S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

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

Том 13, стр. 645–655 (2016) УДК 519.725
DOI 10.17377/semi.2016.13.051 MSC 94B60

О КЛАССЕ СОВЕРШЕННЫХ КОДОВ С МАКСИМАЛЬНЫМИ КОМПОНЕНТАМИ

И.Ю. МОГИЛЬНЫХ, Ф.И. СОЛОВЬЕВА

Abstract. We show the existence of a wide class of binary extended perfect Solov'eva codes of length 16 with ij-components of maximum size.

Keywords: perfect binary codes, component.

1. Введение

Компоненты совершенных двоичных кодов изучались большим числом исследователей. Всюду далее будут рассматриваться двоичные коды и потому термин двоичный будет опущен. Эти объекты имеют весьма сложную структуру, используя их, удалось решить множество открытых проблем, стоящих в теории совершенных кодов, см. обзоры [1, 2]. Множество K в пространстве всех двоичных векторов F_2^n называется *i-компонентой*, если множество векторов, объединение шаров радиуса 1 с центрами в множествах K и $K + e_i = \{k + e_i : k \in K\}$ совпадают, где e_i – двоичный вектор с единицей только в координатной позиции i, $i \in \{1, 2, \ldots, n\}$. Далее будем рассматривать лишь *неразложимые* компоненты, то есть те, которые нельзя разбить на компоненты меньшей мощности. Будем называть i-компоненту *минимальной* (*максимальной* в случае, если мощность компоненты меньше мощности кода), если она имеет наименьшую (наибольшую) возможную мощность. Известно [3], что минимальная компонента совершенного двоичного кода длины $n = 2^m - 1$, $m \geq 3$ единственна с точностью до изоморфизма и может быть представлена формулой $\{(x, |x|, x) : x \in F_2^{(n-1)/2}\}$. Максимальной мощности i-компоненты

Mogilnykh, I.Yu., Solov'eva, F.I., On a class of perfect codes with maximum components.

Работа выполнена при финансовой поддержке гранта Российский Научный Фонд 14-11-00555.

Поступила 29 октября 2015 г., опубликована 15 августа 2016 г.

были впервые построены в 1988 г. в работе [4]. Оказалось, что эти компоненты занимают половину множества кодовых слов совершенного кода. Существование совершенных кодов с i-компонентами различных мощностей установлено в 1995 г. в работе [5]. В 2001 г. в статье [6] было доказано существование максимальных неизоморфных i-компонент, принадлежащих различным совершенным кодам для любой допустимой длины $n = 2^m - 1, m > 3$. П. Р. Ж. Остергард и О. Поттонен, см. [7, 8], перечислили все возможные размеры i-компонент совершенных кодов длины 15 и, в частности, установили, что размер любой компоненты для любого совершенного кода длины 15 всегда кратен размеру минимальной компоненты. Более того, они перечислили все совершенные коды длины 15 с указанием состава мощностей i-компонент, см. [9]. В 2012 г. В. Н. Потапов [10] описал для совершенных кодов возможные размеры компонент мощностей, близких к минимальной, для любой допустимой длины.

К. Т. Фелпс и М. ЛеВан [11], используя конструкцию работы [12], в 1999 г. доказали, что существуют совершенные коды длины 15, которые невозможно получить из кода Хэмминга методом свитчинга. Напомним, что код C' длины n получен из кода C той же длины *свитчингом компоненты* $K \subset C$, если $C' = (C \setminus K) \cup (K + e_i)$ для некоторого $i \in \{1, 2, \ldots, n\}$. Построенный в [11] класс кодов состоит из двух неизоморфных совершенных кодов длины 15, каждый из которых по любой координате разбивается на две максимальные компоненты.

В [8] были перечислены все (многошаговые) свитчинговые классы совершенных кодов длины 15, их оказалось девять, один из которых имеет максимальную мощность, равную 5819, что представляет собой подавляющую часть от общего числа 5983 всех неэквивалентных совершенных кодов длины 15. Среди этих девяти классов обнаружено четыре спорадических класса, каждый состоящий только из одного совершенного кода.

2. Обозначения и необходимые утверждения

Основные определения и обозначения см. в [13]. Напомним определение совершенного кода: произвольное подмножество векторов C из F_2^n называется *совершенным двоичным кодом* длины n, исправляющим одну ошибку, если для любого вектора $x \in F_2^n$ найдется единственный вектор y из C на расстоянии не более 1 от x. Такие коды существуют только при $n = 2^m - 1$, $m > 1$. Далее в статье будем использовать транзитивные разбиения множества векторов четного (нечетного) веса в F_2^n, $n = 2^m$, $m \geq 3$ на максимально непараллельные расширенные коды Хэмминга, предложенные Д.С.Кротовым в [14]. Для $n = 8$ такое разбиение (разбиение под номером 8) было приведено К.Т.Фелпсом в [15], поэтому при $n = 8$ ниже будем ссылаться на него как на разбиение Фелпса.

Следуя терминологии и определениям [14], будем рассматривать линейные коды длины $n = 2^m$, $m \geq 3$ как совокупности подмножеств X конечного поля $\mathbf{F} = GF(2^m)$, элементы которого, занумерованные в порядке возрастания степеней примитивного элемента α, есть кодовые координаты и удовлетворяют некоторым проверочным соотношениям.

Для $\alpha^k \in \mathbf{F}$, $p \in \{0, 1\}$ определим код $H^p_{\alpha^k}$ как совокупность подмножеств X в поле $\mathbf{F}$, удовлетворяющих проверочным соотношениям:

$$\sum_{x \in X} 1 = p,$$

$$\sum_{x\in X}(x+\alpha^k)^3=0.$$

Также определим код Хэмминга $\overline{H}$ как циклический код с порождающим многочленом, являющимся минимальным для α:

$$\sum_{x\in X}1=0,$$

$$\sum_{x\in X}x=0.$$

Легко видно, что H^0_α – расширенный код Хэмминга, а H^1_α – его класс смежности. Всюду далее будем опускать верхний индекс у нечетновесового кода H^1_α и будем его обозначать H_{α^k}, отвечающий ему код Хэмминга – через $\overline{H}_{\alpha^k}$. Из определения ясно, что $H^0_\alpha=\overline{H}_\alpha$. В [14] доказано, что коды H_α, $\alpha\in\mathbf{F}$ образуют транзитивное разбиение множества нечетновесовых слов длины n, причем $\overline{H}_\alpha$ и $\overline{H}_\beta$ для любых различных α и β из $\mathbf{F}$ имеют минимально возможное пересечение, равное 2^{2^m-2m} (при n, равном 8, пересечение состоит из 4-х слов, см. ниже Лемму 1 и Следствие 1). Напомним, что в дальнейшем это транзитивное разбиение при $n=8$ называем разбиением Фелпса.

Для этих разбиений будем изучать строение компонент в коде Соловьевой из [12]. Напомним определение этого кода. Пусть $P=\{C_1,C_2,\dots,C_n\}$ – произвольное разбиение векторов F_2^n весов одной четности (нечетновесовых или четновесовых) на расширенные совершенные коды $C_1,C_2,\dots,C_n$, π – произвольная подстановка на множестве элементов $\{1,2,\dots,n\}$. Тогда множество

$$D_P=\cup_{l\in\{1,2,\dots,n\}}C_l\times C_{\pi(l)}$$

является расширенным совершенным кодом.

Далее $m_1(x)$, $m_3(x)$ – минимальные многочлены элементов α и α^3 поля $\mathbf{F}$. Код БЧХ длины $n=2^m-1$, $m\geq 3$ – циклический код с порождающим многочленом $m_1(x)m_3(x)$, см. [13]. Этот код имеет кодовое расстояние 5 при $m\geq 4$ и 7 при $m=3$.

Лемма 1. *(См.* [14]*.) Для любых $\alpha^i,\alpha^j\in\boldsymbol{F}$ код $\overline{H}_{\alpha^i}\cap\overline{H}_{\alpha^j}$ есть объединение расширенного кода БЧХ с порождающим многочленом $m_1(x)m_3(x)$ и его класса смежности.*

Лемма 2. *Для любого $\alpha^k\in\boldsymbol{F}$ код $\overline{H}\cap\overline{H}_{\alpha^k}$ есть расширенный код БЧХ с порождающим многочленом $m_1(x)m_3(x)$, т.е. удовлетворяющий проверочным соотношениям*

$$\sum_{x\in X}1=0,\ \sum_{x\in X}x=0,\ \sum_{x\in X}x^3=0.$$

Доказательство. В силу определения, для кодового слова X, принадлежащего одновременно кодам $\overline{H}$ и $\overline{H}_{\alpha^k}$, имеем следующие проверочные соотношения:

$$\sum_{x\in X}1=0,\ \sum_{x\in X}x=0,\ \sum_{x\in X}(x+\alpha^k)^3=0.$$

Из последнего равенства вытекает

$$\sum_{x\in X}(x^3+x^2\alpha^k+x\alpha^{2k}+\alpha^{3k})=$$

$$\sum_{x\in X} x^3 + \alpha^k(\sum_{x\in X} x)^2 + \alpha^{2k}\sum_{x\in X} x + \alpha^{3k}\sum_{x\in X} 1 = 0,$$

что, с учетом первых двух соотношений, дает

$$\sum_{x\in X} x^3 = 0.$$

Другими словами, слово X принадлежит коду БЧХ с порождающим многочленом $m_1(x)m_3(x)$. Обратное вложение доказывается аналогично. ▲

Лемма 3. *Пусть слово X веса 4 принадлежит коду $\overline{H}_{\alpha^i} \cap \overline{H}_{\alpha^j}$. Тогда координаты X_{α^i} и X_{α^j} не могут одновременно равняться 1.*

Доказательство. Пусть $X = e_{\alpha^i} + e_{\alpha^j} + e_{\alpha^r} + e_{\alpha^s}$. В силу определения кодов $\overline{H}_{\alpha^i}$, $\overline{H}_{\alpha^j}$, имеем следующие соотношения:

$$(\alpha^j + \alpha^i)^3 + (\alpha^r + \alpha^i)^3 + (\alpha^s + \alpha^i)^3 = 0,$$
$$(\alpha^j + \alpha^i)^3 + (\alpha^r + \alpha^j)^3 + (\alpha^s + \alpha^j)^3 = 0,$$

сложив которые, получим

$$(\alpha^r + \alpha^i)^3 + (\alpha^s + \alpha^i)^3 + (\alpha^r + \alpha^j)^3 + (\alpha^s + \alpha^j)^3 = 0.$$

Преобразовывая левую сторону последнего равенства, выводим равенство

$$(\alpha^i + \alpha^j)(\alpha^r + \alpha^s)(\alpha^i + \alpha^j + \alpha^r + \alpha^s) = 0,$$

откуда по Лемме 2 следует, что X принадлежит расширенному коду БЧХ $\overline{H} \cap \overline{H}_{\alpha^i}$ и, следовательно, не может иметь вес 4. ▲

Из лемм 1–3 при $n = 8$ имеем

Следствие 1. *Пусть $n = 8$. Для произвольных различных α^i, α^j из $GF(2^3)$ справедливо $\overline{H}_{\alpha^i} \cap \overline{H}_{\alpha^j} = \{0^8, 1^8, X^0, X^1\}$, где X^0, X^1 – векторы веса 4, единичные координатные позиции которых разбивают множество координат на два множества, причем α^i и α^j принадлежат различным множествам.*

Далее множества единичных координатных позиций векторов X^0 и X^1 из следствия 1 будем обозначать $\Pi^0_{i,j}$ и $\Pi^1_{i,j}$ соответственно.

3. Структура компонент разбиения Фелпса

Для кодового слова X расширенного совершенного кода D через $N_{ij}(D, X)$ обозначим множество кодовых слов, находящихся на расстоянии 4 от X и различающихся с кодовым словом X в i-й и j-й координатах. Назовем эти кодовые слова *ij-смежными* с кодовым словом X. Совокупность кодовых слов расширенного совершенного кода D, которые можно соединить путем с фиксированным кодовым словом X, каждая последовательная пара которых состоит из ij-смежных кодовых слов, называется *ij-компонентой* кода D и обозначается $R_{ij}(D, X)$.

Вначале выясним структуру ij-смежных кодовых слов в коде Соловьевой D_P для произвольной подстановки π и разбиения P множества векторов одной четности на расширенные совершенные коды, где $i, j \le n/2$. Рассмотрим ij-смежные с $(X, Y) \in C_k \times C_{\pi(k)}$ кодовые слова кода D_P. Прежде всего это слова,

получающиеся из ij-смежных слов с X в коде C_k: $\{(Z,Y) : Z \in N_{ij}(C_k, X)\}$. Затем рассмотрим код C_l, где $X + e_i + e_j \in C_l$. Несложно видеть, что Y, как и всякое другое слово на расстоянии 2 от $C_{\pi(l)}$, находится на расстоянии 2 ровно от $n/2$ кодовых слов кода C_l, которые имеют вид $Y + e_{s_t} + e_{s'_t}$, $t = 1, \ldots, n/2$, где $\cup_{t=1,\ldots,n/2}\{s_t, s'_t\}$ образует разбиение координат $\{1, \ldots, n\}$ на пары $\{s_t, s'_t\}$. Отсюда получаем, что $N_{ij}(D_P, (X,Y)) = N_{ij}(C_k, X) \times Y \cup \{(X + e_i + e_j, Y + e_{s_t} + e_{s'_t}) : t \in \{1, \ldots, n/2\}\}$. Таким образом доказали следующее утверждение, ввиду которого приходим к выводу, что исследование ij-компонент кода Соловьевой D_P напрямую связано с изучением структуры графа расстояний Хэмминга два, индуцированного кодовыми словами различных двух кодов разбиения P:

Утверждение 1. *Пусть $P = \{C_1, C_2, \ldots, C_n\}$ есть разбиение множества векторов длины n одной четности на расширенные совершенные коды, (X,Y) – кодовое слово кода Соловьевой $D_P = \cup_{l\in\{1,\ldots,n\}} C_l \times C_{\pi(l)}$, $X \in C_k$. Тогда, если $X + e_i + e_j \in C_l$, то $N_{ij}(D_P, (X,Y)) = N_{ij}(C_k, X) \times Y \cup \{(X + e_i + e_j, Z) : Z \in C_{\pi(l)}, d(Z,Y) = 2\}$.*

Следствие 2. *Пусть $P = \{C_1, C_2, \ldots, C_n\}$ – разбиение множества нечетновесовых векторов длины n на расширенные совершенные коды, (X,Y) есть кодовое слово кода $D_P = \cup_{j\in\{1,\ldots,n\}} C_j \times C_{\pi(j)}$, $X \in C_k$. Тогда $R_{ij}(C_k, X) \times Y \subset R_{ij}(D_P, (X,Y))$.*

Отметим, что дальнейшие утверждения рассматриваются только для разбиений Фелпса, поскольку для остальных разбиений из [15] утверждения не являются справедливыми.

Утверждение 2. *Пусть $n = 8$, i и j – произвольные координаты, $i \neq j$. Представителей классов смежностей $\overline{H}_{\alpha^i}$ по $\overline{H}_{\alpha^i} \cap \overline{H}_{\alpha^j}$ можно выбрать среди векторов веса не более 4 из ij-компоненты кода $\overline{H}_{\alpha^i}$, содержащей нулевой вектор.*

Доказательство. Пусть $e_{\alpha^i} + e_{\alpha^j} + e_{\alpha^{i_1}} + e_{\alpha^{i_2}}$ и $e_{\alpha^i} + e_{\alpha^j} + e_{\alpha^{i_3}} + e_{\alpha^{i_4}}$ попадают в один класс смежности $\overline{H}_{\alpha^i} \cap \overline{H}_{\alpha^j} + X$, где $X \in \overline{H}_{\alpha^i}$. В силу того, что сумма этих двух векторов имеет нули на позициях α^i и α^j и в силу антиподальности расширенного кода БЧХ с порождающим многочленом $m_1(x)m_3(x)$, получаем, что $\overline{H}_{\alpha^i} \cap \overline{H}_{\alpha^j}$ содержит вектор веса 4 с единицами в позициях α^i и α^j, что противоречит Лемме 3. ▲

Лемма 4. 1. *Для всяких векторов $X \in H_{\alpha^i}$, $Y \in H_{\alpha^j}$, класс смежности $X + Y + \overline{H}_{\alpha^i} \cap \overline{H}_{\alpha^j}$ по подкоду $\overline{H}_{\alpha^i} \cap \overline{H}_{\alpha^j}$ содержит единственного лидера, который имеет вес 2.*

2. *Для различных классов смежности $H_{\alpha^i} + H_{\alpha^j}$ по $\overline{H}_{\alpha^i} \cap \overline{H}_{\alpha^j}$ лидеры различны и множество лидеров $X + Y + \overline{H}_{\alpha^i} \cap \overline{H}_{\alpha^j}$ по всем $X \in \overline{H}_{\alpha^i}$, $Y \in \overline{H}_{\alpha^j}$ есть $\{\alpha^r + \alpha^s : \alpha^r \in \Pi^0_{i,j}, \alpha^s \in \Pi^1_{i,j}\}$.*

Доказательство. Пусть носители векторов веса 4 кода $\overline{H}_{\alpha^i} \cap \overline{H}_{\alpha^j}$ есть $\Pi^0_{i,j} = \{\alpha^i, \alpha^{i_1}, \alpha^{j_1}, \alpha^{k_1}\}$ и $\Pi^1_{i,j} = \{\alpha^j, \alpha^{i_2}, \alpha^{j_2}, \alpha^{k_2}\}$.

1. Векторы $X' = X + e_{\alpha^i}$, $Y' = Y + e_{\alpha^j}$ принадлежат кодам $\overline{H}_{\alpha^i}$ и $\overline{H}_{\alpha^j}$ соответственно. Утверждение леммы очевидно выполнено в случае, когда X' или Y' принадлежат $\overline{H}_{\alpha^i} \cap \overline{H}_{\alpha^j}$. По Утверждению 2 без ограничения общности

имеем: $X' = e_{\alpha^i} + e_{\alpha^j} + e_{\alpha^{i_1}} + e_{\alpha^{i_2}}$, тогда $Y' = e_{\alpha^i} + e_{\alpha^j} + e_{\alpha^{j_1}} + e_{\alpha^{j_2}}$ или $Y' = e_{\alpha^i} + e_{\alpha^j} + e_{\alpha^{i_1}} + e_{\alpha^{j_2}}$.

В первом случае в силу Утверждения 1 класс смежности $X' + Y' + \overline{H}_{\alpha^i} \cap \overline{H}_{\alpha^j} = e_{\alpha^i} + e_{\alpha^j} + e_{\alpha^{j_1}} + e_{\alpha^{j_2}} + e_{\alpha^{i_1}} + e_{\alpha^{i_2}} + \overline{H}_{\alpha^i} \cap \overline{H}_{\alpha^j}$ может иметь только один вектор веса 2, а именно $e_{\alpha^{k_1}} + e_{\alpha^{k_2}}$. Во втором случае класс смежности $X'+Y'+\overline{H}_{\alpha^i}\cap\overline{H}_{\alpha^j} = e_{\alpha^i}+e_{\alpha^j}+e_{\alpha^{i_2}}+e_{\alpha^{j_2}}+\overline{H}_{\alpha^i}\cap\overline{H}_{\alpha^j}$ содержит единственный вектор веса 2, а именно $e_{\alpha^i} + e_{\alpha^{k_2}}$.

2. Очевидно, что различные пары классов смежности $X + \overline{H}_{\alpha^i} \cap \overline{H}_{\alpha^j}$ и $Y + \overline{H}_{\alpha^i}\cap\overline{H}_{\alpha^j}$ имеют различных лидеров для класса $X+Y+\overline{H}_{\alpha^i}\cap\overline{H}_{\alpha^j}$. В противном случае получаем противоречие с тем, что факторизуем по подпространству $\overline{H}_{\alpha^i} \cap \overline{H}_{\alpha^j}$. Так как классов смежности $H_{\alpha^i} + H_{\alpha^j}$ по $\overline{H}_{\alpha^i} \cap \overline{H}_{\alpha^j}$ всего 16, а их лидеры необходимо принадлежат множеству $\{e_r + e_s : r \in \Pi^0_{i,j}, s \in \Pi^1_{i,j}\}$, получаем, что лидеры исчерпывают это множество. ▲

Следствие 3. *Пусть $n = 8$ и k, r, s – произвольные элементы множества $\{-\infty, 0, 1, \ldots, 6\}$, $r \neq s$, векторы X, $X' \in H_{\alpha^k}$ находятся на расстоянии 4 и принадлежат некоторой (α^r, α^s)-компоненте кода H_{α^k}. Тогда векторы $X + e_{\alpha^r} + e_{\alpha^s}$, $X' + e_{\alpha^r} + e_{\alpha^s}$ не принадлежат одному и тому же коду H_{α^l} для некоторого l.*

Доказательство. Пусть X и X' таковы, что $X+e_{\alpha^r}+e_{\alpha^s}$, $X'+e_{\alpha^r}+e_{\alpha^s} \in H_{\alpha^l}$ для некоторого l. Возможны два случая: $X + X' = e_{\alpha^r} + e_{\alpha^s} + e_{\alpha^{i_1}} + e_{\alpha^{j_1}}$ и $X + X' = e_{\alpha^{i_1}} + e_{\alpha^{j_1}} + e_{\alpha^{i_2}} + e_{\alpha^{j_2}}$.

Пусть $X + X' = e_{\alpha^r} + e_{\alpha^s} + e_{\alpha^{i_1}} + e_{\alpha^{j_1}}$ и принадлежит $\overline{H}_{\alpha^l} \cap \overline{H}_{\alpha^k}$. С другой стороны, вектор $X+X' = e_{\alpha^r}+e_{\alpha^s}+e_{\alpha^{i_1}}+e_{\alpha^{j_1}}$ не принадлежит $\overline{H}_{\alpha^l}\cap\overline{H}_{\alpha^k}$, так как по Лемме 4 векторы X и $X + e_{\alpha^r} + e_{\alpha^s}$ не могут принадлежать кодам H_{α^k} и H_{α^l} соответственно (поскольку множество $\{\alpha^r, \alpha^s\}$ является подмножеством $\Pi^0_{l,k}$ или $\Pi^1_{l,k}$).

Второй случай доказывается аналогично. ▲

Определим граф $G_{k,l} = (V, E)$ следующим образом: множество вершин графа есть $V = H_{\alpha^k} \cup H_{\alpha^l}$, множество ребер есть $E = \{(X, X') : X \in H_{\alpha^k}, X' \in H_{\alpha^l}, d(X, X') = 2\}$.

Лемма 5. *Пусть $n = 8$ и l, k – произвольные различные элементы множества $\{-\infty, 0, 1, \ldots, 6\}$. Тогда граф $G_{k,l}$ связен.*

Доказательство. Напомним, что в силу Следствия 1 восемь кодовых координат можно разбить на два множества $\Pi^0_{l,k} = \{\alpha^l, \alpha^{i_1}, \alpha^{j_1}, \alpha^{k_1}\}$ и $\Pi^1_{l,k} = \{\alpha^k, \alpha^{i_2}, \alpha^{j_2}, \alpha^{k_2}\}$. Согласно Лемме 4 достаточно доказать, что всякая пара вершин X, $X' = X + e_{\alpha^l} + e_{\alpha^{i_1}} + e_{\alpha^{j_1}} + e_{\alpha^{k_1}}$ из одного класса смежности кода H_{α^k} по подкоду $\overline{H}_{\alpha^k} \cap \overline{H}_{\alpha^l}$ соединена путем в графе $G_{k,l}$. Так как рассматриваемые коды являются расширенными совершенными, то для всякого кодового слова X одного кода и любого t найдется ровно одно кодовое слово в другом коде, отличающееся от X в α^t-й позиции и какой-то еще позиции, которую обозначим α^{t*}. В силу Леммы 4 элементы α^t и α^{t*} не могут одновременно принадлежать $\Pi^0_{l,k}$ или $\Pi^1_{l,k}$. Построим путь от X до X' в графе $G_{k,l}$. Пусть $i' \in \Pi^0_{l,k} \setminus l$:

$X, X+e_{\alpha^l}+e_{\alpha^{l*}}, X+e_{\alpha^l}+e_{\alpha^{l*}}+e_{\alpha^{i'}}+e_{\alpha^{i'*}}, X+e_{\alpha^l}+e_{\alpha^{l*}}+e_{\alpha^{i'}}+e_{\alpha^{i'*}}+e_{\alpha^{l*}}+e_{\alpha^{(l*)*}}$, $X + e_{\alpha^l} + e_{\alpha^{i'}} + e_{\alpha^{i'*}} + e_{\alpha^{(l*)*}} + e_{\alpha^{i'*}} + e_{\alpha^{(i'*)*}} = X + e_{\alpha^l} + e_{\alpha^{i'}} + e_{\alpha^{(l*)*}} + e_{\alpha^{(i'*)*}}$.

По Лемме 4 элементы $\alpha^{(l*)*}, \alpha^{(i'*)*} \in \Pi^0_{l,k}$ и отличаются от α^l и $\alpha^{i'}$ в силу того, что рассматриваемые коды имеют кодовое расстояние 4. Отсюда немедленно имеем $X + e_{\alpha^l} + e_{\alpha^{i'}} + e_{\alpha^{(l*)*}} + e_{\alpha^{(i'*)*}} = X'$. ▲

Пару координат кода $\cup_{l\in\{-\infty,0,1,\ldots,6\}} H_{\alpha^l} \times H_{\alpha^{\pi(l)}}$ назовем *однородной*, если она принадлежит первой или второй половине кодовых координат одновременно.

Теорема 1. *Пусть* $P = \{H_{-\infty}, H_0, H_1, H_\alpha, \ldots, H_{\alpha^6}\}$ *есть разбиение Фелпса. Тогда код* $D_P = \cup_{l\in\{-\infty,0,1,\ldots,6\}} H_{\alpha^l} \times H_{\alpha^{\pi(l)}}$ *имеет две максимальные компоненты по любой паре однородных координат для произвольной перестановки* π *на множестве* $\{-\infty, 0, 1, \ldots, 6\}$.

Доказательство. Подкод $H_{\alpha^k} \times H_{\alpha^{\pi(k)}}$ для произвольного $k \in \{-\infty, 0, 1, \ldots, 6\}$ будем называть базовым подкодом кода D_P.

Рассмотрим $(X, Y) \in H_{\alpha^k} \times H_{\alpha^{\pi(k)}}$ и компоненту $R_{\alpha^r,\alpha^s}(D_P, (X, Y))$, $r, s \in \in \{-\infty, 0, 1, \ldots, 6\}$. В силу Следствия 2, три кодовых слова на расстоянии 4 от (X, Y) из компоненты $R_{\alpha^r,\alpha^s}(D_P, (X, Y))$ принадлежат базовому подкоду $H_{\alpha^k} \times H_{\alpha^{\pi(k)}}$: $(X + e_{\alpha^r} + e_{\alpha^s} + e_{\alpha^{i_1}} + e_{\alpha^{j_1}}, Y), (X + e_{\alpha^r} + e_{\alpha^s} + e_{\alpha^{i_2}} + e_{\alpha^{j_2}}, Y), (X + e_{\alpha^r} + e_{\alpha^s} + e_{\alpha^{i_3}} + e_{\alpha^{j_3}}, Y)$. В свою очередь, эти кодовые слова находятся на расстоянии 4 от следующих кодовых слов компоненты $R_{\alpha^r,\alpha^s}(D_P, (X, Y))$:

$$(X + e_{\alpha^{i_1}} + e_{\alpha^{j_1}}, Y + e_{\alpha^{i'_1}} + e_{\alpha^{j'_1}})$$
$$(X + e_{\alpha^{i_2}} + e_{\alpha^{j_2}}, Y + e_{\alpha^{i'_2}} + e_{\alpha^{j'_2}})$$
$$(X + e_{\alpha^{i_3}} + e_{\alpha^{j_3}}, Y + e_{\alpha^{i'_3}} + e_{\alpha^{j'_3}}),$$

для некоторых $i'_1, j'_1, i'_2, j'_2, i'_3, j'_3$. К рассматриваемым кодовым словам добавим также для некоторых r' и s' кодовое слово

$$(X + e_{\alpha^r} + e_{\alpha^s}, Y + e_{\alpha^{r'}} + e_{\alpha^{s'}})$$

кода D_P.

В силу Следствия 3 все эти четыре кодовых слова принадлежат четырем различным базовым подкодам, отличным от $H_{\alpha^k} \times H_{\alpha^{\pi(k)}}$, откуда получаем, что компонента $R_{\alpha^r,\alpha^s}(D_P, (X, Y))$ пересекается с каждым базовым подкодом.

Теперь рассмотрим произвольное кодовое слово

$$(X, Y) \in H_{\alpha^k} \times H_{\alpha^{\pi(k)}} \cap R_{\alpha^r,\alpha^s}(D_P, (X, Y))$$

и покажем, что $X \times H_{\alpha^{\pi(k)}} \subset R_{\alpha^r,\alpha^s}(D_P, (X, Y))$. Откуда, в силу того, что компонента всякого кода длины $n = 8$ является максимальной и пересекается с каждым базовым подкодом, получим требуемое.

Пусть $(X, Y) \in H_{\alpha^k} \times H_{\alpha^{\pi(k)}}$, $(X + e_{\alpha^r} + e_{\alpha^s}, Y + e_{\alpha^{r'}} + e_{\alpha^{s'}}) \in H_{\alpha^l} \times H_{\alpha^{\pi(l)}}$. Ввиду Леммы 5 для всякого $Y' \in H_{\alpha^{\pi(k)}}$ существует последовательность $Y, Y^1, Y^2, \ldots, Y^p = Y'$ кодовых слов $H_{\alpha^{\pi(k)}}$ и $H_{\alpha^{\pi(l)}}$, соседние кодовые слова которой различаются в двух координатных позициях:

$$Y,\ Y^1 = Y + e_{\alpha^{a_1}} + e_{\alpha^{b_1}} \in H_{\alpha^{\pi(l)}},$$
$$Y^2 = Y^1 + e_{\alpha^{a_2}} + e_{\alpha^{b_2}} \in H_{\alpha^{\pi(k)}}$$
$$\ldots$$

$$Y' = Y^{p-1} + e_{\alpha^{a_p}} + e_{\alpha^{b_p}} \in H_{\alpha^{\pi(k)}}.$$

Всякой такой последовательности отвечает путь в компоненте $R_{\alpha^r,\alpha^s}(D_P,(X,Y))$ из (X,Y) в (X,Y') в базовых подкодах $H_{\alpha^l} \times H_{\alpha^{\pi(l)}}$ и $H_{\alpha^k} \times H_{\alpha^{\pi(k)}}$:

$$\begin{gathered}(X,Y) \in H_{\alpha^k} \times H_{\alpha^{\pi(k)}},\\ (X + e_{\alpha^r} + e_{\alpha^s}, Y^1) = (X + e_{\alpha^r} + e_{\alpha^s}, Y + e_{\alpha^{a_1}} + e_{\alpha^{b_1}}) \in H_{\alpha^l} \times H_{\alpha^{\pi(l)}}\\ (X,Y^2) = (X, Y^1 + e_{\alpha^{a_2}} + e_{\alpha^{b_2}}) \in H_{\alpha^k} \times H_{\alpha^{\pi(k)}}\\ \dots\\ (X,Y') = (X + e_{\alpha^r} + e_{\alpha^s}, Y^{p-1} + e_{\alpha^{a_p}} + e_{\alpha^{b_p}}) \in H_{\alpha^k} \times H_{\alpha^{\pi(k)}},\end{gathered}$$

что доказывает $X \times H_{\alpha^{\pi(k)}} \subset R_{\alpha^r,\alpha^s}(D_P,(X,Y))$.Максимальность любой компоненты вытекает из того факта, что каждая компонента пересекается с любым базовым подкодом. ▲

Заметим, что аналогичный подход (анализ графа $G_{k,l}$ расстояний Хэмминга два, индуцированного двумя кодами C_k и C_l из разбиения), может быть применен для исследования структуры компонент кодов Соловьевой, полученных из других разбиений. Рассуждениями, сходными с изложенными в Теореме 1, используя аналоги Следствия 3 и Леммы 5, например, можно показать, что коды Соловьевой длины 15, полученные из разбиения под номером 1 работы [15], имеют компоненты мощности хотя бы 512, а для отдельных подстановок и максимальные компоненты по любым однородным координатам.

4. Свойства максимальных компонент

В данном разделе отметим некоторые комбинаторные аспекты компонент, дающих дополнительную мотивацию для исследования этих нетривиальных структур. Рассмотрим случай i-компонент и совершенных кодов (длина $n = 2^m - 1, m > 2$).

В этом случае i-компонента определяется как совокупность кодовых слов совершенного кода D, которые можно соединить путем с кодовым словом X, каждая последовательная пара которых состоит из i-смежных кодовых слов.

Разбиение вершин графа на m множеств-цветов, занумерованных числами $\{1,\dots,m\}$, назовем *совершенной m-раскраской*, если для произвольных i,j всякая вершина цвета i смежна с A_{ij} вершинами цвета j. Квадратная матрица $A = (A_{ij})$ порядка m называется *матрицей параметров* совершенной раскраски. В случае, когда матрицу параметров переименованием цветов раскраски можно привести к трехдиагональному виду, цвет под номером 1 называется *полностью регулярным кодом*. В дальнейшем будем рассматривать лишь совершенные раскраски двоичных графов Хэмминга. Полностью регулярные коды были введены Ф. Дельсартом [16] как обобщения совершенных кодов, сохраняющие их самые замечательные алгебро-комбинаторные свойства. *Радиусом покрытия* $\rho(C)$ кода C назовем максимально возможное расстояние от произвольного вектора из F_2^n до кодовых вершин кода C.

Кодовое слово совершенного кода называется *i-четным* (*i-нечетным*), если оно имеет нечетный (четный) вес и i-я координата равна 1 (0 соответственно) или, имея четный (нечетный) вес, i-я координата равна 0 (1 соответственно). Прежде всего покажем связь i-четных вершин и максимальных компонент с совершенными раскрасками и совершенными кодами.

Утверждение 3. *Пусть I и I' – множества i-четных и i-нечетных кодовых слов совершенного кода C соответственно. Тогда $\rho(I) = \rho(I')=3$ и множество векторов на расстоянии 3 от множества I есть $I' \cup (I' + e_i)$.*

Доказательство. Очевидно, что для всякого i-четного кодового слова x найдется $(n-3)(n-1)/6$ кодовых слов на расстоянии 3, являющихся i-нечетными. Следовательно $d(I, I') = 3$.

Рассмотрим произвольный y, такой что $d(y, I) \geq 2$, $y \notin C$. Тогда y покрывается кодовым словом $u \in I' = C \setminus I : y = u + e_j$. Имеем два случая: $j = i$, тогда $y \in I' + e_i$, но, поскольку код $I \cup (I' + e_i)$ – совершенный с множеством i-четных и i-нечетных вершин I и $I' + e_i$, заключаем, что $d(y, I) = 3$. Если $j \neq i$, тогда найдется кодовое слово z, отличающееся от x в позициях j, a, b, причем a и b не равны i, откуда получаем $z \in I$, $d(y, z) = 2$. ▲

Несложно видеть, что радиус покрытия минимальной компоненты

$$R = \{(x, |x|, x) : x \in F_2^{(n-1)/2}\}$$

равен $(n-1)/2$ (в коде Хэмминга длины n для любого допустимого $n \geq 7$ существует минимальная компонента, состоящая только из кодовых слов весов $(n-1)/2$ и $(n+1)/2$). Естественно предположить, что компоненты, отличные от минимальной и максимальной, имеют радиусы покрытия в пределах от 4 до $(n-3)/2$.

Нерешенная проблема. Пусть R есть i-компонента с $\rho = 3$. Является ли она необходимо максимальной?

Пусть I, I' – множества i-четных и i-нечетных кодовых слов некоторого двоичного совершенного кода C. Рассмотрим раскраску графа Хэмминга в следующие 6 цветов: I, $I + e_i$, I_1, I_1', $I' + e_i$, I', где I_1 и I_1' – вершины на расстоянии 1 от $I \cup (I + e_i)$ и $I' \cup (I' + e_i)$ соответственно.

Следствие 4. *Раскраска графа Хэмминга в цвета $I, I', I_1, I_1', I + e_i, I' + e_i$ является совершенной с матрицей параметров*

(1)

	I	$I + e_i$	I_1	I_1'	$I' + e_i$	I'
I	*0*	*1*	*n-1*	*0*	*0*	*0*
$I + e_i$	*1*	*0*	*n-1*	*0*	*0*	*0*
I_1	*1*	*1*	*1*	*n-3*	*0*	*0*
I_1'	*0*	*0*	*n-3*	*1*	*1*	*1*
$I' + e_i$	*0*	*0*	*0*	*n-1*	*0*	*1*
I'	*0*	*0*	*0*	*n-1*	*1*	*0*

.

Раскраска графа Хэмминга в цвета $I \cup (I + e_i), I_1, I_1', I' \cup (I' + e_i)$ является совершенной с матрицей параметров

	$I \cup (I + e_i)$	I_1	I_1'	$(I' + e_i) \cup I'$
$I \cup (I + e_i)$	*1*	*n-1*	*0*	*0*
I_1	*2*	*1*	*n-3*	*0*
I_1'	*0*	*n-3*	*1*	*2*
$(I' + e_i) \cup I'$	*0*	*0*	*n-1*	*1*

.

Нерешенная проблема. Пусть существует совершенная раскраска графа Хэмминга с матрицей параметров (1). Существует ли такое i, что цвет I есть множество i-четных вершин некоторого совершенного кода?

Следствие 5. *Всякая максимальная компонента либо не достраивается максимальной компонентой до совершенного кода, либо достраивается ровно двумя способами.*

Доказательство. Если I и I' – множества i-четных и i-нечетных кодовых слов кода C, причем I' является гигантской компонентной, то множество I может быть достроено лишь одной гигантской компонентой до другого совершенного кода, это компонента $I'+e_i$. Пусть I'' – гигантская компонента, дополняющая I до совершенного кода, отличная от I' и $I'+e_i$. Тогда, в силу Утверждения 3, $I'' \subset I \cup I'$, а существование пары кодовых слов $x \in I'' \cap I'$ и $y \in I'' \cap (I'+e_i)$, различающихся в трех координатных позициях, включающих i, невозможно. ▲

Следствие 6. *Пусть M – число попарно неизоморфных совершенных кодов длины n, состоящих из двух максимальных компонент по некоторому направлению i. Тогда найдется хотя бы $M/2$ попарно неизоморфных максимальных компонент, вложимых в совершенные коды.*

В случае $n = 15$ лишь 30 классов изоморфизма из 5983 неизоморфных классов совершенных кодов не могут быть представлены как объединение двух максимальных компонент [9, 8]. Этот эмпирический факт подтверждает актуальность исследования таких объектов как максимальные компоненты совершенных кодов. Как следствие имеем хотя бы 2977 попарно неизоморфных максимальных компонент, вложимых в совершенные коды длины n=15.

В заключение авторы выражают благодарность Олли Поттонену за предоставление информации о структуре i-компонент совершенных кодов длины 15. Авторы благодарят рецензента за ряд полезных замечаний, позволивших улучшить презентацию результатов в данной статье.

References

[1] F. I. Solov'eva, *Switching Methods for Error-Correcting Codes*, Aspects of Network and Information Security, IOS Press, NATO Science for Peace and Security, Series D: Information and Communication Security, **17** (2008), 333–342.

[2] F. I. Solov'eva, *A survey on perfect codes*, Matematicheskie voprosi kibrenetiki, **18** (2013), 5–34 (in Russian).

[3] F. I. Solov'eva, *Exact Bounds on the Connectivity of Code-Generated Disjunctive Normal Forms*, Inst. Math. of the Siberian Branch of Acad. of Sciences, USSR, Preprint **10** (1990).

[4] F. I. Solov'eva, *Factorization of code generating d.n.f.*, Methody Diskr. Analiza, **47** (1988), 66–88 (in Russian). Zbl 0719.94027

[5] S. V. Avgustinovich, F. I. Solov'eva, *On projections of perfect binary codes*, Proc. Seventh Joint Swedish-Russian Int. Workshop on Inform. Theory. St.-Petersburg, Russia, (1995), 25–26.

[6] F. I. Solov'eva, *Structure of i-components of perfect binary codes*, Discrete Appl. Math., **111**: 1–2 (2001), 189–197. Zbl 1025.94024

[7] P. R. J. Östergård, O. Pottonen, *The perfect binary one-error-correcting codes of length 15: Part I – Classification*, IEEE Trans. Inform. Theory, **55** (2009), 4657–4660.

[8] P. R. J. Östergård, K. T. Phelps, O. Pottonen, *The perfect binary one-error-correcting codes of length 15: Part II-properties*, IEEE Trans. Inform. Theory, **56**: 6 (2010), 2571–2582.

[9] O. Pottonen, *Private communication.*
[10] V. N. Potapov, *Cardinality spectra of components of correlation immune functions, bent functions, perfect colorings, and codes*, Probl. of Inform. Transm., **48**: 1 (2012), 47–55. Zbl 1276.06008
[11] K. T. Phelps, M. LeVan, *Switching equivalence classes of perfect codes*, Des., Codes and Cryptogr., **56**: 2 (1999), 179–184. Zbl 0938.94015
[12] F. I. Solov'eva, *On binary nongroup codes*, Methody Diskr. Analiza, **37** (1981), 65–76 (in Russian). Zbl 0524.94014
[13] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, 1977. Zbl 0369.94008
[14] D. S. Krotov, *A Partition of the hypercube into Maximally Nonparallel Hamming Codes*, Journal of Combinatorial Designs, **22** (2014), 179–187. Zbl 1286.05114
[15] K. T. Phelps, *An enumeration of* 1*-perfect binary codes of length 15*, Australian Journal of Combinatorics, **21** (2000), 287–298. Zbl 0972.94049
[16] P. Delsarte, *An algebraic approach to association schemes of coding theory*, Philips J. Res., **10** (1973), 1–97. Zbl 1075.05606

Ivan Yurevich Mogilnykh
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090, Novosibirsk, Russia
E-mail address: ivmog84@math.nsc.ru

Faina Ivanovna Solov'eva
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090, Novosibirsk, Russia
E-mail address: sol@math.nsc.ru