ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Сентябрь—октябрь 2013. Том 20, № 5. С. 31–44

УДК 519.8

О ПРЕДЕЛЬНО-ТРАНЗИТИВНЫХ РАСШИРЕННЫХ СОВЕРШЕННЫХ КОДАХ *)

Г. К. Гуськов, Ф. И. Соловьёва

Аннотация. Доказано, что для каждого $n = 2^k, k \geqslant 4$, существуют неэквивалентные предельно-транзитивные расширенные совершенные коды. Код называется *предельно-транзитивным*, если выкалывание любой его координаты приводит к получению нетранзитивного кода. Приведена классификация таких кодов длины 16.

Ключевые слова: расширенный совершенный двоичный код, транзитивный код, система троек Штейнера, Паш-конфигурация.

Введение

Транзитивные коды представляют большой интерес для исследований как наиболее близкие по ряду свойств к линейным кодам. Это обстоятельство, с одной стороны, позволяет сделать вывод о богатстве групп автоморфизмов транзитивных кодов, а с другой стороны, говорит о том, что их число невелико по сравнению с общим числом кодов с такими же параметрами, но тем не менее для всякого оптимального нелинейного кода почти всегда можно найти транзитивный код с теми же параметрами. Например, двоичный образ (под действием отображения Грея) произвольного аддитивного кода является транзитивным кодом.

В [9] получена классификация $\lfloor (k+1)/2 \rfloor$ совершенных аддитивных кодов длины $n = 2^k - 1$. В [2] классифицированы расширенные совершенные аддитивные коды, в [3] перечислены все неэквивалентные транзитивные совершенные двоичные коды длины 15, получаемые из одношаговых свитчингов кода Хэмминга длины 15; таких кодов оказалось 16, включая код Хэмминга. Применение известных методов построения кодов таких, как методы Васильева, Плоткина и Моллара, к транзитивным

*)Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 12–01–00631–а) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (соглашение № 8227).

кодам, удовлетворяющим некоторым дополнительным условиям, позволило получить бесконечные классы транзитивных кодов больших длин, в частности, не менее $\lfloor k/2 \rfloor^2$ неэквивалентных транзитивных совершенных кодов длины $n = 2^k - 1$, $k > 4$, с кодовым расстоянием 3, среди которых имеются коды больших рангов [5, 14]. Для доказательства неэквивалентности построенных кодов использовались ранги и размерности ядер этих кодов. В [4] для каждого допустимого n построено экспоненциальное число неэквивалентных транзитивных расширенных совершенных кодов длины $4n$ малого ранга, а именно, ранга на единицу больше ранга кода Хэмминга такой же длины, что отличает их от класса кодов, полученных в [5, 14]. В [8] доказано, что все транзитивные коды длины 15, перечисленные в [3], являются пропелинейными, в [7] доказано, что существует экспоненциальное число неэквивалентных пропелинейных кодов, т. е. что любой транзитивный код Потапова из [4] является пропелинейным. В [12] классифицированы все совершенные двоичные коды длин 15 и 16 и показано, что для $n = 15$ существует 201 транзитивный совершенный код, а для $n = 16$ обнаружены 101 транзитивный расширенный совершенный код. В ходе работы над данной статьёй вычислены*) такие характеристики, как ранг, размерность ядра, порядок группы автоморфизмов транзитивных совершенных кодов длины 15 и транзитивных расширенных совершенных кодов длины 16. Несомненно данная информация получена авторами работы [12], но в самой публикации приведены только численные характеристики, например, сколько кодов имеют данный ранг, без указания номеров транзитивных кодов, ранга, размерности ядра и других характеристик для каждого кода.

Легко видеть, что применение общей проверки на чётность позволяет получать из транзитивных совершенных двоичных кодов транзитивные расширенные совершенные двоичные коды. Обратное не всегда верно, в частности, в 2004 г. С. А. Малюгиным обнаружен транзитивный расширенный совершенный двоичный код длины 16 такой, что все коды, полученные из него выкалыванием любой координаты, нетранзитивны. Всякий такой расширенный совершенный код произвольной допустимой длины в дальнейшем будем называть *предельно-транзитивным*. Такой код обладает в некотором смысле пограничным свойством, характеризующим отличие класса транзитивных расширенных совершенных кодов от класса транзитивных совершенных кодов. Естественным образом

*) Guskov G. K., Solov'eva F. I. Properties of perfect transitive binary codes of length 15 and extended perfect transitive binary codes of length 16, 2012, http://arxiv.org/abs/1210.5940.

возник вопрос о классификации всех таких транзитивных кодов длины 16, а также вопрос о существовании неэквивалентных предельно-транзитивных расширенных совершенных кодов для любой допустимой длины. В настоящей работе даны положительные ответы на оба этих вопроса.

С помощью системы компьютерной алгебры Magma [10] обнаружено, что существует всего 10 предельно-транзитивных расширенных совершенных кодов длины 16. Приведены свойства этих кодов — их группы автоморфизмов, системы троек, ранги, ядра, а также перечислены аналогичные характеристики для остальных транзитивных кодов длины 15 и 16, имеющих хотя бы одну нетранзитивную координату. Доказано, что восемь из десяти таких кодов обладают специальными свойствами. Эти свойства позволяют для любого из них с помощью конструкции Плоткина получить бесконечную серию предельно-транзитивных расширенных совершенных кодов. Сравнение значений рангов и размерностей ядер этих кодов позволило показать неквивалентность пяти из них для любой допустимой длины, начиная с 32.

1. Необходимые определения и понятия

Через $\mathbb{F}^n$ обозначим пространство двоичных векторов длины n. *Расстояние Хэмминга* $d(x, y)$ между векторами x и y из $\mathbb{F}^n$ равно количеству координат, в которых различаются эти векторы. *Весом* вектора x называется число $w(x) = d(x, 0^n)$, где 0^n — нулевой вектор длины n. *Двоичным кодом* называется произвольное подмножество C из $\mathbb{F}^n$. Код C из $\mathbb{F}^n$ называется *совершенным двоичным кодом, исправляющим одиночные ошибки* (далее, кратко, *совершенным кодом*), если любой вектор пространства $\mathbb{F}^n$ находится на расстоянии не больше 1 от некоторого единственного вектора из C. Известно, что такие коды существуют только при $n = 2^m - 1$, $m \geqslant 2$. В данной работе будем рассматривать только коды, содержащие нулевое слово длины n.

Ядро кода C состоит из всех векторов $x \in C$ таких, что $x + C = C$. Размерности ядра и линейной оболочки кода C обозначим через $k(C)$ и $r(C)$ соответственно, $r(C)$ называется *рангом* кода C. Напомним, что ранг кода Хэмминга равен $n - \log(n + 1)$ и ранги совершенных (расширенных совершенных) кодов длины n (длины $n + 1$) варьируются от $n - \log(n + 1)$ до n.

Группа автоморфизмов $\mathrm{Aut}(\mathbb{F}^n)$ пространства $\mathbb{F}^n$ определяется так:

$$\mathrm{Aut}(\mathbb{F}^n) = \{(v, \pi) \mid v \in \mathbb{F}^n,\ \pi \in S_n\},$$

где S_n — симметрическая группа подстановок порядка n. *Группой автоморфизмов* $\mathrm{Aut}(C)$ кода C длины n называется группа изометрий пространства $\mathbb{F}^n$, переводящих код в себя. Код называется *транзитивным*, если его группа автоморфизмов действует транзитивно на всех его кодовых словах. Для определения транзитивности кодов, содержащих нулевой вектор, удобно пользоваться следующим определением транзитивного кода, эквивалентным приведённому выше: для каждого кодового слова x из C найдётся подстановка π_x из S_n такая, что $(x, \pi_x) \in \mathrm{Aut}(C)$, т. е. $x + \pi_x(C) = C$, где π_x может не принадлежать группе симметрий $\mathrm{Sym}(C) = \{\pi \in S_n \mid \pi(C) = C\}$ кода C. Кодовое слово x из C, для которого не существует такой подстановки π_x, будем называть *нетранзитивным кодовым словом*. Координату транзитивного расширенного кода назовём *нетранзитивной*, если код, полученный выкалыванием этой координаты, нетранзитивен. Таким образом, предельно-транзитивный код — это код, у которого все координаты нетранзитивны.

Системой троек Штейнера STS_n порядка n называется система сочетаний из n-элементного множества $\mathcal{N}_n = \{1, \ldots, n\}$ по три такая, что каждая неупорядоченная пара элементов содержится в точности в одной тройке. Известно [11], что кодовые слова веса 3 в совершенном коде C^n, содержащем нулевой вектор, образуют систему троек Штейнера (каждая тройка системы состоит из номеров ненулевых координат соответствующего кодового слова), будем обозначать её через $\mathrm{STS}(C^n)$.

Паш-конфигурацией для STS_n называется множество троек из STS_n, изоморфное множеству $\{(a, b, c), (a, y, z), (x, b, z), (x, y, c)\}$, т. е. троек, попарно пересекающихся по одному элементу, а в объединении дающих шесть элементов. Кроме того, в Паш-конфигурации сумма любых трёх троек даёт оставшуюся тройку. Известно, что число Паш-конфигураций $P(\mathrm{STS}_n)$ системы троек Штейнера STS_n порядка n является инвариантом, часто позволяющим установить неэквивалентность двух систем троек Штейнера.

Пусть C — произвольный расширенный совершенный код. Систему четвёрок кода C обозначим через $SQ(C)$, т. е. $SQ(C) = \{u + v \mid u, v \in C : w(u + v) = 4\}$.

2. Транзитивные совершенные коды длины 15 и транзитивные расширенные совершенные коды длины 16

В этом разделе исследуются свойства всех совершенных и транзитивных расширенных совершенных кодов длин 15 и 16, имеющих хотя бы одну нетранзитивную координату.

На рис. 1 и 2 показано распределение всех 101 транзитивных расширенных совершенных кодов (201 транзитивных совершенных кодов)

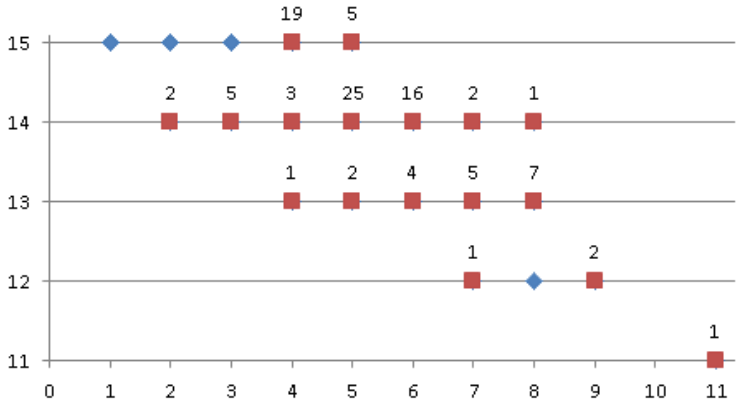

Рис. 1. Распределение пар (ранг, размерность ядра) для транзитивных расширенных совершенных кодов длины 16

из классификации [12] по парам (ранг, размерность ядра), которым они соответствуют. По вертикали выписаны значения рангов кодов, а по горизонтали — размерности ядер. Квадратами отмечены точки, соответствующие парам (ранг, размерность ядра), для которых существуют транзитивные расширенные совершенные коды длины 16 (транзитивные совершенные коды длины 15 соответственно), сверху надписано число таких кодов. Ромбами отмечены точки, отвечающие парам (ранг и размерность ядра), для которых существуют нетранзитивные расширенные совершенные коды длины 16 (нетранзитивные совершенные коды длины 15).

По определению ранги расширенного совершенного кода длины 16 и совершенного кода длины 15 не могут быть больше 15. Следует заметить, что среди точек, отмеченных квадратами на рис. 1 и 2, есть также и нетранзитивные расширенные совершенные (нетранзитивные совершенные) коды.

В табл. 1 приведены все транзитивные расширенные совершенные коды длины 16, которые имеют хотя бы одну нетранзитивную координату. Номера координат согласно их естественной нумерации представлены в третьем столбце. Таких кодов оказалось 51 среди 101 транзитивного кода из [12], десять из них — предельно-транзитивные, последние в таблице выделены жирным шрифтом. Второй столбец содержит номер кода

в классификации из [12], далее следуют номера нетранзитивных координат, ранг, размерность ядра, мощность группы автоморфизмов и мощность множества $SQ(C)$.

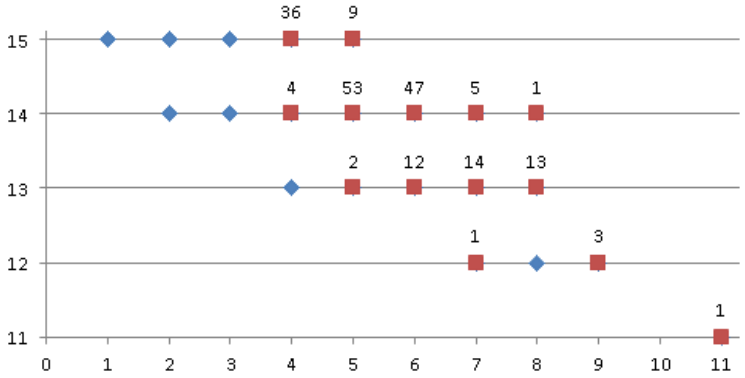

Рис. 2. Распределение пар (ранг, размерность ядра) для транзитивных совершенных кодов длины 15

Таблица 1

Нетранзитивные координаты кодов длины 16

	#	Нетранзитивные координаты	$r(C)$	$k(C)$	$\lvert\mathrm{Aut}(C)\rvert$	$\lvert SQ(C)\rvert$
1	**24**	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	13	5	32768	468
2	**64**	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	13	4	196608	428
3	87	5, 6, 7, 8	13	7	65536	376
4	191	1, 2, 3, 4, 9, 10, 11, 12, 13, 14, 15, 16	13	5	32768	436
5	364	9, 10, 11, 12, 13, 14, 15, 16	14	5	16384	754
6	369	9, 10, 11, 12, 13, 14, 15, 16	14	5	16384	758
7	375	9, 10, 11, 12, 13, 14, 15, 16	14	5	32768	742
8	383	9, 10, 11, 12, 13, 14, 15, 16	14	5	32768	730
9	**424**	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	14	2	4096	872
10	**488**	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	14	3	8192	838
11	495	9, 10, 11, 12, 13, 14, 15, 16	14	4	8192	786
12	555	9, 11, 13, 15	14	6	16384	604
13	560	9, 11, 13, 15	14	6	32768	640
14	635	1, 2, 7, 8, 9, 11, 13, 15	14	5	16384	616
15	671	9, 11, 13, 15	14	5	32768	716

	#	Нетранзитивные координаты	$r(C)$	$k(C)$	$\lvert\mathrm{Aut}(C)\rvert$	$\lvert SQ(C)\rvert$
16	723	9, 11, 13, 15	14	5	16384	672
17	759	1, 2, 7, 8, 9, 11, 13, 15	14	5	16384	680
18	929	9, 11, 13, 15	14	6	16384	616
19	933	9, 11, 13, 15	14	6	32768	636
20	944	9, 11, 13, 15	14	6	16384	612
21	974	9, 11, 13, 15	14	6	32768	624
22	1050	2, 3, 5, 8, 9, 11, 13, 15	14	5	16384	600
23	1070	2, 3, 5, 8, 9, 11, 13, 15	14	5	8192	608
24	1275	2, 3, 5, 8, 9, 11, 13, 15	14	5	8192	664
25	1279	2, 3, 5, 8, 9, 11, 13, 15	14	5	16384	648
26	**1907**	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	14	4	65536	764
27	1962	9, 10, 11, 12, 13, 14, 15, 16	14	6	196608	698
28	**1968**	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	14	3	24576	854
29	**1983**	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	14	2	86016	896
30	2001	1, 5, 6, 8, 10, 11, 12, 16	15	5	8192	988
31	2004	1, 2, 3, 5, 6, 8, 10, 11, 12, 14, 15, 16	15	4	4096	988
32	2015	1, 5, 6, 8, 10, 11, 12, 16	15	4	8192	988
33	2019	1, 2, 3, 5, 6, 8, 10, 11, 12, 14, 15, 16	15	4	4096	964
34	2056	2, 3, 5, 6, 11, 12, 14, 15	15	4	8192	1100
35	2059	1, 2, 3, 8, 10, 14, 15, 16	15	4	8192	1100
36	2063	2, 3, 5, 6, 11, 12, 14, 15	15	4	8192	1068
37	2070	1, 2, 3, 8, 10, 14, 15, 16	15	4	8192	1068
38	2072	1, 2, 3, 7, 9, 14, 15, 16	15	5	8192	956
39	2075	1, 6, 7, 8, 9, 10, 12, 16	15	4	8192	988
40	2080	1, 2, 3, 6, 7, 8, 9, 10, 12, 14, 15, 16	15	4	4096	980
41	2081	2, 3, 6, 8, 10, 12, 14, 15	15	4	8192	956
42	2087	2, 3, 6, 8, 10, 12, 14, 15	15	4	8192	1068
43	2088	1, 2, 3, 6, 7, 8, 9, 10, 12, 14, 15, 16	15	4	4096	1084
44	2093	1, 2, 3, 7, 9, 14, 15, 16	15	4	8192	1036
45	2094	1, 6, 7, 8, 9, 10, 12, 16	15	4	8192	1036
46	**2134**	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	14	3	49152	848
47	2143	1, 3, 5, 7, 10, 12, 14, 16	14	4	8192	854
48	2144	1, 3, 5, 7, 10, 12, 14, 16	14	5	49152	806
49	**2148**	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	14	3	8192	850
50	**2157**	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	14	3	24576	842
51	2159	9, 10, 11, 12, 13, 14, 15, 16	14	5	344064	854

3. Бесконечная серия предельно-транзитивных кодов

В этом разделе рассмотрим задачу построения предельно-транзитивного расширенного совершенного кода для любого допустимого $N = 2^k$, $k \geqslant 4$.

Рассмотрим произвольный расширенный совершенный код C^N длины $N = 2^k$. Через C^{2N} обозначим расширенный код, полученный с помощью конструкции Плоткина [11]:

$$C^{2N} = \{(u+v, u) \mid u \in \mathbb{F}_0^N,\ v \in C^N\}, \tag{1}$$

где $\mathbb{F}_0^N$ — код, состоящий из всех чётно-весовых векторов пространства $\mathbb{F}^N$.

Через C_j^{N-1} обозначим код, полученный выкалыванием кода C^N по j-й координате, $j \in \mathcal{N}_N$.

Пусть V_i^{2n+1} — код, полученный из совершенного кода C_i^n, $i \in \mathcal{N}_N$, $n = 2^k - 1$, $k \geqslant 3$, применением известной конструкции Васильева с функцией $\lambda \equiv 0$ [1]:

$$V_i^{2n+1} = \{(x+y, |x|, x) \mid x \in \mathbb{F}^n,\ y \in C_i^n\}.$$

Заметим, что если C_i^n транзитивен, то и V_i^{2n+1} транзитивен согласно [5]. Аналогичное утверждение, очевидно, верно и для кода, полученного с помощью конструкции Плоткина.

В силу такого выбора кодов Плоткина и Васильева нетрудно убедиться, что справедлива

Лемма 1. *Для любого $j \in \mathcal{N}_{2N}$ найдётся $i \in \mathcal{N}_N$ такое, что код C_j^{2n+1} изоморфен коду Васильева V_i^{2n+1}.*

Непосредственно из определения транзитивности вытекает

Лемма 2. *Пусть C — произвольный совершенный двоичный код длины n, $y \in C$ — некоторое кодовое слово. Если $\mathrm{STS}(C) \ncong \mathrm{STS}(C+y)$, то y — нетранзитивное кодовое слово и код C нетранзитивен.*

Для дальнейшего изложения понадобится частный случай известной конструкции Ассмуса и Маттсона из [6] для построения системы троек Штейнера порядка $2n+1$ из системы троек Штейнера порядка n.

Введём для краткости обозначение $\overline{a} = a + n + 1$. Пусть STS_n — система троек Штейнера порядка n, определённая на множестве $\mathcal{N}_n$, $n \equiv 1, 3 \pmod 6$. Тогда STS_{2n+1} на множестве $\mathcal{N}_{2n+1}$ строится по правилам:

(a) STS_{2n+1} содержит тройки вида

$$(l, n+1, \overline{l}), \quad l \in \mathcal{N}_n; \tag{2}$$

(b) для любой тройки (a, b, c) из STS_n система троек STS_{2n+1} содержит тройки вида

$$(a, b, c), \tag{3}$$

$$(a, \overline{b}, \overline{c}), (\overline{a}, b, \overline{c}), (\overline{a}, \overline{b}, c). \tag{4}$$

Заметим также, что эта система троек Штейнера соответствует системе троек Штейнера кода Васильева V_i^{2n+1} длины $2n+1$, когда $\lambda \equiv 0$ и код C_i^n содержит нулевое кодовое слово 0^n (см., например, теорему 8 из [13]). Кроме того, в силу леммы 1 она соответствует системе троек Штейнера кода, полученного выкалыванием кода Плоткина C^{2N}.

Лемма 3. *Пусть для некоторой системы троек Штейнера* STS_n *порядка* n *число Паш-конфигураций равно* $P(\mathrm{STS}_n)$. *Тогда для числа Паш-конфигураций* $P(\mathrm{STS}_{2n+1})$ *системы троек Штейнера* STS_{2n+1}, *полученной из* STS_n *с помощью конструкции Ассмуса и Маттсона, справедливо равенство*

$$P(\mathrm{STS}_{2n+1}) = 8P(\mathrm{STS}_n) + |\mathrm{STS}_n| + 2\binom{n}{2}.$$

Доказательство. По конструкции Ассмуса и Маттсона, зная произвольную тройку (a, b, c) исходной системы троек Штейнера STS_n, можно записать общий вид троек из STS_{2n+1}:

$$(a, b, c),\ (a, \overline{b}, \overline{c}),\ (\overline{a}, b, \overline{c}),\ (\overline{a}, \overline{b}, c),\ (l, n+1, \overline{l}), \quad \text{где } l \in \mathcal{N}_n.$$

Так как тройки любой Паш-конфигурации сильно связаны между собой (например, сумма любых трёх троек Паш-конфигурации равна четвёртой, а сумма двух произвольных троек конфигурации равна сумме оставшихся двух), зная общий вид троек в STS_{2n+1}, нетрудно перечислить все возможные Паш-конфигурации этой системы троек.

Если хотя бы одна из троек Паш-конфигурации из STS_{2n+1} содержит элемент $n+1$, т. е. имеет вид $(l, n+1, \overline{l})$, то в этой конфигурации должна содержаться ещё одна тройка такого же вида, например, $(l', n+1, \overline{l'})$, для произвольного $l' \in \mathcal{N}_n \setminus \{l\}$. Последний, шестой, элемент, содержащийся в тройках Паш-конфигурации, может принадлежать либо множеству $\mathcal{N}_n$, либо $\mathcal{N}_{2n+1} \setminus \mathcal{N}_{n+1}$. В первом случае он однозначно определяется тройкой, содержащей пару элементов $(\overline{l}, \overline{l'})$, а во втором — тройкой, содержащей пару элементов $(\overline{l}, l')$. Следовательно, существует только две возможности достроить произвольную пару троек, содержащих элемент $n+1$, до следующих Паш-конфигураций:

$$\{(l, n+1, \overline{l}), (l', n+1, \overline{l'}), (\overline{l}, \overline{a}, l'), (\overline{l'}, \overline{a}, l)\},$$

$$\{(l, n+1, \bar{l}), (l', n+1, \overline{l'}), (a, l, l'), (\bar{l}, \overline{l'}, a)\}.$$

Число таких пар, в свою очередь, равно числу выборов неупорядоченной пары чисел l и l' из множества $\mathcal{N}_n$, т. е. $\binom{n}{2}$.

Рассмотрим теперь тройки, не содержащие элемента $n+1$, т. е. имеющие вид (3) или (4). Заметим, что по конструкции Ассмуса и Маттсона все тройки вида (3) являются тройками системы STS_n, а если в любой тройке вида (4) каждый элемент $\bar{t} \in \mathcal{N}_{2n+1} \setminus \mathcal{N}_{n+1}$ заменить элементом $t = \bar{t} - (n+1) \in \mathcal{N}_n$, то получим тройку системы STS_n. Таким образом, если рассмотреть произвольную Паш-конфигурацию системы STS_{2n+1}, не содержащую троек вида (2), и заменить все элементы $\bar{t} \in \mathcal{N}_{2n+1} \setminus \mathcal{N}_{n+1}$, встречающиеся в её тройках, элементами $t = \bar{t} - (n+1) \in \mathcal{N}_n$, то получим либо Паш-конфигурацию системы STS_n, либо четыре одинаковых тройки из STS_n. Воспользуемся этим фактом для подсчёта Паш-конфигураций в STS_{2n+1}.

Пусть Паш-конфигурация содержит тройку (a, b, c), где $a, b, c \in \mathcal{N}_n$. Тогда по определению Паш-конфигурации оставшиеся в ней тройки содержат по одному элементу a, b и c. Если и вторая тройка системы имеет вид (3), то снова по определению Паш-конфигураци любая её тройка должна содержать по два элемента из $\mathcal{N}_n$, что возможно, если только все тройки Паш-конфигурации имеют вид (3). Следовательно, если Паш-конфигурация содержит тройку вида (3), то возможны два случая. В первом случае все оставшиеся тройки Паш-конфигурации имеют вид (3), а значит, эта Паш-конфигурация системы STS_{2n+1} в точности совпадает с Паш-конфигурацией исходной системы STS_n, во втором — имеют вид (4).

Очевидно, что если Паш-конфигурация не содержит троек вида (2) и (3), то она целиком состоит из троек вида (4). Так как из одной тройки системы STS_n по конструкции Ассмуса и Маттсона можно построить только три тройки вида (4), рассмотрев произвольную Паш-конфигурацию из STS_{2n+1}, состоящую из троек вида (4), и заменив каждый элемент $\bar{t} \in \mathcal{N}_{2n+1} \setminus \mathcal{N}_{n+1}$, встречающийся в её тройках, соответствующим ему элементом $\bar{t} - (n+1) = t \in \mathcal{N}_n$, нельзя получить четыре одинаковые тройки из STS_n. Причём для каждой Паш-конфигурации из STS_n найдётся ровно три Паш-конфигурации из STS_{2n+1}, совпадающие с ней после описанной выше замены элементов. Этот факт объясняется тем, что если Паш-конфигурация из STS_n содержит тройку (a, b, c), то любая соответствующая ей Паш-конфигурация из STS_{2n+1} должна содержать одну из троек вида (4).

Следовательно, каждой Паш-конфигурации $\{(a, b, c), (a, y, z), (x, b, z),$

$(x, y, c)\}$ исходной системы STS_n соответствует восемь следующих Паш-конфигураций из STS_{2n+1}:

$$\{(a,b,c),(a,y,z),(x,b,z),(x,y,c)\},\quad \{(a,b,c),(a,\overline{y},\overline{z}),(\overline{x},b,\overline{z}),(\overline{x},\overline{y},c)\},$$

$$\{(a,\overline{b},\overline{c}),(a,y,z),(\overline{x},\overline{b},z),(\overline{x},y,\overline{c})\},\quad \{(\overline{a},b,\overline{c}),(\overline{a},\overline{y},z),(x,b,z),(x,\overline{y},\overline{c})\},$$

$$\{(\overline{a},\overline{b},c),(\overline{a},y,\overline{z}),(x,\overline{b},\overline{z}),(x,y,c)\},\quad \{(\overline{a},\overline{b},c),(\overline{a},\overline{y},z),(\overline{x},\overline{b},z),(\overline{x},\overline{y},c)\},$$

$$\{(\overline{a},b,\overline{c}),(\overline{a},y,\overline{z}),(\overline{x},b,\overline{z}),(\overline{x},y,\overline{c})\},\quad \{(a,\overline{b},\overline{c}),(a,\overline{y},\overline{z}),(x,\overline{b},\overline{z}),(x,\overline{y},\overline{c})\}.$$

Кроме того, по конструкции Ассмуса и Маттсона каждой тройке из STS_n соответствует одна Паш-конфигурация вида

$$\{(a,b,c),(a,\overline{b},\overline{c}),(\overline{a},b,\overline{c}),(\overline{a},\overline{b},c)\}.$$

С учётом того, что среди построенных Паш-конфигураций нет двух одинаковых, остаётся подсчитать число всех полученных Паш-конфигураций. Лемма 3 доказана.

С целью проиллюстрировать метод выбора нетранзитивного вектора при доказательстве нетранзитивности выколотых кодов, получаемых из предельно-транзитивного расширенного совершенного кода любой допустимой длины $N = 2^k,\ k \geqslant 5$, приведём следующее утверждение.

Лемма 4. *Для любого $N = 2^k,\ k \geqslant 4$, существует не менее 8 различных транзитивных расширенных совершенных кодов длины N таких, что для любого из этих кодов C^N для всякого направления $i \in \mathcal{N}_N$ в выколотом коде C_i^n, $n = N - 1$, найдётся нетранзитивное слово y такое, что*

$$P\big(\mathrm{STS}\big(C_i^n\big)\big) \neq P\big(\mathrm{STS}\big(C_i^n + y\big)\big). \tag{5}$$

Доказательство проведём индукцией по $k = \log N$, где N — длина кода, $k \geqslant 4$.

Для $k = 4$, т. е. $N = 16$, лемма верна, поскольку с помощью системы компьютерной алгебры Magma проверено, что для восьми транзитивных расширенных совершенных кодов для любого направления $i \in \mathcal{N}_{16}$ в коде C_i^{15} найдётся нетранзитивное слово y такое, что $P\big(\mathrm{STS}\big(C_i^{15}\big)\big) \neq P\big(\mathrm{STS}\big(C_i^{15} + y\big)\big)$. В табл. 1 эти коды имеют номера $24, 64, 424, 1907, 1968, 1983, 2134, 2157$ согласно нумерации, данной в [12]. Оставшиеся два предельно-транзитивных кода длины 16 под номерами 488 и 2148 этим свойством не обладают.

Пусть лемма верна для некоторого $k \geqslant 4$. Докажем, что она верна для $k{+}1$. Рассмотрим транзитивный расширенный совершенный код C^N,

$N = 2^k$, такой, что для любого направления $i \in \mathcal{N}_N$ в выколотом коде C_i^n найдётся нетранзитивное слово y такое, что

$$P\big(\mathrm{STS}\big(C_i^n\big)\big) \neq P\big(\mathrm{STS}\big(C_i^n + y\big)\big), \quad n = N - 1.$$

Применяя к C^N конструкцию Плоткина (1), получим транзитивный расширенный совершенный код C^{2N}, удовлетворяющий условию (5).

В случае, когда код C_j^{2n+1} получен из C^{2N} выкалыванием одной из первых N координат, для любого $i \in \mathcal{N}_N$ найдётся y из C_i^n такой, что

$$P\big(\mathrm{STS}\big(C_i^n\big)\big) \neq P\big(\mathrm{STS}\big(C_i^n + y\big)\big).$$

В силу леммы 3

$$P\big(\mathrm{STS}\big(V_i^{2n+1}\big)\big) \neq P\big(\mathrm{STS}\big(V_i^{2n+1} + (y, 0^{n+1})\big)\big),$$

где $(y, 0^{n+1}) \in V_i^{2n+1}$. Согласно леммам 1 и 2 из этого неравенства следует, что код C_j^{2n+1} удовлетворяет условию (5).

Случай $j \in \mathcal{N}_{2N} \setminus \mathcal{N}_N$ аналогичен рассмотренному. В качестве нетранзитивного кодового слова кода V_i^{2n+1} может быть выбран вектор $(0^{n+1}, y)$.

Подставляя 8 различных кодов длины $N = 2^k$ в конструкцию Плоткина, получим 8 различных кодов длины $2N = 2^{k+1}$. Лемма 4 доказана.

В дальнейшем понадобится лемма, устанавливающая связь между рангом и размерностью ядра исходного кода и кода, полученного из него с помощью конструкции Плоткина (1). Для совершенных кодов аналог этой леммы доказан в [5, лемма 1].

Лемма 5. *Для ранга $r(C^{2N})$ и размерности ядра $k(C^{2N})$ произвольного расширенного совершенного кода C^{2N}, полученного из расширенного совершенного кода C^N с помощью конструкции Плоткина, имеют место равенства*

$$r(C^{2N}) = N - 1 + r, \quad k(C^{2N}) = N - 1 + k,$$

где r — ранг, а k — размерность ядра совершенного кода C^N.

Из леммы 5, очевидно, следует, что если два расширенных совершенных кода имели различные пары (ранг, размерность ядра), то у кодов, полученных из них с помощью конструкции Плоткина, эти пары также будут различны.

Теорема 1. *Для любого допустимого $N > 16$ существует не менее пяти неэквивалентных предельно-транзитивных расширенных совершенных кодов длины N. При $N = 16$ существует 10 неэквивалентных таких кодов.*

Доказательство. Согласно табл. 1 для $N = 16$ пять из десяти неэквивалентных предельно-транзитивных расширенных совершенных кодов длины 16 имеют различные пары (ранг, размерность ядра). Для удобства сгруппируем информацию для этих десяти кодов в табл. 2.

Таблица 2

(r, k)	Номера кодов
(13, 4)	64
(13, 5)	24
(14, 2)	424, 1983
(14, 3)	488, 1968, 2134, 2148, 2157
(14, 4)	1907

Ввиду лемм 2, 4 и 5 делаем вывод, что с помощью конструкции Плоткина из этих пяти кодов длины 16 можно построить пять бесконечных серий предельно-транзитивных расширенных совершенных кодов таких, что для любой допустимой длины коды из различных серий будут иметь различные ранг и размерность ядра. Очевидно, что если пары значений (ранг, размерность ядра) двух расширенных совершенных приведённых кодов различны, то эти коды неэквивалентны. Теорема 1 доказана.

Если же рассматривать вместо неэквивалентных кодов различные коды, то с использованием лемм 2 и 4 можно продолжить восемь из десяти существующих предельно-транзитивных расширенных совершенных кодов длины 16 до бесконечных серий. Тем самым справедливо

Следствие 1. *Для любого допустимого $N > 16$ существует не менее 8 различных предельно-транзитивных расширенных совершенных кодов длины N.*

Авторы выражают глубокую благодарность И. Ю. Могильных за активное участие в плодотворных дискуссиях в ходе работы над статьёй.

ЛИТЕРАТУРА

1. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Пробл. кибернетики. — 1962. — Вып. 8. — С. 337–339.
2. **Кротов Д. С.** Z_4-линейные совершенные коды // Дискрет. анализ и исслед. операций. Сер. 1. — 2000. — Т. 7, № 4. — С. 78–90.

3. **Малюгин С. А.** О классах эквивалентности совершенных двоичных кодов длины 15 // Препринт № 138. — Новосибирск: Институт математики СО РАН, 2004. — 34 с.
4. **Потапов В. Н.** О нижней оценке числа транзитивных совершенных кодов // Дискрет. анализ и исслед. операций. Сер. 1. — 2006. — Т. 13, № 4. — С. 49–59.
5. **Соловьёва Ф. И.** О построении транзитивных кодов // Пробл. передачи информ. — 2005. — Вып. 3. — С. 23–31.
6. **Assmus E. F., Jr., Mattson H. F., Jr.** On tactical configurations and error correcting codes // J. Comb. Theory. — 1967. — Vol. 2. — P. 243–257.
7. **Borges J., Mogilnykh I. Yu., Rifà J. K., Solov'eva F. I.** On the number of nonequivalent propelinear extended perfect codes // Electron. J. Comb. — 2013. — Vol. 20, N 2. — P. 37–50.
8. **Borges J., Mogilnykh I. Yu., Rifà J. K., Solov'eva F. I.** Structural properties of binary propelinear codes // Adv. Math. Commun. — 2012. — Vol. 6, N 3. — P. 329–346.
9. **Borges J., Rifà J. K.** A characterization of 1-perfect additive codes // IEEE Trans. Inform. Theory. — 1999. — Vol. 45. — P. 1688–1697.
10. **Bosma W., Cannon J., Playoust C.** The Magma algebra system. I. The user language // J. Symb. Comput. — 1997. — Vol. 24. — P. 235–265.
11. **MacWilliams F. G., Sloane N. J. A.** The theory of error correcting codes. — New York: North-Holland, 1977. — 744 p.
12. **Östergård P. R. J., Pottonen O.** The perfect binary one-error-correcting codes of length 15. Part I — Classification // IEEE Trans. Inform. Theory. — 2009. — Vol. 55. — P. 4657–4660.
13. **Solov'eva F. I.** On perfect codes and related topics // *Com*^{2}*Mac* Lect. Notes Ser. 13. — Pohang: Combinatorial and Computational Mathematics Center, Pohang Univ. Sci. Technology (POSTECH), Korea, 2004. — 80 p.
14. **Solov'eva F. I.** On transitive codes // Тр. конф. «Дискретный анализ и исследование операций» (Новосибирск, 28 июня–2 июля 2004 г.). — Новосибирск: Изд-во Ин-та математики СО РАН, 2004. — С. 99.

Гуськов Георгий Константинович,
e-mail: m1lesnsk@gmail.com
Соловьёва Фаина Ивановна,
e-mail: sol@math.nsc.ru

Статья поступила
27 августа 2012 г.

Переработанный вариант —
28 мая 2013 г.