

О ЯДРАХ НЕЛИНЕЙНЫХ КВАЗИСОВЕРШЕННЫХ
КОДОВА.М. РОМАНОВ *Представлено П.П. ПЕТРОВЫМ*

Abstract: We consider quasi-perfect codes with packing radius 1 over a finite field of q elements. We call these codes 1-quasi-perfect q -ary codes. We study the structural properties of nonlinear 1-quasi-perfect q -ary codes, namely the rank and dimension of the kernel. In this paper, we propose a construction of 1-quasi-perfect q -ary codes with parameters of generalized Reed-Muller codes of order $r = (q - 1)m - 2$, where m is a positive integer. For $q \geq 3$, $m \geq 2$, the proposed construction allows one to construct nonlinear 1-quasi-perfect q -ary codes with different kernel dimensions. The dimensions of the kernel of nonlinear 1-quasi-perfect q -ary codes constructed using the proposed construction are calculated.

Keywords: perfect code, quasi-perfect code, nonlinear code, generalized Reed-Muller code, code rank, code kernel, Galois geometry.

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) над полем \mathbb{F}_q . Длина кода $\mathcal{C} \subseteq \mathbb{F}_q^n$ равна

ROMANOV, A.M., ON THE KERNELS OF NONLINEAR QUASI-PERFECT CODES.

© 2025 РОМАНОВ А.М.

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

Поступила 1 января 2023 г., опубликована 31 декабря 2023 г.

размерности пространства \mathbb{F}_q^n . Векторы, принадлежащие пространству \mathbb{F}_q^n , мы будем рассматривать как слова длины n над алфавитом \mathbb{F}_q . Слова, принадлежащие коду $\mathcal{C} \subseteq \mathbb{F}_q^n$, называются *кодowymi словами*. Код называется *линейным*, если он образует линейное подпространство над \mathbb{F}_q . В противном случае код называется *нелинейным*. Мы предполагаем, что нулевой вектор $\mathbf{0}$ всегда принадлежит коду, если не указано иное.

Нелинейные коды представляют собой широкий класс кодов и включают в себя, в частности, аддитивные и K -линейные коды. Код называется *аддитивным*, если его слова образуют аддитивную подгруппу в \mathbb{F}_q^n . Код определенный над \mathbb{F}_q называется *K -линейным*, если он линейен над некоторым подполем $K \subset \mathbb{F}_q$. Очевидно, что код линейный над \mathbb{F}_p является аддитивным кодом. Аддитивные коды определяются также над всевозможными кольцами и над различными смешанными алфавитами. В последнее время аддитивные коды интенсивно изучаются из-за их связи с квантовыми кодами [1].

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

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

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

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

Радиус упаковки $e(\mathcal{C})$ кода \mathcal{C} длины n — это максимальное число $e \in \{0, 1, \dots, n\}$ такое, что $B_e(\mathbf{u}) \cap B_e(\mathbf{v}) = \emptyset$ для всех $\mathbf{u}, \mathbf{v} \in \mathcal{C}$, $\mathbf{u} \neq \mathbf{v}$.

Радиус покрытия $\rho(\mathcal{C})$ кода \mathcal{C} длины n — это минимальное число $\rho \in \{0, 1, \dots, n\}$ такое, что $\cup_{\mathbf{c} \in \mathcal{C}} B_\rho(\mathbf{c}) = \mathbb{F}_q^n$.

Определение радиуса покрытия кода — чрезвычайно сложная и важная задача. Например, вопрос о радиусе покрытия двоичных кодов Рида-Маллера остаётся открытым, за исключением некоторых случаев [2].

Максимальная нелинейность булевых функций от m переменных — это не что иное, как радиус покрытия двоичного кода Рида-Маллера первого порядка длины $n = 2^m$. Нелинейность булевой функции является важным криптографическим критерием при анализе стойкости как потоковых, так и блочных шифров [3].

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).

Код $\mathcal{C} \subseteq \mathbb{F}_q^n$ называется *покрывающим* с радиусом r , если сферы Хэмминга радиуса r с центрами в кодовых словах покрывают всё пространство \mathbb{F}_q^n . Очевидно, что код \mathcal{C} является покрывающим также для всех радиусов, больших r . Минимальный радиус, при котором \mathcal{C} является покрывающим кодом, равен его радиусу покрытия $\rho(\mathcal{C})$ (см.[3]).

Совершенный код — это покрывающий код с радиусом, равным его радиусу упаковки e . Квазисовершенный код — это покрывающий код с радиусом, равным $e + 1$.

Нелинейные покрывающие коды имеют важные приложения, например, в стеганографии [4].

Наименьшее расстояние между любыми двумя различными кодовыми словами кода \mathcal{C} называется *минимальным расстоянием* кода \mathcal{C} . Минимальное расстояние кода определяет способность кода исправлять ошибки.

Мы будем использовать обозначение $(n, M, d)_q$ для q -ичного кода длины n , мощности M и с минимальным расстоянием d . Для линейного q -ичного кода длины n , размерности k и с минимальным расстоянием d мы будем использовать обозначение $[n, k, d]_q$. В случае двоичных кодов индекс q может опускаться.

Ниже мы представляем некоторые известные результаты, касающиеся квазисовершенных кодов.

В 1966 году Терри Дж. Вагнер [5] разработал алгоритм построения проверочных матриц с использованием компьютерного поиска для нахождения квазисовершенных кодов. Вагнер [5] открыл код с параметрами $[23, 14, 5]$, который представляет собой квазисовершенный линейный двоичный код. Брауэр, Дельсарт и Пире [6] использовали смежные классы $\mathcal{C} + \mathbf{v}$, где \mathcal{C} — $[23, 14, 5]$ -код Вагнера, чтобы найти семь улучшений нижних границ для двоичных кодов с постоянным весом. Юриан Симонис [7] доказал, что все линейные двоичные коды с параметрами $[23, 14, 5]$ эквивалентны коду Вагнера.

Вопрос об уникальности $[23, 14, 5]$ -кода Вагнера среди кодов, на которые не накладывается никаких ограничений, по-видимому, остаётся открытым.

В [8] представлен новый $[22, 13, 5]$ -квазисовершенный двоичный код и на основе этого кода получены четыре улучшения нижних границ для двоичных кодов с постоянным весом.

Пусть $q = p^m$, причём $m \geq 3$. Пусть π — примитивный элемент поля \mathbb{F}_q и $j = 0, 1, \dots, q - 2$. Пусть f — отображение из \mathbb{F}_q в себя и \mathcal{C}_f — линейный код длины $q - 1$, проверочная матрица которого имеет столбец $\begin{bmatrix} \pi^j \\ f(\pi^j) \end{bmatrix}$ в качестве своего j -го столбца. Ли и Хеллесет [9] показали, что в случае $p = 2$ код \mathcal{C}_f имеет радиус покрытия 3, когда f является квадратичной APN-функцией. Это дает возможность построить ряд квазисовершенных двоичных кодов с минимальным расстоянием 5. В случае, когда p — нечётное простое число, в [9] доказано, что для всех известных планарных функций f радиус покрытия кода \mathcal{C}_f равен 2, если m нечётное, и 3, если m чётное. В результате было получено несколько классов квазисовершенных p -ичных кодов.

Ли и Хеллесет [9] представили ряд открытых вопросов, связанных с квазисовершенными кодами и криптографическими функциями.

Линейные покрывающие коды и, в частности, линейные квазисовершенные коды имеют тесную связь с объектами конечной проективной геометрии. Существует взаимно однозначное соответствие между линейными квазисовершенными кодами с минимальным расстоянием 4 и полными шапками в проективной геометрии [10].

В [11] установлено, что графы Кэли, соответствующие некоторым p -арным 2-квазисовершенным кодам Ли, являются графами Рамануджана.

Примером нелинейных квазисовершенных кодов являются коды Препараты с параметрами $(2^{2m} - 1, 2^{2^{2m}-4m}, 5)$, где $m \geq 2$ (см. [12]).

В [13] установлена тесная связь 1-совершенных кодов и 1-квазисовершенных кодов с параметрами обобщённых кодов Рида-Маллера порядка $r = (q - 1)m - 2$. В [13] показано, что с помощью конкатенации из 1-квазисовершенных кодов с параметрами обобщённых кодов Рида-Маллера порядка $r = (q - 1)m - 2$ можно построить дважды экспоненциальное число попарно неэквивалентных 1-совершенных кодов над \mathbb{F}_q .

В [13] также показано, что с помощью конкатенации из 1-совершенных кодов можно построить дважды экспоненциальное число попарно неэквивалентных чётных 1-квазисовершенных кодов с параметрами обобщённых кодов Рида-Маллера порядка $r = (q - 1)m - 2$.

В [14] показано, что с помощью переключающей конструкции из обобщённых кодов Рида-Маллера порядка $r = (q - 1)m - 2$ можно построить дважды экспоненциальное число попарно неэквивалентных 1-квазисовершенных кодов над \mathbb{F}_q .

В [15] установлена тесная связь 1-совершенных кодов над смешанным алфавитом и кодов с параметрами обобщённых кодов Рида-Маллера порядка $r = (q - 1)m - 2$. В [15] показано, что из кодов с параметрами обобщённых кодов Рида-Маллера порядка $r = (q - 1)m - 2$ можно построить дважды экспоненциальное число попарно неэквивалентных 1-совершенных кодов над смешанным алфавитом.

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

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

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

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} мы 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

$$0 \leq \dim(\ker(\mathcal{C})) \leq k - 2 \quad \text{при} \quad q = 2$$

и

$$0 \leq \dim(\ker(\mathcal{C})) \leq k - 1 \quad \text{при} \quad q \geq 3 \quad (\text{см. [16]}).$$

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, Z_2Z_4 -линейных кодов, $Z_pZ_{p^2}$ -линейных кодов [16, 17, 18, 19, 20, 21]. В [22] изучались ранг и размерность ядра некоторых подклассов квазисовершенных двоичных кодов.

Обобщённые коды Рида-Маллера порядка $r = (q - 1)m - 2$ имеют параметры $[n = q^m, n - m - 1, 3]_q$. Поскольку обобщённые коды Рида-Маллера порядка $r = (q - 1)m - 2$ являются линейными кодами, то их ранг и размерность ядра равны размерности кода.

В [23], доказано что при любом $s \in \{1, 2, \dots, m + 1\}$ существуют нелинейные 1-квазисовершенные q -ичные коды ранга $n - m - 1 + s$ с параметрами $(n = q^m, q^{n-m-1}, 3)_q$ (т.е. с параметрами обобщённых кодов Рида-Маллера порядка $r = (q - 1)m - 2$). В том числе в [23] доказано, что с данными параметрами существуют нелинейные 1-квазисовершенные q -ичные коды полного ранга. При этом $m \geq 5$ при $q = 3, 4$, $m \geq 4$ при $5 \leq q \leq 19$ и $m \geq 3$ при $q \geq 23$.

Через $[m]_q$ обозначается q -аналог натурального числа m . По определению $[m]_q := 1 + q + \dots + q^{m-1}$.

В [23] также доказано, что при $q \geq 3$, $m \geq 2$ существуют нелинейные 1-квазисовершенные q -ичные коды с параметрами $(n = q^m, q^{n-m-1}, 3)_q$ ранга $n - m$ и с размерностью ядра $n - [m]_q - 1$.

В данной работе предлагается конструкция нелинейных 1-квазисовершенных q -ичных кодов с параметрами $(n = q^m, q^{n-m-1}, 3)_q$ (т.е. с параметрами обобщённых кодов Рида-Маллера порядка $r = (q - 1)m - 2$). При $q \geq 3$ и $m \geq 2$ предложенная конструкция позволяет строить нелинейные 1-квазисовершенные q -ичные коды с различными размерностями ядра. Мы вычисляем размерности ядра нелинейных 1-квазисовершенных q -ичных кодов, построенных с использованием предложенной конструкции.

2 Предварительные сведения

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

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

Вес слова $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$ равен числу ненулевых компонент в \mathbf{x} .

Пусть слово $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$ и пусть $p(\mathbf{x}) := \sum_{i=1}^n x_i$. Тогда слово \mathbf{x} называется *чётным*, если $p(\mathbf{x}) = 0$. Код $\mathcal{C} \subseteq \mathbb{F}_q^n$ называется *чётным*, если он содержит только чётные слова.

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

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

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

Через $H_q(m)$ мы обозначим q -ичный код Хэмминга длины $n = [m]_q$, где $m \geq 2$. Код $H_q(m)$ является линейным 1-совершенным q -ичным кодом и имеет параметры $[n = [m]_q, n - m, 3]_q$. Параметры нелинейных 1-совершенных q -ичных кодов совпадают с параметрами q -ичных кодов Хэмминга [25, гл. 6, §10].

Все расширенные 1-совершенные q -ичные коды являются 1-квазисовершенными кодами.

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. Пространство $AG(m, q)$ называется также *геометрией Галуа*. Более подробные сведения по конечным геометриям можно найти, например, в [24].

Классические коды Рида-Маллера определяются над полем из двух элементов [25, гл. 13]. Обобщённые коды Рида-Маллера определяются над произвольным конечным полем из q элементов. Обобщённые коды Рида-Маллера были предложены Касами и др. в [26].

Пусть $\mathbb{F}_q[X_1, X_2, \dots, X_m]$ — алгебра многочленов от m переменных над \mathbb{F}_q . Для многочлена $f \in \mathbb{F}_q[X_1, X_2, \dots, X_m]$ через $\deg(f)$ обозначим его полную степень. Пусть $n = q^m$ и r — целое число такое, что $0 \leq r \leq (q-1)m$. Пусть точки P_1, P_2, \dots, P_n аффинного пространства $AG(m, q)$ упорядочены произвольным, но фиксированным образом. *Обобщённым кодом Рида-Маллера* длины $n = q^m$ и порядка r над \mathbb{F}_q называется подпространство

$$\left\{ (f(P_1), f(P_2), \dots, f(P_n)) \mid f \in \mathbb{F}_q[X_1, X_2, \dots, X_m], \deg(f) \leq r \right\}.$$

Обобщённый код Рида-Маллера длины $n = q^m$ и порядка r над \mathbb{F}_q мы обозначим через $RM_q(r, m)$. Код $RM_q(r, m)$ имеют следующие параметры (см. [26], [27, теорема 5.5]):

- (1) Длина кода $RM_q(r, m)$ равна q^m ;

(2) Размерность кода $RM_q(r, m)$ равна

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

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

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

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

При $r \leq (q - 1)m - 1$ обобщённый код Рида-Маллера $RM_q(r, m)$ является чётным кодом.

При $q = 2$ и $0 \leq r \leq m$ обобщённый код Рида-Маллера порядка r является классическим двоичным кодом Рида-Маллера порядка r (см. [27, пример 5.4]).

При $q = 2$ обобщённый код Рида-Маллера $RM_q(r, m)$ порядка $r = (q - 1)m - 2$ является расширенным двоичным кодом Хэмминга и имеет параметры $[n = 2^m, n - m - 1, 4]$.

При $q \geq 3$ обобщённый код Рида-Маллера $RM_q(r, m)$ порядка $r = (q - 1)m - 2$ имеет параметры $[n = q^m, n - m - 1, 3]_q$ (см. [13]).

Порядок кода, двойственного обобщённому коду Рида-Маллера порядка $r = (q - 1)m - 2$, равен 1 (см. [13]).

Обобщённые коды Рида-Маллера $RM_q(r, m)$ порядка $r = (q - 1)m - 2$ являются линейными 1-квазисовершенными кодами с радиусом покрытия 2 (см. [13]).

Известно, что обобщённые коды Рида-Маллера порядка $r = (q - 1)m - 2$ при $q = 2$ (т.е. расширенные двоичные коды Хэмминга) являются полностью регулярными кодами [12]. В [13] установлено, что обобщённые коды Рида-Маллера порядка $r = (q - 1)m - 2$ при $q \geq 3$ также являются полностью регулярными кодами с параметрами $[n = q^m, n - m - 1, 3]_q$.

3 Размерности ядра нелинейных 1-квазисовершенных кодов

Проверочная матрица H кода $RM_q((q - 1)m - 2, m)$ представляет собой матрицу, столбцами которой являются все возможные векторы длины $m + 1$ над полем \mathbb{F}_q , первая координата которых равна 1 (см. [29]).

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

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

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

Далее в этом разделе будем считать, что $q \geq 3$. Как было отмечено в разделе 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 $\mathbf{c} = (c_1, c_2, \dots, c_n)$ является тройкой и пусть $\text{supp}(\mathbf{c}) = \{i, j, k\}$. Тогда

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

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

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 обобщённого 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 $m = 2$ обобщённый код Рида-Маллера $RM_q((q-1)m-2, m)$ содержит 24 тройки, носители которых соответствуют 12 прямым аффинной плоскости $AG(2, 3)$.

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

Т.е. код \mathcal{R}_i имеет параметры

$$\left[n = q^m, n - \frac{q^m - 1}{q - 1} - 1, 3 \right]_q.$$

Доказательство. Известно, что при $q \geq 3$ каждая прямая аффинного пространства $AG(m, q)$ лежит в коде $RM_q((q-1)m-2, m)$ (см. [28, 29]). Обобщённый код Рида-Маллера $RM_q((q-1)m-2, m)$ порождается словами минимального веса [29, 30]. В аффинном пространстве $AG(m, q)$ через каждую точку проходит $\frac{n-1}{q-1}$ прямых, причем каждая прямая содержит q точек. Для каждых двух различных точек существует единственная прямая, проходящая через эти точки. Таким образом, для каждой прямой существует $q-2$ линейно независимых троек, лежащих на этой прямой. Следовательно, число линейных независимых троек, порождающих \mathcal{R}_i , равно $(q-2)\frac{n-1}{q-1} = n - [m]_q - 1$. \square

При $m = 1$ обобщенный код Рида-Маллера $RM_q((q-1)m-2, m)$ представляют собой расширенный код Рида-Соломона, который имеет параметры $[q, q-2, 3]_q$. [25, гл. 10, §3].

При $m = 1$ аффинное пространство $AG(1, q)$ является прямой, которая содержит $q-2$ линейно независимых троек. Следовательно, в силу утверждения 1 при $m = 1$

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

Таким образом, при $m = 1$ код \mathcal{R}_i совпадает с кодом Рида-Маллера $RM_q((q-1)m-2, m)$.

Предложение 2. Пусть $q \geq 3$, $m \geq 2$, $n = q^m$. Тогда при любом $i \in \{1, 2, \dots, n\}$ существует подпространство $\mathbb{L} \subseteq \mathbb{F}_q^n$ размерности $[m]_q + 1$ такое, что $\mathcal{R}_i \cap \mathbb{L} = \{\mathbf{0}\}$.

Доказательство. В силу утверждения 1 при $q \geq 3$, $m \geq 2$ и любом $i \in \{1, 2, \dots, n\}$ код \mathcal{R}_i является линейным и имеет размерность $n - [m]_q - 1$. Поскольку каждый линейный код можно сделать систематическим [25, гл. 10, §7], то найдётся подпространство $\mathbb{L} \subseteq \mathbb{F}_q^n$ размерности $[m]_q + 1$ такое, что $\mathcal{R}_i \cap \mathbb{L} = \{\mathbf{0}\}$. \square

Пусть $\mathbb{L} \subseteq \mathbb{F}_q^n$, $\dim(\mathbb{L}) = [m]_q + 1$ и X — множество ненулевых координат пространства \mathbb{L} . Пусть ϕ является биективным отображением из X в $\{1, 2, \dots, [m]_q + 1\}$. Рассмотрим расширенный 1-совершенный q -ичный код \mathcal{C} длины $[m]_q + 1$. Код $\widehat{\mathcal{C}}$ является вложением кода \mathcal{C} в \mathbb{L} , если выполняется следующее условие:

- (1) слово $(c'_1, c'_2, \dots, c'_n)$ принадлежит $\widehat{\mathcal{C}}$ тогда и только тогда, когда существует слово $(c_1, c_2, \dots, c_{[m]_q+1}) \in \mathcal{C}$ такое, что

$$c'_i = \begin{cases} c_{\phi(i)}, & \text{если } i \in X, \\ 0, & \text{если } i \notin X. \end{cases}$$

Теорема 1. Пусть $q \geq 3$, $m \geq 2$, $n = q^m$. Пусть $\mathcal{R}_i \cap \mathbb{L} = \{\mathbf{0}\}$. Пусть код $\widehat{\mathcal{C}}$ является вложением расширенного 1-совершенного q -ичного кода длины $[m]_q + 1$ в подпространство \mathbb{L} . Тогда для любого $i \in \{1, 2, \dots, n\}$ множество

$$\mathcal{C}' = \left((\mathbf{u} + \mathbf{v}) \mid \mathbf{u} \in \mathcal{R}_i, \mathbf{v} \in \widehat{\mathcal{C}} \right)$$

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

Доказательство. В силу утверждения 1 при любом $i \in \{1, 2, \dots, n\}$ код \mathcal{R}_i является линейным и имеет размерность $n - [m]_q - 1$. Следовательно, код \mathcal{R}_i содержит $q^{n-[m]_q-1}$ слов длины $n = q^m$. Любой расширенный 1-совершенный q -ичный код длины $[m]_q + 1$ содержит $q^{[m]_q-m}$ слов. Поскольку код $\widehat{\mathcal{C}}$ является вложением расширенного 1-совершенного q -ичного кода в подпространство \mathbb{L} , то код $\widehat{\mathcal{C}}$ содержит $q^{[m]_q-m}$ слов длины $n = q^m$. В силу утверждения 2 при любом $i \in \{1, 2, \dots, n\}$ существует

подпространство $\mathbb{L} \subseteq \mathbb{F}_q^n$ размерности $[m]_q + 1$ такое, что $\mathcal{R}_i \cap \mathbb{L} = \{\mathbf{0}\}$. Таким образом, код \mathcal{C}' содержит q^{n-m-1} слов длины $n = q^m$.

Далее покажем, что минимальное расстояние кода \mathcal{C}' равно 3. В силу утверждения 2 мы можем предположить, что код \mathcal{R}_i является систематическим и $\mathcal{R}_i \cap \mathbb{L} = \{\mathbf{0}\}$. Далее предположим, что первые $n - [m]_q - 1$ компонент любого вектора из \mathbb{L} равны 0. Тогда любое кодовое слово из \mathcal{C}' можно представить в виде

$$(\mathbf{u}|\mathbf{v}) + (\mathbf{0}|\mathbf{w}),$$

где $(\cdot|\cdot)$ обозначает конкатенацию, $(\mathbf{u}|\mathbf{v}) \in \mathcal{R}_i$, $(\mathbf{0}|\mathbf{w}) \in \mathbb{L}$. Поскольку код \mathcal{R}_i является систематическим, то вектор \mathbf{u} однозначно определяет вектор \mathbf{v} . Следовательно, для любых двух слов $(\mathbf{0}|\mathbf{w})$ и $(\mathbf{0}|\mathbf{w}')$ из кода $\widehat{\mathcal{C}}$ таких, что $\mathbf{w} \neq \mathbf{w}'$ справедливо неравенство

$$d((\mathbf{u}|\mathbf{v}) + (\mathbf{0}|\mathbf{w}), (\mathbf{u}|\mathbf{v}) + (\mathbf{0}|\mathbf{w}')) \geq 3.$$

Пусть $d(\mathbf{u}, \mathbf{u}') = 1$, тогда $d(\mathbf{v}, \mathbf{v}') \geq 2$, так как минимальное расстояние кода \mathcal{R}_i равно 3. Следовательно, в этом случае справедливо неравенство

$$d((\mathbf{u}|\mathbf{v}) + (\mathbf{0}|\mathbf{w}), (\mathbf{u}'|\mathbf{v}') + (\mathbf{0}|\mathbf{w})) \geq 3.$$

Аналогично доказывается случай, когда $d(\mathbf{u}, \mathbf{u}') = 2$. Таким образом, минимальное расстояние кода \mathcal{C}' равно 3.

Поскольку любой расширенный 1-совершенный q -ичный код являются 1-квазисовершенным кодом и подпространство \mathbb{L} разбивает пространство \mathbb{F}_q^n на смежные классы, то радиус покрытия кода \mathcal{C}' равен 2. \square

Конструкция, описываемая теоремой 1 имеет некоторое пересечение с работой [31], где для конструкции кодов используется та же идея.

Теорема 2. Пусть $q \geq 3$, q — простое число. Тогда существует 1-квазисовершенный код \mathcal{C}' с параметрами $(n = q^m, q^{n-m-1}, 3)_q$ и рангом $n - m - 1 + s$ такой, что:

- (1) $\dim(\ker(\mathcal{C}')) = n - [m]_q + q^{m-1} - 2$, если $m \geq 3$, $s = 1$,
- (2) $\dim(\ker(\mathcal{C}')) = n - [m]_q + (q-1)^{s-1}q^{m-s} - 1$, если $m \geq 4$, $m \geq s > 1$.

Доказательство. В [32] установлено, что если $q \geq 3$, q — простое число, то существует 1-совершенный код длины $[m]_q$ с рангом $[m]_q - m + s$ и ядром размерности:

- (1) $q^{m-1} - 1$, если $m \geq 3$, $s = 1$,
- (2) $(q-1)^{s-1}q^{m-s}$, если $m \geq 4$, $s > 1$.

Из утверждения 1 следует, что $\text{rank}(\mathcal{R}_i) = \dim(\ker(\mathcal{R}_i)) = n - [m]_q - 1$. Таким образом, принимая во внимание теорему 1, получаем требуемый результат. \square

Теорема 3. Пусть $q = p^r$, $r > 1$. Тогда существует 1-квазисовершенный код \mathcal{C}' с параметрами $(n = q^m, q^{n-m-1}, 3)_q$ и рангом $n - m - 1 + s$ (кроме $m = 2$ и $q = 4$) такой, что:

- (1) $\dim(\ker(\mathcal{C}')) = n - [m]_q + (q-2)[m-1]_q - 1$, если $m \geq 2$, $s = 1$,

$$(2) \dim(\ker(C')) = n - [m]_q + (q-3)[m-1]_q - 1, \text{ если } m \geq 3, s = 2.$$

Доказательство. В [32] установлено, что если $q = p^r$, $r > 1$, то существует 1-совершенный q -ичный код длины $[m]_q$ с рангом $[m]_q - m + s$ (кроме $m = 2$ и $q = 4$) и ядром размерности:

- (1) $(q-2)[m-1]_q$, если $m \geq 2, s = 1$,
- (2) $(q-3)[m-1]_q$, если $m \geq 3, s = 2$.

Далее, используя рассуждения, аналогичные использованным при доказательстве теоремы 2, получаем требуемый результат. \square

4 Благодарности

Автор хотел бы поблагодарить рецензента за ценные комментарии и исправления.

References

- [1] A.R. Calderbank, E.M. Rains, P.W. Shor, N.J.A. Sloane, *Quantum error correction via codes over $GF(4)$* , IEEE Trans. Inform. Theory, **44**:4 (1998), 1369–1387.
- [2] C. Carlet, S. Mesnager, *Improving the upper bounds on the covering radii of binary Reed-Muller codes*, IEEE Trans. Inf. Theory, **53**:1 (2007), 162–173.
- [3] G.D. Cohen, I. Honkala, S.N. Litsyn, A. Lobstein, *Covering codes*, North-Holland, Amsterdam, 1997.
- [4] J. Bierbrauer, J. Fridrich, *Constructing good covering codes for applications in steganography*, in Y.Q. Shi (ed.), *Transactions on data hiding and multimedia security III*, Lect. Notes Comput. Sci., **4920**, Springer, Berlin, 2008, 1–22.
- [5] T.J. Wagner, *A search technique for quasi-perfect codes*, Inform. Control, **9**:1 (1966), 94–99.
- [6] A. Brouwer, P. Delsarte, P. Piret, *On the (23, 14, 5) Wagner code*, IEEE Trans. Inform. Theory, **26**:6 (1980), 742–743.
- [7] J. Simonis, *The [23, 14, 5] Wagner code is unique*, Discrete Math., **213**:1-3 (2000), 269–282.
- [8] Z. Chen, P. Fan, F. Jin, *On a new binary [22, 13, 5] code*, IEEE Trans. Inform. Theory, **36**:1 (1990), 228–229.
- [9] C. Li, T. Helleseth, *Quasi-perfect linear codes from planar and APN functions*, Cryptogr. Commun., **8**:2 (2016), 215–227.
- [10] M. Giulietti, F. Pasticci, *Quasi-perfect linear codes with minimum distance 4*, IEEE Trans. Inform. Theory, **53**:5 (2007), 1928–1935.
- [11] K. Bibak, B.M. Kapron, V. Srinivasan, *The Cayley graphs associated with some quasi-perfect Lee codes are Ramanujan graphs*, IEEE Trans. Inform. Theory, **62**:11 (2016), 6355–6358.
- [12] J. Borges, J. Rifà, V.A. Zinoviev, *On completely regular codes*, Probl. Inf. Transm., **55**:1 (2019), 1–45.
- [13] A.M. Romanov, *On perfect and Reed-Muller codes over finite fields*, Probl. Inf. Transm. **57**:3 (2021), 199–211.
- [14] A.M. Romanov, *On the number of q -ary quasi-perfect codes with covering radius 2*, Des. Codes Cryptogr., **90**:8 (2022), 1713–1719.

- [15] A.M. Romanov, *Perfect mixed codes from generalized Reed-Muller codes*, Des. Codes Cryptogr., **92**:6 (2024), 1747–1759.
- [16] K.T. Phelps, M. LeVan, *Kernels of nonlinear Hamming codes*, Des. Codes Cryptogr., **6**:3 (1995), 247–257.
- [17] T. Etzion, A. Vardy, *Perfect binary codes: constructions, properties, and enumeration*, IEEE Trans. Inform. Theory, **40**:3 (1994), 754–763.
- [18] K.T. Phelps, M. Villanueva, *Ranks of q -ary 1-perfect codes*, Des. Codes Cryptogr., **27**:1-2 (2002), 139–144.
- [19] K.T. Phelps, J. Rifà, M. Villanueva, *Rank and kernel of binary Hadamard codes*, IEEE Trans. Inform. Theory, **51**:11 (2005), 3931–3937.
- [20] J. Borges, C. Fernandez-Cordoba, J. Rifà, M. Villanueva, *Z_2Z_4 -linear codes*, Springer, Cham, 2022.
- [21] X. Li, M. Shi, S. Wang, H. Lu, Y. Zheng, *Rank and pairs of rank and dimension of kernel of $Z_pZ_{p^2}$ -linear codes*, IEEE Trans. Inform. Theory, **70**:5 (2024), 3202–3212.
- [22] J. Borges, K.T. Phelps, J. Rifà, *The rank and kernel of extended 1-perfect Z_4 -linear and additive non- Z_4 -linear codes*, IEEE Trans. Inform. Theory, **49**:8 (2003), 2028–2034.
- [23] A.M. Romanov, *On nonlinear 1-quasi-perfect codes and their structural properties*, Probl. Inf. Transm. **60**:3 (2024), 141–154.
- [24] L.M. Batten, *Combinatorics of finite geometries*, 2nd edn., Cambridge University Press, Cambridge, 1997.
- [25] F.J. MacWilliams, N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.
- [26] T. Kasami, S. Lin, W.W. Peterson, *New generalizations of the Reed-Muller codes. Part I: Primitive codes*, IEEE Trans. Inform. Theory, **14**:2 (1968), 189–199.
- [27] E.F. Assmus, J.D. Key, *Polynomial codes and finite geometries*, in *Handbook of Coding Theory*, V.S. Pless, W.C. Huffman, R.A. Brualdi, eds., **II**, Elsevier, Amsterdam, 1998, 1269–1344.
- [28] T. Kasami, S. Lin, W.W. Peterson, *Polynomial codes*, IEEE Trans. Inform. Theory, **14**:6 (1968), 807–814.
- [29] P. Delsarte, J.M. Goethals, F.J. MacWilliams, *On generalized Reed-Muller codes and their relatives*, Inform. Contr., **16**:5 (1970), 403–442.
- [30] P. Ding, J.D. Key, *Minimum-weight codewords as generators of generalized Reed-Muller codes*, IEEE Trans. Inform. Theory, **46**:6 (2000), 2152–2158.
- [31] J. Borges, J. Rifà, V.A. Zinoviev, *On completely regular and completely transitive supplementary codes*, Discrete Math., **343**:3 (2020), 111732.
- [32] K.T. Phelps, J. Rifà, M. Villanueva, *Kernels and p -kernels of p^r -ary 1-perfect codes*, Des. Codes Cryptogr., **37**:2 (2005), 243–261.

ALEXANDER MIKHAILOVICH ROMANOV
SOBOLEV INSTITUTE OF MATHEMATICS,
PR. КОПТЮГА, 4,
630090, NOVOSIBIRSK, RUSSIA
E-mail address: rom@math.nsc.ru