

## О СОВЕРШЕННЫХ КОДАХ ПОЛНОГО РАНГА НАД КОНЕЧНЫМИ ПОЛЯМИ \*)

А. М. Романов<sup>1</sup>

<sup>1</sup>Институт математики им. С. Л. Соболева,  
пр. Коптюга, 4, 630090 Новосибирск, Россия  
e-mail: rom@math.nsc.ru

**Аннотация.** Предложена конструкция  $q$ -ичных 1-совершенных кодов полного ранга, которая является обобщением конструкции двоичных 1-совершенных кодов полного ранга Этциона и Варди (1994 г.). Исследованы свойства  $i$ -компонент  $q$ -ичных кодов Хэмминга, конструкция  $q$ -ичных 1-совершенных кодов полного ранга основана на этих свойствах. Дано обобщение свитчинговой конструкции на  $q$ -ичный случай. Предложено обобщение понятия  $i$ -компоненты 1-совершенного кода, и введено понятие  $(i, \sigma)$ -компоненты  $q$ -ичного 1-совершенного кода. Также предложено обобщение конструкции  $q$ -ичных 1-совершенных кодов Линдстрёма — Шёнхейма, для которого дана нижняя оценка числа различных  $q$ -ичных 1-совершенных кодов длины  $n$ . Библиогр. 16.

**Ключевые слова:** код Хэмминга, нелинейный совершенный код, код полного ранга,  $i$ -компонента.

### Введение

Пусть  $\mathbb{F}_q^n$  — векторное пространство размерности  $n$  над конечным полем  $\mathbb{F}_q$ . Расстояние Хэмминга между двумя векторами  $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$  равно числу координат, в которых они различаются, и обозначается через  $d(\mathbf{x}, \mathbf{y})$ . Произвольное подмножество  $\mathcal{C}$  из  $\mathbb{F}_q^n$  называется  $q$ -ичным 1-совершенным кодом, если для каждого вектора  $\mathbf{x} \in \mathbb{F}_q^n$  существует единственный вектор  $\mathbf{c} \in \mathcal{C}$  такой, что  $d(\mathbf{x}, \mathbf{c}) \leq 1$ . Нетривиальные  $q$ -ичные 1-совершенные коды длины  $n$  существуют, если  $n = (q^m - 1)/(q - 1)$ , где  $m$  — натуральное число, не меньшее двух. Два кода  $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$  называются эквивалентными, если существует вектор  $\mathbf{v} \in \mathbb{F}_q^n$  и мономатрица  $M$  размера  $n \times n$  над полем  $\mathbb{F}_q$  такая, что

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

---

\*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 14-01-00507).

Будем предполагать, что нулевой вектор  $\mathbf{0}$  принадлежит коду. Код называется *линейным*, если он образует линейное подпространство над  $\mathbb{F}_q$ . Линейные  $q$ -ичные 1-совершенные коды длины  $n$  единственны с точностью до эквивалентности и называются  *$q$ -ичными кодами Хэмминга*. Будем обозначать  $q$ -ичный код Хэмминга длины  $n = (q^m - 1)/(q - 1)$  через  $\mathcal{H}_{q,m}$ . Коды Хэмминга будут играть ключевую роль в данной работе.

Рангом кода  $\mathcal{C}$  является максимальное число линейно независимых слов кода  $\mathcal{C}$ . Говорят, что код длины  $n$  и ранга  $n$  называется *кодом полного ранга*; в противном случае код не является кодом полного ранга. Заметим, что ранг кода Хэмминга  $\mathcal{H}_{q,m}$  равен  $n - m$ , где  $n = (q^m - 1)/(q - 1)$ ,  $m \geq 2$ .

Данная работа является продолжением работы автора [5], в которой предложено обобщение результатов из [6, 7] на  $q$ -ичный случай.

В двоичном случае 1-совершенные коды полного ранга предложены Этционом и Варди [7]. Двоичные 1-совершенные коды полного ранга построены в [7] с помощью свитчинговой конструкции [1, 7, 10, 13, 16]: в коде Хэмминга выбираются специальные подмножества кодовых слов ( $i$ -компоненты), в этих  $i$ -компонентах кодовые слова изменяются и ранг кода, полученного таким способом, возрастает. Решение Этциона и Варди было конструктивным, т. е. в [7] показано, как, исходя из проверочной матрицы двоичного кода Хэмминга, построить  $i$ -компоненты, сдвиг которых приводит к двоичным 1-совершенным кодам полного ранга.

Существование  $q$ -ичных 1-совершенных кодов полного ранга в неконструктивном смысле доказано в [13]. Фелпс и Вильянуэва [13] показали, что из мощностных соображений в  $q$ -ичном коде Хэмминга существуют  $i$ -компоненты, сдвиг которых превращает  $q$ -ичный код Хэмминга в  $q$ -ичный 1-совершенный код полного ранга. Но в [13] в отличие от [7] остался открытым вопрос о том, какие именно  $i$ -компоненты  $q$ -ичного кода Хэмминга нужно сдвигать, чтобы получить  $q$ -ичный 1-совершенный код полного ранга. В данной работе мы обобщаем результаты Этциона и Варди [13] и даём ответ на остававшийся открытым вопрос о построении  $i$ -компонент в  $q$ -ичном коде Хэмминга, сдвиг которых превращает  $q$ -ичный код Хэмминга в  $q$ -ичный 1-совершенный код полного ранга. Таким образом, предлагается конструкция  $q$ -ичных 1-совершенных кодов полного ранга, которая обобщает конструкцию двоичных 1-совершенных кодов полного ранга Этциона и Варди [7].

В  $q$ -ичном случае свитчинговая конструкция по-прежнему слабо изучена. Остаётся открытым вопрос о минимальной возможной мощности пересечения двух различных  $q$ -ичных 1-совершенных кодов, в двоичном

случае ответ на этот вопрос получен в [7]. Исследуем свойства  $i$ -компонент  $q$ -ичных кодов Хэмминга, конструкция  $q$ -ичных 1-совершенных кодов полного ранга основана на этих свойствах. Свитчинговая конструкция двоичных 1-совершенных кодов обобщается для  $q$ -ичных 1-совершенных кодов. Обобщаем понятие  $i$ -компоненты 1-совершенного кода и вводим понятие  $(i, \sigma)$ -компоненты  $q$ -ичного 1-совершенного кода, а также обобщаем конструкцию Линдстрёма [10] и Шёнхейма [16]  $q$ -ичных 1-совершенных кодов и приводим нижнюю оценку для числа различных таких кодов длины  $n$ .

Установлено [1, 8, 10, 16], что существует не менее чем  $q^{q^{cn}}$  неэквивалентных  $q$ -ичных 1-совершенных кодов длины  $n$ .

### 1. Определение $(i, \sigma)$ -компонент

Обобщим понятие  $i$ -компонент и введём понятие  $(i, \sigma)$ -компонент, а также дадим обобщение свитчинговой конструкции.

Пусть  $\mathcal{C}$  — код над полем  $\mathbb{F}_q$ . *Дистанционным графом кода  $\mathcal{C}$*  называется граф, множество вершин которого есть  $\mathcal{C}$ , и вершины  $\mathbf{x}, \mathbf{y} \in \mathcal{C}$  являются смежными, тогда и только тогда, когда  $d(\mathbf{x}, \mathbf{y}) = d$ , где  $d$  — фиксированное натуральное число. Если  $d$  является минимальным расстоянием кода  $\mathcal{C}$ , то дистанционный граф называется *графом минимального расстояния кода  $\mathcal{C}$* . Можем выколоть код  $\mathcal{C}$ , удалив одну и ту же координату  $i$  в каждом кодовом слове, обозначим выколотый код через  $\mathcal{C}^i$ .

Заметим, что граф минимального расстояния выколотого кода  $\mathcal{C}^i$  разбивается на компоненты связности. Далее дадим определение  $i$ -компоненты двоичного 1-совершенного кода  $\mathcal{C}$  длины  $n$ , где  $i \in \{1, 2, \dots, n\}$ .

**Определение 1.** Подмножество или подкод  $\mathcal{R}$  кода  $\mathcal{C}$  является  $i$ -компонентой кода  $\mathcal{C}$ , если граф минимального расстояния выколотого кода  $\mathcal{R}^i$  является компонентой связности графа минимального расстояния выколотого кода  $\mathcal{C}^i$ .

Аналогично можно определить  $i$ -компоненты для  $q$ -ичных кодов. Приведём обобщение свитчинговой конструкции для  $q$ -ичных 1-совершенных кодов.

Пусть заданы  $i$ -компонента  $\mathcal{R}_i \subseteq \mathbb{F}_q^n$  и перестановка  $\sigma$  элементов в  $\mathbb{F}_q$ . Определим код  $\sigma(\mathcal{R}_i)$ . Пусть

$$\sigma(\mathcal{R}_i) = \{(x_1, x_2, \dots, \sigma(x_i), \dots, x_n) : (x_1, x_2, \dots, x_i, \dots, x_n) \in \mathcal{R}_i\}.$$

**Теорема 1.** Пусть  $\{\mathcal{R}_i(1), \mathcal{R}_i(2), \dots, \mathcal{R}_i(t)\}$  — семейство  $i$ -компонент  $q$ -ичного 1-совершенного кода  $\mathcal{C}_1$  длины  $n$  и  $\sigma_1, \sigma_2, \dots, \sigma_t$  — перестановки элементов в  $\mathbb{F}_q$ . Тогда код

$$\mathcal{C} = \left( \mathcal{C}_1 \setminus \bigcup_{s=1}^t \mathcal{R}_i(s) \right) \cup \left( \bigcup_{s=1}^t \sigma_s(\mathcal{R}_i(s)) \right). \quad (1)$$

является  $q$ -ичным 1-совершенным кодом длины  $n$ .

**ДОКАЗАТЕЛЬСТВО.** Необходимо показать, что число кодовых слов в коде  $\mathcal{C}$  корректно и минимальное расстояние  $d(\mathcal{C})$  кода  $\mathcal{C}$  равно 3. Так как  $|\mathcal{R}_i(s)| = |\sigma_s(\mathcal{R}_i(s))|$ , из определения  $i$ -компоненты следует, что  $i$ -компоненты из  $\{\mathcal{R}_i(1), \mathcal{R}_i(2), \dots, \mathcal{R}_i(t)\}$  попарно не пересекаются. Получаем

$$|\mathcal{C}| = |\mathcal{C}_1| - \sum_{s=1}^t |\mathcal{R}_i(s)| + \sum_{s=1}^t |\sigma_s(\mathcal{R}_i(s))| = |\mathcal{C}_1| = q^{n-m}.$$

Перестановка  $\sigma_s$  определяет изометрическое преобразование пространства  $\mathbb{F}_q^n$ . Следовательно,  $d(\sigma_s(\mathcal{R}_i(s))) = 3$ ,  $s \in \{1, 2, \dots, t\}$ . Рассмотрим выколотые коды  $(\mathcal{R}_i(s))^i$  и  $(\mathcal{C}_1 \setminus \mathcal{R}_i(s))^i$ . Из определения  $i$ -компоненты следует, что для любых  $\mathbf{x} \in (\mathcal{R}_i(s))^i$  и  $\mathbf{y} \in (\mathcal{C}_1 \setminus \mathcal{R}_i(s))^i$  справедливо неравенство  $d(\mathbf{x}, \mathbf{y}) \geq 3$ . Таким образом,  $d(\mathbf{x}, \mathbf{y}) \geq 3$  для любых  $\mathbf{x} \in \sigma_s(\mathcal{R}_i(s))$  и  $\mathbf{y} \in (\mathcal{C}_1 \setminus \mathcal{R}_i(s))$ . Поскольку  $i$ -компоненты из  $\{\mathcal{R}_i(1), \mathcal{R}_i(2), \dots, \mathcal{R}_i(t)\}$  попарно не пересекаются, код  $\mathcal{C}$  является  $q$ -ичным 1-совершенным кодом длины  $n$ . Теорема 1 доказана.

В двоичном случае существует единственная нетривиальная перестановка элементов в  $\mathbb{F}_2$  и (1) принимает вид

$$\mathcal{C} = \left( \mathcal{C}_1 \setminus \bigcup_{s=1}^t \mathcal{R}_i(s) \right) \cup \left( \bigcup_{s=1}^t (\mathcal{R}_i(s) + \mathbf{e}_i) \right),$$

где  $\mathbf{e}_i$  — вектор, в котором  $i$ -я компонента равна 1, а остальные компоненты равны 0.

Теперь обобщим понятие  $i$ -компоненты 1-совершенного кода и введём понятие  $(i, \sigma)$ -компоненты  $q$ -ичного 1-совершенного кода. Частные случаи  $(i, \sigma)$ -компонент рассмотрены в [2, 14]. Представим два определения  $(i, \sigma)$ -компоненты.

Следуя [2], дадим рекурсивное определение  $(i, \sigma)$ -компоненты.

**Определение 2.** Для  $q$ -ичного 1-совершенного кода  $\mathcal{C} \subset \mathbb{F}_q^n$ , координаты  $i$  и перестановки  $\sigma$  элементов в  $\mathbb{F}_q$  подкод  $\mathcal{R}_{(i,\sigma)} \subseteq \mathcal{C}$  является  $(i, \sigma)$ -компонентой кода  $\mathcal{C}$ , если из отношения  $\mathbf{y} \in \mathcal{R}_{(i,\sigma)}$  следует, что

$$\{\mathbf{x} \mid \mathbf{x} \in \mathcal{C}, d(\mathbf{x}, \mathbf{y}(i, \sigma)) = 2\} \subseteq \mathcal{R}_{(i,\sigma)},$$

где  $\mathbf{y}(i, \sigma) = (y_1, y_2, \dots, \sigma(y_i), \dots, y_n)$ .

Следуя [14], дадим определение  $(i, \sigma)$ -компоненты в терминах теории графов. Для заданных  $q$ -ичного 1-совершенного кода  $\mathcal{C} \subset \mathbb{F}_q^n$ , координаты  $i$  и перестановки  $\sigma$  элементов в  $\mathbb{F}_q$  определим код  $\mathcal{C}(i, \sigma)$ . Пусть

$$\mathcal{C}(i, \sigma) = \{(x_1, x_2, \dots, \sigma(x_i), \dots, x_n) \mid (x_1, x_2, \dots, x_i, \dots, x_n) \in \mathcal{C}\}.$$

**Определение 3.** Для  $q$ -ичного 1-совершенного кода  $\mathcal{C} \subset \mathbb{F}_q^n$ , координаты  $i$  и перестановки  $\sigma$  элементов в  $\mathbb{F}_q$  рассмотрим дистанционный двудольный граф, порождённый кодом  $\mathcal{C} \cup \mathcal{C}(i, \sigma)$ . Два кодовых слова  $\mathbf{x} \in \mathcal{C}$  и  $\mathbf{y} \in \mathcal{C}(i, \sigma)$  называются *смежными* тогда и только тогда, когда  $d(\mathbf{x}, \mathbf{y}) = 2$ . Тогда  $(i, \sigma)$ -компоненты кода  $\mathcal{C}$  будут соответствовать компонентам связности дистанционного двудольного графа, порождённого кодом  $\mathcal{C} \cup \mathcal{C}(i, \sigma)$ .

Пусть  $\mathcal{R}_{i,\sigma}$  —  $(i, \sigma)$ -компонента  $q$ -ичного 1-совершенного кода  $\mathcal{C}_1$  длины  $n$  и

$$\sigma(\mathcal{R}_{i,\sigma}) = \{(x_1, x_2, \dots, \sigma(x_i), \dots, x_n) \mid (x_1, x_2, \dots, x_i, \dots, x_n) \in \mathcal{R}_{i,\sigma}\}.$$

Тогда  $\mathcal{C} = (\mathcal{C}_1 \setminus \mathcal{R}_{i,\sigma}) \cup (\sigma(\mathcal{R}_{i,\sigma}))$  является  $q$ -ичным 1-совершенным кодом длины  $n$ .

Пусть  $\mathcal{C}_1$  —  $q$ -ичный 1-совершенный код,  $\mathcal{R}_{i,\sigma}$  —  $(i, \sigma)$ -компонента  $\mathcal{C}_1$  и  $\mathcal{C}_2 = (\mathcal{C}_1 \setminus \mathcal{R}_{i,\sigma}) \cup (\sigma(\mathcal{R}_{i,\sigma}))$ . Тогда говорим, что код  $\mathcal{C}_2$  получается из кода  $\mathcal{C}_1$  *свитчингом*  $(i, \sigma)$ -компоненты  $\mathcal{R}_{i,\sigma}$ .

Пусть  $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_t$  —  $q$ -ичные 1-совершенные коды длины  $n$  и  $\mathcal{C}_{s+1}$  получается из  $\mathcal{C}_s$  свитчингом  $(i_s, \sigma_s)$ -компоненты, где  $s \in \{1, 2, \dots, t-1\}$ ,  $i_s \in \{1, 2, \dots, n\}$  и  $\sigma_s$  — перестановка элементов в  $\mathbb{F}_q$ . Тогда говорим, что код  $\mathcal{C}_t$  получается из кода  $\mathcal{C}_1$  *последовательностью свитчингов*.

*Свитчинговым классом*  $q$ -ичного 1-совершенного кода  $\mathcal{C}$  является совокупность всех неэквивалентных  $q$ -ичных 1-совершенных кодов, которые могут быть получены из кода  $\mathcal{C}$  последовательностью свитчингов.

Будем называть  $q$ -ичный 1-совершенный код полного ранга *кодом 1-го типа*, если его свитчинговый класс содержит коды, не являющиеся кодами полного ранга; в противном случае будем называть его *кодом 2-го типа*.

Вопрос о существовании  $q$ -ичных 1-совершенных кодов 2-го типа остаётся открытым. Впервые этот вопрос поставлен в [4].

Показано [12], что существует 9 свитчинговых классов для двоичных 1-совершенных кодов длины 15, которые имеют размеры 5819, 153, 3, 2, 2, 1, 1, 1 и 1. Свитчинговый класс кода Хэмминга содержит 5819 неэквивалентных кодов и содержит все коды полного ранга за исключением двух. Два кода полного ранга, которые не содержатся в свитчинговом классе кода Хэмминга, содержат ещё один код в их свитчинговом классе, и этот код имеет ранг 14. В двоичном случае  $(i, \sigma)$ -компоненты являются  $i$ -компонентами. Следовательно, двоичных 1-совершенных кодов полного ранга 2-го типа не существует.

## 2. Свойства $i$ -компонент

В этом разделе исследуем свойства  $i$ -компонент  $q$ -ичных кодов Хэмминга, а также обобщим конструкцию Линдстрёма [10] и Шёнхейма [16]. Снабдим эту обобщённую конструкцию нижней оценкой для числа  $q$ -ичных 1-совершенных кодов длины  $n$  и докажем теоремы, описывающие некоторые свойства  $i$ -компонент  $q$ -ичных кодов Хэмминга  $\mathcal{H}_{q,m}$ .

Проверочная матрица  $H = [\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_n]$  кода Хэмминга  $\mathcal{H}_{q,m}$  длины  $n = (q^m - 1)/(q - 1)$  состоит из  $n$  попарно линейно независимых вектор-столбцов  $\mathbf{h}_i$ ,  $i \in \{1, \dots, n\}$ . Транспонированный вектор-столбец  $\mathbf{h}_i^T$  принадлежит  $\mathbb{F}_q^m$ ,  $i \in \{1, \dots, n\}$ . Предполагаем, что столбцы проверочной матрицы  $H$  упорядочены произвольным, но фиксированным образом. Множество  $\mathbb{F}_q^m \setminus \{\mathbf{0}\}$  порождает проективную геометрию  $PG_{m-1}(q)$  размерности  $m - 1$  над конечным полем  $\mathbb{F}_q$ . В этой геометрии точки соответствуют столбцам матрицы  $H$  и точки  $i, j, k$  лежат на одной прямой, если соответствующие им столбцы  $\mathbf{h}_i, \mathbf{h}_j, \mathbf{h}_k$  линейно зависимы.

Обозначим прямую, проходящую через точки  $x$  и  $y$ , через  $l_{xy}$ , а плоскость, порождённую тремя неколлинеарными точками  $x, y, z$ , через  $P_{xyz}$ . Пусть  $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$ . Носителем вектора  $\mathbf{x}$  называется множество  $\text{supp}(\mathbf{x}) = \{i \mid x_i \neq 0\}$ . Вектор веса 3  $q$ -ичного кода Хэмминга  $\mathcal{H}_{q,m}$  называется *тройкой*. Тройка принадлежит прямой  $l$ , если носитель этой тройки принадлежит  $l$ . Тройки пересекаются в точке  $i$ , если их носители пересекаются в точке  $i$ .

Следуя [13], рассмотрим подпространство, порождённое множеством всех троек кода  $\mathcal{H}_{q,m}$  с 1 в  $i$ -й координате. Это подпространство обозначим через  $\mathcal{R}_i$ . Следуя [4], назовём подпространство  $\mathcal{R}_i$  кода Хэмминга  $\mathcal{H}_{q,m}$  *главной  $i$ -компонентой*.

Рассмотрим вектор  $\mathbf{x} \in \mathbb{F}_q^n$  такой, что  $\text{supp}(\mathbf{x})$  является  $(m-2)$ -мерной гиперплоскостью. Обозначим множество всех векторов  $\mathbf{u} \in \mathbb{F}_q^n$  таких, что

$\text{supp}(\mathbf{u}) \subseteq \text{supp}(\mathbf{x})$ , через  $\mathbb{F}_q^n(\mathbf{x})$ . Пусть  $\mathcal{H}_l$  является подкодом кода  $\mathcal{H}_{q,m}$ , определяемым прямой  $l$ , т. е.  $\mathcal{H}_l = \{\mathbf{u} \mid \mathbf{u} \in \mathcal{H}_{q,m} \text{ и } \text{supp}(\mathbf{u}) \subseteq l\}$ .

Рассмотрим пучок прямых  $l_1, l_2, \dots, l_{(n-1)/q}$ , которые проходят через точку  $i$ . Показано [3], что

$$\mathcal{R}_i = \mathcal{H}_{l_1} + \mathcal{H}_{l_2} + \dots + \mathcal{H}_{l_{(n-1)/q}}. \quad (2)$$

Каждая прямая, проходящая через точку  $i$ , содержит  $q-1$  линейно независимых троек. Таким образом, из (2) следует, что размерность  $\mathcal{R}_i$  равна  $(q-1)((n-1)/q) = q^{m-1} - 1$  [13].

**Теорема 2.** Для заданной координаты  $i$  и  $\mathbf{u} \in \mathcal{H}_{q,m}$  код  $\mathcal{R}_i + \mathbf{u}$  является  $i$ -компонентой  $q$ -ичного кода Хэмминга  $\mathcal{H}_{q,m}$  длины  $n = (q^m - 1)/(q - 1)$ ,  $m \geq 2$ .

**ДОКАЗАТЕЛЬСТВО.** Рассмотрим выколотый код  $\mathcal{R}_i^i$ . Код  $\mathcal{R}_i^i$  линейный и порождается словами веса 2. Тем самым код  $\mathcal{R}_i^i$  гамильтонов и граф минимального расстояния кода  $\mathcal{R}_i^i$  связный [15]. Без ограничения общности можем предполагать, что  $i \notin \text{supp}(\mathbf{x})$ , где  $\mathbf{x} \in \mathbb{F}_q^n$  и  $\text{supp}(\mathbf{x})$  является гиперплоскостью размерности  $m-2$ . Следовательно, учитывая лемму 1 в [15], имеем

$$\mathcal{H}_{q,m} = \bigcup_{\mathbf{u} \in \mathcal{H}_{\mathbf{x}}} \mathcal{R}_i + \mathbf{u},$$

где  $\mathcal{H}_{\mathbf{x}}$  — подкод кода  $\mathcal{H}_{q,m}$ , который определяется гиперплоскостью  $\text{supp}(\mathbf{x})$  размерности  $m-2$ . Стало быть, граф минимального расстояния выколотого кода  $(\mathcal{R}_i + \mathbf{u})^i$  является компонентой связности графа минимального расстояния выколотого кода Хэмминга  $\mathcal{H}_{q,m}^i$ . Теорема 2 доказана.

Далее представим конструкцию Линдстрёма [10] и Шёнхейма [16]  $q$ -ичных 1-совершенных кодов.

Пусть заданы  $q$ -ичный 1-совершенный код  $\mathcal{C}_1 \subset \mathbb{F}_q^n$  и функция  $\lambda$ , определённая на множестве  $\mathcal{C}_1$ , со значениями в  $\mathbb{F}_q$ . Построим код  $\mathcal{C} \subset \mathbb{F}_q^{qn+1}$ . Пусть  $\alpha_1, \alpha_2, \dots, \alpha_{q-1}$  — все ненулевые элементы поля  $\mathbb{F}_q$ . Тогда

$$\mathcal{C} = \left\{ (\mathbf{u}_1 | \mathbf{u}_2 | \dots | \mathbf{u}_{q-1} | \mathbf{v} + \sum_{i=1}^{q-1} \mathbf{u}_i \left| \sum_{i=1}^{q-1} \alpha_i p(\mathbf{u}_i) + \lambda(\mathbf{v}) \right| \right. \\ \left. \mathbf{u}_i \in \mathbb{F}_q^n, \alpha_i \in \mathbb{F}_q \setminus \{0\}, i \in \{1, \dots, q-1\}, \mathbf{v} \in \mathcal{C}_1 \right\}$$

является  $q$ -ичным 1-совершенным кодом длины  $qn + 1$  (см. [10, 16]).

Представим обобщение конструкции Линдстрёма [10] и Шёнхейма [16]  $q$ -ичных 1-совершенных кодов.

Пусть  $\mathcal{C}_1$  —  $q$ -ичный 1-совершенный код длины  $n = (q^m - 1)/(q - 1)$ ,  $m \geq 2$ ,  $\mathcal{R}_i$  — главная  $i$ -компонента  $q$ -ичного кода Хэмминга  $\mathcal{H}_{q,m+1}$ ,  $i \leq (q-1)n+1$  и  $\sigma_{\mathbf{c}}$  — перестановка элементов поля  $\mathbb{F}_q$ ,  $\mathbf{c} \in \mathcal{C}_1$ . Определим код  $\mathcal{C}$ . Пусть

$$\mathcal{C} = \bigcup_{\mathbf{c} \in \mathcal{C}_1} \sigma_{\mathbf{c}}(\mathcal{R}_i + (\mathbf{0}|\mathbf{c})), \quad (3)$$

где  $\mathbf{0} \in \mathbb{F}_q^{(q-1)n+1}$  — нулевой вектор.

**Теорема 3.** Код  $\mathcal{C}$  является  $q$ -ичным 1-совершенным кодом длины  $qn + 1$ .

**ДОКАЗАТЕЛЬСТВО.** Рассмотрим вектор  $\mathbf{x} \in \mathbb{F}_q^n$ , носитель которого  $\text{supp}(\mathbf{x})$  является  $(m-2)$ -мерной гиперплоскостью. Без ограничения общности можем считать, что

$$\text{supp}(\mathbf{x}) = \{(q-1)n+2, (q-1)n+3, \dots, qn+1\}.$$

Так как  $i \leq (q-1)n+1$ , имеем  $i \notin \text{supp}(\mathbf{x})$ . Поскольку  $\mathcal{R}_i$  является главной  $i$ -компонентой  $q$ -ичного кода Хэмминга и  $i \notin \text{supp}(\mathbf{x})$ , граф минимального расстояния кода  $(\mathcal{R}_i + (\mathbf{0}|\mathbf{c}))^i$  связный. Из леммы 1 в [15] вытекает, что

$$(\mathcal{R}_i + (\mathbf{0}|\mathbf{c}_1)) \cap (\mathcal{R}_i + (\mathbf{0}|\mathbf{c}_2)) = \emptyset$$

для всех  $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}_1$ ,  $\mathbf{c}_1 \neq \mathbf{c}_2$ .

Рассмотрим выколотые коды  $(\mathcal{R}_i + (\mathbf{0}|\mathbf{c}_1))^i$  и  $(\mathcal{R}_i + (\mathbf{0}|\mathbf{c}_2))^i$ . Так как  $i \notin \text{supp}(\mathbf{x})$ , из леммы 1 в [15] следует, что  $d(\mathbf{u}, \mathbf{v}) \geq 3$  для любых  $\mathbf{u} \in (\mathcal{R}_i + (\mathbf{0}|\mathbf{c}_1))^i$  и  $\mathbf{v} \in (\mathcal{R}_i + (\mathbf{0}|\mathbf{c}_2))^i$ . Поскольку  $\mathcal{R}_i + (\mathbf{0}|\mathbf{c})$  является  $i$ -компонентой кода  $\mathcal{C}$  для всех  $\mathbf{c} \in \mathcal{C}_1$ , множество всех  $i$ -компонент  $\mathcal{R}_i + (\mathbf{0}|\mathbf{c})$  образует разбиение кода  $\mathcal{C}$  и (1) принимает вид (3). Размерность  $\mathcal{R}_i$  равна  $q^m - 1$ . Таким образом,

$$|\mathcal{C}| = |\mathcal{R}_i| \cdot |\mathcal{C}_1| = q^{q^m-1} \cdot q^{n-m} = q^{qn-m}.$$

Следовательно, число слов в  $\mathcal{C}$  корректно. Таким образом, в силу теоремы 1 множество  $\mathcal{C}$  является  $q$ -ичным 1-совершенным кодом длины  $qn + 1$ . Теорема 3 доказана.

Обозначим через  $N(q, n)$  число  $q$ -ичных 1-совершенных кодов длины  $n = (q^m - 1)/(q - 1)$ . Тогда из конструкции Линдстрёма [10] и Шёнхейма [16] следует, что

$$N(q, n) \geq (q)^{q^{\frac{n-1}{q}-m+1}}.$$



Из (3) и определения главной  $i$ -компоненты  $q$ -ичного кода Хэмминга вытекает, что посредством перестановки элементов в  $\mathbb{F}_q$  получаем различные 1-совершенные коды. Таким образом,

$$N(q, n) \geq (q!)^{q^{\frac{n-1}{q}-m+1}}.$$

Заметим, что приведённые выше нижние оценки для числа  $q$ -ичных 1-совершенных кодов длины  $n$  не являются оценками для числа  $q$ -ичных 1-совершенных кодов длины  $n$ , которые получены методом свитчингов из  $q$ -ичного кода Хэмминга длины  $n$ . (Оценки числа  $q$ -ичных 1-совершенных кодов длины  $n$ , которые получены методом свитчингов из  $q$ -ичного кода Хэмминга длины  $n$ , представлены во многих работах (см., например, [9, 11]).)

### 3. Совершенные коды полного ранга

Этцион и Варди [7] предложили свитчинговую конструкцию двоичных 1-совершенных кодов полного ранга и оригинальный метод построения допустимого семейства  $i$ -компонент двоичного кода Хэмминга. Конструкция двоичных 1-совершенных кодов полного ранга основывалась на этом методе. В [5] метод Этциона и Варди обобщён для  $q$ -ичных кодов. В этом разделе представим обобщение (следуя [5]) конструкции Этциона и Варди двоичных 1-совершенных кодов полного ранга до 1-совершенных кодов полного ранга над конечными полями. Сначала обобщим свитчинговую конструкцию [7] для  $q$ -ичных кодов Хэмминга.

Семейство  $\{\mathcal{R}_{i_1} + \mathbf{u}_1, \mathcal{R}_{i_2} + \mathbf{u}_2, \dots, \mathcal{R}_{i_t} + \mathbf{u}_t\}$   $i$ -компонент, где  $i \in \{i_1, i_2, \dots, i_t\}$ ,  $q$ -ичного кода Хэмминга  $\mathcal{H}_{q,m}$  называется *допустимым*, если

$$(\mathcal{R}_{i_r} + \mathbf{u}_r) \cap (\mathcal{R}_{i_s} + \mathbf{u}_s) = \emptyset$$

для любых  $r, s \in \{1, 2, \dots, t\}$ ,  $r \neq s$ .

Докажем теорему о допустимом семействе  $i$ -компонент кода Хэмминга  $\mathcal{H}_{q,m}$  (см. также [11]).

**Теорема 4.** Пусть  $\{\mathcal{R}_{i_1} + \mathbf{u}_1, \mathcal{R}_{i_2} + \mathbf{u}_2, \dots, \mathcal{R}_{i_t} + \mathbf{u}_t\}$  является допустимым семейством  $i$ -компонент  $q$ -ичного кода Хэмминга  $\mathcal{H}_{q,m}$  длины  $n = (q^m - 1)/(q - 1)$ ,  $i \in \{i_1, i_2, \dots, i_t\}$ , и  $\sigma_1, \sigma_2, \dots, \sigma_t$  —  $t$  перестановок элементов поля  $\mathbb{F}_q$ . Тогда множество

$$\mathcal{C} = \left( \mathcal{H}_{q,m} \setminus \bigcup_{s=1}^t \mathcal{R}_{i_s} + \mathbf{u}_s \right) \cup \left( \bigcup_{s=1}^t \sigma_s(\mathcal{R}_{i_s} + \mathbf{u}_s) \right). \quad (4)$$

является  $q$ -ичным 1-совершенным кодом длины  $n = (q^m - 1)/(q - 1)$ .

ДОКАЗАТЕЛЬСТВО. Необходимо показать, что число кодовых слов в  $\mathcal{C}$  корректно и минимальное расстояние  $d(\mathcal{C})$  кода  $\mathcal{C}$  равно 3. Так как  $|\mathcal{R}_{i_s}| = |\sigma_s(\mathcal{R}_{i_s})|$  и семейство  $\{\mathcal{R}_{i_1} + \mathbf{u}_1, \mathcal{R}_{i_2} + \mathbf{u}_2, \dots, \mathcal{R}_{i_t} + \mathbf{u}_t\}$   $i$ -компонент допустимо, из (4) следует, что

$$|\mathcal{C}| = |\mathcal{C}_1| - \sum_{s=1}^t |\mathcal{R}_{i_s}| + \sum_{s=1}^t |\sigma_s(\mathcal{R}_{i_s})| = |\mathcal{C}_1| = q^{n-m}.$$

Перестановка  $\sigma_s$  определяет изометрическое преобразование пространства  $\mathbb{F}_q^n$ . Таким образом,  $d(\sigma_s(\mathcal{R}_{i_s})) = 3$ ,  $s \in \{1, 2, \dots, t\}$ .

Рассмотрим некоторые  $i$ -компоненту  $\mathcal{R}_i + \mathbf{u}$  и  $j$ -компоненту  $\mathcal{R}_j + \mathbf{v}$  из  $\{\mathcal{R}_{i_1} + \mathbf{u}_1, \mathcal{R}_{i_2} + \mathbf{u}_2, \dots, \mathcal{R}_{i_t} + \mathbf{u}_t\}$ . Допустим, что  $i \neq j$ . Если  $i = j$ , то см. теорему 1. Без ограничения общности предполагаем, что  $i \notin \text{supp}(\mathbf{x})$  и  $j \notin \text{supp}(\mathbf{x})$ , где  $\text{supp}(\mathbf{x})$  является  $(m-2)$ -мерной гиперплоскостью,  $\mathbf{x} \in \mathbb{F}_q^n$ . Из условия теоремы следует, что  $(\mathcal{R}_i + \mathbf{u}) \cap (\mathcal{R}_j + \mathbf{v}) = \emptyset$ .

Рассмотрим выколотые коды  $(\mathcal{R}_i + \mathbf{u})^i$  и  $(\mathcal{R}_j + \mathbf{v})^j$ . Так как  $i \notin \text{supp}(\mathbf{x})$  и  $j \notin \text{supp}(\mathbf{x})$ , из леммы 1 в [15] вытекает, что  $d(\mathbf{c}, \mathbf{c}') \geq 3$  для любых  $\mathbf{c} \in (\mathcal{R}_i + \mathbf{u})^i$  и  $\mathbf{c}' \in (\mathcal{R}_j + \mathbf{v})^j$ . Следовательно,  $d(\mathcal{C}) = 3$ . Теорема 4 доказана.

Построим векторы  $\mathbf{c}_1, \mathbf{c}_1, \dots, \mathbf{c}_m$  и покажем, что они являются кодовыми словами кода Хэмминга  $\mathcal{H}_{q,m}$  длины  $n = (q^m - 1)/(q - 1)$ .

В проверочной матрице  $H = [\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_m]$  кода Хэмминга  $\mathcal{H}_{q,m}$  выберем  $m$  линейно независимых столбцов. Без ограничения общности будем считать, что выбрали столбцы  $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_m$ .

Для каждого вектора  $\mathbf{z} \in \mathbb{F}_q^m \setminus \{\mathbf{0}\}$  существуют единственные скаляр  $\alpha \in \mathbb{F}_q \setminus \{0\}$  и вектор-столбец  $\mathbf{h}_i \in H$  такие, что  $\mathbf{z} = \alpha \mathbf{h}_i^T$ . Определим отображение  $\xi$  множества ненулевых векторов из  $\mathbb{F}_q^m$  на множество векторов веса 1 из  $\mathbb{F}_q^n$  следующим образом:

$$\mathbf{z} \in \mathbb{F}_q^m \setminus \{\mathbf{0}\}, \quad \xi(\mathbf{z}) = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n,$$

$$\text{где } x_i = \begin{cases} \alpha, & \text{если } \mathbf{z} = \alpha \mathbf{h}_i^T, \\ 0, & \text{если } \mathbf{z} \neq \alpha \mathbf{h}_i^T. \end{cases}$$

Для простоты будем использовать обозначение  $\xi(\mathbf{h}_i)$  вместо  $\xi(\mathbf{h}_i^T)$ . Следуя [7], определим векторы

$$\mathbf{c}_1 = \xi(\mathbf{h}_1) + \xi(\mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_3) - \xi(\mathbf{h}_1 + \mathbf{h}_2 - \mathbf{h}_4) - \xi(\mathbf{h}_1 + \mathbf{h}_3 + \mathbf{h}_4),$$

$$\mathbf{c}_2 = \xi(\mathbf{h}_1) + \xi(\mathbf{h}_2) - \xi(\mathbf{h}_1 - \mathbf{h}_3 - \mathbf{h}_4) - \xi(\mathbf{h}_2 + \mathbf{h}_3 + \mathbf{h}_4),$$

$$\begin{aligned} \mathbf{c}_4 = & \xi(\mathbf{h}_1) - \xi(\mathbf{h}_2) - \xi(\mathbf{h}_3) + \xi(\mathbf{h}_4) + \xi(\mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_3) - \xi(\mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_4) \\ & - \xi(\mathbf{h}_1 + \mathbf{h}_3 + \mathbf{h}_4) + \xi(\mathbf{h}_2 + \mathbf{h}_3 + \mathbf{h}_4). \end{aligned}$$

Пусть  $j \in \{1, 2, \dots, m\} \setminus \{1, 2, 4\}$ . Если  $j$  нечётно, то положим

$$\mathbf{c}_j = \sum_{i=1}^j \xi(\mathbf{h}_i) - \xi(\mathbf{h}_1 + \mathbf{h}_2 + \dots + \mathbf{h}_j),$$

иначе

$$\mathbf{c}_j = \sum_{i=1}^j \xi(\mathbf{h}_i) - \xi(\mathbf{h}_1 + \mathbf{h}_2 + \dots + \mathbf{h}_{j/2}) - \xi(\mathbf{h}_{j/2+1} + \mathbf{h}_{j/2+2} + \dots + \mathbf{h}_j).$$

**Лемма 1.** Если  $m \geq 4$ , то  $\mathbf{c}_i \in \mathcal{H}_{q,m}$ ,  $i = 1, 2, \dots, m$ .

**ДОКАЗАТЕЛЬСТВО.** Поскольку столбцы  $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_m$  линейно независимы, из конструкции векторов  $\mathbf{c}_i$  следует, что  $\mathbf{c}_i \in \mathcal{H}_{q,m}$ ,  $i = 1, 2, \dots, m$ . Лемма 1 доказана.

Так как  $\mathbf{u} \in \mathcal{H}_{q,m}$ , из теоремы 2 вытекает, что  $\mathcal{R}_i + \mathbf{u}$  —  $i$ -компонента  $q$ -ичного кода Хэмминга  $\mathcal{H}_{q,m}$ . Следовательно, в силу леммы 1 очевидно, что

$$\mathcal{F} = \{\mathcal{R}_1 + \mathbf{c}_1, \mathcal{R}_2 + \mathbf{c}_2, \dots, \mathcal{R}_m + \mathbf{c}_m\}$$

является семейством  $i$ -компонент кода  $\mathcal{H}_{q,m}$ .

**Лемма 2.** Если  $m \geq 4$ , то  $\mathcal{F}$  является допустимым семейством  $i$ -компонент кода Хэмминга  $\mathcal{H}_{q,m}$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $r, s \in \{1, 2, \dots, m\}$ ,  $r \neq s$ . Покажем, что

$$(\mathcal{R}_r + \mathbf{c}_r) \cap (\mathcal{R}_s + \mathbf{c}_s) = \emptyset \quad (5)$$

для  $i$ -компонент  $\mathcal{R}_r + \mathbf{c}_r$  и  $\mathcal{R}_s + \mathbf{c}_s$  из семейства  $\mathcal{F}$ .

Для того чтобы выполнялось равенство (5), достаточно показать, что

$$\mathbf{c}_r - \mathbf{c}_s \notin \mathcal{R}_r + \mathcal{R}_s.$$

В силу теоремы 2 в [5] достаточно показать, что носитель вектора  $\mathbf{c}_r - \mathbf{c}_s$  содержит точку  $x$ , не лежащую на прямой  $l_{rs}$  и такую, что ни одна другая точка (отличная от точек  $r, s, x$ ) в  $\text{supp}(\mathbf{c}_r - \mathbf{c}_s)$  не принадлежит плоскости  $P_{rsx}$ . Рассмотрим несколько случаев.

**СЛУЧАЙ 1.** Пусть  $r = 1$ ,  $s = 2$ . Тогда

$$\text{supp}(\mathbf{c}_1 - \mathbf{c}_2) = \{2\} \cup \text{supp}(\xi(\mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_3)) \cup \text{supp}(\xi(\mathbf{h}_1 + \mathbf{h}_2 - \mathbf{h}_4))$$

$$\cup \text{supp}(\xi(\mathbf{h}_1 + \mathbf{h}_3 + \mathbf{h}_4)) \cup \text{supp}(\xi(\mathbf{h}_1 - \mathbf{h}_3 - \mathbf{h}_4)) \cup \text{supp}(\xi(\mathbf{h}_2 + \mathbf{h}_3 + \mathbf{h}_4)).$$

Допустим, что  $x = \text{supp}(\xi(\mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_3))$ . Поскольку столбцы  $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_m$  линейно независимы, имеем  $\text{supp}(\mathbf{h}_1 + \mathbf{h}_2 - \mathbf{h}_4) \notin P_{12x}$ ,  $\text{supp}(\mathbf{h}_1 + \mathbf{h}_3 + \mathbf{h}_4) \notin P_{12x}$ ,  $\text{supp}(\mathbf{h}_1 - \mathbf{h}_3 - \mathbf{h}_4) \notin P_{12x}$  и  $\text{supp}(\mathbf{h}_2 + \mathbf{h}_3 + \mathbf{h}_4) \notin P_{12x}$ .

Случай, когда  $r = 1$  или  $r = 2$  и  $s = 3$  или  $s = 4$ , доказывается аналогично.

СЛУЧАЙ 2. Пусть  $r, s \in \{1, 2, \dots, m\} \setminus \{1, 2, 4\}$ ,  $r \neq s$  и числа  $r, s$  нечётны. Без ограничения общности можем считать, что  $r < s$ . Тогда

$$\begin{aligned} \text{supp}(\mathbf{c}_r - \mathbf{c}_s) &= \{r+1, r+2, \dots, s\} \\ &\cup \text{supp}\left(\xi\left(\sum_{i=1}^r \mathbf{h}_i\right)\right) \cup \text{supp}\left(\xi\left(\sum_{i=1}^s \mathbf{h}_i\right)\right). \end{aligned}$$

Пусть  $x = r+1$ . Тогда  $y \notin P_{rsr+1}$  для любых  $y \in \text{supp}(\mathbf{c}_r - \mathbf{c}_s) \setminus \{r, s, r+1\}$ .

СЛУЧАЙ 3. Пусть  $r, s \in \{1, 2, \dots, m\} \setminus \{1, 2, 4\}$ ,  $r \neq s$  и числа  $r, s$  чётны. Без ограничения общности предполагаем, что  $r < s$ . Тогда

$$\begin{aligned} \text{supp}(\mathbf{c}_r - \mathbf{c}_s) &= \{r+1, r+2, \dots, s\} \cup \text{supp}\left(\xi\left(\sum_{i=1}^{r/2} \mathbf{h}_i\right)\right) \\ &\cup \text{supp}\left(\xi\left(\sum_{i=r/2+1}^r \mathbf{h}_i\right)\right) \cup \text{supp}\left(\xi\left(\sum_{i=1}^{s/2} \mathbf{h}_i\right)\right) \cup \text{supp}\left(\xi\left(\sum_{i=s/2+1}^s \mathbf{h}_i\right)\right). \end{aligned}$$

Пусть  $x = \text{supp}\left(\xi\left(\sum_{i=1}^{r/2} \mathbf{h}_i\right)\right)$ . Тогда  $y \notin P_{rsx}$  для любых  $y \in \text{supp}(\mathbf{c}_r - \mathbf{c}_s) \setminus \{r, s, x\}$ .

СЛУЧАЙ 4. Пусть  $r, s \in \{1, 2, \dots, m\} \setminus \{1, 2, 4\}$ ,  $r \neq s$ , число  $r$  чётно, а число  $s$  нечётно. Допустим, что  $r < s$ . Тогда

$$\begin{aligned} \text{supp}(\mathbf{c}_r - \mathbf{c}_s) &= \{r+1, r+2, \dots, s\} \cup \text{supp}\left(\xi\left(\sum_{i=1}^{r/2} \mathbf{h}_i\right)\right) \\ &\cup \text{supp}\left(\xi\left(\sum_{i=r/2+1}^r \mathbf{h}_i\right)\right) \cup \text{supp}\left(\xi\left(\sum_{i=1}^s \mathbf{h}_i\right)\right). \end{aligned}$$

Пусть  $x = \text{supp}\left(\xi\left(\sum_{i=1}^{r/2} \mathbf{h}_i\right)\right)$ . Тогда  $y$  не принадлежит  $P_{rsx}$  для любых  $y \in \text{supp}(\mathbf{c}_r - \mathbf{c}_s) \setminus \{r, s, x\}$ . Случай, когда  $r > s$ , доказывается аналогично.

СЛУЧАЙ 5. Пусть  $r = 1$ ,  $s \in \{1, 2, \dots, m\} \setminus \{1, 2, 3, 4\}$  и число  $s$  нечётно. Тогда

$$\begin{aligned} \text{supp}(\mathbf{c}_r - \mathbf{c}_s) &= \{2, 3, \dots, s\} \cup \text{supp}(\xi(\mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_3)) \\ &\cup \text{supp}(\xi(\mathbf{h}_1 + \mathbf{h}_2 - \mathbf{h}_4)) \cup \text{supp}(\xi(\mathbf{h}_1 + \mathbf{h}_3 + \mathbf{h}_4)) \cup \text{supp}\left(\xi\left(\sum_{i=1}^s \mathbf{h}_i\right)\right). \end{aligned}$$

Пусть  $x = s - 1$ . Тогда  $y \notin P_{rsx}$  для любых  $y \in \text{supp}(\mathbf{c}_r - \mathbf{c}_s) \setminus \{r, s, x\}$ .

Случай, когда  $r = 2, 4$ ,  $s \in \{1, 2, \dots, m\} \setminus \{1, 2, 3, 4\}$  и число  $s$  нечётно, доказываются аналогично.

СЛУЧАЙ 6. Пусть  $r = 1$ ,  $s \in \{1, 2, \dots, m\} \setminus \{1, 2, 4\}$  и число  $s$  чётно. Тогда

$$\begin{aligned} \text{supp}(\mathbf{c}_r - \mathbf{c}_s) &= \{2, 3, \dots, s\} \cup \text{supp}(\xi(\mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_3)) \\ &\cup \text{supp}(\xi(\mathbf{h}_1 + \mathbf{h}_2 - \mathbf{h}_4)) \cup \text{supp}(\xi(\mathbf{h}_1 + \mathbf{h}_3 + \mathbf{h}_4)) \\ &\cup \text{supp}\left(\xi\left(\sum_{i=1}^{s/2} \mathbf{h}_i\right)\right) \cup \text{supp}\left(\xi\left(\sum_{i=s/2+1}^s \mathbf{h}_i\right)\right). \end{aligned}$$

Пусть  $x = s - 1$ . Тогда  $y \notin P_{rsx}$  для любых  $y \in \text{supp}(\mathbf{c}_r - \mathbf{c}_s) \setminus \{r, s, x\}$ .

Случай, когда  $r = 2, 4$ ,  $s \in \{1, 2, \dots, m\} \setminus \{1, 2, 4\}$  и число  $s$  чётно, доказываются аналогично. Лемма 2 доказана.

**Теорема 5.** Пусть  $\mathbb{F}_q$  — конечное поле,  $\mathcal{F} = \{\mathcal{R}_1 + \mathbf{c}_1, \mathcal{R}_2 + \mathbf{c}_2, \dots, \mathcal{R}_m + \mathbf{c}_m\}$  — семейство  $i$ -компонент,  $m \geq 4$  и  $\sigma_1, \sigma_2, \dots, \sigma_m$  — перестановки элементов поля  $\mathbb{F}_q$ ,  $\sigma_i(1) \neq 1$  для всех  $1 \leq i \leq m$ . Тогда

$$\mathcal{C} = \left( \mathcal{H}_{q,m} \setminus \bigcup_{i=1}^m \mathcal{R}_i + \mathbf{c}_i \right) \cup \left( \bigcup_{i=1}^m \sigma_i(\mathcal{R}_i + \mathbf{c}_i) \right)$$

является 1-совершенным кодом полного ранга.

**ДОКАЗАТЕЛЬСТВО.** В силу леммы 2  $\mathcal{F}$  является допустимым семейством  $i$ -компонент кода Хэмминга  $\mathcal{H}_{q,m}$ . Следовательно, ввиду теоремы 4 множество  $\mathcal{C}$  —  $q$ -ичный 1-совершенный код длины  $n = (q^m - 1)/(q - 1)$ . Из определения кода Хэмминга  $\mathcal{H}_{q,m}$  следует, что  $\text{rank}(\mathcal{H}_{q,m}) = n - m$ . Размерность подпространства  $\mathcal{R}_i$  равна  $q^{m-1} - 1$ . Учитывая, что

$$\left| \mathcal{H}_{q,m} \setminus \bigcup_{i=1}^m \mathcal{R}_i + \mathbf{c}_i \right| = q^{n-m} - mq^{m-1-1} > \frac{1}{q}q^{n-m} = \frac{1}{q}|\mathcal{H}_{q,m}|,$$

имеем

$$\text{rank}\left(\mathcal{H}_{q,m} \setminus \bigcup_{i=1}^m \mathcal{R}_i + \mathbf{c}_i\right) = n - m.$$

Из конструкции векторов  $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_m$  следует, что векторы  $\mathbf{c}_1(1, \sigma_1), \mathbf{c}_2(2, \sigma_2), \dots, \mathbf{c}_m(m, \sigma_m)$  линейно независимы. По определению  $\mathbf{c}(i, \sigma) = (c_1, c_2, \dots, \sigma(c_i), \dots, c_n)$ . Так как  $\sigma_i(1) \neq 1$  для всех  $1 \leq i \leq m$ ,

$$\{\mathbf{c}_1(1, \sigma_1), \mathbf{c}_2(2, \sigma_2), \dots, \mathbf{c}_m(m, \sigma_m)\} \cap \mathcal{H}_{q,m} = \emptyset.$$

Однако  $\{\mathbf{c}_1(1, \sigma_1), \mathbf{c}_2(2, \sigma_2), \dots, \mathbf{c}_m(m, \sigma_m)\} \subset \mathcal{C}$ . Тем самым  $\text{rank}(\mathcal{C}) = n$ . Теорема 5 доказана.

## ЛИТЕРАТУРА

1. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Пробл. кибернетики. 1962. Вып. 8. С. 375–378.
2. **Романов А. М.** О построении совершенных нелинейных двоичных кодов инверсией символов // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 1. С. 46–52.
3. **Романов А. М.** О разбиениях  $q$ -ичных кодов Хэмминга на непересекающиеся компоненты // Дискрет. анализ и исслед. операций. Сер. 1. 2004. Т. 11, № 3. С. 80–87.
4. **Романов А. М.** Обзор методов построения нелинейных совершенных кодов // Дискрет. анализ и исслед. операций. Сер. 1. 2006. Т. 13, № 4. С. 60–88.
5. **Романов А. М.** О допустимых семействах компонент кодов Хэмминга // Дискрет. анализ и исслед. операций. 2012. Т. 19, № 2. С. 84–91.
6. **Avgustinovich S. V., Krotov D. S.** Embedding in a perfect code // J. Comb. Des. 2009. Vol. 17, No. 5. P. 419–423.
7. **Etzion T., Vardy A.** Perfect binary codes: Constructions, properties, and enumeration // IEEE Trans. Inf. Theory. 1994. Vol. 40, No. 3. P. 754–763.
8. **Etzion T.** Nonequivalent  $q$ -ary perfect codes // SIAM J. Discrete Mat. 1996. Vol. 9, No. 3. P. 413–423.
9. **Krotov D., Heden O.** On the structure of non-full-rank perfect  $q$ -ary codes // Adv. Math. Comb. 2011. Vol. 5, No. 2. P. 149–156.
10. **Lindström B.** On group and nongroup perfect codes in  $q$  symbols // Math. Scand. 1969. Vol. 25. P. 149–158.
11. **Los' A. V.** Construction of perfect  $q$ -ary codes // Proc. 9th Int. Workshop “Algebraic and Combinatorial Coding Theory” (Kranevo, Bulgaria, June 19–25, 2004). Sofia: Acad., 2004. P. 272–276.
12. **Östergård P. R. J., Potttonen O., Phelps K. T.** The perfect binary one-error-correcting codes of length 15: Part II—Properties // IEEE Trans. Inform. Theory. 2010. Vol. 56, No. 6. P. 2571–2582.

13. **Phelps K. T., Villanueva M.** Ranks of  $q$ -ary 1-perfect codes // Des. Codes Cryptogr. 2002. Vol. 27, No. 1–2. P. 139–144.
14. **Phelps K. T., Rifa J., Villanueva M.** Kernels and  $p$ -kernels of  $p^r$ -ary 1-perfect codes // Des. Codes Cryptogr. 2005. Vol. 37, No. 2. P. 243–261.
15. **Romanov A. M.** Hamiltonicity of minimum distance graphs of 1-perfect codes // Electron. J. Comb. 2012. Vol. 19, No. 1. P65.
16. **Schönheim J.** On linear and nonlinear single-error-correcting  $q$ -nary perfect codes // Inform. Control. 1968. Vol. 12. P. 23–26.

*Романов Александр Михайлович*

Статья поступила  
29 декабря 2015 г.

Исправленный вариант —  
17 марта 2016 г.

DISKRETNYYI ANALIZ I ISSLEDOVANIE OPERATSII  
July–August 2016. Volume 23, No. 3. P. 107–123

UDC 519.8

DOI: 10.17377/daio.2016.23.522

## ON FULL-RANK PERFECT CODES OVER FINITE FIELDS

A. M. Romanov<sup>1</sup>

<sup>1</sup>Sobolev Institute of Mathematics,  
4 Koptug Ave., 630090 Novosibirsk, Russia  
e-mail: rom@math.nsc.ru

**Abstract.** We propose a construction of full-rank  $q$ -ary 1-perfect codes over finite fields. This is a generalization of the construction of full-rank binary 1-perfect codes by Etzion and Vardy (1994). The properties of the  $i$ -components of  $q$ -ary Hamming codes are investigated and the construction of full-rank  $q$ -ary 1-perfect codes is based on these properties. The switching construction of 1-perfect codes is generalized for the  $q$ -ary case. We propose a generalization of the notion of  $i$ -component of a 1-perfect code and introduce the concept of an  $(i, \sigma)$ -component of  $q$ -ary 1-perfect codes. We also present a generalization of the Lindström–Schönheim construction of  $q$ -ary 1-perfect codes and provide a lower bound for the number of pairwise distinct  $q$ -ary 1-perfect codes of length  $n$ . Bibliogr. 16.

**Keywords:** Hamming code, nonlinear perfect code, full-rank code,  $i$ -component.

## REFERENCES

1. Yu. L. Vasil'ev, On nongroup close-packed codes, in A. A. Lyapunov, ed., *Problemy kibernetiki* (Problems of Cybernetics), Vol. 8, pp. 375–378, Fizmatgiz, Moscow, 1962.
2. A. M. Romanov, On construction of nonlinear perfect binary codes by inversion of symbols, *Diskretn. Anal. Issled. Oper., Ser. 1*, **4**, No. 1, 46–52, 1997.
3. A. M. Romanov, On partitions of  $q$ -ary Hamming codes into disjoint components, *Diskretn. Anal. Issled. Oper., Ser. 1*, **11**, No. 3, 80–87, 2004.
4. A. M. Romanov, A survey of methods for constructing nonlinear perfect binary codes, *Diskretn. Anal. Issled. Oper., Ser. 1*, **13**, No. 4, 60–88, 2006. Translated in *J. Appl. Ind. Math.*, **2**, No. 2, 252–269, 2008.
5. A. M. Romanov, On admissible families of components of Hamming codes, *Diskretn. Anal. Issled. Oper., Ser. 1*, **19**, No. 2, 84–91, 2012. Translated in *J. Appl. Ind. Math.*, **6**, No. 3, 355–359, 2012.



6. **S. V. Avgustinovich** and **D. S. Krotov**, Embedding in a perfect code, *J. Comb. Des.*, **17**, No. 5, 419–423, 2009.
7. **T. Etzion** and **A. Vardy**, Perfect binary codes: Constructions, properties, and enumeration, *IEEE Trans. Inf. Theory.*, **40**, No. 3, 754–763, 1994.
8. **T. Etzion**, Nonequivalent  $q$ -ary perfect codes, *SIAM J. Discrete Math.*, **9**, No. 3, 413–423, 1996.
9. **O. Heden** and **D. S. Krotov**, On the structure of non-full-rank perfect  $q$ -ary codes, *Adv. Math. Comb.*, **5**, No. 2, 149–156, 2011.
10. **B. Lindström**, On group and nongroup perfect codes in  $q$  symbols, *Math. Scand.*, **25**, 149–158, 1969.
11. **A. V. Los'**, Construction of perfect  $q$ -ary codes, in *Proc. 9th Int. Workshop Algebraic Comb. Coding Theory, Kranevo, Bulgaria, June 19–25, 2004*, pp. 272–276, Inst. Math. Inform., Sofia, 2004.
12. **P. R. J. Östergård**, **O. Pottonen**, and **K. T. Phelps**, The perfect binary one-error-correcting codes of length 15: Part II — Properties, *IEEE Trans. Inform. Theory*, **56**, No. 6, 2571–2582, 2010.
13. **K. T. Phelps** and **M. Villanueva**, Ranks of  $q$ -ary 1-perfect codes, *Des. Codes Cryptogr.*, **27**, No. 1B<sup>2</sup>, 139–144, 2002.
14. **K. T. Phelps**, **J. Rifà**, and **M. Villanueva**, Kernels and  $p$ -kernels of  $p^r$ -ary 1-perfect codes, *Des. Codes Cryptogr.*, **37**, No. 2, 243–261, 2005.
15. **A. M. Romanov**, Hamiltonicity of minimum distance graphs of 1-perfect codes, *Electron. J. Comb.*, **19**, No. 1, P65, 1–6, 2012.
16. **J. Schönheim**, On linear and nonlinear single-error-correcting  $q$ -nary perfect codes, *Inform. Control*, **12**, 23–26, 1968.

Alexander M. Romanov

Received  
29 December 2015  
Revised  
17 March 2016