

УДК 519.8

АФФИННО 3-НЕСИСТЕМАТИЧЕСКИЕ СОВЕРШЕННЫЕ КОДЫ ДЛИНЫ 15 *)

С. А. Малюгин¹

¹Институт математики им. С. Л. Соболева СО РАН,
пр. Акад. Коптюга, 4, 630090 Новосибирск, Россия
e-mail: mal@math.nsc.ru

Аннотация. Совершенный двоичный код C длины $n = 2^k - 1$ называется *аффинно 3-систематическим*, если в пространстве $\{0, 1\}^n$ существует трёхмерное подпространство L такое, что любой его смежный класс $L + u$ либо не пересекается с кодом C , либо пересекается с ним ровно по одному элементу. В противном случае код C называется *аффинно 3-несистематическим*. В настоящей работе найдено четыре неэквивалентных аффинно 3-несистематических кода длины 15 и изучены свойства дополнения $\{0, 1\}^n \setminus (C + C)$. Библиогр. 12.

Ключевые слова: совершенный код, код Хемминга, несистематический код, аффинно несистематический код, аффинно 3-несистематический код, компонента.

Введение

Пусть $\{0, 1\}^n$ — векторное пространство над полем из двух элементов 0 и 1. По определению это пространство состоит из всех последовательностей вида $u = (u_1, \dots, u_n)$, где $u_i \in \{0, 1\}$. Сумма векторов $u, v \in \{0, 1\}^n$ определяется формулой $u + v = (u_1 \oplus v_1, \dots, u_n \oplus v_n)$, где $u = (u_1, \dots, u_n)$, $v = (v_1, \dots, v_n)$ и $u_i \oplus v_i$ — сумма элементов $u_i, v_i \in \{0, 1\}$ в поле Галуа $GF(2)$. Далее всегда будем рассматривать в пространстве $\{0, 1\}^n$ стандартный базис e_1, \dots, e_n , где $e_i = (0, \dots, \underset{i}{1}, \dots, n)$. Нулевой и единичный векторы обозначаем через **0** и **1**. Число ненулевых координат вектора u называется его *весом*. *Носитель* вектора $u \in \{0, 1\}^n$ (множество индексов i , для которых $u_i = 1$) обозначается через $[u]$.

В коде Хемминга H^n рассмотрим подпространство R_i , порожденное всеми векторами веса 3 с i -й координатой, равной единице. Все-

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 13-01-00463, 14-01-00507).

возможные смежные классы вида $R_i^u = R_i + u$ ($u \in H^n$) называются i -компонентами кода H^n , $i = 1, \dots, n$. Рассмотрим некоторое семейство $\mathcal{B} = \{R_{i_1}^{u_1}, \dots, R_{i_m}^{u_m}\}$, состоящее из попарно не пересекающихся i_p -компонент, где $u_p \in H^n$, $p = 1, \dots, m$. Одна из основных конструкций нелинейных совершенных двоичных кодов состоит в том, что в коде H^n сдвигаются по координатам i_p все компоненты из семейства \mathcal{B} , т. е. множество

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

является совершенным кодом [1, 9, 10, 12]. Далее будем говорить, что код $H^n(\mathcal{B})$ построен из кода Хемминга H^n сдвигами (или свитчингами) компонент из семейства \mathcal{B} . Коды вида $H^n(\mathcal{B})$ будем также называть 1-свитчинговыми кодами (свитчинговые коды, которые получаются из кода H^n многократным применением свитчингов линейных, а также нелинейных компонент, в данной работе не рассматриваются). Будем далее применять эту конструкцию для построения 3-несистематических кодов.

Совершенный двоичный код $C \subset \{0, 1\}^n$ длины $n = 2^k - 1$ называется *систематическим*, если существует k -элементное подмножество $K \subset \{1, \dots, n\}$ такое, что любые два неравных вектора $u, v \in C$ различаются хотя бы в одной координате с номером, не принадлежащим K . В противном случае код C называется *несистематическим*. Несистематические совершенные двоичные коды длины $n \geq 255$ впервые построены в [1] сдвигами i -компонент кода H^n для i , пробегающим все значения из $\{1, \dots, n\}$. В [11] предложена модификация конструкции [1], позволяющая строить такие коды для всех $n \geq 63$. Для $n = 15$ и $n = 31$ несистематические коды найдены с помощью компьютера [9, 11].

В этой работе рассмотрим более сильное понятие несистематичности.

Определение 1. Совершенный двоичный код C длины $n = 2^k - 1$ называется *аффинно t -систематическим*, если в пространстве $\{0, 1\}^n$ существует t -мерное подпространство L такое, что любой его смежный класс $L + u$ либо не пересекается с кодом C , либо пересекается с ним ровно по одному элементу. В противном случае код C называем *аффинно t -несистематическим*.

Легко заметить, что совершенный двоичный код C является t -систематическим тогда и только тогда, когда существует t -мерное подпространство $L \subset \{0, 1\}^n$ такое, что $L \cap (C + C) = \{0\}$.

Если $t = k = \log(n + 1)$, то аффинно t -систематический (аффинно

t -несистематический) код называем просто *аффинно систематическим* (*аффинно несистематическим*). Определение аффинной систематичности предложено С. В. Августиновичем. Это свойство является аффинным инвариантом кода, т. е. оно сохраняется при любых невырожденных аффинных преобразованиях пространства $\{0, 1\}^n$. Также С. В. Августинович поставил вопрос о существовании аффинно несистематических кодов, ответ на него анонсирован в [4]. В [6] аффинно несистематические коды построены для всех $n = 2^k - 1$, $k \geq 4$. При $t > k$ (соответственно при $t < 3$) любой совершенный код длины $n = 2^k - 1$ является аффинно t -несистематическим (соответственно аффинно t -систематическим). Поэтому естественно рассматривать только нетривиальные случаи, когда $3 \leq t \leq k$. Случай $t = k$ (аффинной несистематичности) рассмотрен в [6]. Другой крайний случай $t = 3$ рассмотрен в [7] для кодов длины $n > 15$. Случай $n = 15$ требует отдельного исследования. В настоящей работе доказано, что среди 12 неэквивалентных 1-свитчинговых несистематических совершенных двоичных кодов длины 15 ровно четыре кода аффинно 3-несистематические. Для этого подробно изучается структура дополнения к множеству $C + C$ для несистематического кода $C \subset \{0, 1\}^{15}$. В качестве одного из простых применений этих исследований доказывалось, что несистематический двоичный код длины $n = 2^k - 1$, $k \geq 5$, может иметь полную систему множеств мощности m для всех $m = 4l, 4l - 1$, $1 \leq l < (n - 3)/4$. Показана неулучшаемость этого результата в классе 1-свитчинговых кодов. Кроме того, для таких кодов C доказано, что $C + C + C = \{0, 1\}^n$. Данная работа является завершением предыдущей публикации [7].

1. Строение дополнения к множеству $C + C$ для несистематического совершенного двоичного кода C длины 15

На множестве индексов $\{0, 1, \dots, n\}$, $n = 2^k - 1$, можно ввести структуру линейного пространства следующим образом. Пусть $i = i_1 \dots i_k$ — представление числа $0 \leq i \leq n$ в двоичной системе. *Бинарной суммой* $i \oplus j$ чисел $0 \leq i, j \leq n$ называется число, двоичное представление которого есть побитовая сумма двоичных представлений чисел i и j . Таким образом на множестве индексов $\{0, 1, \dots, n\}$, $n = 2^k - 1$, вводится структура линейного пространства. При этом код Хемминга H^n определяется как множество всех векторов $u = (u_1, \dots, u_n) \in \{0, 1\}^n$, для которых $\bigoplus_{i=1}^n u_i i = 0$. Подмножество $\{1, \dots, n\}$ можно также рассматривать как конечную $(k - 1)$ -мерную проективную геометрию $PG_{k-1}(2)$.

Именно этой геометрической интерпретацией будем пользоваться далее, рассматривая плоскости и прямые на множестве индексов $\{1, \dots, n\}$.

k -Мерное подпространство $Q \subset \{0, 1\}^n$ называем *дополнительным к коду Хемминга H^n* , если $Q \cap H^n = \{\mathbf{0}\}$. Так как $Q + H^n = \{0, 1\}^n$, дополнительное подпространство Q пересекается с каждым смежным классом $H^n + e_i$ по единственному ненулевому элементу q_i , $i = 1, \dots, n$.

Пусть $Q = \{q_0, q_1, \dots, q_n\}$ — дополнительное подпространство к коду Хемминга H^n , где $q_0 = \mathbf{0}$, $q_i \in H^n + e_i$, $1 \leq i \leq n$. Тогда $q_{i \oplus j} = q_i + q_j$ для всех $1 \leq i, j \leq n$ [6, лемма 1].

Множество всех векторов пространства $\{0, 1\}^n$ разбивается на орбиты относительно группы перестановочных автоморфизмов $\text{Sym}(H^n)$ кода Хемминга H^n . В [2] получена полная классификация этих орбит в случае $n = 15$. Далее будем пользоваться обозначениями орбит из [2].

Рассмотрим произвольное семейство $\mathcal{B} = \{R_{i_1}^{u_1}, \dots, R_{i_m}^{u_m}\}$ из попарно не пересекающихся компонент кода Хемминга H^n . Обозначим через $I(\mathcal{B})$ множество всех индексов i , для которых существуют i -компоненты, принадлежащие семейству \mathcal{B} .

Теорема 1. Пусть $\mathcal{B} = \{R_{i_1}^{u_1}, \dots, R_{i_m}^{u_m}\}$ — семейство не пересекающихся компонент кода Хемминга H^n и код $C = H^n(\mathcal{B})$ получен из кода H^n сдвигами всех его компонент из семейства \mathcal{B} . Тогда для любой компоненты R_j , $1 \leq j \leq n$, её сдвиг $R_j + e_j$ не пересекается с множеством $C + C$.

Доказательство. Пусть $j \in I(\mathcal{B})$, т. е. $j = i_p$ при некотором $1 \leq p \leq m$. Рассмотрим элемент $v \in R_j + e_j$, который представляется в виде суммы $v = u + w$, где $u \in R_{i_p}^{u_p} + e_{i_p}$,

$$w \in H^n \setminus \left(\bigcup_{q=1}^m R_{i_q}^{u_q} \right) = E(\mathcal{B}) \subset C. \quad (1)$$

Значит, $w = v + u \in R_{i_p} + R_{i_p}^{u_p} = R_{i_p}^{u_p}$, что противоречит включению (1). Рассмотрим теперь любой индекс $1 \leq j \leq n$ и элемент $v \in R_j + e_j$, который представляется в виде суммы $v = u + w$, где $u \in R_{i_p}^{u_p} + e_{i_p}$, $w \in R_{i_q}^{u_q} + e_{i_q}$ и $j = i_p \oplus i_q$. Так как компоненты $R_{i_p}^{u_p}$ и $R_{i_q}^{u_q}$ не пересекаются, их сумма $R_{i_p}^{u_p} + R_{i_q}^{u_q}$ не пересекается с (i_p, i_q, j) -компонентой $R_{i_p} + R_{i_q}$. Из включения $v + e_j \in R_j \subset R_{i_p} + R_{i_q}$ следует, что $v + e_j \notin R_{i_p}^{u_p} + R_{i_q}^{u_q}$, т. е.

$$v \notin (R_{i_p}^{u_p} + e_{i_p}) + (R_{i_q}^{u_q} + e_{i_q}) + e_{i_p} + e_{i_q} + e_j = (R_{i_p}^{u_p} + e_{i_p}) + (R_{i_q}^{u_q} + e_{i_q}),$$

последнее равенство вытекает из того, что вектор $e_{i_p} + e_{i_q} + e_j$ (веса 3) принадлежит компоненте R_{i_p} ; противоречие. Теорема 1 доказана.

Из теоремы 1 следует, что для любой i -компоненты R_i сдвиг $R_i + e_i$ целиком находится в дополнении $\{0, 1\}^n \setminus (C + C)$. Такое свойство характерно для любого 1-свитчингового кода C , получаемого из кода Хемминга сдвигами его непересекающихся компонент.

Далее будем пользоваться терминологией из [2, 5]. Из теоремы 1 следует, что для свитчинговых кодов C длины 15, перечисленных в [2], в дополнении $\{0, 1\}^{15} \setminus (C + C)$ целиком содержатся орбиты O_5^3, O_6^2, O_6^3 и антиподальные им орбиты O_{10}^3, O_9^2, O_9^3 (по терминологии из [2] орбиты O_m^l и O_{15-m}^l *антиподальны*, т. е. $O_{15-m}^l = \{u \in \{0, 1\}^{15} \mid \mathbf{1} + u \in O_m^l\}$). В этом дополнении содержатся также орбиты O_1^1, O_2^1 векторов веса 1 и 2, а также антиподальные им орбиты O_{13}^1, O_{14}^1 . Дальнейшее исследование дополнения к множеству $C + C$ будем проводить только для несистематических кодов C . По классификации из [5] существует ровно 12 неэквивалентных несистематических 1-свитчинговых кодов длины 15. В [5] классы эквивалентности этих кодов обозначаются символами $Y7, Y71, Y72, Y73^0, Y73^1, Y74^1, Y8^0, Y8^1, Y81, Y82, Y83, Y84^1$. В [5] даётся также инструкция по построению представителей этих классов эквивалентности. Начнём с самых простых классов $Y8^0$ и $Y8^1$. В таблице из [5] представитель класса $Y8^0$ кодируется символом $0_8 1_9 2_{10} 3_{11} 4_{12} 5_{13} 6_{14} 7_{15}$. Это означает, что для построения такого кода необходимо в коде Хемминга H^{15} сдвинуть по соответствующим координатам восемь компонент $R_{p+8}^{v_p}$, $p = 0, \dots, 7$, где

$$\begin{aligned} [v_0] &= \emptyset, & [v_1] &= \{1, 2, 5, 6\}, & [v_2] &= \{2, 3, 4, 5\}, & [v_3] &= \{1, 3, 5, 7\}, \\ [v_4] &= \{1, 3, 4, 6\}, & [v_5] &= \{4, 5, 6, 7\}, & [v_6] &= \{2, 3, 6, 7\}, & [v_7] &= \{1, 2, 4, 7\}, \\ [v_0] &= \{1, \dots, 7\}, & [v_1] &= \{3, 4, 7\}, & [v_2] &= \{1, 6, 7\}, & [v_3] &= \{2, 4, 6\}, \\ [v_4] &= \{2, 5, 7\}, & [v_5] &= \{1, 2, 3\}, & [v_6] &= \{1, 4, 5\}, & [v_7] &= \{3, 5, 6\}. \end{aligned}$$

Здесь для удобства принято обозначение $\bar{k} = 15 - k$, $k = 0, \dots, 7$. Представитель класса $Y8^1$ кодируется символом $0_8 1_9 2_{10} 3_{11} 4_{12} 5_{13} 6_{14} \bar{7}_{15}$. Это означает, что для построения такого кода необходимо сдвинуть в коде H^{15} те же семь компонент $R_{p+8}^{v_p}$, $p = 0, \dots, 6$, и восьмую компоненту $R_{15}^{v_7}$, антиподальную к компоненте $R_{15}^{v_7}$. Обозначим построенные таким способом представители символами C_{8^0} и C_{8^1} .

Если вектор u не принадлежит коду Хемминга H^{15} , то бинарная сумма $s(u) = \bigoplus_{i=1}^{15} u_i i$ не равна нулю. Будем называть индекс с номером $s(u)$ *синдромом* вектора u . Для множества векторов U введём обозначение $U(i) = \{u \in U \mid s(u) = i\}$, т. е. это множество всех векторов из U

с фиксированным синдромом i . Векторы с нулевым синдромом принадлежат коду Хемминга H^{15} , далее будем называть их *кодowymi векторами*. Следуя [1], будем говорить, что код C имеет *полную систему троек* (четвёрок и т. д.), если все векторы веса 3 (веса 4 и т. д.) принадлежат множеству $C + C$. Обозначим через h вектор с координатами $(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$.

Лемма 1. Если $C = C_{80}$ или C_{81} , то дополнение $D_{80} = \{0, 1\}^{15} \setminus (C + C)$ имеет следующий вид:

$$D_{80} = D_{\min} \cup \{h, \mathbf{1} + h\} \cup \bigcup_{i=1}^7 [O_7^3(i) \cup O_7^4(i) \cup O_8^3(i) \cup O_8^4(i)],$$

где $D_{\min} = \bigcup_{i=1}^{15} (R_i + e_i) = O_1^1 \cup O_2^1 \cup O_5^3 \cup O_6^2 \cup O_6^3 \cup O_9^2 \cup O_9^3 \cup O_{10}^3 \cup O_{13}^1 \cup O_{14}^1$.

Число элементов в этом множестве равно 2818.

ДОКАЗАТЕЛЬСТВО. Если $i \geq 8$ и $u \in O(i)$, где $O(i)$ — одна из орбит $O_3^2(i)$, $O_4^2(i)$, $O_4^3(i)$, $O_5^2(i)$, $O_5^4(i)$, $O_6^4(i)$, $O_6^5(i)$, $O_7^3(i)$, $O_7^4(i)$, $O_7^5(i)$, $O_7^6(i)$ или одна из антиподальных к ним орбит, то $u + e_i \notin R_i$ и компонента $R_i^{v_{15-i}} + u + e_i$ не принадлежит семейству из восьми компонент $R_{p+8}^{v_p}$, $p = 0, \dots, 7$, которые необходимо сдвинуть для построения кода C_{80} . Тогда дополнение $(R_i^{v_{15-i}} + u + e_i) \setminus \left(\bigcup_{p=0}^7 R_{p+8}^{v_p} \right)$ непусто. Этот факт подробно доказан в [3, теорема 4]. Если взять любой вектор v из этого дополнения, то $v \in C_{80}$ и $w = u + v \in (R_i^{v_{15-i}} + e_i) \subset C_{80}$. Поэтому $u = v + w \in (C_{80} + C_{80})$.

В [3] доказано, что все коды классов $Y8^0$, $Y8^1$, $Y81$, $Y82$, $Y83$, $Y84$ имеют полную систему троек. Поэтому необходимо рассмотреть только части орбит $O(i)$ с синдромом $i \leq 7$ и веса ≥ 4 . Начнём с орбиты $O_4^2(i)$, $i \leq 7$, носители векторов u которой состоят из линейно независимы четвёрок $\{i_1, i_2, i_3, i_4\}$ таких, что $i = i_1 \oplus i_2 \oplus i_3 \oplus i_4$. Вектор v с носителем $\{i_1, i_2, i_3, i_4, i\}$ принадлежит коду H^{15} . Так как четвёрка $\{i_1, i_2, i_3, i_4\}$ линейно независима, по крайней мере для двух индексов, скажем для i_3 и i_4 , выполняются неравенства $i_3 \geq 8$, $i_4 \geq 8$. Предположим, что $i_1, i_2 \leq 7$. Пусть $\pi(i_1) = 1$, $\pi(i_2) = 2$, $\pi(i_3) = 8$, $\pi(i_4) = 12$. Отображение π можно однозначно продолжить по линейности до перестановочного автоморфизма кода Хемминга H^{15} , который оставляет инвариантным множество $\{1, \dots, 7\}$ (далее обозначаем этот автоморфизм той же буквой π). Из определения следует, что $\pi(i) = 7$. При действии этого автоморфизма наш код C_{80} перейдёт в эквивалентный ему код

$\tilde{C} = H^{15}(\tilde{\mathcal{B}})$, где $\tilde{\mathcal{B}} = \{R_{p+8}^{\tilde{v}_p} \mid p = 0, \dots, 7\}$ (набор векторов $(\tilde{v}_0, \dots, \tilde{v}_7)$ является некоторой перестановкой первоначального набора (v_0, \dots, v_7)). Вектор u при действии этого автоморфизма перейдёт в \tilde{u} с носителем $[\tilde{u}] = \{1, 2, 8, 12\}$, а v — в \tilde{v} с носителем $[\tilde{v}] = \{1, 2, 7, 8, 12\}$. Среди четырёх пар компонент $\{R_{j_1}, R_{j_2}\}$ с условиями $j_1, j_2 \geq 8$, $j_1 \oplus j_2 = 7$ рассмотрим две: $\{R_8, R_{15}\}$ и $\{R_{11}, R_{12}\}$. Пусть $w \in R_{15}$ — вектор с носителем $[\tilde{w}] = \{3, 7, 8, 12\}$. Так как $[\tilde{v} + \tilde{w}] = \{1, 2, 3\}$, по лемме 5 из [2] (см. также лемму 4 из [8]) получим $\tilde{v} \notin (R_8 + R_{15} + \tilde{w}) = (R_8 + R_{15})$, т. е. \tilde{v} принадлежит смежному классу по подпространству $R_8 + R_{15}$, который равен $R_8^{\tilde{v}_0} + R_{15}^{\tilde{v}_7}$. Это означает, что $\tilde{u} = \tilde{v} + e_7 \in (R_8^{\tilde{v}_0} + e_8) + (R_{15}^{\tilde{v}_7} + e_{15})$. В случае пары компонент $\{R_{11}, R_{12}\}$ получаем также, что $\tilde{w} \in R_{11}$, поэтому $\tilde{v} \notin (R_{11} + R_{12})$, или $\tilde{u} \in (R_{11}^{\tilde{v}_3} + e_{11}) + (R_{12}^{\tilde{v}_4} + e_{12})$. Применяя к вектору \tilde{u} и коду \tilde{C} обратную перестановку π^{-1} , найдём в коде C_{80} две пары компонент $\{R_{i_1}^{v_{i_1}-8} + e_{i_1}, R_{j_1}^{\tilde{v}_{j_1}-8} + e_{j_1}\}$ и $\{R_{i_2}^{v_{i_2}-8} + e_{i_2}, R_{j_2}^{\tilde{v}_{j_2}-8} + e_{j_2}\}$ таких, что $i_1 \oplus j_1 = i_2 \oplus j_2 = i$ и u принадлежит сумме первой пары и сумме второй пары сдвигаемых компонент кода C_{80} . Пусть $i_1, i_2, i_3, i_4 \geq 8$. В этом случае положим $\pi(i_1) = 8$, $\pi(i_2) = 9$, $\pi(i_3) = 10$, $\pi(i_4) = 12$ и продолжим отображение π по линейности до перестановочного автоморфизма кода Хемминга H^{15} , который тоже оставляет инвариантным множество $\{1, \dots, 7\}$, при этом снова $\pi(i) = 7$. При действии этого автоморфизма код C_{80} перейдёт в другой эквивалентный ему код $\tilde{C} = H^{15}(\tilde{\mathcal{B}})$, вектор u перейдёт в вектор \tilde{u} с носителем $[\tilde{u}] = \{8, 9, 10, 12\}$, а вектор v — в вектор \tilde{v} с носителем $[\tilde{v}] = \{7, 8, 9, 10, 12\}$. Среди четырёх пар компонент $\{R_{j_1}, R_{j_2}\}$ с условиями $j_1, j_2 \geq 8$, $j_1 \oplus j_2 = 7$ рассмотрим те же две $\{R_8, R_{15}\}$ и $\{R_{11}, R_{12}\}$. Положим $[w_1] = \{6, 7, 8, 9\}$, $[w_2] = \{2, 4, 10, 12\}$. Так как $w_1 \in R_{15}$, $w_2 \in R_8$, по лемме 5 из [2] $v \notin (R_8 + R_{15} + w_1 + w_2) = R_8 + R_{15}$. В случае пары компонент $\{R_{11}, R_{12}\}$ полагаем $[w_1] = \{2, 7, 9, 12\}$, $[w_2] = \{4, 6, 8, 10\}$. Из того, что $w_1 \in R_{11}$, $w_2 \in R_{12}$, следует, что $v \notin (R_{11} + R_{12} + w_1 + w_2) = R_{11} + R_{12}$. Отсюда снова получаем $\tilde{u} \in (R_8^{\tilde{v}_0} + e_8) + (R_{15}^{\tilde{v}_7} + e_{15})$ и $\tilde{u} \in (R_{11}^{\tilde{v}_3} + e_{11}) + (R_{12}^{\tilde{v}_4} + e_{12})$. Применяя обратную перестановку π^{-1} , снова найдём в коде C_{80} две пары компонент $\{R_{i_1}^{v_{i_1}-8} + e_{i_1}, R_{j_1}^{\tilde{v}_{j_1}-8} + e_{j_1}\}$ и $\{R_{i_2}^{v_{i_2}-8} + e_{i_2}, R_{j_2}^{\tilde{v}_{j_2}-8} + e_{j_2}\}$ таких, что $i_1 \oplus j_1 = i_2 \oplus j_2 = i$ и u принадлежит сумме первой пары и сумме второй пары сдвигаемых компонент кода C_{80} .

Носители векторов $u \in O_4^3$ представляют собой объединение точки и кодовой тройки, не содержащей эту точку. Пусть $[u] = \{i_1, i_2, i_3, i\}$, где $i_3 = i_1 \oplus i_2$ и синдром $i \notin \{i_1, i_2, i_3\}$, $i \leq 7$. Если $i_1, i_2, i_3 \leq 7$, то положим $\pi(i_1) = 1$, $\pi(i_2) = 2$, $\pi(i) = 7$, $\pi(8) = 8$. Отображение π можно продолжить по линейности до перестановочного автоморфизма кода

Хемминга H^{15} , который оставляет инвариантным множество $\{1, \dots, 7\}$. Вектор u при действии этого автоморфизма перейдёт в вектор \tilde{u} с носителем $[\tilde{u}] = \{1, 2, 3, 7\}$. Как и в прошлый раз, рассмотрим две пары компонент $\{R_8, R_{15}\}$ и $\{R_{11}, R_{12}\}$. Положим $\tilde{v} = \{1, 2, 3\}$, $\tilde{w}_1 = \{7, 8, 15\} \in R_8$, $\tilde{w}_2 = \{4, 8, 12\} \in R_8$, $\tilde{w}_3 = \{3, 12, 15\} \in R_{15}$. Поскольку $[\tilde{v} + \tilde{w}_1 + \tilde{w}_2 + \tilde{w}_3] = \{1, 2, 4, 7\}$, по лемме 5 из [2] получим $\tilde{v} \notin (R_8 + R_{15})$, т. е. $\tilde{u} = \tilde{v} + e_7 \in (R_8^{\tilde{v}_0} + e_8) + (R_{15}^{\tilde{v}_7} + e_{15})$. В случае пары компонент $\{R_{11}, R_{12}\}$ рассмотрим три вектора $\tilde{w}_1 = \{7, 11, 12\} \in R_{11}$, $\tilde{w}_2 = \{3, 8, 11\} \in R_{11}$, $\tilde{w}_3 = \{4, 8, 12\} \in R_{12}$. Опять получаем $[\tilde{v} + \tilde{w}_1 + \tilde{w}_2 + \tilde{w}_3] = \{1, 2, 4, 7\}$, откуда следует, что $\tilde{v} \notin (R_{11} + R_{12})$ или $\tilde{u} \in (R_{11}^{\tilde{v}_3} + e_{11}) + (R_{12}^{\tilde{v}_4} + e_{12})$. Применяя к вектору \tilde{u} и к коду \tilde{C} обратную перестановку π^{-1} , найдём в коде C_{80} две пары компонент $\{R_{i_1}^{v_{i_1}-8} + e_{i_1}, R_{j_1}^{v_{j_1}-8} + e_{j_1}\}$ и $\{R_{i_2}^{v_{i_2}-8} + e_{i_2}, R_{j_2}^{v_{j_2}-8} + e_{j_2}\}$ таких, что $i_1 \oplus j_1 = i_2 \oplus j_2 = i$ и u принадлежит сумме первой пары и сумме второй пары сдвигаемых компонент кода C_{80} .

В доказательствах для частей орбит $O_5^2(i)$, $O_5^4(i)$, $O_6^4(i)$, $O_6^5(i)$, $O_7^5(i)$, $O_7^6(i)$, $i \leq 7$, и антиподальных к ним орбит новых технических моментов не появляется. Можно в точности так же доказать, что вектор u , принадлежащий одной из этих частей орбит, принадлежит также сумме по крайней мере двух пар сдвигаемых компонент кода C_{80} . Поэтому сразу перейдём к следующему этапу.

Следующий этап состоит в доказательстве того, что любой кодовый вектор $u \in H^{15}$, отличный от h и $1 + h$, тоже принадлежит множеству $C_{80} + C_{80}$. Так как известно, что код C_{80} имеет полную систему троек, можем сразу начать с кодовых векторов u веса 4. Пусть $[u] = \{i_1, i_2, i_3, i_4\}$, где $i_1 \oplus i_2 \oplus i_3 \oplus i_4 = 0$. Допустим, что $i_1, i_2, i_3, i_4 \leq 7$. В точности так же, как это делалось ранее, пользуясь подходящим автоморфизмом π кода Хемминга H^{15} , сводим общую ситуацию к конкретному варианту $[\tilde{u}] = \{1, 2, 4, 7\}$. Для любого $i \geq 8$ рассмотрим четвёрку $\{i \oplus 1, i \oplus 2, i \oplus 4, i \oplus 7\}$, а также четыре пары компонент $\{R_i, R_{i \oplus 1}\}$, $\{R_i, R_{i \oplus 2}\}$, $\{R_i, R_{i \oplus 4}\}$, $\{R_i, R_{i \oplus 7}\}$. По лемме 5 из [2] \tilde{u} не принадлежит ни одному из множеств $R_i + R_{i \oplus 1}$, $R_i + R_{i \oplus 2}$, $R_i + R_{i \oplus 4}$, $R_i + R_{i \oplus 7}$. Компонента $R_j^{\tilde{v}_{j-8+h}}$ антиподальна сдвигаемой компоненте $R_j^{\tilde{v}_j-8}$, $j = 8, \dots, 15$, кода \tilde{C} (полученного из кода C_{80} действием автоморфизма π). Поэтому $R_j^{\tilde{v}_{j-8+h}} \subset \tilde{C}$, $j = 8, \dots, 15$, и вектор \tilde{u} принадлежит четырём суммам компонент $R_i^{\tilde{v}_{i-8+h}} + R_{i \oplus 1}^{\tilde{v}_{(i \oplus 1)-8+h}}$, $R_i^{\tilde{v}_{i-8+h}} + R_{i \oplus 2}^{\tilde{v}_{(i \oplus 2)-8+h}}$, $R_i^{\tilde{v}_{i-8+h}} + R_{i \oplus 4}^{\tilde{v}_{(i \oplus 4)-8+h}}$ и $R_i^{\tilde{v}_{i-8+h}} + R_{i \oplus 7}^{\tilde{v}_{(i \oplus 7)-8+h}}$. Предположим, что $i_1, i_2, i_3, i_4 \geq 8$. Существует перестановочный автоморфизм π кода H^{15} такой, что $\pi(i_1) = 8$, $\pi(i_2) = 9$, $\pi(i_3) = 10$, $\pi(i_4) = 11$. Пусть \tilde{u} — образ вектора u при действии это-

го автоморфизма. Для любого индекса $i = 12, \dots, 15$ рассмотрим четыре пары компонент $\{R_i, R_8\}, \{R_i, R_9\}, \{R_i, R_{10}\}, \{R_i, R_{11}\}$. Рассмотрим вектор \tilde{w} с носителем $[\tilde{w}] = \{i \oplus 8, i \oplus 9, i \oplus 10, i \oplus 11, 8, 9, 10, 11\}$. Очевидно, что $\tilde{w} \in R_i$ и по лемме 5 из [2] вектор $\tilde{u} + \tilde{w}$ не принадлежит ни одной из сумм $R_i + R_8, R_i + R_9, R_i + R_{10}, R_i + R_{11}$. Следовательно, вектор \tilde{u} принадлежит четырём суммам компонент $R_i^{\tilde{v}_{i-8+h}} + R_8^{\tilde{v}_0+h}, R_i^{\tilde{v}_{i-8+h}} + R_9^{\tilde{v}_1+h}, R_i^{\tilde{v}_{i-8+h}} + R_{10}^{\tilde{v}_2+h}, R_i^{\tilde{v}_{i-8+h}} + R_{11}^{\tilde{v}_3+h}$. Осталось рассмотреть случай $i_1, i_2 \leq 7, i_3, i_4 \geq 8$. Подберём автоморфизм π кода Хемминга H^{15} такой, что $\pi(i_1) = 2, \pi(i_2) = 3, \pi(i_3) = 8, \pi(i_4) = 9$. Для любого индекса $i = 10, \dots, 15$ рассмотрим четыре пары компонент $\{R_i, R_8\}, \{R_i, R_9\}, \{R_i, R_{i \oplus 2}\}, \{R_i, R_{i \oplus 3}\}$. Вектор \tilde{w} с носителем $[\tilde{w}] = \{i \oplus 8, i \oplus 9, 8, 9\}$ принадлежит компоненте R_i . Отсюда следует, что вектор $\tilde{u} + \tilde{w}$ с носителем $[\tilde{u} + \tilde{w}] = \{2, 3, i \oplus 8, i \oplus 9\}$ не принадлежит ни одной из сумм $R_8 + R_i, R_9 + R_i, R_i + R_{i \oplus 2}, R_i + R_{i \oplus 3}$. Поэтому вектор \tilde{u} принадлежит четырём суммам компонент $R_i^{\tilde{v}_{i-8+h}} + R_8^{\tilde{v}_0+h}, R_i^{\tilde{v}_{i-8+h}} + R_9^{\tilde{v}_1+h}, R_i^{\tilde{v}_{i-8+h}} + R_{i \oplus 2}^{\tilde{v}_{(i \oplus 2)-8+h}}, R_i^{\tilde{v}_{i-8+h}} + R_{i \oplus 3}^{\tilde{v}_{(i \oplus 3)-8+h}}$.

В доказательствах для частей орбит $O_5^1(i), O_6^1(i), O_7^2(i), i \leq 7$, и антиподальных к ним орбит новых технических моментов не появляется. Следует особо отметить, что для любых вектора u из этих множеств и индекса $i \geq 8$ (за исключением двух значений в случае орбиты O_4^1) существует четвёрка $K = \{i_1, i_2, i_3, i_4\} \subset \{8, \dots, 15\}$ такая, что $i \notin K$, $i_1 \oplus i_2 \oplus i_3 \oplus i_4 = 0$ и $u \in R_i^{v_{i-8+h}} + R_j^{v_{j-8+h}}$ для любого $j \in K$. Это свойство неединственности представления вектора u суммами элементов из C_{8^0} будет необходимо для дальнейшего. Перейдём к изучению дополнения к множеству $C_{8^0} + C_{8^0}$.

В геометрической интерпретации носители векторов из орбиты $O_8^3(i)$ являются плоскостями Фано, не содержащими i , с добавленной точкой i . Если $i \geq 8$ и $u \in O_8^3(i)$, то, как отмечалось ранее, дополнение

$$(R_i^{v_{15-i}} + u + e_i) \setminus \left(\bigcup_{p=0}^7 R_{p+8}^{v_p} \right)$$

непусто. Если взять любой вектор v из этого дополнения, то $v \in C_{8^0}$ и $w = u + v \in (R_i^{v_{15-i}} + e_i) \subset C_{8^0}$. Поэтому $u = v + w \in (C_{8^0} + C_{8^0})$. Допустим, что $i \leq 7$. Если $u \in (C_{8^0} + C_{8^0})$, то он может быть получен только как сумма двух векторов из сдвинутых компонент $R_{p+8}^{v_p} + e_{p+8}$ и $R_{q+8}^{v_q} + e_{q+8}$ таких, что $i = (p+8) \oplus (q+8) = p \oplus q$. Докажем, что этого не может быть. Так как носитель вектора $u + e_i$ является плоскостью Фано, не содержащей i , то либо $p+8 \in [u + e_i]$, либо $q+8 \in [u + e_i]$ (в трёхмерной

проективной геометрии прямая и плоскость имеют непустое пересечение). Это означает, что либо $u + e_i \in R_{p+8}$, либо $u + e_i \in R_{q+8}$. В любом случае $u + e_i \in R_{p+8} + R_{q+8}$. Из непересекаемости компонент $R_{p+8}^{v_p}$ и $R_{q+8}^{v_q}$ сразу следует, что $u + e_i \notin (R_{p+8}^{v_p} + R_{q+8}^{v_q})$. Это равносильно тому, что $u \notin (R_{p+8}^{v_p} + e_{p+8}) + (R_{q+8}^{v_q} + e_{q+8})$. Мы доказали, что $u \notin (C_{8^0} + C_{8^0})$. Так как любой код C и дополнение $\{0, 1\}^{15} \setminus (C + C)$ симметричны относительно отображения $u \mapsto \mathbf{1} + u$, для антиподальной орбиты O_7^3 тоже всё доказано. Носители векторов из орбиты O_7^4 являются объединением плоскости Фано с выколотой точкой и точки, не лежащей в этой плоскости. Все доказательства для этого случая аналогичны доказательству для орбиты O_8^3 .

Рассмотрим вектор h из орбиты O_7^1 . Это единственный вектор из кода Хемминга H^{15} , не принадлежащий множеству $C_{8^0} + C_{8^0}$. Действительно, h может быть только суммой двух векторов из пересечения $H^{15} \cap C_{8^0}$. Кроме того, $h \notin R_i$ для всех $i \geq 8$. Поэтому h нельзя представить суммой двух векторов из одной и той же i -компоненты кода C_{8^0} . Для любого $i \geq 8$ вектор h принадлежит сумме компоненты R_i^u с антиподальной компонентой R_i^{u+h} . Но если $R_i^u \subset C_{8^0}$, то антиподальная компонента R_i^{u+h} не пересекается с кодом C_{8^0} , так как компонента $R_i^{u+h} + e_i$ должна быть одной из сдвинутых компонент $R_i^{v_i-8} + e_i \subset C_{8^0}$. Остался последний вариант: $h \in R_i^u + R_j^v$, где $i, j \geq 8$, $i \neq j$ и R_i^u, R_j^v входят в пересечение $H^{15} \cap C_{8^0}$. Но это противоречит непересекаемости компонент R_i^u и R_j^v , так как R_i^u, R_j^v являются элементами одного и того же (8×2) -разбиения. Следовательно, $h, \mathbf{1} + h \notin (C_{8^0} + C_{8^0})$.

Получили полное описание дополнения к множеству $C_{8^0} + C_{8^0}$. Для кода C_{8^1} вышеприведённое доказательство сохраняется без каких либо изменений, в частности $\{0, 1\}^{15} \setminus (C_{8^0} + C_{8^0}) = \{0, 1\}^{15} \setminus (C_{8^1} + C_{8^1})$. Осталось сосчитать число элементов этого множества. Из доказанного следует, что коды C_{8^0}, C_{8^1} имеют полную систему четвёрок. Поэтому в дополнении к $C_{8^0} + C_{8^0}$ имеется 30 векторов веса 1 и 14, 210 векторов веса 2 и 13, 630 векторов из орбит O_5^3, O_{10}^3 , 1050 векторов из орбит $O_6^2, O_9^2, O_6^3, O_9^3$. Так как число векторов из орбит O_7^3, O_7^4 равно 120 и 840 соответственно, $|O_7^3(i)| = 8, |O_7^4(i)| = 56$. Поэтому число векторов из объединения $\bigcup_{i=1}^7 [O_7^3(i) \cup O_7^4(i) \cup O_8^3(i) \cup O_8^4(i)]$ равно 896. С учётом векторов $h, \mathbf{1} + h$ получаем в сумме 2818. Лемма 1 доказана.

Коды из классов эквивалентности $Y_{81}, Y_{82}, Y_{83}, Y_{84}^1$ получаются из кода Хемминга H^{15} также сдвигами кратных компонент. Представитель класса Y_{81} кодируется символом $[0]_8 1_9 2_{10} 3_{11} 4_{12} 5_{13} 6_{14} 7_{15}$. Это означает,

что для построения такого кода необходимо сдвинуть в коде Хемминга H^{15} пару взаимно антиподальных компонент $R_8^{v_0}, R_8^{v_{\bar{0}}}$ на вектор e_8 и компоненты $R_{i+8}^{v_i}$ на векторы e_{i+8} , $i = 1, \dots, 7$. Представитель класса $Y82$ кодируется символом $[0]_8[1]_9 2_{10} 3_{11} 4_{12} 5_{13} 6_{14} 7_{15}$, поэтому для построения такого кода необходимо сдвинуть в H^{15} две пары антиподальных компонент $R_8^{v_0}, R_8^{v_{\bar{0}}}$ и $R_8^{v_1}, R_8^{v_{\bar{1}}}$ и ещё 6 компонент $R_{i+8}^{v_i}$, $i = 2, \dots, 7$, и т. д. Обозначим коды, представляющие вышеуказанные орбиты, символами $C_{81}, C_{82}, C_{83}, C_{84^1}$. Далее используем определение множества D_{\min} из леммы 1.

Лемма 2. Для любого $\lambda = 1, 2, 3$ дополнение $D_{8\lambda}$ к $C_{8\lambda} + C_{8\lambda}$ имеет вид

$$D_{8\lambda} = D_{\min} \cup \bigcup_{i=1}^{\lambda+7} [O_7^3(i) \cup O_7^4(i) \cup O_8^3(i) \cup O_8^4(i)].$$

Дополнение D_{84} к $C_{84^1} + C_{84^1}$ имеет вид

$$D_{84} = D_{83} \cup [O_7^3(12) \cup O_7^4(12) \cup O_8^3(12) \cup O_8^4(12)],$$

$$|D_{8\lambda}| = 2816 + 128\lambda, \quad \lambda = 1, \dots, 4.$$

ДОКАЗАТЕЛЬСТВО. Пусть C обозначает один из перечисленных выше кодов. Если $i \geq 8$ и $u \in O(i)$, где $O(i)$ — одна из орбит $O_3^2(i), O_4^2(i), O_4^3(i), O_5^2(i), O_5^4(i), O_6^4(i), O_6^5(i), O_7^3(i), O_7^4(i), O_7^5(i), O_7^6(i)$ или одна из антиподальных к ним орбит, то доказательство того, что $u \in (C + C)$, приведённое в лемме 1, остаётся в силе, кроме случаев $u \in O_7^3(i)$ и $u \in O_7^4(i)$, где индекс i такой, что для построения кода C необходимо сдвинуть в коде Хемминга пару взаимно антиподальных компонент $R_i^{v_{i-8}}, R_i^{v_{i-8+h}}$ ($i = 8$ для кода C_{81} , $i = 8, 9$ для кода C_{82} , $i = 8, 9, 10$ для кода C_{83} , $i = 8, 9, 10, 12$ для кода C_{84^1}). Это следует из того, что если $u \in O_7^3(i)$ или $u \in O_7^4(i)$, то $R_i^{v_{i-8}} + u = R_i^{v_{i-8+h}} + e_i$ и $(R_i^{v_{i-8}} + e_i) + (R_i^{v_{i-8+h}} + e_i)$ имеет нулевой синдром. Полностью остаётся в силе и доказательство из леммы 1 для случая, когда $i \leq 7$ и u принадлежит одному из множеств $O_4^2(i), O_4^3(i), O_5^2(i), O_5^4(i), O_6^4(i), O_6^5(i), O_7^5(i), O_7^6(i)$. Так как $h \in (R_8^{v_0} + e_8) + (R_8^{v_0+h} + e_8)$, имеем $h \in (C + C)$. Докажем, что весь код Хемминга H^{15} входит в $C + C$. В лемме 1 доказано, что если $u \in H^{15}$ и $u \neq h, 1 + h$, то для любого индекса $i \geq 8$ (за исключением быть может двух значений) существует четвёрка $K = \{i_1, i_2, i_3, i_4\} \subset \{8, \dots, 15\}$ такая, что $i \notin K$, $i_1 \oplus i_2 \oplus i_3 \oplus i_4 = 0$ и $u \in R_i^{v_{i-8+h}} + R_j^{v_{j-8+h}}$ для любого $j \in K$. Такое i найдётся среди трёх индексов 13, 14, 15. Поскольку $8 \oplus 9 \oplus 10 \oplus 12 \neq 0$, можно выбрать $j \in K \setminus \{8, 9, 10, 12\}$. Поэтому $R_i^{v_{i-8+h}}, R_j^{v_{j-8+h}} \subset C$, т. е. $u \in C + C$.

Посмотрим, какие векторы попадают в дополнение к $C + C$. Очевидно, что состав векторов веса $\neq 7, 8$ в дополнении к $C + C$ такой же, какой он в дополнении к $C_{80} + C_{80}$. Векторы u из множеств $O_7^3(i)$, $O_7^4(i)$, $O_8^3(i)$, $O_8^4(i)$ при $i \leq 7$ тоже остаются в дополнении к $C + C$ (все доказательства из леммы 1 остаются в силе). Здесь особо отметим, что в случае кода C_{841} если \mathcal{B} — семейство компонент, сдвигаемых при построении кода C_{84} , то компонента $R_i^{v_{15-i}} + u + e_i$ пересекается только с четырьмя компонентами $R_{i_p}^{v_{15-i_p}}$, $p = 1, \dots, 4$, из семейства \mathcal{B} , причём $i_1 \oplus i_2 \oplus i_3 \oplus i_4 = 0$. При построении кода C_{841} сдвигаются четыре пары взаимно антиподальных компонент с номерами 8, 9, 10, 12 и $8 \oplus 9 \oplus 10 \oplus 12 = 7 \neq 0$. Поэтому опять дополнение $(R_i^{v_{15-i}} + u + e_i) \setminus (\bigcup \mathcal{B})$ будет непустым, и если вектор v из этого дополнения, $w = u + v$, то $w \in R_i^{v_{15-i}} + e_i \subset C_{841}$, $v \in C_{841}$ и $u = v + w \in C_{841} + C_{841}$. В дополнении к $C + C$ появятся также все векторы из множеств $O_7^3(i)$, $O_7^4(i)$, $O_8^3(i)$, $O_8^4(i)$ при $i = 8$ в случае кода C_{81} , $i = 8, 9$ в случае кода C_{82} , $i = 8, 9, 10$ в случае кода C_{83} и $i = 8, 9, 10, 12$ в случае кода C_{841} . Это следует из того, что такой вектор u должен принадлежать множеству $(R_i^{v_{i-8}} + e_i) + v$ при некотором $v \in C \cap H^{15}$. Но, как отмечено выше, $R_i^{v_{i-8}} + u = R_i^{v_{i-8}+h} + e_i$. Поэтому должно быть $v \in R_i^{v_{i-8}+h}$, но эта компонента не входит в код C , если $C = C_{81}$ и $i = 8$, $C = C_{82}$ и $i = 8, 9$, и т. д. Легко видеть, что число элементов в множестве $O_7^3(i) \cup O_7^4(i) \cup O_8^3(i) \cup O_8^4(i)$ равно 128. Это обосновывает формулу $2816 + 128\lambda$ для числа элементов в множестве $D_{8\lambda}$. Лемма 2 доказана.

Шесть несистематических кодов $C_7 = C_{70}, C_{71}, C_{72}, C_{73^0}, C_{73^1}, C_{74^1}$ строятся из кода Хемминга H^{15} сдвигами i -компонент, $8 \leq i \leq 14$ [5]. Из таблицы в [5] следует, что при построении кода C_7 не используются сдвиги кратных компонент; при построении кода C_{71} сдвигается одна пара взаимно антиподальных 8-компонент и шесть i -компонент, $9 \leq i \leq 14$; при построении кода C_{72} сдвигаются две пары взаимно антиподальных 8-компонент и 9-компонент и пять i -компонент, $10 \leq i \leq 14$; при построении C_{73^0} и C_{73^1} кодов сдвигаются три пары взаимно антиподальных компонент и четыре i -компоненты; $i = 11, 12, 13, 14$ для кода C_{73^1} , $i = 10, 11, 12, 13$ для кода C_{73^0} ; при построении кода C_{74^1} сдвигаются четыре пары взаимно антиподальных компонент и три i -компоненты, $i = 11, 13, 14$. Обозначим через $D_{7\lambda}$ дополнение к множеству $C_{7\lambda} + C_{7\lambda}$ для одного из перечисленных кодов, при построении которого сдвигается в коде Хемминга H^{15} λ пар взаимно антиподальных компонент. Далее используем обозначения множеств $D_{8\lambda}$ из лемм 1 и 2, $0 \leq \lambda \leq 4$.

Лемма 3. Дополнение $D_{7\lambda}$ имеет вид $D_{7\lambda} = D_{8\lambda} \cup (H^{15} + e_{15})$. Число

элементов в $D_{7\lambda}$ равно $4736 + 128\lambda$, $0 \leq \lambda \leq 4$.

ДОКАЗАТЕЛЬСТВО. Пусть \mathcal{B} — семейство сдвигаемых компонент кода Хемминга при построении одного из кодов вида $C_{7\lambda}$. Если векторы v и w принадлежат двум сдвинутым компонентам этого семейства, то синдром вектора $v + w$ либо ≤ 7 (если v, w принадлежат разным компонентам с разными номерами), либо равен одному из чисел $8, \dots, 14$ (если v принадлежит одной из сдвинутых компонент семейства \mathcal{B} , а $w \in H^{15}$), либо равен нулю (если v, w принадлежат одной и той же сдвинутой компоненте семейства \mathcal{B} , или $v, w \in H^{15} \cap C_{7\lambda}$). Поэтому в сумме $C_{7\lambda} + C_{7\lambda}$ нет векторов с синдромом 15. Это означает, что $(H^{15} + e_{15}) \subset D_{7\lambda}$ для всех $\lambda = 0, \dots, 4$. Состав векторов с синдромом $\neq 15$ такой же, как и у кодов $C_{8\lambda}$. Например, в доказательстве леммы 1 отмечено, что вектор u , принадлежащий одной из частей орбит $O_4^2(i), O_4^3(i), O_5^2(i), O_5^4(i), O_6^4(i), O_6^5(i), O_7^5(i), O_7^6(i), O_7^7(i), i \leq 7$, или одной из антиподальных к ним орбит, принадлежит также сумме по крайней мере двух пар сдвигаемых компонент кода C_{80} , поэтому по крайней мере одна из них будет парой сдвигаемых компонент кодов $C_{7\lambda}$. Стало быть, все такие векторы принадлежат множеству $C_{7\lambda} + C_{7\lambda}$. Этому множеству при $\lambda > 0$ принадлежат также все кодовые векторы (векторы с нулевым синдромом) в силу того, что они принадлежали множеству $C_{8\lambda} + C_{8\lambda}$. Все кодовые векторы принадлежат множеству $C_{70} + C_{70}$, поскольку больше половины векторов из C_{70} принадлежат коду Хемминга H^{15} , т. е. $H^{15} \subset (C_{7\lambda} + C_{7\lambda})$, $\lambda = 0, \dots, 4$. Так же, как и в случае кодов $C_{8\lambda}$, каждая пара сдвигаемых взаимно антиподальных компонент $R_i^{v_{i-8}} + e_i, R_i^{v_{i-8}+h} + e_i$ поставляет в дополнение к множеству $C_{7\lambda} + C_{7\lambda}$ ещё 128 векторов с синдромом i . Теперь необходимо сосчитать число векторов в дополнении к множеству $C_{70} + C_{70}$. Число векторов из дополнения к $C_{80} + C_{80}$ без учёта двух векторов $h, 1 + h$ равно 1816. К ним необходимо добавить векторы с синдромом 15, которые не были учтены ранее. Число троек с синдромом 15 равно 28, число таких же четвёрок из орбит O_4^2, O_4^3 равно 84. Веса орбит O_5^2 и O_5^4 равны 840 и 1680 соответственно. Поэтому число векторов из этих орбит с синдромом 15 равно 168. Аналогично считается число неучтённых ранее шестёрок из орбит O_6^4 и O_6^5 , равное 280, и семёрок из орбит O_7^3, O_7^4, O_7^5 и O_7^6 , равное 400. Удвоенная их сумма (с учётом векторов веса > 7) равна 4736 — числу векторов в дополнении к множеству $C_{70} + C_{70}$. Так как каждая пара сдвигаемых взаимно антиподальных компонент поставляет в дополнение по 128 векторов, число векторов в дополнении к множеству $C_{7\lambda} + C_{7\lambda}$ равно $4736 + 128\lambda$. Лемма 3 доказана.

2. Основные результаты

В качестве первого результата определим все аффинно 3-несистематические коды длины 15.

Теорема 2. *Четыре кода $C_{81}, C_{82}, C_{83}, C_{84}$ являются аффинно 3-несистематическими, остальные 8 кодов $C_{80}, C_{81}, C_7, C_{71}, C_{72}, C_{73^0}, C_{73^1}, C_{74^1}$ аффинно 3-систематические.*

ДОКАЗАТЕЛЬСТВО. Из леммы 2 следует, что дополнения $D_{8\lambda}, \lambda = 1, \dots, 4$, монотонно возрастают по включению, т. е. $D_{81} \subset D_{82} \subset D_{83} \subset D_{84}$. Поэтому достаточно проверить, что в одном множестве $D_{84} \cup \{0\}$ не содержится ни одного трёхмерного подпространства. Этот факт является результатом компьютерного эксперимента, состоящего в переборе всех троек векторов $u, v, w \in D_{84}$ и проверке того, что хотя бы один из четырёх векторов $u + v, u + w, v + w, u + v + w$ не принадлежит множеству D_{84} . Отсюда сразу следует аффинная 3-несистематичность кодов $C_{8\lambda}, 1 \leq \lambda \leq 4$. Аффинная 3-систематичность кодов $C_{7\lambda}, 0 \leq \lambda \leq 4$, вытекает сразу из того, что все они имеют неполную систему троек. Например, рассмотрим вектор u с носителем $[u] = \{1, 6, 8\}$, имеющим синдром 15. В качестве искомого трёхмерного подпространства из множества $D_{7\lambda} \cup \{0\}$ можно рассмотреть линейную оболочку базисных векторов e_1, e_6, e_8 . Для доказательства аффинной 3-систематичности двух кодов C_{80} и C_{81} рассмотрим линейную оболочку L трёх векторов e_1, e_2 и $v \in O_5^3$ с носителем $[v] = \{3, 4, 5, 6, 7\}$. Так как по лемме 1 и теореме 1 $v \in O_5^3 \subset D_8, e_1 + v, e_2 + v \in O_6^3 \subset D_8, e_1 + e_2 + v = h \in D_8$, имеем $L \subset D_8 \cup \{0\}$. Теорема 2 доказана.

В качестве второго результата докажем аффинную несистематичность (т. е. аффинную 4-несистематичность) всех 12 несистематических 1-свитчинговых кодов длины 15.

Теорема 3. *Все несистематические коды $C_7, C_{71}, C_{72}, C_{73^0}, C_{73^1}, C_{74}, C_{80}, C_{81}, C_{81}, C_{82}, C_{83}, C_{84}$ аффинно несистематические.*

ДОКАЗАТЕЛЬСТВО. Из теоремы 2 следует, что коды $C_{81}, C_{82}, C_{83}, C_{84}$ аффинно 3-несистематические. Поэтому они тем более просто аффинно несистематические. Допустим, что существует четырёхмерное подпространство M в множестве $D_8 \cup \{0\}$. Так как $1 \notin M$, этому подпространству может принадлежать только один из векторов $h, 1 + h$. Для определённости будем считать, что $h \in M$. Рассмотрим в M любое трёхмерное подпространство L , не содержащее вектора h . Тогда $L \setminus \{0\} \subset D_{84}$, что противоречит утверждению теоремы 2. Значит, коды C_{80} и C_{81} аффинно несистематические. Этот приём можно использовать и для до-

казательства аффинной несистематичности кодов серии $C_{7\lambda}$, $0 \leq \lambda \leq 4$. Рассмотрим четырёхмерное подпространство M в множестве $D_{74} \cup \{\mathbf{0}\}$. Так как множество D_{74} не содержит кодовых векторов, M является подпространством, дополнительным к коду Хемминга H^{15} [6]. В силу леммы 1 из [6] векторы u_i из M можно пронумеровать так, что $u_i + u_j = u_{i \oplus j}$, $0 \leq i, j \leq 15$. Следовательно, все векторы u_i , кроме $u_0 = \mathbf{0}$, имеют ненулевой синдром, равный i . Рассмотрим в M трёхмерное подпространство $L = \{u_0, u_1, \dots, u_7\}$. Поскольку все векторы из L имеют синдром $\neq 15$, в силу леммы 3 получаем $L \subset D_{84}$; противоречие с теоремой 2. Поэтому все 6 кодов C_7 , C_{71} , C_{72} , C_{73^0} , C_{73^1} , C_{74^1} аффинно несистематические. Теорема 3 доказана.

Теорема 2 даёт другое альтернативное доказательство аффинной несистематичности всех несистематических 1-свитчинговых кодов длины 15 (см. замечание в конце работы [6]).

Следующий результат носит общий характер, так как он касается всех 1-свитчинговых совершенных кодов длины $n > 15$. Сейчас решим задачу о минимальном дополнении к множеству $C + C$ для 1-свитчинговых кодов. В качестве «экстремальных» в этом смысле кодов рассмотрим коды вида $H^n(\mathcal{B}_n)$, где $\mathcal{B}_n = \{R_1^{v_1}, \dots, R_n^{v_n}\}$ — семейство из n попарно не пересекающихся i -компонент, не содержащее кратных компонент, $i = 1, \dots, n$, $n = 2^k - 1$. Такие семейства компонент существуют в кодах Хемминга H^n , если $n > 15$. Именно такие семейства компонент применялись впервые в [1, 11] для построения несистематических кодов.

Обозначим $D_{\min}^n = \bigcup_{i=1}^n (R_i + e_i)$.

Теорема 4. Пусть $C = H^n(\mathcal{B})$ — любой 1-свитчинговый код, построенный из кода Хемминга сдвигами не пересекающихся компонент некоторого семейства \mathcal{B} . Тогда $D(C) = \{0, 1\}^n \setminus (C + C) \supset D_{\min}^n$. Если $C = H^n(\mathcal{B}_n)$, где $\mathcal{B}_n = \{R_1^{v_1}, \dots, R_n^{v_n}\}$ — семейство из n попарно не пересекающихся i -компонент, не содержащее кратных компонент, $i = 1, \dots, n$, то $D(C) = D_{\min}^n$.

ДОКАЗАТЕЛЬСТВО. Первое утверждение следует из теоремы 1. Пусть $C = H^n(\mathcal{B}_n)$ и $u \notin D_{\min}^n$. Допустим $u \in H^n$. Так как мощность $\bigcup \mathcal{B}_n$ меньше половины мощности всего кода Хемминга H^n , то $H^n \subset (C + C)$, поэтому $u \in (C + C)$. Если $u \notin H^n$, то u имеет ненулевой синдром i . Так как $u \notin R_i + e_i$, имеем $R_i^{v_i} + u \neq R_i^{v_i} + e_i$ и $R_i^{v_i} + u + e_i \notin \mathcal{B}_n$. Отсюда $(R_i^{v_i} + u + e_i) \setminus \bigcup \mathcal{B}_n \neq \emptyset$ (в [11] это часть доказательства несистематичности кода C). Если $w \in (R_i^{v_i} + u + e_i) \setminus \bigcup \mathcal{B}_n$, то $v = u + w \in R_i^{v_i} + e_i \subset C$. Поскольку $w \in C \cap H^n$, имеем $u \in (C + C)$. Теорема 4 доказана.

По определению компонента R_i состоит из векторов u , представимых конечной суммой различных векторов веса 3 с единичной i -й координатой. Отсюда следует, что $u_i = 1$, если u представляется суммой нечётного числа таких векторов веса 3, и $u_i = 0$, если u является суммой чётного числа векторов веса 3, т. е. R_i содержит только векторы u весов 4ℓ или $4\ell + 3$ при некотором $\ell \geq 0$. Соответственно компонента $R_i + e_i$ содержит только векторы с весами $4\ell + 1$ или $4\ell + 2$. Поэтому из теоремы 4 вытекает

Следствие 1. Пусть $C = H^n(\mathcal{B}_n)$, где $\mathcal{B}_n = \{R_1^{v_1}, \dots, R_n^{v_n}\}$ — семейство из n попарно не пересекающихся i -компонент, не содержащее кратных компонент, $i = 1, \dots, n$. Тогда код C имеет полную систему множеств мощности m для любого $m = 4l, 4l - 1$, $1 \leq l < (n - 3)/4$, и этот результат нелучшаем в классе 1-свитчинговых кодов.

Так как $H^n \subset (C + C)$, имеем $v_i + R_i^{v_i} + e_i = R_i + e_i \subset (C + C + C)$. Отсюда получаем

Следствие 2. Если $C = H^n(\mathcal{B}_n)$, где $\mathcal{B}_n = \{R_1^{v_1}, \dots, R_n^{v_n}\}$ — семейство из n попарно не пересекающихся i -компонент, не содержащее кратных компонент, $i = 1, \dots, n$, то $C + C + C = \{0, 1\}^n$.

Поскольку векторы веса 1 и 2 не принадлежат множеству $C + C$, этот результат нелучшаем в классе всех совершенных кодов длины n .

Замечание 1. Среди всех 1-свитчинговых кодов длины 15 только два аффинно несистематических (аффинно 3-систематических) кода $C = C_{80}$ и $C = C_{81}$ имеют минимальное по мощности (но не по включению) дополнение $|\{0, 1\}^{15} \setminus (C + C)| = 2818$.

Замечание 2. Для любого из 12 несистематических 1-свитчинговых кодов C длины 15 имеет место равенство $C + C + C = \{0, 1\}^{15}$.

ЛИТЕРАТУРА

1. Августинovich С. В., Соловьева Ф. И. О несистематических совершенных двоичных кодах // Пробл. передачи информации. 1996. Т. 32, вып. 3. С. 47–50.
2. Малюгин С. А. О перечислении совершенных двоичных кодов длины 15 // Дискрет. анализ и исслед. операций. Сер. 2. 1999. Т. 6, № 2. С. 48–73.
3. Малюгин С. А. Несистематические совершенные двоичные коды // Дискрет. анализ и исслед. операций. Сер. 1. 2001. Т. 8, № 1. С. 55–76.
4. Малюгин С. А. Об аффинно несистематических кодах // Сб. докл. междунар. конф., посвящённой 90-летию со дня рождения

- А. А. Ляпунова (Новосибирск, 8–12 октября 2001 г.). 2001. С. 393–394.
<http://www.sbras.nsc.ru/ws/Lyap2001/2288>
5. **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.
 6. **Малюгин С. А.** Аффинно несистематические коды // Дискрет. анализ и исслед. операций. 2012. – Т. 19, № 4. С. 73–85.
 7. **Малюгин С. А.** Аффинно 3-несистематические коды // Дискрет. анализ и исслед. операций. 2014. Т. 21, № 4. С. 54–61.
 8. **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.
 9. **Романов А. М.** О несистематических совершенных кодах длины 15 // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 4. С. 75–78.
 10. **Phelps K. T., LeVan M. J.** Kernels of nonlinear Hamming codes // Des. Codes Cryptogr. 1995. Vol. 6, No. 3. P. 247–257.
 11. **Phelps K. T., LeVan M. J.** Nonsystematic perfect codes // SIAM J. Discrete Math. 1999. Vol. 12, No. 1. P. 27–34.
 12. **Solov'eva F. I.** Switchings and perfect codes // Numbers, information and complexity. Dordrecht: Kluwer Acad. Publ., 2000. P. 311–324.

Сергей Артемьевич Малюгин

Статья поступила

26 января 2014 г.

Исправленный вариант —

24 сентября 2014 г.

DISKRETNYYI ANALIZ I ISSLEDOVANIE OPERATSII
January–February 2015. Volume 22, No. 1. P. 32–50

UDC 519.8

AFFINE 3-NONSYSTEMATIC PERFECT CODES OF LENGTH 15

S. A. Malyugin¹

¹Sobolev Institute of Mathematics SB RAS,
4 Acad. Koptug Ave., 630090 Novosibirsk, Russia
e-mail: mal@math.nsc.ru

Abstract. A perfect binary code C of length $n = 2^k - 1$ is called *affine 3-systematic* if there exists a 3-dimensional subspace L in the space $\{0, 1\}^n$ such that the intersection of any of its cosets $L + u$ with C is either empty, or a singleton. Otherwise, the code C is called *affine 3-nonsystematic*. In the paper, we construct four nonequivalent affine 3-nonsystematic codes of length 15. Bibliogr. 12.

Keywords: perfect code, Hamming code, nonsystematic code, affine nonsystematic code, affine 3-nonsystematic code, component.

REFERENCES

1. S. V. Avgustinovich and F. I. Solov'eva, On nonsystematic perfect binary codes, *Probl. Peredachi Inf.*, **32**, No. 3, 47–50, 1996. Translated in *Probl. Inf. Transm.*, **32**, No. 3, 47–50, 1996.
2. 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. Translated in *Diskrete Appl. Math.*, **135**, No. 1–3, 161–181, 2004.
3. S. A. Malyugin, Nonsystematic perfect binary codes, *Diskretn. Anal. Issled. Oper.*, Ser. 1, **8**, No. 1, 55–76, 2001.
4. S. A. Malyugin, On affine nonsystematic codes, *Proc. Conf. Devoted to the 90th Anniversary of A. A. Lyapunov, Novosibirsk, Russia, Oct. 8–11, 2001*, pp. 393–394, Novosibirsk, 2009. Available at <http://www.sbras.ru/ws/Lyap2001/2288/>. Accessed Jan. 13, 2015.
5. S. A. Malyugin, On enumeration of nonequivalent perfect binary codes of length 15 and rank 15, *Diskretn. Anal. Issled. Oper.*, Ser. 1, **13**, No. 1, 77–98, 2006. Translated in *J. Appl. Ind. Math.*, **1**, No. 1, 77–80, 2007.
6. S. A. Malyugin, Affine nonsystematic codes, *Diskretn. Anal. Issled. Oper.*, **19**, No. 4, 73–85, 2012. Translated in *J. Appl. Ind. Math.*, **6**, No. 4, 451–459, 2012.

7. **S. A. Malyugin**, Affine 3-nonsystematic codes, *Diskretn. Anal. Issled. Oper.*, **21**, No. 4, 54–61, 2014. Translated in *J. Appl. Ind. Math.*, **8**, No. 4, 552–556, 2014.
8. **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.
9. **A. M. Romanov**, On nonsystematic perfect codes of length 15, *Diskretn. Anal. Issled. Oper.*, Ser. 1, **4**, No. 4, 75–78, 1997. Translated in *Discrete Appl. Math.*, **135**, No. 1–3, 255–258, 2004.
10. **K. T. Phelps** and **M. LeVan**, Kernels of nonlinear Hamming codes, *Des. Codes Cryptogr.*, **6**, No. 3, 247–257, 1995.
11. **K. T. Phelps** and **M. LeVan**, Nonsystematic perfect codes, *SIAM J. Discrete Math.*, **12**, No.1, 27–34, 1999.
12. **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.

Sergey A. Malyugin

Received

26 January 2014

Revised

24 September 2014