

УДК 519.72

## О ПОДВИЖНЫХ МНОЖЕСТВАХ В ДВОИЧНОМ ГИПЕРКУБЕ\*)

Ю. Л. Васильев, С. В. Августинович, Д. С. Кротов

**Аннотация.** Если два кода с расстоянием три имеют одинаковую окрестность, каждый из них называется *подвижным множеством*. В двоичном  $(4k+3)$ -мерном гиперкубе существует подвижное множество мощности  $2 \cdot 6^k$ , которое нельзя разбить на подвижные множества меньшей мощности или представить в виде естественного расширения подвижного множества меньшей размерности.

**Ключевые слова:** 1-совершенный код, булев куб, подвижное множество,  $i$ -компонента.

### Введение

Через  $\mathbb{E}^n$  обозначается метрическое пространство всех двоичных слов длины  $n$  с метрикой Хемминга. Пространство  $\mathbb{E}^n$  иногда называют двоичным, или единичным, или булевым кубом. Базисный вектор с единицей в  $i$ -й координате и нулями в остальных обозначается через  $e_i$ . Подмножество  $M \subseteq \mathbb{E}^n$  будем называть *1-кодом*, если шары радиуса 1 с центрами из  $M$  не пересекаются между собой. *Окрестностью*  $\Omega(M)$  множества  $M$  назовём объединение шаров радиуса 1 с центрами из  $M$ , т. е.  $\Omega(M) = \{x \in \mathbb{E}^n \mid d(x, M) \leq 1\}$ .

Если 1-код  $M$  обладает свойством  $\Omega(M) = \mathbb{E}^n$ , он называется совершенным, или *1-совершенным кодом*. 1-Совершенные коды существуют лишь в размерностях вида  $n = 2^k - 1$ . Для  $n = 7$  такой код единственный (с точностью до изометрий пространства), а именно линейный код Хемминга. При  $n = 15$  проблема описания и перечисления 1-совершенных кодов до сих пор не решена, несмотря на постоянно растущие возможности вычислительной техники (существенное продвижение получено в работах [2, 4]). В контексте упомянутой проблемы представляется актуальным изучение объектов, обобщающих в разных смыслах понятие

---

\*) Исследование второго и третьего авторов выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 07-01-00248-а и 08-01-00673-а соответственно).

1-совершенного кода и существующих не только при  $n = 2^k - 1$ , но и в промежуточных размерностях. Такими объектами являются совершенные раскраски (в частности, двуцветные [8]), центрированные функции [10], а также подвижные множества, о которых пойдёт речь в данной статье.

Множество  $M \subseteq \mathbb{E}^n$  называется *подвижным* (сокращённо *п. м.*), если: 1)  $M$  является 1-кодом, 2) существует непересекающийся с  $M$  1-код  $M'$  с той же окрестностью, т. е.  $M \cap M' = \emptyset$  и  $\Omega(M) = \Omega(M')$ ; такое множество  $M'$  будем называть *альтернативой* множества  $M$ .

Другими словами, 1-код является п. м., если у него есть альтернатива.

Для всякого нечётного  $n = 2m + 1$  несложно построить линейное (замкнутое относительно покомпонентного сложения по модулю 2) подвижное множество в  $\mathbb{E}^n$ :

$$M = \{(x, x, |x|) \mid x \in \mathbb{E}^m\}. \quad (1)$$

Здесь и далее  $|x|$  есть сумма координат вектора  $x$  по модулю 2. Соответственно

$$M' = \{(x, x, |x| \oplus 1) \mid x \in \mathbb{E}^m\}.$$

Убедиться в выполнении условий 1 и 2 для  $M$  и  $M'$  нетрудно.

Основной целью нашей работы является доказательство следующего факта.

**Теорема 1.** *Для всех  $n \geq 7$ , сравнимых с 3 по модулю 4, в  $\mathbb{E}^n$  существует нередуцируемое неделимое подвижное множество.*

Непустое п. м. называется *разделимым* (*неделимым*), если его можно (нельзя) представить в виде объединения двух непустых п. м. Понятие редуцируемости, которое будет сформулировано в разд. 3, отражает естественную сводимость подвижных множеств к подвижным множествам на 2 меньшей размерности.

Простой способ построения п. м. в гиперкубах кодовой размерности  $n = 2^k - 1$  заключается в следующем. Пусть  $C$  и  $C'$  — 1-совершенные коды в  $\mathbb{E}^n$ . Тогда  $M = C \setminus C'$  является п. м. Действительно, в качестве  $M'$  можно взять  $C' \setminus C$ . Мощность такого п. м. равна  $|C| - |C \cap C'|$ . Мы же исследуем вопрос существования п. м. в некодовых размерностях, которые нельзя получить из п. м. в кодовых размерностях при помощи элементарных операций.

В разд. 1 мы определяем расширенные подвижные множества, в терминах которых удобно описывать конструкцию. В разд. 2 описана связь подвижных множеств и  $i$ -компонент, которые активно изучались ранее.

В разд. 3 описывается конструкция увеличения размерности подвижного множества, приводящая к естественному понятию редуцируемого п. м. В разд. 4 приводится основная конструкция и доказательство теоремы. В заключительном разделе мы формулируем несколько задач.

### 1. Расширенные подвижные множества

С подвижными множествами, как и с 1-совершенными кодами, часто бывает удобно работать, расширив их в следующую размерность проверки на чётность. При этом в некоторых случаях получаются более симметричные объекты, что упрощает доказательства и формулировки утверждений. И хотя геометрическая интерпретация объектов после добавления проверки на чётность может казаться не столь изящной и естественной, как в оригинале, а переход к ней требует некоторого привыкания, многие утверждения становятся более простыми и наглядными, будучи сформулированными для расширенного случая.

Напомним, что *расширением* множества  $M \subseteq \mathbb{E}^n$  называется множество  $\overline{M} \subseteq \mathbb{E}^{n+1}$ , полученное добавлением проверки на чётность (нечётность) ко всем словам множества  $M$ :  $\overline{M} = \{(x, |x|) \mid x \in M\}$  или  $\overline{M} = \{(x, |x| \oplus 1) \mid x \in M\}$ . *Выкалывание*  $i$ -й координаты в некотором множестве слов из  $\mathbb{E}^n$  означает удаление  $i$ -го символа во всех словах множества (результат будет лежать в  $\mathbb{E}^{n-1}$ ). Очевидно, что расширение и затем выкалывание последней координаты приводит к исходному множеству, т. е. эти операции в определённом смысле обратны друг другу.

Множество  $\overline{M} \subseteq \mathbb{E}^n$  назовём *расширенным подвижным (р. п. м.)*, если оно получается расширением некоторого п. м.

Нам будет полезна следующая лемма, которая даёт альтернативные определения р. п. м. Как и обычное п. м., р. п. м.  $M$  можно определить в паре с другим р. п. м.  $M'$ , которое также естественно называть *альтернативой* р. п. м.  $M$  (из контекста обычно ясно, подвижные или расширенные подвижные множества рассматриваются). Для формулировки леммы и дальнейшего использования удобно определить понятие *сферической окрестности*  $\dot{\Omega}(M) = \Omega(M) \setminus M$ , которое для расширенных подвижных множеств выполняет роль, аналогичную роли обычной («шаровой») окрестности для п. м. В частности, условие (с) леммы 1 определяет р. п. м. и его альтернативу аналогично случаю с подвижным множеством.

**Лемма 1** (об альтернативных определениях р. п. м.). Пусть  $M$  и  $M'$  — непересекающиеся 1-коды в  $\mathbb{E}^n$ , векторы которых имеют одинаковую чётность (либо все чётновесовые, либо нечётновесовые) и  $i \in \{1, \dots, n\}$ . Следующие условия эквивалентны и влекут тот факт,

что  $M$  и  $M'$  — р. п. м.

(а) Множества  $M_i$  и  $M'_i$ , полученные из  $M$  и  $M'$  выкалыванием  $i$ -й координаты, подвижны и являются альтернативой друг друга.

(б) Двудольный граф  $G(M \cup M')$  расстояний 2 объединения  $M \cup M'$  имеет степень  $n/2$ .

(с)  $\dot{\Omega}(M) = \dot{\Omega}(M')$ .

ДОКАЗАТЕЛЬСТВО. При  $i = n$  из (а) следует, что  $M$  — р. п. м. по определению. Поскольку условия (б) и (с) не зависят от выбора  $i$ , достаточно показать эквивалентность (а), (б) и (с).

(с)  $\Rightarrow$  (б). Рассмотрим вектор  $v$  из  $M$  и множество пар  $k, j \in \{1, \dots, n\}$  таких, что

$$v \oplus e_k \oplus e_j \in M'. \quad (2)$$

Поскольку  $M$  и  $M'$  не пересекаются,  $k$  и  $j$  в такой паре всегда различны. Так как  $M'$  — 1-код, две различные пары не пересекаются. Из условия  $\dot{\Omega}(M) = \dot{\Omega}(M')$  следует, что любой элемент из  $\{1, \dots, n\}$  принадлежит некоторой паре. Таким образом, мы имеем разбиение  $\{1, \dots, n\}$  на пары  $k, j$ , удовлетворяющие (2). Отсюда следует, что степень вершины  $v$  в графе  $G(M \cup M')$  равна  $n/2$ . То же верно для любого  $v'$  из  $M'$ .

(а)  $\Rightarrow$  (с). Рассмотрим вектор  $w$  на расстоянии 1 от  $M$ . Нам нужно показать, что он расположен на расстоянии 1 от  $M'$ . Действительно, в противном случае расстояние от  $w$  до  $M'$  равно как минимум 3 (учитывая одинаковую чётность  $M$  и  $M'$ ) и после выкалывания  $i$ -й координаты  $w$  не попадёт в  $\Omega(M'_i)$ , что противоречит условию  $\Omega(M_i) = \Omega(M'_i)$ . Таким образом,  $\dot{\Omega}(M) \subseteq \dot{\Omega}(M')$ ; аналогично  $\dot{\Omega}(M') \subseteq \dot{\Omega}(M) \setminus M$ .

(б)  $\Rightarrow$  (а). Рассмотрим вектор  $v$  из  $M$ . Поскольку степень  $v$  в  $G(M \cup M')$  равна  $n/2$  и в  $M'$  нет двух векторов на расстоянии 2, все координаты делятся на пары  $k, j$ , удовлетворяющие (2). Отсюда любой вектор вида  $v + e_j$ ,  $1 \leq j \leq n$ , лежит в  $\Omega(M')$ , а после выкалывания  $i$ -й координаты — в  $\Omega(M'_i)$ . Но все такие векторы после выкалывания составляют  $\Omega(M_i)$ . Следовательно,  $\Omega(M_i) \subseteq \Omega(M'_i)$ . Аналогично  $\Omega(M'_i) \subseteq \Omega(M_i)$ . Осталось заметить, что  $M_i \cap M'_i = \emptyset$ , поскольку  $M$  и  $M'$  не пересекаются и имеют одинаковую чётность. Лемма 1 доказана.

Учитывая условие (б) и существование линейного п. м., имеем важное

**Следствие 1.** *Необходимым и достаточным условием существования непустых п. м. (р. п. м.) в  $\mathbb{E}^n$  является нечётность (чётность)  $n$ .*

## 2. $i$ -Компоненты

Содержание данного раздела не используется при доказательстве основного результата. Однако оно необходимо для понимания связей с

предшествующими исследованиями, ориентированными на частный случай п. м., так называемые  $i$ -компоненты.

П. м.  $M$  будем называть  $i$ -компонентой, если  $\Omega(M) = \Omega(M \oplus e_i)$ . Рассмотрим множество  $M_i$ , полученное из  $M$  выкалыванием  $i$ -й координаты. Построим на  $M_i$ , как на вершинах, так называемый граф минимальных расстояний  $G(M_i)$ , соединив ребрами вершины на расстоянии 2. Доказательство следующей леммы аналогично доказательству леммы 1, и мы опускаем его.

**Лемма 2.** 1-Код  $M$  является  $i$ -компонентой тогда и только тогда, когда граф  $G(M_i)$  является однородным степени  $(n-1)/2$  и двудольным.

Таким образом, леммы 1 и 2 устанавливают соответствие между парами альтернативных п. м. в  $\mathbb{E}^{n-1}$  и  $i$ -компонентами в  $\mathbb{E}^{n+1}$  (при фиксированном  $i$ , например,  $n+1$ ). Эта связь проявляется в том, что обоим объектам соответствует множество в  $\mathbb{E}^n$ , граф расстояний 2 которого является двудольным и имеет степень  $n/2$ . В первом случае все вершины множества будут иметь одинаковую чётность. Во втором — не обязательно, однако множества разной чётности будут соответствовать разбиению  $i$ -компоненты на независимые  $i$ -компоненты, « $i$ -чётную» и « $i$ -нечётную». Формально, мы можем сформулировать

**Следствие 2.** Множества  $M, M' \subseteq \mathbb{E}^{n-1}$  являются п. м. и его альтернативой тогда и только тогда, когда множество

$$\{(x, |x|, 0) \mid x \in M\} \cup \{(x, |x|, 1) \mid x \in M'\}$$

является  $i$ -компонентой при  $i = n+1$ .

**Следствие 3.** Множество  $M \subseteq \mathbb{E}^{n+1}$  есть  $i$ -компонента,  $i = n+1$ , если и только если множества

$$M_a^b = \{x \mid (x, |x| \oplus a, b) \in M\}, \quad a, b \in \{0, 1\},$$

подвижные, причём  $M_a^0$  и  $M_a^1$  являются альтернативами друг другу (множества  $M_0^0$  и  $M_0^1$  соответствуют « $i$ -чётной» части  $i$ -компоненты,  $M_1^0$  и  $M_1^1$  — « $i$ -нечётной»; каждая из этих частей может быть пустой, причём, если обе непусты, то  $i$ -компонента разделима).

Примером  $i$ -компоненты является линейное п. м. (1),  $i = n$ . Ранее [6, 9] уже строились многочисленные примеры нелинейных подвижных множеств, являющихся  $i$ -компонентами. Все они вложимы в 1-совершенные коды, каждый из них имеет мощность, кратную мощности линейной компоненты. Кроме того, доказанной была лишь неделимость этих

$i$ -компонент на меньшие  $i$ -компоненты. Вопрос, можно ли такую  $i$ -компоненту разбить на меньшие подвижные множества, не являющиеся  $i$ -компонентами, остаётся открытым. Поэтому, несмотря на то, что исследования посвящены общей проблеме (характеризация множества совершенных кодов) и даже общему подходу к решению этих проблем, направления несколько различны и результаты не перекрываются, а дополняют друг друга: мы отказываемся от вложимости в 1-совершенные коды (что является ослаблением), зато имеем дело с более сильной неделимостью и с бóльшим спектром размерностей.

### 3. Редуцируемость

**Лемма 3** (о линейном расширении п. м.). Пусть  $M, M' \subseteq \mathbb{E}^n$  — р. п. м. и его альтернатива. Тогда

$$\begin{aligned} R &= \{(x, 0, 0) \mid x \in M\} \cup \{(x, 1, 1) \mid x \in M'\}, \\ R' &= \{(x, 1, 1) \mid x \in M\} \cup \{(x, 0, 0) \mid x \in M'\} \end{aligned} \quad (3)$$

суть р. п. м. и его альтернатива в  $\mathbb{E}^{n+2}$ .

**ДОКАЗАТЕЛЬСТВО.** Выполнение условия (b) леммы 1 для  $M$  и  $M'$  непосредственно влечёт справедливость этого условия для  $R$  и  $R'$ . Лемма 3 доказана.

Р. п. м.  $R \subseteq \mathbb{E}^n$  назовём *редуцируемым*, если оно может быть получено конструкцией (3), а также перестановкой координат и инверсией некоторых символов, применёнными ко всем векторам множества одновременно. П. м. назовём *редуцируемым*, если соответствующее ему р. п. м. редуцируемо.

Таким образом, вопрос существования редуцируемых п. м. сводится к существованию п. м. в меньших размерностях. С этой точки зрения задача построения нередуцируемых п. м., рассмотренная в настоящей статье, является естественной.

**Замечание.** Как видно из следствия 3, любая  $i$ -компонента либо является редуцируемым п. м., либо разбивается на две  $i$ -компоненты (« $i$ -чётную» и « $i$ -нечётную»), каждая из которых — редуцируемое п. м. В частности, линейное п. м. (1) является редуцируемым. Более того, линейное р. п. м. с точностью до перестановки координат может быть получено из тривиального р. п. м.  $\{00\}$  в  $\mathbb{E}^2$  последовательным применением конструкции из леммы 3.

### 4. Доказательство теоремы

Зафиксируем  $n$ , кратное четырём:  $n = 4k$ . Разобьём номера координат на  $k$  групп по 4 в каждой и переобозначим соответствующие ор-

ты следующим образом:  $e_0^1, e_1^1, e_2^1, e_3^1, e_0^2, \dots, e_3^k$ . В каждой четвёрке вида  $\{e_0^i, e_1^i, e_2^i, e_3^i\}$  выберем произвольно (всего 6 возможностей) пару несовпадающих ортов  $e_j^i$  и  $e_t^i$  и назовём *индексом* этой пары число  $p\{j, t\}$ , где

$$p\{0, 1\} = p\{2, 3\} = 0, \quad p\{0, 2\} = p\{1, 3\} = 1, \quad p\{0, 3\} = p\{1, 2\} = 2.$$

Просуммировав выбранные пары по всем  $i = 1, 2, \dots, k$ , мы получим вектор веса  $2k$ , который будем называть *стандартным*. Всего получится  $6^k$  стандартных векторов. *Индексом*  $I(v)$  стандартного вектора  $v$  будем называть сумму по модулю 3 всех индексов составляющих его пар ортов.

Разобьём множество стандартных векторов на непересекающиеся подмножества  $S_0, S_1$  и  $S_2$  в соответствии с их индексами.

**Утверждение 1.** Пусть  $i \neq j$ ,  $i, j \in \{0, 1, 2\}$ . Тогда граф  $G(S_i \cup S_j)$  расстояний 2, индуцированный множеством векторов  $S_i \cup S_j$ , является двудольным и однородным степени  $2k$ .

**ДОКАЗАТЕЛЬСТВО.** Для начала заметим, что графы  $G(S_i)$  и  $G(S_j)$  пусты. Действительно, рассмотрим пару векторов  $v, u \in S_i$ . Либо  $v$  и  $u$  различаются в одной четвёрке координат, тогда  $d(v, u) = 4$ , поскольку у них индексы одинаковы, либо  $v$  и  $u$  различаются в большем чем одна числе четвёрок, тогда  $d(v, u) \geq 4$ , поскольку по каждой четвёрке расстояние между стандартными векторами чётно. Таким образом, двудольность графа  $G(S_i \cup S_j)$  установлена.

Также легко понять, что всякий вектор индекса  $i$  имеет ровно двух соседей на расстоянии 2 из  $S_j$ , различающихся с ним в одной фиксированной четвёрке координат. Это означает, что степень графа равна  $2k$ . Утверждение 1 доказано.

Таким образом,  $S_0$  (как  $S_1$  и  $S_2$ ) — р. п. м. мощности  $2 \cdot 6^{k-1}$ .

**Утверждение 2.** Р. п. м.  $S_0$  неделимое.

**ДОКАЗАТЕЛЬСТВО.** Предположим, что  $P \subseteq S_0$  и  $Q = S_0 \setminus P$  — непустые р. п. м. Тогда  $P$  и  $Q$  имеют альтернативы, обозначим их через  $P'$  и  $Q'$  соответственно.

Сначала убедимся, что

(\*)  $P'$  (аналогично  $Q'$ ) состоит только из стандартных векторов, т. е. таких векторов, что в каждой четвёрке координат с номерами вида  $4i-3, 4i-2, 4i-1, 4i$  содержится ровно две единицы.

Действительно, в противном случае  $P'$  содержит вектор с нестандартной четвёркой и, как следствие,  $\dot{\Omega}(P')$  содержит вектор с двумя нестандартными четвёрками. В то же время  $\dot{\Omega}(P)$  состоит из векторов с одной нестандартной четвёркой и, следовательно, не может совпадать с  $\dot{\Omega}(P')$ , что противоречит лемме 1. Утверждение (\*) доказано.

Дальнейшее доказательство проведём в двух вариантах.

СПОСОБ 1. Нам понадобится простое утверждение. (\*\*) Граф  $G(S_i \cup S_j)$  расстояний 2 связан ( $i, j \in \{0, 1, 2\}$ ,  $i \neq j$ ).

Докажем его индукцией по  $k$ . При  $k = 2$  утверждение проверяется непосредственно. Пусть  $k > 2$ . Достаточно показать, что произвольные два слова  $u$  и  $v$  из  $S_i \cup S_j$  принадлежат одной компоненте связности. Если  $u$  и  $v$  совпадают в некоторой четвёрке координат, то требуемое следует из индуктивного предположения (зафиксировав эту четвёрку, мы получим подграф, изоморфный графу, рассмотренному на предыдущем индукционном шаге). Если  $u$  и  $v$  различаются во всех четвёрках, то найдётся слово  $w$  из  $S_i \cup S_j$ , которое совпадает в первой четвёрке с  $u$ , а во второй — с  $v$  (остальные четвёрки подбираются так, чтобы получился нужный индекс,  $i$  или  $j$ ). Аналогично уже рассмотренному случаю,  $u$ ,  $w$  и  $v$  лежат в одной компоненте связности. Утверждение (\*\*) доказано.

Поскольку  $P'$  и  $Q'$  состоят из стандартных векторов, они лежат в  $S_1 \cup S_2$ . Обозначим

$$P_1 = P' \cap S_1, \quad P_2 = P' \cap S_2, \quad Q_1 = Q' \cap S_1, \quad Q_2 = Q' \cap S_2.$$

Если  $P_1 = Q_1 = \emptyset$ , то, как следует из леммы 1(b),  $P \cup P_2$  и  $Q \cup Q_2$  соответствуют компонентам связности графа  $G(S_0 \cup S_2)$ , что противоречит утверждению (\*\*). Аналогично не может быть  $P_2 = Q_2 = \emptyset$ .

Имеем  $\dot{\Omega}(P_1 \cup P_2) \cup \dot{\Omega}(Q_1 \cup Q_2) = \dot{\Omega}(P) \cup \dot{\Omega}(Q) = \dot{\Omega}(S_0)$ . С другой стороны,  $\dot{\Omega}(S_1) = \dot{\Omega}(S_0)$ , поэтому  $\dot{\Omega}(S_1 \setminus P_1 \setminus Q_1) = \dot{\Omega}(P_2 \cup Q_2)$ . Аналогично  $\dot{\Omega}(S_2 \setminus P_2 \setminus Q_2) = \dot{\Omega}(P_1 \cup Q_1)$ . Таким образом,  $S_1$  разбивается на два непустых подвижных множества, альтернативы которых лежат в  $S_2$ . Из леммы 1(b) следует несвязность графа  $G(S_1 \cup S_2)$ , что противоречит утверждению (\*\*) и доказывает утверждение 2.

СПОСОБ 2. Рассмотрим произвольный вектор  $p$  из  $P$  и покажем следующее.

(\*\*\*) Все векторы из  $S_0$ , отличающиеся от  $p$  не более чем в двух четвёрках, также принадлежат  $P$ .

Без потери общности рассмотрим две первые четвёрки. Положим  $p = (h, t)$ , где  $h$  и  $t$  — векторы длины 8 и  $n - 8$  соответственно. Рассмотрим вектор  $p \oplus e_j^i$  из  $\dot{\Omega}(P)$ , где  $i \in \{1, 2\}$  и  $j \in \{0, 1, 2, 3\}$ . Согласно лемме 1 для некоторого  $p'$  из  $P'$  выполнено включение  $p \oplus e_j^i \in \dot{\Omega}(p')$ . Как доказано выше, вектор  $p'$  стандартный, поэтому  $p' = p \oplus e_j^i \oplus e_{j'}^i$ , для некоторого  $j' \in \{0, 1, 2, 3\}$ . Следовательно,  $p'$  совпадает с  $p$  в последних  $n - 8$  координатах. Аналогичными рассуждениями получаем, что

$\dot{\Omega}(P_8) = \dot{\Omega}(P'_8)$ , где  $P_8 = \{b \in \mathbb{E}^8 \mid (b, t) \in P\}$ ,  $P'_8 = \{b \in \mathbb{E}^8 \mid (b, t) \in P'\}$ , и по лемме 1(c)  $P_8$  — р. п. м. в  $\mathbb{E}^8$ . Легко установить (например, пользуясь леммой 1(b)), что мощность р. п. м. в  $\mathbb{E}^8$  больше 6. С другой стороны, по построению ровно 12 векторов из  $S_0$  имеют вид  $(b, t)$ ,  $b \in \mathbb{E}^8$ . Следовательно, больше половины таких векторов принадлежат  $P$ . Если бы не все принадлежали  $P$ , то к оставшимся векторам (из  $S_0 \setminus P$ ) были бы применимы аналогичные рассуждения, что привело бы к противоречию. Следовательно, все 12 векторов из  $S_0$ , совпадающих с  $p$  во всех координатах кроме первых восьми, принадлежат  $P'$ , что доказывает утверждение (\*\*\*)).

Таким образом, любые два вектора из  $S_0$  на расстоянии 4 друг от друга одновременно либо принадлежат  $P$ , либо нет. Поскольку  $S_0$ , очевидно, связно по расстоянию 4, получаем  $P = S_0$ . Утверждение 2 доказано.

**Утверждение 3.** *Р. п. м.  $S_0$  не редуцируемо.*

**ДОКАЗАТЕЛЬСТВО.** Заметим, что в конструкции (3) сумма последних двух координат равна 0 для любого слова из  $R$ . Учитывая перестановку координат и инверсию символов, можно утверждать, что у редуцируемого р. п. м. существуют две координаты, сумма которых равна 0 либо 1 одновременно для всех слов множества. Легко проверить, что  $S_0$  не удовлетворяет этому условию: любые две координаты содержат все четыре комбинации из 0 и 1. Утверждение 3 доказано. Теорема доказана.

## 5. Заключение

Мы построили бесконечный класс неделимых нередуцируемых п. м. Конструкция обобщает пример, упомянутый в конце работы [1]. В заключение сформулируем несколько нерешённых задач, естественно связанных с исследованием подвижных множеств и с основной проблемой, обобщающей проблему характеристики совершенных кодов:

- характеризовать многообразие подвижных множеств.

Для построения п. м. можно применять принцип обобщённой каскадной конструкции для 1-совершенных кодов [3]. В частности, конструкция из разд. 4 может быть интерпретирована в таких терминах. неделимые п. м., построенные таким образом, будут иметь неполный ранг, т. е. для всех слов множества координаты будут удовлетворять некоторому линейному уравнению (неполной проверке на чётность или нечётность).

**Задача 1.** *Построить бесконечный класс неделимых п. м. полного ранга.*

**Пример.** Рассмотрим четыре слова

$$\begin{pmatrix} 100 \\ 110 \\ 010 \end{pmatrix}, \quad \begin{pmatrix} 011 \\ 110 \\ 000 \end{pmatrix}, \quad \begin{pmatrix} 101 \\ 001 \\ 011 \end{pmatrix}, \quad \begin{pmatrix} 001 \\ 100 \\ 111 \end{pmatrix}$$

из  $\mathbb{E}^9$ , записанные для удобства в виде массива  $3 \times 3$ , а также все слова, полученные из них циклическими перестановками строк и/или столбцов массива. Получим неделимое п. м. полного ранга мощности 36. Альтернатива получается инверсией всех слов.

**Задача 2.** Построить богатый класс транзитивных неделимых п. м., р. п. м.

Множество  $M \subseteq \mathbb{E}^n$  называется *транзитивным*, если стабилизатор  $\text{Stab}_I(M)$  множества  $M$  в группе  $I$  изометрий гиперкуба действует транзитивно на элементах  $M$ , т. е. для любых  $x, y$  из  $M$  найдётся изометрия  $\sigma \in \text{Stab}_I(M)$  такая, что  $\sigma(x) = y$ . Например, нетрудно показать, что п. м., построенные в данной работе, являются транзитивными. Известно несколько конструкций транзитивных 1-совершенных и расширенных 1-совершенных кодов, последние результаты см. в [7, 5].

**Задача 3.** Исследовать вопрос вложимости п. м. в 1-совершенный код: существование невложимых п. м. в кодовых размерностях  $n = 2^k - 1$ ; существование п. м., невложимых при помощи линейного расширения (лемма 3) в 1-совершенный код ни в одной большей размерности.

В частности, для п. м., построенных в разд. 4, вопросы вложимости открыты при  $n \geq 11$ .

**Задача 4.** Оценить максимальный размер неделимого п. м.

**Задача 5.** Оценить минимальный размер нелинейного п. м. (конструкция разд. 4 вместе с леммой 3 даёт верхнюю оценку  $1,5L(n)$ , где  $L(n) = 2^{(n-1)/2}$  — мощность линейного п. м.), нередуцируемого неделимого п. м. (конструкция даёт верхнюю оценку  $1,5^{(n-3)/4}L(n)$ ) и неделимого п. м. полного ранга.

**Задача 6.** Изучить подвижные множества в других пространствах, в частности, в  $q$ -ичных пространствах Хемминга, где  $q > 2$  — произвольное целое число, не обязательно степень простого.

## ЛИТЕРАТУРА

1. Васильев Ю. Л., Соловьева Ф. И. Кодообразующие факторизации  $n$ -мерного единичного куба и совершенных двоичных кодов // Проблемы передачи информации. — 1997. — Т. 33, вып. 1. — С. 64–74.

2. **Зиновьев В. А., Зиновьев Д. В.** Двоичные расширенные совершенные коды длины 16 ранга 14 // Проблемы передачи информации. — 2006. — Т. 42, вып. 2. — С. 63–80.
3. **Зиновьев В. А., Лобстейн А.** Об обобщённых каскадных конструкциях совершенных двоичных нелинейных кодов // Проблемы передачи информации. — 2000. — Т. 36, вып. 4. — С. 59–73.
4. **Малюгин С. А.** О перечислении неэквивалентных совершенных двоичных кодов длины 15 и ранга 15 // Дискрет. анализ и исслед. операций. Сер. 1. — 2006. — Т. 13, № 1. — С. 77–98.
5. **Потапов В. В.** О нижней оценке числа транзитивных совершенных кодов // Дискрет. анализ и исслед. операций. Сер. 1. — 2006. — Т. 13, № 4. — С. 49–59.
6. **Соловьева Ф. И.** О факторизации кодообразующих д.н.ф. // Методы дискретного анализа в исследовании функциональных систем. Сб. научн. тр. Вып. 47. — Новосибирск: Ин-т математики СО АН СССР, 1988. — С. 66–88.
7. **Соловьева Ф. И.** О построении транзитивных кодов // Проблемы передачи информации. — 2005. — Т. 41, вып. 3. — С. 23–31.
8. **Фон-Дер-Флаасс Д. Г.** Совершенные 2-раскраски гиперкуба // Сиб. мат. журн. — 2007. — Т. 48, № 4. — С. 923–930.
9. **Solov'eva F. I.** Structure of  $i$ -components of perfect binary codes // Discrete Appl. Math. — 2001. — Vol. 111, N 1–2. — P. 189–197. — DOI: 10.1016/S0166-218X(00)00352-8.
10. **Vasil'eva A. Yu.** A representation of perfect binary codes // Proc. seventh international workshop on algebraic and combinatorial coding theory. — Bansko, Bulgaria: 2000, June. — P. 311–315.

Васильев Юрий Леонидович,  
e-mail: vas@math.nsc.ru

Августинович Сергей Владимирович,  
e-mail: avgust@math.nsc.ru

Кротов Денис Станиславович,  
e-mail: krotov@math.nsc.ru

Статья поступила  
27 декабря 2007 г.

Переработанный вариант —  
3 апреля 2008 г.