

УДК 621.391.15

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

Д. И. Ковалевская, Ф. И. Соловьёва

Аннотация. Известно, что кодовые слова веса 4 расширенного совершенного двоичного кода, содержащего нулевой вектор, образуют систему четвёрок Штейнера. Предложена модификация конструкции Линднера для систем четвёрок Штейнера порядка $N = 2^r$, которая может быть описана специальными свитчингами из хэмминговой системы четвёрок Штейнера. Доказано, что любая такая система четвёрок Штейнера вложима в некоторый расширенный совершенный двоичный код, построенный методом свитчингов $ijkl$ -компонент из двоичного расширенного кода Хэмминга. Приводится нижняя оценка числа различных систем четвёрок Штейнера порядка N ранга не более $N - \log N + 1$, вложимых в расширенные совершенные коды длины N .

Ключевые слова: система четвёрок Штейнера, расширенный совершенный двоичный код, свитчинг, $ijkl$ -компонента, il -компонента.

Введение

Пусть \mathbb{F}^n — n -мерное метрическое пространство над полем Галуа $GF(2)$ с метрикой Хэмминга. *Двоичным кодом* длины n называется произвольное подмножество метрического пространства \mathbb{F}^n . *Параметры* произвольного двоичного кода C из \mathbb{F}^n обозначаются через $(n, |C|, d)$, где n — длина кодовых слов (элементов кода), $|C|$ — мощность кода и d — кодовое расстояние (т. е. минимальное хэммингово расстояние между кодовыми словами). *Носителем* $\text{supp}(x)$ вектора x из \mathbb{F}^n называется множество ненулевых координатных позиций x . Двоичный код C длины n с расстоянием $d = 2d' + 1$ называется *совершенным*, если для любого

*) Исследование первого автора поддержано грантом Президента РФ для молодых российских учёных (грант МК-1700.2011.1), второго — Российским фондом фундаментальных исследований (проекты 10-01-00424-а и 12-01-00631).

$x \in \mathbb{F}^n$ существует единственный x' из C такой, что расстояние Хэмминга $d(x, x')$ равно $(d-1)/2$. Известно [7], что нетривиальный совершенный двоичный код, исправляющий одну ошибку (упоминаемый далее как совершенный), существует тогда и только тогда, когда $n = 2^r - 1$ для некоторого целого $r \geq 2$.

Если V — множество, состоящее из v элементов, то t -(v, k, λ)-схемой называется такое размещение v различных элементов по блокам, что каждый блок содержит точно k различных элементов и любое t -элементное подмножество из V появляется точно в λ блоках. Системой троек Штейнера порядка v (обозначим её через $\text{STS}(v)$) и системой четвёрок Штейнера порядка v (обозначаемой через $\text{SQS}(v)$) называются 2 -($v, 3, 1$)- и 3 -($v, 4, 1$)-схемы соответственно. Две системы четвёрок Штейнера изоморфны, если существует взаимно однозначное отображение множеств из v элементов, переводящее все блоки одной системы в блоки другой. Известно [10], что система четвёрок $\text{SQS}(v)$ существует тогда и только тогда, когда $v \equiv 2, 4 \pmod{6}$, а наилучшие нижняя [14] и верхняя [12] оценки числа $N(v)$ всех неизоморфных систем четвёрок Штейнера порядка v имеют вид

$$2^{v^3/24} \leq N(v) \leq 2^{v^3 \log v(1+o(1))/24}.$$

Пусть \bar{C} — расширенный совершенный код, полученный из совершенного кода C длины $2^r - 1$, $r \geq 2$, добавлением общей проверки на чётность (т. е. добавлением координаты, равной сумме остальных по модулю 2). Далее будем рассматривать только совершенные (следовательно, и расширенные совершенные) коды, содержащие нулевой вектор. Известно [7], что носители всех кодовых слов веса 3 в коде C образуют систему троек Штейнера $\text{STS}(2^r - 1)$, а носители кодовых слов веса 4 в коде \bar{C} образуют систему четвёрок Штейнера $\text{SQS}(2^r)$.

Говорят [1], что код $C' = (C \setminus M) \cup M'$ 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 . Если же $M' = M \oplus e_i$ для некоторого $i \in \{1, 2, \dots, n\}$, где e_i — вектор веса 1 с единицей в i -й координатной позиции, то множество M называется i -компонентой кода C длины n . Пусть $\alpha \subseteq \{1, \dots, n\}$. Множество называется α -компонентой кода C , если оно является i -компонентой для любого $i \in \alpha$ [1].

Аналогично определяется понятие свитчинга для t -($v, k, 1$)-схемы. Два множества R и R' , состоящие из k -элементных подмножеств множества V , называются равновесными, если каждое неупорядоченное подмножество

из t элементов, которое может быть найдено в k -элементных подмножествах одного множества, встречается также и в k -элементных подмножествах другого множества. Говорят, что t -($v, k, 1$)-схема $A' = (A \setminus R) \cup R'$ получена *свитчингом* множества блоков R на множество блоков R' в t -($v, k, 1$)-схеме A , если R и R' — равновесные множества [2, 6, 8] (см. определение равновесных множеств в [8]). В [6] такое множество R (равно как и множество R') названо *компонентой*.

Существует множество открытых вопросов, касающихся систем троек и четвёрок Штейнера, в том числе проблема классификации систем троек и четвёрок Штейнера, проблема вложимости произвольной системы троек (четвёрок) Штейнера в совершенный (расширенный совершенный) код.

Интересен также вопрос соответствия разных конструкций для систем троек (четвёрок) Штейнера с конструкциями для совершенных (совершенных расширенных) двоичных кодов, например, взаимосвязь свитчинговых и каскадных конструкций для данных объектов.

В [16] доказано, что только 33 из 80 неизоморфных систем троек Штейнера порядка 15 вложимы в совершенные коды и только 15590 из 1054163 систем четвёрок Штейнера порядка 16 вложимы в расширенные совершенные коды.

Рангом кода C называется размерность линейного подпространства пространства \mathbb{F}^n , образованного векторами из C . Известно, что ранг системы троек Штейнера STS($2^r - 1$) (системы четвёрок Штейнера SQS(2^r)) варьируется от $2^r - r - 1$, ранга кода Хэмминга (линейного совершенного кода) длины $2^r - 1$ [11, 17], до полного ранга $2^r - 1$.

В [19] найдено число различных систем троек Штейнера порядка $2^r - 1$ ранга $2^r - r$, что на 1 превышает минимально возможный ранг, а в [18] получена аналогичная формула для числа различных систем четвёрок Штейнера порядка 2^r ранга $2^r - r$.

Напомним, что *параллельный класс* в 3-($v, 4, 1$)-схеме, $v \equiv 0 \pmod{4}$, определяется как множество из $v/4$ блоков, попарно не пересекающихся по элементам (иными словами, параллельный класс является тривиальной 1-($v, 4, 1$)-схемой). Система четвёрок Штейнера, в которой множество блоков можно разбить на $r = (v - 1)(v - 2)/6$ непересекающихся параллельных классов, называется *разрешимой*. В [5] приведены конструкции, которые строят все различные системы четвёрок Штейнера порядка $N = 2^r$ ранга не больше $2^r - r + 1$, доказано, что все такие системы разрешимы, и найдено число различных разрешимых систем четвёрок

Штейнера, имеющих один фиксированный параллельный класс:

$$\frac{2^{N+2} \cdot (N/4)! \cdot 6^{N(N-4)/2^5} \cdot 55296^{N(N-4)(N-8)/(3 \cdot 2^9)}}{N(N-4)(N-8) \dots (N-N/2)}. \quad (1)$$

Отсюда с учётом того, что существует $N!/24^{N/4}$ таких различных параллельных классов, несложно найти число всех различных систем четвёрок Штейнера, построенных с помощью этих конструкций из системы четвёрок Штейнера порядка $N/4$ ранга не более $2^r - r + 1$:

$$\frac{2^{N+2} \cdot N! \cdot (N/4)! \cdot 6^{N(N-4)/2^5} \cdot 55296^{N(N-4)(N-8)/(3 \cdot 2^9)}}{24^{N/4} \cdot N(N-4)(N-8) \dots (N-N/2)}. \quad (2)$$

В [4] показано, что класс систем троек Штейнера порядка $2^r - 1$, полученный специальными свитчингами из хэмминговой системы троек Штейнера, вложим в класс совершенных кодов, построенных методом ijk -компонент, и приведена нижняя оценка числа систем троек Штейнера порядка $2^r - 1$ ранга не более $2^r - r + 1$.

Основная цель нашей работы состоит в выяснении следующего вопроса: какие системы четвёрок Штейнера вложимы в двоичные совершенные расширенные коды, построенные известным методом $ijkl$ -компонент из кода Хэмминга? Для этой цели приводится свитчинговая конструкция системы четвёрок Штейнера $SQS(N)$, построенная из произвольной системы четвёрок Штейнера $SQS(m)$, $N = 4m$, и основанная на конструкции Линднера. Показано, что разбиение $SQS(N)$ при $N = 2^r$ на определённого вида подмножества-компоненты соответствует некоторому разбиению на $ijkl$ -компоненты расширенного совершенного кода и такая система четвёрок Штейнера вложима в расширенный совершенный код, построенный методом $ijkl$ -компонент. В статье приводится нижняя оценка числа различных систем четвёрок Штейнера $SQS(N)$ ранга не более $N - \log N + 1$, вложимых в расширенный совершенный код.

1. Системы четвёрок Штейнера $SQS(4m)$, вложимые в расширенный совершенный код

Рассмотрим конструкцию системы четвёрок Штейнера $SQS(N)$ порядка $N = 4m$, которая строится из системы четвёрок Штейнера $SQS(m)$ порядка m и является свитчинговой конструкцией, базирующейся на конструкции Линднера [15], которая, в свою очередь, является обобщением известной конструкции Ханани [13]. Из построения будет следовать, что некоторые такие $SQS(4m)$ вложимы в расширенные совершенные коды.

Для полноты изложения рассмотрим конструкцию Линднера [15].

Пусть $M = \{1, 2, 3, \dots, m\}$ — множество, на котором задана произвольная система четвёрок Штейнера $\text{SQS}(m)$, $m \equiv 2, 4 \pmod{6}$. На множестве элементов $M \cup \{i_1, \dots, i_m, j_1, \dots, j_m, k_1, \dots, k_m\}$ построим систему четвёрок порядка $4m$, в дальнейшем упоминаемую как Q_N , $N = 4m$, и покажем, что она является штейнеровой. Для этой цели рассмотрим таблицу

$$T_M = \begin{array}{|c|c|c|c|c|} \hline 1 & 2 & 3 & \dots & m \\ \hline i_1 & i_2 & i_3 & \dots & i_m \\ \hline j_1 & j_2 & j_3 & \dots & j_m \\ \hline k_1 & k_2 & k_3 & \dots & k_m \\ \hline \end{array}.$$

Сначала для наглядности опишем построение $\text{SQS}(4m)$ в частном случае, когда $m = 4$. Пусть, например, $\text{SQS}(4) = \{(a, b, c, d)\}$. В этом случае система четвёрок Штейнера $\text{SQS}(4m)$ имеет порядок 16 и таблица T_M принимает вид

$$\begin{array}{|c|c|c|c|} \hline a & b & c & d \\ \hline i_a & i_b & i_c & i_d \\ \hline j_a & j_b & j_c & j_d \\ \hline k_a & k_b & k_c & k_d \\ \hline \end{array}.$$

Обозначим полученную таблицу через T_{abcd} . Для построения $\text{SQS}(16)$ поступим следующим образом. Включим в строящееся множество четвёрок все строки и столбцы таблицы T_{abcd} , а также четвёрки, полученные из каждой пары строк и столбцов, которые схематично можно изобразить следующим образом:


(3)

Например, для первой пары строк получим четвёрки

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

Включим также все миноры второго порядка, т. е. четвёрки

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

Кроме того, добавим в это множество всевозможные сочетания элементов, находящихся в разных строках и столбцах таблицы T_{abcd} (все трансверсали таблицы T_{abcd}), т. е. множество четвёрок вида

$$\begin{aligned} &\{(a, i_b, j_c, k_d), (a, i_b, j_d, k_c), (a, i_c, j_b, k_d), (a, i_d, j_b, k_c), (a, i_c, j_d, k_b), \\ &(a, i_d, j_c, k_b), (b, i_a, j_c, k_d), (b, i_a, j_d, k_c), (b, i_c, j_a, k_d), (b, i_d, j_a, k_c), \\ &(b, i_c, j_d, k_a), (b, i_d, j_c, k_a), (c, i_a, j_b, k_d), (c, i_a, j_d, k_b), (c, i_b, j_a, k_d), \\ &(c, i_d, j_a, k_b), (c, i_b, j_d, k_a), (c, i_d, j_b, k_a), (d, i_a, j_b, k_c), (d, i_a, j_c, k_b), \\ &(d, i_b, j_a, k_c), (d, i_c, j_a, k_b), (d, i_b, j_c, k_a), (d, i_c, j_b, k_a)\}. \end{aligned} \quad (5)$$

С учётом того, что в конструкцию включили 4 строки, 4 столбца, 6 четвёрок вида (3), применённых к каждому C_4^2 строкам и C_4^2 столбцам таблицы, $6 \cdot C_4^2$ миноров и 24 четвёрки — трансверсали таблицы T_{abcd} , общее число получившихся четвёрок равно

$$4 + 4 + 2 \cdot 6 \cdot C_4^2 + 6 \cdot C_4^2 + 24 = 140,$$

что совпадает с количеством блоков в SQS(16). Из построения множества четвёрок видно, что каждая неупорядоченная тройка элементов содержится в единственном блоке. Таким образом, из SQS(4) построена система SQS(16).

Пусть m — произвольное число такое, что существует SQS(m). Тогда в конструируемое множество четвёрок Q_N , где $N = 4m$, включим все столбцы, а также для любой пары столбцов — все миноры вида (4) и четвёрки вида (3). Тем самым получим

$$m + 6 \cdot C_m^2 + 6 \cdot C_m^2 = m + 6m(m - 1)$$

четвёрок. Далее для любой четвёрки (a, b, c, d) из $\text{SQS}(m)$ рассмотрим подматрицу T_{abcd} . Для этой матрицы в множество Q_N включим (a, b, c, d) , оставшиеся строки, четвёрки вида (3), применённые к каждой паре строк, а также четвёрки вида (5).

Нетрудно видеть, что каждой матрице вида T_{abcd} в Q_N соответствуют $1 + 3 + 6 \cdot C_4^2 + 4 \cdot 6 = 64$ четвёрки. Число таблиц совпадает с числом четвёрок в $\text{SQS}(m)$ и равно $m(m-1)(m-2)/24$. Следовательно, общее число четвёрок в конструкции равно

$$m + 6m(m-1) + 64 \cdot m(m-1) \cdot (m-2)/24 = 4m(4m-1) \cdot (4m-2)/24 = |Q_N|.$$

Из построения множества четвёрок легко видеть, что каждая неупорядоченная тройка элементов встречается ровно в одной четвёрке. Таким образом, построена система четвёрок Штейнера Q_N порядка $N = 4m$ из системы четвёрок Штейнера $\text{SQS}(m)$ порядка m и справедлива

Теорема 1 [15]. *Из произвольной системы четвёрок Штейнера порядка m можно построить систему четвёрок Штейнера порядка $4m$.*

Напомним, что в оригинальной конструкции Ханани [13] $\text{SQS}(2n)$ порядка $2n$ строится из системы $\text{SQS}(n)$ для любого допустимого n , а в конструкции Линднера [15] $\text{SQS}(n \cdot t)$ порядка $n \cdot t$ строится из двух систем $\text{SQS}(n)$ и $\text{SQS}(t)$ для любых допустимых n и t . Систему четвёрок Штейнера порядка N , соответствующую двоичному расширенному коду Хэмминга \mathcal{H}^N , будем называть *хэмминговой системой четвёрок Штейнера* $\text{SQS}(\mathcal{H}^N)$. Легко показать, что справедливо

Следствие 1. *Если $\text{SQS}(m)$ — хэммингова система четвёрок Штейнера, то система четвёрок Q_N , $N = 4m$, — хэммингова система четвёрок Штейнера порядка N .*

Введём специального вида компоненты для расширенных совершенных кодов и системы четвёрок расширенного кода Хэмминга. Пусть K — i -компонента кода Хэмминга длины $N - 1$, $N = 2^r$, $r \geq 3$ [1]. Множество \overline{K} будем называть *il -компонентой расширенного кода Хэмминга* длины N , полученного из кода Хэмминга с помощью общей проверки на чётность по l -й координатной позиции, $l \in \{1, \dots, N\} \setminus i$. Аналогичным образом можно определить jl -, kl -, а также ij -, ik -, jk -компоненты расширенного кода Хэмминга. Пусть x — произвольное кодовое слово расширенного кода Хэмминга такое, что $\text{supp}(x) = \{i, j, k, l\}$. Множество \overline{M} называется *$ijkl$ -компонентой расширенного кода Хэмминга*, если \overline{M} — $s_1 s_2$ -компонента расширенного кода Хэмминга для любых различных s_1

и s_2 из $\{i, j, k, l\}$. Отметим, что il - и jk -, jl - и ik -, kl - и ij -компоненты расширенного кода Хэмминга попарно совпадают.

Множество Q назовём il -компонентой хэмминговой системы четвёрок Штейнера $SQS(\mathcal{H}^N)$, если Q — подмножество векторов веса 4 из il -компоненты расширенного кода Хэмминга \mathcal{H}^N длины N . Если il -компонента системы четвёрок Штейнера Q является также jl -компонентой и kl -компонентой, то Q назовём $ijkl$ -компонентой хэмминговой системы четвёрок Штейнера $SQS(\mathcal{H}^N)$.

Отметим, что определение понятия компоненты из [6] является более общим. Изучающиеся там минимальные компоненты порядка 8 и мощности 8 совпадают с определёнными выше $s_1 s_2$ -компонентами хэмминговой системы четвёрок Штейнера, $ijkl$ -компоненты в [6] не рассматриваются.

Теорема 2 [1]. Пусть $\{i, j, k, l\}$ — носитель произвольного вектора веса 4 любого расширенного двоичного кода Хэмминга \mathcal{H}^N длины N . Тогда код \mathcal{H}^N можно представить в виде объединения непересекающихся $ijkl$ -компонент R_{ijkl}^t , каждая из которых, в свою очередь, может быть представлена объединением непересекающихся il -компонент R_{il}^{pt} :

$$\mathcal{H}^N = \bigcup_{t=0}^{N_2-1} R_{ijkl}^t = \bigcup_{t=0}^{N_2-1} \bigcup_{p=0}^{N_1-1} R_{il}^{pt},$$

где $N_1 = 2^{(N-4)/4}$, $N_2 = 2^{(N+4)/4 - \log N}$.

Эти разбиения позволяют делать свитчинги расширенного кода Хэмминга и в результате получить широкий класс расширенных совершенных кодов.

Далее будем рассматривать компоненты системы четвёрок Штейнера, отвечающие подмножествам компонент R_{ijkl}^0 , R_{il}^{p0} , $R_{ijkl}^{\alpha_t}$, $R_{il}^{p\alpha_t}$ расширенного совершенного кода, содержащего эту систему четвёрок, которые обозначим через R_{ijkl} , R_{il}^p , $R_{ijkl}^{\alpha_t}$ и $R_{il}^{p\alpha_t}$ соответственно.

Лемма 1. Пусть $\{i, j, k, l\}$ — носитель любого вектора веса 4 произвольного расширенного двоичного кода Хэмминга длины N . Тогда хэммингова система четвёрок Штейнера $SQS(\mathcal{H}^N)$ представима в виде объединения подмножеств $1 + N(N-4)(N-8)/(3 \cdot 2^9)$ непересекающихся $ijkl$ -компонент, каждая из которых, в свою очередь, является объединением подмножеств либо $N/4 + (N-4)(N-8)/2^5$, либо 8 непересекающихся il -компонент.

ДОКАЗАТЕЛЬСТВО. Пусть без ограничения общности (i, j, k, l) — четвёрка из $\text{SQS}(\mathcal{H}^m)$, которой отвечает некоторый столбец таблицы T_M .

По теореме 2 имеем $R_{ijkl} = \bigcup_{p=1}^{N_1} R_{il}^p$, где R_{il}^1 — линейная оболочка векторов с носителями $\{(i, a, i_a, l), (i, j, k, l), (i, j_a, k_a, l) \mid a \in M' = M \setminus l\}$. Далее $R_{il} = R_{il}^1$. Представим оставшиеся R_{il}^p , $p > 1$, в виде всех возможных классов смежности по компоненте R_{il} . Заметим, что $(j, a, j_a, l) \in R_{ijkl}$, $(j, a, j_a, l) \notin R_{il}$ для любого $a \in M'$ и $(j, a, j_a, l) \notin R_{il} + (j, b, j_b, l)$ для различных элементов a и b из M' . Поэтому существует $N/4 - 1$ классов смежности по компоненте R_{il} вида $R_{il} + (j, a, j_a, l)$, где $a \in M'$. Далее несложно увидеть, что $(j, a, j_a, l) + (j, b, j_b, l) \in R_{ijkl}$, $(j, a, j_a, l) + (j, b, j_b, l) \notin R_{il}$ для любых различных a и b из M' , $(j, a, j_a, l) + (j, b, j_b, l) \notin R_{il} + (j, c, j_c, l)$ для любых попарно различных элементов a, b и c из M' и

$$(j, a, j_a, l) + (j, b, j_b, l) \notin R_{il} + (j, c, j_c, l) + (j, d, j_d, l)$$

для любых попарно различных элементов a, b, c и d из M' . Поэтому существует $C_{N/4-1}^2 = (N/4 - 1)(N/4 - 2)/2 = (N - 4)(N - 8)/2^5$ классов смежности по компоненте R_{il} вида $R_{il} + (j, a, j_a, l) + (j, b, j_b, l)$, где a и b — различные элементы из M' . Проводя аналогичные рассуждения для классов смежности по компоненте R_{il} вида $R_{il} + (j, a, j_a, l) + (j, b, j_b, l) + (j, c, j_c, l), \dots, R_{il} + (j, a, j_a, l) + (j, b, j_b, l) + \dots + (j, m', j_{m'}, l)$, с учётом того, что

$$1 + (N/4 - 1) + C_{N/4-1}^2 + C_{N/4-1}^3 + \dots + C_{N/4-1}^{N/4-1} = 2^{N/4-1} = N_1,$$

получаем

$$R_{il}^p = R_{il} + (j, a, j_a, l) \text{ для любого } a \in M', \quad 2 \leq p \leq N/4;$$

$$R_{il}^p = R_{il} + (j, a, j_a, l) + (j, b, j_b, l) \text{ для различных элементов } a \text{ и } b \text{ из } M', \\ 1 + N/4 \leq p \leq N/4 + (N - 4)(N - 8)/2^5;$$

$$R_{il}^p = R_{il} + (j, a, j_a, l) + (j, b, j_b, l) + (j, c, j_c, l) \text{ для различных элементов } a, b, c \text{ из } M', \\ 1 + N/4 + (N - 4)(N - 8)/2^5 \leq p \leq N/4 + (N - 4)(N - 8)/2^5 + (N - 4)(N - 8)(N - 12)/(3 \cdot 2^7);$$



$$\dots \\ R_{il}^{N_1} = R_{il} + (j, a, j_a, l) + (j, b, j_b, l) + \dots + (j, m', j_{m'}, l),$$

$$M' = \{a, b, \dots, m'\}.$$

Поэтому для системы четвёрок Штейнера $\text{SQS}(\mathcal{H}^N)$ выполняется следующее: компонента R_{ijkl} для $\text{SQS}(\mathcal{H}^N)$ содержит все столбцы таблицы T_M , а также миноры (4) и блоки вида (3) для каждой пары столбцов таблицы.



Более конкретно,

$$R_{ijkl} = \bigcup_{p=1}^{\frac{N/4+(N-4)(N-8)}{2^5}} R_{il}^p,$$

где $R_{il} = \{(i, j, k, l), (i, a, i_a, l), (i, j_a, k_a, l), (a, i_a, j_a, k_a), (a, i_a, j, k), (j, k, j_a, k_a)\}$ для всех $a \in M'$; $(a, i_a, j_b, k_b), (a, b, i_a, i_b), (j_a, k_a, j_b, k_b)$ для любых различных a и b из M' , т.е. R_{il} содержит все столбцы таблицы, некоторые миноры и четвёрки вида  и  для каждой пары столбцов таблицы.

Для всех компонент вида $R_{il}^p \subset R_{il} + (j, a, j_a, l)$, $2 \leq p \leq N/4$, для всех $a \in M'$

$$R_{il}^p = \{(i_a, j, k_a, l), (i_a, j_a, k, l), (a, i, j_a, k), (a, i, j, k_a), (j, a, j_a, l), (k, a, k_a, l), (i, j, i_a, j_a), (i, k, i_a, k_a)\},$$

т.е. R_{il}^p , $2 \leq p \leq 4$, содержит некоторые миноры и четвёрки из (3) вида  и  для пары столбцов (i, j, k, l) и $(a, i_a, j_a, k_a)^T$ и для всех $a \in M'$.



Так как

$$R_{il}^p \subset R_{il} + (j, a, j_a, l) + (j, b, j_b, l),$$

$$N/4 + 1 \leq p \leq N/4 + (N - 4) \cdot (N - 8)/2^5,$$

для любых различных $a, b \in M'$, то

$$R_{il}^p = \{(a, i_b, j_a, k_b), (a, i_b, j_b, k_a), (b, i_a, j_b, k_a), (b, i_a, j_a, k_b), (a, j_a, b, j_b), (a, k_a, b, k_b), (i_a, j_a, i_b, j_b), (i_a, k_a, i_b, k_b)\},$$

т.е. R_{il}^p , $N/4 + 1 \leq p \leq N/4 + (N - 4)(N - 8)/2^5$, содержит некоторые миноры и четвёрки из (3) вида  и  для пары столбцов (a, i_a, j_a, k_a) и $(b, i_b, j_b, k_b)^T$ и для любых различных элементов a и b из M' .

Далее, $R_{ijkl}^{\alpha_t} = R_{ijkl} + \alpha_t$, где $\alpha_t \in \text{SQS}(m)$, поэтому $R_{ijkl}^{\alpha_t} = \bigcup_{p=1}^8 R_{il}^{p\alpha_t}$.

Приведём пример разбиения компоненты $R_{ijkl}^{\alpha_1} = R_{ijkl}^{abcl} = R_{ijkl} + (a, b, c, l)$. Строение остальных компонент $R_{ijkl}^{\alpha_t}$, $2 \leq t \leq m(m - 1)/6$, где $\alpha_t \in \text{SQS}(m)$, выглядит аналогично.

Рассмотрим таблицу

$$T_{abcl} = \begin{array}{|c|c|c|c|} \hline l & a & b & c \\ \hline i & i_a & i_b & i_c \\ \hline j & j_a & j_b & j_c \\ \hline k & k_a & k_b & k_c \\ \hline \end{array}.$$

Первая il -компонента состоит из двух первых строк (a, b, c, l) и (i, i_a, i_b, i_c) этой матрицы, а также из четвёрок вида (3), построенных на этих строках,

$$R_{il}^{1\alpha_1} = \{(a, b, c, l), (i, i_a, i_b, i_c), (a, i_b, i_c, l), (i, i_a, b, c), \\ (i_a, b, i_c, l), (i, a, i_b, c), (i_a, i_b, c, l), (i, a, b, i_c)\}.$$

Остальные il -компоненты устроены следующим образом:

$$R_{il}^{2\alpha_1} = \{(j, j_a, b, c), (j, j_a, i_b, i_c), (k, k_a, b, c), (k, k_a, i_b, i_c), \\ (j, k_a, b, i_c), (k, j_a, b, i_c), (j, k_a, i_b, c), (k, j_a, i_b, c)\};$$

$$R_{il}^{3\alpha_1} = \{(j, a, j_b, c), (j, i_a, j_b, i_c), (k, a, k_b, c), (k, i_a, k_b, i_c), \\ (j, a, k_b, i_c), (k, a, j_b, i_c), (j, i_a, k_b, c), (k, i_a, j_b, c)\};$$

$$R_{il}^{4\alpha_1} = \{(j, a, b, j_c), (j, i_a, i_b, j_c), (k, a, b, k_c), (k, i_a, i_b, k_c), \\ (j, a, i_b, k_c), (k, a, i_b, j_c), (j, i_a, b, k_c), (k, i_a, b, j_c)\};$$

$$R_{il}^{5\alpha_1} = \{(j_a, j_b, c, l), (k_a, k_b, c, l), (i, j_a, j_b, i_c), (i, k_a, k_b, i_c), \\ (j_a, k_b, i_c, l), (k_a, j_b, i_c, l), (i, j_a, k_b, c), (i, k_a, j_b, c)\};$$

$$R_{il}^{6\alpha_1} = \{(j_a, b, j_c, l), (k_a, b, k_c, l), (i, j_a, i_b, j_c), (i, k_a, i_b, k_c), \\ (j_a, i_b, k_c, l), (k_a, i_b, j_c, l), (i, j_a, b, k_c), (i, k_a, b, j_c)\};$$

$$R_{il}^{7\alpha_1} = \{(a, j_b, j_c, l), (a, k_b, k_c, l), (i, i_a, j_b, j_c), (i, i_a, k_b, k_c), \\ (i_a, j_b, k_c, l), (i_a, k_b, j_c, l), (i, a, j_b, k_c), (i, a, k_b, j_c)\}.$$

Компонента $R_{il}^{8\alpha_1}$ состоит из двух последних строк (j, j_a, j_b, j_c) и (k, k_a, k_b, k_c) матрицы T_{abcl} , а также из четвёрок вида (3), построенных на этих строках,

$$R_{il}^{8\alpha_1} = \{(j, j_a, j_b, j_c), (k, k_a, k_b, k_c), (j, j_a, k_b, k_c), (k, k_a, j_b, j_c), \\ (j, k_a, j_b, k_c), (k, j_a, k_b, j_c), (j, k_a, k_b, j_c), (k, j_a, j_b, k_c)\}.$$

Для $R_{ijkl}^{\alpha_t}$, $2 \leq t \leq N(N-4)(N-8)/(3 \cdot 2^9)$, выполняется $R_{ijkl}^{\alpha_t} = \bigcup_{p=1}^8 R_{il}^{p\alpha_t}$, причём $R_{il}^{p\alpha_t}$ строятся аналогично предыдущему случаю, но каждый раз для своей таблицы T_{α_t} . Лемма 1 доказана.

Теорема 3. Система четвёрок Штейнера, полученная методом свитчингов $ijkl$ -компонент из системы $SQS(\mathcal{H}^N)$, вложима в расширенный совершенный код, полученный из расширенного кода Хэмминга \mathcal{H}^N методом свитчингов $ijkl$ -компонент.

ДОКАЗАТЕЛЬСТВО. Из доказательства леммы 1 непосредственно следует, что свитчинги компонент системы четвёрок Штейнера $SQS(\mathcal{H}^N)$ полностью определяются свитчингами соответствующих компонент расширенного кода Хэмминга \mathcal{H}^N . Так как il -, jl -, kl - и $ijkl$ -компоненты системы четвёрок Штейнера $SQS(\mathcal{H}^N)$ являются подмножествами соответствующих il -, jl -, kl - и $ijkl$ -компонент расширенного кода Хэмминга \mathcal{H}^N , система четвёрок Штейнера, полученная методом свитчингов из системы $SQS(\mathcal{H}^N)$, вложима в совершенный код, полученный методом свитчингов из кода \mathcal{H}^N . Теорема 3 доказана.

Следует заметить, что согласно [1] ранг расширенного совершенного кода длины N , полученного из расширенного двоичного кода Хэмминга длины N методом свитчингов $ijkl$ -компонент (следовательно, и ранг системы четвёрок Штейнера порядка N , полученной методом свитчингов $ijkl$ -компонент из хэмминговой системы четвёрок Штейнера порядка N), не превосходит $N - \log N + 1$. Приведём нижнюю оценку числа различных систем четвёрок Штейнера порядка N ранга не более $N - \log N + 1$, вложимых в расширенный совершенный код длины N , построенный методом свитчингов $ijkl$ -компонент.

Теорема 4. Число $R(N)$ различных систем четвёрок Штейнера $SQS(N)$ порядка N ранга не более $N - \log N + 1$, вложимых в расширенный совершенный код, не меньше, чем

$$(3^2 \cdot 2^8 - 8)^{N(N-4)(N-8)/(3 \cdot 2^9)} \cdot (2^{N(N-4)/2^5} - 1) \cdot \frac{N(N-1)(N-2)}{2^3} \cdot R^*(N/4),$$

где $R^*(N/4) = (N/4)! / ((N/4-1)(N/4-2)(N/4-2^2) \dots (N/4)/2)$ — число различных хэмминговых систем четвёрок Штейнера порядка $N/4$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим хэммингову систему четвёрок Штейнера $SQS(\mathcal{H}^N)$, построенную указанным выше способом (см. теорему 1), в ней — компоненту R_{ijkl}^{abcl} из леммы 1 и для неё — следующую таблицу.

$abcl$	$ajbjcl$	$jabjcl$	$jajbcl$	$jabjc$	$jajbc$	$jjabc$	$jjaibjc$
ai_bicl	ak_bkcl	$jaibkcl$	jak_bicl	$jaibkc$	jak_bic	$jjaibic$	$jjaibkc$
$iabicl$	$iajbkcl$	$kabkcl$	$kajbicl$	$iaibkc$	$iajbic$	$jkaibic$	$jkaibkc$
$iaibcl$	$akbjcl$	$kajbjcl$	$kajbcl$	$iaibjc$	$iajbkc$	$jkaibc$	$jkaibkc$
$iabi_c$	$iajbkc$	$iajbkc$	$iajbic$	$kabkc$	$kajbic$	$jkaibic$	$jkaibkc$
$iaibc$	$iajbkc$	$iaibjc$	$iajbkc$	$kajbic$	$kajbc$	$jkaibc$	$jkaibkc$
$iiabc$	$iajbjc$	$ikabjc$	$ikajbc$	$kiaibjc$	$kiajbkc$	$kkaibc$	$kkaibkc$
$iiab_c$	$iajbkc$	$ikabkc$	$ikajbc$	$kiaibkc$	$kiaibic$	$kkaibic$	$kkaibkc$

Её строки соответствуют jl -компонентам, столбцы — il -компонентам. Далее нам потребуются следующие диагонали данной таблицы, которые отвечают kl -компонентам R_{ijkl}^{abcl} :

$$D_1 = \{(a, b, c, l), (a, k_b, k_c, l), (k_a, b, k_c, l), (k_a, k_b, c, l), \\ (k, a, b, k_c), (k, a, k_b, c), (k, k_a, b, c), (k, k_a, k_b, k_c)\};$$

$$D_2 = \{(a, j_b, j_c, l), (a, i_b, i_c, l), (k_a, j_b, i_c, l), (k_a, i_b, j_c, l), \\ (k, a, j_b, i_c), (k, a, i_b, j_c), (k, k_a, j_b, j_c), (k, k_a, i_b, i_c)\};$$

$$D_3 = \{(j_a, b, j_c, l), (j_a, k_b, i_c, l), (i_a, b, i_c, l), (i_a, k_b, j_c, l), \\ (k, j_a, b, i_c), (k, j_a, k_b, j_c), (k, i_a, b, j_c), (k, i_a, k_b, i_c)\};$$

$$D_4 = \{(j_a, j_b, c, l), (j_a, i_b, k_c, l), (i_a, j_b, k_c, l), (i_a, i_b, c, l), \\ (k, j_a, j_b, k_c), (k, j_a, i_b, c), (k, i_a, j_b, c), (k, i_a, i_b, k_c)\};$$

$$D_5 = \{(i, a, b, i_c), (i, a, k_b, j_c), (i, k_a, b, j_c), (i, k_a, k_b, i_c), \\ (j, a, b, j_c), (j, a, k_b, i_c), (j, k_a, b, i_c), (j, k_a, k_b, j_c)\};$$

$$D_6 = \{(i, a, j_b, k_c), (i, a, i_b, c), (i, k_a, j_b, c), (i, k_a, i_b, k_c), \\ (j, a, j_b, c), (j, a, i_b, k_c), (j, k_a, j_b, k_c), (j, k_a, i_b, c)\};$$

$$D_7 = \{(i, i_a, b, c), (i, i_a, k_b, k_c), (i, j_a, b, k_c), (i, j_a, k_b, c), \\ (j, i_a, b, k_c), (j, i_a, k_b, c), (j, j_a, b, c), (j, j_a, k_b, k_c)\};$$

$$D_8 = \{(i, i_a, i_b, i_c), (i, i_a, j_b, j_c), (i, j_a, i_b, j_c), (i, j_a, j_b, i_c), \\ (j, i_a, i_b, j_c), (j, i_a, j_b, i_c), (j, j_a, i_b, i_c), (j, j_a, j_b, j_c)\}.$$

При этом для каждой из 1–4 и 5–8 строк возможны свитчинги $l \leftrightarrow j$, $i \leftrightarrow k$ соответственно. Заметим, что здесь полностью меняются il -компоненты.

Если сначала применить соответствующие приведённые свитчинги для всех строк таблицы (т. е. уже для $ijkl$ -компоненты R_{ijkl}^{abcl} мощности 64), то для каждого из получившихся 1–4 и 5–8 столбцов или 1–4 и 5–8 диагоналей допустимы также дополнительные свитчинги $j \leftrightarrow k$, $l \leftrightarrow i$ или $i \leftrightarrow j$, $l \leftrightarrow k$ соответственно.

Аналогично для каждого из 1–4 и 5–8 столбцов (1–4 и 5–8 диагоналей) таблицы возможны свитчинги $l \leftrightarrow i$, $j \leftrightarrow k$ ($l \leftrightarrow k$, $i \leftrightarrow j$) соответственно. В этом случае полностью меняются jl -компоненты (kl -компоненты). Если применить соответствующие приведённые свитчинги сначала для всех столбцов (диагоналей) таблицы, то для каждой из получившихся 1–4 и 5–8 строк или 1–4 и 5–8 диагоналей (1–4 и 5–8 строк или 1–4 и 5–8 столбцов) допустимы дополнительные свитчинги $i \leftrightarrow k$, $l \leftrightarrow j$ или $i \leftrightarrow j$, $l \leftrightarrow k$ ($i \leftrightarrow k$, $l \leftrightarrow j$ или $j \leftrightarrow k$, $l \leftrightarrow i$) соответственно.

Таким образом, в каждом из приведённых 9 случаев преобразований либо только строк, столбцов, диагоналей (преобразований $s_1 s_2$ -компонент), либо их попарных комбинаций (преобразований $ijkl$ - и соответствующих $s_1 s_2$ -компонент) возможны 2^8 вариантов свитчингов. С учётом появляющихся дублирований (например, результат свитчинга всех строк, а затем всех столбцов таблицы совпадает с результатом свитчинга всех столбцов, затем всех строк таблицы) можно сделать вывод, что существует по крайней мере $9 \cdot 2^8 - 8$ вариантов изменений компоненты R_{ijkl}^{abcl} .

Проводя аналогичные рассуждения для остальных компонент вида $R_{ijkl}^{\alpha t}$, можно найти по крайней мере $9 \cdot 2^8 - 8$ вариантов изменений компоненты $R_{ijkl}^{\alpha t}$. Следует заметить, что в результате таких преобразований меняются четвёрки в $\text{SQS}(\mathcal{H}^N)$, но получившаяся система остаётся системой четвёрок Штейнера, уже не хэмминговой.

Рассмотрим компоненту R_{ijkl} . Для каждой из её il -, jl -, kl -подкомпонент вида $R_{il} + (j, a, j_a, l), \dots, R_{il} + (a, b, j_a, j_b), R_{jl} + (k, a, k_a, l), \dots, R_{jl} + (a, b, k_a, k_b), R_{kl} + (i, a, i_a, l), \dots, R_{kl} + (a, b, i_a, i_b)$, где $a, b \in M'$, возможны свитчинги $l \leftrightarrow i$, $a \leftrightarrow i_a$, $l \leftrightarrow j$, $a \leftrightarrow j_a$, $l \leftrightarrow k$, $a \leftrightarrow k_a$ соответственно. Здесь также полностью меняются il -, jl - либо kl -компоненты и возможно по крайней мере $3 \cdot (2^{N/4+(N-4)(N-8)/2^5-1} - 1)$ вариантов изменений компоненты R_{ijkl} .

В итоге с учётом того, что в качестве четвёрки (i, j, k, l) можно выбрать любую четвёрку системы $\text{SQS}(\mathcal{H}^N)$, а в качестве исходной системы четвёрок $\text{STS}(N/4)$ — любую из $R^*(N/4)$ имеющихся различных хэммин-

говых систем четвёрок Штейнера порядка $N/4$, получаем

$$(3^2 \cdot 2^8 - 8)^{N(N-4)(N-8)/(3 \cdot 2^9)} \cdot 3 \cdot (2^{N/4+(N-4)(N-8)/2^5-1} - 1) \\ \frac{N(N-1)(N-2)}{3 \cdot 2^3} \cdot ((N/4)!/(N/4-1)(N/4-2)(N/4-2^2) \cdot \dots \cdot (N/4)/2)$$

возможных свитчингов. Теорема 4 доказана.

Отметим, что полученная оценка меньше (2). Вопрос о том, все ли системы четвёрок Штейнера из [5] вложимы в расширенные совершенные коды, остаётся открытым.

Следует также заметить, что рассуждения, аналогичные приведённым в данной работе, но гораздо более громоздкие, можно провести и для α -компонент расширенных совершенных кодов, где $|\alpha| > 4$.

ЛИТЕРАТУРА

1. **Августинович С. В., Соловьева Ф. И.** Построение совершенных двоичных кодов последовательными сдвигами $\hat{\alpha}$ -компонент // Проблемы передачи информации. — 1997. — Т. 33, вып. 3. — С. 15–21.
2. **Алиев И. Ш. о.** Комбинаторные схемы и алгебры // Сиб. мат. журн. — 1972. — Т. 13, № 3. — С. 499–509.
3. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Проблемы кибернетики. — 1962. — Вып. 8. — С. 337–339.
4. **Глухих Е. С.** Вложимость систем троек Штейнера в совершенные коды: Магистерская диссертация. — Новосибирск: Новосибирск. гос. ун-т, 2005. — 18 с.
5. **Зиновьев В. А., Зиновьев Д. В.** О разрешимости систем Штейнера $S(v = 2^m, 4, 3)$ ранга $r \leq v - m + 1$ над \mathbb{F}^2 // Проблемы передачи информации. — 2007. — Т. 43, вып. 1. — С. 39–55.
6. **Зиновьев В. А., Зиновьев Д. В.** Системы Штейнера $S(v, k, k-1)$: компоненты и ранг // Проблемы передачи информации. — 2011. — Т. 47, вып. 2. — С. 52–71.
7. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж.** Теория кодов, исправляющих ошибки. — М.: Связь, 1979. — 744 с.
8. **Петренюк А. Я.** Признаки неизоморфности систем троек Штейнера // Укр. мат. журн. — 1972. — Т. 24, № 6. — С. 772–780.
9. **Соловьева Ф. И.** Введение в теорию кодирования. Учеб. пособие. — Новосибирск: Новосибирск. гос. ун-т, 2006. — 124 с.
10. **Холл М.** Комбинаторика. — М.: Мир, 1970. — 424 с.
11. **Doyen J., Hubaut X., Vandensavel M.** Ranks of incidence matrices of Steiner triple systems // Math. Z. 1978. — Bd 163, Heft 3. — S. 251–259.
12. **Doyen J., Vandensavel M.** Nonisomorphic Steiner quadruple systems // Bull. Soc. Math. Belg. — 1971. — Vol. 23. — P. 393–410.

13. **Hanani H.** The existence and construction of balanced incomplete block designs // Ann. Math. Stat. — 1961. — Vol. 32, N 2. — P. 361–386.
14. **Lenz H.** On the number of Steiner quadruple systems // Mitt. Math. Seminar Giessen. — 1985. — Vol. 169. — P. 55–71.
15. **Lindner C. C.** On the construction of nonisomorphic Steiner quadruple systems // Colloq. Math. — 1974. — Vol. 29. — P. 303–306.
16. **Östergård P. R., 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. **Teirlinck L.** On projective and affine hyperplanes // J. Comb. Theory, Ser. A. — 1980. — Vol. 28, N 3. — P. 290–306.
18. **Tonchev V. D.** A formula for the number of Steiner quadruple systems on 2^n points of 2-rank $2^n - n$ // J. Comb. Des. — 2003. — Vol. 11, N 4. — P. 260–274.
19. **Tonchev V. D.** A mass formula for Steiner triple systems $\text{STS}(2^n - 1)$ of 2-rank $2^n - n$ // J. Comb. Theory, Ser. A. — 2001. — Vol. 95, N 2. — P. 197–208.

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

Статья поступила
14 октября 2011 г.
Переработанный вариант —
10 февраля 2012 г.