ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Май—июнь 2013. Том 20, № 3. С. 3–25

УДК 621.391.15

О СИСТЕМАХ ТРОЕК ШТЕЙНЕРА МАЛОГО РАНГА, ВЛОЖИМЫХ В СОВЕРШЕННЫЕ ДВОИЧНЫЕ КОДЫ *)

Д. И. Ковалевская, Ф. И. Соловьёва, Е. С. Филимонова

Аннотация. Свитчинговым методом получена классификация систем троек Штейнера STS(n) порядка $n = 2^r - 1$, $r > 3$, малого ранга r_n (на 2 отличного от ранга кода Хэмминга длины n), вложимых в совершенные двоичные коды длины n такого же ранга. Приведены верхняя и нижняя оценки числа различных таких STS. Дано описание класса систем STS(n) ранга r_n, не вложимых в совершенные двоичные коды длины n такого же ранга, и приведена нижняя оценка числа этих систем. Доказана вложимость любой системы STS(n) ранга $r_n - 1$ в совершенный код Васильева длины n такого же ранга.

Ключевые слова: система троек Штейнера, совершенный двоичный код, свитчинг, Паш-конфигурация, ijk-компонента, i-компонента.

Введение

Существует множество открытых вопросов, касающихся систем троек Штейнера (STS). Классификация STS(n) является одной из основных задач теории блок-схем. Известна классификация STS порядка не больше 19 [11, 13]. Открытым является вопрос о вложимости произвольной STS(n), $n = 2^r - 1,\ r > 4$, в некоторый совершенный двоичный код длины n. В [16] доказано, что только 33 из 80 неизоморфных STS(15) вложимы в двоичные совершенные коды (см. также [17]). В [21, 22] доказано, что все системы троек Штейнера STS(n), $n > 7$, ранга не более $r_n = n - \log(n+1) + 2$ (здесь и далее log обозначает логарифм по основанию 2) вложимы в некоторые совершенные коды длины n, но неясно, каким будет ранг таких кодов. Интересен вопрос соответствия различных конструкций для STS и для совершенных двоичных кодов, например, взаимосвязь свитчинговых и каскадных конструкций для данных

*)Исследование выполнено при частичной финансовой поддержке Российского фонда фундаментальных исследований (проект 12–01–00631–а) и поддержке ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009—2013 гг. (соглашение 8227).

объектов.

Пусть $\mathbb{F}^n$ — n-мерное метрическое пространство над полем Галуа $GF(2)$ с метрикой Хэмминга. Непустое множество C из $\mathbb{F}^n$ называется *двоичным кодом*, векторное подпространство в $\mathbb{F}^n$ — *двоичным линейным кодом*. Элементы C называются *кодовыми словами*. *Хэммингово расстояние* $d(x, y)$ между векторами x, y из $\mathbb{F}^n$ определяется числом координат, в которых x и y отличаются, *вес Хэмминга* $w(x)$ вектора $x \in \mathbb{F}^n$ — числом ненулевых координат x. Множество ненулевых координат $x \in \mathbb{F}^n$ называется *носителем* x и обозначается через $\mathrm{supp}(x)$. *Кодовым расстоянием* d_C кода C является наименьшее из расстояний Хэмминга между любой парой кодовых слов. Двоичный код C длины n называется *совершенным кодом, исправляющим одну ошибку* (далее, кратко, *совершенным*), если каждый вектор x из $\mathbb{F}^n$ находится на расстоянии 1 ровно от одного кодового слова C. Известно, что совершенные коды имеют следующие параметры: длина $n = 2^r - 1,\ r > 1$, число кодовых слов 2^{n-r}, кодовое расстояние 3. Линейный совершенный код длины n, называемый *кодом Хэмминга* H^n, единствен с точностью до эквивалентности. Известно, что все автоморфизмы пространства $\mathbb{F}^n$ задаются отображениями вида $(\pi, v) : x \to \pi(x) + v$, где $\pi \in S_n$ — перестановка координат, $v \in \mathbb{F}^n$. Два кода C и D из $\mathbb{F}^n$ называются *эквивалентными*, если существует автоморфизм пространства $\mathbb{F}^n$, переводящий код C в код D, т. е. $\pi(C) + v = D$ для некоторых $\pi \in S_n$ и $v \in \mathbb{F}^n$. Коды C и D из $\mathbb{F}^n$ называются *перестановочно эквивалентными*, если существует подстановка $\pi \in S_n$, переводящая код C в код D, т. е. $\pi(C) = D$.

Пусть R — подмножество совершенного двоичного кода C. *Свитчингом* множества R по i-й координате называется замена её значения во всех векторах из R. Получившееся в результате такого свитчинга множество будем обозначать через $R + i$ (его часто обозначают через $R + e_i$, где e_i — вектор веса 1 с ненулевой i-й координатой [2], но в целях более удобного изложения используем первое обозначение). Множество R называется *i-компонентой* совершенного кода C, если $K(R) = K(R + i)$, где $K(R)$ — множество всех векторов из $\mathbb{F}^n$, находящихся на расстоянии не больше 1 от R. В результате получим новый совершенный код $C' = (C \setminus R) \cup (R + i)$ с теми же параметрами, что и C, который зачастую не эквивалентен исходному совершенному коду. В этом случае говорят, что код C' получен из кода C *свитчингом* i-компоненты R. Пусть $\alpha \subseteq \{1, \ldots, n\}$. Множество R называется *α-компонентой* совершенного кода C, если R является i-компонентой для любого $i \in \alpha$. Если $\alpha = \{i_1, \ldots, i_k\}$, $k \geqslant 2$, то для множества, получившегося в результате

свитчинга множества R по координатам из α, будем для удобства использовать обозначение $R+(i_1,\ldots,i_k)$ вместо $R+i_1+\ldots+i_k$. Известно [19], что любой совершенный код длины n ранга r_n-1 является кодом Васильева [3], построенным свитчингами i-компонент (по одной координате) из кода Хэмминга с помощью некоторой функции $\lambda: H^{\frac{n-1}{2}} \to \{0,1\}$. Код Васильева V_λ^n может быть представлен с точностью до эквивалентности в виде

$$V_\lambda^n = \{(|x|+\lambda(y), x+y, x) \mid x \in \mathbb{F}^{\frac{n-1}{2}},\ y \in \mathcal{H}^{\frac{n-1}{2}}\} \qquad (1)$$

для некоторой функции $\lambda: \mathcal{H}^{\frac{n-1}{2}} \to \{0,1\}$. В общем случае [2] говорят, что код $C' = (C\backslash M)\cup M'$ *получен свитчингом* множества M на множество M' в двоичном коде C, если код C' имеет те же параметры, что и C. Такое множество M называется *компонентой* кода C.

Семейство 3-элементных подмножеств (называемых также *тройками* или *блоками*) базового множества $N=\{1,2,\ldots,n\}$ такое, что любое 2-элементное подмножество из N содержится ровно в одной тройке (3-элементном подмножестве) из N, называется *системой троек Штейнера порядка* n и обозначается через $\mathrm{STS}(n)$ или кратко STS, если не будет интересовать порядок системы. Известно, что $\mathrm{STS}(n)$ существует тогда и только тогда, когда $n \equiv 1,3 \pmod 6$. Каждому блоку (i,j,k) из $\mathrm{STS}(n)$ сопоставим вектор из $\mathbb{F}^n$ с единицами только в координатах с номерами i, j и k. Далее из контекста всегда будет ясно, рассматриваются блоки, носители или отвечающие им векторы. Понятие свитчинга для STS определяется аналогично понятию свитчинга для совершенного двоичного кода. Два множества R и R' из 3-элементных подмножеств множества N называются *равновесными*, если каждая пара элементов, которая может быть найдена в тройках одного множества, встречается также и в тройках другого множества [9]. Говорят, что $\mathrm{STS}'(n) = (\mathrm{STS}(n)\backslash R)\cup R'$ *получена свитчингом* множества блоков R на множество блоков R' в $\mathrm{STS}(n)$, если R и R' — равновесные множества [6, 9]. В [6] такое множество R (равно как и множество R') названо *компонентой*. Две STS называются *изоморфными*, если существует взаимно однозначное отображение их базовых множеств, переводящее все блоки одной системы в блоки другой. Нижняя и верхняя оценки числа $N(n)$ всех неизоморфных $\mathrm{STS}(n)$ [4, 15] имеют вид

$$(e^{-2}3^{-3/2}n)^{n^2/6} \leqslant N(n) \leqslant ((1+o(1))e^{-1/2}n)^{n^2/6}.$$

Известно, что совокупность носителей кодовых слов веса 3 в любом двоичном совершенном коде C длины n, содержащем нулевой вектор 0^n, определяет систему троек Штейнера порядка n [8]. Будем обозначать её

через $\mathrm{STS}(C, n)$. Хорошо известно, что система $\mathrm{STS}(H, n)$, отвечающая коду H^n, называемая *хэмминговой* STS, имеет ранг $r_n - 2$. *Рангом* $r(C)$ *кода* C (*рангом* STS) в векторном пространстве $\mathbb{F}^n$ размерности n над двоичным полем F называется размерность подпространства из $\mathbb{F}^n$, натянутого на код C (на STS). Известно, что конструкция Ассмуса и Маттсона для $\mathrm{STS}(n)$, $n = 2^r - 1$, соответствует конструкции Васильева [12]. В [20] приведено описание $\mathrm{STS}(n)$, $n = 2^r - 1$, $r > 3$, ранга $r_n - 1$ и найдено число таких различных STS. В [21, 22] рассмотрены $\mathrm{STS}(n)$, $n > 7$, ранга r_n и доказано, что они вложимы в совершенные коды длины n.

1. Конструкция систем троек Штейнера

Приведём свитчинговую конструкцию STS. Эти системы получены из хэмминговой STS такого же порядка применением к последней серий последовательных свитчингов. В качестве исходной конструкции рассмотрим следующий известный итеративный метод построения STS. Пусть $\mathrm{STS}(m)$ — произвольная STS порядка $m \equiv 1, 3 \pmod 6$, $m > 1$, на множестве $M = \{1, 2, 3, \ldots, m\}$. Пусть $\{i, j, k\}$ — множество чисел такое, что $M \cap \{i, j, k\} = \varnothing$, и пусть $N = \{1, 2, 3, \ldots, 4m + 3\}$, $m \equiv 1, 3 \pmod 6$, $m > 1$. В таблице

$$T = \begin{array}{|c|c|c|c|c|c|c|} \hline & 1 & 2 & \ldots & a & \ldots & m \\ \hline i & i_1 & i_2 & \ldots & i_a & \ldots & i_m \\ \hline j & j_1 & j_2 & \ldots & j_a & \ldots & j_m \\ \hline k & k_1 & k_2 & \ldots & k_a & \ldots & k_m \\ \hline \end{array}$$

первая строка соответствует множеству M, первый столбец — множеству $\{i, j, k\}$. Остальные элементы — числа $N \backslash (M \cup \{i, j, k\})$ — расположены в произвольном порядке. Для удобства изложения конструкции $\mathrm{STS}(4m + 3)$ обозначим элементы второй строки T через $i, i_1, i_2, \ldots, i_m$, третьей и четвёртой строк — через $j, j_1, j_2, \ldots, j_m$ и $k, k_1, k_2, \ldots, k_m$ соответственно. Используя T и её элементы, построим множество троек $S(T, n)$, где $n = 4m + 3$, и докажем, что оно является $\mathrm{STS}(n)$.

Возьмём произвольный элемент a из M, элементы столбца $(a\ i_a\ j_a\ k_a)^T$ в таблице T и множества $\{i, j, k\}$ и построим из них 6 троек

$$\{(i, j_a, k_a),\ (i, a, i_a),\ (j, a, j_a),\ (j, i_a, k_a),\ (k, i_a, j_a),\ (k, a, k_a)\}, \qquad (2)$$

которые включим в систему троек $S(T, n)$. Так как a — произвольный элемент множества M и $|M| = m$, в $S(T, n)$ включается $6m$ троек.

Далее, для каждой тройки $(a,b,c) \in \mathrm{STS}(m)$ рассмотрим таблицу

$$T_{abc} = \begin{array}{|c|c|c|} \hline a & b & c \\ \hline i_a & i_b & i_c \\ \hline j_a & j_b & j_c \\ \hline k_a & k_b & k_c \\ \hline \end{array},$$

являющуюся подтаблицей T. С помощью таблицы T_{abc} построим следующие 16 троек, включаемые в множество $S(T,n)$:

$$\begin{array}{cccc} (a,b,c), & (a,j_b,j_c), & (j_a,j_b,c), & (j_a,b,j_c), \\ (a,i_b,i_c), & (a,k_b,k_c), & (j_a,k_b,i_c), & (j_a,i_b,k_c), \\ (i_a,b,i_c), & (i_a,j_b,k_c), & (k_a,j_b,i_c), & (k_a,b,k_c), \\ (i_a,i_b,c), & (i_a,k_b,j_c), & (k_a,k_b,c), & (k_a,i_b,j_c). \end{array} \tag{3}$$

Поскольку $|\mathrm{STS}(m)| = m(m-1)/6$, получим $16 \times m(m-1)/6$ троек. Также в $S(T,n)$ включим тройку (i,j,k).

Из приведённого построения множества $S(T,n)$ несложно посчитать, что $|S(T,n)| = n(n-1)/6$. Все тройки в $S(T,n)$ различны. Действительно, любая пара элементов, встречающихся в одном столбце T, содержится в одной из троек (2) либо в $\{i,j,k\}$, каждая пара элементов из одной строки таблицы — в одной из троек (3). Любая пара элементов из разных строк и столбцов, содержащая один элемент из множества $\{i,j,k\}$, находится в одной из троек (2), а не содержащая ни одного из элементов $\{i,j,k\}$ — в одной из троек (3). Из конструкции легко видно, что все тройки различны и пересекаются друг с другом не более чем по одному элементу.

Утверждение 1. *Множество $S(T,n)$ является* $\mathrm{STS}(n)$, $n = 4m+3$.

Заметим, что приведённая конструкция является частным случаем конструкции I из [22].

Следствие 1. *Если* $\mathrm{STS}(m)$ *— хэммингова* STS, *то множество троек $S(T,n)$, $n = 4m+3$, является хэммингово́й* STS *порядка n.*

Приведём правила, позволяющие делать свитчинги в данной $\mathrm{STS}(n)$.

Правило $\mathcal{A}$. Для произвольного элемента $a \in M$ рассмотрим множество всех элементов из столбца $(a\ i_a\ j_a\ k_a)^T$ в T и множество $\{i,j,k\}$.

Правило $\mathcal{A}1$. Очевидно, что множество (2) вместе с тройкой (i,j,k) образует $\mathrm{STS}(7)$ — плоскость Фано. Известно, что множество (2) содер-

жит три известные Паш-конфигурации

$$P_1 = \{(i, j_a, k_a), (i, a, i_a), (j, a, j_a), (j, i_a, k_a)\},$$
$$P_2 = \{(i, j_a, k_a), (i, a, i_a), (k, i_a, j_a), (k, a, k_a)\},$$
$$P_3 = \{(j, a, j_a), (j, i_a, k_a), (k, i_a, j_a), (k, a, k_a)\},$$

где P_1 допускает свитчинг $i \leftrightarrow j$, P_2 — свитчинг $i \leftrightarrow k$, а P_3 — свитчинг $j \leftrightarrow k$. Например, для P_1 после свитчинга $i \leftrightarrow j$ получим равновесное множество $\{(j, j_a, k_a), (j, a, i_a), (i, a, j_a), (i, i_a, k_a)\}$. Заметим, что она кроме $i \leftrightarrow j$ допускает свитчинги $i_a \leftrightarrow j_a$ и $a \leftrightarrow k_a$, но все они преобразуют исходную Паш-конфигурацию в одно и то же множество из четырёх блоков. То же самое верно для P_2 и свитчингов $i \leftrightarrow k$, $a \leftrightarrow j_a$, $i_a \leftrightarrow k_a$, а также для P_3 и свитчингов $j \leftrightarrow k$, $a \leftrightarrow i_a$, $j_a \leftrightarrow k_a$. Поэтому в дальнейшем будем учитывать лишь свитчинг $i \leftrightarrow j$ в применении к P_1, а также свитчинги $i \leftrightarrow k$ и $j \leftrightarrow k$ в применении к P_2 и P_3 соответственно.

В результате применения подходящего свитчинга к одной из приведённых Паш-конфигураций получим множество, равновесное исходному множеству. Стало быть, существует 4 возможности для выбора множества из 6 троек, равновесного множеству (2), а именно:

$$\{(j, j_a, k_a),\ (j, a, i_a),\ (i, a, j_a),\ (i, i_a, k_a),\ (k, i_a, j_a),\ (k, a, k_a)\},$$
$$\{(k, j_a, k_a),\ (k, a, i_a),\ (j, a, j_a),\ (j, i_a, k_a),\ (i, i_a, j_a),\ (i, a, k_a)\},$$
$$\{(i, j_a, k_a),\ (i, a, i_a),\ (k, a, j_a),\ (k, i_a, k_a),\ (j, i_a, j_a),\ (j, a, k_a)\},$$

а также само множество (2). Заметим, что некоторый подходящий свитчинг, который переводит исходное множество (2) в равновесное ему, можно применить к каждому элементу a из множества M.

Правило $\mathcal{A}2$. Несложно заметить, что множество троек (2) вместе с тройкой (i, j, k) содержит четыре Паш-конфигурации

$$\Pi_1 = \{(i, j, k), (i, j_a, k_a), (j, a, j_a), (k, a, k_a)\},$$
$$\Pi_2 = \{(i, j, k), (i, j_a, k_a), (j, i_a, k_a), (k, i_a, j_a)\},$$
$$\Pi_3 = \{(i, j, k), (i, a, i_a), (j, a, j_a), (k, i_a, j_a)\},$$
$$\Pi_4 = \{(i, j, k), (i, a, i_a), (k, a, k_a), (j, i_a, k_a)\},$$

где Π_1 допускает свитчинг $j \leftrightarrow k_a$, Π_2 — свитчинг $j \leftrightarrow j_a$, Π_3 — свитчинг $k \leftrightarrow a$, а Π_4 — свитчинг $k \leftrightarrow i_a$. В результате применения подходящего свитчинга к одной из четырёх приведённых Паш-конфигураций получим множество, равновесное исходному множеству. Очевидно, что

существует 5 возможностей для выбора множества из 7 троек, равновесного множеству (2), объединённому с тройкой (i, j, k), а именно:

$$\{(i, k_a, k),\ (i, j_a, j),\ (i, a, i_a),\ (k_a, a, j_a),\ (j, i_a, k_a),\ (k, i_a, j_a),\ (k, a, j)\},$$
$$\{(i, j_a, k),\ (i, j, k_a),\ (i, a, i_a),\ (j, a, j_a),\ (j_a, i_a, k_a),\ (k, i_a, j),\ (k, a, k_a)\},$$
$$\{(i, j, a),\ (i, j_a, k_a),\ (i, k, i_a),\ (j, k, j_a),\ (j, i_a, k_a),\ (a, i_a, j_a),\ (k, a, k_a)\},$$
$$\{(i, j, i_a),\ (i, j_a, k_a),\ (i, a, k),\ (j, a, j_a),\ (j, k, k_a),\ (k, i_a, j_a),\ (i_a, a, k_a)\},$$

а также само множество $\{(i, j, k),\ (i, j_a, k_a),\ (i, a, i_a),\ (j, a, j_a),\ (j, i_a, k_a),\ (k, i_a, j_a),\ (k, a, k_a)\}$.

Заметим, что тройка (i, j, k) содержится в каждой указанной Паш-конфигурации. Тем самым после применения к этой Паш-конфигурации некоторого подходящего свитчинга построение множества $\{(i, j, k),\ (i, j_b, k_b),\ (i, b, i_b),\ (j, b, j_b),\ (j, i_b, k_b),\ (k, i_b, j_b),\ (k, b, k_b)\}$ для любого элемента $b \neq a$, становится невозможным в силу того, что тройка (i, j, k) после свитчинга преобразуется в другую тройку. Следовательно, приведённый свитчинг применим только к какому-то одному элементу a из M.

Правило $\mathcal{B}$. Рассмотрим следующие трансверсали из (3), представляемые в виде квадратной матрицы порядка 4:

$$\begin{aligned}
&\{(a, b, c),\ (a, k_b, k_c), (k_a, b, k_c), (k_a, k_b, c)\},\\
&\{(a, j_b, j_c),\ (a, i_b, i_c), (k_a, j_b, i_c), (k_a, i_b, j_c)\},\\
&\{(j_a, b, j_c),\ (j_a, k_b, i_c),\ (i_a, b, i_c),\ (i_a, k_b, j_c)\},\\
&\{(j_a, j_b, c),\ (j_a, i_b, k_c),\ (i_a, j_b, k_c),\ (i_a, i_b, c)\}.
\end{aligned} \tag{4}$$

Каждому из элементов множества $\{i, j, k\}$ сопоставим столбцы, строки и трансверсали из (3) по правилу: элементу i соответствуют столбцы, элементу j — строки, элементу k — трансверсали (4).

Далее будем действовать по одному из следующих трёх вариантов.

Правило $\mathcal{B}1$. Выберем элемент i, j или k и рассмотрим множество троек (3). Каждые строка и столбец приведённых шестнадцати троек являются Паш-конфигурациями и допускают свитчинги. Например, к строкам можно применить свитчинги $a \leftrightarrow j_a$, $a \leftrightarrow j_a$, $i_a \leftrightarrow k_a$, $i_a \leftrightarrow k_a$, к столбцам — $a \leftrightarrow i_a$, $a \leftrightarrow i_a$, $j_a \leftrightarrow k_a$, $j_a \leftrightarrow k_a$ соответственно. Более того, четыре приведённые трансверсали (4) также образуют Паш-конфигурации, которые допускают свитчинги $a \leftrightarrow k_a$, $a \leftrightarrow k_a$, $j_a \leftrightarrow i_a$, $j_a \leftrightarrow i_a$ соответственно. Ясно, что все тройки, полученные под действием приведённых свитчингов, различны. Поэтому получим шестнадцать

троек, разделяемых тремя различными способами на подмножества с четырьмя тройками в каждом, образующие Паш-конфигурации и допускающие свитчинг. Так как свитчинг данных шестнадцати троек, оставляющий их без изменения, учитывается три раза (по одному для каждого выбора элемента из множества $\{i, j, k\}$), а для подсчёта общего количества различных свитчингов нужно учесть лишь один из трёх повторов, получаем всего $3 \times 2^4 - 3 + 1 = 46$ различных свитчингов.

Правило $\mathcal{B}2$. Рассмотрим любой элемент из множества $\{i, j, k\}$, например j, и применим допустимые свитчинги (из $\mathcal{B}1$) сначала одновременно ко всем блокам, соответствующим этому элементу (т. е. к строкам), а затем — к некоторым блокам, соответствующим одному из оставшихся элементов множества $\{i, j, k\}$ (т. е. к столбцам или диагоналям). В результате получим множество, равновесное исходному множеству троек (3). Аналогично можно действовать с элементом i (k), т. е. со столбцами (диагоналями) матрицы блоков (3), применяя допустимые свитчинги сначала ко всем, а затем — к некоторым строкам или диагоналям (строкам или столбцам). В результате получим множество, равновесное исходному множеству (3). Таким образом, координата, по которой сдвигаются все 4 подмножества блоков из (3), может быть выбрана тремя способами, а координата, по которой сдвигается часть блоков, может быть выбрана двумя способами. Так как каждое из 4 подмножеств далее может быть либо сдвинуто, либо нет, для каждой из 6 пар выбранных направлений получаем 2^4 свитчингов. Следовательно, всего получаем $3 \times 2 \times 2^4 = 96$ свитчингов. Существует шесть способов, по которым можно применить свитчинги, учитываемые здесь каждый по два раза и в то же время совпадающие со свитчингами из правила $\mathcal{B}1$. Они либо оставляют без повторного изменения полностью сдвинутые в результате применения свитчингов из $\mathcal{B}1$ тройки (3), либо полностью их повторно сдвигают. В итоге получаем $96 - 12 = 84$ новых различных свитчинга.

Правило $\mathcal{B}3$. Выберем элемент i, j или k и снова рассмотрим множество троек (3). Пусть для определённости выбран элемент j. Тогда рассмотрим строки из (3), к которым применимы свитчинги $a \leftrightarrow j_a$ в подмножестве $\{(a, b, c), (a, j_b, j_c), (j_a, j_b, c), (j_a, b, j_c), (a, i_b, i_c), (a, k_b, k_c), (j_a, k_b, i_c), (j_a, i_b, k_c)\}$ и независимо $i_a \leftrightarrow k_a$ для троек $\{(i_a, b, i_c), (i_a, j_b, k_c), (k_a, j_b, i_c), (k_a, b, k_c), (i_a, i_b, c), (i_a, k_b, j_c), (k_a, k_b, c), (k_a, i_b, j_c)\}$. Будем выбирать свитчинг какого-то одного из двух приведённых подмножеств. После этого в каждом из двух множеств Паш-конфигураций

$$\{(a, b, c), (a, i_b, i_c), (i_a, b, i_c), (i_a, i_b, c)\},$$

$$\{(a, j_b, j_c), (a, k_b, k_c), (i_a, j_b, k_c), (i_a, k_b, j_c)\},$$
$$\{(j_a, j_b, c), (j_a, k_b, i_c), (k_a, j_b, i_c), (k_a, k_b, c)\},$$
$$\{(j_a, b, j_c), (j_a, i_b, k_c), (k_a, b, k_c), (k_a, i_b, j_c)\},$$

$$\{(a, b, c), (a, k_b, k_c), (k_a, b, k_c), (k_a, k_b, c)\},$$
$$\{(a, j_b, j_c), (a, i_b, i_c), (k_a, j_b, i_c), (k_a, i_b, j_c)\},$$
$$\{(j_a, b, j_c),\ (j_a, k_b, i_c),\ (i_a, b, i_c),\ (i_a, k_b, j_c)\},$$
$$\{(j_a, j_b, c), (j_a, i_b, k_c), (i_a, j_b, k_c), (i_a, i_b, c)\}$$

(или отвечающих им множеств троек, полученных в результате свитчингов указанных подмножеств троек) можно повторно произвести независимые свитчинги $c \leftrightarrow i_c$, $c \leftrightarrow i_c$, $j_c \leftrightarrow k_c$ и $j_c \leftrightarrow k_c$, либо $c \leftrightarrow k_c$, $i_c \leftrightarrow j_c$, $i_c \leftrightarrow j_c$ и $c \leftrightarrow k_c$ соответственно. То же самое можно проделать, выбрав в качестве исходного элемента для свитчинга элемент i (или k), и производя повторные свитчинги в строках или диагоналях (строках или столбцах) соответственно. В результате снова получим множество, равновесное исходному множеству троек (3). Таким образом, первоначальное направление для сдвига может быть выбрано тремя способами. Далее, двумя способами можно выбрать одно из двух подмножеств из восьми блоков. Для повторного свитчинга можно выбрать одно из двух существующих множеств из 16 блоков, которые разбиты на четыре подмножества из четырёх блоков в каждом. Каждое из этих четырёх имеющихся подмножеств в выбранном множестве может быть либо сдвинуто, либо оставлено без изменения. Поэтому для выбранного множества из 16 блоков получаем 2^4 свитчингов. Следовательно, всего получаем $3 \times 2 \times 2 \times 2 \times 2^4 = 192$ свитчинга. Существуют три способа свитчингов, которые совпадают со свитчингами из правила $\mathcal{B}1$. Они оставляют без повторного изменения сдвинутые в результате первого применения свитчинга 16 троек. Эти свитчинги отвечают каждому из элементов i, j, k и учитываются каждый по четыре раза. С учётом этих повторов получаем $192 - 12 = 180$ новых различных свитчингов.

Теорема 1. *Множество, полученное свитчингами из $S(T, n)$ по правилу $\mathcal{A}1$ или $\mathcal{A}2$ с одним из правил $\mathcal{B}1$, $\mathcal{B}2$ или $\mathcal{B}3$, является* STS(n).

Следствие 2. *Число различных* STS(n), $n = 4m + 3$, *полученных из фиксированной таблицы, отвечающей* STS(m) *и множеству $\{i, j, k\}$, по правилам $\mathcal{A}1$ или $\mathcal{A}2$ с одним из правил $\mathcal{B}1$, $\mathcal{B}2$ или $\mathcal{B}3$, равно*

$$((n + 1) \cdot 2^{(n-7)/2} + n - 3) \cdot 310^{(n-3)(n-7)/3 \cdot 2^5}.$$

Доказательство. Подсчитаем число указанных различных STS, вернувшись к конструкции $\mathrm{STS}(n)$, приведённой выше. По правилу $\mathcal{A}1$ для каждого столбца T кроме первого можно независимо построить четыре различных Паш-конфигурации на элементах $\{a, i_a, j_a, k_a\}$. Следовательно, имеем 4^m различных возможностей выбрать тройки на столбцах T. По правилу $\mathcal{A}2$ дополнительно существует $4m$ вариантов выбора троек на столбцах T. С учётом комбинаций правил $\mathcal{A}1$ и $\mathcal{A}2$ получаем всего $4^m + 4m + 4m \cdot 4^{m-1} = 4^m(m+1) + 4m = (n+1) \cdot 2^{(n-7)/2} + n - 3$ возможностей выбрать тройки на столбцах T.

Далее, для каждой тройки $(a, b, c) \in \mathrm{STS}(m)$ с учётом приведённых рассуждений получаем $46 + 84 + 180 = 310$ различных свитчингов по правилам $\mathcal{B}1$, $\mathcal{B}2$ и $\mathcal{B}3$. Таким образом, существует по крайней мере $310^{|\mathrm{STS}(m)|} = 310^{(n-3)(n-7)/3\cdot 2^5}$ различных возможных свитчингов. С учётом того, что свитчинги можно применять независимо, получаем

$$((n+1) \cdot 2^{(n-7)/2} + n - 3) \cdot 310^{(n-3)(n-7)/3\cdot 2^5}$$

различных STS, которые можно построить из фиксированной $\mathrm{STS}(m)$ и множества $\{i, j, k\}$. Следствие 2 доказано.

Следствие 3. *Число различных* $\mathrm{STS}(n)$, $n = 4m + 3$, *полученных из фиксированной таблицы, отвечающей* $\mathrm{STS}(m)$ *и множеству* $\{i, j, k\}$, *по правилу*$\mathcal{A}1$ *в сочетании с одним из правил* $\mathcal{B}1$ *или* $\mathcal{B}2$, *равно* $2^{(n-3)/2} \cdot 130^{(n-3)(n-7)/3\cdot 2^5}$.

Найдём нижнюю оценку числа систем $\mathrm{STS}(n)$, которые можно получить с помощью приведённой конструкции.

Теорема 2. *Для числа* $R(n)$ *различных систем* $\mathrm{STS}(n)$, $n = 4m + 3$, $m \geqslant 3$, *построенных с помощью приведённой конструкции, верна оценка*

$$R(n) \geqslant (((n+1) \cdot 2^{(n-5)/2} + 2n - 6) \times 310^{(n^2-10n+21)/3\cdot 2^5} - 3n + 9) \cdot n(n-1)/12 \cdot R((n-3)/4)$$

Доказательство. Число $R(n)$ различных систем $\mathrm{STS}(n)$, $n = 4m+3$, удовлетворяет неравенству $R(n) \geqslant P(n) \cdot R(m)$, где $P(n)$ — число различных $\mathrm{STS}(n)$, полученных из фиксированной таблицы T и фиксированной базовой системы $\mathrm{STS}(m)$, $R(m)$ — число различных $\mathrm{STS}(m)$ порядка m. Найдём оценку снизу для $P(n)$.

Заметим, что $\mathrm{STS}(n)$, получающиеся из различных $\mathrm{STS}(m)$ с помощью различных свитчингов, различны. Действительно, предположим, что $S_1(n)$ и $S_2(n)$ — одинаковые $\mathrm{STS}(n)$, полученные из различных STS

$S_1(m)$ и $S_2(m)$ порядка m с помощью различных свитчингов по приведённым правилам. Тогда существуют такие различные элементы a, b, c, d из множества M, что $(a, b, c) \in S_1(m)$ и $(a, b, d) \in S_2(m)$. Для равенства систем $S_1(n)$ и $S_2(n)$ необходимо, чтобы два набора из 16 троек, аналогичные (3) и построенные с помощью подтаблиц исходной таблицы размера 3×3, которые отвечают тройкам (a, b, c) и (a, b, d), могли быть получены один из другого свитчингами вида $c \leftrightarrow d$, $i_c \leftrightarrow i_d$, $j_c \leftrightarrow j_d$, $k_c \leftrightarrow k_d$. Но правила $\mathcal{A}$ и $\mathcal{B}$ допускают свитчинги элементов вида c, i_c, j_c, k_c лишь из одного столбца исходной таблицы и не допускают свитчингов между элементами вида c, i_c, j_c, k_c и d, i_d, j_d, k_d из разных столбцов исходной таблицы. Следовательно, из разных $\mathrm{STS}(m)$ с помощью разных свитчингов по приведённым правилам не могут быть получены одинаковые системы троек порядка n.

С учётом следствия 2 и того факта, что в качестве $\{i, j, k\}$ можно выбирать любую тройку из $S(T, n)$, получаем

$$((n+1) \cdot 2^{(n-7)/2} + n - 3) \cdot 310^{(n^2-10n+21)/3 \cdot 2^5} \cdot n(n-1)/6 \cdot R((n-3)/4)$$

систем порядка n. Среди них могут оказаться совпадающие. Изучим эти ситуации.

Рассмотрим произвольную $\mathrm{STS}(n)$, отвечающую фиксированной таблице и фиксированной $\mathrm{STS}(m)$. При различных разбиениях $\mathrm{STS}(n)$ на компоненты и дальнейшем применении к ней свитчингов по правилам $\mathcal{A}1$, $\mathcal{B}1$ или $\mathcal{B}2$ могут образовываться одинаковые $\mathrm{STS}(n)$. Рассмотрим подробнее процесс образования таких систем.

Зафиксируем некоторую тройку $(i, j, k) \in \mathrm{STS}(n)$, любой элемент из этой тройки, например i, и произвольный элемент $a \in M$. В этом случае несложно заметить, что система, полученная из исходной $\mathrm{STS}(n)$ по правилу $\mathcal{A}1$ с помощью свитчинга $j \leftrightarrow k$, применённого ко всем тройкам, содержащим элементы j или k, в сочетании с правилом $\mathcal{B}1$ с помощью свитчинга $a \leftrightarrow i_a$, применённого ко всем оставшимся тройкам, содержащим элементы a или i_a, совпадает с системой, полученной из исходной $\mathrm{STS}(n)$ по правилу $\mathcal{A}1$ с помощью свитчинга $a \leftrightarrow i_a$, применённого ко всем тройкам, содержащим элементы a или i_a.

Заметим также, что система, полученная из исходной $\mathrm{STS}(n)$ с помощью свитчинга $j \leftrightarrow k$, применённого ко всем тройкам, содержащим элементы j или k, по правилу $\mathcal{A}1$, в сочетании со свитчингом $j_a \leftrightarrow k_a$, применённым ко всем оставшимся тройкам, содержащим элементы j_a или k_a, по правилу $\mathcal{B}1$, совпадает с $\mathrm{STS}(n)$, полученной из исходной с помощью свитчинга $j_a \leftrightarrow k_a$, применённого ко всем тройкам, содержащим элементы j_a или k_a, по правилу $\mathcal{A}1$. Таким образом, для выбранного элемента i

некоторой фиксированной тройки получаем 2 повторения. Аналогичные рассуждения верны для оставшихся элементов j и k тройки (i,j,k) и для всех оставшихся $m-1$ элементов из M.

Следовательно, в случае разбиения $\mathrm{STS}(n)$ на ijk-компоненты существует $3\cdot 2\cdot m = 6m$ повторов. Так как в качестве тройки (i,j,k) для разбиения $\mathrm{STS}(n)$ на ijk-компоненты может быть выбрана любая из $n(n-1)/6$ троек системы $\mathrm{STS}(n)$, всего получаем $\frac{n(n-1)}{6}\cdot 6m = mn(n-1) = \frac{n(n-1)(n-3)}{4}$ повторений. Учитывая подсчитанное выше число $\mathrm{STS}(n)$, включающее одинаковые, нижняя оценка числа $P(n)$ различных $\mathrm{STS}(n)$, построенных из фиксированных таблицы T и базовой системы $\mathrm{STS}(m)$ с помощью приведённой конструкции, принимает вид

$$P(n) \geqslant (((n+1)\cdot 2^{(n-5)/2}+2n-6)\cdot 310^{(n^2-10n+21)/3\cdot 2^5}-3n+9)\cdot n(n-1)/12.$$

Отсюда с учётом того, что $n = 4m+3$, получаем требуемую оценку. Теорема 2 доказана.

Следует заметить, что ранг таких $\mathrm{STS}(n)$ зависит от ранга $\mathrm{STS}\left(\frac{n-3}{4}\right)$ и потому может превышать r_n.

Следствие 4. *Для ранга* $r(\mathrm{STS}(n))$ *системы* $\mathrm{STS}(n)$, *построенной по конструкции теоремы* 2 *из некоторой* $\mathrm{STS}\left(\frac{n-3}{4}\right)$, *справедлива оценка*

$$r\left(\mathrm{STS}\left(\frac{n-3}{4}\right)\right) + \frac{3(n-3)}{4} + 1 \leqslant r(\mathrm{STS}(n)) \leqslant r\left(\mathrm{STS}\left(\frac{n-3}{4}\right)\right) + \frac{3(n-3)}{4} + 3.$$

2. Вложимость $S(T,n)$ в совершенный код

Свитчинговые методы (метод α-компонент и метод i-компонент) позволяют строить широкие классы совершенных кодов с различными свойствами [18]. Мы используем метод ijk-компонент, который является частным случаем метода α-компонент [2]. Для полноты изложения напомним краткое описание этого метода. Пусть H^n — код Хэмминга длины n, x — вектор из H^n веса 3, $\mathrm{supp}(x) = \{i,j,k\}$. Подпространство, порождённое совокупностью векторов веса 3 кода H^n с единичной i-й координатой, обозначим через R_i. Через R_{ij} и R_{ijk} обозначим подпространства, натянутые на R_i, R_j и на R_i, R_j, R_k соответственно.

Утверждение 2. *Пусть* $(i,j,k) \in \mathrm{STS}(H,n)$. *Тогда* $R_{ij} = R_{ik} = R_{jk} = R_{ijk}$.

Пусть $N_1 = 2^{\frac{n-3}{4}}$, $N_2 = 2^{\frac{n+5}{4}-\log(n+1)}$.

Утверждение 3. *Множество R_{ijk} является ijk-компонентой и представимо в виде $R_{ijk} = \bigcup\limits_{l=1}^{N_1} R_i^l$, где R_i^l — различные непересекающиеся i-компоненты, $R_i^1 = R_i$. То же верно для j и k.*

Утверждение 4. *Код H^n представим в виде $H^n = \bigcup\limits_{t=1}^{N_2} R_{ijk}^t$, где R_{ijk}^t — различные непересекающиеся ijk-компоненты, $R_{ijk}^1 = R_{ijk}$.*

Рассмотрим произвольную функцию $\nu : \{1, 2, \ldots, N_2\} \to \{i, j, k\}$. Через $R_{\nu(t)}$ обозначим $\nu(t)$-компоненту для $t \in \{1, 2, \ldots, N_2\}$.

Утверждение 5. *Код H^n представим в виде $H^n = \bigcup\limits_{t=1}^{N_2} \bigcup\limits_{l=1}^{N_1} R_{\nu(t)}^l$, где $R_{\nu(t)}^l$ — различные непересекающиеся $\nu(t)$-компоненты, $R_{\nu(t)}^1 = R_{\nu(t)}$.*

Рассмотрим функцию $\lambda : \{1, 2, \ldots, N_2\} \times \{1, 2, \ldots, N_1\} \to \{0, 1\}$. Напомним, что *множеством $R_{\nu(t)} + \nu(t)$, полученным свитчингом* из множества $R_{\nu(t)}$ по $\nu(t)$-й координате, $t \in \{1, 2, \ldots, N_2\}$, называется множество, полученное заменой значений $\nu(t)$-й координаты всех векторов $R_{\nu(t)}$ противоположными.

Утверждение 6. *Множество $C_{\lambda,\nu} = \bigcup\limits_{t=1}^{N_2} \bigcup\limits_{l=1}^{N_1} \big(R_{\nu(t)}^l + \nu(t)\lambda(t,l)\big)$ является совершенным кодом.*

Пусть π — циклическая перестановка чисел i, j и k, μ — произвольная функция из множества $\{1, 2, \ldots, N_2\}$ в множество $\{0, 1\}$, $P_{\lambda,\nu}^t$ — множество векторов вида $\bigcup\limits_{l=1}^{N_1} \big(R_{\nu(t)}^l + \nu(t)\lambda(t,l)\big)$.

Теорема 3 [2]. *Множество $C_{\lambda,\nu,\mu} = \bigcup\limits_{t=1}^{N_2} P_{\lambda,\nu}^t + \mu(t)\pi(\nu(t))$ является совершенным кодом.*

Из утверждения 3 (см. также [2]) следует, что код H^n представим в виде $H^n = \bigcup\limits_{\alpha \in H'} R_{ijk}^\alpha$, где $R_{ijk}^\alpha = R_{ijk} + \alpha$, H' — подкод Хэмминга размерности $\frac{n-3}{4} - \log(\frac{n+1}{4})$ кода H^n размерности $n - \log(n+1)$, R_{ijk} содержит нулевой вектор. Опишем векторы веса 3 в R_{ijk}.

Из определения R_i, R_j и R_k имеем

$$R_i = \{(i,j,k),\ (i,a_p,i_{a_p}),\ p=1,\dots,(n-3)/2\},$$
$$R_j = \{(i,j,k),\ (j,a_p,j_{a_p}),\ p=1,\dots,(n-3)/2\},$$
$$R_k = \{(i,j,k),\ (k,a_p,k_{a_p}),\ p=1,\dots,(n-3)/2\}$$

для некоторого a_p. Для векторов веса 3 кода Хэмминга справедливо

Утверждение 7 [1]. *Пусть* $(i,j,k) \in \mathrm{STS}(H^n)$. *Множество троек из* $\mathrm{STS}(H^n)\backslash(i,j,k)$, *содержащих элемент* i, *разбивается на* $(n-3)/4$ *пар троек* $(i,a,b),(i,c,d)$ *таких, что* $(j,a,c),(j,b,d)$ *и* $(k,a,d),(k,b,c)$ *принадлежат* $\mathrm{STS}(H^n)$.

Докажем, что свитчинги i- (j- или k-)компонент из компоненты R_{ijk} (R^{α}_{ijk}) в коде H^n соответствуют свитчингам по правилу $\mathcal{A}1$ (по правилу $\mathcal{B}1$ или $\mathcal{B}2$), применённому к $\mathrm{STS}(H,n)$.

Далее для определённости разбиваем R_{ijk} на i-компоненты, те же рассуждения можно провести для j- и k-компонент. Таким образом, множество R_i (из утверждения 2) содержит $(n-1)/2$ троек $\{(i,j,k),(i,a_p,i_{a_p}),(i,j_{a_p},k_{a_p}),\ a_p \in \{1,\dots,m\}\}$. Представляя оставшиеся компоненты R^l_i, $l=2,\dots,N_1$, в виде $R^l_i = R_i + (j,a_l,j_{a_l})$, получим, что каждая компонента R^l_i содержит четыре тройки (j,a_l,j_{a_l}), $(j,k_{a_l},i_{a_l}),(k,j_{a_l},i_{a_l}),(k,a_l,k_{a_l})$ (т. е. последнюю Паш-конфигурацию из (3)), где i_{a_l}, j_{a_l}, k_{a_l} определены из условий $(i,a_l,i_{a_l}) \in R_i, (j,a_l,j_{a_l}) \in R_j, (k,a_l,k_{a_l}) \in R_k$.

Векторы веса 3 совершенного двоичного кода длины n образуют систему $\mathrm{STS}(n)$ только в случае, если нулевой вектор 0^n принадлежит коду. Поэтому нельзя сдвигать компоненту R_{ijk} ни по одной из i, j, k координат. По этой же причине компоненту R_i нельзя сдвигать по i-й координате. Остальные компоненты R^l_i, $l>1$, можно сдвигать по i-й координате согласно функции λ. При сдвиге R^l_i, $l>1$, при переходе от компоненты R^l_i к $R^l_i + i = R_i + (i,j,a_l,j_{a_l})$ получаются следующие тройки:

$$\{(j,a_l,j_{a_l}),(j,k_{a_l},i_{a_l}),(k,j_{a_l},i_{a_l}),(k,a_l,k_{a_l})\} \subset R^l_i$$
$$\to \{(k,a_l,j_{a_l}),(k,k_{a_l},i_{a_l}),(j,j_{a_l},i_{a_l}),(j,a_l,k_{a_l})\} \subset R^l_i + i,$$

что соответствует свитчингу $j \leftrightarrow k$, применённому к последней Паш-конфигурации из (3). Нетрудно понять, что множества R_j и R_k содержат по $(n-1)/2$ троек:

$$\{(i,j,k),(j,a_p,j_{a_p}),(j,i_{a_p},k_{a_p}),a_p \in \{1,\dots,m\}\} \subset R_j,$$
$$\{(i,j,k),(k,a_p,k_{a_p}),(k,i_{a_p},j_{a_p}),a_p \in \{1,\dots,m\}\} \subset R_k.$$

Пусть $R_j^l = R_j + (i, a_l, i_{a_l})$, $R_k^l = R_k + (i, a_l, i_{a_l})$, $l > 1$. Тогда R_j^l содержит четыре тройки $(i, a_l, i_{a_l}), (i, j_{a_l}, k_{a_l}), (k, j_{a_l}, i_{a_l}), (k, a_l, k_{a_l})$, R_k^l — четыре тройки $(i, a_l, i_{a_l}), (i, j_{a_l}, k_{a_l}), (j, i_{a_l}, k_{a_l}), (j, a_l, j_{a_l})$, где i_{a_l}, j_{a_l}, k_{a_l} определены из условий $(i, a_l, i_{a_l}) \in R_i, (j, a_l, j_{a_l}) \in R_j, (k, a_l, k_{a_l}) \in R_k$. Тогда тройки, полученные при сдвигах R_j^l и R_k^l, $l > 1$, когда R_j^l переходит в $R_j^l + j = R_j + (i, j, a_l, i_{a_l})$, а R_k^l — в $R_k^l + k = R_k + (i, k, a_l, i_{a_l})$, выглядят следующим образом:

$$\{(i, a_l, i_{a_l}), (i, j_{a_l}, k_{a_l}), (k, j_{a_l}, i_{a_l}), (k, a_l, k_{a_l})\} \subset R_j^l$$
$$\to \{(k, a_l, i_{a_l}), (k, j_{a_l}, k_{a_l}), (i, j_{a_l}, i_{a_l}), (i, a_l, k_{a_l})\} \subset R_j^l + j,$$

$$\{(i, a_l, i_{a_l}), (i, j_{a_l}, k_{a_l}), (j, i_{a_l}, k_{a_l}), (j, a_l, j_{a_l})\} \subset R_k^l$$
$$\to \{(j, a_l, i_{a_l}), (j, j_{a_l}, k_{a_l}), (i, i_{a_l}, k_{a_l}), (i, a_l, j_{a_l})\} \subset R_k^l + k,$$

что соответствует свитчингам $i \leftrightarrow k$ и $i \leftrightarrow j$, применённым ко второй и первой Паш-конфигурациям из (3) соответственно. Таким образом, убеждаемся, что свитчинги i- (j- или k-)компоненты из R_{ijk} отвечают правилу $\mathcal{A}1$ приведённой в разд. 2 конструкции, если исходная система троек хэммингова.

Рассмотрим тройки из $R_{ijk}^\alpha, \alpha \neq 0$. Компоненту R_{ijk}^α можно представить в виде $R_{ijk}^\alpha = R_{ijk} + (a, b, c)$ для некоторой $(a, b, c) \in H'$. Каждая такая компонента содержит 16 троек, разбитых на подмножества. В каждом подмножестве содержится по 4 тройки из разных i-компонент (для определённости разбиваем R_{ijk}^α на i-компоненты, которые обозначим через $R_i^{\alpha 1}, \ldots, R_i^{\alpha 4}$; то же для j и k). Тройки выглядят следующим образом:

$$\{(a, b, c), (a, i_b, i_c), (i_a, b, i_c), (i_a, i_b, c)\} \subset R_i^{\alpha 1},$$
$$\{(a, j_b, j_c), (i_a, k_b, j_c), (a, k_b, k_c), (i_a, j_b, k_c)\} \subset R_i^{\alpha 4},$$
$$\{(j_a, j_b, c), (k_a, k_b, c), (j_a, k_b, i_c), (k_a, j_b, i_c)\} \subset R_i^{\alpha 2},$$
$$\{(j_a, b, j_c), (k_a, i_b, j_c), (j_a, i_b, k_c), (k_a, b, k_c)\} \subset R_i^{\alpha 3},$$

где i_s, j_s, k_s, $s \in \{a, b, c\}$ определяются из условий $(i, s, i_s) \in R_i$, $(j, s, j_s) \in R_j$, $(k, s, k_s) \in R_k$, т. е. получили в точности систему блоков (3), столбцы которой совпадают с i-компонентами, строки и диагонали системы (3) отвечают j- и k-компонентам соответственно. Каждый из полученных столбцов (строк, диагоналей) можно сдвигать по соответствующей координате или оставлять на месте в соответствии с функцией λ. Опишем тройки, полученные при сдвиге, например, $R_i^{\alpha 1}$, когда $R_i^{\alpha 1}$ преобразуется

в $R_i^{\alpha 1} + i$:

$$\{(a,b,c),(a,i_b,i_c),(i_a,b,i_c),(i_a,i_b,c)\} \subset R_i^{\alpha 1} \\ \to \{(i_a,b,c),(i_a,i_b,i_c),(a,b,i_c),(a,i_b,c)\} \subset R_i^{\alpha 1} + i,$$

т. е. векторы веса 3 из $R_i + i$ могут быть получены из компоненты R_i при помощи свитчинга $a \leftrightarrow i_a$. Проводя аналогичные рассуждения для оставшихся столбцов, в общем случае получим, что векторы веса 3 компонент $R_i^l + i$, $R_i^l + (i,j)$ и $R_i^l + (i,k)$, $l = 1,\dots,4$, могут быть получены из векторов веса 3 компоненты R_i^l при помощи свитчингов $a \leftrightarrow i_a, j_a \leftrightarrow k_a$ и $a \leftrightarrow k_a, i_a \leftrightarrow j_a$, а также $a \leftrightarrow j_a, i_a \leftrightarrow k_a$ соответственно. Аналогичные рассуждения можно провести для j- и k-компонент. Заметим, что приведённые свитчинги соответствуют правилу $\mathcal{B}1$ конструкции из разд. 1. Каждую из компонент R_{ijk}^{α}, $\alpha \neq 0^n$, можно сдвигать в соответствии с функцией μ по координате с номером $\pi(\nu)$: $R_{ijk}^{\alpha} \to R_{ijk}^{\alpha} + \pi(\nu)$. Опишем векторы веса 3, которые получаются при сдвиге R_{ijk}^{α}, когда $\pi(\nu) = j$:

$$\{(a,b,c),(a,i_b,i_c),(i_a,b,i_c),(i_a,i_b,c)\} \subset R_i^{\alpha 1} \\ \to \{(j_a,b,c),(j_a,i_b,i_c),(k_a,b,i_c),(k_a,i_b,c)\} \subset R_i^1 + \pi(\nu),$$

$$\{(j_a,j_b,c),(k_a,k_b,c),(j_a,k_b,i_c),(k_a,j_b,i_c)\} \subset R_i^{\alpha 2} \\ \to \{(a,j_b,c),(a,k_b,i_c),(i_a,k_b,c),(i_a,j_b,i_c)\} \subset R_i^2 + \pi(\nu),$$

$$\{(j_a,b,j_c),(k_a,i_b,j_c),(j_a,i_b,k_c),(k_a,b,k_c)\} \subset R_i^{\alpha 3} \\ \to \{(j_a,j_b,j_c),(j_a,k_b,k_c),(k_a,j_b,k_c),(k_a,k_b,j_c)\} \subset R_i^3 + \pi(\nu),$$

$$\{(a,j_b,j_c),(i_a,k_b,j_c),(a,k_b,k_c),(i_a,j_b,k_c)\} \subset R_i^{\alpha 4} \\ \to \{(a,b,j_c),(a,i_b,k_c),(i_a,b,k_c),(i_a,i_b,j_c)\} \subset R_i^4 + \pi(\nu),$$

т. е. получили систему троек (3), к которым применены свитчинги $a \leftrightarrow j_a$, $i_a \leftrightarrow k_a$.

Полученные строки (столбцы, диагонали) сдвинутой ijk-компоненты можно, в свою очередь, сдвигать по другой координате (ν или $\pi^2(\nu)$) или оставлять на месте в соответствии с функцией λ. Например,

$$\{(a,b,c),(a,i_b,i_c),(i_a,b,i_c),(i_a,i_b,c)\} \subset R_i^{\alpha 1} \\ \to \{(k_a,b,c),(k_a,i_b,i_c),(j_a,b,i_c),(j_a,i_b,c)\} \subset R_i^{\alpha 1} + (i,j),$$

т. е. векторы веса 3 из $R_i^{\alpha 1} + (i,j)$ могут быть получены из компоненты $R_i^{\alpha 1}$ свитчингами $a \leftrightarrow k_a$, $i_a \leftrightarrow j_a$ (что соответствует правилу $\mathcal{B}2$ приведённой в разд. 2 конструкции STS). Таким образом, справедлива

Лемма 1. *Класс* $\mathrm{STS}(n)$, $n = 4m + 3$, *полученный свитчингами по правилам* $\mathcal{A}1$, $\mathcal{B}1$ *и* $\mathcal{B}2$, *применённым к* $\mathrm{STS}(H, n)$, *описанной в следствии* 1, *совпадает с классом троек* $\mathrm{STS}(n)$, *вложимых в совершенные двоичные коды, построенные методом* ijk*-компонент из кода Хэмминга* H^n.

Из леммы 1 непосредственно вытекает

Следствие 5. *Системы* $\mathrm{STS}(n)$, $n = 4m+3$, *полученные свитчингами по правилам* $\mathcal{A}2$ *и* (*или*) $\mathcal{B}3$ (*в сочетании с правилами* $\mathcal{B}1$, $\mathcal{B}2$ *или* $\mathcal{A}1$ *соответственно*), *применёнными к* $\mathrm{STS}(H, n)$, *не вложимы в совершенные коды, построенные свитчингами* ijk*-компонент из кода Хэмминга* H^n.

3. Число различных $\mathrm{STS}(n)$ рангов $r_n - 1$ и r_n, вложимых в совершенные двоичные коды

Используя приведённую выше конструкцию, найдём оценки числа различных $\mathrm{STS}(n)$, вложимых в совершенные двоичные коды длины n, построенные методом свитчингов ijk-компонент из кода Хэмминга.

Порядок группы автоморфизмов произвольной $\mathrm{STS}(n)$, $n = 2^r - 1$, $r > 3$, меньше порядка группы автоморфизмов STS кода H^n [10]. По этой причине ограничимся нахождением нижней границы числа различных $\mathrm{STS}(n)$, так как нижняя оценка числа таких неизоморфных систем может быть легко получена из первой.

Известно (см., например, [8, гл. 13]), что порядок группы симметрий кода $\mathcal{H}^n$ равен

$$|\mathrm{Sym}(H, n)| = n(n-1)(n+1-2^2)(n+1-2^3)\cdot\ldots\cdot(n+1)/2.$$

Через $R(H, n)$ обозначим число различных $\mathrm{STS}(H, n)$ порядка n. Тогда

$$R(\mathcal{H}, n) = n!/|\mathrm{Sym}(\mathcal{H}^n)|.$$

Известно, что ранг любого кода Васильева V_λ^n (следовательно, и ранг его $\mathrm{STS}(n)$, полученной свитчингами i-компонент из $\mathrm{STS}(H, n)$), не превосходит $r_n - 1$. Согласно [19] любой совершенный код C длины n ранга не больше $r_n - 1$ является кодом Васильева, полученным из некоторого двоичного кода H^n свитчингами i-компонент. На основе этого факта, известной конструкции Ассмуса — Маттсона [12] для STS, вложимых в коды Васильева, а также сопоставляя с полученным в [20] числом различных $\mathrm{STS}(n)$ ранга не больше $r_n - 1$, можно сделать вывод, что справедлива следующая теорема (заметим, что она является аналогом соответствующего результата для систем четвёрок Штейнера из [5], использующей

каскадные методы доказательства в отличие от свитчинговых методов данной статьи).

Теорема 4. *Любая* $\mathrm{STS}(n)$, $n \geqslant 15$, *ранга* $r_n - 1$ *вложима в совершенный код длины* n *такого же ранга, а именно, в код Васильева* V_λ^n. *Число* $R_1(n)$ *таких различных* $\mathrm{STS}(n)$ *равно*

$$R_1(n) = \left(2^{|\mathrm{STS}(\frac{n-1}{2})| - \frac{n-1}{2}} - \frac{2}{n+1}\right) \cdot n! / \left|\mathrm{Sym}\left(\mathcal{H}^{\frac{n-1}{2}}\right)\right|.$$

Доказательство. Пусть A — матрица инцидентности некоторой $\mathrm{STS}(H, n)$, $n = 2^r - 1$. Тогда согласно [20] матрица G, состоящая из строк матрицы A и вектора $(1, 0, 0, \ldots, 0)$, является порождающей матрицей кода C, содержащего $2^{\frac{(n-1)(n-3)}{24}} 2^{|\mathrm{STS}(\frac{n-1}{2})|}$ различных $\mathrm{STS}(n)$ ранга не более $r_n - 1$, и существует всего

$$\frac{n!}{2^{\frac{n-1}{2}} \cdot (\frac{n-1}{2}) \cdot (\frac{n+1}{2} - 2) \cdot \ldots \cdot (\frac{n+1}{4})} = \frac{n!}{2^{\frac{n-1}{2}} \cdot |\mathrm{Sym}(\mathcal{H}^{\frac{n-1}{2}})|}$$

таких различных кодов.

Докажем, что каждая STS из кода C вложима в некоторый код Васильева V_λ^n длины n такого же ранга. Поскольку согласно [19] любой совершенный код длины n ранга не более $r_n - 1$ является кодом Васильева, построенным из кода $H^{(n-1)/2}$ с помощью нелинейной функции λ, получим вложимость всякой STS из кода C в некоторый совершенный код. Код Хэмминга $\mathcal{H}^n$ с порождающей матрицей A можно с точностью до эквивалентности представить в виде

$$\mathcal{H}^n = \{(|x|, x + y, x) \mid x \in \mathbb{F}^{\frac{n-1}{2}},\ y \in \mathcal{H}^{\frac{n-1}{2}}\}.$$

Код V_λ^n представляется в виде (1) с точностью до эквивалентности.

Произвольный вектор веса 3 в коде C является либо строкой матрицы A, либо получен добавлением вектора $(1, 0, 0, \ldots, 0)$ к вектору веса 4 из $\mathcal{H}^n$ с первой ненулевой координатой. Если через B' обозначить матрицу, строками которой являются векторы веса 3 второго типа, через A' — матрицу, полученную из A удалением строк с первой ненулевой координатой, различные STS получаются заменой некоторых k строк матрицы A' подходящими k строками матрицы B' [20]. Отвечающие этим строкам тройки будут равновесными множествами. Совокупность таких строк будем также называть *равновесными*. По k строкам из B' можно однозначно восстановить k векторов веса 4 из кода $\mathcal{H}^n$.

Определим функцию $\lambda : \mathcal{H}^{\frac{n-1}{2}} \to \{0,1\}$, соответствующую коду Васильева V^n_λ, в который будет вложима получающаяся в результате такой замены STS, следующим образом:

(i) $\lambda = 1$ на векторах веса 3 из кода $\mathcal{H}^{\frac{n-1}{2}}$, которые соответствуют k заменяемым строкам матрицы A' и k векторам веса 4, которые отвечают k заменяющим строкам матрицы B';

(ii) $\lambda = 0$ на оставшихся векторах.

Пусть $y \in \mathcal{H}^{\frac{n-1}{2}}$ — некоторый вектор с носителем $\{a_1, a_2, a_3\}$, на котором $\lambda = 1$. Тогда в пространстве $\mathbb{F}^{\frac{n-1}{2}}$ существуют три вектора веса 2, которые пересекаются с y по двум координатам, образуя векторы веса 3 в $\mathcal{H}^n$ вида $\big(a_1, \frac{n+1}{2}+a_2, \frac{n+1}{2}+a_3\big), \big(a_2, \frac{n+1}{2}+a_1, \frac{n+1}{2}+a_3\big), \big(a_3, \frac{n+1}{2}+a_1, \frac{n+1}{2}+a_2\big)$. Также в пространстве $\mathbb{F}^{\frac{n-1}{2}}$ найдутся ровно три вектора веса 1, которые пересекаются с y в единственной координате, образуя векторы веса 4 в $\mathcal{H}^n$ вида $\big(1, a_1, a_2, \frac{n+1}{2}+a_3\big), \big(1, a_1, a_3, \frac{n+1}{2}+a_2\big), \big(1, a_2, a_3, \frac{n+1}{2}+a_1\big)$. Вместе с векторами (a_1, a_2, a_3) и $(1, \frac{n+1}{2}+a_1, \frac{n+1}{2}+a_2, \frac{n+1}{2}+a_3)$ получим два набора векторов вида $\big\{\big(a_1, a_2, a_3\big), \big(a_1, \frac{n+1}{2}+a_2, \frac{n+1}{2}+a_3\big), \big(a_2, \frac{n+1}{2}+a_1, \frac{n+1}{2}+a_3\big), \big(a_3, \frac{n+1}{2}+a_1, \frac{n+1}{2}+a_2\big)\big\}$ и $\big\{\big(\frac{n+1}{2}+a_1, \frac{n+1}{2}+a_2, \frac{n+1}{2}+a_3\big), \big(a_1, a_2, \frac{n+1}{2}+a_3\big), \big(a_1, a_3, \frac{n+1}{2}+a_2\big), \big(a_2, a_3, \frac{n+1}{2}+a_1\big)\big\}$, которые являются равновесными подмножествами троек из $\mathcal{H}^n$ и V^n_λ соответственно и отвечают свитчингам Паш-конфигураций, указанным в теореме 2.1 из [20]. Отметим, что приведённые свитчинги в точности соответствуют конструкции Ассмуса — Маттсона [12] для хэммингових STS.

Несложно заметить, что STS, получившаяся в результате такой замены некоторых k строк матрицы A' равновесными k строками матрицы B', вложима в код V^n_λ с вышеуказанной функцией λ. Так как все коды Васильева, построенные из кода $\mathcal{H}^{\frac{n-1}{2}}$, имеют ранг не более $r_n - 1$, любая STS(n) ранга не больше $r_n - 1$ вложима в некоторый совершенный код длины n такого же ранга и существует всего

$$S(n) = 2^{|\mathrm{STS}(\frac{n-1}{2})|} \cdot n!/2^{\frac{n-1}{2}} \cdot |\mathrm{Sym}(\mathcal{H}^{\frac{n-1}{2}})|$$

таких различных STS. С учётом того, что согласно [20] существует ровно

$$2 \cdot n!/((n+1) \cdot |\mathrm{Sym}(\mathcal{H}^{\frac{n-1}{2}})|)$$

STS(n) ранга $n - \log(n+1)$, получим указанную в формулировке оценку. Теорема 4 доказана.

Согласно [2] ранг любого совершенного кода длины n, полученного из двоичного кода Хэмминга длины n методом свитчингов ijk-компонент,

не превосходит r_n. Следовательно, и ранг его системы $\mathrm{STS}(n)$, полученной методом свитчингов ijk-компонент из $\mathrm{STS}(H,n)$, также не превосходит r_n.

Теорема 5 [7]. *Любой совершенный код C длины n ранга не больше r_n может быть получен из некоторого кода Хэмминга конечным числом последовательных свитчингов i-компонент. Более того, для получения кода C из кода Хэмминга достаточно использовать свитчинги i-компонент не более чем по двум координатам i.*

Обозначим

$$Q(n) = (2^{(n-1)/2} \cdot 130^{(n^2-10n+21)/96} - 3n + \ + 9) \cdot n(n-1)/12.$$

Из теорем 2, 5 и леммы 1 следует

Теорема 6. *Любая система* $\mathrm{STS}(n)$, $n = 4m+3$, $m \geqslant 63$, *ранга r_n, полученная применением свитчингов по правилам $\mathcal{A}1$, $\mathcal{B}1$ или $\mathcal{B}2$ к* $\mathrm{STS}(H,n)$, *вложима в некоторый совершенный двоичный код длины n такого же ранга. Число $R_2(n)$ таких различных* $\mathrm{STS}(n)$ *удовлетворяет неравенствам*

$$Q(n) \cdot R(\mathcal{H}, (n-3)/4) - S(n) \leqslant R_2(n) \leqslant Q(n) \cdot R(\mathcal{H}, n) - S(n).$$

Доказательство. Аналогично рассуждениям доказательства следствия 2 для каждой тройки $\{i,j,k\}$ из любой $\mathrm{STS}(H,n)$ по правилу $\mathcal{A}1$ можно получить $4^m = 4^{(n-3)/4}$ различных свитчингов, а также $(46+84)^{|\mathrm{STS}(\frac{n-3}{4})|} = 130^{(n-3)(n-7)/3\cdot 2^5}$ различных свитчингов — по правилам $\mathcal{B}1$ и $\mathcal{B}2$. Учитывая число кодов Хэмминга предыдущей длины и рассуждения о дублируемых $\mathrm{STS}(n)$, из теоремы 2 получаем по крайней мере

$$(2^{(n-1)/2} \cdot 130^{(n^2-10n+21)/96} - 3n + 9) \cdot n(n-1)/12 \cdot R(\mathcal{H}, (n-3)/4)$$

различных совершенных кодов длины n, которые можно построить из кода H^n свитчингами ijk-компонент и которым соответствуют различные $\mathrm{STS}(n)$ ранга не более r_n.

Так как свитчинги по указанным выше правилам можно применить не более чем к $R(\mathcal{H},n)$ кодам Хэмминга H^n, получаем не более

$$(2^{(n-1)/2} \cdot 130^{(n^2-10n+21)/96} - 3n + 9) \cdot n(n-1)/12 \cdot R(\mathcal{H}, n)$$

совершенных кодов длины n, которые можно построить из кода H^n свитчингами ijk-компонент и которым соответствуют все различные $\mathrm{STS}(n)$ ранга не более r_n.

Используя теоремы 4 и 5, получаем указанную оценку. Теорема 6 доказана.

Из теорем 2, 4 и 6 с учётом того, что все $S(n)$ систем $\mathrm{STS}(n)$ ранга не больше $r_n - 1$ уже подсчитаны в $Q(n) \cdot R(\mathcal{H}, n)$ системах $\mathrm{STS}(n)$ ранга не больше r_n, легко найти нижнюю оценку для числа $\mathrm{STS}(n)$, не вложимых в совершенные коды длины n ранга не больше r_n.

Утверждение 7. *Число различных систем* $\mathrm{STS}(n)$, $n \geqslant 511$, *ранга* r_n, *не вложимых в совершенные коды длины* n *ранга* r_n, *можно оценить снизу как* $P(n) \cdot R(\mathcal{H}, (n-3)/4) - Q(n) \cdot R(\mathcal{H}, n)$.

Заметим, что число различных $\mathrm{STS}(n)$ ранга не больше r_n, вложимых в совершенные двоичные коды такого же ранга (см. теоремы 4 и 6), намного меньше числа различных $\mathrm{STS}(n)$ ранга не больше r_n. Последняя оценка существенно отличается от нижней оценки для числа $\mathrm{STS}(n)$. Таким образом, число всех $\mathrm{STS}(n)$ ранга не больше r_n невелико по сравнению с числом $\mathrm{STS}(n)$ рангов, больших, чем упомянутые.

Замечание. В [22] доказано, что любая $\mathrm{STS}(n)$ ранга r_n вложима в некоторый совершенный код длины n. Но при этом в отличие от данной работы в [22] не известен точный ранг этого совершенного кода. Кроме того, нами используются свитчинговые методы, а в [22] — каскадные.

Из замечания следует, что все STS из утверждения 7 вложимы в совершенные коды рангов, больших чем r_n. Результаты [22] и настоящей работы анонсированы на конференции ACCT'12 в [14, 21].

В заключение авторы выражают благодарность рецензенту за полезные замечания.

ЛИТЕРАТУРА

1. **Августинович С. В., Соловьёва Ф. И.** О несистематических совершенных кодах // Пробл. передачи информ. — 1996. — Т. 32, № 3. — С. 47–50.
2. **Августинович С. В., Соловьёва Ф. И.** Построение совершенных двоичных кодов последовательными сдвигами $\tilde{\alpha}$-компонент // Пробл. передачи информ. — 1997. — Т. 33, № 3. — С. 15–21.
3. **Васильев Ю. Л.** О негрупповых плотно-упакованных кодах // Пробл. кибернетики. — 1962. — Вып. 8. — С. 337–339.
4. **Егорычев Г. П.** Доказательство гипотезы Ван дер Вардена для перманентов // Сиб. мат. журн. — 1981. — Т. 22, № 6. — С. 65–71.
5. **Зиновьев В. А., Зиновьев Д. В.** О кодах Васильева длины $n = 2^m$ и удвоение систем Штейнера $S(n, 4, 3)$ заданного ранга // Пробл. передачи информ. — 2006. — Т. 42, вып. 1. — С. 13–33.

6. **Зиновьев В. А., Зиновьев Д. В.** Системы Штейнера $S(v, k, k-1)$: компоненты и ранг // Пробл. передачи информ. — 2011. — Т. 47, № 2. — С. 52–71.
7. **Кротов Д. С., Потапов В. Н.** О свитчинговой эквивалентности n-арных квазигрупп порядка 4 и совершенных двоичных кодов // Пробл. передачи информ. — 2010. — Т. 46, № 3. — С. 22–28.
8. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж.** Теория кодов, исправляющих ошибки. — М.: Связь, 1979. — 744 с.
9. **Петренюк А. Я.** Признаки неизоморфности систем троек Штейнера // Укр. мат. журн. — 1972. — Т. 24, № 6. — С. 772–780.
10. **Соловьёва Ф. И., Топалова С. Т.** Совершенные двоичные коды и системы троек Штейнера с максимальными порядками групп автоморфизмов // Дискрет. анализ и исслед. операций. Сер. 1. — 2000. — Т. 7, № 4. — С. 101–110.
11. **Холл М.** Комбинаторика. — М.: Мир, 1970. — 424 с.
12. **Assmus E. F., Mattson H. F. Jr.** On tactical configurations and error correcting codes // J. Comb. Theory. — 1967. — Vol. 2. — P. 243–257.
13. **Kaski P., Östergård P. R. J.** The Steiner triple systems of order 19 // Math. Comput. — 2004. — Vol. 73. — P. 2075–2092.
14. **Kovalevskaya D. I., Filimonova E. S., Solov'eva F. I.** Steiner triple (quadruple) systems of small ranks embedded into perfect (extended perfect) binary codes // Proc. 13th Int. Workshop «Algebraic and combinatorial coding theory» (Pomorie, Bulgaria, June 15–21, 2012). — Pomorie: Inst. Math. Informatics, Bulg. Acad. Sci., 2012. — P. 203–208.
15. **Linial N., Luria Z.** An upper bound on the number of Steiner triple systems // Random Structures & Algorithms, accepted, 2013. DOI: 10.1002/rsa.20487.
16. **Östergård P. R. J., Pottonen O.** The perfect binary one-error-correcting codes of length 15. Part 1. — Classification // IEEE Trans. Inform. Theory. — 2009. — Vol. 55. — P. 4657–4660.
17. **Östergård P. R. J., Pottonen O.** There exist Steiner triple systems of order 15 that do not occur in a perfect binary one-error-correcting code // J. Comb. Des. — 2007. — Vol. 15. — P. 465–468.
18. **Solov'eva F. I.** On perfect codes and related topics // Com^{2}Mac Lect. Notes. Ser. 13. — Pohang, Korea: Pohang Univ. Sci. Tech., 2004. — 80 p.
19. **Solov'eva F.I., Avgustinovich S.V., Heden O.** The classification of some perfect codes // Des. Codes Cryptogr. — 2004. — Vol. 31, N 3. — P. 313–318.
20. **Tonchev V. D.** A mass formula for Steiner triple systems STS$(2^n - 1)$ of 2-rank $2^n - n$ // J. Comb. Theory. Ser. A. — 2001. — Vol. 95. — P. 197–208.
21. **Zinoviev D. V., Zinoviev V. A.** Steiner triple systems $S(2^m - 1, 3, 2)$ of 2-rank $r \leqslant 2^m - m + 1$: construction and properties // Proc. 13th Int. Workshop «Algebraic and combinatorial coding theory» (Pomorie, Bulgaria, June 15–21, 2012). — Pomorie: Inst. Math. Informatics, Bulg. Acad. Sci., 2012. —

P. 358—363.

22. Zinoviev V. A., Zinoviev D. V. Steiner triple systems $S(2^m - 1, 3, 2)$ of rank $2^m - m + 1$ over F_2 // Probl. Inform. Transm. — 2012. — Vol. 48, N 2. — P. 102–126.

Ковалевская Дарья Игоревна,
e-mail: daryik@rambler.ru
Соловьёва Фаина Ивановна,
e-mail: sol@math.nsc.ru
Филимонова Елена Сергеевна,
e-mail: filimones@rambler.ru

Статья поступила
2 августа 2012 г.

Переработанный вариант —
20 марта 2013 г.