Math-Net.Ru

All Russian mathematical portal

S. A. Malyugin, Systematic and nonsystematic perfect codes of infinite length over finite fields, *Sib. Elektron. Mat. Izv.*, 2019, Volume 16, 1732–1751

DOI: <https://doi.org/10.33048/semi.2019.16.122>

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use

<http://www.mathnet.ru/eng/agreement>

Download details:

IP: 52.6.47.48

April 26, 2023, 04:12:29

СИБИРСКИЕ ЭЛЕКТРОННЫЕ МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports

<http://semr.math.nsc.ru>

Том 16, стр. 1732–1751 (2019)

УДК 519.72

DOI 10.33048/semi.2019.16.122

MSC 94B60

СИСТЕМАТИЧЕСКИЕ И НЕСИСТЕМАТИЧЕСКИЕ СОВЕРШЕННЫЕ КОДЫ БЕСКОНЕЧНОЙ ДЛИНЫ НАД КОНЕЧНЫМИ ПОЛЯМИ

С.А. МАЛЮГИН

ABSTRACT. Let F_q be a finite field of q elements ($q = p^k$, p is a prime number). An infinite-dimensional q -ary vector space $F_q^{\mathbb{N}_0}$ consists of all sequences $u = (u_1, u_2, \dots)$, where $u_i \in F_q$ and all u_i are 0 except some finite set of indices $i \in \mathbb{N}$. A subset $C \subset F_q^{\mathbb{N}_0}$ is called a perfect q -ary code with distance 3 if all balls of radius 1 (in the Hamming metric) with centers in C are pairwise disjoint and their union covers the space. Define the infinite perfect q -ary Hamming code H_q^∞ as the infinite union of the sequence of finite q -ary codes $\tilde{H}_q^n$ where for all $n = (q^m - 1)/(q - 1)$, $\tilde{H}_q^n$ is a subcode of $\tilde{H}_q^{q^n + 1}$. We prove that all linear perfect q -ary codes of infinite length are affine equivalent. A perfect q -ary code $C \subset F_q^{\mathbb{N}_0}$ is called systematic if $\mathbb{N}$ could be split into two subsets N_1, N_2 such that C is a graphic of some function $f : F_q^{N_{1,0}} \rightarrow F_q^{N_{2,0}}$. Otherwise, C is called nonsystematic. Further general properties of systematic codes are proved. We also prove a version of Shapiro–Slotnik theorem for codes of infinite length. Then, we construct nonsystematic codes of infinite length using the switchings of $s < q - 1$ disjoint components. We say that a perfect code C has the complete system of triples if for any three indices i_1, i_2, i_3 the set $C - C$ contains the vector with support $\{i_1, i_2, i_3\}$. We construct perfect codes of infinite length having the complete system of triples (in particular, such codes are nonsystematic). These codes can be obtained from the Hamming code H_q^∞ by switching some family of disjoint components $\mathcal{B} = \{R_1^{u_1}, R_2^{u_2}, \dots\}$. Unlike the codes of finite

MALYUGIN, S.A., SYSTEMATIC AND NONSYSTEMATIC PERFECT CODES OF INFINITE LENGTH OVER FINITE FIELDS.

© 2019 Малугин С.А.

The work was supported by the program of fundamental scientific researches of the SB RAS № I.5.1, project № 0314-2019-0017.

Поступила 19 июля 2019 г., опубликована 28 ноября 2019 г.

length, the family $\mathcal{B}$ must obey the rigid condition of sparsity. It is shown particularly that if the family of components $\mathcal{B}$ does not satisfy the condition of sparsity then it can generate a perfect code having non-complete system of triples.

Keywords: perfect q -ary code, code of infinite length, component, systematic code, nonsystematic code, complete system of triples, condition of sparsity

1. ВВЕДЕНИЕ

Пусть F_q — конечное поле Галуа из q элементов ($q = p^k$, p — простое число). Через $F_q^{\mathbb{N}_0}$ будем обозначать множество, элементами которого являются всевозможные бесконечные последовательности $u = (u_1, u_2, \dots)$, где $u_i \in F_q$ и все $u_i = 0$ кроме конечного множества индексов $i \in \mathbb{N}$ (индекс 0 после символа $\mathbb{N}$ означает, что мы рассматриваем только векторы из $F_q^{\mathbb{N}}$, имеющие финитные носители). Относительно покоординатных операций сложения и умножения на элементы из F_q множество $F_q^{\mathbb{N}_0}$ является бесконечномерным векторным пространством над полем F_q . Стандартный базис этого пространства образуют векторы с единичной i -й координатой ($e_i = (0, \dots, 0, \underset{i}{1}, 0, \dots)$). Множество индексов i , для которых $u_i \neq 0$, называется *носителем* вектора $u \in F_q^{\mathbb{N}_0}$ и обозначается через $[u]$. Число ненулевых координат вектора u называется его *весом* и обозначается символом $|u|$. Расстояние Хэмминга между векторами $u, v \in F_q^{\mathbb{N}_0}$ определяется как $|u - v|$.

Определение 1. Подмножество C в $F_q^{\mathbb{N}_0}$ называется совершенным q -значным кодом с расстоянием 3, если все шары радиуса 1 (в метрике Хэмминга) с центрами из C попарно не пересекаются и их объединение покрывает пространство $F_q^{\mathbb{N}_0}$.

Совершенный код называется *линейным*, если он является линейным подпространством в $F_q^{\mathbb{N}_0}$.

Для любого совершенного кода $C \subset F_q^{\mathbb{N}_0}$ обозначим через $ST_3(C)$ множество всех векторов из C , имеющих вес 3.

Лемма 1. Любой линейный совершенный код $C \subset F_q^{\mathbb{N}_0}$ является линейной оболочкой множества $ST_3(C)$.

Доказательство. Любой ненулевой вектор $u \in C$ имеет конечный вес $n \geq 3$. Если $u = \sum u_i e_i$ и $u_{i_1} \neq 0$, $u_{i_2} \neq 0$, то вектор $v = u_{i_1} e_{i_1} + u_{i_2} e_{i_2}$ имеет вес 2 и он должен находиться на расстоянии Хэмминга 1 от некоторого кодового вектора $w_1 \in C$. Очевидно, вес $|w_1| = 3$ и поэтому $w_1 = u_1 e_{i_1} + u_2 e_{i_2} + v_3 e_{i_3}$ при некоторых $i_3 \in \mathbb{N}$, $i_3 \neq i_1, i_2$, $v_3 \in F_q$, $v_3 \neq 0$. Вектор $u_1 = u - w_1$ принадлежит коду C и его вес $|u_1| < |u| = n$. Продолжая этот процесс индуктивно, мы построим конечную последовательность векторов $u_1, \dots, u_m \in C$ такую, что $0 = |u_m| < \dots < |u_1| < |u|$, $|u_i - u_{i-1}| = 3$, $1 < i \leq m$, $\square$

Линейный код можно построить следующим образом. Рассмотрим в $F_q^{\mathbb{N}_0}$ максимальное множество, состоящее из всех ненулевых попарно неколлинеарных векторов. Например, в качестве такого множества можно взять все векторы вида

$$\vec{n} = \begin{pmatrix} i_1 \\ \vdots \\ i_k \\ 0 \\ \vdots \end{pmatrix},$$

полагая $i_k = 1$, $i_j = 0$ при $j > k = k(\vec{n})$. Обозначим это множество через N . Все векторы $\vec{n}$ этого вида пронумеруем в одну последовательность $\vec{n}_1, \vec{n}_2, \dots, \vec{n}_p, \dots$ так, чтобы номера координат $k(\vec{n}_p)$, для которых $i_{k(\vec{n}_p)} = 1$ и $i_j = 0$ при $j > k(\vec{n}_p)$ образовывали монотонно неубывающую последовательность. Рассмотрим *бесконечномерную проверочную матрицу*

$$D = \begin{pmatrix} 1 & 0 & i_1 & i_2 & \cdot & 0 & \cdot \\ 0 & 1 & 1 & 1 & \cdot & 0 & \cdot \\ 0 & 0 & 0 & 0 & 0 & 1 & \cdot \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}. \quad (1)$$

В дальнейшем k -й столбец проверочной матрицы (1) будем обозначать символом $\vec{k}$. Множество всех столбцов матрицы (1) обозначаем через N . Мы иногда будем даже отождествлять индексы $k \in \mathbb{N}$ с векторами $\vec{k} \in N$. Говорим, что вектор $u = (u_1, \dots, u_n, \dots) \in F_q^{\mathbb{N}_0}$ принадлежит линейному коду тогда и только тогда, когда

$$\sum_{k \in \mathbb{N}} u_k \vec{k} = 0 \quad (2)$$

(в этой бесконечной сумме только конечное число ненулевых слагаемых). Легко видеть, что так определенное множество векторов u является линейным совершенным кодом в $F_q^{\mathbb{N}_0}$. Этот код будем называть *q -значным кодом Хэмминга бесконечной длины* и обозначается символом H_q^∞ .

Код Хэмминга H_q^∞ можно определить и как объединение конечномерных q -значных кодов Хэмминга следующим образом. Для конечных n код Хэмминга H_q^n длины $n = (q^m - 1)/(q - 1)$ ($m > 1$) определяется стандартным образом (см. например [6]). Добавляя справа к векторам $u \in H_q^n$ бесконечное число нулевых координат, можно вложить код H_q^n в $F_q^{\mathbb{N}_0}$. Это вложение будем обозначать символом $\tilde{H}_q^n$. Тогда, так как $\tilde{H}_q^n \subset \tilde{H}_q^{q^{n+1}}$ ($n = (q^m - 1)/(q - 1)$), то можно положить $H_q^\infty = \bigcup_{m=2}^{\infty} \tilde{H}_q^{(q^m - 1)/(q - 1)}$.

Изучение кодов бесконечной длины с расстоянием 2 (МДР-кодов, задаваемых квазигруппами с бесконечным числом аргументов) предпринято В. Н. Потаповым в [10]. Им также была предложена задача об изучении совершенных кодов бесконечной длины. Совершенные двоичные коды бесконечной длины начали изучаться впервые в [7, 8]. Настоящая работа является продолжением двух предыдущих публикаций [6, 8]. В ней начинается изучение q -значных

кодов бесконечной длины. Основной целью этой работы является доказательство эквивалентности всех линейных кодов, изучение общих свойств систематических кодов, построение несистематических кодов свитчингами семи и более компонент, а также кодов с полной системой троек. В последнее время совершенные q -значные коды приобретают достаточно большой интерес, см. [2, 3, 4, 6, 12, 15].

2. ЭКВИВАЛЕНТНОСТЬ СОВЕРШЕННЫХ КОДОВ БЕСКОНЕЧНОЙ ДЛИНЫ

Множество ненулевых элементов поля F_q будем обозначать далее через F_q^* . Изометрией пространства $F_q^{\mathbb{N}_0}$ называем любое взаимно-однозначное отображение $A : F_q^{\mathbb{N}_0} \rightarrow F_q^{\mathbb{N}_0}$, сохраняющее расстояние Хэмминга. Изометрию A , являющуюся аффинным отображением пространства $F_q^{\mathbb{N}_0}$, называем *аффинной изометрией*.

Определение 2. Два совершенных q -значных кода C_1, C_2 в $F_q^{\mathbb{N}_0}$ называются (аффинно) эквивалентными, если существует (аффинная) изометрия A пространства $F_q^{\mathbb{N}_0}$ такая, что $A(C_1) = C_2$.

В данной работе мы будем далее рассматривать только понятие аффинной эквивалентности. Любое аффинное отображение $A : F_q^{\mathbb{N}_0} \rightarrow F_q^{\mathbb{N}_0}$ имеет вид $A(u) = \alpha(u) + a$ ($u \in F_q^{\mathbb{N}_0}$), где $a \in F_q^{\mathbb{N}_0}$, а α – линейный изоморфизм пространства $F_q^{\mathbb{N}_0}$, сохраняющий расстояние Хэмминга. Так как α сохраняет веса векторов, то для любого базисного вектора e_i будем иметь $\alpha(e_i) = \lambda_i e_{\pi(i)}$, где $\lambda_i \in F_q^*$, а $\pi : \mathbb{N} \rightarrow \mathbb{N}$ – перестановка на множестве натуральных чисел $\mathbb{N}$. Основным результатом этого параграфа является следующая

Лемма 2. Все линейные совершенные q -значные коды бесконечной длины аффинно эквивалентны.

Доказательство. Рассмотрим линейный совершенный код $C \subset F_q^{\mathbb{N}_0}$ и покажем, что он эквивалентен коду Хэмминга H_q^∞ . Обозначим через $\tilde{F}_q^n$ n -мерное подпространство всех векторов $u \in F_q^{\mathbb{N}_0}$ таких, что $u_i = 0$ для всех $i > n$. Мы будем индуктивно строить линейные отображения $\alpha_m : \tilde{F}_q^n \rightarrow F_q^{\mathbb{N}_0}$ ($n = (q^m - 1)/(q - 1)$) такие, что $\alpha_m(\tilde{H}_q^{(q^m - 1)/(q - 1)}) \subset C$ и отображение α_{m+1} является продолжением отображения α_m .

1) База индукции: $m = 2$, $n = q + 1$. Для любого $\lambda \in F_q^*$ существуют единственный элемент $\mu(\lambda)$ и номер $2 < i(\lambda) \leq q + 1$ такие, что вектор $u(\lambda) = e_1 + \lambda e_2 + \mu(\lambda) e_{i(\lambda)} \in H_q^\infty$. Если $\lambda_1 \neq \lambda_2$, то $i(\lambda_1) \neq i(\lambda_2)$ (иначе мы получим, что $|u(\lambda_1) - u(\lambda_2)| < 3$). Заметим, что векторы $u(\lambda)$ ($\lambda \in F_q^*$) линейно независимы и порождают весь код $\tilde{H}_q^{q+1}$. Это следует из того, что размерность кода $\tilde{H}_q^{q+1}$ равна $q - 1$.

Теперь начнём строить линейное отображение $\alpha_2 : \tilde{F}_q^{q+1} \rightarrow F_q^{\mathbb{N}_0}$. Полагаем $\pi_2(1) = 1$, $\pi_2(2) = 2$. Для любого $\lambda \in F_q^*$ в совершенном коде C существует единственный элемент $\nu(\lambda)$ и номер $2 < j(\lambda) \leq q + 1$ такие, что вектор $v(\lambda) = e_1 + \lambda e_2 + \nu(\lambda) e_{j(\lambda)}$ принадлежит коду C . Полагаем $\pi_2(i(\lambda)) = j(\lambda)$. Если λ пробегает множество F_q^* , то $i(\lambda)$ пробегает отрезок натуральных чисел $\{3, \dots, q + 1\}$. Поэтому отображение π_2 переводит отрезок натуральных чисел $I_2 = \{1, \dots, q + 1\}$ в множество $J_2 = \{1, 2\} \cup \{j(\lambda) : \lambda \in F_q^*\}$. Также как и выше, из $\lambda_1 \neq \lambda_2$ следует

$j(\lambda_1) \neq j(\lambda_2)$. Поэтому отображение π_2 является взаимно-однозначным, а множество векторов $\{v(\lambda) : \lambda \in F_q^*\}$ линейно независимым. Определим линейное отображение $\alpha_2 : \tilde{F}_q^{q+1} \rightarrow F_q^{\mathbb{N}_0}$ следующим образом. $\alpha_2(e_1) = e_1$, $\alpha_2(e_2) = e_2$, $\alpha_2(e_{i(\lambda)}) = (\nu(\lambda)/\mu(\lambda))e_{j(\lambda)}$ ($\lambda \in F_q^*$), $\alpha_2(e_i) = 0$ ($i > q+1$). Непосредственно проверяется, что $\alpha_2(u(\lambda)) = v(\lambda)$. Это значит, что $\alpha_2(\tilde{H}_q^{q+1}) \subset C$ и множество векторов $\{v(\lambda) : \lambda \in F_q^*\}$ является базисом в подкоде $\alpha_2(\tilde{H}_q^{q+1})$, который эквивалентен конечному q -значному коду длины $q+1$, определённого на множестве индексов J_2 . В частности, если $v \in C$ и носитель $[v] \subset J_2$, то $v \in \alpha_2(\tilde{H}_q^{q+1})$.

2) Индукционный шаг. Допустим, что для некоторого $m \geq 2$ построены линейное инъективное отображение $\alpha_m : \tilde{F}_q^n \rightarrow F_q^{\mathbb{N}_0}$ ($n = (q^m - 1)/(q - 1)$) и взаимно-однозначное отображение $\pi_m : \{1, \dots, n\} \rightarrow J_m \subset \mathbb{N}$ такие, что $\alpha_m(\tilde{H}_q^n) = \{v : v \in C, [v] \subset J_m\}$. Рассмотрим наименьший номер $j_{n+1} \in \mathbb{N} \setminus J_m$ и положим $\pi_{m+1}(n+1) = j_{n+1}$, $\pi_{m+1}(i) = \pi_m(i)$ ($1 \leq i \leq n$). Для любого фиксированного ($1 \leq k \leq n$) и любого $\lambda \in F_q^*$ существует единственный вектор $u_k(\lambda) \in H_q^\infty$, находящийся на расстоянии 1 от вектора $e_k + \lambda e_{n+1}$. Пусть $u_k(\lambda) = e_k + \lambda e_{n+1} + \mu_k(\lambda)e_{i_k(\lambda)}$ при некоторых $i_k(\lambda) \neq k$, $i_k(\lambda) \neq n+1$, $\mu_k(\lambda) \in F_q^*$. Как было доказано в 1), из $\lambda_1 \neq \lambda_2$ следует $i_k(\lambda_1) \neq i_k(\lambda_2)$. Предположение $i_k(\lambda) \leq n$ ведёт к противоречию, так как тогда вектор $e_k + \mu_k(\lambda)e_{i_k(\lambda)}$ будет находиться на расстоянии 1 от кодового вектора $u_k(\lambda) \in H_q^\infty$ и от ещё одного кодового вектора $w \in \tilde{H}_q^n \subset H_q^\infty$. Предположим, что при некоторых $k_1 \neq k_2$ имеем $i_{k_1}(\lambda_1) = i_{k_2}(\lambda_2)$. Тогда вектор $v = \lambda_1^{-1}u_{k_1}(\lambda_1) - \lambda_2^{-1}u_{k_2}(\lambda_2)$, имеющий вес 3, принадлежит коду H_q^∞ . Значит вектор $\lambda_1^{-1}e_{k_1} - \lambda_2^{-1}e_{k_2}$ будет находиться на расстоянии 1 от кодового вектора v и от ещё одного вектора w , принадлежащего коду $\tilde{H}_q^n$. Поэтому все номера $i_k(\lambda)$ различны при $k = 1, \dots, n$, $\lambda \in F_q^*$.

Аналогичным образом, $v_k(\lambda) = e_{\pi_m(k)} + \lambda e_{j_{n+1}} + \nu_k(\lambda)e_{j_k(\lambda)} \in C$ при некоторых $j_k(\lambda) \notin J_m \cup \{j_{n+1}\}$, $\nu_k(\lambda) \in F_q^*$. По тем же самым вышеприведённым причинам все номера $j_k(\lambda)$ различны. Далее определяем $\pi_{m+1}(i_k(\lambda)) = j_k(\lambda)$ ($1 \leq k \leq n$, $\lambda \in F_q^*$). В результате мы построили взаимно-однозначное отображение π_{m+1} множества номеров $\{1, \dots, qn+1\}$ на некоторое множество $J_{m+1} \supset J_m$, которое является продолжением отображения π_m .

Теперь продолжаем линейное отображение α_m , полагая на базисных векторах $\alpha_{m+1}(e_{n+1}) = e_{j_{n+1}}$, $\alpha_{m+1}(e_{i_k(\lambda)}) = (\nu_k(\lambda)/\mu_k(\lambda))e_{j_k(\lambda)}$, $\alpha_{m+1}(e_k) = \alpha_m(e_k)$ ($1 \leq k \leq n$, $\lambda \in F_q^*$). Из этого определения следует, что $\alpha_{m+1}(u_k(\lambda)) = v_k(\lambda)$. Пусть $\{u_1, \dots, u_{n-m}\}$ – базис в пространстве $\tilde{H}_q^n$, состоящий из векторов веса 3. Все векторы u_k , $u_k(\lambda)$ ($1 \leq k \leq n$, $\lambda \in F_q^*$) линейно независимы. Линейно независимы также все векторы $v_k = \alpha_m(u_k)$, $v_k(\lambda)$ ($1 \leq k \leq n$, $\lambda \in F_q^*$). Их количество равно $n - m + n(q - 1) = nq + 1 - (m + 1)$. Поэтому набор векторов веса 3 u_k , $u_k(\lambda)$ ($1 \leq k \leq n$, $\lambda \in F_q^*$) является базисом в следующем коде $\tilde{H}_q^{(q^{m+1}-1)/(q-1)}$, а набор векторов v_k , $v_k(\lambda)$ ($1 \leq k \leq n$, $\lambda \in F_q^*$) будет базисом в подкоде $\alpha_{m+1}(\tilde{H}_q^{(q^{m+1}-1)/(q-1)})$, который является совершенным q -значным кодом, определённым на множестве индексов $J_{m+1} \supset J_m$. В частности, отсюда следует, что если $v \in C$ и носитель $[v] \subset J_{m+1}$, то $v \in \alpha_{m+1}(\tilde{H}_q^{(q^{m+1}-1)/(q-1)})$.

3) Заключительный шаг. Применяя пункты 1) и 2), мы строим расширяющиеся множества индексов $J_2 \subset \dots \subset J_m \subset \dots$ и взаимно-однозначные отображения $\pi_m : \{1, \dots, n\} \rightarrow J_m$ ($n = (q^m - 1)/(q - 1)$), а также линейные инъективные отображения $\alpha_m : \tilde{F}_q^n \rightarrow F_q^{\mathbb{N}_0}$ такие, что $\alpha_m(\tilde{H}_q^n) = \{v : v \in C, [v] \subset J_m\}$, причём на каждом шаге отображение π_{m+1} является продолжением отображения π_m , а отображение α_{m+1} является продолжением отображения α_m . Теперь можно определить отображение α как объединение всех отображений α_m , а отображение $\pi : \mathbb{N} \rightarrow \mathbb{N}$, как объединение всех отображений π_m . Очевидно, $\alpha(\tilde{H}_q^\infty) \subseteq C$. Так как при доказательстве индукционного шага 2) мы выбрали наименьший номер $j_{m+1} \notin J_m$, то $\bigcup_{m=2}^{\infty} J_m = \mathbb{N}$. Поэтому $\alpha(\tilde{H}_q^\infty) = C$, а отображение π является перестановкой на множестве $\mathbb{N}$. $\square$

Замечание 1. Из определения проверочной матрицы (1), а также из доказательства леммы 2 следует, что множество индексов $\mathbb{N}$ можно наделять структурой бесконечномерного проективного пространства, которое можно обозначить символом $PG_q(\infty)$. А именно, если за основу взять линейный совершенный код C , то прямая, проходящая через две точки $j_1, j_2 \in \mathbb{N}$ определяется как объединение носителей всех векторов веса 3 из C , которые содержат обе точки j_1 и j_2 . Тогда множества $J_m \subset \mathbb{N}$, построенные в доказательстве леммы 2, являются $(m - 1)$ -мерными конечными проективными подпространствами в N , которые стандартно обозначаются как $\widetilde{PG}_q(m - 1)$. В частности, из этих определений следует, что $PG_q(\infty) = \bigcup_{m=2}^{\infty} \widetilde{PG}_q(m - 1)$

3. СИСТЕМАТИЧЕСКИЕ q -ЗНАЧНЫЕ КОДЫ БЕСКОНЕЧНОЙ ДЛИНЫ

Определение 3. Совершенный двоичный код $C \subset F_q^{\mathbb{N}_0}$ называется систематическим, если множество $\mathbb{N}$ можно разбить на два подмножества N_1 и N_2 ($N_1 \cap N_2 = \emptyset$, $\mathbb{N} = N_1 \cup N_2$) такие, что для любого вектора $x \in F_q^{N_{1,0}}$ (индекс 0 после символа N_1 означает, что мы рассматриваем только векторы из $F_q^{N_1}$, имеющие финитные носители) существует единственный вектор $y \in F_q^{N_{2,0}}$ для которого вектор z с координатами $z_i = x_i$ при $i \in N_1$, $z_i = y_i$ при $i \in N_2$ принадлежит коду C . В противном случае код C называется несистематическим.

Множество N_1 называют информационным, а множество N_2 — проверочным. Если в определении 3 ввести обозначение $y = f(x)$, то мы получим отображение $f : F_q^{N_{1,0}} \rightarrow F_q^{N_{2,0}}$ такое, что систематический код C будет графиком этого отображения в пространстве $F_q^{\mathbb{N}_0} = F_q^{N_{1,0}} \times F_q^{N_{2,0}}$.

Далее будем считать, что пространства $F_q^{N_{1,0}}$, $F_q^{N_{2,0}}$ вложены в $F_q^{\mathbb{N}_0}$, определяя недостающие координаты векторов $x \in F_q^{N_{1,0}}$, $y \in F_q^{N_{2,0}}$ нулевыми значениями.

Лемма 3. (1) Линейный код Хэмминга H_q^∞ является систематическим. (2) Если код C систематический с информационным множеством N_1 и проверочным множеством N_2 , то N_1 и N_2 бесконечны. (3) Отображение $f : F_q^{N_{1,0}} \rightarrow F_q^{N_{2,0}}$, графиком которого является систематический код C , сюръективно.

Доказательство. (1): В качестве проверочного множества для кода H_q^∞ возьмём $N_2 = \{1, 2, \dots, \frac{q^m-1}{q-1}+1, \dots\}$ и положим $N_1 = \mathbb{N} \setminus N_2$. Пусть $x \in F_q^{N_{1,0}}$. Представим x в виде $x = \alpha_1 e_{i_1} + \dots + \alpha_m e_{i_m}$. Так как $x \in F_q^{N_{1,0}}$, то $[x] = \{i_1, \dots, i_m\} \subset N_1$. Положим $\vec{j} = \alpha_1 \vec{i}_1 + \dots + \alpha_m \vec{i}_m$ (мы отождествляем $i_1, \dots, i_m$ с соответствующими столбцами проверочной матрицы (1)). Столбец $\vec{j}$ пропорционален некоторому столбцу проверочной матрицы (1) с номером j и с коэффициентом пропорциональности α . Символически это можно записать в виде равенства $\alpha \vec{j} = \alpha_1 \vec{i}_1 + \dots + \alpha_m \vec{i}_m$. Так как множество N_2 является базисом, то $\vec{j} = \beta_1 \vec{j}_1 + \dots + \beta_n \vec{j}_n$, $j_1, \dots, j_n \in N_2$. Полагаем $y = f(x) = -\alpha \beta_1 e_{j_1} - \dots - \alpha \beta_n e_{j_n}$. Так как $\alpha_1 \vec{i}_1 + \dots + \alpha_m \vec{i}_m - \alpha \beta_1 \vec{j}_1 - \dots - \alpha \beta_n \vec{j}_n = 0$, то по определению кода Хэмминга H_q^∞ , вектор $(x, f(x)) = x + y = \alpha_1 e_{i_1} + \dots + \alpha_m e_{i_m} - \alpha \beta_1 e_{j_1} - \dots - \alpha \beta_n e_{j_n} \in H_q^\infty$. Обратное, если $(x, y) \in H_q^\infty$, то также $(0, y - f(x)) \in H_q^\infty$, поэтому $\sum_{j \in N_2} (y_j - f(x)_j) \vec{j} = 0$.

Так как множество N_2 является базисом для столбцов проверочной матрицы (1), то $y_j = f(x)_j$ ($j \in N_2$).

(2): Доказательство этого пункта не отличается от соответствующего пункта теоремы 2 из [8].

(3): Пусть совершенный код C является систематическим с информационными и проверочными множествами N_1 и N_2 . Докажем, что отображение $f : \{0, 1\}_0^{N_1} \rightarrow \{0, 1\}_0^{N_2}$, графиком которого является код C , сюръективно. Допустим, что $0 \in C$. Рассмотрим любой ненулевой вектор $y \in F_q^{N_{2,0}}$, $y = \beta_1 e_{j_1} + \dots + \beta_n e_{j_n}$ ($j_1, \dots, j_n \in N_2$, $\beta_1, \dots, \beta_n \in F_q^*$). Допустим, что $y \in C$. Тогда вектор $0 \in F_q^{N_{1,0}}$ будет двумя различными способами достраиваться до кодовых векторов $0 + 0 \in C$ (так как $f(0) = 0$) и $0 + y \in C$. Это противоречит систематичности кода C . Поэтому $y \notin C$ и, если $n > 1$, то существуют базисный вектор e_i и $\alpha \in F_q^*$, для которых $\alpha e_i + y \in C$. Из предыдущего рассуждения следует, что $i \notin N_2$. Поэтому $i \in N_1$ и $f(\alpha e_i) = y$. Если $n = 1$ и $y = \beta_1 e_{j_1}$, то рассмотрим ещё один вектор $y' = \beta_1 e_{j_1} + \beta_2 e_{j_2} + \beta_3 e_{j_3}$, где также $j_2, j_3 \in N_2$, $\beta_2, \beta_3 \neq 0$. Уже доказано, что существуют $i \in N_1$ и $\alpha \in F_q^*$, для которых $f(\alpha e_i) = y'$. Рассмотрим теперь вектор $\alpha e_i + \beta_1 e_{j_1}$. Он тоже должен находиться на расстоянии 1 от некоторого кодового вектора, поэтому $\alpha e_i + \beta_1 e_{j_1} + \gamma e_k \in C$ ($\gamma \in F_q^*$). Если $k \in N_2$, то получим $f(\alpha e_i) = \beta_1 e_{j_1} + \gamma e_k \neq y'$, а это противоречит однозначности функции f . Поэтому $k \in N_1$ и $f(\alpha e_i + \gamma e_k) = \beta_1 e_{j_1}$.

Допустим теперь, что $0 \notin C$. Этот случай сводится к предыдущему. Существуют номер $i \in \mathbb{N}$, и $\alpha \in F_q^*$ для которых $\alpha e_i \in C$. Совершенный код $C' = C - \alpha e_i$, содержащий нулевой вектор, тоже систематический с теми же информационными и проверочными множествами N_1, N_2 , являющийся графиком функции $f'(x) = f(x + \alpha e_i)$, если $i \in N_1$, $f'(x) = f(x) - \alpha e_i$, если $i \in N_2$. $\square$

Следующая теорема является существенным усилением пункта (3) предыдущей леммы 3.

Теорема 1. Пусть $C \subset F_q^{N_0}$ — произвольный систематический код, содержащий 0 и являющийся графиком отображения $f : F_q^{N_{1,0}} \rightarrow F_q^{N_{2,0}}$. Тогда для любого $y \in F_q^{N_{2,0}}$ и любого $k \geq 0$ прообраз $f^{-1}(y)$ содержит бесконечное количество векторов веса k , кроме следующих случаев: 1) $y = 0$, $k = 0, 1, 2$; 2) $y \neq 0$, $k = 0$; 3) $|y| = 1, 2$, $k = 1$.

Доказательство. Докажем, что прообраз нуля $f^{-1}(0)$ бесконечен в каждом слое веса $k \geq 3$. Рассмотрим три различных номера $j_1, j_2, j_3 \in N_2$ и вектор $y = \beta e_{j_1} + e_{j_2} + e_{j_3} \in F_q^{N_{2,0}}$ при некотором $\beta \in F_q^*$. Очевидно, $y \notin C$. Существуют $i \in \mathbb{N}$ и $\alpha \in F_q^*$, для которых $z = \alpha e_i + y \in C$. По той же причине $i \notin N_2$. Допустим, что для бесконечного числа номеров j_3 номер i будет одним и тем же. Так как число элементов в поле F_q конечно, то и α будет одним и тем же для некоторой пары различных номеров $j_3, j'_3 \in N_2$. Тогда расстояние между соответствующими векторами $z = \alpha e_i + y$ и $z' = \alpha e_i + y'$ из C будет меньше 3. Поэтому, увеличивая номер $j_3 \in N_2$, мы можем считать номер i сколь угодно большим. Рассмотрим другой систематический код $C' = C - z$ и вектор $y' = -e_{j_2} - e_{j_3}$. Аналогичным образом, для вектора y' существуют $i' \in \mathbb{N}$, $\alpha' \in F_q^*$, для которых $z' = \alpha' e_{i'} + y' \in C'$. Очевидно $i' \notin N_2$ (так как вес вектора z' больше 1) и вектор $u = z' + z = \alpha e_i + \alpha' e_{i'} + \beta e_{j_1} \in C$. Отсюда следует, в частности, что $i' \neq i$. То есть, заменяя в предыдущей конструкции номер j_3 на другие номера из N_2 , мы можем сделать номера $i, i' \in N_1$ сколь угодно большими. Поэтому существует последовательность векторов $u_n = \alpha_n e_{i_n} + \alpha'_n e_{i'_n} + \beta e_{j_1}$ ($n \in \mathbb{N}$) веса 3, принадлежащих коду $C' = C - u$, при этом $i_n, i'_n \in N_1$, $i_n \neq i'_n$ и $i_n, i'_n \rightarrow \infty$. Векторы $v_n = u_n - u = \alpha_n e_{i_n} + \alpha'_n e_{i'_n} + \alpha e_i + \alpha' e_{i'}$ ($n \in \mathbb{N}$) имеют вес 4, принадлежат коду C и, поэтому, $f(v_n) = 0$. Далее будем строить бесконечное количество векторов веса 3 из прообраза $f^{-1}(0)$. Для произвольно выбранных трёх номеров $j_1, j_2, j_3 \in N_2$ рассмотрим три вектора $y_1 = e_{j_1} - e_{j_2}$, $y_2 = e_{j_2} - e_{j_3}$, $y_3 = e_{j_3} - e_{j_1}$. Существуют $\alpha_1 \in F_q^*$, $i_1 \in N_1$, для которых $x = \alpha_1 e_{i_1} + y_1 \in C$. Рассмотрим другой систематический код $C_1 = C - x$. Для него тоже будут существовать α_2 и i_2 , для которых $\alpha_2 e_{i_2} + y_2 \in C_1$, или $x' = \alpha_1 e_{i_1} + \alpha_2 e_{i_2} + e_{j_1} - e_{j_3} \in C$. Рассмотрим ещё один систематический код $C_3 = C - x'$. Опять существуют α_3 и i_3 , для которых $\alpha_3 e_{i_3} + y_3 \in C_3$, или $\alpha_1 e_{i_1} + \alpha_2 e_{i_2} + \alpha_3 e_{i_3} \in C$. Как было отмечено ранее, увеличивая неограниченно номера $j_2, j_3 \in N_2$, можно сделать номера i_1, i_2, i_3 различными и сколь угодно большими. Теперь, с помощью переноса систематического кода C на различные векторы $x \in C$, легко можно построить в прообразе $f^{-1}(0)$ бесконечное количество векторов любого веса $k \geq 3$, $k \neq 5$. Переходим к построению векторов веса 5 из $f^{-1}(0)$. Ранее, при построении векторов веса 4 из $f^{-1}(0)$, было показано, что для любых $\beta_1 \in F_q^*$ и $j_1 \in N_2$ существуют $\alpha_n, \alpha'_n \in F_q^*$ и сколь угодно большие номера $i_n, i'_n \in N_1$, для которых $u_n \alpha_n e_{i_n} + \alpha'_n e_{i'_n} + \beta_1 e_{j_1} \in C$. В точности так же, для любых $n \in \mathbb{N}$, $\beta_2 \in F_q^*$ и $j_2 \in N_2$ существуют α''_n, α'''_n и $i''_n, i'''_n \in N_1$, для которых $v_n = \alpha''_n e_{i''_n} + \alpha'''_n e_{i'''_n} + \beta_2 e_{j_2} \in C - u_n$. Значит для бесконечного числа векторов имеем $z_n = \alpha_n e_{i_n} + \alpha'_n e_{i'_n} + \alpha''_n e_{i''_n} + \alpha'''_n e_{i'''_n} + \beta_1 e_{j_1} + \beta_2 e_{j_2} \in C$. В систематическом коде $C - z_n$ существуют $\alpha \in F_q^*$, $i \in N_1$, для которых $\alpha e_i - \beta_1 e_{j_1} - \beta_2 e_{j_2} \in C - z_n$. Поэтому, при достаточно больших n векторы $w_n = \alpha_n e_{i_n} + \alpha'_n e_{i'_n} + \alpha''_n e_{i''_n} + \alpha'''_n e_{i'''_n} + \alpha e_i$ будут иметь вес 5 и принадлежать прообразу $f^{-1}(0)$.

Теперь докажем, что для любого вектора $0 \neq y \in F_q^{N_{2,0}}$ прообраз $f^{-1}(y)$ имеет бесконечную мощность в каждом слое веса $k \geq 2$. Из уже доказанной сюръективности отображения f следует существование вектора $w \in F_q^{N_{1,0}}$, для которого $f(w) = y$ и вектор $w' = w + y$ принадлежит C . Систематический код $C' = C - w'$ имеет те же информационные и проверочные множества N_1, N_2 , при этом он является графиком функции $f'(x) = f(x + w) - y$ ($x \in F_q^{N_{1,0}}$). Для

него тоже существует в каждом слое веса $k \geq 3$ бесконечная последовательность различных векторов $v'_n \in F_q^{N_1,0}$, для которых $f'(v'_n) = 0$. По построению, для последовательности $w_n = v'_n + w \in C$ получим $f(v'_n + w) = y$. Если вес $|y| \geq 2$, то в пункте (3) было доказано, что можно выбрать вес $|w| = 1$. Это означает, что существует бесконечное количество векторов $v'_n + w$ любого веса $k+1 \geq 4$, для которых $f(v'_n + w) = y$. Для построения векторов веса 3 рассмотрим номер $j \in N_2 \setminus [y]$ и два вектора $y_1 = y - e_j$, $y_2 = e_j$. Так как вес $|y_1| \geq 2$, то для некоторых $\alpha \in F_q^*$ и $i_1 \in N_1$ получим $z = \alpha e_{i_1} + y_1 \in C$. Ранее было показано, что для подходящих $\alpha_n, \alpha'_{n'} \in F_q^*$ и сколь угодно больших $i_n, i'_{n'} \in N_1$ имеем $\alpha_{i_n} e_{i_n} + \alpha'_{i'_{n'}} e_{i'_{n'}} + e_j \in C - z$. Отсюда, $\alpha e_{i_1} + \alpha_{i_n} e_{i_n} + \alpha'_{i'_{n'}} e_{i'_{n'}} + y \in C$. То есть, $f(\alpha e_{i_1} + \alpha_{i_n} e_{i_n} + \alpha'_{i'_{n'}} e_{i'_{n'}}) = y$. Остался ещё один случай, когда $|y| = 1$, (то есть $y = \beta e_j$, $j \in N_2$). Как и в предыдущем случае, для $j_1, j'_1 \in N_2 \setminus [y]$ рассматриваем два вектора $y_1 = y - e_{j_1} - e_{j'_1}$, $y_2 = e_{j_1} + e_{j'_1}$. Так как вес $|y_1| = 3$, то по ранее доказанному находим $\alpha \in F_q^*$, $i \in N_1$, для которых $\alpha e_i + y_1 \in C$. Так как вес $|y_2| = 2$, то для систематического кода $C' = C - \alpha e_i - y_1$ можно найти бесконечное число векторов v'_n любого веса $k \geq 3$, для которых $v'_n + y_2 \in C'$, что эквивалентно условию $v'_n + \alpha e_i + y_1 + y_2 = v'_n + \alpha e_i + y \in C$. То есть, если $|y| = 1$, то также существует бесконечное количество векторов $w_n = v'_n + \alpha e_1$ веса $k+1 \geq 4$, для которых $f(w_n) = y$. Остался нерассмотренным ещё случай веса $k = 2$. Если $y = \beta e_j$ ($\beta \in F_q^*$, $j \in N_2$), то ранее было доказано существование бесконечного количества векторов $x_n = \alpha_n e_{i_n} + \alpha'_n e_{i'_n}$ ($i_n, i'_n \in N_1$), для которых $f(x_n) = y$. Поэтому считаем, что вес $|y| \geq 2$. Пусть $y = \beta_1 e_{j_1} + \dots + \beta_k e_{j_k}$. Для $j \in N_2 \setminus [y]$ полагаем $y_1 = \beta_1 e_{j_1} + e_j$, $y_2 = y - y_1$. Существуют $i \in N_1$, $\alpha \in F_q^*$ такие, что $\alpha e_i + y \in C$. Существуют также $\alpha_1, \alpha_2 \in F_q^*$, $i_1, i_2 \in N_1$ для которых $\alpha_1 e_{i_1} + y_1 \in C$, $\alpha_2 e_{i_2} + y_2 \in C - \alpha_1 e_{i_1} - y_1$. Можно взять номер $j \in N_2$ настолько большим, чтобы выполнялось $i_1 > i$. Отсюда получаем $\alpha_1 e_{i_1} + \alpha_2 e_{i_2} + y \in C$. Предположение $i_1 = i_2 > i$ приводит к противоречию с $\alpha e_i + y \in C$.

Перечислим теперь случаи, когда прообраз $f^{-1}(y)$ конечен. 1) Если $y = 0$ и вес $k = 1, 2$, то прообраз пуст, а если $k = 0$, то прообраз состоит из одного нулевого вектора. 2) Если $|y| = 1$ и вес $k = 0, 1$, то прообраз тоже пуст. Если $|y| \geq 2$ и вес $k = 0$ то прообраз пуст, а если вес $k = 1$, то прообраз состоит из одного ненулевого вектора веса 1. $\square$

Случай, когда $0 \notin C$, как было сказано ранее, можно отдельно не рассматривать.

Для совершенных двоичных кодов в [17] (теорема 1 и следствие 4) установлено в частности, что для любого $y \in \{0, 1\}^{N_2}$, весовое распределение векторов из $f^{-1}(y)$ одинаково для всех систематических кодов длины $n = 2^m - 1$ с проверочным множеством N_2 ($|N_2| = m$). В отличие от кодов конечной длины, здесь весовой спектр тривиален и состоит только из трёх значений $0, 1, \infty$.

Следующую теорему можно считать бесконечномерным аналогом известной теоремы Шапиро-Злотника [13] ([14], теорема 16) о весовом распределении кодовых векторов совершенного кода бесконечной длины (не обязательно систематического).

Теорема 2. Пусть $C \subset F_q^{N_0}$ — произвольный q -значный код бесконечной длины, содержащий нулевой вектор. Тогда для любого $k \geq 3$ в C содержится бесконечное количество векторов веса k .

Доказательство. Фиксируем $\alpha \in F_q^*$, $i \in \mathbb{N}$. Для любых $\alpha' \in F_q^*$, $i' \in \mathbb{N}$, $i' \neq i$, существуют единственные $\alpha_1 \in F_q^*$, $i_1 \in \mathbb{N}$ такие, что $z(\alpha, i, \alpha', i') = \alpha e_i + \alpha' e_{i'} + \alpha_1 e_{i_1} \in C$. Из доказательства предыдущей теоремы 2 следует, что увеличивая номер i' можно сделать оба номера i', i_1 сколь угодно большими. В результате построено в коде C бесконечное количество векторов $z(\alpha, i, \alpha', i')$ веса 3. Рассмотрим любой такой вектор $z(\alpha, i, \alpha', i')$. Теперь в коде $C' = C - z(\alpha, i, \alpha', i')$ рассмотрим ещё один такой вектор $z'(-\alpha, i, \alpha'', i'')$, для которого соответствующие ему номера i'', i_1'' больше номеров i', i_1' . Тогда бесконечное количество векторов вида $z(\alpha, i, \alpha', i') + z'(-\alpha, i, \alpha'', i'')$ будут иметь вес 4 и принадлежать коду C . Теперь, так же как и в доказательстве теоремы 2, используя переносы кода C на построенные выше векторы веса 3 и 4, мы можем построить в C бесконечное количество векторов любого веса $k \geq 3$, $k \neq 5$. Для построения векторов веса 5 фиксируем в C вектор z веса 4 и номер i из носителя $[z]$, а также число α такое, что $|z - \alpha e_i| = 3$. В коде $C' = C - z$ рассмотрим векторы $z'(-\alpha, i, \alpha'', i'') = -\alpha e_i + \alpha'' e_{i''} + \alpha_1'' e_{i_1''}$, имеющими вес 3, со сколь угодно большими номерами i'', i_1'' . Тогда бесконечное количество векторов вида $z'(-\alpha, i, \alpha'', i'') + z$ будут иметь вес 5 и принадлежать коду C . $\square$

Замечание 2. В доказательствах теорем 1 и 2 полевая структура F_q не используется. Поэтому теоремы 1 и 2 останутся справедливыми, если считать F_q произвольной абелевой группой из q элементов ($q \geq 2$). Вопрос о существовании таких кодов здесь не рассматривается.

4. ПОСТРОЕНИЕ НЕЛИНЕЙНЫХ СОВЕРШЕННЫХ КОДОВ БЕСКОНЕЧНОЙ ДЛИНЫ СВИТЧИНГАМИ КОМПОНЕНТ

В коде Хэмминга H_q^∞ рассмотрим подпространство R_i , порожденное всеми векторами веса 3 с i -й координатой, равной единице. Всевозможные смежные классы вида $R_i^u = R_i + u$ ($u \in H_q^\infty$ называются i -компонентами кода H_q^∞ , $i \in \mathbb{N}$). Обозначим через $B_1(x)$ шар единичного радиуса с центром в точке $x \in F_q^{\mathbb{N}_0}$. Основное свойство i -компоненты состоит в следующем:

Лемма 4. 1-окрестности множеств R_i^u и $R_i^u + \alpha e_i$ ($\alpha \in F_q^*$) совпадают, то есть

$$\bigcup_{x \in R_i^u} B_1(x) = \bigcup_{x \in R_i^u + \alpha e_i} B_1(x).$$

Доказательство. Пусть $v \in B_1(x)$ при некотором $x \in R_i^u$ и $v = x$, тогда $v \in B_1(y)$, если $y = v + \alpha e_i$, поэтому $v \in R_i^u + \alpha e_i$. Теперь пусть $v \in B_1(x)$ и $v = x + \beta e_j$ при некоторых $j \in \mathbb{N}$, $\beta \in F_q^*$. Если $j \neq i$, то вектор $w = -\alpha e_i + \beta e_j + \gamma e_k$ принадлежит коду H_q^∞ и компоненте R_i при некоторых $k \in \mathbb{N}$, $\gamma \in F_q^*$. Поэтому вектор $y = x + w + \alpha e_i$ принадлежит $R_i^u + R_i + \alpha e_i = R_i^u + \alpha e_i$. Так как $v - y = -\gamma e_k$, то $v \in B_1(y)$. Если $j = i$, то $v \in B_1(y)$ при $y = x + \alpha e_i$ принадлежащем $R_i^u + \alpha e_i$. Обратно, предположив, что $v \in B_1(y)$ при некотором $y \in R_i^u + \alpha e_i$ и, обращая предыдущие рассуждения, мы получим, что $v \in B_1(x)$ при некотором $x \in R_i^u$. $\square$

Рассмотрим некоторое семейство $\mathcal{B} = \{R_{i_1}^{u_1}, R_{i_2}^{u_2}, \dots\}$, состоящее из конечно-го или бесконечного числа попарно непересекающихся i_p -компонент, где $\mathbf{u}_p \in H^\infty$, $1 \leq p < m + 1$ ($m \in \mathbb{N} \cup \{\infty\}$). Одна из основных конструкций нелинейных совершенных двоичных кодов состоит в том, что в коде H_q^∞ сдвигаются

по координатам i_p все компоненты из семейства $\mathcal{B}$. То есть, для любого набора $\alpha = (\alpha_1, \alpha_2, \dots) \in F_q^{\mathbb{N}}$ рассмотрим множество

$$H_q^\infty(\mathcal{B}, \alpha) = \left(H_q^\infty \setminus \bigcup_{p=1}^m R_{i_p}^{u_p} \right) \cup \left(\bigcup_{p=1}^m (R_{i_p}^{u_p} + \alpha_p e_{i_p}) \right).$$

Лемма 5. *Множество $H_q^\infty(\mathcal{B}, \alpha)$ является совершенным кодом в $F_q^{\mathbb{N}_0}$.*

Доказательство этой леммы такое же, как и доказательство леммы 2 для двоичных кодов из [8].

Будем говорить, что код $H_q^\infty(\mathcal{B})$ построен из кода Хэмминга H_q^∞ свитчингами компонент из семейства $\mathcal{B}$. Первая конструкция нелинейных двоичных кодов методом свитчинга непересекающихся компонент была предложена в [16]. Свитчинговая конструкция нелинейных совершенных q -значных кодов рассматривалась в [15].

5. НЕЛИНЕЙНЫЕ СИСТЕМАТИЧЕСКИЕ КОДЫ БЕСКОНЕЧНОЙ ДЛИНЫ

Сейчас нам известен только один пример систематического кода бесконечной длины — это линейный код Хэмминга H_q^∞ . Далее мы приведём достаточно общую конструкцию таких кодов.

Пусть $J = \{j_1, j_2, \dots\}$ — некоторое линейно независимое множество индексов, являющееся базисом в множестве всех столбцов проверочной матрицы (1). Обозначим

$$L_2(J) = \{i \in N : \exists \beta, \gamma \in F_q, \exists j, j' \in J, \vec{i} = \alpha \vec{j} + \beta \vec{j}'\}$$

На языке проективной геометрии $L_2(J)$ — это объединение всех прямых, проходящих через любые пары точек из базиса J .

Определение 4. *Множество индексов $I = \{i_1, i_2, \dots\} \subset N$ называется систематическим, если для некоторого базисного набора индексов $J \subset N$ выполняется $I \subset L_2(J)$. В противном случае множество I называется несистематическим.*

Рассмотрим в коде H_q^∞ произвольное семейство непересекающихся компонент $\mathcal{B} = \{R_{i_1}^{u_1}, R_{i_2}^{u_2}, \dots\}$. Обозначим $I_{\mathcal{B}} = \{i : \exists r, i = i_r\}$ — множество всех индексов i , для которых существуют i -компоненты, принадлежащие семейству $\mathcal{B}$.

Теорема 3. *Если множество $I_{\mathcal{B}}$ систематическое, то совершенный код $C = H_q^\infty(\mathcal{B}, \alpha)$ является систематическим при любом $\alpha = (\alpha_1, \alpha_2, \dots) \in F_q^{\mathbb{N}}$.*

Доказательство. Пусть $I \subset L_2(J)$ для базисного множества J . Возьмём $N_1 = N \setminus J$ в качестве информационного множества, а $N_2 = J$ в качестве проверочного множества. Нам необходимо доказать, что если $u, v \in C$ и $u \neq v$, то $[u - v] \not\subset J$. Доказательство этого факта ничем не отличается от доказательства соответствующей части теоремы 1 из [6]. Поэтому мы его опускаем.

В случае кодов конечной длины доказательство на этом заканчивается. Для кодов бесконечной длины установлен только тот факт, что для любого $x \in F_q^{N_{1,0}}$ существует не более одного $y \in F_q^{N_{2,0}}$ такого, что $x + y \in C$. Необходимо ещё проверить, что для любого вектора $x \in F_q^{N_{1,0}}$ существует (единственный)

вектор $y \in F_q^{N_2,0}$, для которого $x + y \in C$. Представим x в виде $x = \sum_{k=1}^s x_k e_{i_k}$, где $i_1, \dots, i_s \in N_1$. Так как $J = N_2$ является базисом, то любой индекс i_k имеет разложение $\vec{i}_k = \sum_{l=1}^p \beta_{k,l} \vec{j}_l$, где $j_1, \dots, j_p \in N_2$, $\beta_{k,l} \in F_q$. По определению кода Хэмминга H_q^∞ , вектор

$$z = \sum_{k=1}^s x_k e_{i_k} - \sum_{k=1}^s \sum_{l=1}^p x_k \beta_{k,l} e_{j_l}$$

принадлежит H_q^∞ . Если z не принадлежит ни одной компоненте $R_{i_k}^{u_k}$, то $z \in C$ и можно положить $y = z - x = - \sum_{k=1}^s \sum_{l=1}^p x_k \beta_{k,l} e_{j_l}$. Если z принадлежит одной из компонент $R_{i_{k'}}^{u_{k'}}$, то $z + \alpha_{k'} e_{i_{k'}} \in C$ и $i_{k'} \in L_2(J)$, $\vec{i}_{k'} = \beta \vec{j} + \beta' \vec{j}'$ при некоторых $\beta, \beta' \in F_q$, $j, j' \in N_2$. Положим $y = - \sum_{k=1}^s \sum_{l=1}^{s'} x_k \beta_{k,l} e_{j_l} + \alpha_{k'} \beta e_j + \alpha_{k'} \beta' e_{j'}$. Тогда $x + y = z + \alpha_{k'} \beta e_j + \alpha_{k'} \beta' e_{j'} = z + \alpha_{k'} e_{i_{k'}} + w \in R_{i_{k'}}^{u_{k'}} + \alpha_{k'} e_{i_{k'}} + w \subset C$, так как $w = \alpha_{k'} \beta e_j + \alpha_{k'} \beta' e_{j'} - \alpha_{k'} e_{i_{k'}} \in R_{i_{k'}}$. $\square$

Если множество индексов I конечное и $I \subset L_2(J)$ для некоторого базисного множества индексов J , то $I \subset L_2(J_m)$ для некоторого конечного подмножества $J_m = \{j_1, \dots, j_m\} \subset J$. Тогда из [6] леммы 3 следует, что если для семейства непересекающихся компонент $\mathcal{B}$ (конечного или бесконечного) выполняется $|I_B| \leq 6$, то код $H_q^\infty(\mathcal{B}, \alpha)$ будет систематическим при любом $\alpha \in F_q^{\mathbb{N}}$. При $|I_B| = 1$ (т.е. $i_k = i_0$ для всех k) коды $H_q^\infty(\mathcal{B}, \alpha)$ принято называть *кодами Шонхейма* [15]. Если $q = 2$, то такие коды традиционно называются *кодами Васильева* [16]. Эти коды наиболее удобны для доказательства того, что существует континуум попарно неэквивалентных систематических кодов бесконечной длины, см. теорему 1 из [7].

6. НЕСИСТЕМАТИЧЕСКИЕ q -ЗНАЧНЫЕ КОДЫ БЕСКОНЕЧНОЙ ДЛИНЫ

Определение 5. Говорим, что семейство непересекающихся компонент $\mathcal{B} = \{R_{i_1}^{u_1}, R_{i_2}^{u_2}, \dots\}$ кода Хэмминга H_q^∞ не содержит кратных компонент, если $i_k \neq i_{k'}$ при $k \neq k'$.

Далее будем рассматривать только такие семейства компонент.

Рассмотрим такое конечное семейство компонент $\mathcal{B}_s = \{R_{i_1}^{u_1}, \dots, R_{i_s}^{u_s}\}$.

Лемма 6. Если $q > s + 1$ и код $H_q^\infty(\mathcal{B}_s, \alpha)$ является систематическим при некотором $\alpha = (\alpha_1, \dots, \alpha_s) \in F_q^s$ с информационным множеством N_1 и проверочным множеством N_2 , то множество N_2 является базисом в N .

Доказательство. Допустим, что проверочное множество N_2 является зависимым. То есть, $\sum_{k=1}^{s'} \beta_k \vec{j}_k = 0$ для некоторого конечного множества индексов

$j_1, \dots, j_{s'} \in N_2$. Тогда вектор $u = \sum_{k=1}^{s'} \beta_k e_{j_k}$ принадлежит коду H_q^∞ . При достаточно большом номере n' больше половины элементов конечного подкода

$\tilde{H}_q^{n'}$ не будет принадлежать объединению всех компонент $\bigcup_{k=1}^s R_{i_k}^{u_k}$. Это следует из оценки $2sq^{\frac{n'-1}{q}} < q^{n'-m'}$, справедливой при достаточно больших m' и $n' = (q^{m'} - 1)/(q - 1)$. Так как тогда $\tilde{Q} = \tilde{H}_q^{n'} \setminus \bigcup_{k=1}^s R_{i_k}^{u_k} \subset C$ и $u \in \tilde{H}_q^{n'}$, при достаточно большом n' , то $u = u_1 - u_2$ для некоторых $u_1, u_2 \in \tilde{Q} \subset C$. Но тогда $[u] \subset N_2$ и $u \in C - C$, $u \neq 0$, что противоречит предполагаемой систематичности кода C . Поэтому проверочное множество N_2 должно быть независимым. Тогда его можно расширить до базисного множества $J \supset N_2$. Рассмотрим любой индекс $j \in J \setminus N_2$. Из систематичности кода C следует, что для любого $\beta \in F_q^*$ вектор $u(\beta) = \beta e_j + \sum_{k=1}^t \beta_k e_{j_k}$ принадлежит C для некоторых $\beta_1, \dots, \beta_t \in F_q$, $j_1, \dots, j_t \in N_2$. так как $\vec{j}, \vec{j}_1, \dots, \vec{j}_t$ линейно независимы, то $u(\beta) \notin H_q^\infty$. Следовательно, $u(\beta) \in R_{i_k}^{u_k} + \alpha_k e_{i_k}$ для некоторого k . Допустим, что для другого $\beta' \in F_q^*$ также получаем $u(\beta') \in R_{i_k}^{u_k} + \alpha_k e_{i_k}$. Тогда $u(\beta) - u(\beta') \in R_{i_k} \subset H_q^\infty$, но носитель $[u(\beta) - u(\beta')]$ входит в линейно независимое множество J . Следовательно, $u(\beta') \in R_{i_{k'}}^{u_{k'}}$ при другом $k' \neq k$. Так как из $k' \neq k$ следует $i_{k'} \neq i_k$, то при разных β векторы $u(\beta)$ должны принадлежать разным компонентам. Это невозможно при $s < q - 1$. $\square$

Лемма 7. Пусть для множества индексов $I = \{i_1, \dots, i_s\}$ выполняются неравенства $i_1, \dots, i_s \leq n = (q^m - 1)(q - 1)$. В этом случае множество I является несистематическим тогда и только тогда, когда оно несистематическое в конечном коде $\tilde{H}_q^n$ в смысле определения 3 из [6].

Доказательство. Допустим, что множество I систематическое в смысле определения 4. Тогда для некоторого базисного множества J получим $I \subset L_2(J)$. Следовательно, для подходящего конечного подмножества $J_t = \{j_1, \dots, j_t\} \subset J$ тоже выполняется $I \subset L_2(J_t)$. Рассмотрим номер $n' = (q^{m'} - 1)(q - 1)$ такой, что $j_1, \dots, j_t \leq n'$. Значит множество I является систематическим в конечном подкоде $\tilde{H}_q^{n'}$. Из [6], леммы 1 (о ранге) следует, что свойство множества I быть систематическим не зависит от того, в каком конечном коде Хэмминга изучается этот вопрос. В частности I будет систематическим и в коде $\tilde{H}_q^n$. Обратно, если множество I систематическое в коде $\tilde{H}_q^n$, то $I \subset L_2(J_m)$ для некоторого множества $J_m = \{j_1, \dots, j_m\}$, являющегося базисом для первых n столбцов проверочной матрицы (1). Распирив J_m до базиса J для всей проверочной матрицы (1), получим $I \subset L_2(J)$. $\square$

Лемма 8. Пусть $v = e_i - \beta_1 e_{j_1} - \dots - \beta_m e_{j_m} \in H_q^\infty$ и множество индексов $J_m = \{j_1, \dots, j_m\}$ линейно независимо. Тогда, если $\beta_r \neq 0$ по крайней мере трёх различных номеров r , то $v \notin R_i$

Доказательство. Будем доказывать от противного. Допустим, что $v = \delta_1 w_1 + \dots + \delta_k w_k$ для некоторых векторов $w_1, \dots, w_k \in H_q^\infty$ веса 3, у которых i -я координата равна 1. Рассмотрим номер $n' = (q^{m'} - 1)(q - 1)$ такой, что n' больше номеров $i, j_1, \dots, j_m$ и всех номеров из носителей $[w_1], \dots, [w_k]$. Тогда все векторы $v, w_1, \dots, w_k$ будут принадлежать конечному подкоду $\tilde{H}_q^{n'}$, изоморфному

совершенному коду $H_q^{n'}$. Для совершенных кодов конечной длины утверждение $v \notin \tilde{R}_i = R_i \cap \tilde{H}_q^{n'}$ было уже доказано, см. доказательство теоремы 2 из [6]. Это противоречие доказывает лемму. $\square$

Теорема 4. Пусть для конечного семейства непересекающихся компонент $\mathcal{B}_s = \{R_{i_1}^{u_1}, \dots, R_{i_s}^{u_s}\}$ кода H_q^∞ множество $I_{\mathcal{B}_s}$ является несистематическим. Тогда при $q > s + 1$ совершенный код $H_q^\infty(\mathcal{B}_s, \alpha)$ будет несистематическим для любого $\alpha = (\alpha_1, \dots, \alpha_s) \in F_q^s$ ($\alpha_k \neq 0, k = 1, \dots, s$).

Доказательство. Допустим противное, то есть код $H_q^\infty(\mathcal{B}_s, \alpha)$ при некотором $\alpha = (\alpha_1, \dots, \alpha_s) \in F_q^s$ ($\alpha_k \neq 0, k = 1, \dots, s$) является систематическим с информационным множеством N_1 и проверочным множеством N_2 . Из леммы 6 следует, что множество N_2 является базисом, а из определения 4 следует $I_{\mathcal{B}_s} \not\subset L_2(N_2)$. Пусть $i \in I_{\mathcal{B}_s} \setminus L_2(N_2)$, то есть $i = i_k$ для некоторого $k = 1, \dots, s$. Так как N_2 – базис, то $\vec{i}_k = \beta_1 \vec{j}_1 + \dots + \beta_m \vec{j}_m$ для некоторых $j_1, \dots, j_m \in N_2$. Из $i_k \notin L_2(N_2)$ заключаем, что $\beta_r \neq 0$ по крайней мере для трёх различных номеров r . Из определения кода Хэмминга H_q^∞ следует, что вектор $v = e_{i_k} - \beta_1 e_{j_1} - \dots - \beta_m e_{j_m} \in H_q^\infty$. Из леммы 8 следует $v \notin R_i$. Поэтому компоненты $R_{i_k}^{u_k}$ и $R_{i_k}^{u_k + \alpha_k v}$ не пересекаются. Рассмотрим номер $n = (q^m - 1)(q - 1)$ настолько большим, чтобы $i_1, \dots, i_s \leq n$, чтобы все векторы $u_1, \dots, u_s, v$ принадлежали коду $\tilde{H}_q^n$ и, чтобы выполнялись неравенства

$$s|R_i \cap \tilde{H}_q^n| < \frac{1}{2}|\tilde{H}_q^n|, \quad s|R_i \cap R_j \cap \tilde{H}_q^n| \leq |R_i \cap \tilde{H}_q^n| \quad (i \neq j) \quad (3)$$

(условия (1), (2) из [6]). В коде $\tilde{H}_q^n$ рассмотрим компоненты $\tilde{R}_{i_k}^{u_k} = R_{i_k}^{u_k} \cap \tilde{H}_q^n$, ($k = 1, \dots, s$). Теперь мы полностью находимся в условиях теоремы 2 из [6]. Для полноты изложения приведём финальную часть доказательства этой теоремы.

Так как $\mathcal{B}_s$ не содержит кратных компонент, то $R_{i_k}^{u_k + \alpha_k v} \notin \mathcal{B}_s$. Из условий (3) следует существование вектора $w \in \tilde{R}_{i_k}^{u_k + \alpha_k v}$ такого, что $w \notin \tilde{R}_{i_l}^{u_l}$ ($l = 1, \dots, s$). Значит $w \in R_{i_k}^{u_k + \alpha_k v} \setminus \bigcup_{l=1}^s R_{i_l}^{u_l} \subset C$. Из $w - \alpha_k v \in R_{i_k}^{u_k}$ следует, что $w' = w - \alpha_k v + \alpha_k e_{i_k} \in C$. Рассмотрим вектор $w' - w = \alpha_k \beta_1 e_{j_1} + \dots + \alpha_k \beta_m e_{j_m}$. Его носитель $[w' - w] \subset N_2$, чего не может быть для систематического кода с проверочным множеством N_2 . Поэтому код C несистематический. $\square$

Из леммы 7 и из [6], следствия 1 заключаем, что в коде H_q^∞ существуют семиэлементные несистематические множества для всех $q \neq 3, 5$ и из теоремы 4 получаем

Следствие 1. Если $q \geq 9$, то существуют семиэлементные семейства непересекающихся компонент $\mathcal{B}_7 = \{R_{i_1}^{u_1}, \dots, R_{i_7}^{u_7}\}$, для которых код $C = H_q^\infty(\mathcal{B}_7, \alpha)$ будет несистематическим при любом $\alpha = (\alpha_1, \dots, \alpha_7) \in F_q^7$, ($\alpha_k \neq 0, k = 1, \dots, 7$).

7. Коды с полной системой троек

Далее будем рассматривать бесконечные семейства непересекающихся компонент, не содержащие кратных компонент и такие, что для каждого $i \in \mathbb{N}$ существует ровно одна i -компонента из этого семейства. Обозначим такое семейство символом $\mathcal{B}_\infty = \{R_1^{u_1}, R_2^{u_2}, \dots, R_n^{u_n}, \dots\}$. Предварительно докажем несколько вспомогательных лемм.

Для $n = (q^m - 1)/(q - 1)$ в коде Хэмминга H_q^{qn+1} длины $qn + 1$ рассмотрим подкод $\tilde{H}_q^n$, изоморфный коду H_q^n . Для векторов $\tilde{u} \in \tilde{H}_q^n$ ($\tilde{u} = (u_1, \dots, u_{qn+1})$) все координаты $u_i = 0$ при $n < i \leq qn + 1$. Пусть $1 \leq i_1, i_2 \leq n$ и $\tilde{u}_1, \tilde{u}_2 \in \tilde{H}_q^n$. Рассмотрим в коде H_q^{qn+1} две компоненты $R_{i_1}^{\tilde{u}_1}, R_{i_2}^{\tilde{u}_2}$. Тогда пересечения $\tilde{R}_{i_1}^{\tilde{u}_1} = R_{i_1}^{\tilde{u}_1} \cap \tilde{H}^n$, $\tilde{R}_{i_2}^{\tilde{u}_2} = R_{i_2}^{\tilde{u}_2} \cap \tilde{H}_q^n$ будут компонентами в коде $\tilde{H}_q^n$.

Лемма 9. Если компоненты $\tilde{R}_{i_1}^{\tilde{u}_1}$ и $\tilde{R}_{i_2}^{\tilde{u}_2}$ не пересекаются, то компоненты $R_{i_1}^{\tilde{u}_1}$ и $R_{i_2}^{\tilde{u}_2}$ тоже не пересекаются. Кроме этого, если $\{\tilde{v}\} \in \tilde{H}_q^n \setminus \tilde{R}_{i_1}^{\tilde{u}_1}$ и $n < j \leq qn + 1$, то компоненты $R_j^{\tilde{v}}$ и $R_{i_1}^{\tilde{u}_1}$ не пересекаются.

Доказательство. Если компоненты $\tilde{R}_{i_1}^{\tilde{u}_1}$ и $\tilde{R}_{i_2}^{\tilde{u}_2}$ не пересекаются, то из [12], леммы 4 следует, что для любого $n < j \leq qn + 1$ множества $R_{i_1}^{\tilde{u}_1} + R_j$ и $R_{i_2}^{\tilde{u}_2} + R_j$ не пересекаются. Так как $0 \in R_j$, то отсюда сразу следует, что множества $R_{i_1}^{\tilde{u}_1}$ и $R_{i_2}^{\tilde{u}_2}$ также будут непересекающимися. Это доказывает первое утверждение леммы. Для доказательства второго утверждения рассмотрим непересекающиеся множества $R_{i_1}^{\tilde{u}_1} + R_j$ и $R_{i_2}^{\tilde{u}_2} + R_j$ при $i_2 = i_1$ и $\tilde{u}_2 = \tilde{v} \in \tilde{H}_q^n \setminus \tilde{R}_{i_1}^{\tilde{u}_1}$ (так как $\tilde{v} \notin \tilde{R}_{i_1}^{\tilde{u}_1}$, то смежные классы $\tilde{R}_{i_1}^{\tilde{u}_1}$ и $\tilde{R}_{i_1}^{\tilde{v}}$ не пересекаются и к ним можно ещё раз применить лемму 4 из [12]). Из равенства $R_{i_1}^{\tilde{v}} + R_j = R_{i_1} + R_j^{\tilde{v}}$ сразу следует непересекаемость компонент $R_{i_1}^{\tilde{u}_1}$ и $R_j^{\tilde{v}}$. $\square$

В подкоде $\tilde{H}_q^n$ кода Хэмминга H_q^{qn+1} рассмотрим ещё один подкод $\tilde{H}^{\frac{n-1}{q}}$, изоморфный коду $H_q^{\frac{n-1}{q}}$.

Лемма 10. Пусть $\tilde{\mathcal{B}} = \{\tilde{R}_1^{\tilde{u}_1}, \dots, \tilde{R}_n^{\tilde{u}_n}\}$ — семейство непересекающихся компонент кода $\tilde{H}_q^n$ ($n = (q^m - 1)/(q - 1)$, $m \geq 5$) и $R_1^{\tilde{u}_1}, \dots, R_n^{\tilde{u}_n}$ — компоненты кода H_q^{qn+1} , для которых $R_i^{\tilde{u}_i} \cap \tilde{H}^n = \tilde{R}_i^{\tilde{u}_i}$ ($i = 1, \dots, n$). Тогда существуют компоненты $R_{n+1}^{\tilde{u}_{n+1}}, \dots, R_{qn+1}^{\tilde{u}_{qn+1}}$ такие, что семейство $\mathcal{B} = \{R_1^{\tilde{u}_1}, \dots, R_{qn+1}^{\tilde{u}_{qn+1}}\}$ состоит из попарно не пересекающихся компонент кода H_q^{qn+1} и $R_i^{\tilde{u}_i} \cap \tilde{H}^{\frac{n-1}{q}} = \emptyset$ ($i = n + 1, \dots, qn + 1$).

Доказательство. Требуемое семейство компонент будем строить по индукции. Допустим, что для $n \leq s < qn + 1$ уже найдено требуемое семейство компонент $\mathcal{B}_s = \{R_1^{\tilde{u}_1}, \dots, R_s^{\tilde{u}_s}\}$. Код H_q^{qn+1} относительно подпространства R_{s+1} разбивается на смежные классы $R_{s+1} + u$, $u \in H_q^{qn+1}$. Число таких смежных классов равно q^{n-m} . Каждое множество $R_i^{\tilde{u}_i} + R_{s+1}$ разбивается на $q^{\frac{n-1}{q}}$ этих смежных классов. Поэтому множество $\bigcup_{i=1}^s (R_i^{\tilde{u}_i} + R_{s+1})$ является объединением не более чем $s \cdot q^{\frac{n-1}{q}}$ смежных классов. Число элементов кода $\tilde{H}^{\frac{n-1}{q}}$ равно $q^{\frac{n-1}{q}-m+1}$. Если

$$q^{n-m} > s \cdot q^{\frac{n-1}{q}} + q^{\frac{n-1}{q}-m+1},$$

то существует смежный класс R_{s+1}^u не пересекающийся с множеством $\bigcup_{i=1}^s (R_i^{\tilde{u}_i} + R_{s+1})$ и с кодом $\tilde{H}^{\frac{n-1}{q}}$. При $n = (q^m - 1)/(q - 1)$ это возможно, если $m \geq 5$ (если $q \geq 3$, то вышеприведённое неравенство будет выполняться начиная с $m \geq 3$). Известно, что компонента R_{s+1}^u кода H_q^{qn+1} пересекается с кодом

предыдущей размерности $\tilde{H}_q^n$ по единственному элементу $\tilde{u}_{s+1}$, см. лемму 4 из [5] (для двоичных кодов) или лемму 1 из [12]. Поэтому компонента $R_{s+1}^{\tilde{u}_{s+1}} = R_{s+1} + u$ будет искомой. $\square$

Определение 6. Семейство непересекающихся компонент $\mathcal{B}_\infty = \{R_1^{u_1}, R_2^{u_2}, \dots\}$ кода H_q^∞ называем разреженным, если существует номер m_0 такой, что $R_i^{u_i} \cap \tilde{H}_q^{(q^m-1)/(q-1)} = \emptyset$ для всех $i > (q^{m+1} - 1)/(q - 1)$ и всех $m \geq m_0$.

Из [6] известно, что при $m \geq 6$ в коде Хэмминга $H_q^{(q^m-1)/(q-1)}$ существует семейство $\mathcal{B} = \{R_1^{u_1}, \dots, R_n^{u_n}\}$, состоящее из $n = (q^m - 1)/(q - 1)$ попарно не пересекающихся i -компонент $R_i^{u_i}$ ($1 \leq i \leq n$), см., например, [1, 9]. Поэтому, применяя индуктивно лемму 10 начиная с $n_0 = (q^6 - 1)/(q - 1)$, мы получаем

Следствие 2. В коде Хэмминга бесконечной длины H_q^∞ существуют разреженные семейства компонент.

Определение 7. Семейство непересекающихся компонент $\mathcal{B}_\infty = \{R_1^{u_1}, R_2^{u_2}, \dots\}$ кода H_q^∞ называем неплотным, если существует номер m_0 такой, что для любого $m \geq m_0$ количество i -компонент $R_i^{u_i}$ при $i > (q^m - 1)/(q - 1) = n$, пересекающихся с кодом $\tilde{H}_q^n$, меньше, чем $q^{\frac{n-1}{q}} - (n-1)q^{(q-1)q^{m-2}}$.

Из леммы 10 следует, что при $i > n$ количество i -компонент семейства $\mathcal{B}_\infty$, пересекающихся с подкодом $\tilde{H}_q^n$ не превышает $n + 1$. Так как $n + 1 < q^{\frac{n-1}{q}} - (n-1)q^{(q-1)q^{m-2}}$ при $n \geq (q^6 - 1)/(q - 1)$, то из определений 6 и 7 следует, что любое разреженное семейство компонент является неплотным.

Определение 8. Говорим, что совершенный код $C \subset F_q^{\mathbb{N}_0}$ имеет полную систему троек, если для любого вектора $u \in F_q^{\mathbb{N}_0}$ веса 3 существуют $\alpha \in F_q^*$ и два кодовых вектора $v, w \in C$ такие, что $[u] = [v - w]$.

Лемма 11. Если совершенный код $C \subset F_q^{\mathbb{N}_0}$ имеет полную систему троек, то он несистематический.

Доказательство. Допустим, что код C систематический с информационными и проверочными множествами N_1, N_2 и функцией $f : F_q^{N_{1,0}} \rightarrow F_q^{N_{2,0}}$, графиком которой он является. Так как множество N_2 бесконечное, то можно рассмотрим три различных номера $j_1, j_2, j_3 \in N_2$ и вектор $w = e_{j_1} + e_{j_2} + e_{j_3} \in F_q^{N_{2,0}}$. Существуют $\alpha \in F_q^*$ и два вектора $z, z' \in C$ такие, что $[z' - z] = [w]$. Из предполагаемой систематичности кода C следует, что $z = x + y, z' = x' + y'$, где $x, x' \in F_q^{N_{1,0}}, y = f(x) \in F_q^{N_{2,0}}, y' = f(x') \in F_q^{N_{2,0}}$. Так как $[z' - z] \subset N_2$, то $x = x'$ и $[y' - y] = [w] \neq \emptyset$, что противоречит однозначности функции f . $\square$

Теорема 5. Если бесконечное семейство непересекающихся компонент $\mathcal{B}_\infty = \{R_1^{u_1}, R_2^{u_2}, \dots\}$ является неплотным, то код $H_q^\infty(\mathcal{B}_\infty, \alpha)$ имеет полную систему троек при любом $\alpha = (\alpha_1, \alpha_2, \dots) \in F_q^{\mathbb{N}}$ ($\alpha_k \neq 0, k \in \mathbb{N}$).

Доказательство. Пусть вектор $u \in F_q^{\mathbb{N}_0}$ имеет вес 3 и $u = \beta_1 e_{j_1} + \beta_2 e_{j_2} + \beta_3 e_{j_3}$. Допустим, что $u \notin H_q^\infty$. Тогда существует единственный номер $i \in \mathbb{N}$ и $\delta \in F_q^*$, для которых вектор $v = \delta e_i - \beta_1 e_{j_1} - \beta_2 e_{j_2} - \beta_3 e_{j_3}$ принадлежит коду Хэмминга H_q^∞ . Предположим сперва, что $i \notin [u]$. Существует такой номер $m \geq m_0$, что $i, j_1, j_2, j_3 \leq (q^m - 1)/(q - 1) = n$ и подкод $\tilde{H}_q^n$ ($n = (q^m - 1)/(q - 1)$) содержит

вектор u_i из компоненты $R_i^{u_i}$. Для любого $s \in \mathbb{N}$ обозначим $\tilde{R}_s^{u_s} = R_s^{u_s} \cap \tilde{H}_q^n$. Если $s = i$, то $\tilde{R}_i^{u_i}$ является i -компонентой кода $\tilde{H}_q^n$. Если $1 \leq s \leq n$, и $s \neq i$, то $\tilde{R}_s^{u_s}$ либо пусто, либо является s -компонентой кода $\tilde{H}_q^n$. Если $n < s$, то в силу леммы 5, $\tilde{R}_s^{u_s}$ либо пусто, либо состоит из одного элемента $\tilde{u}_s \in \tilde{H}_q^n$. В коде $\tilde{H}_q^n$ рассмотрим ещё одну i -компоненту $\tilde{R}_i^{u_i} + \frac{\alpha_i}{\delta}v$. Так как $u \notin H_q^\infty$, то номера j_1, j_2, j_3 линейно независимы (как столбцы проверочной матрицы (1)). Из леммы 8 следует, что $v \notin R_i$. Поэтому компонента $\tilde{R}_i^{u_i} + \frac{\alpha_i}{\delta}v$ не пересекается с компонентой $\tilde{R}_i^{u_i}$. Если $1 \leq s \leq n$, $s \neq i$ и $\tilde{R}_s^{u_s}$ является s -компонентой кода $\tilde{H}_q^n$, то пересечение $\tilde{R}_s^{u_s} \cap (\tilde{R}_i^{u_i} + \frac{\alpha_i}{\delta}v)$ либо пусто, либо состоит из $q^{(q-1)q^{m-2}}$ элементов. Всего таких компонент с непустым пересечением не больше $n - 1$. При $s > n$ непустые пересечения компонент $R_s^{u_s}$ с кодом $\tilde{H}_q^n$ могут быть только одноточечные. Поэтому, в силу определения 7, число элементов в пересечении компоненты $\tilde{R}_i^{u_i} + \frac{\alpha_i}{\delta}v$ с множеством $\bigcup_{i=1}^{\infty} R_i^{u_i}$ меньше, чем $(n - 1)q^{(q-1)q^{m-2}} + \left(q^{\frac{n-1}{q}} - (n - 1)q^{(q-1)q^{m-2}}\right) = q^{\frac{n-1}{q}}$ (это число является мощностью компоненты $\tilde{R}_i$). Значит существует вектор $w \in (\tilde{R}_i^{u_i} + \frac{\alpha_i}{\delta}v) \setminus \bigcup_{i=1}^{\infty} R_i^{u_i}$. Это означает, что $w \in H_q^\infty(\mathcal{B}_\infty) = C$ и $w - \frac{\alpha_i}{\delta}v \in \tilde{R}_i^{u_i}$. Поэтому $w' = w - \frac{\alpha_i}{\delta}v + \alpha_i e_i \in R_i^{u_i} + \alpha_i e_i \subset C$ и $\frac{\alpha_i}{\delta}u = -\frac{\alpha_i}{\delta}v + \alpha_i e_i = w' - w \in C - C$, то есть $[w' - w] = [u]$.

Рассмотрим теперь случай $i \in [u]$. Без ограничения общности считаем $i = j_1$. Тогда $v = (\delta - \beta_1)e_{j_1} - \beta_2 e_{j_2} - \beta_3 e_{j_3}$. Вектор v веса 3 принадлежит компоненте R_{j_1} . Рассмотрим любой вектор $w \in R_{j_1}^{u_{j_1}} + \alpha_{j_1} e_{j_1} \subset C$. Вектор $w' = w + v$ тоже принадлежит той же компоненте $R_{j_1}^{u_{j_1}} + \alpha_{j_1} e_{j_1}$ и $w' - w = v \in C - C$, причём $[w' - w] = [u]$.

В случае, когда $u \in H_q^\infty$. Существует $m \geq m_0$ такое, что $u \in \tilde{H}_q^n$ ($n = (q^m - 1)/(q - 1)$). Число элементов в множестве $\tilde{H}_q^n \setminus \bigcup_{i=1}^{\infty} R_i^{u_i}$ больше, чем $q^{n-m} - (n + 1)q^{\frac{n-1}{q}} + (n - 1)q^{(q-1)q^{m-2}}$, что составляет больше половины числа элементов всего линейного кода $\tilde{H}_q^n$, если $m \geq 6$. Следовательно, существуют два вектора $w, w' \in \tilde{H}_q^n \setminus \bigcup_{i=1}^{\infty} R_i^{u_i} \subset C$, для которых $u = w - w' \in C - C$. $\square$

Непосредственно из определения 8, теоремы 5 и леммы 11 получаем

Следствие 3. Если $\mathcal{B}_\infty = \{R_1^{u_1}, R_2^{u_2}, \dots\}$ — неплотное семейство компонент кода Хэмминга H_q^∞ , то совершенный код $C = H_q^\infty(\mathcal{B})$ является несистематическим.

Замечание 3. Первая конструкция двоичных нелинейных кодов с полной системой троек предложена в [1]. В этой работе впервые были построены несистематические двоичные коды длины $n \geq 255$. В [9] эта конструкция была усовершенствована, что дало возможность строить коды с полной системой троек для $n = 31, 63, 127$. Для $n = 15$ такие коды были найдены с применением компьютерных вычислений [9, 11]. Конструкция q -значных совершенных кодов с полной системой троек получена впервые в настоящей работе даже для кодов конечной длины.

Следствие 4. Пусть $\mathcal{B}_n = \{R_1^{u_1}, \dots, R_n^{u_n}\}$ — семейство непересекающихся компонент кода Хэмминга H_q^n ($n = (q^m - 1)(q - 1)$). Тогда при $m \geq 5$ и $q \geq 3$, либо $m = 4$ и $q \geq 5$, код $H_q^n(\mathcal{B}_n)$ имеет полную систему троек. Следовательно, он является несистематическим.

Вопрос о существовании нелинейных q -значных кодов длины $n = (q^m - 1)/(q - 1)$ при $m = 3, 4$ и $q = 3, 4$ с полной системой троек, является открытым.

Далее мы покажем, что требование неплотности семейства компонент $\mathcal{B}_\infty$ в теореме 5 является оправданным.

Пусть $N_2 = \{1, 2, \dots, \frac{q^m - 1}{q - 1} + 1, \dots\}$, $N_1 = \mathbb{N} \setminus N_2$. Любой вектор $x \in F_q^{N_0}$ однозначно разлагается на сумму проекций $x = x_1 + x_2$, $x_1 \in F_q^{N_{1,0}}$, $x_2 \in F_q^{N_{2,0}}$. Число $|x_1|$ будем называть *информационным весом* вектора x , а наименьший информационный вес векторов из $R_i^{u_i} - R_j^{u_j}$ будем называть *информационным расстоянием* между i -компонентой $R_i^{u_i}$ и j -компонентой $R_j^{u_j}$.

Лемма 12. В коде Хэмминга H_q^∞ существует семейство попарно не пересекающихся компонент $\mathcal{B}_\infty = \{R_1^{u_1}, R_2^{u_2}, \dots\}$, для которого $H_q^\infty = \bigcup_{i=1}^\infty R_i^{u_i}$ и информационное расстояние между любой парой компонент $R_i^{u_i}$ и $R_j^{u_j}$, для которых $i < j$ и $j \in N_1$, больше двух.

Доказательство. Так же как и в доказательстве леммы 10 мы будем выбирать компоненты с помощью индуктивного процесса.

(а). Пусть $\tilde{\mathcal{B}}_n = \{\tilde{R}_1^{u_1}, \dots, \tilde{R}_n^{u_n}\}$ — семейство непересекающихся компонент кода $\tilde{H}_q^n$ ($n = (q^m - 1)/(q - 1)$) и $R_1^{u_1}, \dots, R_n^{u_n}$ — компоненты кода H_q^{qn+1} , для которых $R_i^{u_i} \cap \tilde{H}^n = \tilde{R}_i^{u_i}$ ($i = 1, \dots, n$). В подкоде $\tilde{H}_q^n$ рассмотрим его подкод $\tilde{H}_q^r$ с наименьшим номером r , для которого $\tilde{H}_q^r \setminus \left(\bigcup_{i=1}^n \tilde{R}_i^{u_i}\right) \neq \emptyset$. Выберем любой вектор $\tilde{u}_{n+1} \in \tilde{H}_q^r \setminus \left(\bigcup_{i=1}^n \tilde{R}_i^{u_i}\right)$ и рассмотрим в коде Хэмминга H_q^{qn+1} семейство компонент $\mathcal{B}_{n+1} = \{R_1^{u_1}, R_2^{u_2}, \dots, R_{n+1}^{u_{n+1}}\}$. В силу леммы 9 это семейство состоит из попарно не пересекающихся компонент, при этом мощность множества $\tilde{H}_q^r \setminus \left(\bigcup_{i=1}^{n+1} \tilde{R}_i^{u_i}\right)$ уменьшилась на единицу. Так же как и в доказательстве леммы 10 расширяем это семейство до семейства непересекающихся компонент $\mathcal{B}_{qn+1} = \{R_1^{u_1}, \dots, R_{qn+1}^{u_{qn+1}}\}$.

Покажем, что при этом расширении мы можем выбирать компоненты так, чтобы удовлетворить условиям на информационное расстояние. Допустим, что для $n < s < qn + 1$ найдено требуемое семейство компонент $\mathcal{B}_s = \{R_1^{u_1}, \dots, R_s^{u_s}\}$. Код H_q^{qn+1} относительно подпространства R_{s+1} разбивается на q^{n-m} смежных классов $R_{s+1} + u$, $u \in H_q^{qn+1}$. Каждое множество $R_i^{u_i} + R_{s+1}$ разбивается на $q^{\frac{n-1}{q}}$ смежных классов (см. доказательство леммы 10). Поэтому число смежных классов в коде H_q^{qn+1} по подпространству $R_i + R_{s+1}$ равно $q^{q^{m-1}-m}$. Количество векторов кода H_q^{qn+1} , информационный вес которых не превышает 2, равно $1 + ((q-1)(qn-m) + (q-1)^2 \binom{qn-m}{2})$. Поэтому, если $1 + ((q-1)(qn-m) + (q-1)^2 \binom{qn-m}{2}) < q^{q^{m-1}-m}$, то существует по крайней мере $q^{n-m} - 1 - ((q -$

$1)(qn - m) + (q - 1)^2 \binom{qn-m}{2} q^{\frac{n-1}{q}}$ различных $(s + 1)$ -компонент вида R_{s+1}^u , информационное расстояние которых до компоненты $R_i^{\tilde{u}_i}$ больше двух. Отсюда следует, что общее число различных компонент вида R_{s+1}^u , информационное расстояние которых до каждой компоненты $R_i^{\tilde{u}_i}$ ($i = 1, \dots, s$) больше двух, не меньше, чем $q^{n-m} - s(1 + (q - 1)(qn - m) + \binom{qn-m}{2}) q^{\frac{n-1}{q}}$. Так как $s < qn + 1$, то это число компонент будет положительно, если

$$q^{n-m} - qn \left(1 + (q - 1)(qn - m) + (q - 1)^2 \binom{qn-m}{2} \right) q^{\frac{n-1}{q}} > 0.$$

Это неравенство выполняется начиная с $n = n_0 = (q^6 - 1)/(q - 1)$. Одну из таких компонент R_{s+1}^u обозначим через $R_{s+1}^{\tilde{u}_{s+1}}$ (где можно выбрать $[\tilde{u}_{s+1}] \subset \{1, \dots, n\}$).

Пункт (а) вышеприведённого доказательства гарантирует индуктивный переход от номера $n = (q^m - 1)/(q - 1)$ к следующему номеру $qn + 1$. Нам осталось только определить базу индукции.

(b). В качестве базы рассмотрим код $\tilde{H}_q^{n_0}$, вложенный в следующий код Хэмминга $H_q^{qn_0+1}$. Компонента $\tilde{R}_1$ не является информационной, поэтому мы выбираем $\tilde{u}_1 \in \tilde{H}_q^{n_0}$ произвольным образом и определяет первую компоненту $\tilde{R}_1^{\tilde{u}_1}$. Далее, следуя пункту (а), индукцией по $s = 2, \dots, n_0$ выбираем компоненты $\tilde{R}_s^{\tilde{u}_s}$, каждая из которых находится на информационном расстоянии больше чем 2 от компонент, выбранных на предыдущих шагах.

Итак, начиная с базового кода $H_q^{qn_0+1}$, в котором вложен код $\tilde{H}_q^{n_0}$ с уже выбранными в нём компонентами $\{\tilde{R}_1^{\tilde{u}_1}, \dots, \tilde{R}_{n_0}^{\tilde{u}_{n_0}}\}$, мы применяем пункт (а) индуктивно по переменной $n = (q^m - 1)(q - 1)$, $m \geq 6$ до бесконечности. В результате получим бесконечное семейство непересекающихся компонент $\mathcal{B} = \{R_1^{u_1}, R_2^{u_2}, \dots\}$, компоненты которого покрывают весь код H^∞ и информационное расстояние между любыми двумя компонентами $R_i^{\tilde{u}_i}$ и $R_j^{\tilde{u}_j}$, $i < j$ ($j \in N_1$), больше двух. $\square$

Теорема 6. Пусть бесконечное семейство непересекающихся компонент $\mathcal{B} = \{R_1^{u_1}, R_2^{u_2}, \dots\}$ является покрытием кода Хэмминга H_q^∞ и информационное расстояние между любой парой компонент $R_i^{u_i}$, $R_j^{u_j}$, $i < j$, $j \in N_1$, этого семейства больше двух. Тогда совершенный код $C = H_q^\infty(\mathcal{B})$ будет иметь неполную систему троек.

Доказательство. Рассмотрим любой вектор x веса 3, носитель которого входит в N_2 . Предположим, что существуют два вектора $u, v \in H_q^\infty(\mathcal{B})$, для которых $u - v = x$. Если $u, v \in R_i^{u_i} + \alpha_i e_i$ для некоторой i -компоненты семейства $\mathcal{B}$, то $u + v \in H_q^\infty$ и поэтому носитель $[u - v]$ не может входить в проверочное множество N_2 . Пусть теперь $u \in R_i^{u_i} + \alpha_i e_i$, $v \in R_j^{u_j} + \alpha_j e_j$ при $i < j$ и допустим, что $[u - v] \subset N_2$. Это означает, что $u - \alpha_i e_i \in R_i^{u_i}$, $v - \alpha_j e_j \in R_j^{u_j}$. Если $i, j \in N_2$, то из $[u - v] \subset N_2$ следует $[u - v - \alpha_i e_i + \alpha_j e_j] \subset N_2$. Это противоречит тому, что $u - v - \alpha_i e_i + \alpha_j e_j \in H_q^\infty$. Если $i, j \in N_1$, то $u - v - \alpha_i e_i + \alpha_j e_j \in H_q^\infty$. Из $[u - v] \subset N_2$ следует, что информационное расстояние между компонентами $R_i^{u_i}$ и $R_j^{u_j}$ не больше двух, что противоречит условию теоремы. Такое же противоречие получим, если $i < j$ и $i \in N_2$, $j \in N_1$. Осталось рассмотреть случай, когда $i < j$ и $i \in N_1$, $j \in N_2$. То есть, $u - v - \alpha_i e_i + \alpha_j e_j \in H_q^\infty$ и $[u - v + \alpha_j e_j] \subset N_2$. Так как

$\vec{i} = \sum_{s \in [u-v+\alpha_j e_j]} \vec{s}$, то для любого $s \in [u-v+\alpha_j e_j]$ должно выполняться $s < i$.

Поэтому из $i < j$ следует, что $j \notin [u-v-\alpha_j e_j]$. Это означает, что множество $[u-v-\alpha_j e_j]$ состоит только из двух номеров $s_1, s_2 \in N_2$ и $\vec{i} = \gamma_1 \vec{s}_1 + \gamma_2 \vec{s}_2$. То есть, вектор веса 3 $u-v-\alpha_i e_i + \alpha_j e_j$ принадлежит компоненте R_i . Поэтому $0 \in R_i + R_i^{u_i} - R_j^{u_j} = R_i^{u_i} - R_j^{u_j}$, что противоречит непересекаемости компонент $R_i^{u_i}$ и $R_j^{u_j}$. Мы доказали, что разность кодов $C - C$ не содержит ни одного вектора веса 3, носитель которого входит в N_2 . $\square$

Автор благодарит рецензента за замечания, которые были учтены в окончательной версии работы.

REFERENCES

- [1] Avgustinovich S. V., Solov'eva F. I., *On the nonsystematic perfect binary codes*, Problems Inform. Transmission, **32**:3 (1996), 258–261. MR1441513
- [2] Krotov D. S., Potapov V. N., *Propelinear 1-perfect codes from quadratic functions* IEEE Trans. Inform Theory, **60**:4 (2014), 2065–2068. MR3181510
- [3] Krotov D. S., Sotnikova E. V., *Embedding in q-ary 1-Perfect Codes and Partitions*, Discrete Mathematics, **338**:11 (2015), 1856–1859. MR3357771
- [4] Los' A. V., *Construction of perfect q-ary codes by sequential switchings of $\tilde{\alpha}$ -components*, Problems Inform. Transmission, **40**:1 (2004), 37–43. Zbl 1085.94022
- [5] Malyugin S. A. *On enumeration of the perfect binary codes of length 15*, Discrete Applied Mathematics, **135**:1–3 (2004), 161–181. MR2046666
- [6] Malyugin S. A., *On nonsystematic perfect codes over finite fields*, J. Appl. Indust. Math., **4**:2 (2010), 218–230.
- [7] Malyugin S. A., *Perfect binary codes of infinite length*, J. Appl. Indust. Math., **8**:4 (2017), 552–556. MR3665877
- [8] Malyugin S. A., *Perfect binary codes of infinite length with complete system of triples*, Sib. Elektron. Mat. Izv., **14** (2017), 877–888. (in Russian) MR3703590
- [9] Phelps K. T., Levan M. J., *Nonsystematic perfect codes*, SIAM J. Discrete Math., **12**:1 (1999), 27–34. MR1666049
- [10] Potapov V. N., *Infinite-Dimensional Quasigroups of finite orders*, Math. Notes, **93**:3 (2013), 479–486. Zbl 1283.20071
- [11] Romanov A. M., *On nonsystematic perfect codes of length 15*, Diskretn. Anal. Issled. Oper. Ser 1, **4**:4 (1997), 75–78. (in Russian) MR1658757
- [12] Romanov A. M., *On partitions of q-ary Hamming codes into disjoint components*, Diskretn. Anal. Issled. Oper. Ser 1, **11**:3 (2004), 80–87. (in Russian) MR2109793
- [13] Shapiro O. S., Slotnik D. L., *On the mathematical theory of error correcting codes*, IBM J. Res. and Devel., **3**:1 (1959), 25–34. MR98636
- [14] Solov'eva F. I., *Introduction to coding theory*, Novosibirsk: Novosibirsk State University, 2006. (in Russian)
- [15] Shönheim J., *On linear and nonlinear single-error-correcting q-ary perfect codes*, Inform and Control, **12**:1 (1968), 23–26.
- [16] Vasil'ev Yu. L., *On Nongroup Close-Packed Codes*, Problems of Cybernetics, **8** (1962), 337–339. Zbl 0202.50305
- [17] Vasil'eva A. Yu., *Local spectra of perfect binary codes*, Diskretn. Anal. Issled. Oper. Ser 1, **6**:1 (1999), 3–11. (in Russian) Zbl 0930.94045

SERGEY ARTEM'EVICH MALYUGIN
 SOBOLEV INSTITUTE OF MATHEMATICS,
 4, KOPTYUGA AVE.,
 NOVOSIBIRSK, 630090, RUSSIA
E-mail address: mal@math.nsc.ru