ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль—декабрь 1999. Серия 2. Том 6, № 2, 48–73

УДК 519.72

О ПЕРЕЧИСЛЕНИИ СОВЕРШЕННЫХ ДВОИЧНЫХ КОДОВ ДЛИНЫ 15*)

С. А. Малюгин

Рассматривается следующая конструкция кодов. Сначала в коде Хемминга H^n выделяется некоторое семейство из m попарно непересекающихся i_q-компонент, $q = 1, \ldots, m$. Затем для каждого q изменяется координата i_q у всех векторов i_q-компоненты из выделенного набора. Полученное таким способом семейство совершенных кодов содержит коды Васильева, а также многие другие коды, обладающие различными интересными свойствами: несистематические коды, коды полного ранга, коды с тривиальной группой автоморфизмов. В настоящей работе перечисляются все получаемые с помощью такой конструкции совершенные коды длины $n = 15$. Число различных кодов, которые можно построить этим способом из кода Хемминга H^{15}, равно 131224492.

Введение

Наиболее известными совершенными двоичными кодами являются коды Хемминга длины $n = 2^k - 1$ $(k \in \mathbf{N})$. Они характеризуются тем, что образуют в n-мерном двоичном кубе линейное подпространство размерности $n - k$. Большой класс нелинейных совершенных кодов был впервые построен Ю. Л. Васильевым [3]. Подход Васильева в общих чертах состоит в следующем. В коде выделяется его «подвижная часть», т. е. такое подмножество, после сдвига которого по какой-либо координате i (изменяется значение i-й координаты у всех векторов этого множества) снова получается совершенный код. Эта «подвижная часть» кода называется i-компонентой, или решеткой. Начиная с кода Хемминга путем последовательных сдвигов i-компонент можно получать различные нелинейные коды. Если при этом координата i фиксируется, то мы получаем коды Васильева. Если на каждом шаге перехода к следующему сдвигу координату i можно менять, то получается более широкий класс кодов, который мы будем называть свитчинговым классом кода

*) Работа выполнена при финансовой поддержке Федеральной целевой программы «Интеграция» (проект 1997–473).

Хемминга [17]. Возникает вопрос: насколько широк такой класс? Недавние исследования указывают на то, что этот класс достаточно мощный. Например, в настоящее время нижние оценки числа различных кодов длины n получены именно подсчетом числа кодов из свитчингового класса кода Хемминга (см. [2–4, 18]. Кроме того, были построены коды из этого же класса, обладающие различными интересными свойствами: несистематические коды [1, 5, 15]; коды с тривиальным ядром [11, 15]; коды полного ранга [10, 11]; коды с тривиальной группой автоморфизмов [9, 12]. Следует также отметить, что существуют нелинейные коды, которые не попадают в свитчинговый класс кода Хемминга [16].

В связи с этим возникает задача описания свитчинговых классов кодов Хемминга различной длины. Нелинейные коды появляются, начиная с длины $n = 15$. Но даже в этом простейшем случае задача перечисления всех кодов оказывается нетривиальной. В настоящей работе решается задача классификации всех совершенных двоичных кодов, которые могут быть получены из кода Хемминга H^{15} сдвигами его непересекающихся компонент.

В первом разделе приводятся основные определения. Во втором разделе перечисляются все орбиты векторов из E^{15} ($E = \{0,1\}$) при действии группы перестановочных автоморфизмов кода Хемминга H^{15} (теорема 1). Решению задачи классификации способствовали два обстоятельства. Во-первых, был найден жесткий запрет на непересекаемость компонент кода H^{15}. С этого начинается третий раздел (лемма 2). Лемма 2 и теорема 1 дают возможность сразу исключить из рассмотрения значительную часть наборов компонент, содержащих пересекающиеся компоненты. Во-вторых, получен удобный критерий непересекаемости компонент в терминах элементов подкода $H^7 \subset H^{15}$ (леммы 5 и 9), который является усилением признака непересекаемости компонент, полученного в [6]. Благодаря этим обстоятельствам, наборов непересекающихся компонент кода H^{15} остается не так много. Все они перечислены в четвертом разделе. Среди этих наборов особо выделяются $(k \times l)$-разбиения кода H^{15} ($k = 1, 2, 4, 8$), которые при k различных значениях номеров i содержат ровно $l = 16/k$ непересекающихся i-компонент, а также тупиковые наборы из десяти компонент, содержащие по две непересекающиеся i-компоненты, где i пробегает пять значений (тупиковость означает, что такие наборы нельзя пополнить новыми компонентами с сохранением непересекаемости). Код называем $(k \times l)$-*кодом*, если он получается из H^{15} сдвигами по соответствующим координатам некоторых компонент либо одного из $(k \times l)$-разбиений (при $k = 1, 2, 4, 8, l = 16/k$), либо из тупикового набора десяти компонент (при $k = 5$, $l = 2$). В лемме 11 найдены ранги всех $(k \times l)$-кодов. Основным

результатом является теорема 2, в которой утверждается, что любой совершенный код, получаемый из кода Хемминга H^{15} сдвигами по соответствующим координатам некоторого семейства его непересекающихся компонент, является $(k \times l)$-кодом при некотором $k = 1, 2, 4, 5, 8$ ($l = 16/k$ при $k = 1, 2, 4, 8$ и $l = 2$ при $k = 5$). Число $(k \times l)$-кодов, получаемых из кода H^{15}, равно 131224492.

Автор благодарит Ф. И. Соловьеву и С. В. Августиновича за многочисленные обсуждения, А. М. Романова, заинтересовавшего автора совершенными кодами, А. Д. Коршунова и А. А. Евдокимова за замечания, которые позволили значительно повысить качество оформления работы.

1. Обозначения и основные определения

Пусть E^n — векторное пространство размерности n над полем Галуа $GF(2)$. Сумму векторов $\mathbf{u}, \mathbf{v} \in E^n$ обозначим $\mathbf{u} \oplus \mathbf{v}$. Базисный вектор, в котором i-я координата равна единице, обозначим через $\mathbf{e}_i$, а нулевой и единичный векторы — через $\mathbf{0}$ и $\mathbf{1}$. Для вектора $\mathbf{u} \in E^n$ множество его ненулевых координат будем называть *носителем* этого вектора и обозначать через $[\mathbf{u}]$. Количество элементов в $[\mathbf{u}]$ называем *весом* вектора $\mathbf{u}$. Пусть $n = 2^k - 1$, $k \in \mathbf{N}$. Множество $C \subseteq E^n$ называется *совершенным кодом* длины n с расстоянием 3, если C состоит из 2^{n-k} векторов и расстояние Хемминга между любыми двумя векторами из C не меньше 3. *Рангом* совершенного кода C называется наименьшая размерность подпространств $L \subseteq E^n$ таких, что $C \subseteq L \oplus \mathbf{u}$ при некотором $\mathbf{u} \in E^n$. Совершенный код, являющийся подпространством в E^n, называется кодом Хемминга. Рассмотрим следующее представление кода Хемминга. Каждому $i = 0, \ldots, n$ поставим в соответствие вектор $(i_1, \ldots, i_k) \in E^k$, представляющий число i в двоичной системе счисления. Для $n = 15$ и $k = 4$ это представление имеет следующий вид (табл. 1):

Таблица 1

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
i_1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
i_2	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
i_3	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
i_4	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Рассмотрим множество H^n, состоящее из всех векторов $\mathbf{u} \in E^n$ таких, что $\bigoplus\{i \mid i \in [\mathbf{u}]\} = 0$. Известно, что H^n является кодом Хемминга и любой код Хемминга длины n получается из кода H^n некоторой перестановкой координат всех его векторов. Для вектора $\mathbf{u}$ веса 3 из кода H^n

множество $[\mathbf{u}]$ называем *кодовой тройкой.* Аналогично определяются *кодовые четверки, пятерки* и т. д.

Сдвигом множества $S \subseteq E^n$ по координате i называем множество $S \oplus \mathbf{e}_i$. Подмножество S в совершенном коде C называется *i-компонентой* этого кода, если множество $C' = (C \setminus S) \cup (S \oplus \mathbf{e}_i)$ является совершенным кодом. Если $S_1, \ldots, S_m$ — непересекающиеся подмножества кода C такие, что S_p является i_p-компонентой кода C для каждого $p = 1, \ldots, m$, то множество

$$C' = \left(C \setminus \bigcup_{p=1}^{m} S_p \right) \cup \left(\bigcup_{p=1}^{m} (S_p \oplus \mathbf{e}_{i_p}) \right)$$

является совершенным кодом [2, 6]. В коде Хемминга H^n рассмотрим подпространство R_i, порожденное всеми векторами $\mathbf{u}$ веса 3 с i-й координатой, равной единице. Всевозможные классы смежности вида $R_i^{\mathbf{u}} = R_i \oplus \mathbf{u}$ $(\mathbf{u} \in H^n)$ представляют собой совокупность всех *минимальных* по мощности i-компонент кода Хемминга H^n, $i = 1, \ldots, n$.

Пусть S^n — группа всех перестановок на множестве $\{1, \ldots, n\}$ и пусть символом e обозначена тождественная перестановка. Для $\pi \in S^n$ и $\mathbf{u} = u_1 \ldots u_n \in E^n$ полагаем $\pi(\mathbf{u}) = u_{\pi^{-1}(1)} \ldots u_{\pi^{-1}(n)}$. Пусть $\mathrm{Aut}(E^n)$ — группа всех автоморфизмов пространства E^n, т. е. группа всех отображений $A_\pi^{\mathbf{v}} : E^n \to E^n$ вида $A_\pi^{\mathbf{v}}(\mathbf{u}) = \pi(\mathbf{u}) \oplus \mathbf{v}$ $(\mathbf{u} \in E^n)$ для некоторых $\pi \in S^n$, $\mathbf{v} \in E^n$. Обозначим через $\mathrm{Aut}(C)$ группу автоморфизмов совершенного кода C. В $\mathrm{Aut}(C)$ рассматриваются также две подгруппы: группа перестановочных автоморфизмов $\mathrm{Sym}(C) = \{A_\pi^{\mathbf{0}} \mid \pi(C) = C\}$ и ядро кода $\mathrm{Ker}(C) = \{A_e^{\mathbf{v}} \mid C \oplus \mathbf{v} = C\}$. Для кода H^n группа $\mathrm{Aut}(H^n)$ является полупрямым произведением группы $\mathrm{Sym}(H^n)$ и группы $\mathrm{Ker}(H^n)$, изоморфной коду H^n. Группа $\mathrm{Sym}(H^n)$ изоморфна группе $GL_k(2)$ всех невырожденных квадратных матриц порядка k над полем $GF(2)$, $k = \log(n+1)$*). При этом изоморфизме каждой матрице $A \in GL_k(2)$ ставится в соответствие элемент $A_\pi^{\mathbf{0}} \in \mathrm{Sym}(H^n)$ такой, что перестановка π удовлетворяет соотношению $Ai^t = \pi(i)^t$, $i = 1, \ldots, n$ (символ t означает транспонирование вектора $i = (i_1, \ldots, i_k) \in E^k$). Пространство $E^k \setminus \{0\} = \{1, \ldots, n\}$ можно также рассматривать как конечную $(k-1)$-мерную проективную геометрию $PG_{k-1}(2)$, а группу $GL_k(2)$ — как группу всех проективных преобразований в этой геометрии.

2. Орбиты векторов в E^{15} относительно группы перестановок $\mathrm{Sym}(H^{15})$

В пространстве E^n введем следующее отношение эквивалентности. Будем говорить, что элементы $\mathbf{u}, \mathbf{v} \in E^n$ находятся на одной орбите, если

*) Всюду log обозначает логарифм по основанию 2.

существует перестановка π из группы $\mathrm{Sym}(H^n)$ такая, что $\pi(\mathbf{u}) = \mathbf{v}$. Наша задача состоит в том, чтобы выбрать по одному представителю из каждой орбиты и найти длины всех орбит. Решим эту задачу для кода H^{15}. Это позволит далее сразу исключить из рассмотрения большую часть наборов компонент кода H^{15}, содержащих пересекающиеся компоненты. Для удобства вместо векторов $\mathbf{u} \in E^n$ будем рассматривать их носители $[\mathbf{u}]$, являющиеся подмножествами из $\{1, 2, \ldots, n\}$. Потребуется следующая вспомогательная

Лемма 1. *Пусть (b_{ij}) — матрица размера $m \times k$ над полем $GF(2)$ с попарно различными строками. Различные подмножества $\{j_1, \ldots, j_m\}$ из $\{1, \ldots, n\}$ $(n = 2^k - 1)$ такие, что $j_p = \bigoplus\{i_q \mid b_{pq} = 1\}$, $p = 1, \ldots, m$, составляют одну орбиту, если $\{i_1, \ldots, i_k\}$ пробегает всевозможные линейно независимые наборы векторов из E^k.*

Доказательство. Так как $\{i_1, \ldots, i_k\}$ — независимый набор, а строки матрицы (b_{ij}) различны, то среди элементов $j_1, \ldots, j_m$ нет совпадающих. Допустим что подмножество $\{j_1, \ldots, j_m\}$ получено из независимого набора $\{i_1, \ldots, i_k\}$, а подмножество $\{j'_1, \ldots, j'_m\}$ получено из другого независимого набора $\{i'_1, \ldots, i'_k\}$. Существует невырожденная матрица $A \in GL_k(2)$, преобразующая первый независимый набор во второй. Соответствующая ей при изоморфизме групп $\mathrm{Sym}(H^n)$ и $GL_k(2)$ перестановка π будет переводить $\{j_1, \ldots, j_m\}$ в $\{j'_1, \ldots, j'_m\}$. Лемма доказана.

Теорема 1. *Пространство E^{15} под действием группы $\mathrm{Sym}(H^{15})$ разбивается на 46 орбит O_0^1, O_1^1, O_{14}^1, O_{15}^1, O_m^l, $1 \leqslant m \leqslant 13$, $1 < l < \min(m, 15 - m)$, которые перечислены в табл. 2 вместе с их представителями и длинами.*

Доказательство. Очевидно, что вектор $\mathbf{u} = \mathbf{0}$ образует одноэлементную орбиту O_0^1. Кроме того, все векторы веса 1 и веса 2 образуют по одной орбите O_1^1 и O_2^1 в силу того, что группа $\mathrm{Sym}(H^{15})$ дважды транзитивна. Понятно, что если веса векторов $\mathbf{u}$ и $\mathbf{v}$ различны, то $\mathbf{u}$ и $\mathbf{v}$ находятся в разных орбитах. Поэтому мы будем классифицировать орбиты по весам их представителей (или, как еще говорят, по слоям куба E^{15}).

Орбиты веса 3. Тройки бывают двух типов, кодовые и некодовые. Хорошо известно, что для $n = 15$ имеется 35 кодовых троек (составляющих систему троек Штейнера) и все они переводятся друг в друга автоморфизмами кода H^{15}. На геометрическом языке кодовые тройки интерпретируются как прямые в проективной геометрии $PG_3(2)$. Обозначим орбиту этих троек через O_3^1.

Таблица 2

O_m^l	Представитель	$\lvert O_m^l\rvert$	O_m^l	Представитель	$\lvert O_m^l\rvert$
O_0^1	000000000000000	1	O_{15}^1	111111111111111	1
O_1^1	100000000000000	15	O_{14}^1	011111111111111	15
O_2^1	110000000000000	105	O_{13}^1	001111111111111	105
O_3^1	111000000000000	35	O_{12}^1	000111111111111	35
O_3^2	110100000000000	420	O_{12}^2	001011111111111	420
O_4^1	110011000000000	105	O_{11}^1	001100111111111	105
O_4^2	110100010000000	840	O_{11}^2	001011101111111	840
O_4^3	111100000000000	420	O_{11}^3	000011111111111	420
O_5^1	110100010000001	168	O_{10}^1	001011101111110	168
O_5^2	110100110000000	840	O_{10}^2	001011001111111	840
O_5^3	111100100000000	315	O_{10}^3	000011011111111	315
O_5^4	111100010000000	1680	O_{10}^4	000011101111111	1680
O_6^1	111100010001000	280	O_9^1	000011101110111	280
O_6^2	110100110010000	420	O_9^2	000011001101111	420
O_6^3	111111000000000	105	O_9^3	000000111111111	105
O_6^4	111100010000001	1680	O_9^4	000011101111110	1680
O_6^5	111110010000000	2520	O_9^5	000001101111111	2520
O_7^1	111111100000000	15	O_8^1	000000011111111	15
O_7^2	111110011000000	420	O_8^2	000001100111111	420
O_7^3	000000001111111	120	O_8^3	111111110000000	120
O_7^4	111111010000000	840	O_8^4	000000101111111	840
O_7^5	110101110100000	2520	O_8^5	001010001011111	2520
O_7^6	110100111000010	2520	O_8^6	001011000111101	2520

Для некодовой тройки $[\mathbf{u}] = \{i_1, i_2, i_3\}$ ($\mathbf{u} \in E^{15}$) векторы i_1,i_2,i_3 будут линейно независимы в E^4. Следовательно, все такие тройки переводятся друг в друга автоморфизмами и составляют одну некодовую орбиту O_3^2. Легко также показать, что число независимых троек из E^4 равно 420.

Орбиты веса 4. Начнем с кодовой четверки $[\mathbf{u}] = \{i_1, i_2, i_3, i_4\}$, $\mathbf{u} \in H^{15}$. Из определения кода Хемминга следует, что должно выполняться равенство $i_4 = i_1 \oplus i_2 \oplus i_3$. Следовательно, тройка $\{i_1, i_2, i_3\}$ независима и по лемме 1 множество векторов из O_4^1, носители которых являются кодовыми четверками, образует одну орбиту. На геометрическом языке кодовая четверка — это симметрическая разность двух пересекающихся прямых (кодовых троек). Так как такая четверка

однозначно определяется по любой содержащейся в ней независимой тройке, то $|O_4^1| = 420/4 = 105$.

Некодовые четверки могут быть двух типов. Во-первых, это множество независимых четверок. По определению $\mathbf{u} \in O_4^2$, если $[\mathbf{u}] = \{i_1, i_2, i_3, i_4\}$ для некоторой независимой четверки векторов i_1, i_2, i_3, i_4. Длина орбиты O_4^2 равна $15 \cdot 14 \cdot 12 \cdot 8/4! = 840$.

Во-вторых, есть еще четверки, содержащие кодовые тройки. Множество O_4^3 можно задать с помощью уравнения $\mathbf{u} \in O_4^3$ тогда и только тогда, когда для некоторой независимой тройки $\{i_1, i_2, i_3\}$ выполняется равенство $[\mathbf{u}] = \{i_1, i_2, i_3, i_4\}$, где $i_4 = i_2 \oplus i_3$. На геометрическом языке каждая такая четверка есть объединение прямой и не лежащей на ней точки. По лемме 1 они образуют одну орбиту длины $35 \cdot (15 - 3) = 420$. Так как $|O_4^1| + |O_4^2| + |O_4^3| = \binom{15}{3}$, то множество всех векторов веса 4 исчерпано.

Орбиты веса 5. Начнем с орбиты O_5^1, представляющей кодовые пятерки. Если $\mathbf{u} \in O_5^1$, то $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5\}$, где $i_5 = i_1 \oplus i_2 \oplus i_3 \oplus i_4$. Любая четверка векторов, выбранная из пятерки $\{i_1, i_2, i_3, i_4, i_5\}$, является линейно независимой. По лемме 1 множество O_5^1 составляет одну орбиту. Ее длина равна $840/5 = 168$. Геометрически кодовая пятерка представляется симметрической разностью трех прямых (кодовых троек), среди которых есть только одна пара непересекающихся прямых.

Среди орбит некодовых векторов есть орбита O_5^2, элементы которой представляются объединением кодовой четверки и точки, не лежащей в плоскости, проходящей через эту четверку. Такую орбиту можно задать одним уравнением. Если $\mathbf{u} \in O_5^2$ и $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5\}$, то набор векторов $\{i_1, i_2, i_3, i_4\}$ можно считать линейно независимым, а $i_5 = i_1 \oplus i_2 \oplus i_3$. Для подсчета длины этой орбиты нужно знать, что число плоскостей в геометрии $PG_3(2)$ равно 15, а также следует вспомнить, что число кодовых четверок в плоскости Фано равно 7. Кроме этого, плоскость Фано состоит из семи точек. Следовательно, $|O_5^2| = 15 \cdot 7 \cdot (15 - 7) = 840$.

Следующая орбита — O_5^3. Ее элементы представляются объединениями двух пересекающихся прямых (или кодовых троек). Она также задается с помощью уравнений. Если $\mathbf{u} \in O_5^3$ и $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5\}$, то можно считать, что $i_4 = i_1 \oplus i_2$ и $i_5 = i_1 \oplus i_2 \oplus i_3$. Число пересекающихся кодовых троек легко считается, оно равно 315.

Наконец, последнюю орбиту O_5^4 можно задать следующим уравнением. Вектор $\mathbf{u}$ принадлежит O_5^4 тогда и только тогда, когда $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5\}$, где набор $\{i_1, i_2, i_3, i_4\}$ линейно независим, а $i_5 = i_1 \oplus i_2$. Следовательно, каждая такая пятерка содержит ровно одну кодовую тройку. Теперь легко найти длину орбиты. Для построения пятерки

надо взять любую из 35 кодовых троек, добавить к ней один из 12 не принадлежащих ей элементов, а затем добавить еще один элемент так, чтобы не получилась пятерка из орбиты O_5^3. Для этого необходимо, чтобы этот последний элемент i_4 не совпал ни с одним элементом вида $i_1 \oplus i_3$, $i_2 \oplus i_3$, $i_5 \oplus i_3$. Таким образом, для выбора последнего элемента остается 8 вариантов. Это означает, что $|O_5^4| = 35 \cdot 12 \cdot 8/2 = 1680$ (деление на 2 соответствует тому, что два последних элемента можно поменять ролями). Так как $|O_5^1| + |O_5^2| + |O_5^3| + |O_5^4| = \binom{15}{5}$, то найдены все орбиты веса 5.

Орбиты веса 6. Элементы кодовой орбиты O_6^1 представляются объединениями непересекающихся пар кодовых троек. Если $\mathbf{u} \in O_6^1$ и $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5, i_6\}$, то можно считать, что $i_5 = i_1 \oplus i_2$ и $i_6 = i_3 \oplus i_4$, где набор векторов $\{i_1, i_2, i_3, i_4\}$ является линейно независимым. Число неупорядоченных пар непересекающихся прямых равно 280.

Элементы следующей орбиты O_6^2 представляются объединениями трех некомпланарных прямых с выкинутой их точкой пересечения. Ее можно задать двумя уравнениями. Пусть $\mathbf{u} \in O_6^2$ и $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5, i_6\}$. Тогда $i_5 = i_1 \oplus i_2 \oplus i_3$ и $i_6 = i_2 \oplus i_3 \oplus i_4$. Как и в предыдущем случае, легко считается число неупорядоченных троек некомпланарных прямых, имеющих общую точку пересечения; это число равно 420.

Элементы орбиты O_6^3 можно охарактеризовать как плоскости Фано без одной точки, т. е. $\mathbf{u} \in O_6^3$ тогда и только тогда, когда $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5, i_6\}$, где тройка векторов $\{i_1, i_2, i_3\}$ линейно независима и $i_4 = i_1 \oplus i_2$, $i_5 = i_1 \oplus i_3$, $i_6 = i_2 \oplus i_3$. Как легко видеть, $|O_6^3| = 105$.

Элементы орбиты O_6^4 можно задать как объединение прямой и таких трех точек, не лежащих на этой прямой, что никакая плоскость, проходящая через любую пару этих точек, не содержит данную прямую. В уравнениях эта комбинация выглядит так. Пусть $\mathbf{u} \in O_6^4$ и $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5, i_6\}$. Тогда можно считать, что $i_5 = i_1 \oplus i_2 \oplus i_3$ и $i_6 = i_1 \oplus i_2 \oplus i_3 \oplus i_4$, где четверка $\{i_1, i_2, i_3, i_4\}$ линейно независима. Нам осталось только определить длину орбиты. Для построения элемента такой орбиты нужно взять любую из 35 прямых, добавить любую из 12 точек, не лежащих на выбранной прямой, затем добавить еще одну из 8 точек, которая не лежит в плоскости, проходящей через прямую и уже выбранную точку, и наконец, добавить одну из 3 точек, которая не лежит в плоскостях, проходящих через прямую и уже выбранные точки, и не лежит на прямой, проходящей через выбранные ранее две точки. В результате получаем $|O_6^4| = 35 \cdot 12 \cdot 8 \cdot 3/6 = 1680$.

Элементы последней орбиты O_6^5 можно задать как объединения двух пересекающихся прямых и точки, не лежащей в плоскости этих прямых. Чтобы задать элемент $\mathbf{u} \in O_6^5$, $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5, i_6\}$ уравнениями,

нужно взять независимую четверку $\{i_1, i_2, i_3, i_4\}$ и положить $i_5 = i_1 \oplus i_2$, $i_6 = i_1 \oplus i_3$. Длина такой орбиты считается просто: $|O_6^5| = 15 \cdot C_7^2 \cdot (15-7) = 2520$. Так как $|O_6^1| + |O_6^2| + |O_6^1| + |O_6^3| + |O_6^4| + |O_6^5| = \binom{15}{6}$, то все орбиты веса 6 перечислены.

Орбиты веса 7. Имеются две различные кодовые орбиты веса 7. В первую орбиту O_7^1 входят элементы, которые являются плоскостями Фано. Число таких элементов равно 15.

Во вторую кодовую орбиту O_7^2 входят элементы, которые можно задать в виде объединения трех некомпланарных прямых, имеющих общую точку пересечения. Уравнения, задающие эту орбиту, имеют следующий вид. Для четверки независимых векторов $\{i_1, i_2, i_3, i_4\}$ рассмотрим векторы $i_5 = i_1 \oplus i_2$, $i_6 = i_1 \oplus i_3$ и $i_7 = i_1 \oplus i_4$. В этом случае вектор $\mathbf{u}$ такой, что $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5, i_6, i_7\}$, попадает в орбиту O_7^1. Не представляет труда найти число троек некомпланарных прямых в геометрии $PG_3(2)$, имеющих общую точку пересечения; в результате получаем $|O_7^2| = 420$.

Пусть каждый элемент орбиты O_7^3 задается подмножеством, которое не пересекается с некоторой плоскостью Фано. Так как все плоскости переводятся друг в друга автоморфизмами, то достаточно проверить, переводятся ли друг в друга автоморфизмами все семиэлементные подмножества из дополнения к одной конкретной плоскости, например содержащей базисный набор $\{1, 2, 4\}$. Если i_1 и i_2 — два вектора, не принадлежащие этой плоскости, то существует преобразование из $GL_4(2)$, переводящее линейно независимый набор $\{1, 2, 4, i_1\}$ в набор $\{1, 2, 4, i_2\}$; при этом плоскость остается неподвижной, а i_1 переходит в i_2. Следовательно, множество O_7^3 образует одну орбиту длины $15 \cdot 8 = 120$.

Следующую орбиту O_7^4 определим как совокупность векторов, которые представляются в виде объединения плоскости с выколотой точкой и точки, не лежащей в этой плоскости. Чтобы получить уравнения для этой орбиты, рассмотрим любой линейно независимый набор $\{i_1, i_2, i_3, i_4\}$, добавим к нему три вектора $i_5 = i_1 \oplus i_2$, $i_6 = i_2 \oplus i_3$, $i_7 = i_1 \oplus i_3$ и скажем, что множество $\{i_1, \ldots, i_7\}$ представляет элемент орбиты O_7^4. Очевидно, что длина этой орбиты равна $15 \cdot 7 \cdot 8 = 840$.

Элементы орбиты O_7^5 представляются как объединение трех некомпланарных прямых $\{i_1, i_5, i_6\}$, $\{i_2, i_3, i_5\}$ и $\{i_2, i_4, i_7\}$. Уравнения, задающие такое объединение, имеют следующий вид: $i_5 = i_2 \oplus i_3$, $i_6 = i_1 \oplus i_2 \oplus i_3$, $i_7 = i_2 \oplus i_4$, где четверка векторов $\{i_1, i_2, i_3, i_4\}$ линейно независима. Полученное таким образом множество $\{i_1, \ldots, i_7\}$ содержит только три приведенные выше прямые. Среди них только одна прямая $\{i_2, i_3, i_5\}$ пересекается с двумя другими. Это позволяет определить длину орбиты O_7^5. Для нахождения элемента из этой орбиты следует взять любую из 35 прямых, затем выбрать на ней пару точек, далее через одну точку этой

пары провести одну из 6 прямых, отличную от уже выбранной прямой, и наконец, через другую точку выбранной пары провести одну из 4 прямых, не лежащих в плоскости, проходящей через две выбранные прямые. Всего получим $35 \cdot 3 \cdot 6 \cdot 4 = 2520$ вариантов.

Элементы последней орбиты O_7^6 геометрически можно задать следующим образом. К объединению двух пересекающихся прямых $\{i_1, i_4, i_7\}$, $\{i_5, i_6, i_7\}$ добавим две точки, не лежащие в плоскости, проходящей через эти две прямые, причем прямая, проходящая через добавленные точки, не должна пересекаться с выбранными прямыми. Такой элемент задается следующими уравнениями: $i_5 = i_1 \oplus i_2 \oplus i_3$, $i_6 = i_2 \oplus i_3 \oplus i_4$, $i_7 = i_1 \oplus i_4$, где четверка $\{i_1, i_2, i_3, i_4\}$ линейно независима. Легко заметить, что множество $\{i_1, \ldots, i_7\}$ содержит только две приведенные выше прямые. После этого легко определить длину орбиты. Оказывается, что $|O_7^6| = 2520$. Эта орбита не может совпасть с O_7^5, так как каждый ее представитель содержит по две прямые, а представители орбиты O_7^5 содержат по три прямые. Так как $|O_7^1| + |O_7^2| + |O_7^3| + |O_7^4| + |O_7^5| + |O_7^6| = \mathrm{C}_{15}^7$, то все орбиты веса 7 перечислены.

Если вес $m > 7$, то $\mathbf{u} \in O_m^l$ тогда и только тогда, когда существует вектор $\mathbf{v} \in O_{15-m}^l$ такой, что $[\mathbf{u}] = [\mathbf{1}] \setminus [\mathbf{v}]$. Поэтому мы можем выписать все характеристики орбит веса больше 7 (см. табл. 2). Теорема доказана.

3. Непересекающиеся компоненты кода H^n

Рассмотрим следующую конструкцию кодов. Сначала в коде Хемминга H^n выделяется некоторое семейство $\left\{R_{i_1}^{\mathbf{u}_1}, \ldots, R_{i_m}^{\mathbf{u}_m}\right\}$, состоящее из попарно непересекающихся i_q-компонент, где $\mathbf{u}_q \in H^n$, $q = 1, \ldots, m$. Затем строится совершенный код C путем сдвига в H^n каждой компоненты $R_{i_q}^{\mathbf{u}_q}$ на вектор $\mathbf{e}_{i_q}$, $q = 1, \ldots, m$. Первая задача состоит в том, чтобы охарактеризовать все наборы из попарно непересекающихся компонент кода H^n.

Лемма 2. *Если тройка $\{i, j, k\}$ является кодовой в H^{15}, то для любых векторов $\mathbf{u}, \mathbf{v}, \mathbf{w} \in H^{15}$ среди компонент $R_i^{\mathbf{u}}$, $R_j^{\mathbf{v}}$, $R_k^{\mathbf{w}}$ найдутся две с непустым пересечением.*

Доказательство. В [2] доказано, что при $i \neq j$ размерность суммы $R_i \oplus R_j$ равна $(3n-5)/4$. В частности, при $n = 15$ имеем $|R_i \oplus R_j| = 2^{10}$, т. е. размерность пространства $R_i \oplus R_j$ на единицу меньше размерности кода H^{15}. Если компоненты $R_i^{\mathbf{u}}$ и $R_j^{\mathbf{v}}$ не пересекаются, то это означает, что $\mathbf{u} \oplus \mathbf{v} \notin R_i \oplus R_j$. Аналогично $\mathbf{v} \oplus \mathbf{w} \notin R_j \oplus R_k$ и $\mathbf{u} \oplus \mathbf{w} \notin R_i \oplus R_k$. В [2] были доказаны равенства $R_i \oplus R_j = R_j \oplus R_k = R_i \oplus R_k$. Так как в коде H^{15} имеется только два класса смежности по подпространству $R_i \oplus R_j$, то среди векторов $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$ по крайней мере два попадут в один и тот же класс смежности. Пусть это будут, например, векторы $\mathbf{v}$ и $\mathbf{w}$. Тогда

$\mathbf{v} \oplus \mathbf{w} \in R_i \oplus R_j = R_j \oplus R_k$, что противоречит сделанному предположению. Лемма доказана.

Лемма 2 дает жесткий запрет на непересекаемость компонент, поскольку в H^{15} не существует, например, набора попарно непересекающихся i-компонент $R_i^{\mathbf{u}_i}$ при $i = 1, \ldots, 15$, в то время как это не так для H^n при $n > 15$ [1, 15].

Из леммы 2 следует, что наборы различных координат $\{i_1, \ldots, i_m\}$, для которых существуют попарно непересекающиеся i_q-компоненты при $q = 1, \ldots, m$, не должны содержать кодовых троек. Пользуясь теоремой 1, теперь мы можем охарактеризовать все такие наборы.

Лемма 3. *Любое множество координат* $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, 15\}$ *при* $m \geqslant 9$ *содержит хотя бы одну кодовую тройку. Не содержат кодовых троек только множества, представляющие векторы из орбит* O_0^1, O_1^1, O_2^1, O_3^2, O_4^1, O_4^2, O_5^1, O_5^2, O_6^2, O_7^3, O_8^1.

Доказательство. Для веса $m \leqslant 7$ список орбит, не содержащих кодовые тройки, составляется исходя из их описания, приведенного в доказательстве теоремы 1. При $m = 8$ это можно установить непосредственной проверкой. Действительно, представляющие множества векторов из орбиты O_8^3 содержат плоскости Фано, в каждой из которых содержится 7 кодовых троек. Представляющие множества $[\mathbf{u}]$ векторов $\mathbf{u}$ из орбит O_8^2, O_8^4, O_8^5, O_8^6 содержат соответственно кодовые тройки $\{6, 10, 12\}$, $\{7, 11, 12\}$, $\{5, 9, 12\}$, $\{6, 10, 12\}$ (см. табл. 2). Аналогично убеждаемся в том, что во всех пяти представителях орбит веса 9 содержатся кодовые тройки. Лемма 3 доказана.

Оказалось, что во всех не запрещенных леммой 2 случаях существуют наборы непересекающихся компонент, а значит, существуют нелинейные коды, которые получаются сдвигами этих компонент по соответствующим координатам. Теперь рассматриваемая задача состоит в том, чтобы найти алгоритм построения всех таких кодов. Для этого докажем ряд лемм, из них некоторые справедливы для кодов Хемминга H^n любой длины $n \geqslant 15$.

В коде H^n рассмотрим вектор $\mathbf{h}$ такой, что носитель $[\mathbf{h}]$ есть $(k-2)$-мерная плоскость в $PG_{k-1}(2)$. Поэтому $[\mathbf{h}]$ состоит из $m = (n-1)/2$ элементов и все такие множества образуют одну орбиту O_m^1 длины n относительно группы $\mathrm{Sym}(H^n)$. Обозначим через $H^m(\mathbf{h})$ множество всех векторов $\mathbf{u} \in H^n$ таких, что $[\mathbf{u}] \subseteq [\mathbf{h}]$. Очевидно, что $H^m(\mathbf{h})$ образует в H^n подкод Хемминга предыдущей размерности.

Из конструкции Васильева [3] следует, в частности, что код Хемминга H^n можно разложить в прямую сумму двух подпространств, одно из которых является компонентой, а другое — подкодом предыдущей размерности, лежащим в некоторой грани куба E^n размерности $(n-1)/2$.

Здесь этот факт удобно будет сформулировать в виде следующей леммы.

Лемма 4. *Для любого $i \notin [\mathbf{h}]$ и для любой i-компоненты $R_i^{\mathbf{u}}$ ($\mathbf{u} \in H^n$) пересечение $R_i^{\mathbf{u}} \cap H^m(\mathbf{h})$ состоит из одного элемента.*

Доказательство. Пусть $\mathbf{v}, \mathbf{w} \in R_i^{\mathbf{u}} \cap H^m(\mathbf{h})$, $\mathbf{v} \neq \mathbf{w}$. Тогда $\mathbf{v} \oplus \mathbf{w} \in R_i \cap H^m(\mathbf{h})$. Пусть $j \in [\mathbf{v} \oplus \mathbf{w}]$. Так как $j \in [\mathbf{h}]$, то $k \notin [\mathbf{h}]$, где $k = i \oplus j$. Следовательно, $k \notin [\mathbf{v} \oplus \mathbf{w}]$, а это противоречит определению подпространства R_i. Значит, множество $R_i^{\mathbf{u}} \cap H^m(\mathbf{h})$ содержит не более одного элемента. С другой стороны, весь код H^n разбивается на $2^{m-\log(n+1)+1}$ классов смежности по подпространству R_i [2] и каждый элемент кода $H^m(\mathbf{h})$ должен попасть в какой-то из этих классов. Это означает, что каждый класс смежности содержит ровно по одному элементу из кода $H^m(\mathbf{h})$. Лемма доказана.

Вектор $\mathbf{v} \in R_i^{\mathbf{u}} \cap H^m(\mathbf{h})$ далее будем называть $H^m(\mathbf{h})$-представителем компоненты $R_i^{\mathbf{u}}$, поскольку $R_i^{\mathbf{v}} \cap H^m(\mathbf{h}) = \{\mathbf{v}\}$. Рассматриваемую задачу теперь можно переформулировать следующим образом. Какие координаты $i_q \notin [\mathbf{h}]$ следует поставить в соответствие векторам $u_q \in H^m(\mathbf{h})$, чтобы все компоненты $R_{i_q}^{\mathbf{u}_q}$ ($q = 1, \ldots, p$) были попарно непересекающимися? Для решения этой задачи важно иметь критерий непересекаемости компонент в терминах координат i_q и $H^m(\mathbf{h})$-представителей $\mathbf{u}_q$. Один достаточный признак непересекаемости компонент для кодов Хемминга любой длины n был получен А. М. Романовым [6]. Как оказалось, для $n = 15$ этот признак является критерием, который формулируется и доказывается в следующей лемме. Теперь элемент $\mathbf{h}$ следует брать из орбиты O_7^1 кода H^{15}.

Лемма 5. *Если $\mathbf{u}, \mathbf{v} \in H^7(\mathbf{h})$ и $i, j \notin [\mathbf{h}]$ ($i \neq j$), то компоненты $R_i^{\mathbf{u}}$ и $R_j^{\mathbf{v}}$ имеют пустое пересечение тогда и только тогда, когда в множестве $[\mathbf{u} \oplus \mathbf{v}] \setminus \{k\}$ содержится нечетное число элементов, где $k = i \oplus j$.*

Доказательство. Достаточность условия непересекаемости компонент доказана в [6] (см. лемму 4). Поэтому проверим только необходимость приведенного выше условия.

Допустим, что множество $[\mathbf{u} \oplus \mathbf{v}] \setminus \{k\}$ состоит из четного числа элементов. Тогда множество $[\mathbf{u} \oplus \mathbf{v}]$ является либо кодовой тройкой, содержащей k, либо кодовой четверкой, не содержащей k, либо кодовой семеркой $[\mathbf{h}]$. Следовательно, вектор $\mathbf{u} \oplus \mathbf{v}$ попадает в k-компоненту $R_k(\mathbf{h}) = R_k \cap H^7(\mathbf{h})$ кода $H^7(\mathbf{h})$. Так как $R_k \subset R_i \oplus R_j$, то $\mathbf{u} \oplus \mathbf{v} \in R_i \oplus R_j$. Это означает, что пересечение $(R_i \oplus \mathbf{u}) \cap (R_j \oplus \mathbf{v})$ непусто. Лемма доказана.

Назовем i-компоненту $R_i^{\mathbf{u}}$ кода H^n *антиподальной* i-компоненте $R_i^{\mathbf{v}}$, если существует вектор $\mathbf{w} \in R_i^{\mathbf{u} \oplus \mathbf{v}} \cap O_m^1$ такой, что $i \notin [\mathbf{w}]$.

Лемма 6. *Если i-компоненты $R_i^{\mathbf{u}}$ и $R_i^{\mathbf{v}}$ антиподальны друг другу, то $R_i^{\mathbf{u}\oplus\mathbf{v}}$ является единственной i-компонентой, содержащей $(n+1)/2$ векторов $\mathbf{w}$ из O_m^1 таких, что $i \notin [\mathbf{w}]$.*

Доказательство. Пусть $\mathbf{w} \in R_i^{\mathbf{u}\oplus\mathbf{v}} \cap O_m^1$ и $i \notin [\mathbf{w}]$. Рассмотрим другой вектор $\mathbf{w}' \in O_m^1$ такой, что $i \notin [\mathbf{w}']$. Необходимо доказать, что $\mathbf{w} \oplus \mathbf{w}' \in R_i$. Это означает, что любая кодовая тройка, содержащая i и пересекающаяся с множеством $[\mathbf{w}]$, будет пересекаться и с множеством $[\mathbf{w}']$. Но это очевидно, так как в проективной геометрии прямая и плоскость всегда пересекаются. Лемма доказана.

Из леммы 6 следует, что существует единственная i-компонента, антиподальная данной i-компоненте.

Будем называть i-компоненту $R_i^{\mathbf{u}}$ *i-четной* (*i-нечетной*), если для любого вектора $\mathbf{u} \in R_i^{\mathbf{u}}$ множество $[\mathbf{u}]\backslash\{i\}$ состоит из четного (нечетного) числа элементов. Факт сохранения i-четности элементов в минимальной i-компоненте любого совершенного кода C отмечался в [8] (лемма 2.1). Для кода H^{15} справедливо следующее утверждение.

Лемма 7. *Среди всех i-нечетных компонент $R_i^{\mathbf{u}}$ кода H^{15} имеется единственная компонента, которая не содержит векторов веса 3. Эта компонента антиподальна компоненте $R_i^{\mathbf{0}} = R_i$. Если две i-компоненты антиподальны друг другу в коде H^{15}, то они антиподальны в любом другом коде Хемминга, содержащем эти компоненты.*

Доказательство. Семь векторов веса 3 с единичной i-й координатой попадают в $R_i^{\mathbf{0}}$. Допустим, что в i-нечетной компоненте $R_i^{\mathbf{u}}$ есть вектор $\mathbf{u}$ веса 3 такой, что $i \notin [\mathbf{u}]$. Проведем через i и $[\mathbf{u}]$ плоскость Фано. В этой плоскости есть только четыре кодовые тройки, не содержащие i. Поэтому четыре вектора, носителями которых являются эти тройки, попадают в $R_i^{\mathbf{u}}$. Следовательно, 28 векторов веса 3 с нулевой i-й координатой находятся в семи i-нечетных компонентах по 4 вектора в каждой компоненте. Одна i-нечетная компонента остается без векторов веса 3, и, как легко видеть, именно эта компонента антиподальна i-компоненте $R_i^{\mathbf{0}}$. Пусть теперь в коде H^{15} даны две антиподальные i-компоненты $R_i^{\mathbf{u}}$ и $R_i^{\mathbf{v}}$. Они будут также i-компонентами в любом другом содержащем их коде [2]. Антиподальность этих компонент в любом содержащем их коде Хемминга следует из того, что $R_i^{\mathbf{u}\oplus\mathbf{v}}$ — единственная i-нечетная компонента без векторов веса 3. Лемма доказана.

Лемма 8. *Если при $i \neq j$ компоненты $R_i^{\mathbf{u}}$ и $R_j^{\mathbf{w}}$ кода H^n не пересекаются и компонента $R_i^{\mathbf{v}}$ антиподальна к $R_i^{\mathbf{u}}$, то компоненты $R_i^{\mathbf{v}}$ и $R_j^{\mathbf{w}}$ не пересекаются.*

Доказательство. В силу антиподальности i-компонент $R_i^{\mathbf{u}}$ и $R_i^{\mathbf{v}}$ можно считать, что вектор $\mathbf{h} = \mathbf{u} \oplus \mathbf{v} \in O_m^1$ и $i, j \notin [\mathbf{h}]$. Кроме того,

векторы $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$ можно выбрать так, чтобы $[\mathbf{u}]$, $[\mathbf{v}]$, $[\mathbf{w}]$ были подмножествами $[\mathbf{h}]$ (заменив их на $H^m(\mathbf{h})$-представители). Непересекаемость компонент $R_i^{\mathbf{u}}$, $R_j^{\mathbf{w}}$ означает, что $\mathbf{u} \oplus \mathbf{w} \notin R_i \oplus R_j$. Так как при $k = i \oplus j$ имеет место включение $R_k \subset R_i \oplus R_j$ [2], то $\mathbf{u} \oplus \mathbf{w} \notin R_k$. Из $\mathbf{h} \in R_k$ следует также, что $\mathbf{v} \oplus \mathbf{w} = \mathbf{h} \oplus \mathbf{u} \oplus \mathbf{w} \notin R_k$. Обозначим $R_k(\mathbf{h}) = R_k \cap H^m(\mathbf{h})$. Для любого $\mathbf{v}' \in H^m(\mathbf{h})$ множество $R_i^{\mathbf{v}'} \cap H^m(\mathbf{h})$ в силу леммы 4 одноэлементное. Поэтому

$$R_i \oplus R_k(\mathbf{h}) = \cup \{R_i \oplus \mathbf{v}' \mid \mathbf{v}' \in R_k(\mathbf{h})\} \subseteq R_i \oplus R_k = R_i \oplus R_j.$$

По формулам из [2] получаем

$$|R_i \oplus R_j| = |R_i| \cdot |R_k(\mathbf{h})| = 2^{\frac{3n-5}{4}}.$$

Следовательно, $(R_i \oplus R_j) \cap H^m(\mathbf{h}) = R_k(\mathbf{h})$. Поэтому $\mathbf{v} \oplus \mathbf{w} \notin R_i \oplus R_j$. Лемма доказана.

Из леммы 8 следует, что достаточно уметь строить семейства непересекающихся i-четных компонент. Добавление компонент, антиподальных компонентам этого семейства, гарантирует непересекаемость всех компонент полученного таким образом набора. В связи с этим нам потребуется следующий критерий непересекаемости трех компонент кода H^{15}, среди которых одна содержит нулевой вектор.

Лемма 9. *Пусть R_i^0, $R_j^{\mathbf{v}}$, $R_k^{\mathbf{w}}$ — три компоненты из кода H^{15} такие, что координаты i, j, k различны и не принадлежат $[\mathbf{h}]$, а векторы $\mathbf{v}, \mathbf{w} \in H^7(\mathbf{h})$ имеют вес 4. Такие компоненты являются попарно непересекающимися тогда и только тогда, когда либо $j' \in [\mathbf{v}] \cap [\mathbf{w}]$ и $k' \in [\mathbf{w}] \setminus [\mathbf{v}]$, либо $k' \in [\mathbf{v}] \cap [\mathbf{w}]$ и $j' \in [\mathbf{v}] \setminus [\mathbf{w}]$, где $j' = i \oplus j$, $k' = i \oplus k$.*

Доказательство леммы 9 легко получается из леммы 5. Поэтому мы его опустим.

4. Перечисление кодов, получаемых из кода H^{15} сдвигами непересекающихся минимальных компонент

Функцию $\phi : H^n \to \{0, 1, \ldots, n\}$ назовем *функцией сдвига* совершенного кода C длины n, если $\mathbf{v} \oplus \mathbf{e}_{\phi(\mathbf{v})} \in C$ для любого вектора $\mathbf{v} \in H^n$, где $\mathbf{e}_0 = 0$ и $\phi(\mathbf{v}) = 0$ означает, что $\mathbf{v} \in C$. Легко заметить, что каждый совершенный код однозначно определяется своей функцией сдвига, причем несовпадающие коды имеют разные функции сдвига [2]. Из этого замечания следует, что совершенные коды, получаемые из одного и того же кода Хемминга сдвигами по соответствующим координатам различных наборов минимальных i-компонент, различны. Следовательно, задача перечисления таких совершенных кодов эквивалентна задаче о нахождении всевозможных наборов непересекающихся минимальных i-компонент кода Хемминга H^n.

Лемма 10. *Любой носитель* $[\mathbf{u}]$ *вектора* $\mathbf{u}$, *который принадлежит одной из орбит* O_4^2, O_5^2, O_6^2, O_7^3, *содержится в носителе* $[\mathbf{v}]$ *единственного вектора* $\mathbf{v}$ *из орбиты* O_8^1. *Любой носитель вектора из орбит* O_3^2, O_4^1 *содержится в носителях ровно двух векторов из орбиты* O_8^1. *Обратно, если носитель вектора* $\mathbf{u}$ *содержит не менее трех элементов и является подмножеством* $[\mathbf{v}]$ $(\mathbf{v} \in O_8^1)$, *то* $\mathbf{u}$ *принадлежит одной из перечисленных выше орбит. Для любого* $\mathbf{u} \in O_5^1$ *и любого* $i \in [\mathbf{u}]$ *имеется единственный вектор* $\mathbf{v} \in O_8^1$ *такой, что* $[\mathbf{u}] \setminus [\mathbf{v}] = \{i\}$.

Доказательство. Если $\mathbf{u} \in O_4^2$, то рассмотрим подмножество $\{8,9,10,12\} \subset \{8,\ldots,15\}$. Оно не лежит в кодовой орбите O_4^1 и не содержит ни одной кодовой тройки. Поэтому $\{8,9,10,12\} = [\mathbf{w}]$, где $\mathbf{w} \in O_4^2$. Следовательно, существует перестановка $\pi \in \mathrm{Sym}(H^{15})$ такая, что $\pi(\mathbf{w}) = \mathbf{u}$. Это означает, что $[\mathbf{u}] \subset \{\pi(8),\ldots,\pi(15)\} = [\mathbf{v}]$. Осталось только убедиться, что множество $\{8,\ldots,15\}$ является носителем вектора из орбиты O_8^1 (см. табл. 2). Оставшиеся утверждения устанавливаются аналогично. Для доказательства единственности множества $[\mathbf{v}]$ рассмотрим пересечение двух различных восьмерок $[\mathbf{v}]$ и $[\mathbf{w}]$, где $\mathbf{v}, \mathbf{w} \in O_8^1$. Оно является дополнением к объединению двух плоскостей Фано $[\mathbf{1} \oplus \mathbf{v}]$ и $[\mathbf{1} \oplus \mathbf{w}]$. Это объединение можно также представить в виде симметрической разности множеств $[\mathbf{1} \oplus \mathbf{v}]$, $[\mathbf{1} \oplus \mathbf{w}]$ и их пересечения, которое является кодовой тройкой $[\mathbf{u}]$, $\mathbf{u} \in O_3^1$. Следовательно, пересечение $[\mathbf{v}] \cap [\mathbf{w}] = [\mathbf{1} \oplus \mathbf{u} \oplus \mathbf{v} \oplus \mathbf{w}]$ будет кодовой четверкой. Таким образом, единственность $[\mathbf{v}]$ для множеств, не являющихся кодовыми четверками, доказана. Кроме этого, мы получили кодовую четверку, являющуюся пересечением носителей двух векторов из O_8^1. Применяя к этой четверке перестановки из $\mathrm{Sym}(H^{15})$, покажем, что таким способом можно получить любую кодовую четверку. В пересечении носителей трех различных векторов из орбиты O_8^1 содержится только два элемента. Поэтому кодовая четверка не может содержаться в носителях трех векторов из O_8^1. Если теперь $[\mathbf{u}]$ — кодовая пятерка и $i \in [\mathbf{u}]$, то множество $[\mathbf{u}] \setminus \{i\}$, которое является некодовой четверкой, не содержащей кодовых троек, содержится, по предыдущему, в носителе единственного вектора из орбиты O_8^1. Лемма доказана.

Легко заметить, что перестановка π из $\mathrm{Sym}(H^{15})$ переводит i-компоненту в $\pi(i)$-компоненту. Поэтому из леммы 10 следует, что достаточно решить задачу о перечислении всех непересекающихся наборов i_q-компонент $\{R_{i_q}^{\mathbf{u}_q} \mid q = 1\ldots,m\}$ только для двух частных случаев, когда либо все $i_q \in \{8,\ldots,15\}$, либо все $i_q \in \{1,8,11,13,15\}$ $(q = 1,\ldots,m)$. При этом можно всегда считать, что $i_1 = 8$. После переноса компонент на подходящий вектор из H^{15} можно еще добиться выполнения равенства $\mathbf{u}_1 = \mathbf{0}$, т. е. $R_{i_1}^{\mathbf{u}_1} = R_8$. Все остальные решения могут быть получены

переносом на вектор из H^{15} с последующей перестановкой координат из группы $\mathrm{Sym}(H^{15})$.

Далее мы даем конструкцию $(k \times l)$-кодов (где $l = 16/k$ при $k = 1, 2, 4, 8$ и $l = 2$ при $k = 5$), которые строятся либо из определяемых ниже $(k \times l)$-разбиений кода H^{15} (при $k = 1, 2, 4, 8$), либо из тупикового набора компонент кода H^{15} (при $k = 5$).

(1×16)-коды. Начнем с кодов Васильева. Этот случай хорошо известен, но мы рассмотрим его для полноты классификации. Считаем, что все $i_q = i$ $(q = 1, \ldots, m,\ m \leqslant 16)$, а наборы векторов $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ пробегают всевозможные подмножества из кода $H^7(\mathbf{h})$, где $\mathbf{h} \in O_7^1$ и $i \notin [\mathbf{h}]$. Коды Васильева получаются из кода Хемминга H^{15} сдвигом на вектор $\mathbf{e}_i$ всех его компонент $R_i^{\mathbf{u}_q}$ $(q = 1, \ldots, m)$, составляющих часть разбиения кода H^{15} на i-компоненты. Имеется 15 различных разбиений кода H^{15} на i-компоненты, $i = 1, \ldots, 15$. Эти разбиения будем также называть (1×16)-*разбиениями*, а коды, получаемые сдвигами i-компонент таких разбиений, — (1×16)-*кодами*.

(2×8)-коды. В этой серии кодов для некоторых $i \neq j$ выполняется либо $i_q = i$, либо $i_q = j$ $(q = 1, \ldots, m;\ m \leqslant 16)$. Такие коды любой длины $n = 2^k - 1$ были построены в [2, 6]. Полагаем $i_1 = i$, $i_2 = j$. Подпространство $R_i \oplus R_j$ можно представить как объединение восьми непересекающихся i-компонент. Объединение всех j-компонент, не пересекающихся с R_i, является классом смежности по подпространству $R_i \oplus R_j$. В результате получаем разбиение кода Хемминга H^{15} на 16 компонент $R_i^{\mathbf{v}_{r,0}}$, $R_j^{\mathbf{v}_{r,1}}$ $(r = 0, \ldots, 7)$, где $\mathbf{v}_{r,s} \in H^7(\mathbf{h})$ $(r = 0, \ldots 7;\ s = 0, 1;\ \mathbf{h} \in O_7^1;\ i, j \notin [\mathbf{h}])$. Известно [6], что если вес вектора $\mathbf{v}_{r,0}$ четный (нечетный), то $i \oplus j \notin [\mathbf{v}_{r,0}]$ $(i \oplus j \in [\mathbf{v}_{r,0}])$. Остальные восемь векторов $\mathbf{v}_{r,1} \in H^7(\mathbf{h})$ имеют противоположную характеристику, т. е. если вес $\mathbf{v}_{r,1}$ четный (нечетный), то $i \oplus j \in [\mathbf{v}_{r,1}]$ $(i \oplus j \notin [\mathbf{v}_{r,1}])$. Если разбить подпространство $R_i \oplus R_j$ на восемь непересекающихся j-компонент и добавить восемь i-компонент, не пересекающихся с R_j, то получим еще одно разбиение кода H^{15} на компоненты $R_j^{\mathbf{v}_{r,0}}$, $R_i^{\mathbf{v}_{r,1}}$ $(r = 0, \ldots, 7)$, являющееся переносом предыдущего разбиения на вектор $\mathbf{w}_1 \notin R_i \oplus R_j$. Такие разбиения кода H^{15} будем называть (2×8)-*разбиениями*, а коды, получаемые сдвигами произвольного числа компонент одного из таких разбиений, — (2×8)-*кодами*. Число (2×8)-разбиений равно $2 \cdot \mathrm{C}_{15}^2 = 210$.

(4×4)-коды. Эта группа кодов характеризуется тем, что $i_q \in [\mathbf{u}]$ для некоторого $\mathbf{u} \in O_4^1$ и всех $q = 1, \ldots, m$ $(m \leqslant 16)$. Можно считать, что $[\mathbf{u}] = \{8, 10, 12, 14\}$ и $[\mathbf{h}] = \{1, \ldots, 7\}$. Из леммы 5 следует, что если для вектора $\mathbf{v} \in H^7(\mathbf{h})$ веса 4 компонента $R_j^{\mathbf{v}}$ не пересекается с компонентой R_8, то $j \oplus 8 \in [\mathbf{v}]$ $(j = 10, 12, 14)$. Только один вектор $\mathbf{v}_{2,0} \in H^7(\mathbf{h})$ веса 4 при каждом $j = 10, 12, 14$ не удовлетворяет условию $j \oplus 8 \in [\mathbf{v}_{2,0}]$, его

носитель $[\mathbf{v}_{2,0}] = \{1,3,5,7\}$. Следовательно, вектор $\mathbf{v}_{2,0}$ можно отнести только к 8-компоненте $R_8^{\mathbf{v}_{2,0}}$. Полагая $\mathbf{v}_{0,0} = \mathbf{0}$ и переходя к антиподальным компонентам, найдем всего четыре вектора $\mathbf{v}_{0,0}, \mathbf{v}_{1,0}, \mathbf{v}_{2,0}, \mathbf{v}_{3,0} \in H^7(\mathbf{h})$ с носителями $[\mathbf{v}_{0,0}] = \varnothing$, $[\mathbf{v}_{1,0}] = \{1,\ldots,7\}$, $[\mathbf{v}_{2,0}] = \{1,3,5,7\}$, $[\mathbf{v}_{3,0}] = \{2,4,6\}$, которые можно отнести только к 8-компонентам $R_8^{\mathbf{v}_{r,0}}$ $(r = 0,1,2,3)$. Кодовую четверку $[\mathbf{v}_{0,1}] = \{2,3,4,5\}$ $(\mathbf{v}_{0,1} \in H^7(\mathbf{h}))$ можно отнести либо к 10-компоненте, либо к 12-компоненте (по леммам 5 и 8 только в этом случае они не пересекаются ни с одной компонентой $R_8^{\mathbf{v}_{r,0}}$ $(r = 0,1,2,3)$).

Сначала отнесем вектор $\mathbf{v}_{0,1}$ к 10-компоненте. Все дальнейшие сопоставления векторов с компонентами осуществляются теперь однозначно. По лемме 9 существуют только две четверки $[\mathbf{v}_{0,2}] = \{4,5,6,7\}$, $[\mathbf{v}_{2,2}] = \{1,3,4,6\}$ $(\mathbf{v}_{0,2}, \mathbf{v}_{2,2} \in H^7(\mathbf{h}))$ такие, что компоненты $R_{12}^{\mathbf{v}_{0,2}}$, $R_{12}^{\mathbf{v}_{2,2}}$ не пересекаются с $R_{10}^{\mathbf{v}_{0,1}}$. Добавляя еще антиподальные компоненты и полагая $[\mathbf{v}_{1,2}] = \{1,2,3\}$, $[\mathbf{v}_{3,2}] = \{2,5,7\}$, мы получаем, что четверку векторов $\mathbf{v}_{r,2}$ $(r = 0,1,2,3)$ можно отнести только к 12-компонентам. Полагая $[\mathbf{v}_{1,1}] = \{1,6,7\}$, $[\mathbf{v}_{2,1}] = \{1,2,4,7\}$, $[\mathbf{v}_{3,1}] = \{3,5,6\}$ и еще раз применяя лемму 9, видим, что четверку векторов $\mathbf{v}_{r,1}$ $(r = 0,1,2,3)$ можно отнести только к 10-компонентам. Для оставшейся четверки векторов из $H^7(\mathbf{h})$ положим $[\mathbf{v}_{0,3}] = \{2,3,6,7\}$, $[\mathbf{v}_{1,3}] = \{1,4,5\}$, $[\mathbf{v}_{2,3}] = \{1,2,5,6\}$, $[\mathbf{v}_{3,3}] = \{3,4,7\}$ и отнесем ее однозначно к 14-компонентам. В результате получим разбиение всего кода Хемминга H^{15} на непересекающиеся компоненты

$$R_{2s+8}^{\mathbf{v}_{r,s}} \quad (r,s = 0,1,2,3). \tag{1}$$

Если теперь вектор $\mathbf{v}_{0,1}$ отнести к 12-компоненте, то таким же образом получается второе разбиение кода Хемминга, которое является переносом разбиения (1) на вектор $\mathbf{w}_1 = 100000011000000 \in R_8$, т. е. это разбиение совпадает с разбиением $R_{2s+8}^{\mathbf{v}_{r,s} \oplus \mathbf{w}_1}$ $(r,s = 0,1,2,3)$. Для проверки этого достаточно заново пересчитать $H^7(\mathbf{h})$-представитель одной компоненты $R_{10}^{\mathbf{v}_{0,1} \oplus \mathbf{w}_1}$. Прибавив к вектору $\mathbf{v}_{0,1} \oplus \mathbf{w}_1$ вектор из компоненты R_{10}, равный 011000011000000, получаем вектор $\mathbf{v}_{1,3} = 100110000000000$ из $H^7(\mathbf{h})$. Это означает, что $R_{10}^{\mathbf{v}_{0,1} \oplus \mathbf{w}_1} = R_{10}^{\mathbf{v}_{1,3}}$, т. е. разбиение, получаемое переносом разбиения (1) на вектор $\mathbf{w}_1$, содержит компоненту $R^{\mathbf{v}_{1,3}}$. Следовательно, оно отличается от разбиения (1). Как было показано выше, других разбиений, содержащих компоненту R_8, быть не может. Положив $\mathbf{w}_0 = \mathbf{0}$, можно задать $H^7(\mathbf{h})$-представители компонент каждого из полученных разбиений с помощью векторов $\mathbf{v}_{r,s}^q$ таких, что $R_{2s+8}^{\mathbf{v}_{r,s}^q} = R_{2s+8}^{\mathbf{v}_{r,s} \oplus \mathbf{w}_q}$ $(q = 0,1;\ r,s = 0,1,2,3)$. Оба разбиения приводятся в табл. 3. Число в верхней строке указывает номер координаты, по которой можно сдвигать компоненту, содержащую один из векторов, носитель которого находится в той же колонке.

Таблица 3

$2s+8=$	8	10	12	14
$[\mathbf{v}^0_{0,s}]=$	$\varnothing$	$\{2,3,4,5\}$	$\{4,5,6,7\}$	$\{2,3,6,7\}$
$[\mathbf{v}^0_{1,s}]=$	$\{1,\ldots,7\}$	$\{1,6,7\}$	$\{1,2,3\}$	$\{1,4,5\}$
$[\mathbf{v}^0_{2,s}]=$	$\{1,3,5,7\}$	$\{1,2,4,7\}$	$\{1,3,4,6\}$	$\{1,2,5,6\}$
$[\mathbf{v}^0_{3,s}]=$	$\{2,4,6\}$	$\{3,5,6\}$	$\{2,5,7\}$	$\{3,4,7\}$
$[\mathbf{v}^1_{0,s}]=$	$\varnothing$	$\{1,4,5\}$	$\{1,6,7\}$	$\{1,2,3\}$
$[\mathbf{v}^1_{1,s}]=$	$\{1,\ldots,7\}$	$\{2,3,6,7\}$	$\{2,3,4,5\}$	$\{4,5,6,7\}$
$[\mathbf{v}^1_{2,s}]=$	$\{1,3,5,7\}$	$\{3,4,7\}$	$\{3,5,6\}$	$\{2,5,7\}$
$[\mathbf{v}^1_{3,s}]=$	$\{2,4,6\}$	$\{1,2,5,6\}$	$\{1,2,4,7\}$	$\{1,3,4,6\}$

Если не требовать, чтобы одна из 8-компонент содержала нулевой вектор, то следует также рассмотреть разбиения кода H^{15}, которые получаются из двух разбиений, приведенных в табл. 3, переносами на векторы из различных классов смежности кода $H^7(\mathbf{h})$ по подпространству $\{\mathbf{v}_{0,0},\mathbf{v}_{1,0},\mathbf{v}_{2,0},\mathbf{v}_{3,0}\}$. В качестве дополняющего это подпространство в $H^7(\mathbf{h})$ можно взять, например, подпространство $P=\{\mathbf{v}_{0,p}\mid p=0,1,2,3\}$. В результате получается восемь различных разбиений кода Хемминга H^{15} на i-компоненты, где $i=8,10,12,14$. Рассмотрим теперь любую четверку $[\mathbf{u}]=\{i_1,i_2,i_3,i_4\}$, где $\mathbf{u}\in O^1_4$. Существует перестановка π из $\mathrm{Sym}(H^{15})$ такая, что $\pi(8)=i_1$, $\pi(10)=i_2$, $\pi(12)=i_3$, $\pi(14)=i_4$. При любых $p=0,1,2,3$ и $q=0,1$ разбиение кода H^{15} вида

$$R^{\pi(\mathbf{v}_{r,s}\oplus\mathbf{v}_{0,p}\oplus\mathbf{w}_q)}_{\pi(2s+8)}\quad(r,s=0,1,2,3)\tag{2}$$

называем (4×4)-*разбиением*, а коды, получаемые сдвигами некоторых компонент одного из разбиений (2), называем (4×4)-*кодами*. Число различных (4×4)-разбиений, очевидно, равно $8\cdot|O^1_4|=840$.

(8×2)-коды. Полагаем $\mathbf{v}_{0,0}=\mathbf{0}$ и отнесем этот вектор к компоненте R_8. Попытаемся теперь все семь векторов веса 4 из $H^7(\mathbf{h})$ отнести к i-компонентам с различными $i=9,\ldots,15$ так, чтобы вместе с R_8 получилось семейство из восьми попарно непересекающихся i-компонент с различными $i=8,\ldots,15$. Пусть $\mathbf{v}_{0,0}=\mathbf{0}$, $[\mathbf{v}_{0,4}]=\{1,3,4,6\}$. По лемме 5 компонента $R_i^{\mathbf{v}_{0,4}}$ не пересекается с R_8 только в случае, когда $i=9,11,12,14$. Следовательно, вектор $\mathbf{v}_{0,4}$ можно отнести четырьмя способами к одной из этих четырех компонент. Сначала отнесем его к 12-компоненте. По лемме 9 для вектора $\mathbf{v}_{0,6}$ с носителем $[\mathbf{v}_{0,6}]=\{2,3,6,7\}$ компонента $R_i^{\mathbf{v}_{0,6}}$ не будет пересекаться с R_8 и $R_9^{\mathbf{v}_{0,4}}$ только при $i=11,14$. Это означает, что вектор $\mathbf{v}_{0,6}$ можно двумя способами отнести к одной из этих компонент. Отнесем его к 14-компоненте. Оставшиеся

сопоставления осуществляются однозначно. Выпишем только результат $[\mathbf{v}_{0,1}] = \{1,2,5,6\}$, $[\mathbf{v}_{0,2}] = \{2,3,4,5\}$, $[\mathbf{v}_{0,3}] = \{1,3,5,7\}$, $[\mathbf{v}_{0,5}] = \{4,5,6,7\}$, $[\mathbf{v}_{0,7}] = \{1,2,4,7\}$. Получившуюся восьмерку попарно непересекающихся компонент дополним антиподальными компонентами, т. е. положим $[\mathbf{v}_{1,0}] = \{1,\dots,7\}$, $[\mathbf{v}_{1,1}] = \{3,4,7\}$, $[\mathbf{v}_{1,2}] = \{1,6,7\}$, $[\mathbf{v}_{1,3}] = \{2,4,6\}$, $[\mathbf{v}_{1,4}] = \{2,5,7\}$, $[\mathbf{v}_{1,5}] = \{1,2,3\}$, $[\mathbf{v}_{1,6}] = \{1,4,5\}$, $[\mathbf{v}_{1,7}] = \{3,5,6\}$. В результате получим разбиение кода H^{15} на компоненты

$$R_{s+8}^{\mathbf{v}_{r,s}} \quad (r = 0,1;\ s = 0,\dots,7). \tag{3}$$

Как видно из этой конструкции, можно получить восемь различных таких разбиений. Эти разбиения можно также получить переносами разбиения (3) на соответствующие векторы из R_8, которые являются представителями различных классов смежности компоненты R_8 по ее подпространству $S = R_8 \cap (R_{12} \oplus \{\mathbf{0},\mathbf{h}\}) \cap (R_{14} \oplus \{\mathbf{0},\mathbf{h}\})$. В данное подпространство входят, прежде всего, четыре вектора из пересечения $R_8 \cap R_{12} \cap R_{14}$, имеющие вид $abababababababa$ $(a,b \in \{0,1\})$. Далее следует найти по одному представителю из трех пересечений

$$R_8 \cap R_{12} \cap (R_{14} \oplus \mathbf{h}),\quad R_8 \cap R_{14} \cap (R_{12} \oplus \mathbf{h}),\quad R_8 \cap (R_{12} \oplus \mathbf{h}) \cap (R_{14} \oplus \mathbf{h}),$$

которые непусты, так как иначе можно получить больше восьми различных разбиений кода H^{15}. Представителями этих пересечений являются векторы 100110011001100, 011110000111100, 111000011110000. Складывая их с предыдущей четверкой векторов, убеждаемся в том, что подпространство S состоит из следующих векторов:

000000000000000, 010101010101010, 101010101010101, 111111111111111,
100110011001100, 110011001100110, 001100110011001, 011001100110011,
011110000111100, 001011010010110, 110100101101001, 100001111000011,
111000011110000, 101101001011010, 010010110100101, 000111100001111.

Положим

$$\mathbf{w}_0 = 000000000000000,\quad \mathbf{w}_1 = 100000011000000,$$
$$\mathbf{w}_2 = 010000010100000,\quad \mathbf{w}_3 = 110000001100000 = \mathbf{w}_1 \oplus \mathbf{w}_2.$$

Эти векторы находятся в $R_8 \setminus S$. Вектор $\mathbf{w}_4 = 000100010001000$ и суммы
$\mathbf{w}_5 = \mathbf{w}_1 \oplus \mathbf{w}_4 = 100100001001000$, $\mathbf{w}_6 = \mathbf{w}_2 \oplus \mathbf{w}_4 = 010100000101000$,
$\mathbf{w}_7 = \mathbf{w}_3 \oplus \mathbf{w}_4 = 110100011101000$
также принадлежат множеству $R_8 \setminus S$. Мы нашли в компоненте R_8 (не единственное) подпространство $Q = \{\mathbf{w}_q \mid q = 0,\dots,7\}$, дополнительное к S, т. е. элементы из Q являются представителями различных классов смежности компоненты R_8 по подпространству S. Теперь можно утверждать, что разбиения $R_{s+8}^{\mathbf{v}_{r,s} \oplus \mathbf{w}_q}$ $(r = 0,1;\ s = 0,\dots,7)$ при

Таблица 4

$s+8=$	8	9	10	11	12	13	14	15
$\mathbf{v}^0_{0,s}=$	$\mathbf{v}_{0,0}$	$\mathbf{v}_{0,1}$	$\mathbf{v}_{0,2}$	$\mathbf{v}_{0,3}$	$\mathbf{v}_{0,4}$	$\mathbf{v}_{0,5}$	$\mathbf{v}_{0,6}$	$\mathbf{v}_{0,7}$
$\mathbf{v}^0_{1,s}=$	$\mathbf{v}_{1,0}$	$\mathbf{v}_{1,1}$	$\mathbf{v}_{1,2}$	$\mathbf{v}_{1,3}$	$\mathbf{v}_{1,4}$	$\mathbf{v}_{1,5}$	$\mathbf{v}_{1,6}$	$\mathbf{v}_{1,7}$
$\mathbf{v}^1_{0,s}=$	$\mathbf{v}_{0,0}$	$\mathbf{v}_{0,1}$	$\mathbf{v}_{1,6}$	$\mathbf{v}_{1,4}$	$\mathbf{v}_{1,7}$	$\mathbf{v}_{1,2}$	$\mathbf{v}_{1,5}$	$\mathbf{v}_{1,3}$
$\mathbf{v}^1_{1,s}=$	$\mathbf{v}_{1,0}$	$\mathbf{v}_{1,1}$	$\mathbf{v}_{0,6}$	$\mathbf{v}_{0,4}$	$\mathbf{v}_{0,7}$	$\mathbf{v}_{0,2}$	$\mathbf{v}_{0,5}$	$\mathbf{v}_{0,3}$
$\mathbf{v}^2_{0,s}=$	$\mathbf{v}_{0,0}$	$\mathbf{v}_{1,7}$	$\mathbf{v}_{0,2}$	$\mathbf{v}_{1,4}$	$\mathbf{v}_{1,5}$	$\mathbf{v}_{1,3}$	$\mathbf{v}_{1,1}$	$\mathbf{v}_{1,6}$
$\mathbf{v}^2_{1,s}=$	$\mathbf{v}_{1,0}$	$\mathbf{v}_{0,7}$	$\mathbf{v}_{1,2}$	$\mathbf{v}_{0,4}$	$\mathbf{v}_{0,5}$	$\mathbf{v}_{0,3}$	$\mathbf{v}_{0,1}$	$\mathbf{v}_{0,6}$
$\mathbf{v}^3_{0,s}=$	$\mathbf{v}_{0,0}$	$\mathbf{v}_{1,7}$	$\mathbf{v}_{1,6}$	$\mathbf{v}_{0,3}$	$\mathbf{v}_{0,2}$	$\mathbf{v}_{0,1}$	$\mathbf{v}_{0,4}$	$\mathbf{v}_{0,5}$
$\mathbf{v}^3_{1,s}=$	$\mathbf{v}_{1,0}$	$\mathbf{v}_{0,7}$	$\mathbf{v}_{0,6}$	$\mathbf{v}_{1,3}$	$\mathbf{v}_{1,2}$	$\mathbf{v}_{1,1}$	$\mathbf{v}_{1,4}$	$\mathbf{v}_{1,5}$
$\mathbf{v}^4_{0,s}=$	$\mathbf{v}_{0,0}$	$\mathbf{v}_{1,3}$	$\mathbf{v}_{1,7}$	$\mathbf{v}_{1,6}$	$\mathbf{v}_{0,4}$	$\mathbf{v}_{1,2}$	$\mathbf{v}_{1,1}$	$\mathbf{v}_{1,5}$
$\mathbf{v}^4_{1,s}=$	$\mathbf{v}_{1,0}$	$\mathbf{v}_{0,3}$	$\mathbf{v}_{0,7}$	$\mathbf{v}_{0,6}$	$\mathbf{v}_{1,4}$	$\mathbf{v}_{0,2}$	$\mathbf{v}_{0,1}$	$\mathbf{v}_{0,5}$
$\mathbf{v}^5_{0,s}=$	$\mathbf{v}_{0,0}$	$\mathbf{v}_{1,3}$	$\mathbf{v}_{0,1}$	$\mathbf{v}_{0,2}$	$\mathbf{v}_{1,7}$	$\mathbf{v}_{0,5}$	$\mathbf{v}_{0,4}$	$\mathbf{v}_{0,6}$
$\mathbf{v}^5_{1,s}=$	$\mathbf{v}_{1,0}$	$\mathbf{v}_{0,3}$	$\mathbf{v}_{1,1}$	$\mathbf{v}_{1,2}$	$\mathbf{v}_{0,7}$	$\mathbf{v}_{1,5}$	$\mathbf{v}_{1,4}$	$\mathbf{v}_{1,6}$
$\mathbf{v}^6_{0,s}=$	$\mathbf{v}_{0,0}$	$\mathbf{v}_{0,4}$	$\mathbf{v}_{1,7}$	$\mathbf{v}_{0,2}$	$\mathbf{v}_{1,5}$	$\mathbf{v}_{0,1}$	$\mathbf{v}_{0,6}$	$\mathbf{v}_{0,3}$
$\mathbf{v}^6_{1,s}=$	$\mathbf{v}_{1,0}$	$\mathbf{v}_{1,4}$	$\mathbf{v}_{0,7}$	$\mathbf{v}_{1,2}$	$\mathbf{v}_{0,5}$	$\mathbf{v}_{1,1}$	$\mathbf{v}_{1,6}$	$\mathbf{v}_{1,3}$
$\mathbf{v}^7_{0,s}=$	$\mathbf{v}_{0,0}$	$\mathbf{v}_{0,4}$	$\mathbf{v}_{0,1}$	$\mathbf{v}_{1,6}$	$\mathbf{v}_{0,2}$	$\mathbf{v}_{1,3}$	$\mathbf{v}_{1,5}$	$\mathbf{v}_{1,7}$
$\mathbf{v}^7_{1,s}=$	$\mathbf{v}_{1,0}$	$\mathbf{v}_{1,4}$	$\mathbf{v}_{1,1}$	$\mathbf{v}_{0,6}$	$\mathbf{v}_{1,2}$	$\mathbf{v}_{0,3}$	$\mathbf{v}_{0,5}$	$\mathbf{v}_{0,7}$

$q=0,\ldots,7$ являются различными. Явный вид $H^7(\mathbf{h})$-представителей этих компонент вычисляется точно так же, как и в случае (4×4)-разбиений. Все восемь разбиений определяются векторами $\mathbf{v}^q_{r,s}$ такими, что $R^{\mathbf{v}^q_{r,s}}_{s+8}=R^{\mathbf{v}_{r,s}\oplus\mathbf{w}_q}_{s+8}$, носители которых приведены в табл. 4. С целью экономии места оформление табл. 4 отличается от оформления табл. 3 тем, что вместо носителей приводятся векторы $\mathbf{v}_{r,s}\in H^7(\mathbf{h})$, через которые выражаются векторы $\mathbf{v}^q_{r,s}$ из q-го разбиения. Как и раньше, в верхней строке указан номер координаты, по которой следует сдвигать компоненту, содержащую вектор из той же колонки.

Следует рассмотреть также разбиения, которые получаются переносами полученных ранее разбиений на векторы из различных классов смежности кода H^{15} по подпространству $R_8\cup R_8^{\mathbf{v}_{1,0}}$. Дополнением в H^{15} к этому подпространству можно взять подпространство $P=\{\mathbf{v}_{0,p}\mid p=0,\ldots,7\}$. Получим 64 различных разбиения вида $R^{\mathbf{v}_{r,s}\oplus\mathbf{v}_{0,p}\oplus\mathbf{w}_q}_{s+8}$ $(r=0,1;\ s=0,\ldots,7)$, где $p,q=0,\ldots,7$. Далее рассмотрим произвольный вектор $\mathbf{u}\in O^1_8$ такой, что $[\mathbf{u}]=\{i_1,\ldots,i_8\}$. Возьмем такую перестановку

$\pi \in \mathrm{Sym}(H^{15})$, что $\pi(8) = i_1, \ldots, \pi(15) = i_8$. При любых $p, q = 0, \ldots, 7$ разбиение кода H^{15} вида

$$R^{\pi(\mathbf{v}_{r,s} \oplus \mathbf{v}_{0,p} \oplus \mathbf{w}_q)}_{\pi(s+8)} \quad (r = 0, 1;\ s = 0, \ldots, 7) \tag{4}$$

будем называть (8×2)-*разбиением*, а коды, получаемые сдвигами некоторых компонент одного из таких разбиений, называем (8×2)-*кодами*. Число различных (8×2)-разбиений равно $64 \cdot |O_8^1| = 960$.

Замечание. Среди кодов этого семейства встречаются несистематические, которые были найдены в [15] с помощью компьютера. Два неэквивалентных несистематических (8×2)-кода были также построены в [6].

(5×2)-коды. Семейство попарно непересекающихся компонент $R^{\mathbf{u}_q}_{i_q}$ $(q = 1, \ldots, p)$ кода H^{15} назовем *тупиковым*, если, во-первых, объединение всех компонент этого семейства не покрывает кода H^{15} и, во-вторых, любая компонента $R^{\mathbf{v}}_i$ кода H^{15} имеет непустое пересечение хотя бы с одной компонентой $R^{\mathbf{u}_q}_{i_q}$. Покажем, что тупиковые семейства компонент существуют.

Обратимся к орбите O_5^1. По лемме 10 можно рассмотреть пятерку координат $\{1, 8, 11, 13, 15\}$. Пользуясь разбиением (3), начнем с четверки попарно непересекающихся компонент $R_8^{\mathbf{v}_{r,0}}$, $R_{11}^{\mathbf{v}_{r,3}}$, $R_{13}^{\mathbf{v}_{r,5}}$, $R_{15}^{\mathbf{v}_{r,7}}$ $(r = 0, 1)$. Рассмотрим вектор $\mathbf{h}_1 \in O_7^1$ с носителем $[\mathbf{h}_1] = \{2, 4, 6, 8, 10, 12, 14\}$. Для каждого $s = 3, 5, 7$ существует единственный вектор $\mathbf{u}_{0,s+8}$, принадлежащий множеству $H^7(\mathbf{h}_1) \cap R^{\mathbf{v}_{0,s}}_{s+8}$. Эти векторы легко находятся по известным векторам $\mathbf{v}_{0,s}$. В результате получим $[\mathbf{u}_{0,11}] = \{8, 10, 12, 14\}$, $[\mathbf{u}_{0,13}] = \{4, 6, 8, 10\}$, $[\mathbf{u}_{0,15}] = \{2, 4, 8, 14\}$. По лемме 5 находим единственный вектор $\mathbf{u}_{0,1} \in H^7(\mathbf{h}_1)$, $[\mathbf{u}_{0,1}] = \{2, 6, 8, 12\}$, такой, что компонента $R_1^{\mathbf{u}_{0,1}}$ не пересекается со всеми компонентами $R_s^{\mathbf{u}_{0,s}}$ $(s = 11, 13, 15)$. Осталось проверить, что $R_1^{\mathbf{u}_{0,1}}$ не пересекается также и с компонентой R_8. Для этого рассмотрим вектор $\mathbf{h}_2 \in O_7^1$, $[\mathbf{h}_2] = \{2, 4, 6, 9, 11, 13, 15\}$ и найдем единственный вектор $\mathbf{u}$ из $H^7(\mathbf{h}_2) \cap R_1^{\mathbf{u}_{0,1}}$. Ясно, что $[\mathbf{u}] = \{2, 6, 9, 13\}$. Так как $1, 8 \notin [\mathbf{h}_2]$ и $9 \in [\mathbf{u}]$, то из леммы 5 следует, что компоненты $R_1^{\mathbf{u}_{0,1}}$ и R_8 не пересекаются. Пусть $\mathbf{u}_{0,8} = \mathbf{0}$. Добавляя к полученной пятерке компонент антиподальные компоненты, т. е. полагая $[\mathbf{u}_{1,1}] = \{4, 11, 15\}$, $[\mathbf{u}_{1,8}] = [\mathbf{h}_1]$, $[\mathbf{u}_{1,11}] = \{2, 4, 6\}$, $[\mathbf{u}_{1,13}] = \{2, 12, 14\}$, $[\mathbf{u}_{1,15}] = \{6, 10, 12\}$, получим следующее семейство из десяти компонент: $R_s^{\mathbf{u}_{r,s}}$ $(r = 0, 1;\ s = 1, 8, 11, 13, 15)$. При каждом $i \in \{1, 8, 11, 13, 15\}$ любая i-компонента $R^{\mathbf{v}}_i$ пересекается с некоторыми компонентами построенного семейства. Это следует также из конструкции предыдущей серии (8×2)-разбиений. Если $i \notin \{1, 8, 11, 13, 15\}$, то шестерка $\{i, 1, 8, 11, 13, 15\}$ не может быть носителем вектора из орбиты O_6^2. Поэтому в ней содержится хотя бы одна кодовая тройка. Следовательно, любая i-компонента $R^{\mathbf{v}}_i$

пересекается с рассматриваемым семейством, что доказывает его тупиковость.

Максимальное семейство из попарно непересекающихся десяти компонент впредь будем называть *тупиковым набором*. Из построения видно, что тройка попарно непересекающихся компонент $R_{11}^{\mathbf{v}_{0,3}}$, $R_{13}^{\mathbf{v}_{0,5}}$, $R_{15}^{\mathbf{v}_{0,7}}$ принадлежит единственному тупиковому набору и единственному (8×2)-разбиению на i-компоненты, где $i \in \{8, \ldots, 15\}$. Поэтому можно утверждать, что существует 64 различных тупиковых набора из попарно непересекающихся компонент вида $R_s^{\mathbf{u}_r, s \oplus \mathbf{v}_{0,p} \oplus \mathbf{w}_q}$ $(r = 0, 1;\ s = 1, 8, 11, 13, 15)$, где $p, q = 0, \ldots, 7$. Применяя перестановки $\pi \in \mathrm{Sym}(H^{15})$, можно получить $64 \times |O_5^1| = 10752$ различных тупиковых наборов компонент вида

$$R_{\pi(s)}^{\pi(\mathbf{u}_r, s \oplus \mathbf{v}_{0,p} \oplus \mathbf{w}_q)} \quad (r = 0, 1,\ s = 1, 8, 11, 13, 15),$$

где $p, q = 0, \ldots, 7$. Совершенный код будем называть (5×2)-*кодом*, если он получен из кода H^{15} сдвигами некоторых компонент одного из тупиковых наборов.

Лемма 11. *Ранг любого нелинейного кода Васильева равен* 12. *Ранг любого нелинейного* (2×8)*-кода, не являющегося кодом Васильева, равен* 13. *Ранг* (4×4)*-кода, получающегося из некоторого* (4×4)*-разбиения сдвигами всех его шестнадцати компонент, равен* 13. *Ранг любого другого* (4×4)*-кода, не являющегося* (2×8)*-кодом, равен* 14. *Ранг* (8×2)*-кода, получающегося из некоторого* (8×2)*-разбиения сдвигами всех его шестнадцати компонент, равен* 14. *Ранг любого другого* (8×2)*-кода и любого* (5×2)*-кода, не попадающего ни в один из предыдущих классов, равен* 15.

Доказательство. Любой вектор из кода Васильева C принадлежит либо H^{15}, либо $H^{15} \oplus \mathbf{e}_i$. Поэтому ранг C не больше 12, а для нелинейного кода он должен быть равен 12. Рассмотрим любой нелинейный (2×8)-код C, не являющийся кодом Васильева. Такой код должен содержать хотя бы одну несмещенную компоненту $R_i^{\mathbf{u}_1}$ и хотя бы одну смещенную компоненту $R_i^{\mathbf{u}_2} \oplus \mathbf{e}_i$, где $\mathbf{u}_1, \mathbf{u}_2 \in H^{15}$, $\mathbf{u}_1 \oplus \mathbf{u}_2 \in R_i \oplus R_j$ (иначе C будет кодом Васильева). Аналогично код C содержит хотя бы одну несмещенную компоненту $R_j^{\mathbf{v}_1}$ и хотя бы одну смещенную компоненту $R_j^{\mathbf{v}_2} \oplus \mathbf{e}_j$, где $\mathbf{v}_1, \mathbf{v}_2 \in H^{15} \setminus (R_i \oplus R_j \oplus \mathbf{u}_1)$. Поэтому множество $C \oplus C$ содержит множества R_i, R_j и $R_i \oplus R_j \oplus \mathbf{u}_1 \oplus \mathbf{v}_1$, причем $\mathbf{u}_1 \oplus \mathbf{v}_1 \notin R_i \oplus R_j$. Следовательно, подпространство L, порожденное множеством $C \oplus C$, содержит весь код H^{15}. Кроме этого, L содержит множества $R_i^{\mathbf{u}_1 \oplus \mathbf{u}_2} \oplus \mathbf{e}_i$ и $R_j^{\mathbf{v}_1 \oplus \mathbf{v}_2} \oplus \mathbf{e}_j$. Отсюда следует, что L должно содержать подпространство $H^{15} \oplus \{\mathbf{0}, \mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_i \oplus \mathbf{e}_j\}$. Так как по построению размерность подпространства L не может быть больше 13, то $L = H^{15} \oplus \{\mathbf{0}, \mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_i \oplus \mathbf{e}_j\}$. Допустим, что (4×4)-код C содержит три смещенные компоненты $R_i^{\mathbf{u}} \oplus \mathbf{e}_i$,

$R_j^{\mathbf{v}} \oplus \mathbf{e}_j$, $R_k^{\mathbf{w}} \oplus \mathbf{e}_k$, где тройка $\{i, j, k\}$ независима. Тогда подпространство L, порожденное множеством $C \oplus C$, содержит сумму $R_i^{\mathbf{u}} \oplus R_j^{\mathbf{v}} \oplus R_k^{\mathbf{w}}$, равную H^{15}. Кроме этого в случае $L \cap H^{15} \neq \varnothing$ подпространство L содержит сумму $H^{15} \oplus \{\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k\}$. Это означает, что размерность подпространства L равна 14. В случае $L \cap H^{15} = \varnothing$ код C получается из некоторого (4×4)-разбиения сдвигами всех его 16 компонент. Тогда, как легко заметить, $C \oplus C \subseteq H^{15} \oplus \{\mathbf{0}, \mathbf{e}_{i \oplus j}, \mathbf{e}_{i \oplus k}\}$ и ранг кода C равен 13. Для (8×2)-кодов и (5×2)-кодов доказательства аналогичны вышеприведенному. Лемма доказана.

Следствие. *Все (4×4)-коды, (8×2)-коды и (5×2)-коды, не являющиеся кодами Васильева и (2×8)-кодами, нелинейны. Не являющийся кодом Васильева (2×8)-код нелинеен тогда и только тогда, когда он пересекается с H^{15}.*

Следующая теорема подводит итог приведенной классификации совершенных кодов.

Теорема 2. *Любой совершенный код C, полученный из кода Хемминга H^{15} сдвигами его непересекающихся компонент, является $(k \times l)$-кодом, где $(k \times l)$ может принимать следующие значения: (1×16), (2×8), (4×4), (8×2), (5×2). Общее количество различных совершенных кодов, получаемых таким способом, равно 131224492, и среди них имеется 676 линейных кодов и их классов смежности в E^{15}.*

Доказательство. Пусть код C получается из H^{15} сдвигами непересекающихся i_q-компонент из семейства $R_{i_q}^{\mathbf{u}_q}$, где $\mathbf{u}_q \in H^{15}$, $q = 1, \ldots, m$ и $m \leqslant 16$. Обозначим через I множество всех координат i, совпадающих с i_q при некотором $q = 1, \ldots, m$. Возможны следующие случаи.

1. Множество I одноэлементно ($I = \{i\}$). Это случай кодов Васильева. Число таких кодов, которые можно получить из кода Хемминга H^{15}, равно $15 \cdot (2^{16} - 1) + 1 = 983026$. Среди них есть линейные коды и их классы смежности, являющиеся сдвигами в E^{15} различных кодов Хемминга. Число таких кодов равно сумме числа классов смежности кода H^{15} и удвоенного числа подпространств в H^{15}, которые при некотором i являются объединением восьми i-компонент. Всего из кода H^{15} получается 466 линейных кодов (вместе с классами смежности).

2. $I = \{i, j\}$ для некоторых $i \neq j$. Любая компонента $R_{i_q}^{\mathbf{u}_q}$ из рассматриваемого семейства либо является подмножеством множества $R_i \oplus R_j$, либо не пересекается с $R_i \oplus R_j$. Это означает, что такое семейство компонент является частью одного (и только одного) (2×8)-разбиения из 210 разбиений. Поэтому общее число совершенных кодов, порождаемых этим семейством компонент, равно $2 \cdot \binom{15}{2} \cdot (2^8 - 1)^2 = 13655250$. Среди них

содержатся линейные коды. Классы смежности линейных кодов, не учитываемые при подсчете кодов Васильева, получаются только в случае, когда все восемь i-компонент сдвигаются по направлению i, а остальные восемь j-компонент сдвигаются по направлению j. Число таких случаев равно $2 \cdot \binom{15}{2} = 210$.

3. Либо I — трехэлементное множество, либо I является кодовой четверкой. В этом случае можно считать, что вместе с каждой компонентой $R_{i_p}^{\mathbf{u}_p}$ в рассматриваемом наборе содержится и антиподальная ей компонента (в силу леммы 8 при необходимости ее всегда можно добавить). Можно также положить $i_1 = 8$, $i_2 = 10$, $i_3 = 12$, $\mathbf{u}_1 = \mathbf{0}$ и можно считать, что векторы $\mathbf{u}_2$, $\mathbf{u}_3 \in H^7(\mathbf{h})$ имеют вес 4, где $[\mathbf{h}] = \{1, \ldots, 7\}$. Так как компоненты $R_{10}^{\mathbf{u}_2}$ и $R_{12}^{\mathbf{u}_3}$ не пересекаются с R_8, то из леммы 5 следует, что $2 \in [\mathbf{u}_2]$ и $4 \in [\mathbf{u}_3]$. Из леммы 9 следует, что если для вектора $\mathbf{v} \in H^7(\mathbf{h})$ веса 4 компонента $R_8^{\mathbf{v}}$ не пересекается с $R_{10}^{\mathbf{u}_2}$ и $R_{12}^{\mathbf{u}_3}$, то $2, 4 \notin [\mathbf{v}]$. Существует только один вектор $\mathbf{v}_{2,0} \in H^7(\mathbf{h})$ веса 4 такой, что $[\mathbf{v}_{2,0}] = \{1, 3, 5, 7\}$. Добавляя антиподальные компоненты, т. е. полагая $[\mathbf{v}_{1,0}] = \{1, \ldots, 7\}$ и $[\mathbf{v}_{3,0}] = \{2, 4, 6\}$, видим, что все компоненты $R_8^{\mathbf{v}_{r,0}}$ не пересекаются с компонентами $R_{10}^{\mathbf{u}_2}$, $R_{12}^{\mathbf{u}_3}$ $(r = 0, 1, 2, 3)$. Оставшиеся двенадцать 8-компонент по лемме 5 будут пересекаться либо с $R_{10}^{\mathbf{u}_2}$, либо с $R_{12}^{\mathbf{u}_3}$. Следовательно, любая 8-компонента из первоначального набора совпадает с одной из компонент четверки $R_8^{\mathbf{v}_{r,0}}$ $(r = 0, 1, 2, 3)$. Так как компоненты $R_{10}^{\mathbf{u}_2}$ и $R_{12}^{\mathbf{u}_3}$ не пересекаются, то из леммы 9 следует, что либо $2, 4 \in [\mathbf{u}_2]$, либо $2, 4 \in [\mathbf{u}_3]$. В первом случае по этой же лемме имеем $2 \notin [\mathbf{u}_3]$ и $4 \in [\mathbf{u}_3]$. Действуя таким же образом, найдем еще две четверки компонент $R_{10}^{\mathbf{v}_{r,1}}$, $R_{12}^{\mathbf{v}_{r,2}}$ $(r = 0, 1, 2, 3)$, которые уже были определены выше при построении (4×4)-разбиений. При этом любая 10-компонента из исходного набора совпадает с одной из компонент $R_{10}^{\mathbf{v}_{r,1}}$, а любая 12-компонента попадает в четверку компонент $R_{12}^{\mathbf{v}_{r,2}}$ $(r = 0, 1, 2, 3)$. Рассмотрим еще четыре неиспользованных вектора $\mathbf{v}_{r,3}$ из $H^7(\mathbf{h})$ $(r = 0, 1, 2, 3)$. Действуя точно так же, можно показать, что если в исходном наборе существуют 14-компоненты, то они попадают в четверку компонент $R_{14}^{\mathbf{v}_{p,3}}$ $(p = 0, 1, 2, 3)$. Таким образом, мы получили разбиение кода Хемминга H^{15} на компоненты $R_{2s+8}^{\mathbf{v}_{r,s}}$ $(r, s = 0, 1, 2, 3)$ такое, что первоначальный набор компонент $R_{i_q}^{\mathbf{u}_q}$ $(q = 1, \ldots, p)$ является частью этого разбиения.

Во втором случае $2, 4 \in [\mathbf{u}_3]$, $4 \notin [\mathbf{u}_2]$ и $2 \in [\mathbf{u}_2]$. В результате получаем второе разбиение кода H^{15} на компоненты $R_{2s+8}^{\mathbf{v}_{r,s} \oplus \mathbf{v}_{2,0}}$ $(r, s = 0, 1, 2, 3)$. Таким образом, рассматриваемое семейство компонент является частью одного и только одного (4×4)-разбиения. Следовательно, это семейство компонент порождает (4×4)-код. Общее количество таких совершенных кодов равно $8 \cdot (|O_3^2| \cdot (2^4 - 1)^3 + |O_4^1| \cdot (2^4 - 1)^4) = 53865000$.

4. Множество I содержит хотя бы одну независимую четверку и не содержит кодовых пятерок. Вектор, носитель которого совпадает с I, в силу леммы 3 попадает в одну из орбит O_4^2, O_5^2, O_6^2, O_7^3, O_8^1. По лемме 10 существует единственный вектор $\mathbf{u}$ из орбиты O_8^1, носитель которого содержит I. Можно считать, что $[\mathbf{u}] = \{8, \ldots, 15\}$. В этом случае аналогично доказывается, что рассматриваемое семейство компонент является частью одного и только одного (8×2)-разбиения. Это означает, что такие семейства компонент всегда порождают (8×2)-коды, число которых равно $64 \cdot (|O_4^2| \cdot 3^4 + |O_5^2| \cdot 3^5 + |O_6^2| \cdot 3^6 + |O_7^3| \cdot 3^7 + |O_8^1| \cdot 3^8) = 60108480$.

5. Множество I является кодовой пятеркой. В силу леммы 10 можно считать, что $I = \{1, 8, 11, 13, 15\}$. Аналогично показывается, что такое семейство компонент является частью только одного тупикового набора. Поэтому коды, порождаемые такими семействами компонент, являются (5×2)-кодами, число которых равно $64 \cdot |O_5^1| \cdot 3^5 = 2612736$.

Суммируя, получаем 131224492 кода, среди которых имеется 676 линейных кодов и их классов смежности. Теорема доказана.

ЛИТЕРАТУРА

1. **Августинович С. В., Соловьева Ф. И.** О несистематических совершенных двоичных кодах // Проблемы передачи информации. 1996. Т. 32, вып. 3. С. 47–50.
2. **Августинович С. В., Соловьева Ф. И.** Построение совершенных двоичных кодов последовательными сдвигами $\widetilde{\alpha}$-компонент // Проблемы передачи информации. 1997. Т. 33, вып. 3. С. 15–21.
3. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Физматгиз, 1962. Вып. 8. С. 75–78.
4. **Малюгин С. А.** О нижней оценке числа совершенных двоичных кодов // Дискрет. анализ и исслед. операций. Сер. 1. 1999. Т. 6, № 4. С. 44–48.
5. **Романов А. М.** О несистематических совершенных кодах длины 15 // Дискретный анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 4. С. 75–78.
6. **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.
7. **Соловьева Ф. И.** О двоичных негрупповых кодах // Методы дискретного анализа в изучении булевых функций и графов: Сб. науч. тр. Новосибирск: Ин-т математики СО АН СССР, 1981. Вып. 37. С. 65–76.
8. **Соловьева Ф. И.** Геометрический подход к негрупповым плотно упакованным кодам (способы построения, свойства проекций): Дис. ... канд. физ.-мат. наук. Новосибирск, 1990. 76 с.

9. **Avgustinovich S. V., Solov'eva F. I.** Perfect binary codes with trivial automorphism group // Proc. of IEEE Intern. Workshop on Inform. Theory. Killarney, Ireland, 1998 (June). P. 114–115.
10. **Etzion T., Vardy A.** Perfect binary codes: Constructions, properties and enumeration // IEEE Trans. Inform. Theory. 1994. V. 40, N 3. P. 754–763.
11. **Heden O.** A binary perfect code of length 15 and codimension 0 // Designs, Codes and Cryptogr. 1994. V. 4, N 3. P. 213–220.
12. **Malyugin S. A.** Perfect codes with trivial automorphism group // Proc. Second Intern. Workshop on Optimal Codes and Related Topics. Sozopol, Bulgaria, 1998 (June). P. 163–167.
13. **Phelps K. T.** A combinatorial construction of perfect codes // SIAM J. Algebraic and Discrete Methods. 1983. V. 5, N 3. P. 398–403.
14. **Phelps K. T., LeVan M. J.** Kernels of nonlinear Hamming codes // Designs, Codes and Cryptogr. 1995. V. 6, N 3. P. 247–257.
15. **Phelps K. T., LeVan M. J.** Non-sistematic perfect codes // SIAM J. Discrete Math. 1999. V. 12, N 1. P. 27–34.
16. **Phelps K. T.** Switching equivalence classes of perfect codes // Designs, Codes and Cryptogr. 1999. V. 16, N 2. P. 179–184.
17. **Solov'eva F. I.** Switchings and perfect codes // Numbers, Information and Complexity. Dordrecht: Kluwer Acad. Publ. (to appear.)
18. **Vasil'ev Y. L., Solov'eva F. I.** Interdependence between perfect binary codes and their projections // Proc. Seventh Joint Swedish-Russian Intern. Workshop on Inform. Theory (St.-Peterburg, Russia. June, 1995). Moscow, 1995. P. 239–242.

Адрес автора:

Институт математики
им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090 Новосибирск,
Россия

Статья поступила
7 сентября 1999 г.