $\mathcal{R}_i$ совпадает с кодом $RM_q(q-3, 1)$. Следовательно, при $m = 1$

$$\dim(RM_q((q-1)m-2, m)) = \dim(\mathcal{R}_i) = q-2.$$

Предложение 5. *Пусть* $q \geqslant 3$, $m = 2$ *и* $n = q^m$. *Тогда при любых* $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, *справедливо неравенство*

$$\dim(\mathcal{R}_i \cap \mathcal{R}_j) \geqslant q(q-2) - 1.$$

Предложение 6. *Пусть* $q \geqslant 3$, $m \geqslant 2$ *и* $n = q^m$. *Тогда при любых* $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, *справедливо неравенство*

$$\dim(\mathcal{R}_i \cap \mathcal{R}_j) \geqslant n - [m]_q - q^{m-1}.$$

Доказательство. Пусть ℓ_{ij} – прямая, проходящая через точки P_i и P_j. При $m = 2$ на прямой ℓ_{ij} лежит $q-2$ линейно независимых элементов базиса подпространства $\mathcal{R}_i \cap \mathcal{R}_j$, а остальные элементы базиса подпространства $\mathcal{R}_i \cap \mathcal{R}_j$ принадлежат плоскости, проходящей через прямую ℓ_{ij}. В аффинном пространстве $AG(m, q)$ число плоскостей, проходящих через данную прямую, равно $\dfrac{q^{m-1}-1}{q-1}$. В силу предложения 5 при $m = 2$ и при любых $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, базис подпространства $\mathcal{R}_i \cap \mathcal{R}_j$ содержит не менее чем $q(q-2)-1$ линейно независимых векторов. Следовательно, при $m \geqslant 2$ и при любых $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, базис подпространства $\mathcal{R}_i \cap \mathcal{R}_j$ содержит не менее чем

$$\frac{q^{m-1}-1}{q-1}\big(q(q-2) - 1 - (q-2)\big) + (q-2)$$

элементов. Поскольку

$$\frac{q^{m-1}-1}{q-1}\big(q(q-2) - 1 - (q-2)\big) + (q-2) = n - [m]_q - q^{m-1},$$

то при $m \geqslant 2$ и при любых $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, имеем

$$\dim(\mathcal{R}_i \cap \mathcal{R}_j) \geqslant n - [m]_q - q^{m-1}. \quad \blacktriangle$$

§ 4. Ранг и ядро

В этом параграфе мы покажем существование нелинейных 1-квазисовершенных q-ичных кодов различных рангов и в некоторых случаях построим их, а также покажем существование и в некоторых случаях построим нелинейные 1-квазисовершенные q-ичные коды с ядрами различных размерностей. Доказательства приведены в работе [17].

Теорема 1. *Пусть* $q \geqslant 3$, $m \geqslant 2$, $n = q^m$. *Пусть* $i \in \{1, 2, \ldots, n\}$ *и* $\lambda \in \mathbb{F}_q \setminus \{0\}$. *Пусть* $\boldsymbol{x} \in RM_q((q-1)m-2, m) \setminus \mathcal{R}_i$ *и*

$$\mathcal{C}' = \big(RM_q((q-1)m-2, m) \setminus (\mathcal{R}_i + \boldsymbol{x})\big) \cup \big(\mathcal{R}_i + \boldsymbol{x} + \lambda \cdot \boldsymbol{e}_i\big).$$

Тогда множество $\mathcal{C}'$ *является нелинейным* 1*-квазисовершенным кодом с параметрами* $(n, q^{n-m-1}, 3)_q$. *При этом*

$$\operatorname{rank}(\mathcal{C}') = n - m,$$
$$\dim(\ker(\mathcal{C}')) = n - [m]_q - 1.$$

Пусть $t \in \{2, 3, \ldots, m+1\}$. Координаты $i_1, i_2, \ldots, i_t$ векторного пространства $\mathbb{F}_q^n$ будем называть *независимыми*, если соответствующие этим координатам столбцы $\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_t$ проверочной матрицы H кода $RM_q((q-1)m-2, m)$ являются линейно независимыми.

Заметим, что любая пара координат $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, является независимой, поскольку минимальное расстояние кода $RM_q((q-1)m-2, m)$ равно 3.

Предложение 7. *Пусть*

- $m \geqslant 5$ *при* $q = 3, 4$,
- $m \geqslant 4$ *при* $5 \leqslant q \leqslant 19$,
- $m \geqslant 3$ *при* $q \geqslant 23$.

Пусть $n = q^m$, $t \in \{2, 3, \ldots, m+1\}$, *и пусть* $i_1, i_2, \ldots, i_t$ *являются независимыми координатами векторного пространства* $\mathbb{F}_q^n$. *Тогда существуют кодовые слова* $\boldsymbol{x}_{i_1}, \boldsymbol{x}_{i_2}, \ldots, \boldsymbol{x}_{i_t}$, *такие что*

$$\boldsymbol{x}_{i_s} \in RM_q((q-1)m-2, m) \setminus \mathcal{R}_{i_s}$$

при $i_s \in \{i_1, i_2, \ldots, i_t\}$ *и*

$$d(\mathcal{R}_i + \boldsymbol{x}_i, \mathcal{R}_j + \boldsymbol{x}_j) \geqslant 5$$

при любых $i, j \in \{i_1, i_2, \ldots, i_t\}$, $i \neq j$.

Теорема 2. *Пусть*

- $m \geqslant 5$ *при* $q = 3, 4$,
- $m \geqslant 4$ *при* $5 \leqslant q \leqslant 19$,
- $m \geqslant 3$ *при* $q \geqslant 23$.

Пусть $n = q^m$, $t \in \{2, 3, \ldots, m+1\}$, *и пусть* $i_1, i_2, \ldots, i_t$ *являются независимыми координатами векторного пространства* $\mathbb{F}_q^n$. *Пусть кодовые слова*

$$\boldsymbol{x}_{i_s} \in RM_q((q-1)m-2, m) \setminus \mathcal{R}_{i_s}$$

при $i_s \in \{i_1, i_2, \ldots, i_t\}$ *таковы, что*

$$d(\mathcal{R}_i + \boldsymbol{x}_i, \mathcal{R}_j + \boldsymbol{x}_j) \geqslant 5$$

при любых $i, j \in \{i_1, i_2, \ldots, i_t\}$, $i \neq j$.

Тогда при любых $\lambda_{i_1}, \lambda_{i_2}, \ldots, \lambda_{i_t} \in \mathbb{F}_q \setminus \{0\}$ *множество*

$$\mathcal{C}_t = \left(RM_q((q-1)m-2, m) \setminus \bigcup_{s=1}^{t} (\mathcal{R}_{i_s} + \boldsymbol{x}_{i_s})\right) \cup \left(\bigcup_{s=1}^{t} (\mathcal{R}_{i_s} + \boldsymbol{x}_{i_s} + \lambda_{i_s} \cdot \boldsymbol{e}_{i_s})\right)$$

является нелинейным 1*-квазисовершенным кодом с параметрами* $(n, q^{n-m-1}, 3)_q$.

При этом

$$\operatorname{rank}(\mathcal{C}_t) = n - m - 1 + t.$$

Следствие. *Пусть*

- $m \geqslant 5$ *при* $q = 3, 4$,
- $m \geqslant 4$ *при* $5 \leqslant q \leqslant 19$,
- $m \geqslant 3$ *при* $q \geqslant 23$.

Пусть $n = q^m$. *Тогда существуют нелинейные* 1*-квазисовершенные* q*-ичные коды полного ранга длины* n.

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

СПИСОК ЛИТЕРАТУРЫ

1. *Романов А.М.* О совершенных кодах и кодах Рида – Маллера над конечными полями // Пробл. передачи информ. 2021. Т. 57. № 3. С. 3–16. https://doi.org/10.31857/S0555292321030013
2. *Romanov A.M.* On the Number of q-ary Quasi-perfect Codes with Covering Radius 2 // Des. Codes Cryptogr. 2022. V. 90. № 8. P. 1713–1719. https://doi.org/10.1007/s10623-022-01070-y
3. *Romanov A.M.* Perfect Mixed Codes from Generalized Reed–Muller Codes // Des. Codes Cryptogr. 2024. V. 92. № 6. P. 1747–1759. https://doi.org/10.1007/s10623-024-01364-3
4. *Baicheva T., Bouyukliev I., Dodunekov S., Fack V.* Binary and Ternary Linear Quasi-Perfect Codes With Small Dimensions // IEEE Trans. Inform. Theory. 2008. V. 54. № 9. P. 4335–4339. https://doi.org/10.1109/TIT.2008.928277
5. *Etzion T., Mounits B.* Quasi-perfect Codes with Small Distance // IEEE Trans. Inf. Theory. 2005. V. 51. № 11. P. 3938–3946. https://doi.org/10.1109/TIT.2005.856944
6. *Etzion T.* Perfect Codes and Related Structures. Hackensack, NJ: World Sci., 2022.
7. *Phelps K.T., LeVan M.* Kernels of Nonlinear Hamming Codes // Des. Codes Cryptogr. 1995. V. 6. № 3. P. 247–257. https://doi.org/10.1007/BF01388478
8. *Heden O.* On Perfect p-ary Codes of Length $p + 1$ // Des. Codes Cryptogr. 2008. V. 46. № 1. P. 45–56. https://doi.org/10.1007/s10623-007-9133-y
9. *Romanov A.M.* Hamiltonicity of Minimum Distance Graphs of 1-Perfect Codes // Electron. J. Combin. 2012. V. 19. № 1. Article P65 (6 pp.). https://doi.org/10.37236/2158
10. *Romanov A.M.* Disjoint Hamiltonian Cycles in Minimum Distance Graphs of 1-Perfect Codes // Australas. J. Combin. 2017. V. 69. № 2. Part 2. P. 215–221. Available at https://ajc.maths.uq.edu.au/pdf/69/ajc_v69_p215.pdf
11. *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
12. *Phelps K.T., Villanueva M.* Ranks of q-ary 1-Perfect Codes // Des. Codes Cryptogr. 2002. V. 27. № 1–2. P. 139–144. https://doi.org/10.1023/A:1016510804974
13. *Phelps K.T., Rifà J., Villanueva M.* Rank and Kernel of Binary Hadamard Codes // IEEE Trans. Inform. Theory. 2005. V. 51. № 11. P. 3931–3937. https://doi.org/10.1109/TIT.2005.856940
14. *Li X., Shi M., Wang S., Lu H., Zheng Y.* Rank and Pairs of Rank and Dimension of Kernel of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-Linear Codes // IEEE Trans. Inform. Theory. 2024. V. 70. № 5. P. 3202–3212. https://doi.org/10.1109/TIT.2023.3317064
15. *Borges J., Phelps K.T., Rifà J.* The Rank and Kernel of Extended 1-Perfect $\mathbb{Z}_4$-Linear and Additive Non-$\mathbb{Z}_4$-Linear Codes // IEEE Trans. Inform. Theory. 2003. V. 49. № 8. P. 2028–2034. https://doi.org/10.1109/TIT.2003.814490
16. *Васильев Ю.Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. Т. 8. М.: Физматлит, 1962. С. 337–339.
17. *Romanov A.M.* On Nonlinear 1-Quasi-perfect Codes and Their Structural Properties // Probl. Inf. Transm. 2024. V. 60. № 3. P. 141–154. https://doi.org/10.1134/S0032946024030013

18. *Batten L.M.* Combinatorics of Finite Geometries, Cambridge: Cambridge Univ. Press, 1997.
19. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
20. *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
21. *Assmus E.F., Key J.D.* Polynomial Codes and Finite Geometries // Handbook of Coding Theory. Amsterdam: Elsevier, 1998. Vol. II. P. 1269–1344.
22. *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
23. *Августинович С.В., Соловьева Ф.И.* О несистематических совершенных двоичных кодах // Пробл. передачи информ. 1996. Т. 32. № 3. С. 47–50. https://www.mathnet.ru/rus/ppi344

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

Поступила в редакцию
03.06.2024
После доработки
07.11.2024
Принята к публикации
16.11.2024