S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 14, стр. 877–888 (2017) УДК 519.72
DOI 10.17377/semi.2017.14.074 MSC 94B60

СОВЕРШЕННЫЕ ДВОИЧНЫЕ КОДЫ БЕСКОНЕЧНОЙ ДЛИНЫ С ПОЛНОЙ СИСТЕМОЙ ТРОЕК

С.А.МАЛЮГИН

Abstract. An infinite-dimensional binary cube $\{0,1\}_0^{\mathbb{N}}$ consists of all sequences $u=(u_1,u_2,\dots)$, where $u_i=0,1$, and all $u_i=0$ except some finite set of indices $i\in\mathbb{N}$. A subset $C\subset\{0,1\}_0^{\mathbb{N}}$ is called a perfect binary 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 this binary cube. We say that the perfect code C has the complete system of triples if $C+C$ contains all vectors of $\{0,1\}_0^{\mathbb{N}}$ having weight 3. In this article we construct perfect binary codes having the complete system of triples (in particular, such codes are nonsystematic). These codes can be obtained from the Hamming code H^∞ by switchings a some family of disjoint components $\mathcal{B}=\{R_1^{u_1},R_2^{u_2},\dots\}$. Unlike the codes of finite 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 binary code, component, complete system of triples, nonsystematic code, condition of sparsity

1. Введение

Пусть $\mathbb{N}$ — множество натуральных чисел. *Бесконечномерный финитный куб* $\{0,1\}_0^{\mathbb{N}}$ состоит из всевозможных последовательностей $u=(u_1,u_2,\dots)$, где $u_i=0,1$ и все $u_i=0$ кроме конечного множества индексов $i\in\mathbb{N}$. Относительно побитовой операции сложения $u+v=(u_1\oplus v_1,\dots,u_n\oplus v_n,\dots)$ куб $\{0,1\}_0^{\mathbb{N}}$ является бесконечномерным векторным пространством над полем Галуа $GF(2)$ (в [4] такой куб был назван нулевым слоем куба $\{0,1\}^{\mathbb{N}}$). Базисные векторы с

Malyugin, S.A., Perfect binary codes of infinite length with complete system of triples.

Поступила 26 июля 2017 г., опубликована 14 сентября 2017 г.

единичной i-й координатой обозначаем через $e_i = (0, \dots, 0, \underset{i}{1}, 0, \dots)$. *Носитель* вектора $u \in \{0,1\}^{\mathbb{N}}$ (множество индексов i для которых $u_i = 1$) обозначается через $[u]$. Число ненулевых координат вектора u называется его *весом* и обозначается символом $|u|$. *Расстояние Хэмминга* между векторами $u, v \in \{0,1\}_0^{\mathbb{N}}$ определяется как $|u+v|$.

Определение 1. *Подмножество C в $\{0,1\}_0^{\mathbb{N}}$ называется совершенным двоичным кодом с расстоянием 3, если все шары радиуса 1 (в метрике Хэмминга) с центрами из C попарно не пересекаются и их объединение покрывает куб $\{0,1\}_0^{\mathbb{N}}$.*

Совершенный код в $\{0,1\}_0^{\mathbb{N}}$ называется *линейным*, если он является линейным подпространством в $\{0,1\}_0^{\mathbb{N}}$. Линейный код можно построить следующим образом. Любое натуральное число $n \in \mathbb{N}$ представляем в двоичной системе счисления $n = i_k \dots i_1$ и сопоставляем ему бесконечный вектор-столбец

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

полагая $i_m = 0$ при $m > k$. Для $n, m \in \mathbb{N}$, $n = \dots i_k \dots i_1$, $m = \dots j_k \dots j_1$ полагаем $(\vec{m} \oplus \vec{n})_k = i_k \oplus j_k$, $k \in \mathbb{N}$. Относительно такой побитовой операции сложения множество $\mathbb{N} \cup \{0\}$ тоже становится векторным пространством над полем $GF(2)$. Векторы $\vec{n}$ являются столбцами бесконечномерной проверочной матрицы D, которая выглядит следующим образом:

$$D = \begin{pmatrix} 1 & 0 & 1 & 0 & \cdot \\ 0 & 1 & 1 & 0 & \cdot \\ 0 & 0 & 0 & 1 & \cdot \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

Исходя из этого говорим, что вектор $u = (u_1, \dots, u_n, \dots) \in \{0,1\}_0^{\mathbb{N}}$ принадлежит коду Хэмминга тогда и только тогда, когда

$$\bigoplus_{n \in \mathbb{N}} u_n \cdot \vec{n} = 0$$

(в этой бесконечной сумме только конечное число ненулевых слагаемых). Легко видеть, что так определенное множество векторов u является линейным совершенным кодом в $\{0,1\}_0^{\mathbb{N}}$. Этот код по традиции называется *кодом Хэмминга бесконечной длины* и обозначается символом H^∞, см. [4].

Код Хэмминга H^∞ можно определить по-другому. Для конечных n код Хэмминга H^n длины $n = 2^k - 1$ $(k > 1)$ определяется стандартным образом, см., например [1,2,3]. Добавляя справа к векторам $u \in H^n$ бесконечное число нулевых координат, можно вложить код H^n в нулевой слой $\{0,1\}_0^{\mathbb{N}}$. Это вложение будем обозначать символом $\widetilde{H}^n$. Тогда, так как $\widetilde{H}^n \subset \widetilde{H}^{2n+1}$ $(n = 2^k - 1)$, то можно положить $H^\infty = \bigcup\limits_{k=2}^{\infty} \widetilde{H}^{2^k-1}$.

Изучение кодов бесконечной длины с расстоянием 2 (МДР-кодов, задаваемых квазигруппами с бесконечным числом аргументов) предпринято В. Н. Потаповым в [5]. Им также была предложена задача об изучении совершенных кодов бесконечной длины.

2. Построение нелинейных совершенных кодов бесконечной длины свитчингами компонент

В коде Хэмминга H^∞ рассмотрим подпространство R_i, порожденное всеми векторами веса 3 с i-й координатой, равной единице. Всевозможные смежные классы вида $R_i^u = R_i + u \ \ (u \in H^\infty)$ называются *i-компонентами* кода H^∞, $i \in \mathbb{N}$. Обозначим через $B_1(x)$ шар единичного радиуса с центром в точке $x \in \{0,1\}_0^{\mathbb{N}}$. Основное свойство i-компоненты состоит в следующем:

Лемма 1. *1-окрестности множеств R_i^u и $R_i^u + e_i$ совпадают, то есть*

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

Доказательство. Пусть $v \in B_1(x)$ при некотором $x \in R_i^u$ и $v = x$, тогда $v \in B_1(y)$, если $y = v + e_i$ принадлежит $R_i^u + e_i$. Теперь пусть $v \in B_1(x)$ и $v = x + e_j$ при некотором $j \in \mathbb{N}$. Если $j \neq i$, то вектор $w = e_i + e_j + e_{i \oplus j}$ принадлежит R_i и вектор $y = x + w + e_i$ принадлежит $R_i^u + R_i + e_i = R_i^u + e_i$. Так как $v + y = e_{i \oplus j}$, то $v \in B_1(y)$. Если $j = i$, то $v \in B_1(y)$ при $y = v = x + e_i$ принадлежащем $R_i^u + e_i$. Обратно, предположив, что $v \in B_1(y)$ при некотором $y \in R_i^u + e_i$ и, обращая предыдущие рассуждения, мы получим, что $v \in B_1(x)$ при некотором $x \in R_i^u$. □

Рассмотрим некоторое семейство $\mathcal{B} = \left\{R_{i_1}^{u_1}, R_{i_2}^{u_2}, \dots\right\}$, состоящее из конечного 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^∞ сдвигаются по координатам i_p все компоненты из семейства $\mathcal{B}$. То есть, рассмотрим множество

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

Лемма 2. *Множество $H^\infty(\mathcal{B})$ является совершенным кодом в $\{0,1\}_0^{\mathbb{N}}$.*

Доказательство. Доказательство состоит из следующей цепочки равенств.

$$\{0,1\}_0^{\mathbb{N}} = \bigcup_{x \in H^\infty} B_1(x) = \left(\bigcup_{x \in H^\infty \setminus \bigcup\limits_{p=1}^{m} R_{i_p}^{u_p}} B_1(x)\right) \cup \bigcup_{p=1}^{m} \left(\bigcup_{x \in R_{i_p}^{u_p}} B_1(x)\right) =$$

$$= \left(\bigcup_{x \in H^\infty \setminus \bigcup\limits_{p=1}^{m} R_{i_p}^{u_p}} B_1(x)\right) \cup \bigcup_{p=1}^{m} \left(\bigcup_{x \in R_{i_p}^{u_p} + e_{i_p}} B_1(x)\right) = \bigcup_{x \in H^\infty(\mathcal{B})} B_1(x),$$

при этом все шары $B_1(x)$ при различных x в каждом из этих равенств попарно не пересекаются. □

Будем говорить, что код $H^\infty(\mathcal{B})$ построен из кода Хэмминга H^∞ *сдвигами* (или *свитчингами*) компонент из семейства $\mathcal{B}$.

Для кодов конечной длины леммы 1 и 2 хорошо известны, см. [1, 2, 6, 7, 8]. Из леммы 2 следует, что нелинейные совершенные коды можно строить, одновременно сдвигая в коде Хэмминга H^∞ не только конечные но и бесконечные семейства компонент.

3. Разреженные семейства компонент

Далее мы будем рассматривать в коде Хэмминга H^∞ только семейства непересекающихся компонент, для которых $i_p = p$ ($p \in \mathbb{N}$), т. е. $\mathcal{B} = \{R_1^{u_i}, R_2^{u_2}, \dots\}$ (для каждого $i \in \mathbb{N}$ в семействе $\mathcal{B}$ имеется ровно одна i-компонента).

Для $n = 2^k - 1$ в коде Хэмминга H^{2n+1} длины $2n+1$ рассмотрим подкод $\widetilde{H}^n$, изоморфный коду H^n. Для векторов $\widetilde{u} \in \widetilde{H}^n$ ($\widetilde{u} = (u_1, \dots, u_{2n+1})$) все координаты $u_i = 0$ при $n < i \le 2n+1$. Пусть $1 \le i, j \le n$ и $\widetilde{u}, \widetilde{v} \in \widetilde{H}^n$. Рассмотрим в коде H^{2n+1} две компоненты $R_i^{\widetilde{u}}$, $R_j^{\widetilde{v}}$. Тогда пересечения $\widetilde{R}_i^{\widetilde{u}} = R_i^{\widetilde{u}} \cap \widetilde{H}^n$, $\widetilde{R}_j^{\widetilde{v}} = R_j^{\widetilde{v}} \cap \widetilde{H}^n$ будут компонентами в коде $\widetilde{H}^n$.

Лемма 3. *Если компоненты $R_i^{\widetilde{u}}$ и $R_j^{\widetilde{v}}$ пересекаются, то компоненты $\widetilde{R}_i^{\widetilde{u}}$ и $\widetilde{R}_j^{\widetilde{v}}$ тоже пересекаются.*

Доказательство. Из $R_i^{\widetilde{u}} \cap R_j^{\widetilde{v}} \ne \emptyset$ следует, что $\widetilde{u} + \widetilde{v} \in R_i + R_j$. Любой вектор $x \in R_i$ является конечной суммой векторов веса 3 с единичной i-й координатой. Сумму тех векторов веса 3, носители которых входят в множество $\{1, \dots, n\}$ обозначим через x'. Носители оставшихся векторов веса 3 пересекаются с $\{1, \dots, n\}$ только по одному элементу i. Их сумму обозначим через x''. Если этих оставшихся векторов веса 3 было чётное число, то носитель $[x'']$ не пересекается с $\{1, \dots, n\}$, в противном случае будет $[x''] \cap \{1, \dots, n\} = \{i\}$. Мы разложили x в виде суммы $x = x' + x''$. Аналогично, любой вектор $y \in R_j$ разлагается в сумму $y = y' + y''$, где $[y'] \subset \{1, \dots, n\}$ а $[y''] \cap \{1, \dots, n\} = \emptyset$ в чётном случае, либо $[y''] \cap \{1, \dots, n\} = \{j\}$ в нечётном случае. Если $\widetilde{u} + \widetilde{v} = x + y$ ($x \in R_i$, $y \in R_j$), то $\widetilde{u} + \widetilde{v} = (x' + y') + (x'' + y'')$. Так как $[\widetilde{u} + \widetilde{v}], [x' + y'] \subset \{1, \dots, n\}$, то $[x'' + y''] \subset \{1, \dots, n\}$. Если x'', y'' являются суммами нечётного числа троек, то $[x'' + y''] \cap \{1, \dots, n\} = \{i, j\}$. В коде с расстоянием 3 это невозможно. Поэтому x'', y'' представляются суммами чётного числа троек и $x'' + y'' = 0$. То есть, $\widetilde{u} + \widetilde{v} = x' + y' \in \widetilde{R}_i + \widetilde{R}_j$, что означает пересекаемость компонент $\widetilde{R}_i^{\widetilde{u}}$ и $\widetilde{R}_j^{\widetilde{v}}$. □

Далее мы будем применять лемму 3 в отрицательной форме, т. е., если компоненты $\widetilde{R}_i^{\widetilde{u}}$ и $\widetilde{R}_j^{\widetilde{v}}$ не пересекаются, то и компоненты $R_i^{\widetilde{u}}$, $R_j^{\widetilde{v}}$ тоже не пересекаются.

В подкоде $\widetilde{H}^n$ кода Хэмминга H^{2n+1} рассмотрим ещё один подкод $\widetilde{H}^{\frac{n-1}{2}}$, изоморфный коду $H^{\frac{n-1}{2}}$.

Лемма 4. *Пусть $\widetilde{\mathcal{B}} = \{\widetilde{R}_1^{\widetilde{u}_1}, \dots, \widetilde{R}_n^{\widetilde{u}_n}\}$ — семейство непересекающихся компонент кода $\widetilde{H}^n$ ($n = 2^k - 1$, $k \ge 5$) и $R_1^{\widetilde{u}_1}, \dots, R_n^{\widetilde{u}_n}$ — компоненты кода H^{2n+1}, для которых $R_i^{\widetilde{u}_i} \cap \widetilde{H}^n = \widetilde{R}_i^{\widetilde{u}_i}$ ($i = 1, \dots, n$). Тогда существуют компоненты $R_{n+1}^{\widetilde{u}_{n+1}}, \dots, R_{2n+1}^{\widetilde{u}_{2n+1}}$ такие, что семейство $\mathcal{B} = \{R_1^{\widetilde{u}_1}, \dots, R_{2n+1}^{\widetilde{u}_{2n+1}}\}$ состоит из попарно не пересекающихся компонент кода H^{2n+1} и $R_i^{\widetilde{u}_i} \cap \widetilde{H}^{\frac{n-1}{2}} = \emptyset$ ($i = n+1, \dots, 2n+1$).*

Доказательство. Требуемое семейство компонент будем строить по индукции. Допустим, что для $n \le s < 2n+1$ уже найдено требуемое семейство компонент $\mathcal{B}_s = \{R_1^{\widetilde{u}_1}, \dots, R_s^{\widetilde{u}_s}\}$. Код H^{2n+1} относительно подпространства R_{s+1} разбивается на смежные классы $R_{s+1} + u$, $u \in H^{2n+1}$. Число таких смежных классов равно $2^{n-\log_2(n+1)}$. Каждое множество $R_i^{\widetilde{u}_i} + R_{s+1}$ разбивается на $2^{\frac{n-1}{2}}$ этих смежных классов. Поэтому множество $\bigcup\limits_{i=1}^{s}(R_i^{\widetilde{u}_i} + R_{s+1})$ является объединением не более чем $s \cdot 2^{\frac{n-1}{2}}$ смежных классов. Число элементов кода $\widetilde{H}^{\frac{n-1}{2}}$ равно $2^{\frac{n-1}{2}-\log_2\frac{n+1}{2}}$. Если

$$2^{n-\log_2(n+1)} > s \cdot 2^{\frac{n-1}{2}} + 2^{\frac{n-1}{2}-\log_2\frac{n+1}{2}},$$

то существует смежный класс R_{s+1}^u не пересекающийся с множеством $\bigcup\limits_{i=1}^{s}(R_s^{\widetilde{u}_s} + R_{s+1})$ и с кодом $\widetilde{H}^{\frac{n-1}{2}}$. При $n = 2^k - 1$ это возможно, если $k \ge 5$. Известно, что компонента R_{s+1}^u кода H^{2n+1} пересекается с кодом предыдущей размерности $\widetilde{H}^n$ по единственному элементу $\widetilde{u}_{s+1}$, см. лемму 4 из [3] или лемму 5 этой работы. Поэтому компонента $R_{s+1}^{\widetilde{u}_{s+1}} = R_{s+1} + u$ будет искомой. □

Определение 2. *Семейство непересекающихся компонент $\mathcal{B} = \{R_1^{u_1}, R_2^{u_2}, \dots\}$ кода H^∞ называем разреженным, если существует номер k_0 такой, что $R_i^{u_i} \cap \widetilde{H}^{2^k-1} = \emptyset$ для всех $i > 2^{k+1}-1$ и всех $k \ge k_0$.*

Известно, что при $k \ge 5$ в коде Хэмминга H^{2^k-1} существует семейство $\mathcal{B} = \{R_1^{u_1}, \dots, R_n^{u_n}\}$, состоящее из $n = 2^k - 1$ попарно не пересекающихся i-компонент $R_i^{u_i}$ $(1 \le i \le n)$, см.,например, [1,8]. Поэтому, применяя индуктивно лемму 3 (в отрицательной форме) и лемму 4 начиная с $n = 31$, мы получаем

Следствие 1. *В коде Хэмминга бесконечной длины H^∞ существуют разреженные семейства компонент.*

4. Коды с полной системой троек

Определение 3. *Говорим, что совершенный код $C \subset \{0,1\}_0^{\mathbb{N}}$ имеет полную систему троек, если для любого вектора $u \in \{0,1\}_0^{\mathbb{N}}$ веса 3 существуют два кодовых вектора $v, w \in C$ такие, что $u = v + w$, т. е. $u \in C + C$.*

Для построения кодов с полной системой троек нам потребуется следующая

Лемма 5. *Для любого подкода $\widetilde{H}^n \subset H^\infty$ $(n = 2^k - 1)$ и любой i-компоненты R_i^u с $i > n$ пересечение $R_i^u \cap \widetilde{H}^n$ состоит из не более чем одного элемента. Если $n < i \le 2n+1$ и $u \in \widetilde{H}^{2n+1}$, то пересечение $R_i^u \cap \widetilde{H}^n$ состоит в точности из одного элемента.*

Доказательство. Пусть $x, y \in R_i^u \cap \widetilde{H}^n$. Тогда $x + y \in R_i \cap \widetilde{H}^n$ и носитель $[x + y]$ входит в $\{1, \dots, n\}$. Так как вектор $x + y$ является суммой векторов веса 3 с единичной i-й координатой, то $j \in [x + y]$ тогда и только тогда, когда $k = i \oplus j \in [x + y]$. Так как всегда один из номеров j, k больше n, то должно выполняться $[x + y] = \emptyset$, т. е. $x = y$. Мы доказали, что пересечение $R_i^u \cap \widetilde{H}^n$ состоит из не более чем одного элемента.

Допусти теперь, что $n < i \le 2n+1$ и $u \in \widetilde{H}^{2n+1}$. Если $j \in [u] \setminus \{1, \dots, n\}$ то вектор $u_1 = u + e_i + e_j + e_{i\oplus j}$ тоже принадлежит компоненте R_i^u. Так как $n <$

$i, j \le 2n+1$, то $i \oplus j \le n$. Поэтому число элементов не равных i в множестве $[u_1] \setminus \{1, \dots, n\}$ на единицу меньше, чем число таких элементов в множестве $[u] \setminus \{1, \dots, n\}$. Продолжая индуктивно этот процесс, мы через конечное число шагов найдём вектор $u_k \in R_i^u$ такой, что либо $[u_k] \subset \{1, \dots, n\}$, либо $[u_k] \setminus \{1, \dots, n\} = \{i\}$. Так как вектор h с носителем $[h] = \{1, \dots, n\}$ принадлежит коду Хэмминга $\widetilde{H}^n \subset H^\infty$ и расстояние между векторами u_k и h не больше единицы, то последний вариант невозможен. □

Определение 4. *Семейство непересекающихся компонент $\mathcal{B} = \{R_1^{u_1}, R_2^{u_2}, \dots\}$ кода H^∞ называем неплотным, если существует номер k_0 такой, что для любого $k \ge k_0$ количество i-компонент $R_i^{u_i}$ при $i > 2^k - 1 = n$, пересекающихся с кодом $\widetilde{H}^n$, меньше, чем $2^{\frac{n-1}{2}} - (n-1)2^{\frac{n+1}{4}}$.*

Из леммы 5 следует, что при $i > n$ количество i-компонент, пересекающихся с подкодом $\widetilde{H}^n$ не превышает $n+1$. Так как $n+1 < 2^{\frac{n-1}{2}} - (n-1)2^{\frac{n+1}{4}}$ при $n \ge 31$, то из определений 2 и 4 следует, что любое разреженное семейство компонент является неплотным.

Теорема 1. *Если семейство компонент $\mathcal{B}$ является неплотным, то код $C = H^\infty(\mathcal{B})$ имеет полную систему троек.*

Доказательство. Пусть вектор $u \in \{0,1\}_0^{\mathbb{N}}$ имеет вес 3 и $[u] = \{j, k, l\}$. Допустим, что $u \notin H^\infty$. Тогда существует единственный номер $i \in \mathbb{N}$, для которого вектор v с носителем $[v] = \{i, j, k, l\}$ принадлежит коду Хэмминга H^∞. Существует такой номер $k \ge k_0$, что $j, j, k, l \le 2^k - 1 = n$ и подкод $\widetilde{H}^n$ содержит вектор u_i из компоненты $R_i^{u_i}$. Для любого $s \in \mathbb{N}$ обозначим $\widetilde{R}_s^{u_s} = R_s^{u_s} \cap \widetilde{H}^n$. Если $s = i$, то $\widetilde{R}_i^{u_i}$ является i-компонентой кода $\widetilde{H}^n$. Если $1 \le s \le n$, и $s \ne i$, то $\widetilde{R}_s^{u_s}$ либо пусто, либо является s-компонентой кода $\widetilde{H}^n$. Если $n < s$, то в силу леммы 5, $\widetilde{R}_s^{u_s}$ либо пусто, либо состоит из одного элемента $\widetilde{u}_s \in \widetilde{H}^n$. В коде $\widetilde{H}^n$ рассмотрим ещё одну i-компоненту $\widetilde{R}_i^{u_i+v}$. Эта компонента не пересекается с компонентой $\widetilde{R}_i^{u_i}$, так как $v \notin R_i$. Если $1 \le s \le n$, $s \ne i$ и $\widetilde{R}_s^{u_s}$ является s-компонентой кода $\widetilde{H}^n$, то пересечение $\widetilde{R}_s^{u_s} \cap \widetilde{R}_i^{u_i+v}$ либо пусто, либо состоит из $2^{\frac{n+1}{4}}$ элементов. Всего таких компонент с непустым пересечением не больше $n-1$. При $s > n$ непустые пересечения компонент $R_s^{u_s}$ с кодом $\widetilde{H}^n$ могут быть только одноточечные. Поэтому, в силу определения 4, число элементов в пересечении компоненты $\widetilde{R}_i^{u_i+v}$ с множеством $\bigcup\limits_{i=1}^{\infty} R_i^{u_i}$ меньше, чем $(n-1)2^{\frac{n+1}{4}} + \left(2^{\frac{n-1}{2}} - (n-1)2^{\frac{n+1}{4}}\right) = 2^{\frac{n-1}{2}}$. Значит существует вектор $w \in \widetilde{R}_i^{u_i+v} \setminus \bigcup\limits_{i=1}^{\infty} R_i^{u_i}$. Это означает, что $w \in H^\infty(\mathcal{B}) = C$ и $v + w \in \widetilde{R}_i^{u_i}$. Поэтому $w' = v + w + e_i \in R_i^{u_i} + e_i \subset C$ и $u = v + e_i = w + w' \in C + C$.

Осталось рассмотреть случай, когда $u \in H^\infty$. Существует $k \ge k_0$ такое, что $u \in \widetilde{H}^n$ $(n = 2^k - 1)$. Число элементов в множестве $\widetilde{H}^n \setminus \bigcup\limits_{i=1}^{\infty} R_i^{u_i}$ больше, чем $2^{n-\log_2(n+1)} - (n-1)2^{\frac{n-1}{2}} + (n-1)2^{\frac{n+1}{4}}$, что составляет больше половины числа элементов всего линейного кода $\widetilde{H}^n$, если $n \ge 31$. Следовательно, существуют два вектора $w, w' \in \widetilde{H}^n \setminus \bigcup\limits_{i=1}^{\infty} R_i^{u_i} \subset C$, для которых $u = w + w' \in C + C$. □

5. Систематические и несистематические коды бесконечной длины

Определение 5. *Совершенный двоичный код $C \subset \{0,1\}_0^{\mathbb{N}}$ 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 $x \in \{0,1\}_0^{N_1}$ существует единственный вектор $y \in \{0,1\}_0^{N_2}$ 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 принято называть *информационным*, а множество N_2 — *проверочным*. Если в определении 5 ввести обозначение $y = f(x)$, то мы получим отображение $f\colon \{0,1\}_0^{N_1} \to \{0,1\}_0^{N_2}$ такое, что систематический код C будет графиком этого отображения.

Далее будем считать, что пространства $\{0,1\}_0^{N_1}$, $\{0,1\}_0^{N_2}$ вложены в $\{0,1\}_0^{\mathbb{N}}$, доопределяя недостающие координаты векторов $x \in \{0,1\}_0^{N_1}$, $y \in \{0,1\}_0^{N_2}$ нулевыми значениями.

В следующей теореме мы отметим несколько общих свойств систематических кодов.

Теорема 2. (1) *Линейный код Хэмминга H^∞ 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 $f : N_1 \to N_2$, графиком которого является систематический код C, сюръективно и прообраз $f^{-1}(y)$ любой точки $y \in N_2$ имеет бесконечную мощность.*

Доказательство. (1): В качестве проверочного множества для кода H^∞ возьмём $N_2 = \{1, 2, \dots, 2^k, \dots\}$ и положим $N_1 = \mathbb{N} \setminus N_2$. Пусть $x \in \{0,1\}_0^{N_1}$. Представим x в виде $x = e_{i_1} + \cdots + e_{i_m}$. Так как $x \in \{0,1\}^{N_1}$, то $[x] = \{i_1, \dots, i_m\} \subset N_1$. Положим $j = i_1 \oplus \cdots \oplus i_m$. Мы рассматриваем $\mathbb{N} \cup \{0\}$ как векторное пространство с побитовой операцией сложения $\oplus$, в котором множество N_2 является базисом. То есть, $j = j_1 \oplus \cdots \oplus j_n$, $j_1, \dots j_n \in N_2$. Полагаем $y = f(x) = e_{j_1} + \cdots + e_{j_n}$. Так как $i_1 \oplus \cdots \oplus i_m \oplus j_1 \cdots \oplus j_n = 0$, то по определению кода Хэмминга H^∞, $(x, f(x)) = x + y = e_{i_1} + \cdots + e_{i_m} + e_{j_1} + \cdots + e_{j_n} \in H^\infty$.

(2): Пусть совершенный код $C \subset \{0,1\}_0^{\mathbb{N}}$ является систематическим с информационным и проверочным множествами N_1 и N_2. Если предположить, что информационное множество N_1 конечное, то можно будет получить только конечное множество векторов вида $(x, f(x)) = x + f(x)$, составляющих график кода C. Это противоречит бесконечности совершенного кода C. Допустим, что множество N_2 является конечным. Так как множество N_1 бесконечно, то $N_1 = \{i_1, i_2, \dots\}$. Все векторы e_{i_1}, $e_{i_2}, \dots$ принадлежат $\{0,1\}_0^{N_1}$. Для каждого такого вектора e_{i_k} существует (единственный) вектор $f(e_{i_k}) = y_k \in \{0,1\}_0^{N_2}$, для которого $e_{i_k} + y_k \in C$. Так как пространство $\{0,1\}_0^{N_2}$ конечномерно, то существует только конечное число различных векторов y_k. Существует два различных индекса $k, l \in \mathbb{N}$, для которых $y_k = y_l$. Отсюда следует, что векторы $u = e_{i_k} + y_k, v = e_{i_l} + y_l$ находятся на расстоянии Хэмминга 2 друг от друга, что противоречит включению $u, v \in C$.

(3): Пусть совершенный код C является систематическим с информационным и проверочным множествами N_1 и N_2. Докажем, что отображение $f : \{0,1\}_0^{N_1} \to \{0,1\}_0^{N_2}$, графиком которого является код C, сюръективно. Допустим, что $0 \in C$. Рассмотрим любой ненулевой вектор $y \in \{0,1\}_0^{N_2}$, $y =$

$e_{j_1}+\cdots+e_{j_n}$ $(j_i,\ldots,j_n\in N_2)$. Допустим, что $y\in C$. Тогда вектор $0\in\{0,1\}_0^{N_1}$ 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 существует базисный вектор e_i, для которого $e_i+y\in C$. Из предыдущего рассуждения следует, что $i\notin N_2$. Поэтому $i\in N_1$ и $f(e_i)=y$. Допустим теперь, что $0\notin C$. Этот случай сводится к предыдущему. Существует номер $i\in\mathbb{N}$, для которого базисный вектор $e_i\in C$. Совершенный код $C'=C+e_i$, содержащий нулевой вектор, тоже систематический с теми же информационными и проверочными множествами N_1,N_2, являющийся графиком функции $f'(x)=f(x+e_i)$, если $i\in N_1$, $f'(x)=f(x)+e_i$, если $i\in N_2$.

В случае $0\in C$ докажем теперь, что прообраз нуля $f^{-1}(0)$ бесконечен. Рассмотрим три различных номера $j_1,j_2,j_3\in N_2$ и вектор $y=e_{j_1}+e_{j_2}+e_{j_3}\in\{0,1\}_0^{N_2}$. Очевидно, $y\notin C$ (иначе $f(0)$ будет определяться неоднозначно). Существует базисный вектор e_i, для которого $z=e_i+y\in C$. По той же причине $i\notin N_2$. Рассмотрим другой систематический код $C'=C+z$ и вектор $y'=e_{j_2}+e_{j_3}$. Аналогичным образом, для вектора y' существует базисный вектор $e_{i'}$, для которого $z'=e_{i'}+y'\in C'$. Очевидно $i'\notin N_2$ и вектор $u=z+z'=e_i+e_{i'}+e_{j_1}\in C$. 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 $u_n=e_{i_n}+e_{i'_n}+e_{j_1}$ $(n\in\mathbb{N})$ веса 3, принадлежащих коду C, при этом $i_n,i'_n\in N_1$, $i_n\neq i'_n$ и $i_n,i'_n\to\infty$. Векторы $v_n=u_n+u=e_{i_n}+e_{i'_n}+e_i+e_{i'}$ $(n\in\mathbb{N})$ принадлежат коду C и, по построению, $f(v_n)=0$.

Теперь докажем, что для любого вектора $y\in\{0,1\}_0^{N_2}$ прообраз $f^{-1}(y)$ имеет бесконечную мощность. Из уже доказанной сюръективности отображения f следует существование вектора $w\in\{0,1\}_0^{N_1}$, 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 $f'(x)=f(x+w)+y$, $x\in\{0,1\}_0^{N_1}$. Для него тоже существует бесконечная последовательность различных векторов $v'_n\in C'$, для которых $f'(v'_n)=0$. По построению, для последовательности $w_n=v'_n+w\in C$ получим $f(w_n)=y$. Случай, когда $0\notin C$, как было показано выше, можно отдельно не рассматривать. □

Лемма 6. *Если совершенный код $C\subset\{0,1\}_0^{\mathbb{N}}$ имеет полную систему троек, то он несистематический.*

Доказательство. Допустим, что код C систематический с информационными и проверочными множествами N_1,N_2 и функцией $f:\{0,1\}_0^{N_1}\to\{0,1\}_0^{N_2}$, 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 $w=e_{i_1}+e_{i_2}+e_{i_3}\in\{0,1\}_0^{N_2}$. Существуют 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 $x,x'\in\{0,1\}_0^{N_1}$, $y=f(x)\in\{0,1\}_0^{N_2}$, $y'=f(x')\in\{0,1\}_0^{N_2}$. Так как $z+z'\in\{0,1\}_0^{N_2}$, то $x=x'$ и $y+y'=w\neq 0$, что противоречит однозначности функции f. □

Непосредственно из определения 5, теоремы 1 и леммы 6 получаем

Следствие 2. *Если $\mathcal{B} = \{R_1^{u_1}, R_2^{u_2}, \dots\}$ — достаточно разреженное семейство компонента кода Хэмминга H^∞, то совершенный код $C = H^\infty(\mathcal{B})$ является несистематическим.*

Далее мы покажем, что требование неплотности семейства компонент $\mathcal{B}$ в теореме 1 и следствии 2 является оправданным. Для $n = 2^k - 1$ рассмотрим в коде Хэмминга H^{2n+1} длины $2n+1$ подкод $\widetilde{H}^n$ предыдущей размерности. Для $1 \le i \le n$ рассмотрим в коде H^{2n+1} i-компоненту $R_i^{\widetilde{u}}$ ($\widetilde{u} \in \widetilde{H}^n$), а в подкоде $\widetilde{H}^n$ компоненту $\widetilde{R}_i^{\widetilde{u}} = R_i^{\widetilde{u}} \cap \widetilde{H}^n$. Следующая лемма является существенным дополнением к лемме 3.

Лемма 7. *Если $\widetilde{v} \in \widetilde{H}^n \setminus \widetilde{R}_i^{\widetilde{u}}$ и $n < j \le 2n+1$, то компоненты $R_i^{\widetilde{u}}$ и $R_j^{\widetilde{v}}$ не пересекаются.*

Доказательство. Осуществляя перенос обеих компонент на вектор $\widetilde{v}$, можно без ограничения общности считать, что $\widetilde{v} = 0$. Допустим, что существует вектор $w \in R_j \cap R_i^{\widetilde{u}}$, т. е. $\widetilde{u} + w \in R_i$. Рассмотрим вектор $\widetilde{w}$ с носителем $[\widetilde{w}] = [w] \cap \{1, \dots, n\}$ и рассмотрим вектор $w' = \sum\limits_{k \in [\widetilde{w}]} e_{j \oplus k}$. Так как w является суммой всех векторов веса 3 вида $e_j + e_k + e_l$, где $k \in [\widetilde{w}]$, $l = j \oplus k$, то $w = \widetilde{w} + w'$, если вес $|\widetilde{w}|$ чётен и $w = \widetilde{w} + w' + e_j$, если вес $\widetilde{w}$ нечётен. Пусть вес $|\widetilde{w}| = |w'|$ чётен. Из $\widetilde{u} + w \in R_i$ следует, что $l \in [w']$ тогда и только тогда, когда $i \oplus l \in [w']$. То есть $j \oplus l \in [\widetilde{w}]$ тогда и только тогда, когда $i \oplus l \oplus j \in [\widetilde{w}]$. Так как $j \notin [w']$, то $l \ne j$ для всех $l \in [w']$ и $i \notin [\widetilde{w}]$, иначе будет $i \oplus j \in [w']$, что влечёт $j = i \oplus (i \oplus j) \in [w']$. Обозначив $l' = i \oplus j$, получаем, что $l' \in [\widetilde{w}]$ тогда и только тогда, когда $i \oplus l' \in [\widetilde{w}]$. Это означает, что $\widetilde{w}$ является суммой *чётного* числа векторов веса 3 с единичной i-й координатой, т. е. $\widetilde{w} \in \widetilde{R}_i$. Так как $\widetilde{u} + w = \widetilde{u} + \widetilde{w} + w' \in R_i$, то $\widetilde{u} \in \widetilde{R}_i$. Это противоречит условию $0 \notin \widetilde{R}_i^{\widetilde{u}}$. Допустим, что вес $|\widetilde{w}| = |w'|$ нечётен. В этом случае заменяем вектор w на вектор $w_1 = w + e_i + e_j + e_{i \oplus j}$, который тоже принадлежит пересечению компонент $R_j \cap R_i^{\widetilde{u}}$ и для которого векторы $\widetilde{w}_1, w_1'$ будут иметь чётные веса. Мы полностью свели этот случай к предыдущему. □

Пусть $N_2 = \{1, 2, \dots, 2^k, \dots\}$, $N_1 = \mathbb{N} \setminus N_2$. Любой вектор $x \in \{0,1\}_0^{\mathbb{N}}$ однозначно разлагается на сумму проекций $x = x_1 + x_2$, $x_1 \in \{0,1\}_0^{N_1}$, $x_2 \in \{0,1\}_0^{N_2}$. 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 $R_j^{u_j}$.

Мы используем леммы 3 и 7 для построения семейства непересекающихся компонент $\mathcal{B} = \{R_1^{u_1}, R_2^{u_2}, \dots\}$, в котором для каждого $i \in \mathbb{N}$ имеется ровно по одной i-компоненте $R_i^{u_i}$ и которое обладает совершенно неожиданным свойством.

Лемма 8. *В коде Хэмминга H^∞ существует семейство попарно не пересекающихся компонент $\mathcal{B} = \{R_1^{u_1}, R_2^{u_2}, \dots\}$, для которого $H^\infty = \bigcup\limits_{i=1}^{\infty} R_i^{u_i}$ 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 4 мы будем выбирать компоненты с помощью индуктивного процесса.

(a). Пусть $\widetilde{\mathcal{B}}_n = \{\widetilde{R}_1^{\widetilde{u}_1}, \dots, \widetilde{R}_n^{\widetilde{u}_n}\}$ — семейство непересекающихся компонент кода $\widetilde{H}^n$ $(n = 2^k - 1)$ и $R_1^{\widetilde{u}_1}, \dots, R_n^{\widetilde{u}_n}$ — компоненты кода H^{2n+1}, для которых $R_i^{\widetilde{u}_i} \cap \widetilde{H}^n = \widetilde{R}_i^{\widetilde{u}_i}$ $(i = 1, \dots, n)$. В подкоде $\widetilde{H}^n$ рассмотрим его подкод $\widetilde{H}^m$ с наименьшим номером m, для которого $\widetilde{H}^m \setminus \left(\bigcup_{i=1}^{n} \widetilde{R}_i^{\widetilde{u}_i} \right) \neq \emptyset$. Выберем любой вектор $\widetilde{u}_{n+1} \in \widetilde{H}^m \setminus \left(\bigcup_{i=1}^{n} \widetilde{R}_i^{\widetilde{u}_i} \right)$ и рассмотрим в коде Хэмминга H^{2n+1} семейство компонент $\mathcal{B}_{n+1} = \{R_1^{u_1}, R_2^{u_2}, \dots, R_{n+1}^{\widetilde{u}_{n+1}}\}$. В силу лемм 3 и 7 это семейство состоит из попарно не пересекающихся компонент, при этом мощность множества $\widetilde{H}^m \setminus \left(\bigcup_{i=1}^{n+1} R_i^{\widetilde{u}_i} \right)$ уменьшилась на единицу. Так же как и в доказательстве леммы 4 расширяем это семейство до семейства непересекающихся компонент $\mathcal{B}_{2n+1} = \{R_1^{\widetilde{u}_1}, \dots, R_{2n+1}^{\widetilde{u}_{2n+1}}\}$.

Покажем, что при этом расширении мы можем выбирать компоненты так, чтобы удовлетвоить условиям на информационное расстояние. Допустим, что для $n < s < 2n+1$ уже найдено требуемое семейство компонент $\mathcal{B}_s = \{R_1^{\widetilde{u}_1}, \dots, R_s^{\widetilde{u}_s}\}$. Код H^{2n+1} относительно подпространства R_{s+1} разбивается на $2^{n-\log_2(n+1)}$ смежных класса $R_{s+1} + u$, $u \in H^{2n+1}$. Каждое множество $R_i^{\widetilde{u}_i} + R_{s+1}$ разбивается на $2^{\frac{n-1}{2}}$ смежных классов (см. доказательство леммы 4). Поэтому число смежных классов в коде H^{2n+1} по подпространству $R_i + R_{s+1}$ равно $2^{\frac{n+1}{2} - \log_2(n+1)}$. Оценим количество векторов кода H^{2n+1}, информационный вес которых не превышает 2. Количество векторов, носитель которых входит в множество $\widetilde{N}_2 = \{1, 2, \dots, 2^{k+1}\}$ равно $2^{k+1} = 2n+2$, а количество векторов веса не больше чем 2, носители которых входят в множество $\{1, \dots, 2n+1\} \setminus \widetilde{N}_2$ равно $2n - k + \binom{2n-k}{2}$. То есть, общее количество векторов кода H^{2n+1}, информационный вес которых не больше чем 2, меньше $(2n+2)(2n-k+\binom{2n-k}{2})$. Поэтому, если $(2n+2)(2n-k+\binom{2n-k}{2}) < 2^{\frac{n+1}{2} - \log_2(n+1)}$, то существует по крайней мере $2^{n-\log_2(n+1)} - (2n+2)(2n-k+\binom{2n-k}{2})2^{\frac{n-1}{2}}$ различных $(s+1)$-компонент вида R_{s+1}^u, информационное расстояние которых до компоненты $R_i^{\widetilde{u}_i}$ больше двух. Отсюда следует, что общее число различных компонент вида R_{s+1}^u, информационное расстояние которых до каждой компоненты $R_i^{\widetilde{u}_i}$ $(i = 1, \dots, s)$ больше двух, не меньше, чем $2^{n-\log_2(n+1)} - s(2n+2)(2n-k+\binom{2n-k}{3}2^{\frac{n-1}{2}}$. Это число компонент будет положительно, если

$$2^{n-\log_2(n+1)} - 2n(2n+2)\binom{2n-k}{2}2^{\frac{n-1}{2}} > 0.$$

Это неравенство выполняется начиная с $n = 2^k - 1$ $(k \geq 6)$. Одну из таких компонент R_{s+1}^u обозначим через $R_{s+1}^{\widetilde{u}_{s+1}}$ (где можно выбрать $[\widetilde{u}_{s+1}] \subset \{1, \dots, n\}$).

Пункт (a) вышеприведённого доказательства гарантирует индуктивный переход от номера $n = 2^k - 1$ к следующему номеру $2n + 1 = 2^{k+1} - 1$. Нам осталось только определить базу индукции.

(b). В качестве базы рассмотрим код $\widetilde{H}^{63}$, вложенный в следующий код Хэмминга H^{127}. Компонента $\widetilde{R}_1$ не является информационной, поэтому мы выбираем $\widetilde{u}_1 \in \widetilde{H}^{63}$ произвольным образом и определяет первую компоненту $\widetilde{R}_1^{\widetilde{u}_1}$. Далее, следуя пункту (a), индукцией по $s = 2, \dots, 63$ выбираем компоненты

$\widetilde{R}_s^{\widetilde{u}_s}$, каждая из которых находится на информационном расстоянии бельше чем 2 от компонент, выбранных на предыдущих шагах.

Итак, начиная с базового кода H^{127}, в котором вложен код $\widetilde{H}^{63}$ с уже выбранными в нём компонентами $\{\widetilde{R}_1^{\widetilde{u}_1}, \dots, \widetilde{R}_{63}^{\widetilde{u}_{63}}\}$, мы применяем пункт (а) индуктивно по переменной $n = 2^k - 1$, $k \geq 6$ 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 $R_i^{\widetilde{u}_i}$ и $R_j^{\widetilde{u}_j}$, $i < j$ ($j \in N_1$), больше двух. □

Теорема 3. *Пусть бесконечное семейство непересекающихся компонент $\mathcal{B} = \{R_1^{u_1}, R_2^{u_2}, \dots\}$ является покрытием кода Хэмминга H^∞ 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 $C = H^\infty(\mathcal{B})$ будет иметь неполную систему троек.*

Доказательство. Рассмотрим любой вектор x веса 3, носитель которого входит в N_2. Предположим, что существуют два вектора $u, v \in H^\infty(\mathcal{B})$, для которых $u + v = x$. Если $u, v \in R_i^{u_i} + e_i$ для некоторой i-компоненты семейства $\mathcal{B}$, то $u + v \in H^\infty$ и поэтому $\bigoplus\limits_{i \in [u+v]} i = 0$. Следовательно, $[u + v]$ не может входить в информационное множество N_2, являющееся базисом векторного пространства $\mathbb{N} \cup \{0\}$. Пусть теперь $u \in R_i^{u_i} + e_i$, $v \in R_j^{u_j} + e_j$ при $i < j$ и допустим, что $[u + v] \subset N_2$. Это означает, что $u + e_i \in R_i^{u_i}$, $v + e_j \in R_j^{u_j}$. Если $i, j \in N_2$, то из $[u + v] \subset N_2$ следует $[u + v + e_i + e_j] \subset N_2$. Это противоречит тому, что $u+v+e_i+e_j \in H^\infty$. Если $i, j \in N_1$, то $u+v+e_i+e_j \in H^\infty$. 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, $u+v+e_i+e_j \in H^\infty$ и $[u+v+e_j] \subset N_2$. Так как $i = \bigoplus\limits_{s \in [u+v+e_j]} s$, то для любого $s \in [u+v+e_j]$ должно выполняться $s < i$. Поэтому из $i < j$ следует, что $j \in [u+v+e_j]$. Это означает, что множество $[u+v+e_j]$ состоит только из двух номеров $s_1, s_2 \in N_2$ и $i = s_1 \oplus s_2$. То есть, вектор веса 3 $u + v + e_i + e_j$ 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 сумма кодов $C + C$ не содержит ни одного вектора веса 3, носитель которого входит в N_2. □

Замечание. Теорема 3 показывает, что условие неплотности семейства компонент в теореме 1 является оправданным. Без этого условия теорема 1 перестаёт быть верной.

Остаётся открытым вопрос о существовании такого семейства непересекающихся компонент $\mathcal{B} = \{R_1^{u_1}, R_2^{u_2}, \dots\}$, покрывающего код Хэмминга H^∞, для которого код $H^\infty(\mathcal{B})$ является систематическим.

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] Vasil'ev Yu. L., *On Nongroup Close-Packed Codes*, Problems of Cybernetics, **8**, (1962), 337–339. Zbl 0202.50305
[3] Malyugin S. A., *On enumeration of the perfect binary codes of length 15*, Discrete Applied Mathematics, **135**:1–3 (2004), 161–181. MR2046666
[4] Malyugin S. A., *Perfect binary codes of infinite length*, J. Appl. Indust. Math., **8**:4 (2017), 552–556.
[5] Potapov V. N., *Infinite-Dimensional Quasigroups of finite orders*, Math. Notes, **93**:3 (2013), 479–486. MR3205994
[6] Romanov A. M., *On the construction of perfect nonlinear binary codes by symbol inversion*, Discretn. Anal. Issled. Oper. Ser 1., **4**:1 (1997), 46–52. (in Russian) MR1490441
[7] Phelps K. T., LeVan M. J., *Kernels of nonlinear Hamming codes*, Designs, Codes and Cryptogr., **6**:3 (1995), 247–257. MR1351847
[8] Phelps K. T., LeVan M. J., *Nonsystematic perfect codes*, SIAM J. Discrete Math., **12**:1 (1999), 27–34. MR1666049

Sergey Artem'evich Malyugin
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090, Novosibirsk, Russia
E-mail address: mal@math.nsc.ru