ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Апрель–июнь 2017. Том 24, № 2. С. 53–67

УДК 519.8 DOI: 10.17377/daio.2017.24.535

СОВЕРШЕННЫЕ ДВОИЧНЫЕ КОДЫ БЕСКОНЕЧНОЙ ДЛИНЫ *)

С. А. Малюгин

Институт математики им. С. Л. Соболева СО РАН,
пр. Акад. Коптюга, 4, 630090 Новосибирск, Россия
E-mail: mal@math.nsc.ru

Аннотация. Подмножество C в бесконечномерном двоичном кубе называется *совершенным двоичным кодом с расстоянием* 3, если все шары единичного радиуса (в метрике Хемминга) с центрами из C попарно не пересекаются и их объединение покрывает этот двоичный куб. Аналогичным образом определяется совершенный код в нулевом слое, состоящем из всех векторов бесконечномерного двоичного куба, имеющих конечные носители. В работе доказывается, что мощность всех классов эквивалентности совершенных двоичных кодов в нулевом слое бесконечномерного двоичного куба равна континууму, а мощность классов эквивалентности совершенных двоичных кодов во всём таком кубе равна гиперконтинууму. Библиогр. 9.

Ключевые слова: совершенный двоичный код, код Хемминга, код Васильева, компонента, континуум, гиперконтинуум.

1. Основные определения

Пусть $\mathbb{N}$ — множество натуральных чисел. *Бесконечномерный куб* $\{0,1\}^{\mathbb{N}}$ состоит из всевозможных бесконечных последовательностей $u = (u_1, \dots, u_n, \dots)$, где $u_n \in \{0,1\}$, $n \in \mathbb{N}$. Сумма двух элементов $u, v \in \{0,1\}^{\mathbb{N}}$ определяется формулой $u + v = (u_1 \oplus v_1, \dots, u_n \oplus v_n, \dots)$, где $u = (u_1, \dots, u_n, \dots)$, $v = (v_1, \dots, v_n, \dots)$ и $u_n \oplus v_n$ — сумма элементов u_n, v_n в двухэлементном поле Галуа $GF(2) = \{0,1\}$. Относительно такой операции сложения куб $\{0,1\}^{\mathbb{N}}$ является бесконечномерным векторным пространством над полем $GF(2)$. Элементы куба $\{0,1\}^{\mathbb{N}}$ далее будем называть векторами. Нулевой вектор обозначаем через $\mathbf{0}$, а базисные векторы с единичной i-й координатой — 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

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 14–01–00507).

весом и обозначается через $|u|$. В отличие от конечномерного случая вес может принимать также значение ∞. *Расстояние Хемминга* между векторами $u, v \in \{0,1\}^{\mathbb{N}}$ определяется как $|u+v|$. Расстояние Хемминга задаёт в пространстве $\{0,1\}^{\mathbb{N}}$ «обобщённую» *метрику Хемминга* со значениями в $\mathbb{N} \cup \{\infty\}$, которую можно при желании заменить эквивалентной ей метрикой $\rho(u,v) = |u+v|/(1+|u+v|)$, $u, v \in \{0,1\}^{\mathbb{N}}$, принимающей только конечные значения из отрезка $[0,1]$. Ясно, что $|u+v| = \infty \iff \rho(u,v) = 1$ и $|u+v| = n \iff \rho(u,v) = n/(n+1)$.

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

Далее будем рассматривать только совершенные двоичные коды с расстоянием 3. Вопрос о существовании совершенных двоичных кодов с другими расстояниями в данной работе не изучается.

Рассмотрим в $\{0,1\}^{\mathbb{N}}$ следующее отношение эквивалентности:

$$u \sim v \iff |u+v| \neq \infty, \quad u, v \in \{0,1\}^{\mathbb{N}}.$$

Куб $\{0,1\}^{\mathbb{N}}$ относительно этого отношения эквивалентности разбивается на попарно не пересекающиеся классы эквивалентности, которые будем называть *слоями* куба $\{0,1\}^{\mathbb{N}}$. Слой, содержащий нулевой вектор, будем обозначать символом $\{0,1\}^{\mathbb{N}}_0$ и называть *нулевым слоем*. Он состоит из всех векторов куба $\{0,1\}^{\mathbb{N}}$ конечного веса (такие векторы будем называть *финитными*). Очевидно, что нулевой слой является подпространством в $\{0,1\}^{\mathbb{N}}$, а любой другой слой $\mathcal{L}$ является смежным классом по этому подпространству. Пусть $\mathcal{L}$ — произвольный слой в кубе $\{0,1\}^{\mathbb{N}}$.

Определение 1′. Подмножество $C \subset \mathcal{L}$ называем *совершенным двоичным кодом слоя* $\mathcal{L}$, если все шары единичного радиуса с центрами из C попарно не пересекаются и их объединение покрывает слой $\mathcal{L}$.

Легко видеть, что если C — совершенный код в $\{0,1\}^{\mathbb{N}}$, то для любого слоя $\mathcal{L}$ пересечение $C \cap \mathcal{L}$ является совершенным кодом слоя $\mathcal{L}$. Обратно, если в каждом слое $\mathcal{L}$ выбран совершенный код $C_{\mathcal{L}}$, то множество C, являющееся объединением кодов $C_{\mathcal{L}}$ по всем слоям $\mathcal{L}$, будет совершенным кодом в кубе $\{0,1\}^{\mathbb{N}}$. Следовательно, изучение совершенных кодов в кубе $\{0,1\}^{\mathbb{N}}$ фактически сводится к изучению совершенных кодов в нулевом слое $\{0,1\}^{\mathbb{N}}_0$. Следует отметить, что изучение кодов бесконечной длины (МДР-кодов, задаваемых квазигруппами с бесконечным числом аргументов) впервые предпринято В. Н. Потаповым в [6]. В настоящей

работе приводятся подробные доказательства результатов, анонсированных в [5].

Совершенный код в $\{0,1\}_0^{\mathbb{N}}$ называется *линейным*, если он является линейным подпространством в $\{0,1\}_0^{\mathbb{N}}$. Есть стандартный способ построения линейного кода. Любое натуральное число $n \in \mathbb{N}$ представляем в двоичной системе счисления $n = i_k \dots i_1$ и сопоставляем ему бесконечный вектор-столбец

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

где $i_m = 0$ 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:

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

Говорим, что вектор $u = (u_1, \dots, u_n, \dots) \in \{0,1\}_0^{\mathbb{N}}$ принадлежит коду Хемминга тогда и только тогда, когда $\bigoplus\limits_{n \in \mathbb{N}} u_n \cdot \vec{n} = 0$ (в этой бесконечной сумме только конечное число ненулевых слагаемых). Легко видеть, что так определённое множество векторов u является линейным совершенным кодом в $\{0,1\}_0^{\mathbb{N}}$. Этот код по традиции называется *кодом Хемминга*. Будем далее обозначать его символом H^∞.

Код Хемминга H^∞ можно определить по-другому. Для конечных n код Хемминга H^n длины $n = 2^k - 1$, $k > 1$, определяется стандартным образом (см., например, [3,4]). 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 $\widetilde{H}^n$. Так как $\widetilde{H}^n \subset \widetilde{H}^{2n+1}$, $n = 2^k - 1$, можно положить $H^\infty = \bigcup\limits_{k=2}^{\infty} \widetilde{H}^{2^k-1}$. Как легко видеть, это определение кода H^∞ совпадает с определением, приведённым выше.

2. Эквивалентность линейных совершенных кодов в нулевом слое и их группа автоморфизмов

Как и в конечномерном случае, для любой изометрии $\alpha\colon \{0,1\}_0^{\mathbb{N}} \to \{0,1\}_0^{\mathbb{N}}$ существуют вектор $a \in \{0,1\}_0^{\mathbb{N}}$ и перестановка $\pi\colon \mathbb{N} \to \mathbb{N}$ такие, что $\alpha(u) = \widetilde{\pi}(u) + a$, где $\widetilde{\pi}((u_1, \dots, u_n, \dots)) = (u_{\pi^{-1}(1)}, \dots, u_{\pi^{-1}(n)}, \dots)$.

Определение 2. Два совершенных двоичных кода $C_1, C_2 \subset \{0,1\}_0^{\mathbb{N}}$ называются *эквивалентными*, если существует изометрия α нулевого слоя $\{0,1\}_0^{\mathbb{N}}$ такая, что $\alpha(C_1) = C_2$. Два совершенных двоичных кода $C_1, C_2 \subset \{0,1\}_0^{\infty}$ называются *изоморфными*, если существует перестановка $\pi\colon \mathbb{N} \to \mathbb{N}$ такая, что $\widetilde{\pi}(C_1) = C_2$.

Лемма 1. *Все линейные совершенные двоичные коды в слое* $\{0,1\}_0^{\mathbb{N}}$ *эквивалентны между собой.*

Доказательство. Пусть $C \subset \{0,1\}_0^{\mathbb{N}}$ — некоторый линейный код. Докажем, что он эквивалентен коду Хемминга H^{∞}. Обозначим через $\mathrm{STS}\,(C)$ *систему троек Штейнера кода* C, т. е. множество носителей всех векторов из C, имеющих вес 3. Покажем, что существует перестановка π на множестве $\mathbb{N}$ такая, что $\pi(\mathrm{STS}(H^{\infty})) = \mathrm{STS}(C)$. Возьмём любой вектор $u \in C$ веса 3. Пусть $[u] = \{i_1, i_2, i_3\}$. Полагаем $\pi(1) = i_1$, $\pi(2) = i_2$, $\pi(3) = i_3$. Далее действуем по индукции. Допустим, что для некоторого $n \in \mathbb{N}$, $n = 2^k - 1$, $k \geqslant 2$, мы уже определили $\pi(m) = i_m$ для всех $m \in \{1, \dots, n\}$, причём π отображает взаимно однозначно систему троек Штейнера кода Хемминга H^n на множество троек кода C, входящих в множество $\{i_1, \dots, i_n\}$. Возьмём наименьший номер $i_{n+1} \notin \{i_1, \dots, i_n\}$ и положим $\pi(n+1) = i_{n+1}$. Пусть $1 \leqslant s \leqslant n$. Так как код C совершенный, вектор v с носителем $\{i_s, i_{n+1}\}$ находится на расстоянии 1 от единственного кодового вектора $u \in C$, имеющего вес 3. Очевидно, что $i_s, i_{n+1} \in [u]$, т. е. $[u] = \{i_s, j, i_{n+1}\}$ для некоторого номера $j \notin \{i_1, \dots, i_n\}$. Используя введённую выше побитовую операцию сложения на множестве $\mathbb{N}$, полагаем $\pi(s \oplus (n+1)) = j$. Таким образом распространяем отображение π на множество $\{1, \dots, (2n+1)\}$. Оно отображает систему троек Штейнера кода H^{2n+1} на систему троек Штейнера кода C, входящих в множество $\{i_1, \dots, i_{2n+1}\}$. Для доказательства этого рассмотрим любой вектор $u \in C$ веса 3, для которого $[u] \subset \{i_1, \dots, i_{2n+1}\}$ и $[u] \not\subset \{i_1, \dots, i_n\}$. Осталось рассмотреть только случай $i_{n+1} \notin [u]$. Пусть $[u] = \{j_1, j_2, j_3\}$, где $j_2, j_3 \notin \{i_1, \dots, i_n\}$. Пусть $k_2 = \pi^{-1}(j_2)$, $k_3 = \pi^{-1}(j_3)$. Так как $k_2, k_3 \notin \{1, \dots, n\}$, то $k_1 = k_2 \oplus k_3 \in \{1, \dots, n\}$. Положим $j_1' = \pi(k_1)$. Поскольку вектор v с носителем $\{k_1, k_2, k_3\}$ есть сумма трёх векторов v_1, v_2, v_3 с носителями $\{k_2 \oplus (n+1), k_2, n+1\}$,

$\{k_3 \oplus (n+1), k_3, n+1\}$, $\{k_1, k_2 \oplus (n+1), k_3 \oplus (n+1)\}$ и отображение $\widetilde{\pi}$ линейно, $\pi([v]) = \{j_1', j_2, j_3\}$ тоже является суммой трёх векторов из линейного кода C веса 3. Тем самым $\widetilde{\pi}^{-1}(v) \in C$ и $|u + \widetilde{\pi}^{-1}(v)| < 3$. Следовательно, $\widetilde{\pi}(u) = v$, или $\pi([v]) = [u]$. Таким образом, определили инъективное отображение π множества $\mathbb{N}$ в $\mathbb{N}$, переводящее систему троек $\mathrm{STS}\,(H^\infty)$ в систему троек кода C. На каждом индуктивном шаге n мы выбирали наименьший номер $i_{n+1} \notin \{i_1, \ldots, i_n\}$, поэтому отображение $\pi\colon \mathbb{N} \to \mathbb{N}$ сюръективно, т. е. π является перестановкой на множестве $\mathbb{N}$ и $\pi(\mathrm{STS}(H^\infty)) = \mathrm{STS}(C)$.

Пусть u — любой вектор из кода C веса $m \geqslant 3$. Пусть $u_{j_1} = \cdots = u_{j_m} = 1$ и $u_k = 0$ при $k \neq j_1, \ldots, j_m$. Так как код C совершенный, вектор $v = e_{j_1} + e_{j_2}$ находится на расстоянии 1 от некоторого кодового вектора $w_1 \in C$. Очевидно, что вес w_1 равен трём, т. е. $w_1 = e_{j_1} + e_{j_2} + e_k$ (при некотором $k \neq j_1, j_2$). Вектор $u_{(1)} = u + w_1$ имеет вес $\leqslant m - 1$. Для $u_{(1)}$ можно повторить эти же рассуждения и, действуя по индукции, получить представление вектора u в виде суммы $u = w_1 + \cdots + w_k$ векторов $w_1, \ldots, w_k \in C$ веса 3, поэтому $\widetilde{\pi}(C) = H^\infty$. Лемма 1 доказана.

Переходим к описанию группы автоморфизмов кода Хемминга H^∞. *Группой автоморфизмов* совершенного двоичного кода C в нулевом слое $\{0,1\}_0^{\mathbb{N}}$ называется подгруппа всех изометрий слоя $\{0,1\}_0^{\mathbb{N}}$, оставляющих код C на месте. Группу автоморфизмов кода C будем обозначать через $\mathrm{Aut}\,(C)$. В этой группе естественным образом выделяются две подгруппы: подгруппа перестановочных автоморфизмов $\mathrm{Sym}\,(C)$ и ядро кода $\mathrm{Ker}\,(C)$. Подгруппа $\mathrm{Sym}\,(C)$ состоит из всех перестановок $\pi\colon \mathbb{N} \to \mathbb{N}$ таких, что $\widetilde{\pi}(C) = C$, а подгруппа $\mathrm{Ker}\,(C)$ состоит из всех векторов $u \in \{0,1\}_0^\infty$, для которых $C + u = C$. Очевидно, что если $0 \in C$, то $\mathrm{Ker}\,(C) \subset C$.

Перестановка π на множестве $\mathbb{N}$ называется *линейной*, если $\pi(m \oplus n) = \pi(m) \oplus \pi(n)$ для всех $m, n \in \mathbb{N}$ (полагая $\pi(0) = 0$, получим обратимое линейное отображение $\mathbb{N} \cup \{0\}$ на $\mathbb{N} \cup \{0\}$). Легко видеть, что перестановка π линейна тогда и только тогда, когда $\pi(\mathrm{STS}(H^\infty)) = \mathrm{STS}(H^\infty)$. Отсюда сразу следует, что группа перестановочных автоморфизмов $\mathrm{Sym}\,(H^\infty)$ кода Хемминга H^∞ состоит из всех линейных перестановок множества $\mathbb{N}$. Так как $\mathrm{Ker}\,(H^\infty)$ является нормальной подгруппой в $\mathrm{Sym}\,(H^\infty)$ и $\mathrm{Ker}\,(H^\infty) \cap \mathrm{Sym}\,(H^\infty)$ состоит лишь из одного тождественного преобразования, так же, как в случае кодов Хемминга конечной длины, группа автоморфизмов $\mathrm{Aut}\,(H^\infty)$ есть полупрямое произведение групп $\mathrm{Sym}\,(H^\infty)$ и группы $\mathrm{Ker}\,(H^\infty) = H^\infty$.

3. Континуальность множества классов эквивалентности совершенных двоичных кодов бесконечной длины

В коде Хемминга H^∞ рассмотрим подпространство R_i, порождённое 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^∞, $i \in \mathbb{N}$. Рассмотрим семейство $\mathcal{B} = \{R_{i_1}^{u_1}, R_{i_2}^{u_2}, \dots\}$, состоящее из конечного или бесконечного числа попарно не пересекающихся i_p-компонент, где $\mathbf{u}_p \in H^\infty$, $1 \leqslant p < m+1$, $m \in \mathbb{N} \cup \{\infty\}$. Одна из основных конструкций нелинейных совершенных двоичных кодов состоит в том, что в коде H^∞ сдвигаются по координатам i_p все компоненты из семейства $\mathcal{B}$, т. е. множество

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

является совершенным кодом. Для доказательства этого возьмём два различных вектора $u, v \in H^\infty(\mathcal{B})$ и покажем, что расстояние между ними не меньше трёх. Например, рассмотрим случай $u \in R_{i_p}^{u_p} + e_{i_p}$, $v \in R_{i_q}^{u_q} + e_{i_q}$. Так как по вышеизложенному $H^\infty = \bigcup\limits_{k=2}^{\infty} \widetilde{H}^{2^k-1}$, при достаточно большом k имеем $u + e_{i_p}, v + e_{i_q}, u_p, u_q \in \widetilde{H}^{2^k-1}$ и $i_p, i_q \leqslant 2^k - 1$. Мы свели эту проверку к случаю кодов конечной длины, и теперь можно сослаться на [1, 7–9]. Проверка того, что любой вектор из $\{0,1\}_0^{\mathbb{N}}$ находится на расстоянии, не большем 1, от $H^\infty(\mathcal{B})$, проводится аналогично. Далее будем говорить, что код $H^\infty(\mathcal{B})$ построен из кода Хемминга H^∞ *сдвигами* (или *свитчингами*) компонент из семейства $\mathcal{B}$. Если при фиксированном индексе i имеем $i_p = i$ для всех p, то код $H^\infty(\mathcal{B})$ называем *кодом Васильева бесконечной длины*. Такие коды конечной длины впервые построены в [2]. Для нахождения мощности множества всех классов эквивалентности кодов бесконечной длины достаточно ограничиться рассмотрением кодов Васильева.

Положим $i = 1$. Компонента R_1 порождается всеми векторами v_p веса 3 с носителями $[v_p] = \{1, 2p, 2p+1\}$, $p \in \mathbb{N}$. Рассмотрим векторы $w_1 = 0$, $w_p = e_8 + e_{10} + \dots + e_{2^{p+2}-2}$, $p \in \mathbb{N}$, $p \geqslant 2$. Из определения проверочной матрицы (1) следует, что $w_p \in H^\infty$, $p \in \mathbb{N}$. Для бесконечного семейства компонент $\mathcal{B}_1 = \{R_1^{w_p}\}_{p=1}^{\infty}$ и любого $\varepsilon \in \{0,1\}^{\mathbb{N}}$, $\varepsilon = (\varepsilon_1, \varepsilon_2, \dots)$, рассмотрим следующий код Васильева:

$$H^\infty(\mathcal{B}_1, \varepsilon) = \left(H^\infty \setminus \bigcup_{p=1}^{\infty} R_1^{w_p}\right) \cup \left(\bigcup_{p=1}^{\infty} \left(R_1^{w_p} + \varepsilon_p e_1\right)\right), \qquad (2)$$

т. е. код $H^\infty(\mathcal{B}_1, \varepsilon)$ получается из кода Хемминга H^∞ сдвигами только тех компонент $R_1^{u_p}$ из семейства $\mathcal{B}_1$, для которых $\varepsilon_p = 1$.

Следующая лемма доказана в [4, лемма 7], но здесь она потребуется в несколько иной редакции.

Лемма 2. *Пусть L — аффинное пространство конечной размерности над полем $GF(2)$ (считаем, что L является подмножеством некоторого объемлющего линейного пространства L') и множество $M \subset L$ имеет мощность $|M| > |L|/2$. Тогда любой вектор из L представляется суммой трёх векторов из M.*

Доказательство. Для любого фиксированного $a \in M$ рассмотрим множество $M' = M + a$. По лемме 7 из [4] любой вектор $v \in L + a$ представляется суммой двух векторов $v_1, v_2 \in M'$. Если $u \in L$, то $u + a = v_1 + v_2$ для некоторых $v_1, v_2 \in M'$. Поэтому $u = a + v_1 + v_2 = a + u_1 + u_2$, где $u_1 = v_1 + a$, $u_2 = v_2 + a$. Лемма 2 доказана.

Лемма 3. *Пусть L — любое линейное пространство над полем $GF(2)$ и $H \subset L$ — его подпространство. Пусть $A\colon L \to L$ — аффинный изоморфизм пространства L, $A(u) = \alpha(u) + a$, где $a \in L$, а α — линейный изоморфизм L на L. Пусть $F\colon L \to \{0,1\}^3$ — линейное отображение такое, что $F(H) = \{0,1\}^3$ и $F \circ A(H) = \{0,1\}^3$. Рассмотрим два подмножества $C_1, C_2 \subset L$, удовлетворяющие условиям*

$$C_1 \setminus \mathrm{Ker} F = C_2 \setminus \mathrm{Ker} F = H \setminus \mathrm{Ker} F. \tag{3}$$

Тогда если $A(C_1) = C_2$, то $A(H) = H$ и $a \in H$.

Доказательство. Рассмотрим отображение $G\colon L \to \{0,1\}^3$, $G = F \circ \alpha^{-1}$. Так как A — аффинный изоморфизм L на L, также $G(A(H))) = \{0,1\}^3$. Поскольку

$$A(H \setminus \mathrm{Ker}\, F) = A(C_1 \setminus \mathrm{Ker}\, F) \subset A(C_1) = C_2,$$

имеем

$$A(H \setminus \mathrm{Ker}\, F) \setminus \mathrm{Ker} F \subset C_2 \setminus \mathrm{Ker}\, F \subset H.$$

Обозначим $M = A(H \setminus \mathrm{Ker}\, F) \setminus \mathrm{Ker}\, F$ и покажем, что любой вектор $u \in A(H) \setminus M$ представляется суммой трёх векторов $u_1, u_2, u_3 \in M$. Очевидно, что $u \in M$ тогда и только тогда, когда $u \in A(H)$ и $F(u) \neq 0$, $G(u) \neq F(\alpha^{-1}(a))$. Рассмотрим подпространство $H' = A(H) + a = \alpha(H)$ и множество $M' = M + a \subset H'$. Очевидно, что $v \in M'$ означает, что $v \in H'$ и $F(v) \neq F(a)$, $G(v) \neq 0$. Так как $F(H') = \{0,1\}^3$ и $G(H') = \{0,1\}^3$, подпространство $L_0 = \mathrm{Ker}\, F \cap \mathrm{Ker}\, G \cap H'$ имеет в H' коразмерность k не менее 3 и не более 6. Рассмотрим в L_0 подпространство L_1, имеющее коразмерность 6 в H', и шестимерное фактор-пространство $H'/L_1 \approx \{0,1\}^6$.

Обозначим через $P\colon H' \to H'/L_1$ соответствующее отображение факторизации. Образы $P((\operatorname{Ker} F + a) \cap H')$ и $P(\operatorname{Ker} G \cap H')$ имеют размерность 3, поэтому число точек в $P(M')$ составляет больше половины числа точек всего пространства H'/L_1. Из леммы 2 следует, что любой вектор $\gamma \in P(H')$ представляется суммой трёх векторов из $P(M')$. Переходя к смежным классам $P^{-1}(\gamma)$, получаем, что любой смежный класс из H' представляется суммой трёх смежных классов из M'. Из определения следует, что M' является объединением некоторого числа таких смежных классов. Как следствие, любой вектор $v \in H'$ представляется суммой трёх векторов $v_1, v_2, v_3 \in M'$. Следовательно, любой вектор $u \in A(H)$ имеет вид $u = v + a$ для некоторого $v \in H'$ и представляется суммой $u = a + v_1 + v_2 + v_3 = u_1 + u_2 + u_3$, где $u_i = (v_i + a) \in M$, $i = 1, 2, 3$. Таким образом, $A(H) \subseteq (M + M + M) \subseteq H$. В частности, отсюда следует, что $a \in H$. Если в условии леммы заменить A на A^{-1} и поменять ролями G_1 и G_2, то в результате получим $A^{-1}(H) \subseteq H$, поэтому $A(H) = H$. Лемма 3 доказана.

Эта лемма позволяет доказать следующий ключевой факт.

Теорема 1. *Если $\varepsilon, \varepsilon' \in \{0,1\}^{\mathbb{N}}$, $\varepsilon \neq \varepsilon'$, $\varepsilon_1 = \varepsilon'_1 = 1$, то коды Васильева $H^\infty(\mathcal{B}_1, \varepsilon)$, $H^\infty(\mathcal{B}_1, \varepsilon')$ не эквивалентны.*

Доказательство. Допустим, что для вектора $a \in \{0,1\}_0^{\mathbb{N}}$ и некоторой перестановки $\pi\colon \mathbb{N} \to \mathbb{N}$ имеем $\widetilde{\pi}(H^\infty(\mathcal{B}_1, \varepsilon)) + a = H^\infty(\mathcal{B}_1, \varepsilon')$. Далее хотим применить лемму 3. Для этого положим $L = \{0,1\}_0^{\mathbb{N}}$, $C_1 = H^\infty(\mathcal{B}_1, \varepsilon)$, $C_2 = H^\infty(\mathcal{B}_1, \varepsilon')$. Для $u = (u_1, u_2, \dots) \in L$ полагаем также $f_1(u) = u_2 + u_3$, $f_2(u) = u_4 + u_5$, $f_3(u) = u_6 + u_7$. Носители векторов веса 3 из компоненты R_1 имеют вид $\{1, 2n, 2n+1\}$, поэтому $f_1(R_1) = f_2(R_1) = f_3(R_1) = 0$. Для векторов $w_p = e_8 + e_{10} + \dots + e_{2^{p+2}-2}$, $p \geqslant 2$, используемых в построении кодов C_1, C_2, тоже получаем $f_1(w_p) = f_2(w_p) = f_3(w_p) = 0$. Кроме этого, $f_1(e_1) = f_2(e_1) = f_3(e_1) = 0$, поэтому $F\big(R_1^{w_p}\big) = F\big(R_1^{w_p} + e_1\big) = 0$, где $F = (f_1, f_2, f_3)\colon L \to \{0,1\}^3$. Пусть $H = H^\infty$, $A(u) = \widetilde{\pi}(u) + a$ $(u \in L)$. Отсюда следует, что условия (3) леммы 3 тоже выполняются. Проверим условия $F(H) = \{0,1\}^3$, $F \circ A(H) = \{0,1\}^3$. Для этого достаточно найти хотя бы один вектор $u = (u_1, u_2, \dots) \in H^\infty$, для которого выполняется одно из условий: 1) $u_2 = 1$, $u_k = 0$, $k = 3, 4, 5, 6, 7$; 2) $u_4 = 1$, $u_k = 0$, $k = 2, 3, 5, 6, 7$; 3) $u_6 = 1$, $u_k = 0$, $k = 2, 3, 4, 5, 7$. Например, для проверки условия 1 перебираем пары номеров (k, l) таких, что $k \oplus l = 2$. Среди таких номеров всегда есть пара (k, l), для которой $k > 7$ и $l > 7$. Вектор $u = e_2 + e_k + e_l \in H^\infty$ будет требуемым, при этом $F(u) = (1, 0, 0)$. Условия 2 и 3 проверяются аналогично; в случае 2 получаем $F(u) = (0, 1, 0)$, а в случае 3 — $F(u) = (0, 0, 1)$. Так как образ

$F(H)$ содержит базис пространства $\{0,1\}^3$, то $F(H)=\{0,1\}^3$. Проверка условия $F\circ A(H)=\{0,1\}^3$ (которую мы опускаем) сводится к нахождению векторов $u\in H^\infty$, для которых выполняется одно из условий: 1) $u_{\pi^{-1}(2)}=1$, $u_{\pi^{-1}(k)}=0$, $k=3,4,5,6,7$; 2) $u_{\pi^{-1}(4)}=1$, $u_{\pi^{-1}(k)}=0$, $k=2,3,5,6,7$; 3) $u_{\pi^{-1}(6)}=1$, $u_{\pi^{-1}(k)}=0$, $k=2,3,4,5,7$. Теперь можно сослаться на лемму 3 и утверждать, что $a\in H^\infty$ и $A(H^\infty)=H^\infty$, т. е. отображение A является автоморфизмом кода Хемминга H^∞.

Так как $\widetilde{\pi}(C_1)+a=C_2$, вектор a должен принадлежать одной из сдвигаемых компонент $\widetilde{\pi}\big(R_1^{w_{p_0}}\big)$ (иначе код C_1, не содержащий нулевого вектора, будет изоморфен коду C_2+a, содержащему нулевой вектор). Так как e_1 — единственный вектор веса 1, принадлежащий коду C_1, он должен принадлежать и изоморфному ему коду C_2+a. Поэтому $\pi(1)=1$ и отображение $\widetilde{\pi}$ переводит 1-компоненты $R_1^{w_p}$ в 1-компоненты $R_1^{\widetilde{\pi}(w_p)}$ кода H^∞. Если заменим вектор a любым вектором $a'=a+u$, $u\in R_1$, то по-прежнему имеем $\widetilde{\pi}(C_1)=C_2+a'$. Тем самым можно заменить вектор $a\in R_1^{\widetilde{\pi}(w_{p_0})}$ вектором $\widetilde{\pi}(w_{p_0})$.

Теперь посмотрим, на каком расстоянии от 0 находятся компоненты $R_1^{w_p}$. Вектор w_p имеет вес $d_p=2^{p+1}-4$, $p\geqslant 1$. Так как у любого вектора $v\in R_1$ число ненулевых нечётных координат не меньше числа ненулевых чётных координат, вес любого вектора w_p+v будет не меньше d_p, а значит, расстояние от компоненты $R_1^{w_p}$ до нуля равно d_p. Соответственно расстояние от сдвинутой компоненты $R_1^{w_p}+e_1$ до нуля равно d_p+1. Отображение $\widetilde{\pi}$ переведёт эту компоненту в компоненту $R_1^{\widetilde{\pi}(w_p)}+e_1$ того же кода H^∞, находящуюся на таком же расстоянии d_p+1 от нуля. Тем самым отображение эквивалентности A переведёт компоненту $R_1^{\widetilde{\pi}(w_p)}+e_1$ в компоненту $R_1^{\widetilde{\pi}(w_p)+a}+e_1=R_1^{\widetilde{\pi}(w_p+w_{p_0})}+e_1$. Пусть $p\neq 1,p_0$ и $\varepsilon_p=1$. Тогда компонента $R_1^{\widetilde{\pi}(w_p+w_{p_0})}+e_1$ должна совпасть с одной из компонент $R_1^{w_{p'}}$, находящейся на расстоянии $d_{p'}+1$ от нуля, причём $p'\neq 1,p_0$. Расстояние компоненты $R_1^{\widetilde{\pi}(w_p+w_{p_0})}+e_1$ до нуля равно $2^{p+1}-2^{p_0+1}+1=d_{p'}+1=2^{p'+1}-3$. Если $w_{p_0}\neq 0$, то $p_0\geqslant 2$, и из условия $p\geqslant 2$ следует, что число $2^{p+1}+4=2^{p'+1}+2^{p_0+1}$ должно делиться на 8. В результате получим, что либо $w_{p_0}=0$ (что эквивалентно условию $a=0$), либо код G_1 получен из кода Хемминга H^∞ сдвигами не более двух компонент (если сдвигаются две компоненты R_1 и $R_1^{\widetilde{w}_{p_0}}$, то код C_2 тоже должен строиться из кода H^∞ сдвигами тех же двух компонент и ненулевой перенос на вектор a просто переставляет эти компоненты). Стало быть, если код C_1 получается из кода H^∞ сдвигами более чем двух компонент, то из эквивалентности кодов C_1 и C_2 следует их изоморф-

ность. Так как $d_p \neq d_{p'}$ при $p \neq p'$, равенство $\widetilde{\pi}(H^\infty(\mathcal{B}_1, \varepsilon)) = H^\infty(\mathcal{B}_1, \varepsilon')$ может выполняться только при условии $\varepsilon = \varepsilon'$. Теорема 1 доказана.

Мы построили континуум попарно не эквивалентных кодов Васильева бесконечной длины. Так как в счётном множестве $\{0,1\}_0^{\mathbb{N}}$ может быть не более континуума различных кодов, из теоремы 1 выводим

Следствие 1. *Мощность множества всех классов эквивалентности совершенных двоичных кодов бесконечной длины равна континууму.*

4. Совершенные двоичные коды в кубе $\{0,1\}^{\mathbb{N}}$

Существование совершенных двоичных кодов в кубе $\{0,1\}^{\mathbb{N}}$ сразу следует из существования таких кодов в слое $\{0,1\}_0^{\mathbb{N}}$. Для этого пронумеруем все слои числами из отрезка $[0,1]$, т. е. каждому числу $\alpha \in [0,1]$ сопоставим слой $\mathcal{L}_\alpha \subset \{0,1\}^{\mathbb{N}}$, при этом $\{0,1\}^{\mathbb{N}} = \bigcup\limits_{\alpha\in[0,1]} \mathcal{L}_\alpha$. Выберем в каждом слое по одному элементу u_α и для любого совершенного кода $C_0 \subset \mathcal{L}_0 = \{0,1\}_0^{\mathbb{N}}$ полагаем $C = \bigcup\limits_{\alpha\in[0,1]} (C_0 + u_\alpha)$. Очевидно, что множество C является совершенным двоичным кодом в $\{0,1\}^{\mathbb{N}}$. Отметим, что при построении кода C применена аксиома выбора.

Лемма 4. *В кубе $\{0,1\}^{\mathbb{N}}$ существуют линейные совершенные двоичные коды.*

Доказательство. Рассмотрим базис Гамеля в фактор-пространстве $\{0,1\}^{\mathbb{N}}/\mathcal{L}_0$. Пусть для некоторого (континуального) множества $A \subset [0,1]$ семейство слоёв $\{\mathcal{L}_\alpha \mid \alpha \in A\}$ является этим базисом. Выберем в каждом таком слое $\mathcal{L}_\alpha$ по одному элементу u_α. Если $\beta \in [0,1] \setminus A$, то для некоторого конечного подсемейства $\{\alpha_i\}_{i=1}^n \subset A$ имеем $\mathcal{L}_\beta = \sum\limits_{i=1}^n \mathcal{L}_{\alpha_i}$. Тогда для этого β полагаем $u_\beta = \sum\limits_{i=1}^n u_{\alpha_i}$. Таким способом выбираем в каждом слое $\mathcal{L}_\beta$ элемент u_β. Поскольку множество представителей $\{u_\alpha\}_{\alpha\in A}$ линейно независимо, построенное так множество $L = \{u_\beta\}_{\beta\in[0,1]}$ является линейным подпространством в $\{0,1\}^{\mathbb{N}}$, дополнительным к подпространству $\mathcal{L}_0$, т. е. $\mathcal{L}_0 \cap L = \{0\}$ и $\mathcal{L}_0 + L = \{0,1\}^{\mathbb{N}}$. Искомый линейный код теперь определяется формулой $C_L = H^\infty + L$. Лемма 4 доказана.

Прежде чем давать определение эквивалентности кодов, посмотрим, как устроены изометрии куба $\{0,1\}^{\mathbb{N}}$. Так как разные слои этого куба находятся на бесконечном расстоянии Хемминга друг от друга, изометрия допускает, во-первых, произвольную перестановку (континуально-

го) множества всех слоёв. В каждом слое $\mathcal{L}_\alpha$ допускается (независимо от других слоёв) перестановка координат π_α и перенос на вектор $a_\alpha \in \{0,1\}_0^{\mathbb{N}}$. Изометрия может не быть аффинным преобразованием всего куба. На этом основании вводим два различных определения.

Определение 3. Два совершенных кода $C_1, C_2 \subset \{0,1\}^{\mathbb{N}}$ называются *изометричными* (соответственно *эквивалентными*), если существует изометрия A пространства $\{0,1\}^{\mathbb{N}}$ (соответственно изометрия, являющаяся аффинным преобразованием пространства $\{0,1\}^{\mathbb{N}}$) такая, что $A(C_1) = C_2$.

Такое определение эквивалентности кодов введено в связи с тем, что линейный код может быть эквивалентен только линейному коду, но изометричен нелинейному коду.

Лемма 5. *Все линейные совершенные коды в* $\{0,1\}^{\mathbb{N}}$ *эквивалентны между собой.*

Доказательство. Рассмотрим любой линейный совершенный код $H_1 \subset \{0,1\}^{\mathbb{N}}$. В доказательстве леммы 4 построено подпространство L, дополнительное к слою $\mathcal{L}_0 = \{0,1\}^{\mathbb{N}}$. Докажем, что код H_1 эквивалентен построенному в доказательстве леммы 4 линейному коду $C_L = H^\infty + L$. В доказательстве леммы 4 пространство L порождалось базисом Гамеля $\{u_\alpha\}_{\alpha\in A}$, $A \subset [0,1]$, который состоит из представителей $u_\alpha \in \mathcal{L}_\alpha$ базиса Гамеля $\{\mathcal{L}_\alpha \mid \alpha \in A\}$ фактор-пространства $\{0,1\}^{\mathbb{N}}/\mathcal{L}_0$. Выберем в этих слоях $\mathcal{L}_\alpha$ ещё по одному элементу $v_\alpha \in \mathcal{L}_\alpha \cap H_1$. Так как совершенные коды H^∞ и $H_1 \cap \{0,1\}_0^{\mathbb{N}}$ эквивалентны в слое $\{0,1\}_0^{\mathbb{N}} = \mathcal{L}_0$, в силу леммы 1 существует линейная изометрия A_0 пространства $\mathcal{L}_0$, переводящая код H^∞ в код $H_1 \cap \mathcal{L}_0$. Для любого $\alpha \in A$ и любого элемента $u \in \mathcal{L}_\alpha$ полагаем $A_\alpha(u) = v_\alpha + A_0(u_\alpha + u)$. Очевидно, что A_α является аффинной изометрией в слое $\mathcal{L}_\alpha$, причём $A_\alpha(u_\alpha) = v_\alpha$. Пусть $u \in H^\infty \cap \mathcal{L}_\alpha = H^\infty + u_\alpha$. Тогда $u = u_\alpha + h$ для некоторого $h \in H^\infty$ и $A_\alpha(u) = v_\alpha + A_0(u_\alpha + u) = v_\alpha + A_0(h) \in H_1 \cap \mathcal{L}_\alpha$, так как $v_\alpha \in H_1 \cap \mathcal{L}_\alpha$, $A_0(H^\infty) = H_1 \cap \mathcal{L}_0$. Для любого $\beta \in [0,1]$ существует конечный набор индексов $\{\alpha_i\}_{i=1}^n$, для которого $u_\beta = \sum\limits_{i=1}^{n} u_\alpha$. Тогда для любого $u \in \mathcal{L}_\beta$ полагаем $A_\beta(u) = \left(\sum\limits_{i=1}^{n} v_{\alpha_i}\right) + A_0(u + u_\beta)$. Теперь искомая линейная изометрия $A\colon \{0,1\}^{\mathbb{N}} \to \{0,1\}^{\mathbb{N}}$ определяется путём объединения всех отображений A_β (т. е. $A|_{\mathcal{L}_\beta} = A_\beta$, $\beta \in [0,1]$). Лемма 5 доказана.

Мощность континуума принято обозначать символом $\mathfrak{c}$. Мощность всех подмножеств континуального множества будем обозначать симво-

лом $2^{\mathfrak{c}}$. Эту мощность называют также *гиперконтинуумом*.

Пример. Построим в пространстве $\{0,1\}^{\mathbb{N}}$ гиперконтинуальное семейство линейных совершенных двоичных кодов $\mathcal{H} = \{H_\gamma\}_{\gamma\in\Gamma}$ такое, что для любых $H_{\gamma_1}, H_{\gamma_2} \in \mathcal{H}$, $\gamma_1 \neq \gamma_2$, не существует ни одной перестановки $\pi\colon \mathbb{N} \to \mathbb{N}$ такой, что $H_{\gamma_2} = \widetilde{\pi}(H_{\gamma_1})$. Как и в доказательстве леммы 5, рассмотрим в фактор-пространстве $\{0,1\}^{\mathbb{N}}/\mathcal{L}_0$ базис Гамеля $\{\mathcal{L}_\alpha \mid \alpha \in A\}$, $A \subset [0,1]$. Известно, что множество A имеет континуальную мощность. Выберем семейство представителей $u_\alpha \in \mathcal{L}_\alpha$, $\alpha \in A$. Далее в каждом слое $\mathcal{L}_\alpha$ выберем ещё по одному элементу $v_\alpha \notin u_\alpha + H^\infty$, $\alpha \in A$. Это означает, что $(u_\alpha + H^\infty) \cap (v_\alpha + H^\infty) = \varnothing$. Для любого подмножества $B \subset A$ полагаем $w_\alpha = u_\alpha$, если $\alpha \in B$, и $w_\alpha = v_\alpha$, если $\alpha \in A \setminus B$. Каждому такому множеству B сопоставим линейное подпространство L_B, являющееся линейной оболочкой семейства $\{w_\alpha\}_{\alpha\in A}$, и линейный совершенный код $H_B = L_B + H^\infty$. По построению все эти коды различны и их число равно $2^{\mathfrak{c}}$ (числу подмножеств $B \subset A$). Всего имеется континуум различных перестановок $\pi\colon \mathbb{N} \to \mathbb{N}$, поэтому гиперконтинуальное семейство линейных кодов разбивается на континуальные классы эквивалентности относительно действия группы всех перестановок множества $\mathbb{N}$. Выбрав в каждом таком классе эквивалентности по одному коду H_γ, получим гиперконтинуальное семейство кодов с требуемым свойством.

Завершим статью следующим утверждением.

Теорема 2. *Мощность множества всех классов эквивалентности совершенных двоичных кодов в пространстве* $\{0,1\}^{\mathbb{N}}$, *а также мощность множества всех классов изометрий этих кодов равны гиперконтинууму* $2^{\mathfrak{c}}$.

Доказательство. Для доказательства теоремы достаточно построить гиперконтинуальное семейство попарно не изометричных кодов. Обозначим через $\mathcal{C} = \{C_t\}_{t\in T}$ какое-нибудь семейство всех попарно не эквивалентных совершенных двоичных кодов в нулевом слое $\mathcal{L}_0 = \{0,1\}_0^{\mathbb{N}}$. Из теоремы 1 следует, что мощность множества индексов T равна континууму. Пусть $L = \{u_\alpha\}_{\alpha\in[0,1]}$ — подпространство, дополнительное к слою $\mathcal{L}_0$, $u_\alpha \in \mathcal{L}_\alpha$, $\alpha \in [0,1]$. Для любой функции $f\colon [0,1] \to T$ рассмотрим в пространстве $\{0,1\}^{\mathbb{N}}$ совершенный двоичный код $C(f) = \bigcup\limits_{\alpha\in[0,1]} (u_\alpha + C_{f(\alpha)})$. Для $t \in T$ мощность множества $\{\alpha \in [0,1] \mid f(\alpha) = t\}$ обозначим через $\mathfrak{m}_t(f)$ и назовём *кратностью вхождения* кода C_t в код $C(f)$. Из приведённого выше описания всех изометрий пространства $\{0,1\}^{\mathbb{N}}$ следует, что для двух функций $f, f'\colon [0,1] \to T$ коды $C(f)$ и $C(f')$ изометричны тогда и только тогда, когда $\mathfrak{m}_t(f) = \mathfrak{m}_t(f')$ для всех $t \in T$. Для любого непустого множества $S \subset T$ выберем какое-нибудь сюръек-

тивное отображение $f_S\colon [0,1] \to S$. Тогда гиперконтинуальное семейство $\{C(f_S) \mid S \subset T, S \neq \varnothing\}$ состоит из попарно не изометричных (и тем более не эквивалентных) кодов. Теорема 2 доказана.

Автор благодарит рецензента за замечания, которые способствовали значительному улучшению содержания этой работы.

ЛИТЕРАТУРА

1. **Августинович С. В., Соловьева Ф. И.** Построение совершенных двоичных кодов последовательными сдвигами $\widetilde{\alpha}$-компонент // Пробл. передачи информации. 1997. Т. 33, вып. 3. С. 15–21.
2. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Пробл. кибернетики. 1962. Вып. 8. С. 337–339.
3. **Малюгин С. А.** О перечислении совершенных двоичных кодов длины 15 // Дискрет. анализ и исслед. операций. Сер. 2. 1999. Т. 6, № 2. С. 48–73.
4. **Малюгин С. А.** Несистематические совершенные двоичные коды // Дискрет. анализ и исслед. операций. Сер. 1. 2001. Т. 8, № 1. С. 55–76.
5. **Малюгин С. А.** Совершенные двоичные коды бесконечной длины // Прикл. дискрет. математика. Прил. 2015. № 8. С. 117–120.
6. **Потапов В. Н.** Бесконечномерные квазигруппы конечных порядков // Мат. заметки. 2013. Т. 93, вып. 3. С. 457–465.
7. **Романов А. М.** О построении совершенных нелинейных двоичных кодов инверсией символов // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 1. С. 46–52.
8. **Phelps K. T., LeVan M.** Kernels of nonlinear Hamming codes // Des. Codes Cryptogr. 1995. Vol. 6, No. 3. P. 247–257.
9. **Solov'eva F. I.** Switchings and perfect codes // Numbers, information and complexity. Dordrecht: Kluwer Acad. Publ., 2000. P. 311–324.

Малюгин Сергей Артемьевич

Статья поступила
31 марта 2016 г.

Исправленный вариант —
29 августа 2016 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
April–June 2017. Volume 24, No. 2. P. 53–67

UDC 519.8 DOI: 10.17377/daio.2017.24.535

PERFECT BINARY CODES OF INFINITE LENGTH

S. A. Malyugin
Sobolev Institute of Mathematics,
4 Acad. Koptyug Ave., 630090 Novosibirsk, Russia
E-mail: mal@math.nsc.ru

Abstract. A subset C of infinite-dimensional binary cube 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 cover this binary cube. Similarly, we can define a perfect binary code in zero layer, consisting of all vectors of infinite-dimensional binary cube having finite supports. In this article we prove that the cardinality of all cosets of perfect binary codes in zero layer is the cardinality of the continuum. Moreover, the cardinality of all cosets of perfect binary codes in the whole binary cube is equal to the cardinality of the hypercontinuum. Bibliogr. 9.

Keywords: perfect binary code, Hamming code, Vasil'ev code, component, continuum, hypercontinuum.

REFERENCES

1. **S. V. Avgustinovich** and **F. I. Solov'eva,** Construction of perfect binary codes by sequential shifts of $\tilde{\alpha}$-components, *Probl. Peredachi Inf.,* **33**, No. 3, 15–21, 1997 [Russian]. Translated in *Probl. Inf. Transm.,* **33**, No. 3, 202–207, 1997.
2. **Yu. L. Vasil'ev,** On nongroup close-packed codes, in A. A. Lyapunov, ed., *Problemy kibernetiki* (Problems of Cybernetics), Vol. 8, pp. 337–339, Fizmatgiz, Moscow, 1962 [Russian].
3. **S. A. Malyugin,** On enumeration of the perfect binary codes of length 15, *Diskretn. Anal. Issled. Oper., Ser. 2,* **6**, No. 2, 48–73, 1999 [Russian]. Translated in *Discrete Appl. Math.,* **135**, No. 1–3, 161–181, 2004.
4. **S. A. Malyugin,** Nonsystematic perfect binary codes, *Diskretn. Anal. Issled. Oper., Ser. 1,* **8**, No. 1, 55–76, 2001 [Russian].
5. **S. A. Malyugin,** Perfect binary codes of infinite length, *Prikl. Diskretn. Mat., Prilozh.,* No. 8, 117–120, 2015 [Russian].
6. **V. N. Potapov**, Infinite-dimensional quasigroups of finite orders, *Mat. Zametki,* **93**, No. 3, 457–465, 2013 [Russian]. Translated in *Math. Notes,* **93**, No. 3, 479–486, 2013.

7. A. M. Romanov, On construction of perfect nonlinear binary codes by symbol inversion, *Diskretn. Anal. Issled. Oper., Ser. 1,* **4**, No. 1, 46–52, 1997 [Russian].

8. K. T. Phelps and **M. LeVan,** Kernels of nonlinear Hamming codes, *Des. Codes Cryptogr.,* **6**, No. 3, 247–257, 1995.

9. F. I. Solov'eva, Switchings and perfect codes, in I. Althöfer et al., eds., *Numbers, Information and Complexity,* pp. 311–324, Kluwer Acad. Publ., Dordrecht, 2000.

Serguey A. Malyugin

Received
31 March 2016
Revised
29 August 2016