

УДК 621.391.15

СИСТЕМЫ ЧЕТВЁРОК ШТЕЙНЕРА МАЛЫХ РАНГОВ И РАСШИРЕННЫЕ СОВЕРШЕННЫЕ ДВОИЧНЫЕ КОДЫ *)

Д. И. Ковалевская, Ф. И. Соловьёва

Аннотация. С помощью свитчингового подхода указана классификация систем четвёрок Штейнера порядка $N > 8$ ранга r_N (на 2 отличного от ранга кода Хэмминга длины N), вложимых в расширенные совершенные двоичные коды длины N такого же ранга. Приведены нижняя и верхняя оценки числа таких различных систем. Дано описание класса систем четвёрок Штейнера порядка N ранга r_N , не вложимых в расширенные совершенные двоичные коды длины N того же ранга, указана нижняя оценка числа таких различных систем четвёрок.

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

Введение

Пусть \mathbb{F}^n — n -мерное метрическое пространство над полем Галуа $GF(2)$ с метрикой Хэмминга. *Хэммингово расстояние* $d(x, y)$ между векторами x, y из \mathbb{F}^n равно числу координат, в которых x и y отличаются, *вес Хэмминга* $w(x)$ вектора $x \in \mathbb{F}^n$ равен числу ненулевых координатных позиций x . *Двоичным кодом* длины n называется произвольное подмножество метрического пространства \mathbb{F}^n , *двоичным линейным кодом* — векторное подпространство в \mathbb{F}^n . Элементы кода называются *кодowymi словами*. Параметры произвольного двоичного кода C из \mathbb{F}^n обозначаются через $(n, |C|, d)$, где n — длина кодовых слов (элементов кода), $|C|$ — мощность кода, d — кодовое расстояние (т. е. минимальное хэммингово расстояние между кодowymi словами). *Носителем* вектора x из \mathbb{F}^n называется множество ненулевых координат x . Двоичный код C длины n с расстоянием $d = 2d' + 1$ называется *совершенным двоичным кодом, исправляющим одну ошибку* (далее — *совершенным*), если для любого

*) Исследование выполнено при частичной 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).

$x \in \mathbb{F}^n$ существует единственный y из C такой, что $d(x, y) = 1$. Кодом Хэмминга \mathcal{H}^n называется линейный совершенный код длины n (он единствен с точностью до эквивалентности). Известно [10], что совершенные коды имеют следующие параметры: длину $n = 2^r - 1$, $r > 1$, число кодовых слов 2^{n-r} и кодовое расстояние, равное 3. Пусть \overline{C} — *расширенный совершенный код* длины $N = 2^r$, 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 и расширенные совершенные коды, содержащие нулевой вектор. Рангом кода C называется размерность линейного подпространства пространства \mathbb{F}^n , образованного векторами из C .

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 . Множество M называется *il-компонентой* кода \overline{C} длины N , полученного из C расширением по l -й координате, если $M' = M \oplus e_i \oplus e_l$ для некоторого $i \in \{1, 2, \dots, N\}$, где e_i и e_l — векторы веса 1 с единицей в i -й и l -й координате соответственно. Множество R называется *ijkl-компонентой* кода \overline{C} , если R является $t_1 t_2$ -компонентой для любых $t_1, t_2 \in \{i, j, k, l\}$.

Известно [20], что любой расширенный совершенный код длины N ранга $r_N - 1 = N - \log N$ является кодом Васильева [3]. Он может быть построен свитчингами *il*-компонент из расширенного кода Хэмминга с помощью некоторой функции $\lambda : \mathcal{H}^{\frac{N}{2}-1} \rightarrow \{0, 1\}$. Обозначим этот код через \overline{V}_λ^N . Код \overline{V}_λ^N с точностью до эквивалентности представим в виде

$$\overline{V}_\lambda^N = \{(|x| + |y| + \lambda(y), |x| + \lambda(y), x + y, x) \mid x \in \mathbb{F}^{\frac{N}{2}-1}, y \in \mathcal{H}^{\frac{N}{2}-1}\}. \quad (1)$$

Пусть V — v -элементное множество. Назовём t -(v, k, λ)-*схемой* размещение v различных элементов по блокам такое, что каждый блок содержит точно k различных элементов и любое t -элементное подмножество из V появляется точно в λ блоках. *Системой четвёрок Штейнера порядка v* , обозначаемой через $SQS(v)$ (кратко SQS , если не важен порядок системы), называется 3-($v, 4, 1$)-схема. Каждому блоку (i, j, k, l) из $SQS(v)$ сопоставим вектор из \mathbb{F}^v с единицами только в i -й, j -й, k -й и l -й координатах. Далее из контекста будет ясно, идёт речь о блоках, о носителях или о векторах. Известно [15], что $SQS(v)$ существует тогда и только тогда, когда $v \equiv 2, 4 \pmod{6}$. Носители кодовых слов веса 4 в коде \overline{C} образуют $SQS(2^r)$ [10]. Систему $SQS(\overline{\mathcal{H}}, N)$, отвечающую расширенному коду Хэмминга $\overline{\mathcal{H}}^N$ длины N , будем называть *хэмминго-*

вой системой четвёрок Штейнера по аналогии с хэмминговой системой троек Штейнера [7, 12]. Они называются также *булевыми* [5, 6]. Две SQS *изоморфны*, если существует взаимно однозначное отображение их базовых множеств, переводящее блоки одной системы в блоки другой. Основные задачи данной области — классификация и определение числа неизоморфных SQS (ссылки на полученные по этим задачам результаты см. в [4, 5]). Наилучшие нижняя [17] и верхняя [14] оценки числа $N(v)$ всех неизоморфных $SQS(v)$ имеют вид

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

Рангом $SQS(N)$, $N = 2^r$, называется размерность линейного подпространства пространства \mathbb{F}^N , образованного векторами из $SQS(N)$. Известно, что ранг $SQS(N)$ варьируется от $r_N - 2$, ранга кода Хэмминга длины $N - 1$ [13], до полного ранга $N - 1$.

Понятие свитчинга для SQS определяется аналогично понятию свитчинга для расширенного совершенного двоичного кода. Два множества R и R' , состоящие из четырёхэлементных подмножеств множества V , называются *равновесными*, если каждая тройка элементов, которая может быть найдена в четвёрках одного множества, встречается также и в четвёрках другого множества. Говорят, что

$$SQS'(N) = (SQS(N) \setminus R) \cup R'$$

получена *свитчингом* множества блоков R на множество блоков R' в $SQS(N)$, если R и R' равновесные (см. определение равновесных множеств, например, в [11], о свитчинговых методах — см. [6]). В [6] такое множество R (а также множество R') названо *компонентой*.

В [21] найдено число $R_1(N)$ различных $SQS(N)$ ранга $r_N - 1$, что на 1 превышает минимально возможный ранг:

$$R_1(N) = (2^{|SQS(N/2)| - N/2} - 1/N) \cdot N! / |\text{Sym}(\overline{\mathcal{H}}, N/2)|. \quad (2)$$

Параллельный класс в $3-(N, 4, 1)$ -схеме, где $N \equiv 0 \pmod{4}$, определяется как множество из $N/4$ блоков, попарно не пересекающихся по элементам. $SQS(N)$ называется *разрешимой*, если множество её блоков можно разбить на $r = (N - 1)(N - 2)/6$ непересекающихся параллельных классов. В [5] приведены конструкции различных $SQS(N)$ ранга не больше r_N . Доказано, что все такие системы разрешимы, и найдено число различных разрешимых SQS , имеющих один фиксированный параллельный класс:

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

Так как всего существует $N!/24^{N/4}$ разных параллельных классов, из [5] вытекает, что число всех различных $SQS(N)$ ранга не более r_N равно

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

В [19] доказано, что только 15590 из 1054163 систем $SQS(16)$ вложимы в расширенные совершенные коды. В [22] показано, что все системы троек Штейнера порядка $n = N - 1 = 2^r - 1 > 7$ ранга r_N вложимы в некоторые совершенные коды, но остаётся неясным ранг таких кодов.

В [7] предложена конструкция SQS , вложимых в расширенные совершенные двоичные коды, построенные известным методом $ijkl$ -компонент из кода Хэмминга, и приведена нижняя оценка числа таких различных SQS . Известно [1], что построенные таким методом коды (и соответствующие им SQS) имеют ранг, не более чем на 2 превышающий минимально возможный ранг совершенного кода — ранг кода Хэмминга. Однако оставалось неясным, существуют ли другие SQS , вложимые в такой класс расширенных совершенных кодов.

Данная работа является продолжением [7, 8]. Основными её результатами являются классификация $SQS(N)$, $N = 2^r > 8$, ранга r_N , вложимых в расширенные совершенные коды длины N такого же ранга, и доказательство того, что класс построенных в [7] $SQS(N)$, $N = 2^r > 8$, ранга r_N совпадает с классом SQS , вложимых в расширенные совершенные коды длины N такого же ранга. Неясно, все ли SQS , имеющие ранг, не более чем на 2 превышающий ранг хэмминговой SQS , вложимы в некоторые расширенные совершенные коды, но уже большего ранга. В [4] приведена классификация SQS ранга $r_N - 1$ и показано, что эти SQS вложимы в расширенные коды Васильева такого же ранга. В настоящей работе с помощью свитчингового подхода дано другое доказательство этого факта, отличное от приведённого в [4]. Кроме того, найдено описание $SQS(N)$ ранга не более r_N , не вложимых в расширенные совершенные коды длины N , построенные методом $ijkl$ -компонент из расширенного кода Хэмминга, и приведена нижняя оценка числа таких различных SQS .

1. Число различных $SQS(N)$ рангов $r_N - 1$ и r_N , вложимых в расширенные совершенные двоичные коды таких же рангов

Порядок группы симметрий расширенного кода Хэмминга $\overline{\mathcal{H}}^N$ равен [10, гл. 13]

$$|\text{Sym}(\overline{\mathcal{H}}, N)| = (N-1)(N-2)(N-2^2)(N-2^3) \dots N/2. \quad (3)$$

Известно, что ранг любого расширенного совершенного кода \bar{V}_λ^N длины N , полученного из произвольного кода $\bar{\mathcal{H}}^N$ свитчингами il -компонент с помощью функции λ (следовательно, и ранг его $SQS(N)$, полученной свитчингами il -компонент из хэмминговой $SQS(N)$), не превосходит $r_N - 1$. На основе этого факта, известной конструкции Линднера [18] для SQS , вложимых в расширенные коды Васильева, а также сопоставления с полученным в [21] числом различных $SQS(N)$ ранга не больше $r_N - 1$ свитчинговым методом докажем, что класс $SQS(N)$ ранга $r_N - 1$ совпадает с классом SQS , вложимых в коды \bar{V}_λ^N такого же ранга. Другое доказательство этого факта, использующее каскадный метод, см. в [4].

Теорема 1. *Любая $SQS(N)$ ранга $r_N - 1$ вложима в некоторый расширенный совершенный код Васильева длины N такого же ранга.*

ДОКАЗАТЕЛЬСТВО. Пусть A — матрица инцидентности некоторой хэмминговой $SQS(N)$, $N = 2^r$. Строками этой матрицы, очевидно, являются двоичные векторы веса 4 с единицами в координатах, номера которых образуют блоки данной хэмминговой SQS . Тогда (см. [21]) матрица G , состоящая из строк матрицы A и вектора $(1, 1, 0, \dots, 0)$, является порождающей матрицей кода C , который содержит $2^{|SQS(N/2)|}$ различных $SQS(N)$ ранга не более $r_N - 1$, и число таких различных кодов равно $\frac{N!}{2^{N/2} \cdot |\text{Sum}(\bar{\mathcal{H}}, N/2)|}$.

Докажем, что каждая SQS кода C вложима в некоторый расширенный код Васильева \bar{V}_λ^N длины N такого же ранга. Так как любой совершенный код длины N ранга не более $r_N - 1$ является расширенным кодом Васильева [20], построенным из кода Хэмминга длины $N/2 - 1$ с помощью нелинейной функции λ , имеем вложимость всякой SQS из кода C в некоторый расширенный совершенный код.

Расширенный код Хэмминга $\bar{\mathcal{H}}^N$ можно с точностью до эквивалентности представить в виде

$$\bar{\mathcal{H}}^N = \{(|x| + |y|, |x|, x + y, x) \mid x \in \mathbb{F}^{\frac{N}{2}-1}, y \in \mathcal{H}^{\frac{N}{2}-1}\}. \quad (4)$$

Произвольное кодовое слово веса 4 кода C является либо строкой матрицы A , либо получено добавлением вектора $(1, 1, 0, \dots, 0)$ к кодовому слову веса 4 из $\bar{\mathcal{H}}^N$ с первой или второй ненулевой координатой, т. е. имеющему вид $(1, 0, \dots)$ или $(0, 1, \dots)$, либо получено добавлением вектора $(1, 1, 0, \dots, 0)$ к кодовому слову веса 6 из $\bar{\mathcal{H}}^N$ с первыми двумя ненулевыми координатами, т. е. имеющему вид $(1, 1, \dots)$.

Обозначим через A_0, A_1, A_2 и A_3 множество строк матрицы A таких, что первые два элемента равны 1; первый элемент равен 1, второй — 0;

первый элемент равен 0, второй — 1; первые два элемента равны 0 соответственно.

Через B_1 , B_2 и B_3 обозначим множества векторов веса 4 с единичной первой и нулевой второй координатами, получающиеся добавлением вектора $(1, 1, 0, \dots, 0)$ к строкам из A_2 ; с нулевой первой и единичной второй координатами, которые получаются добавлением вектора $(1, 1, 0, \dots, 0)$ к строкам из A_1 ; с нулевыми первыми двумя координатами, получающиеся добавлением вектора $(1, 1, 0, \dots, 0)$ к кодовым словам веса 6 из $\overline{\mathcal{H}}^N$ вида $(1, 1, \dots)$ с первыми двумя ненулевыми координатами соответственно.

Тогда согласно [21] различные SQS получаются заменой некоторых k' строк матрицы $A_{123} = A_1 \cup A_2 \cup A_3$ подходящими k' строками матрицы $B_{123} = B_1 \cup B_2 \cup B_3$. Соответствующие этим строкам тройки будут равновесными множествами. Совокупность таких строк будем также называть *равновесными*. Более того, множества A_{123} и B_{123} могут быть разделены на подмножества из 8 блоков каждое так, что для каждой восьмёрки блоков из A_{123} можно найти единственную восьмёрку блоков из B_{123} , т. е.

$$k' = 8t', \quad 1 \leq t' \leq \left\lfloor \frac{(N+3)(N-2)(N-4)}{192} \right\rfloor.$$

Определим функцию $\lambda : \mathcal{H}^{\frac{N}{2}-1} \rightarrow \{0, 1\}$ для кода \overline{V}_λ^N , в котором будет содержаться получающаяся в результате такой замены SQS : на векторах веса 3 и (или) 4, отвечающих k' заменяемым строкам матрицы $A_1 \cup A_2 \cup A_3$ и k' заменяющим строкам матрицы $B_1 \cup B_2 \cup B_3$, функция λ принимает значение 1, на остальных векторах из $\mathcal{H}^{\frac{N}{2}-1}$ — значение 0.

Пусть $y \in \mathcal{H}^{\frac{N}{2}-1}$ — некоторый вектор с носителем $\{a_1, a_2, a_3\}$, на котором функция λ принимает значение 1. Тогда в $\mathbb{F}^{\frac{N}{2}-1}$ существуют три вектора веса 1, пересекающиеся с y в одной координатной позиции. По конструкции кода \overline{V}_λ^N каждый из этих трёх векторов вместе с y образует векторы веса 4 в \overline{V}_λ^N вида $(1, a_2, a_3, \frac{N}{2} + 1 + a_1)$, $(1, a_1, a_3, \frac{N}{2} + 1 + a_2)$, $(1, a_1, a_2, \frac{N}{2} + 1 + a_3)$, отвечающие векторам веса 4 в $\overline{\mathcal{H}}^N$ вида $(2, a_2, a_3, \frac{N}{2} + 1 + a_1)$, $(2, a_1, a_3, \frac{N}{2} + 1 + a_2)$, $(2, a_1, a_2, \frac{N}{2} + 1 + a_3)$ соответственно.

Также в $\mathbb{F}^{\frac{N}{2}-1}$ найдутся три вектора веса 2, пересекающиеся с y по двум координатам. По конструкции кода \overline{V}_λ^N каждый из этих трёх векторов вместе с y образует векторы веса 4 в \overline{V}_λ^N вида $(2, a_3, \frac{N}{2} + 1 + a_1, \frac{N}{2} + 1 + a_2)$, $(2, a_2, \frac{N}{2} + 1 + a_1, \frac{N}{2} + 1 + a_3)$, $(2, a_1, \frac{N}{2} + 1 + a_2, \frac{N}{2} + 1 + a_3)$, которые отвечают векторам веса 4 в $\overline{\mathcal{H}}^N$ вида $(1, a_3, \frac{N}{2} + 1 + a_1, \frac{N}{2} + 1 + a_2)$,

$(1, a_2, \frac{N}{2} + 1 + a_1, \frac{N}{2} + 1 + a_3), (1, a_1, \frac{N}{2} + 1 + a_2, \frac{N}{2} + 1 + a_3)$ соответственно.

Вместе с вектором $0^{\frac{N}{2}-1}$ и вектором веса 3 из $\mathbb{F}^{\frac{N}{2}-1}$ с носителем $\{a_1, a_2, a_3\}$ дополнительно получим векторы из \bar{V}_λ^N вида $(2, a_1, a_2, a_3)$ и $(1, \frac{N}{2} + 1 + a_1, \frac{N}{2} + 1 + a_2, \frac{N}{2} + 1 + a_3)$, отвечающие векторам веса 4 в $\bar{\mathcal{H}}^N$ вида $(1, a_1, a_2, a_3)$ и $(2, \frac{N}{2} + 1 + a_1, \frac{N}{2} + 1 + a_2, \frac{N}{2} + 1 + a_3)$ соответственно.

Таким образом, имеются два равновесных множества из \bar{V}_λ^N и $\bar{\mathcal{H}}^N$, состоящие из восьми четвёрок каждое.

Пусть $y = (b_1, b_2, b_3, b_4)$ — вектор с носителем $\{b_1, b_2, b_3, b_4\}$, на котором функция λ равна 1. В $\mathbb{F}^{\frac{N}{2}-1}$ существуют четыре вектора веса 1, пересекающиеся с вектором y по одной координате. Каждый из них вместе с y согласно конструкции кода \bar{V}_λ^N образует векторы веса 4 в \bar{V}_λ^N вида $(b_2, b_3, b_4, \frac{N}{2} + 1 + b_1), (b_1, b_3, b_4, \frac{N}{2} + 1 + b_2), (b_1, b_2, b_4, \frac{N}{2} + 1 + b_3), (b_1, b_2, b_3, \frac{N}{2} + 1 + b_4)$.

В $\mathbb{F}^{\frac{N}{2}-1}$ также найдутся четыре вектора веса 3, пересекающиеся с y по трём координатам. Каждый из них вместе с y согласно конструкции кода \bar{V}_λ^N образует в \bar{V}_λ^N векторы веса 4 вида $(b_4, \frac{N}{2} + 1 + b_1, \frac{N}{2} + 1 + b_2, \frac{N}{2} + 1 + b_3), (b_3, \frac{N}{2} + 1 + b_1, \frac{N}{2} + 1 + b_2, \frac{N}{2} + 1 + b_4), (b_2, \frac{N}{2} + 1 + b_1, \frac{N}{2} + 1 + b_3, \frac{N}{2} + 1 + b_4), (b_1, \frac{N}{2} + 1 + b_2, \frac{N}{2} + 1 + b_3, \frac{N}{2} + 1 + b_4)$.

Учитывая, что в $\mathbb{F}^{\frac{N}{2}-1}$ найдутся шесть векторов веса 2, пересекающихся с y по двум координатам, которые вместе с y по конструкции (4) образуют в $\bar{\mathcal{H}}^N$ векторы веса 4 вида $(b_3, b_4, \frac{N}{2} + 1 + b_1, \frac{N}{2} + 1 + b_2), (b_2, b_4, \frac{N}{2} + 1 + b_1, \frac{N}{2} + 1 + b_3), (b_2, b_3, \frac{N}{2} + 1 + b_1, \frac{N}{2} + 1 + b_4), (b_1, b_4, \frac{N}{2} + 1 + b_2, \frac{N}{2} + 1 + b_3), (b_1, b_3, \frac{N}{2} + 1 + b_2, \frac{N}{2} + 1 + b_4), (b_1, b_2, \frac{N}{2} + 1 + b_3, \frac{N}{2} + 1 + b_4)$, и ввиду того, что в $\mathbb{F}^{\frac{N}{2}-1}$ имеются единственный вектор веса 0 и вектор веса 4 с носителем $\{b_1, b_2, b_3, b_4\}$, которые вместе с y по конструкции (4) образуют в $\bar{\mathcal{H}}^N$ вектор веса 4 вида (b_1, b_2, b_3, b_4) и $(\frac{N}{2} + 1 + b_1, \frac{N}{2} + 1 + b_2, \frac{N}{2} + 1 + b_3, \frac{N}{2} + 1 + b_4)$ соответственно, делаем вывод, что получены два равновесных множества, каждое из восьми четвёрок, являющиеся подмножествами \bar{V}_λ^N и $\bar{\mathcal{H}}^N$ соответственно. Заметим, что соответствующие наборы четвёрок из первого и второго рассмотренных случаев не содержат совпадающих четвёрок. Оба варианта равновесных наборов из 8 четвёрок отвечают свитчингам, указанным в [21].

Таким образом, SQS , построенная в результате замены некоторых k' строк матрицы $A_1 \cup A_2 \cup A_3$ равновесными k' строками матрицы $B_1 \cup B_2 \cup B_3$, вложима в код \bar{V}_λ^N с вышеуказанной функцией λ .

Так как все расширенные коды длины N ранга не более $r_N - 1$ являются

ся кодами Васильева длины N , построенными из кода Хэмминга $\mathcal{H}^{\frac{N}{2}-1}$ по конструкции (1), любая $SQS(N)$ ранга $r_N - 1$ вложима в некоторый расширенный совершенный код Васильева длины N ранга $r_N - 1$, и существует всего $2^{|SQS(\frac{N}{2})| - \frac{N}{2}} \cdot N! / |\text{Sym}(\overline{\mathcal{H}}, N/2)|$ таких различных SQS . С учётом того, что согласно [21] число $SQS(N)$ ранга $r_N - 2$ равно $N! / N \cdot |\text{Sym}(\overline{\mathcal{H}}, N/2)|$, получим оценку (2). Теорема 1 доказана.

Отметим, что приведённые свитчинги соответствуют свитчингам при переходе от $SQS(N)$, построенным согласно конструкции Ханани [16], к $SQS(N)$, полученным конструкцией Алиева [2]. Известно, что конструкция Ханани является частным случаем конструкции Линднера [18].

Через $R(\overline{\mathcal{H}}, N)$ обозначим число различных $SQS(\overline{\mathcal{H}}, N)$ порядка N . С учётом (3) имеем $R(\overline{\mathcal{H}}, N) = N! / |\text{Sym}(\overline{\mathcal{H}}, N)|$.

Согласно [1] ранг любого расширенного совершенного кода длины N , полученного из двоичного расширенного кода Хэмминга длины N методом свитчингов $ijkl$ -компонент, не превосходит r_N . Следовательно, и ранг $SQS(N)$, полученной методом свитчингов $ijkl$ -компонент из хэмминговой $SQS(N)$, также не превосходит r_N . Справедлива следующая

Теорема 2 [9]. *Любой расширенный совершенный двоичный код \overline{C} длины N ранга не больше r_N может быть получен из некоторого расширенного кода Хэмминга последовательными свитчингами il -компонент не более чем по двум парам координат (il - и jl - для некоторых i, j, l).*

В [7, теорема 4] приведена конструкция систем четвёрок Штейнера и указаны правила свитчингов il - и $ijkl$ -компонент, позволяющие из хэмминговой $SQS(N)$ получать $SQS(N)$ большего ранга. Обозначим класс таким образом построенных $SQS(N)$ ранга r через $\text{Sw}(SQS(N), r)$.

Пусть

$$P(N) = \left(2296^{\frac{N(N-4)(N-8)}{3 \cdot 2^9}} \cdot (2^{\frac{N(N-4)}{32}} - 1) - \frac{N^2 + 8N + 12}{4} \right) \cdot \frac{N(N-1)(N-2)}{8}$$

и $S(N) = 2^{|SQS(\frac{N}{2})| - \frac{N}{2}} \cdot N! / |\text{Sym}(\overline{\mathcal{H}}, N/2)|$. Основным результатом данной работы является

Теорема 3. *Класс $\text{Sw}(SQS(N), r_N)$ совпадает с классом $SQS(N)$, вложимых в расширенные совершенные коды того же ранга, построенные методом $ijkl$ -компонент из расширенного кода Хэмминга длины N . Число $R_2(N)$ таких различных SQS удовлетворяет неравенствам*

$$P(N) \cdot R(\overline{\mathcal{H}}, N/4) - S(N) \leq R_2(N) \leq P(N) \cdot R(\overline{\mathcal{H}}, N) - S(N).$$

ДОКАЗАТЕЛЬСТВО. По теореме 4 из [7] число $SQS(N)$, построенных методом $ijkl$ -компонент из фиксированной $SQS(N/4)$ и множества $\{i, j, k, l\}$, равно $2296^{\frac{N(N-4)(N-8)}{3 \cdot 2^9}} \cdot (2^{\frac{N(N-4)}{2^5}} - 1)$.

Заметим, что $SQS(N)$, получающиеся из различных $SQS(N/4)$ с помощью различных свитчингов, различны. Действительно, пусть $S_1(N)$ и $S_2(N)$ — одинаковые $SQS(N)$, полученные методом $ijkl$ -компонент из различных SQS $S_1(N/4)$ и $S_2(N/4)$ порядка $N/4$ различными свитчингами. Тогда существуют различные элементы a, b, c, d, e из множества M такие, что $(a, b, c, d) \in S_1(N/4)$ и $(a, b, c, e) \in S_2(N/4)$. Для равенства $S_1(N)$ и $S_2(N)$ необходимо, чтобы два набора из 64 четвёрок, отвечающих матрицам T_{abcd} и T_{abce} (см. [7]), были получены один из другого свитчингами вида $d \leftrightarrow e, i_d \leftrightarrow i_e, j_d \leftrightarrow j_e, k_d \leftrightarrow k_e$. Но метод $ijkl$ -компонент допускает свитчинги элементов вида d, i_d, j_d, k_d лишь из одного столбца исходной таблицы и не допускает свитчингов между элементами вида d, i_d, j_d, k_d и e, i_e, j_e, k_e из разных столбцов исходной таблицы. Следовательно, из разных $SQS(N/4)$ с помощью разных свитчингов не могут быть получены одинаковые $SQS(N/4)$.

В силу произвольности выбора четвёрки (i, j, k, l) в $SQS(N)$ имеем

$$2296^{\frac{N(N-4)(N-8)}{3 \cdot 2^9}} \cdot (2^{\frac{N(N-4)}{2^5}} - 1) \cdot |SQS(N)| \cdot R(\overline{\mathcal{H}}, N/4) \quad (5)$$

систем порядка N . Изучим, какие из них могут совпасть.

Рассмотрим произвольную $SQS(\overline{\mathcal{H}}, N)$, отвечающую фиксированной таблице T_M (см. [7]) и $SQS(\overline{\mathcal{H}}, N/4)$. При различных разбиениях системы $SQS(\overline{\mathcal{H}}, N)$ на компоненты и дальнейшем применении к ней свитчингов $ijkl$ -компонент могут появиться одинаковые $SQS(\overline{\mathcal{H}}, N)$. Рассмотрим это подробнее. Зафиксируем некоторую четвёрку $(i, j, k, l) \in SQS(\overline{\mathcal{H}}, N)$ и любой элемент из $\{i, j, k\}$, например, i . В этом случае имеем разбиение исходной $SQS(\overline{\mathcal{H}}, N)$ на il -компоненты. Несложно заметить, что $SQS(N)$, полученная из исходной $SQS(\overline{\mathcal{H}}, N)$ свитчингом $l \leftrightarrow i$, применённым ко всем четвёркам, содержащим элементы l или i , совпадает с $SQS(\overline{\mathcal{H}}', N)$, отвечающей коду Хэмминга $\overline{\mathcal{H}}' = (li)\overline{\mathcal{H}}$, полученному из кода $\overline{\mathcal{H}}$ применением к нему перестановки (li) . То же верно для свитчингов $j \leftrightarrow k, a \leftrightarrow i_a, j_a \leftrightarrow k_a$ для всякого $a \in M \setminus l$, а также для разбиений исходной $SQS(\overline{\mathcal{H}}, N)$ на jl - и kl -компоненты, т. е. для свитчингов $l \leftrightarrow j, i \leftrightarrow k, a \leftrightarrow j_a, i_a \leftrightarrow k_a$ и $l \leftrightarrow k, i \leftrightarrow j, a \leftrightarrow k_a, i_a \leftrightarrow j_a$ для любого $a \in M \setminus l$. Таким образом, получаем $3 \cdot 2 \cdot (1 + (N/4 - 1)) = 3N/2$ повторений.

Также можно разбить исходную $SQS(\overline{\mathcal{H}}, N)$ на il -компоненты и применить сначала свитчинг $l \leftrightarrow i$ ко всем $ijkl$ -компонентам этой $SQS(\overline{\mathcal{H}}, N)$,

содержащим элементы l и i , после этого выбрать элемент j или k и применить какой-либо из свитчингов $l \leftrightarrow j$, $i \leftrightarrow k$, $a \leftrightarrow j_a$, $i_a \leftrightarrow k_a$ для любого $a \in M \setminus l$ или $l \leftrightarrow k$, $i \leftrightarrow j$, $a \leftrightarrow k_a$, $i_a \leftrightarrow j_a$ для любого $a \in M \setminus l$ ко всем lj - или lk -компонентам, содержащим элементы из выбранного свитчинга. Получившаяся $SQS(N)$ совпадает с $SQS(\overline{\mathcal{H}}^l, N)$, отвечающей какому-то из кодов Хэмминга $(lij)\overline{\mathcal{H}}$, $(lki)\overline{\mathcal{H}}$, $(li)(aj_a)\overline{\mathcal{H}}$, $(li)(i_ak_a)\overline{\mathcal{H}}$ или $(lik)\overline{\mathcal{H}}$, $(lji)\overline{\mathcal{H}}$, $(li)(ak_a)\overline{\mathcal{H}}$, $(li)(i_aj_a)\overline{\mathcal{H}}$, полученных из кода $\overline{\mathcal{H}}$ посредством соответствующих перестановок. Легко видеть, что эти два кода совпадают. Аналогичные рассуждения верны, если вместо первоначального свитчинга выбрать один из свитчингов $j \leftrightarrow k$, $a \leftrightarrow i_a$, $j_a \leftrightarrow k_a$, а также если исходную $SQS(\overline{\mathcal{H}}, N)$ разбивать на jl - или kl -компоненты. Таким образом, получаем $3 \cdot 4 \cdot 2 \cdot (1 + 1 + N/4 - 1 + N/4 - 1) = 12N$ повторов.

Заметим, что $SQS(N)$, полученная из исходной $SQS(\overline{\mathcal{H}}, N)$ при разбиении её на $ijkl$ -компоненты и применении свитчинга $a \leftrightarrow i_a$ ко всем il -компонентам, содержащим элементы a и i_a , совпадает с $SQS'(N)$, полученной из исходной $SQS(\overline{\mathcal{H}}, N)$ при разбиении её на $ii_at_1t_2$ -компоненты и дальнейшем применении свитчинга $a \leftrightarrow i_a$ ко всем ii_a -компонентам, содержащим элементы a и i_a . Так как всего существует $N/2 - 1$ четвёрок вида $ii_at_1t_2$, получаем $N/2 - 1$ повторов. Аналогично для свитчинга $j_a \leftrightarrow k_a$, а также для свитчингов $a \leftrightarrow j_a$ и $i_a \leftrightarrow k_a$, применённых к jl -компонентам, и для свитчингов $a \leftrightarrow k_a$ и $i_a \leftrightarrow j_a$, применённых к kl -компонентам. Отсюда получаем $6(N/2 - 1)$ дублей. Такие рассуждения верны для любого $a \in M \setminus l$, поэтому имеем $(N/4 - 1)(3N - 6) = 3(N - 2)(N - 4)/4$ повторов.

Таким образом, для выбранного разбиения на $ijkl$ -компоненты получаем $3N/2 + 12N + 3(N - 2)(N - 4)/4 = 3(N + 2)(N + 6)/4$ повторов. Поскольку (i, j, k, l) — произвольно выбранная четвёрка из $SQS(\overline{\mathcal{H}}, N)$, где $|SQS(\overline{\mathcal{H}}, N)| = N(N - 1)(N - 2)/24$, всего имеем

$$N(N^2 - 4)(N + 6)(N - 1)/32$$

повторов. Учитывая подсчитанное в (5) число $SQS(N)$, включающее одинаковые, нижняя оценка числа различных $SQS(N)$, построенных из фиксированных таблицы Q и базовой $SQS(m)$ с помощью приведённой конструкции, принимает вид

$$\left(\frac{2296^{\frac{N(N-4)(N-8)}{3 \cdot 2^9}} \cdot (2^{\frac{N(N-4)}{2^5}} - 1)}{3} - \frac{N^2 + 8N + 12}{4} \right) \cdot \frac{N(N-1)(N-2)}{8}.$$

Поскольку существует $R(\overline{\mathcal{H}}, N/4)$ расширенных двоичных кодов Хэмминга, получаем по крайней мере

$$\left(\frac{2296^{\frac{N(N-4)(N-8)}{3 \cdot 2^9}} \cdot (2^{\frac{N(N-4)}{2^5}} - 1)}{3} - \frac{N^2 + 8N + 12}{4} \right) \times \frac{N(N-1)(N-2)}{8} \cdot R(\overline{\mathcal{H}}, N/4)$$

расширенных совершенных кодов длины N , построенных из расширенного кода Хэмминга длины N свитчингами $ijkl$ -компонент. Так как свитчинги $ijkl$ -компонент можно применить не более чем к $R(\overline{\mathcal{H}}, N)$ расширенным кодам Хэмминга длины N , имеем не более

$$\left(\frac{2296^{\frac{N(N-4)(N-8)}{3 \cdot 2^9}} \cdot (2^{\frac{N(N+4)}{2^5}} - 1)}{3} - \frac{N^2 + 8N + 12}{4} \right) \times \frac{N(N-1)(N-2)}{8} \cdot R(\overline{\mathcal{H}}, N)$$

расширенных совершенных кодов длины N , которые можно построить из расширенного кода Хэмминга длины N свитчингами $ijkl$ -компонент и которым соответствуют все различные $SQS(N)$ ранга не более r_N .

С учётом теоремы 2 получаем, что других $SQS(N)$ ранга не больше r_N , вложимых в расширенные совершенные двоичные коды такого же ранга, не существует. Так как в силу теоремы 1 существует в точности $2^{|SQS(\frac{N}{2})| - \frac{N}{2}} \cdot N! / |\text{Sym}(\overline{\mathcal{H}}, N/2)|$ различных $SQS(N)$ ранга не больше $r_N - 1$, вложимых в расширенные совершенные коды длины N такого же ранга, приходим к указанной в формулировке теоремы оценке. Теорема 3 доказана.

2. Системы четвёрок Штейнера, не вложимые в расширенные совершенные коды, построенные методом $ijkl$ -компонент

Теорема 4. Число $R'(N)$ различных $SQS(N)$ порядка $N \geq 128$ ранга r_N , не вложимых в расширенные совершенные двоичные коды, построенные методом $ijkl$ -компонент из расширенного двоичного кода Хэмминга, удовлетворяет неравенству

$$R'(N) \geq \frac{N(N-4)(N-8)}{3 \cdot 2^9} \cdot \left(\frac{N^2 + 16N - 512}{32} \right)^{N/64-1} \cdot 18912^{\frac{N}{64}} \cdot R(\overline{\mathcal{H}}, N/4).$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим $SQS(\overline{\mathcal{H}}, N)$, построенную способом, указанным в [7, теорема 1], а в ней — компоненты R_{ijkl}^{abcl} и R_{il}^1 . Напомним, что R_{il}^1 является линейной оболочкой векторов с носителями

$$\{ijkl, iaial, ijakal \mid a \in M \setminus l\},$$

а компонента R_{ijkl}^{abcl} и её разбиение на il -компоненты $R_{il}^{1abcl}, \dots, R_{il}^{8abcl}$ представлены в табл. 1.

Каждую компоненту $R_{il}^{1abcl}, \dots, R_{il}^{8abcl}$ можно разбить на два равных по мощности подмножества так, что R_{1il}^{1abcl} и $R_{2il}^{1abcl}, \dots, R_{1il}^{8abcl}$ и R_{2il}^{8abcl} соответствует одно и то же четырёхэлементное подмножество R_{1il}, \dots, R_{8il} из R_{il}^1 такое, что для каждого из множеств $R_{1il}^{1abcl} \cup R_{1il}, R_{2il}^{1abcl} \cup R_{1il}, \dots, R_{1il}^{8abcl} \cup R_{8il}, R_{2il}^{8abcl} \cup R_{8il}$ допустимы свитчинги элементов, переводящие эти множества в равновесные.

Таблица 1

R_{il}^{1abcl}	R_{il}^{2abcl}	R_{il}^{3abcl}	R_{il}^{4abcl}	R_{il}^{5abcl}	R_{il}^{6abcl}	R_{il}^{7abcl}	R_{il}^{8abcl}
$abcl$	aj_bj_cl	$jabj_cl$	$j_a j_b cl$	$jabj_c$	$ja j_b c$	$j j_a b c$	$j j_a j_b j_c$
$ai_b i_c l$	$ak_b k_c l$	$ja i_b k_c l$	$j_a k_b i_c l$	$ja i_b k_c$	$ja k_b i_c$	$j j_a i_b i_c$	$j j_a k_b k_c$
$ia b i_c l$	$ia j_b k_c l$	$ka b k_c l$	$ka j_b i_c l$	$ja b k_c$	$ja j_b i_c$	$j k_a b i_c$	$j k_a j_b k_c$
$ia i_b cl$	$ak_b j_c l$	$ka i_b j_c l$	$ka k_b cl$	$ja i_b j_c$	$ja k_b c$	$j k_a i_b c$	$j k_a k_b j_c$
$iab i_c$	$ia j_b k_c$	$ij_a b k_c$	$ij_a j_b i_c$	$kab k_c$	$ka j_b i_c$	$k j_a b i_c$	$k j_a j_b k_c$
$ia i_b c$	$ia k_b j_c$	$ij_a i_b j_c$	$ij_a k_b c$	$ka i_b j_c$	$ka k_b c$	$k j_a i_b c$	$k j_a k_b j_c$
$ii_a bc$	$ii_a j_b j_c$	$ik_a b j_c$	$ik_a j_b c$	$ki_a b j_c$	$ki_a j_b c$	$kk_a bc$	$kk_a j_b j_c$
$ii_a i_b i_c$	$ii_a k_b k_c$	$ik_a i_b j_c$	$ik_a k_b i_c$	$ki_a i_b k_c$	$ki_a k_b i_c$	$kk_a i_b i_c$	$kk_a k_b k_c$

Например, компонента $R_{il}^{1abcl} = \{abcl, ai_b i_c l, ia b i_c l, ia i_b cl, iab i_c, ia i_b c, ii_a bc, ii_a i_b i_c\}$ представима в виде

$$R_{il}^{1abcl} = \{abcl, ai_b i_c l, ii_a bc, ii_a i_b i_c\} \cup \{ia b i_c l, ia i_b cl, iab i_c, ia i_b c\},$$

т. е. $R_{1il}^{1abcl} = \{abcl, ai_b i_c l, ii_a bc, ii_a i_b i_c\}$ и $R_{2il}^{1abcl} = \{ia b i_c l, ia i_b cl, iab i_c, ia i_b c\}$. Тогда соответствующее им множество имеет вид

$$R_{1il} = \{ibi_b l, ici_c l, abi_a i_b, aci_a i_c\},$$

а каждое из множеств $R_{1il}^{1abcl} \cup R_{1il}$ и $R_{2il}^{1abcl} \cup R_{1il}$ допускает свитчинги $b \leftrightarrow i_c, l \leftrightarrow i_a, a \leftrightarrow i_a, c \leftrightarrow i_b$ и $b \leftrightarrow c, i_b \leftrightarrow i_c, l \leftrightarrow a, i \leftrightarrow i_a$ соответственно. Каждый из свитчингов $b \leftrightarrow i_c, l \leftrightarrow i_a, a \leftrightarrow i_a, c \leftrightarrow i_b$ переводит исходное множество $R_{1il}^{1abcl} \cup R_{1il}$ в одно и то же множество, равновесное ему. Также каждый из свитчингов $b \leftrightarrow c, i_b \leftrightarrow i_c, l \leftrightarrow a, i \leftrightarrow i_a$ переводит исходное множество $R_{2il}^{1abcl} \cup R_{1il}$ в одно и то же множество, равновесное ему.

Существует по крайней мере три таких различных разбиения каждой из компонент $R_{il}^{1abcl}, \dots, R_{il}^{8abcl}$.

Заметим, что перечисленные случаи не исчерпывают всех возможных, что позволяет получить только нижнюю оценку числа $SQS(N)$ ранга r_N , не вложимых в расширенные совершенные двоичные коды длины N такого же ранга.

Т а б л и ц а 2

R_{1il}^{rabc}	R_{2il}^{rabc}	R_{ril}^1	свитчинги $R_{1il}^{rabc} \cup R_{ril}^1$	свитчинги $R_{2il}^{rabc} \cup R_{ril}^1$
$labc$	$liabi_c$	$libib_b$	$b \leftrightarrow i_c$	$b \leftrightarrow c$
$lai_b i_c$	$li_a i_b c$	$lici_c$	$l \leftrightarrow i_a$	$i_b \leftrightarrow i_c$
$ii_a bc$	$ia i_b c$	$abi_a i_b$	$a \leftrightarrow i$	$l \leftrightarrow a$
$ii_a i_b i_c$	$iabi_c$	$aci_a i_c$	$c \leftrightarrow i_b$	$i \leftrightarrow i_a$
$jj_a bc$	$jkabi_c$	$jkbi_b$	$b \leftrightarrow i_c$	$b \leftrightarrow c$
$jj_a i_b i_c$	$jk_a i_b c$	$jkci_c$	$c \leftrightarrow i_b$	$i_b \leftrightarrow i_c$
$kk_a bc$	$kjabi_c$	$ja k_a bi_b$	$j \leftrightarrow k_a$	$j \leftrightarrow j_a$
$kk_a i_b i_c$	$kj_a i_b c$	$ja k_a ci_c$	$k \leftrightarrow j_a$	$k \leftrightarrow k_a$
$ja j_b c$	$ji_a j_b i_c$	$jkj_b k_b$	$j_b \leftrightarrow i_c$	$j_b \leftrightarrow c$
$jak_b i_c$	$ji_a k_b c$	$jkci_c$	$k_b \leftrightarrow c$	$k_b \leftrightarrow i_c$
$ki_a j_b c$	$kaj_b i_c$	$ai_a j_b k_b$	$j \leftrightarrow i_a$	$j \leftrightarrow a$
$ki_a k_b i_c$	$kak_b c$	$ai_a ci_c$	$k \leftrightarrow a$	$k \leftrightarrow i_a$
$jabj_c$	$jiabk_c$	$jkbi_b$	$b \leftrightarrow k_c$	$b \leftrightarrow j_c$
$jai_b k_c$	$ji_a i_b j_c$	$jkj_c k_c$	$i_b \leftrightarrow j_c$	$i_b \leftrightarrow k_c$
$ki_a bj_c$	$kabk_c$	$ai_a bi_b$	$j \leftrightarrow i_a$	$j \leftrightarrow a$
$ki_a i_b k_c$	$kai_b j_c$	$ai_a j_c k_c$	$k \leftrightarrow a$	$k \leftrightarrow i_a$
$lja j_b c$	$lk_a j_b i_c$	$lij_b k_b$	$j_b \leftrightarrow i_c$	$j_b \leftrightarrow c$
$lj_a k_b i_c$	$lk_a k_b c$	$lici_c$	$k_b \leftrightarrow c$	$k_b \leftrightarrow i_c$
$ika j_b c$	$ija j_b i_c$	$ja k_a j_b k_b$	$l \leftrightarrow k_a$	$l \leftrightarrow j_a$
$ika k_b i_c$	$ija k_b c$	$ja k_a ci_c$	$i \leftrightarrow j_a$	$i \leftrightarrow k_a$
$lja bj_c$	$lkabk_c$	$libib_b$	$b \leftrightarrow k_c$	$b \leftrightarrow j_c$
$lja i_b k_c$	$lk_a i_b j_c$	$lij_c k_c$	$i_b \leftrightarrow j_c$	$i_b \leftrightarrow k_c$
$ika bj_c$	$ijabk_c$	$ja k_a bi_b$	$l \leftrightarrow k_a$	$l \leftrightarrow j_a$
$ika i_b k_c$	$ija i_b j_c$	$ja k_a j_c k_c$	$i \leftrightarrow j_a$	$i \leftrightarrow k_a$
$la j_b j_c$	$lia j_b k_c$	$lij_b k_b$	$j_b \leftrightarrow k_c$	$j_b \leftrightarrow j_c$
$lak_b k_c$	$lia k_b j_c$	$lij_c k_c$	$k_b \leftrightarrow j_c$	$k_b \leftrightarrow k_c$
$ii_a j_b j_c$	$ia j_b k_c$	$ai_a j_b k_b$	$l \leftrightarrow i_a$	$l \leftrightarrow a$
$ii_a k_b k_c$	$iak_b j_c$	$ai_a j_c k_c$	$i \leftrightarrow a$	$i \leftrightarrow i_a$
$jj_a j_b j_c$	$jk_a j_b k_c$	$jkj_b k_b$	$j_b \leftrightarrow k_c$	$j_b \leftrightarrow j_c$
$jj_a k_b k_c$	$jk_a k_b j_c$	$jkj_c k_c$	$k_b \leftrightarrow j_c$	$k_b \leftrightarrow k_c$
$kk_a j_b j_c$	$kj_a j_b k_c$	$ja k_a j_b k_b$	$j \leftrightarrow k_a$	$j \leftrightarrow j_a$
$kk_a k_b k_c$	$kj_a k_b j_c$	$ja k_a j_c k_c$	$k \leftrightarrow j_a$	$k \leftrightarrow k_a$

В табл. 2–4 перечислены разбиения компонент, соответствующие им множества из R_{il}^1 и возможные свитчинги в каждом из трёх случаев. Многие из множеств R_{ril}^s , $r \in \{1, \dots, 8\}$, $s \in \{1, 2, 3\}$, как для фиксированных s и различных r , так и для различных s и r , пересекаются между собой, поэтому нельзя применять свитчинги ко всем множествам независимо.

Т а б л и ц а 3

R_{1il}^{rabc}	R_{2il}^{rabc}	R_{ril}^2	свитчинги $R_{1il}^{rabc} \cup R_{ril}^2$	свитчинги $R_{2il}^{rabc} \cup R_{ril}^2$
$labc$	$lai_b i_c$	$liai_a$	$a \leftrightarrow i_c$	$a \leftrightarrow c$
$li_a bi_c$	$li_a i_b c$	$lici_c$	$i_a \leftrightarrow c$	$i_a \leftrightarrow i_c$
$iai_b c$	$iabi_c$	$abi_a i_b$	$l \leftrightarrow i_b$	$l \leftrightarrow b$
$ii_a i_b i_c$	$ii_a bc$	$bci_b i_c$	$i \leftrightarrow b$	$i \leftrightarrow i_b$
$jja bc$	$jja i_b i_c$	$jkja k_a$	$j_a \leftrightarrow i_c$	$j_a \leftrightarrow c$
$jk_a bi_c$	$jk_a i_b c$	$jkci_c$	$k_a \leftrightarrow c$	$k_a \leftrightarrow i_c$
$kja i_b c$	$kja bi_c$	$ja k_a bi_b$	$j \leftrightarrow i_b$	$j \leftrightarrow b$
$kk_a i_b i_c$	$kk_a bc$	$bci_b i_c$	$k \leftrightarrow b$	$k \leftrightarrow i_b$
$ja j_b c$	$jak_b i_c$	$jkai_a$	$a \leftrightarrow i_c$	$a \leftrightarrow c$
$ji_a j_b i_c$	$ji_a k_b c$	$jkci_c$	$i_a \leftrightarrow c$	$i_a \leftrightarrow i_c$
$kak_b c$	$kaj_b i_c$	$j_b k_b ai_a$	$j \leftrightarrow k_b$	$j \leftrightarrow j_b$
$ki_a k_b i_c$	$ki_a j_b c$	$j_b k_b ci_c$	$k \leftrightarrow j_b$	$k \leftrightarrow k_b$
$jab j_c$	$jai_b k_c$	$jkai_a$	$a \leftrightarrow k_c$	$a \leftrightarrow j_c$
$ji_a bk_c$	$ji_a i_b j_c$	$jkj_c k_c$	$i_a \leftrightarrow j_c$	$i_a \leftrightarrow k_c$
$kai_b j_c$	$kab k_c$	$ai_a bi_b$	$j \leftrightarrow i_b$	$j \leftrightarrow b$
$ki_a i_b k_c$	$ki_a b j_c$	$bi_b j_c k_c$	$k \leftrightarrow b$	$k \leftrightarrow i_b$
$lja j_b c$	$lja k_b i_c$	$lija k_a$	$j_a \leftrightarrow i_c$	$j_a \leftrightarrow c$
$lk_a j_b i_c$	$lk_a k_b c$	$lici_c$	$k_a \leftrightarrow c$	$k_a \leftrightarrow i_c$
$ija k_b c$	$ija j_b i_c$	$ja k_a j_b k_b$	$l \leftrightarrow k_b$	$l \leftrightarrow j_b$
$ika k_b i_c$	$ika j_b c$	$j_b k_b ci_c$	$i \leftrightarrow j_b$	$i \leftrightarrow k_b$
$lja b j_c$	$lja i_b k_c$	$lija k_a$	$j_a \leftrightarrow k_c$	$j_a \leftrightarrow j_c$
$lk_a bk_c$	$lk_a i_b j_c$	$lij_c k_c$	$k_a \leftrightarrow j_c$	$k_a \leftrightarrow k_c$
$ija i_b j_c$	$ija bk_c$	$ja k_a bi_b$	$l \leftrightarrow i_b$	$l \leftrightarrow b$
$ika i_b k_c$	$ika b j_c$	$bi_b j_c k_c$	$i \leftrightarrow b$	$i \leftrightarrow i_b$
$laj_b j_c$	$lak_b k_c$	$liai_a$	$a \leftrightarrow k_c$	$a \leftrightarrow j_c$
$li_a j_b k_c$	$li_a k_b j_c$	$lij_c k_c$	$i_a \leftrightarrow j_c$	$i_a \leftrightarrow k_c$
$iak_b j_c$	$iaj_b k_c$	$ai_a j_b k_b$	$l \leftrightarrow k_b$	$l \leftrightarrow j_b$
$ii_a k_b k_c$	$ii_a j_b j_c$	$j_b k_b j_c k_c$	$i \leftrightarrow j_b$	$i \leftrightarrow k_b$
$jja j_b j_c$	$jja k_b k_c$	$jkja k_a$	$j_a \leftrightarrow k_c$	$j_a \leftrightarrow j_c$
$jk_a j_b k_c$	$jk_a k_b j_c$	$jkj_c k_c$	$k_a \leftrightarrow j_c$	$k_a \leftrightarrow k_c$
$kja k_b j_c$	$kja j_b k_c$	$ja k_a j_b k_b$	$j \leftrightarrow k_b$	$j \leftrightarrow j_b$
$kk_a k_b k_c$	$kk_a j_b j_c$	$j_b k_b j_c k_c$	$k \leftrightarrow j_b$	$k \leftrightarrow k_b$

Из табл. 2, 3 и 4 видно, что множества $R_{1il}^1, R_{2il}^1, R_{7il}^1, R_{8il}^1$ и $R_{3il}^1, R_{4il}^1, R_{5il}^1, R_{6il}^1$; $R_{1il}^2, R_{3il}^2, R_{6il}^2, R_{8il}^2$ и $R_{2il}^2, R_{4il}^2, R_{5il}^2, R_{7il}^2$; $R_{1il}^3, R_{4il}^3, R_{5il}^3, R_{8il}^3$ и $R_{2il}^3, R_{3il}^3, R_{6il}^3, R_{7il}^3$ соответственно не пересекаются между собой. Таким образом, имеем 6 наборов попарно не пересекающихся множеств.

Т а б л и ц а 4

R_{1il}^{rabc}	R_{2il}^{rabc}	R_{ril}^3	свитчинги $R_{1il}^{rabc} \cup R_{ril}^3$	свитчинги $R_{2il}^{rabc} \cup R_{ril}^3$
$labc$	$lai_b i_c$	$liai_a$	$a \leftrightarrow i_b$	$a \leftrightarrow b$
$li_a i_b c$	$li_a bi_c$	$libi_b$	$i_a \leftrightarrow b$	$i_a \leftrightarrow i_b$
$iabi_c$	$iai_b c$	$aci_a i_c$	$l \leftrightarrow i_c$	$l \leftrightarrow c$
$ii_a i_b i_c$	$ii_a bc$	$bci_b i_c$	$i \leftrightarrow c$	$i \leftrightarrow i_c$
$jj_a bc$	$jj_a i_b i_c$	$jkj_a k_a$	$j_a \leftrightarrow i_b$	$j_a \leftrightarrow b$
$jk_a i_b c$	$jk_a bi_c$	$jkbi_b$	$k_a \leftrightarrow b$	$k_a \leftrightarrow i_b$
$kj_a bi_c$	$kj_a i_b c$	$j_a k_a ci_c$	$j \leftrightarrow i_c$	$j \leftrightarrow c$
$kk_a i_b i_c$	$kk_a bc$	$bi_b ci_c$	$k \leftrightarrow c$	$k \leftrightarrow i_c$
$ja_j b c$	$jak_b i_c$	$jkai_a$	$a \leftrightarrow k_b$	$a \leftrightarrow j_b$
$ji_a k_b c$	$ji_a j_b i_c$	$jkj_b k_b$	$i_a \leftrightarrow j_b$	$i_a \leftrightarrow k_b$
$kaj_b i_c$	$kak_b c$	$ai_a ci_c$	$j \leftrightarrow i_c$	$j \leftrightarrow c$
$ki_a k_b i_c$	$ki_a j_b c$	$j_b k_b ci_c$	$k \leftrightarrow c$	$k \leftrightarrow i_c$
$jab_j c$	$jai_b k_c$	$jkai_a$	$a \leftrightarrow i_b$	$a \leftrightarrow b$
$ji_a i_b j_c$	$ji_a bk_c$	$jkbi_b$	$i_a \leftrightarrow b$	$i_a \leftrightarrow i_b$
$kabk_c$	$kai_b j_c$	$ai_a j_c k_c$	$j \leftrightarrow k_c$	$j \leftrightarrow j_c$
$ki_a i_b k_c$	$ki_a bj_c$	$bi_b j_c k_c$	$k \leftrightarrow j_c$	$k \leftrightarrow k_c$
$l_j a j_b c$	$l_j a k_b i_c$	$li_j a k_a$	$j_a \leftrightarrow k_b$	$j_a \leftrightarrow j_b$
$lk_a k_b c$	$lk_a j_b i_c$	$li_j b k_b$	$k_a \leftrightarrow j_b$	$k_a \leftrightarrow k_b$
$i_j a j_b i_c$	$i_j a k_b c$	$j_a k_a ci_c$	$l \leftrightarrow i_c$	$l \leftrightarrow c$
$ik_a k_b i_c$	$ik_a j_b c$	$j_b k_b ci_c$	$i \leftrightarrow c$	$i \leftrightarrow i_c$
$l_j a b j_c$	$l_j a i_b k_c$	$li_j a k_a$	$j_a \leftrightarrow i_b$	$j_a \leftrightarrow b$
$lk_a i_b j_c$	$lk_a bk_c$	$libi_b$	$k_a \leftrightarrow b$	$k_a \leftrightarrow i_b$
$i_j a bk_c$	$i_j a i_b j_c$	$j_a k_a j_c k_c$	$l \leftrightarrow k_c$	$l \leftrightarrow j_c$
$ik_a i_b k_c$	$ik_a bj_c$	$bi_b j_c k_c$	$i \leftrightarrow j_c$	$i \leftrightarrow k_c$
$la_j b j_c$	$lak_b k_c$	$liai_a$	$a \leftrightarrow k_b$	$a \leftrightarrow j_b$
$li_a k_b j_c$	$li_a j_b k_c$	$li_j b k_b$	$i_a \leftrightarrow j_b$	$i_a \leftrightarrow k_b$
$ia_j b k_c$	$iak_b j_c$	$ai_a j_c k_c$	$l \leftrightarrow k_c$	$l \leftrightarrow j_c$
$ii_a k_b k_c$	$ii_a j_b j_c$	$j_b k_b j_c k_c$	$i \leftrightarrow j_c$	$i \leftrightarrow k_c$
$jj_a j_b j_c$	$jj_a k_b k_c$	$jkj_a k_a$	$j_a \leftrightarrow k_b$	$j_a \leftrightarrow j_b$
$jk_a k_b j_c$	$jk_a j_b k_c$	$jkj_b k_b$	$k_a \leftrightarrow j_b$	$k_a \leftrightarrow k_b$
$kj_a j_b k_c$	$kj_a k_b j_c$	$j_a k_a j_c k_c$	$j \leftrightarrow k_c$	$j \leftrightarrow j_c$
$kk_a k_b k_c$	$kk_a j_b j_c$	$j_b k_b j_c k_c$	$k \leftrightarrow j_c$	$k \leftrightarrow k_c$

Поскольку каждому из 4 множеств вида R_{ril}^s любого набора соответствует 2 множества вида $R_{1il}^{rabc} \cup R_{ril}^s$ и $R_{2il}^{rabc} \cup R_{ril}^s$, к каждому из которых можно применить (либо не применять) допустимый свитчинг, каждый из наборов допускает $3^4 - 1$ различных свитчингов. Также не пересекаются между собой следующие комбинированные множества из различных

табл. 2–4:

$$\begin{array}{ll}
 R_{1il}^1, R_{8il}^1, R_{2il}^2, R_{7il}^2, R_{4il}^3, R_{5il}^3; & R_{1il}^1, R_{8il}^1, R_{3il}^2, R_{6il}^2, R_{2il}^3, R_{7il}^3; \\
 R_{2il}^1, R_{7il}^1, R_{1il}^2, R_{8il}^2, R_{3il}^3, R_{6il}^3; & R_{2il}^1, R_{7il}^1, R_{4il}^2, R_{5il}^2, R_{1il}^3, R_{8il}^3; \\
 R_{3il}^1, R_{6il}^1, R_{1il}^2, R_{8il}^2, R_{4il}^3, R_{5il}^3; & R_{3il}^1, R_{6il}^1, R_{4il}^2, R_{5il}^2, R_{2il}^3, R_{7il}^3; \\
 R_{4il}^1, R_{5il}^1, R_{2il}^2, R_{7il}^2, R_{3il}^3, R_{6il}^3; & R_{4il}^1, R_{5il}^1, R_{3il}^2, R_{6il}^2, R_{1il}^3, R_{8il}^3.
 \end{array}$$

Таким образом, имеем дополнительно 8 наборов попарно не пересекающихся множеств. Так как каждому из 6 множеств вида R_{ril}^s любого набора соответствует 2 множества вида $R_{1il}^{abcl} \cup R_{ril}^s$ и $R_{2il}^{abcl} \cup R_{ril}^s$, к каждому из которых можно применить (либо не применять) допустимый свитчинг, каждый из наборов допускает $3^6 - 1$ различных свитчингов.

Поскольку в таблицах приведены разбиения компонент и свитчинги, приводящие их к равновесным множествам, получающиеся в результате системы четвёрок являются SQS . Отсюда для разбиения R_{ijkl}^{abcl} на il -компоненты получаем по крайней мере

$$6 \cdot (3^4 - 1) + 8 \cdot (3^6 - 1) = 2 \cdot 3^5(1 + 12) - 14 = 6304$$

различных свитчингов. Для разбиения R_{ijkl}^{abcl} на jl - и kl -компоненты ситуация аналогична. Следовательно, всего имеем $3 \cdot 6304 = 18912$ различных свитчингов для любой четвёрки из $SQS(N/4)$. Для того чтобы свитчинги могли быть применены к компонентам вида $R_{ijkl}^{\alpha_t}$ для различных четвёрок $\alpha_t \in SQS(N/4)$ независимо, эти четвёрки не должны пересекаться. Так как для любой четвёрки α_t из $SQS(N/4)$ существует $4(N-4)(N-8)/3 \cdot 2^5$ четвёрок, пересекающихся с ней по одному элементу, и $3N/4 - 18$ четвёрок, пересекающихся с ней по паре элементов, для α_t существует всего $z = (N-4)(N-8)/3 \cdot 2^3 + 3N/4 - 18 = (N^2 + 6N - 376)/24$ четвёрок, имеющих с ней общие элементы, и

$$|SQS(N/4)| - 1 - z = \frac{(N-4)(N-8)(N-64)}{3} \cdot 2^9 - \frac{3N}{4} + 17$$

четвёрок, поэлементно не пересекающихся с α_t . Таким образом, первую четвёрку для свитчинга внутри компоненты R_{ijkl}^{abcl} можно выбрать среди всех $|SQS(N/4)|$ четвёрок, вторую, не имеющую с первой общих элементов — среди $|SQS(N/4)| - z - 1$ четвёрок. Третью четвёрку, не имеющую общих элементов с первыми двумя, можно выбрать среди оставшихся $|SQS(N/4)| - 2(z - 1)$ четвёрок. Продолжая процесс таким образом, нетрудно посчитать, что можно найти по крайней мере $N/64$ четвёрок, попарно не имеющих общих элементов. Далее, существует не менее

$$|SQS(N/4)| \cdot (|SQS(N/4)| - z + 1) \cdot (|SQS(N/4)| - 2(z + 1))$$

$$\begin{aligned} & \times \dots \times (|SQS(N/4)| - (N/64 - 1)(z + 1)) \\ & > |SQS(N/4)| \cdot \left(\frac{N^2 + 16N - 512}{32} \right)^{N/64-1} \end{aligned}$$

вариантов выбора таких наборов из 64 четвёрок. Поскольку для произвольной такой четвёрки существует по крайней мере 18912 различных свитчингов, каждый из которых переводит исходную компоненту в равновесное ей множество, найдётся по крайней мере

$$\frac{N(N-4)(N-8)}{3 \cdot 2^9} \cdot \left(\frac{N^2 + 16N - 512}{32} \right)^{N/64-1} \cdot 18912^{\frac{N}{64}}$$

разных свитчингов, приводящих исходную SQS к различным $SQS(N)$. Получающиеся системы различны, так как при таких свитчингах задействованы разные подмножества исходного множества четвёрок. Так как в качестве исходной $SQS(N/4)$ можно брать любую хэммингову, указанная в формулировке оценка становится очевидной. Ранг таких $SQS(N)$ зависит от ранга $SQS(N/4)$ и потому может превышать r_N .

В результате этих свитчингов не меняется полностью ни одна из il -, jl -, kl -компонент исходной SQS . Значит, получающиеся в результате приведённых свитчингов системы не совпадают с SQS , отвечающими расширенным совершенным кодам, получающимся из расширенного кода Хэмминга свитчингами $ijkl$ -компонент. Теорема 4 доказана.

Следствие 1. Ранг $r(SQS(N))$ системы $SQS(N)$, построенной с помощью свитчингов, указанных в теореме 4, из некоторой $SQS(N/4)$ ранга $r(SQS(N/4))$, удовлетворяет неравенству

$$r(SQS(N)) \geq r(SQS(N/4)) + 3N/4 - 1.$$

Вопрос о том, вложимы ли SQS из теоремы 4 в расширенные совершенные коды, остаётся открытым.

ЛИТЕРАТУРА

1. **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.
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 // Пробл. кибернетики. — Вып. 8. — С. 337–339.

4. 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.
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 // Пробл. передачи информ. — 2007. — Т. 43, № 1. — С. 39–55.
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. Ковалевская Д. И., Соловьёва Ф. И. О системах четвёрок Штейнера малого ранга, вложимых в расширенные совершенные двоичные коды // Дискрет. анализ и исслед. операций. — 2012. — Т. 19, № 5. — С. 47–62.
8. Ковалевская Д. И., Соловьёва Ф. И., Филимонова Е. С. О системах троек Штейнера малого ранга, вложимых в совершенные двоичные коды // Дискрет. анализ и исслед. операций. — 2013. — Т. 20, № 3. — С. 3–25.
9. 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.
10. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. Теория кодов, исправляющих ошибки. — М.: Связь, 1979. — 744 с.
11. Петренюк А. Я. Признаки неизоморфности систем троек Штейнера // Укр. мат. журн. — 1972. — Т. 24, № 6. — С. 772–780.
12. 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.
13. Doyen J., Hubaut X., Vandensavel M. Ranks of incidence matrices of Steiner triple systems // Math. — 1978. — Vol. 163. — P. 251–259.
14. Doyen J., Vandensavel M. Nonisomorphic Steiner quadruple systems // Bull. Soc. Math. Belg. — 1971. — Vol. 23. — P. 393–410.
15. Hanani H. On quadruple systems // Can. J. Math. — 1960. — Vol. 12. — P. 145–157.
16. Hanani H. The existence and construction of balanced incomplete block designs // Ann. Math. Stat. — 1961. — Vol. 32, N 2. — P. 361–386.
17. Lenz H. On the number of Steiner quadruple systems // Mitt. Math. Seminar Giessen. — 1985. — Vol. 169. — P. 55–71.
18. Lindner C. C. On the construction of nonisomorphic Steiner quadruple systems // Colloq. Math. — 1974. — Vol. 29. — P. 303–306.
19. 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.
20. 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.

- 21. 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. — P. 260–274.
- 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

Статья поступила
11 октября 2012 г.
Переработанный вариант —
6 июня 2013 г.