ISSN 1990-4789, Journal of Applied and Industrial Mathematics, 2013, Vol. 7, No. 4, pp. 522–536. © Pleiades Publishing, Ltd., 2013.
Original Russian Text © D.I. Kovalevskaya, F.I. Solov'eva, 2013, published in Diskretnyi Analiz i Issledovanie Operatsii, 2013, Vol. 20, No. 4, pp. 46–64.

Steiner Quadruple Systems of Small Rank and Extended Perfect Binary Codes

D. I. Kovalevskaya[1*] and F. I. Solov'eva[1,2]**

[1]*Sobolev Institute of Mathematics, pr. Akad. Koptyuga 4, Novosibirsk, 630090 Russia*
[2]*Novosibirsk State University, ul. Pirogova 2, Novosibirsk, 630090 Russia*
Received October 11, 2012; in final form, June 6, 2013

Abstract—Using the switching method, we give a classification for the Steiner quadruple systems of order $N > 8$ and rank r_N (different by 2 from the rank of the Hamming code of length N) which are embedded into the extended perfect binary codes of length N and the same rank. Some lower and upper bounds are provided on the number of these different systems. The lower bound and description of different Steiner quadruple systems of order N and rank r_N which are not embedded into the extended perfect binary codes of length N and the same rank are given.

DOI: 10.1134/S1990478913040078

Keywords: *Steiner quadruple system, extended perfect binary code, switching, il- and ijkl-components, rank*

INTRODUCTION

Let $\mathbb{F}^n$ be the n-dimensional metric space over the Galois field $GF(2)$ with respect to the Hamming metric. The *Hamming distance* $d(x, y)$ between every pair of vectors x and y from $\mathbb{F}^n$ is the number of coordinates in which x and y differ. The *Hamming weight* $w(x)$ of $x \in \mathbb{F}^n$ is the number of nonzero coordinates of x. A nonempty subset C of $\mathbb{F}^n$ is a *binary code*. A vector subspace of $\mathbb{F}^n$ is a *binary linear code*. The elements of C are called *codewords*. The parameters of a binary code C from $\mathbb{F}^n$ are denoted by $(n, |C|, d)$, where n is the length of the codewords (elements of the code), $|C|$ is the size of the code, and d is the minimum distance of the code (i.e., the minimum Hamming distance between the codewords). The set of nonzero coordinate entries of a vector $x \in \mathbb{F}^n$ is called a *support* of x and denoted by $\mathrm{supp}(x)$.

A binary code C of length n with distance $d = 2d' + 1$ is called *perfect one-error correcting* (further mentioned as *perfect*) if, for every vector $x \in \mathbb{F}^n$, there exists only one codeword y in C such that $d(x, y) = 1$. A linear perfect code of length n, called the *Hamming code* (we denote it by $\mathcal{H}^n$), is unique up to equivalence. It is known ([10]) that perfect codes have the following parameters: length $n = 2^r - 1$ with $r > 1$, 2^{n-r} codewords, and the minimum distance 3.

Let $\overline{C}$ be the *extended perfect code* of length $N = 2^r$ obtained from a perfect code C of length $2^r - 1$, $r \geq 2$, by parity checking; i.e., adding the coordinate entry equals the sum by modulo 2 of all other entries. In the sequel, we will consider only perfect and extended perfect codes containing all-zero vector. The *rank* of a code C is the dimension of the linear span of C in $\mathbb{F}^n$.

It is said that the code $C' = (C \backslash M) \cup M'$ is obtained by a *switching* of M to M' in the binary code C if C' has the same parameters as C, see [1]. The set M is called a *component* of C. The set M is called the *il-component* of the code $\overline{C}$ of length N obtained from C by extending by lth coordinate if $M' = M \oplus e_i \oplus e_l$ for some $i \in \{1, 2, \ldots, N\}$, where e_i and e_l are the vectors of weight 1 with 1 in the ith and lth coordinate entries respectively. The set R is called the *ijkl-component* of $\overline{C}$ if R is the t_1t_2-component for every $t_1, t_2 \in \{i, j, k, l\}$.

*E-mail: daryik@rambler.ru
**E-mail: sol@math.nsc.ru

It is known [20] that every extended perfect code of length N and rank $r_N - 1 = N - \log N$ is a Vasil'ev code [3]. The code can be constructed by switchings of il-components from an extended Hamming code by some function $\lambda : \mathcal{H}^{N/2-1} \to \{0,1\}$. Denote the code by $\overline{V}_\lambda^N$. Up to equivalence the code $\overline{V}_\lambda^N$ has the following representation:

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

Let V be some v-element set, a t-(v,k,λ)-*design* is a collection of blocks from v different elements such that every block contains k different elements and each t-element subset from V is appeared in exactly λ blocks. A 3-$(v,4,1)$-design is called a *Steiner quadruple system of order* v and denoted by SQS(v) (or briefly SQS if the order of the system does not matter). Given a block (i,j,k,l) from SQS(v), we match up the vector from $\mathbb{F}^n$ with 1 only in the ith, jth, kth, and lth coordinate entries. Further, from the context it will always be clear if we consider blocks, supports, or vectors corresponding to them. It is known [15] that SQS(v) exists if and only if $v \equiv 2, 4 \pmod 6$. The supports of the codewords of weight 4 in a code $\overline{C}$ define SQS(2^r) [10]. The system SQS$(\overline{\mathcal{H}}, N)$ corresponding to an extended Hamming code $\overline{\mathcal{H}}^N$ of length N is called the *Hamming–Steiner quadruple system* by analogy to the Hamming–Steiner triple systems in [7, 12]. They are called also *Boolean* [5, 6]. Two SQSs are *equivalent* if there exists a one-to-one correspondence of their ground sets mapping the blocks of one system into the blocks of the other.

The main problem in this field is the classification and enumeration of all nonequivalent SQSs (see the progress in [4, 5]). The best lower [17] and upper [14] bounds on the number $N(v)$ of all nonequivalent SQS(v)s are as follows:

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

The *rank* of SQS(N), $N = 2^r$, is the dimension of a linear subspace in $\mathbb{F}^N$ spanned over SQS(N). It is known that the rank of SQS(N) can vary from $r_N - 2$, which is the rank of the Hamming code of length $N - 1$ [13], till the full rank $N - 1$.

The notion of switching for SQS is defined similarly to that for the extended perfect binary code. Two sets R and R' consisted of 4-element subsets of V are called *equilibrium* if every unordered triple of elements, which can be found in the quadruples of one set, appears also in the quadruples of the other. It is said that

$$\mathrm{SQS}'(N) = (\mathrm{SQS}(N) \backslash R) \cup R'$$

is obtained by a *switching* from the set of blocks R to the set of blocks R' in SQS(N) if R and R' are equilibrium sets (see the definition of an equilibrium set in [11] and the description of switching methods in [6]). In [6], the set R as far as the set R' is called *component*.

In [21], the number $R_1(N)$ is obtained of different SQS(N)s of rank $r_N - 1$ which is more by 1 than the minimal possible rank:

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

A *parallel class* in 3-$(N,4,1)$-design, where $N \equiv 0 \pmod 4$, is defined as the set of the $N/4$ pairwise disjoint blocks. SQS(N) is called *resolvable* if the set of its blocks can be partition into

$$r = (N-1)(N-2)/6$$

nonintersecting parallel classes. In [5], the constructions of different SQS(N)s of rank at most r_N are presented. It is proved that all these systems are resolvable and the number of all different resolvable SQSs having some fixed parallel class is found:

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

Since there exist $N!/24^{N/4}$ different parallel classes; therefore, using [5], we obtain that the number of all different SQS(N)s of rank at most r_N is

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

It is proved in [19] that only 15590 of 1054163 Steiner quadruple systems SQS(16) are embedded into the perfect codes. It is shown in [22] that all Steiner triple systems of order $n = N - 1 = 2^r - 1 > 7$ and rank r_N are embedded into some perfect codes, but the ranks of these codes are still unknown.

In [7], the construction of SQS embedded into the extended perfect binary codes built from an extended Hamming code by the method of $ijkl$-components is obtained. There is given the lower bound on the number of different such systems. It is known [1] that the codes (and also the corresponding SQSs) obtained by this method have the rank at most 2 more than the rank of the Hamming code. But it was unknown if there exist other SQSs embedded into the extended perfect binary codes.

This paper is a development of [7, 8]. The main results are the following: a classification of SQS(N)s, $N = 2^r > 8$, of rank r_N embedded into the extended perfect binary codes of length N and the same rank; the proof that the class of SQS(N)s, $N = 2^r > 8$, of rank r_N obtained in [7] coincides with the class of SQSs embedded into the extended perfect binary codes of length N and the same rank. It is unclear if all SQSs with the rank that exceeds the rank of the Hamming SQS by at most 2 are embedded in some extended perfect binary codes of bigger ranks. In [4], the classification of SQSs of rank $r_N - 1$ using the concatenation approach is given; and it is shown that all these SQSs are embeddable into the extended Vasil'ev codes of the same rank. In the presented paper, we give another proof of this fact by the switching method. Moreover, we describe all SQS(N)s of rank r_N that are not embeddable into the extended perfect codes of length N obtained by the method of $ijkl$-component from an extended Hamming code; and the lower bound is given on the number of these SQSs.

1. THE NUMBER OF DIFFERENT SQS(N)S OF RANKS $r_N - 1$ AND r_N EMBEDDED INTO THE EXTENDED PERFECT CODES OF THE SAME RANKS

The order of the group of symmetries of an extended Hamming code $\overline{\mathcal{H}}^N$ satisfies

$$|\mathrm{Sym}(\overline{\mathcal{H}}, N)| = (N-1)(N-2)(N-2^2)(N-2^3)\ldots N/2, \tag{3}$$

see [10, Chapt. 13]. It is known that the rank of every extended perfect code $\overline{V}_\lambda^N$ of length N which is obtained from a code $\overline{\mathcal{H}}^N$ by switchings of il-components using some function λ is at most $r_N - 1$. Therefore, the same is true for the rank of SQS(N) corresponding to this extended perfect code, obtained by switchings of il-components from a Hamming SQS(N). By this, applying the well-known Lindner's construction [18] for an SQS embedded into the extended perfect Vasil'ev codes, and also comparing with the number of different SQS(N)s of rank at most $r_N - 1$ (obtained in [21]), we prove by the switching method that the class of SQS(N)s having rank $r_N - 1$ coincides with the class of SQSs embedded into the codes $\overline{V}_\lambda^N$ of the same rank. Another proof of this fact—using the concatenation construction—see in [4].

Theorem 1. *Each* SQS(N) *of rank* $r_N - 1$ *is embeddable into some extended perfect Vasil'ev code of length N and the same rank.*

Proof. Let A be the incident matrix of a Hamming SQS(N) with $N = 2^r$. The rows of the matrix are the binary vectors of weight 4 with 1s in the coordinates corresponding to the blocks of this Hamming SQS. Then (see [21]) the matrix G consisting of the rows of the matrix A and the vector $(1, 1, 0, \ldots, 0)$ is the generating matrix of the code C which contains $2^{|\mathrm{SQS}(N/2)|}$ different SQS(N)s of rank at most $r_N - 1$. The number of different such codes is equal to

$$\frac{N!}{2^{N/2} \cdot |\mathrm{Sym}(\overline{\mathcal{H}},\, N/2)|}.$$

Let us prove that every SQS of the code C is embedded into some extended Vasil'ev code $\overline{V}_\lambda^N$ of length N and the same rank. Since every perfect code of length N and rank at most $r_N - 1$ is an extended Vasil'ev code [20], constructed from the Hamming code of length $N/2-1$ with some nonlinear function λ; therefore, we have the embeddability of each SQS from C into some extended perfect code.

Up to equivalence an extended Hamming code $\overline{\mathcal{H}}^N$ can be represented as

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

A codeword of weight 4 of the code C is either a row of the matrix A, or is obtained by adding $(1,1,0,\dots,0)$ to the codeword of weight 4 from $\overline{\mathcal{H}}^N$ having nonzero first or second coordinates (i.e., of the type $(1,0,\dots)$ or $(0,1,\dots)$), or is obtained by adding $(1,1,0,\dots,0)$ to the codeword of weight 6 from $\overline{\mathcal{H}}^N$ with the first two nonzero coordinates (i.e., of the type $(1,1,\dots)$).

Let A_0, A_1, A_2, and A_3 denote the set of rows of the matrix A such that the first two elements are equal to 1, the first element equals 1 and the second is 0, the first element is equal to 0 and the second to 1, the first two elements equal 0 respectively.

Let B_1, B_2, and B_3 stand for the sets of weight 4 of the vectors

- with the first coordinate equal to 1 and the second equal to 0 that are obtained by adding the vector $(1,1,0,\dots,0)$ to the rows of A_2,
- with the first coordinate equal to 0 and the second equal to 1 that are obtained by adding the vector $(1,1,0,\dots,0)$ to the rows of A_1,
- with the first two coordinates equal to 0 obtained by adding $(1,1,0,\dots,0)$ to the codewords of weight 6 from $\overline{\mathcal{H}}^N$ of the type $(1,1,\dots)$ with the first two nonzero coordinates.

Then, by [21], the different SQSs are obtained by switchings of some k' rows of $A_{123} = A_1 \cup A_2 \cup A_3$ by some appropriate k' rows of the matrix $B_{123} = B_1 \cup B_2 \cup B_3$. The sets of triples corresponding to the rows will be equilibrium sets. The sets of such rows we also call *equilibrium*. Moreover, A_{123} and B_{123} can be partition into the subsets consisting of 8 blocks so that, for every eight blocks from A_{123}, there exits a unique set of eight blocks from B_{123}; i.e.,

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

Define the function $\lambda : \mathcal{H}^{N/2-1} \to \{0,1\}$ for the code $\overline{V}_\lambda^N$ containing SQS obtained in result of the following switching: for the vectors of weight 3 and (or) 4 corresponding to the k' replaceable rows of A_{123} and the k' replacing rows of B_{123}, put $\lambda = 1$; for the other vectors from $\mathcal{H}^{N/2-1}$ put $\lambda = 0$.

Let $y \in \mathcal{H}^{N/2-1}$ be a vector with the support $\{a_1, a_2, a_3\}$, where $\lambda = 1$. Then, in $\mathbb{F}^{N/2-1}$, there exist the three vectors of weight 1 intersecting y in one coordinate entry. By the construction of $\overline{V}_\lambda^N$, every of these three vectors together with y defines the weight 4 vectors in $\overline{V}_\lambda^N$ of the type

$$\Big(1, a_2, a_3, \frac{N}{2}+1+a_1\Big), \qquad \Big(1, a_1, a_3, \frac{N}{2}+1+a_2\Big), \qquad \Big(1, a_1, a_2, \frac{N}{2}+1+a_3\Big),$$

corresponding to the weight 4 vectors in H^N of the type

$$\Big(2, a_2, a_3, \frac{N}{2}+1+a_1\Big), \qquad \Big(2, a_1, a_3, \frac{N}{2}+1+a_2\Big), \qquad \Big(2, a_1, a_2, \frac{N}{2}+1+a_3\Big)$$

respectively.

We can find the three weight 2 vectors in $\mathbb{F}^{N/2-1}$ intersecting y in two coordinate entries. By the construction of $\overline{V}_\lambda^N$, every of these vectors together with y generates the weight 4 vectors in $\overline{V}_\lambda^N$ of the type

$$\Big(2, a_3, \frac{N}{2}+1+a_1, \frac{N}{2}+1+a_2\Big), \qquad \Big(2, a_2, \frac{N}{2}+1+a_1, \frac{N}{2}+1+a_3\Big),$$
$$\Big(2, a_1, \frac{N}{2}+1+a_2, \frac{N}{2}+1+a_3\Big),$$

that correspond to weight 4 vectors in H^N of the type

$$\Big(1, a_3, \frac{N}{2}+1+a_1, \frac{N}{2}+1+a_2\Big), \qquad \Big(1, a_2, \frac{N}{2}+1+a_1, \frac{N}{2}+1+a_3\Big),$$
$$\Big(1, a_1, \frac{N}{2}+1+a_2, \frac{N}{2}+1+a_3\Big)$$

respectively.

Moreover, using the vector $0^{N/2-1}$ and the weight 3 vector from $\mathbb{F}^{N/2-1}$ with the support $\{a_1, a_2, a_3\}$, we additionally obtain the vectors from $\overline{V}_\lambda^N$ of the types

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

corresponding to the weight 4 vectors in H^N of the types

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

respectively.

In result, we have the two equilibrium sets in $\overline{V}_\lambda^N$ and $\overline{\mathcal{H}}^N$, each one containing eight quadruples.

Let $y = (b_1, b_2, b_3, b_4)$ be the vector with the support $\{b_1, b_2, b_3, b_4\}$ such that $\lambda(y) = 1$. In $\mathbb{F}^{N/2-1}$, there exist the four weight 1 vectors intersecting y in one coordinate entry. By the construction of $\overline{V}_\lambda^N$, these vectors together with y define the weight 4 vectors in $\overline{V}_\lambda^N$ of the type

$$\Big(b_2, b_3, b_4, \frac{N}{2}+1+b_1\Big), \qquad \Big(b_1, b_3, b_4, \frac{N}{2}+1+b_2\Big),$$
$$\Big(b_1, b_2, b_4, \frac{N}{2}+1+b_3\Big), \qquad \Big(b_1, b_2, b_3, \frac{N}{2}+1+b_4\Big).$$

The four weight 3 vectors exist in $\mathbb{F}^{N/2-1}$ which intersect y in three coordinate entries. By the construction of $\overline{V}_\lambda^N$, each of them together with y generates the weight 4 vectors in $\overline{V}_\lambda^N$ of the type

$$\Big(b_4, \frac{N}{2}+1+b_1, \frac{N}{2}+1+b_2, \frac{N}{2}+1+b_3\Big), \qquad \Big(b_3, \frac{N}{2}+1+b_1, \frac{N}{2}+1+b_2, \frac{N}{2}+1+b_4\Big),$$
$$\Big(b_2, \frac{N}{2}+1+b_1, \frac{N}{2}+1+b_3, \frac{N}{2}+1+b_4\Big), \qquad \Big(b_1, \frac{N}{2}+1+b_2, \frac{N}{2}+1+b_3, \frac{N}{2}+1+b_4\Big).$$

There exist the six weight 2 vectors in $\mathbb{F}^{N/2-1}$ intersecting y in some two coordinates so that, by the construction (4), together with y they define in $\overline{\mathcal{H}}^N$ the following weight 4 vectors of the type

$$\Big(b_3, b_4, \frac{N}{2}+1+b_1, \frac{N}{2}+1+b_2\Big), \qquad \Big(b_2, b_4, \frac{N}{2}+1+b_1, \frac{N}{2}+1+b_3\Big),$$
$$\Big(b_2, b_3, \frac{N}{2}+1+b_1, \frac{N}{2}+1+b_4\Big), \qquad \Big(b_1, b_4, \frac{N}{2}+1+b_2, \frac{N}{2}+1+b_3\Big),$$
$$\Big(b_1, b_3, \frac{N}{2}+1+b_2, \frac{N}{2}+1+b_4\Big), \qquad \Big(b_1, b_2, \frac{N}{2}+1+b_3, \frac{N}{2}+1+b_4\Big).$$

Moreover, we have in $\mathbb{F}^{N/2-1}$ the unique all-zero vector and a unique weight 4 vector with the support $\{b_1, b_2, b_3, b_4\}$ such that, by the construction (4), together with y they define the weight 4 vectors in $\overline{\mathcal{H}}^N$ of the type

$$(b_1, b_2, b_3, b_4), \qquad \left(\frac{N}{2}+1+b_1, \frac{N}{2}+1+b_2, \frac{N}{2}+1+b_3, \frac{N}{2}+1+b_4\right)$$

respectively. Therefore, we can conclude that we obtain the two equilibrium sets and each contains eight vectors. These are the subsets from $\overline{V}_\lambda^N$ and $\overline{\mathcal{H}}^N$ respectively. Note that the sets of quadruples from the first and second cases under consideration do not intersect each other. Both equilibrium sets of eight quadruples correspond to the switchings described in [21].

Hence, the system SQS obtained by switchings of some k' row of the matrix $A_1 \cup A_2 \cup A_3$ by equilibrium k' rows of $B_1 \cup B_2 \cup B_3$ is embeddable into the code $\overline{V}_\lambda^N$ by the above-defined function λ.

Since all extended codes of length N of the rank at most $r_N - 1$ are the Vasil'ev codes of length N obtained from the Hamming code $\mathcal{H}^{N/2-1}$ by construction (1), each SQS(N) of rank $r_N - 1$ is embeddable into some extended perfect Vasil'ev code of length N and rank $r_N - 1$. Moreover, there exist

$$2^{|\mathrm{SQS}(N/2)|-N/2} \cdot N!/|\mathrm{Sym}(\overline{\mathcal{H}},\ N/2)$$

different such SQSs. Taking it into account that, by [21], the number of SQS(N)s having rank $r_N - 2$ is equal to $N!/N \cdot |\mathrm{Sym}(\overline{\mathcal{H}},\ N/2)|$, we obtain (2). This completes the proof of Theorem 1. $\square$

Note that the described switchings correspond to the switchings under transition from SQS(N) obtained by the Hahani's construction [16] to SQS(N) obtained by the Aliev's construction [2]. It is known that the Lindner's construction is a generalization of the Hahani's construction [18].

Let $R(\overline{\mathcal{H}}, N)$ denote the number of different SQS$(\overline{\mathcal{H}}, N)$s of order N. Taking into account (3), we have

$$R(\overline{\mathcal{H}}, N) = \frac{N!}{|\mathrm{Sym}(\overline{\mathcal{H}}, N)|}.$$

By [1], the rank of an extended perfect code of length N obtained from an extended Hamming code of length N by switchings of $ijkl$-components is at most r_N. Therefore, the rank of SQS(N) obtained from a Hamming SQS(N) by switchings of $ijkl$-components is at most r_N. We have

Theorem 2 [9]. *Each extended perfect binary code $\overline{C}$ of length N and rank at most r_N can be obtained from some extended Hamming code by consecutive switchings of il-components using at most two coordinates (il- and jl- for some i, j, l).*

In [7, Theorem 4], it is presented the construction of a Steiner quadruple system and the corresponding switchings of il- and $ijkl$-components which allow us to obtain from a Hamming SQS(N) some SQS(N) of a bigger rank. Denote the class of SQS(N)s of rank r obtained in such a way by Sw(SQS$(N), r$).

Let

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

$$S(N) = 2^{|\mathrm{SQS}(\frac{N}{2})|-\frac{N}{2}} \cdot \frac{N!}{|\mathrm{Sym}(\overline{\mathcal{H}}, N/2)|}.$$

The main result of this paper is

Theorem 3. *The class* Sw(SQS$(N), r_N$) *coincides with the class of* SQS(N)*s embeddable into the perfect codes of the same rank constructed from an extended Hamming code of length N by the method of $ijkl$-components. The number $R_2(N)$ of these different* SQSs *satisfies*

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

Proof. By Theorem 4 in [7], the number of SQS(N)s built by the method of $ijkl$-components from a fixed SQS($N/4$) and the set $\{i,j,k,l\}$ is equal to

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

Note that SQS(N)s obtained from different SQS($N/4$)s by means of different switchings are distinguished. Indeed, let $S_1(N)$ and $S_2(N)$ be two equal SQS(N)s obtained by method of switchings of $ijkl$-components from different SQSs, say $S_1(N/4)$ and $S_2(N/4)$ of order $N/4$, by means of different switchings. Then there exist some different elements a, b, c, d, and e from the set M such that

$$(a,b,c,d)\in S_1(N/4),\qquad (a,b,c,e)\in S_2(N/4).$$

For the equality of $S_1(N)$ and $S_2(N)$ it is necessary that for the two collections of 64 quadruples corresponding to the matrices T_{abcd} and T_{abce} (see [7]) be obtained one from the other by the switchings

$$d\leftrightarrow e,\qquad i_d\leftrightarrow i_e,\qquad j_d\leftrightarrow j_e,\qquad k_d\leftrightarrow k_e.$$

But the method of $ijkl$-components admits the switchings of elements of the form d, i_d, j_d, k_d which belong to the same column of the initial table and does not admit the switchings between the elements of the form di_d, j_d, k_d and e, i_e, j_e, k_e which belong to different columns of the initial table. Therefore, it is impossible to obtain some equal SQS($N/4$) from different SQS($N/4$)s by means of different switchings.

As we choose an arbitrary quadruple (i,j,k,l) from SQS(N), we have

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

systems of order N. Let us understand which of them can coincide.

Consider an arbitrary SQS($\overline{\mathcal{H}},N$) that corresponds to a fixed table T_M (see [7]) and a SQS($\overline{\mathcal{H}},N/4$). While different partitions of the system SQS($\overline{\mathcal{H}},N$) into the components and further applying switchings of $ijkl$-components to it, the same SQS($\overline{\mathcal{H}},N$) can appear. Let us carefully study these situations.

Fix some quadruple $(i,j,k,l)\in$ SQS($\overline{\mathcal{H}},N$) and an arbitrary element from $\{i,j,k\}$, for example, i. In this case, we have a partition of the initial SQS($\overline{\mathcal{H}},N$) into il-components. It is easy to see that SQS(N) that is obtained from the initial SQS($\overline{\mathcal{H}},N$) by switching $l\leftrightarrow i$ applied to all quadruples containing the elements l or i coincides with SQS($\overline{\mathcal{H}}',N$) that corresponds to the Hamming code $\overline{\mathcal{H}}'=(li)\overline{\mathcal{H}}$ obtained from the code $\overline{\mathcal{H}}$ by applying the permutation (li). The same is true for switchings $j\leftrightarrow k$, $a\leftrightarrow i_a$, and $j_a\leftrightarrow k_a$ for each $a\in M\backslash l$, as well as for the partition of the initial SQS($\overline{\mathcal{H}},N$) into jl- and kl-components; i.e., for the switchings

$$l\leftrightarrow j,\quad i\leftrightarrow k,\quad a\leftrightarrow j_a,\quad i_a\leftrightarrow k_a,\qquad\text{and}\qquad l\leftrightarrow k,\quad i\leftrightarrow j,\quad a\leftrightarrow k_a,\quad i_a\leftrightarrow j_a$$

for each $a\in M\backslash l$. Hence, we have $3\cdot 2\cdot(1+(N/4-1))=3N/2$ repetitions.

We can also partition the initial SQS($\overline{\mathcal{H}},N$) into il-components and first apply the switching $l\leftrightarrow i$ to all $ijkl$-components of this SQS($\overline{\mathcal{H}},N$), containing the elements l and i; after that we can choose the element j or k and apply one of the switchings $l\leftrightarrow j$, $i\leftrightarrow k$, $a\leftrightarrow j_a$, $i_a\leftrightarrow k_a$ for each $a\in M\backslash l$ or $l\leftrightarrow k$, $i\leftrightarrow j$, $a\leftrightarrow k_a$, $i_a\leftrightarrow j_a$ for each $a\in M\backslash l$ to all lj- or lk-components, containing elements from the chosen switching. The so-obtained SQS(N) coincides with the SQS(H',N) corresponding to one of the Hamming codes

$$(lij)\overline{\mathcal{H}},\ (lki)\overline{\mathcal{H}},\ (li)(aj_a)\overline{\mathcal{H}},\ (li)(i_ak_a)\overline{\mathcal{H}}\quad\text{or}\quad(lik)\overline{\mathcal{H}},\ (lji)\overline{\mathcal{H}},\ (li)(ak_a)\overline{\mathcal{H}},\ (li)(i_aj_a)\overline{\mathcal{H}},$$

obtained from $\overline{\mathcal{H}}$ by means of the corresponding permutations. It is easy that these two codes coincide.

The same argumentations are also true if we would choose one of the switchings $j\leftrightarrow k$, $a\leftrightarrow i_a$, and $j_a\leftrightarrow k_a$ as the initial switching and if the initial SQS($\overline{\mathcal{H}},N$) would be partitioned into jl- or kl-components. Thus, we have $3\cdot 4\cdot 2\cdot(1+1+N/4-1+N/4-1)=12N$ repetitions.

Let us note that SQS(N) which is obtained from the initial SQS($\overline{\mathcal{H}},N$) while partitioning it into $ijkl$-components and further applying the switching $a\leftrightarrow i_a$ to all il-components containing a and i_a coincides with SQS$'(N)$ which is obtained from the initial SQS(H,N) while partitioning it into $ii_at_1t_2$-components and further applying the switching $a\leftrightarrow i_a$ to all ii_a-components containing a and i_a. Since there exist exactly $N/2-1$ quadruples of the type $ii_at_1t_2$, we obtain $N/2-1$ repetitions. The same fact is true for the switching $j_a \leftrightarrow k_a$ and also for the switchings $a \leftrightarrow j_a$ and $i_a \leftrightarrow k_a$ applied to the jl-components, as well as for the switchings $a \leftrightarrow k_a$ and $i_a \leftrightarrow j_a$, applied to the kl-components. Hence, we obtain $6(N/2-1)$ repetitions. These argumentations are true for every $a \in M\backslash l$; therefore, we have $(N/4-1)(3N-6) = 3(N-2)(N-4)/4$ repetitions.

Thereby, for the chosen partitioning into $ijkl$-components we obtain

$$3N/2 + 12N + 3(N-2)(N-4)/4 = 3(N^2+12N+8)/4$$

repetitions. Since (i,j,k,l) is an arbitrary quadruple from $\mathrm{SQS}(\overline{\mathcal{H}}, N)$, where

$$|\mathrm{SQS}(\overline{\mathcal{H}}, N)| = N(N-1)(N-2)/24,$$

we have the total of

$$N(N-1)(N-2)(N^2+12N+8)/32$$

repetitions. Taking into account the calculated in (5) number of $\mathrm{SQS}(N)$s which includes the identical ones, we obtain the lower bound of the number of different $\mathrm{SQS}(N)$s built from a fixed table Q and base $\mathrm{SQS}(m)$ by means of the above-mentioned construction:

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

Since there exist $R(\overline{\mathcal{H}}, N/4)$ extended binary Hamming codes, we have at least

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

extended perfect codes of length N that are built from the extended Hamming code of length N by means of the switchings of $ijkl$-components. The switchings of $ijkl$-components can be applied to at most $R(\overline{\mathcal{H}}, N)$ extended Hamming codes of length N; therefore, we have at most

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

extended perfect codes of length N which can be obtained from the extended Hamming code of length N by switchings of $ijkl$-components and to which all different $\mathrm{SQS}(N)$s of rank at most r_N correspond.

By Theorem 2, we obtain that there is no other $\mathrm{SQS}(N)$s of rank at most r_N embeddable into extended perfect binary codes of the same rank. Since, by Theorem 1, there exist exactly

$$2^{|SQS(N/2)|-N/2} \cdot N!/|\mathrm{Sym}(\overline{\mathcal{H}}, N/2)|$$

different $SQS(N)$s of rank at most $r_N - 1$ embedded into extended perfect codes of length N and the same rank, we have the bound given in the statement of the theorem.

The proof of Theorem 3 is complete. □

2. THE STEINER QUADRUPLE SYSTEMS NOT EMBEDDED INTO THE EXTENDED PERFECT CODES OBTAINED BY THE METHOD OF SWITCHING OF $ijkl$-COMPONENTS

Theorem 4. *Let $R'(N)$ be the number of different $\mathrm{SQS}(N)$s of order $N \geq 128$ and rank r_N which are not embeddable into the extended perfect binary codes that are obtained by the method of switching of the ijkl-components from an extended binary Hamming code. Then*

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

Table 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	j_abj_cl	j_aj_bcl	$jabj_c$	jaj_bc	jj_abc	$jj_aj_bj_c$
ai_bi_cl	ak_bk_cl	$j_ai_bk_cl$	$j_ak_bi_cl$	jai_bk_c	jak_bi_c	$jj_ai_bi_c$	$jj_ak_bk_c$
i_abi_cl	$i_aj_bk_cl$	k_abk_cl	$k_aj_bi_cl$	ji_abk_c	$ji_aj_bi_c$	jk_abi_c	$jk_aj_bk_c$
i_ai_bcl	ak_bj_cl	$k_ai_bj_cl$	k_ak_bcl	$ji_ai_bj_c$	ji_ak_bc	jk_ai_bc	$jk_ak_bj_c$
$iabi_c$	iaj_bk_c	ij_abk_c	$ij_aj_bi_c$	$kabk_c$	kaj_bi_c	kj_abi_c	$kj_aj_bk_c$
iai_bc	iak_bj_c	$ij_ai_bj_c$	ij_ak_bc	kai_bj_c	kak_bc	kj_ai_bc	$kj_ak_bj_c$
ii_abc	$ii_aj_bj_c$	ik_abj_c	ik_aj_bc	ki_abj_c	ki_aj_bc	kk_abc	$kk_aj_bj_c$
$ii_ai_bi_c$	$ii_ak_bk_c$	$ik_ai_bj_c$	$ik_ak_bi_c$	$ki_ai_bk_c$	$ki_ak_bi_c$	$kk_ai_bi_c$	$kk_ak_bk_c$

Proof. Consider SQS(H,N) obtained by the method of [7, Theorem 1] and the components R_{ijkl}^{abcl} and R_{il}^1 therein. Recall that R_{il}^1 is the linear span of the vectors with the supports

$$\{ijkl, iai_al, ij_ak_al \mid a \in M\backslash l\}.$$

The component R_{ijkl}^{abcl} and its partitioning into il-components $R_{il}^{1abcl},\dots,R_{il}^{8abcl}$ are represented in Table 1.

Every component $R_{il}^{1abcl},\dots,R_{il}^{8abcl}$ can be partitioned into two subsets of equal total size so that to R_{1il}^{1abcl} and R_{2il}^{1abcl}, ..., R_{1il}^{8abcl} and R_{2il}^{8abcl} there corresponds the same four-element subset $R_{1il},\dots,R_{8il}$ from R_{il}^1 respectively; and moreover, for each of the sets

$$R_{1il}^{1abcl}\cup R_{1il},\quad R_{2il}^{1abcl}\cup R_{1il},\quad \dots,\quad R_{1il}^{8abcl}\cup R_{8il},\quad R_{2il}^{8abcl}\cup R_{8il},$$

the switchings of elements which transform these sets to the equilibrium are allowable.

For example, the component

$$R_{il}^{1abcl}=\{abcl,\ ai_bi_cl,\ i_abi_cl,\ i_ai_bcl,\ iabi_c,\ iai_bc, ii_abc,\ ii_ai_bi_c\}$$

can be represented as

$$R_{il}^{1abcl}=\{abcl,\ ai_bi_cl,\ ii_abc,\ ii_ai_bi_c\}\cup\{i_abi_cl,\ i_ai_bcl,\ iabi_c,\ iai_bc\},$$

i.e.,

$$R_{1il}^{1abcl}=\{abcl,\ ai_bi_cl,\ ii_abc,\ ii_ai_bi_c\},\qquad R_{2il}^{1abcl}=\{i_abi_cl,\ i_ai_bcl,\ iabi_c,\ iai_bc\}.$$

Then the set corresponding to them looks as

$$R_{1il}=\{ibi_bl,\ ici_cl,\ abi_ai_b,\ aci_ai_c\},$$

and each of the sets $R_{1il}^{1abcl}\cup R_{1il}$ and $R_{2il}^{1abcl}\cup R_{1il}$ allows the switchings

$$b\leftrightarrow i_c,\qquad l\leftrightarrow i_a,\qquad a\leftrightarrow i_a,\qquad c\leftrightarrow i_b$$

and

$$b\leftrightarrow c,\qquad i_b\leftrightarrow i_c,\qquad l\leftrightarrow a,\qquad i\leftrightarrow i_a$$

correspondingly. Each of the switchings

$$b\leftrightarrow i_c,\qquad l\leftrightarrow i_a,\qquad a\leftrightarrow i_a,\qquad c\leftrightarrow i_b$$

transforms the initial set $R_{1il}^{1abcl}\cup R_{1il}$ into the same set equilibrium to it. Also, each of the switchings

$$b\leftrightarrow c,\qquad i_b\leftrightarrow i_c,\qquad l\leftrightarrow a,\qquad i\leftrightarrow i_a$$

transforms the initial set $R_{2il}^{1abcl} \cup R_{1il}$ to the same equilibrium set.

There exist at least three such different partitions of each of the components $R_{il}^{1abcl}, \ldots, R_{il}^{8abcl}$.

Let us note that the above-listed cases do not exhaust all possibilities, which allows us to obtain only the lower bound on the number of SQS(N)s of rank r_N such that they are not embeddable into the extended perfect binary codes of length N and the same rank.

In Tables 2–4, all partitions of the components, the sets from R_{il}^1 corresponded to them, and the possible switchings in each of the three cases are specified. Many of the sets R_{ril}^s, $r \in \{1, \ldots, 8\}$ and $s \in \{1, 2, 3\}$, intersect between themselves for fixed s and different r as well as for different s and r. Therefore, it is impossible to apply switchings to all of the sets independently.

From the Tables 2, 3, and 4 we can see that the sets

$$R_{1il}^1,\ R_{2il}^1,\ R_{7il}^1,\ R_{8il}^1 \quad \text{and} \quad R_{3il}^1,\ R_{4il}^1,\ R_{5il}^1,\ R_{6il}^1;$$

$$R_{1il}^2,\ R_{3il}^2,\ R_{6il}^2,\ R_{8il}^2 \quad \text{and} \quad R_{2il}^2,\ R_{4il}^2,\ R_{5il}^2,\ R_{7il}^2;$$

$$R_{1il}^3,\ R_{4il}^3,\ R_{5il}^3,\ R_{8il}^3 \quad \text{and} \quad R_{2il}^3,\ R_{3il}^3,\ R_{6il}^3,\ R_{7il}^3$$

correspondingly do not intersect between themselves. Thereby, we have 6 collections of pairwise disjoint sets.

Since to each of the four sets of the form R_{ril}^s from every collection there correspond two sets of the form $R_{1il}^{rabcl} \cup R_{ril}^s$ and $R_{2il}^{rabcl} \cup R_{ril}^s$, and we can apply (or do not apply) the allowable switching to any of them; therefore, each collection allows $3^4 - 1$ different switchings. Also, the next composite sets compounded from different Tables 2–4 do not intersect each other:

$$R_{1il}^1,\ R_{8il}^1,\ R_{2il}^2,\ R_{7il}^2,\ R_{4il}^3,\ R_{5il}^3; \qquad R_{1il}^1,\ R_{8il}^1,\ R_{3il}^2,\ R_{6il}^2,\ R_{2il}^3,\ R_{7il}^3;$$

$$R_{2il}^1,\ R_{7il}^1,\ R_{1il}^2,\ R_{8il}^2,\ R_{3il}^3,\ R_{6il}^3; \qquad R_{2il}^1,\ R_{7il}^1,\ R_{4il}^2,\ R_{5il}^2,\ R_{1il}^3,\ R_{8il}^3;$$

$$R_{3il}^1,\ R_{6il}^1,\ R_{1il}^2,\ R_{8il}^2,\ R_{4il}^3,\ R_{5il}^3; \qquad R_{3il}^1,\ R_{6il}^1,\ R_{4il}^2,\ R_{5il}^2,\ R_{2il}^3,\ R_{7il}^3;$$

$$R_{4il}^1,\ R_{5il}^1,\ R_{2il}^2,\ R_{7il}^2,\ R_{3il}^3,\ R_{6il}^3; \qquad R_{4il}^1,\ R_{5il}^1,\ R_{3il}^2,\ R_{6il}^2,\ R_{1il}^3,\ R_{8il}^3.$$

Hence we also have eight collections of pairwise disjoint sets. Since two sets of the form $R_{1il}^{rabcl} \cup R_{ril}^s$ and $R_{2il}^{rabcl} \cup R_{ril}^s$ correspond to each of the six sets of the form R_{ril}^s from every collection and we can apply (or do not apply) an allowable switching to each of them; therefore, each collection allows $3^6 - 1$ different switchings.

As far as the above-listed tables contain the partitions of the components and the switchings which transform them to the equilibrium sets, the resulting quadruple systems are SQSs. Hence, for the partition of R_{ijkl}^{abcl} into il-components we obtain at least

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

different switchings. For the partition of R_{ijkl}^{abcl} into jl- and kl-components the situation is similar. Therefore, for each quadruple from SQS($N/4$), we have $3 \cdot 6304 = 18912$ different switchings. In order for switchings could be applied to the components of the form $R_{ijkl}^{\alpha_t}$ for different quadruples $\alpha_t \in \mathrm{SQS}(N/4)$ independently, these quadruples should not have common elements. As for each quadruple α_t from SQS($N/4$) there exist $4(N-4)(N-8)/3 \cdot 2^5$ quadruples which have the only common element with the initial quadruple, and there exist $3N/4 - 18$ quadruples which have two common elements with the initial quadruple, for α_t there are exactly

$$z = (N-4)(N-8)/3 \cdot 2^3 + 3N/4 - 18 = (N^2 + 6N - 376)/24$$

quadruples having common elements with it and

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

Table 2.

R_{1il}^{rabcl}	R_{2il}^{rabcl}	R_{ril}^{1}	switchings $R_{1il}^{rabcl} \cup R_{ril}^{1}$	switchings $R_{2il}^{rabcl} \cup R_{ril}^{1}$
$labc$	li_abi_c	$libi_b$	$b \leftrightarrow i_c$	$b \leftrightarrow c$
lai_bi_c	li_ai_bc	$lici_c$	$l \leftrightarrow i_a$	$i_b \leftrightarrow i_c$
ii_abc	iai_bc	abi_ai_b	$a \leftrightarrow i$	$l \leftrightarrow a$
$ii_ai_bi_c$	$iabi_c$	aci_ai_c	$c \leftrightarrow i_b$	$i \leftrightarrow i_a$
jj_abc	jk_abi_c	$jkbi_b$	$b \leftrightarrow i_c$	$b \leftrightarrow c$
$jj_ai_bi_c$	jk_ai_bc	$jkci_c$	$c \leftrightarrow i_b$	$i_b \leftrightarrow i_c$
kk_abc	kj_abi_c	$j_ak_abi_b$	$j \leftrightarrow k_a$	$j \leftrightarrow j_a$
$kk_ai_bi_c$	kj_ai_bc	$j_ak_aci_c$	$k \leftrightarrow j_a$	$k \leftrightarrow k_a$
jaj_bc	$ji_aj_bi_c$	jkj_bk_b	$j_b \leftrightarrow i_c$	$j_b \leftrightarrow c$
jak_bi_c	ji_ak_bc	$jkci_c$	$k_b \leftrightarrow c$	$k_b \leftrightarrow i_c$
ki_aj_bc	kaj_bi_c	$ai_aj_bk_b$	$j \leftrightarrow i_a$	$j \leftrightarrow a$
$ki_ak_bi_c$	kak_bc	ai_aci_c	$k \leftrightarrow a$	$k \leftrightarrow i_a$
$jabj_c$	ji_abk_c	$jkbi_b$	$b \leftrightarrow k_c$	$b \leftrightarrow j_c$
jai_bk_c	$ji_ai_bj_c$	jkj_ck_c	$i_b \leftrightarrow j_c$	$i_b \leftrightarrow k_c$
ki_abj_c	$kabk_c$	ai_abi_b	$j \leftrightarrow i_a$	$j \leftrightarrow a$
$ki_ai_bk_c$	kai_bj_c	$ai_aj_ck_c$	$k \leftrightarrow a$	$k \leftrightarrow i_a$
lj_aj_bc	$lk_aj_bi_c$	lij_bk_b	$j_b \leftrightarrow i_c$	$j_b \leftrightarrow c$
$lj_ak_bi_c$	lk_ak_bc	$lici_c$	$k_b \leftrightarrow c$	$k_b \leftrightarrow i_c$
ik_aj_bc	$ij_aj_bi_c$	$j_ak_aj_bk_b$	$l \leftrightarrow k_a$	$l \leftrightarrow j_a$
$ik_ak_bi_c$	ij_ak_bc	$j_ak_aci_c$	$i \leftrightarrow j_a$	$i \leftrightarrow k_a$
lj_abj_c	lk_abk_c	$libi_b$	$b \leftrightarrow k_c$	$b \leftrightarrow j_c$
$lj_ai_bk_c$	$lk_ai_bj_c$	lij_ck_c	$i_b \leftrightarrow j_c$	$i_b \leftrightarrow k_c$
ik_abj_c	ij_abk_c	$j_ak_abi_b$	$l \leftrightarrow k_a$	$l \leftrightarrow j_a$
$ik_ai_bk_c$	$ij_ai_bj_c$	$j_ak_aj_ck_c$	$i \leftrightarrow j_a$	$i \leftrightarrow k_a$
laj_bj_c	$li_aj_bk_c$	lij_bk_b	$j_b \leftrightarrow k_c$	$j_b \leftrightarrow j_c$
lak_bk_c	$li_ak_bj_c$	lij_ck_c	$k_b \leftrightarrow j_c$	$k_b \leftrightarrow k_c$
$ii_aj_bj_c$	iaj_bk_c	$ai_aj_bk_b$	$l \leftrightarrow i_a$	$l \leftrightarrow a$
$ii_ak_bk_c$	iak_bj_c	$ai_aj_ck_c$	$i \leftrightarrow a$	$i \leftrightarrow i_a$
$jj_aj_bj_c$	$jk_aj_bk_c$	jkj_bk_b	$j_b \leftrightarrow k_c$	$j_b \leftrightarrow j_c$
$jj_ak_bk_c$	$jk_ak_bj_c$	jkj_ck_c	$k_b \leftrightarrow j_c$	$k_b \leftrightarrow k_c$
$kk_aj_bj_c$	$kj_aj_bk_c$	$j_ak_aj_bk_b$	$j \leftrightarrow k_a$	$j \leftrightarrow j_a$
$kk_ak_bk_c$	$kj_ak_bj_c$	$j_ak_aj_ck_c$	$k \leftrightarrow j_a$	$k \leftrightarrow k_a$

Table 3.

R_{1il}^{rabcl}	R_{2il}^{rabcl}	R_{ril}^{2}	switchings $R_{1il}^{rabcl} \cup R_{ril}^{2}$	switchings $R_{2il}^{rabcl} \cup R_{ril}^{2}$
$labc$	lai_bi_c	$liai_a$	$a \leftrightarrow i_c$	$a \leftrightarrow c$
li_abi_c	li_ai_bc	$lici_c$	$i_a \leftrightarrow c$	$i_a \leftrightarrow i_c$
iai_bc	$iabi_c$	abi_ai_b	$l \leftrightarrow i_b$	$l \leftrightarrow b$
$ii_ai_bi_c$	ii_abc	bci_bi_c	$i \leftrightarrow b$	$i \leftrightarrow i_b$
jj_abc	$jj_ai_bi_c$	jkj_ak_a	$j_a \leftrightarrow i_c$	$j_a \leftrightarrow c$
jk_abi_c	jk_ai_bc	$jkci_c$	$k_a \leftrightarrow c$	$k_a \leftrightarrow i_c$
kj_ai_bc	kj_abi_c	$j_ak_abi_b$	$j \leftrightarrow i_b$	$j \leftrightarrow b$
$kk_ai_bi_c$	kk_abc	bci_bi_c	$k \leftrightarrow b$	$k \leftrightarrow i_b$
jaj_bc	jak_bi_c	$jkai_a$	$a \leftrightarrow i_c$	$a \leftrightarrow c$
$ji_aj_bi_c$	ji_ak_bc	$jkci_c$	$i_a \leftrightarrow c$	$i_a \leftrightarrow i_c$
kak_bc	kaj_bi_c	$j_bk_bai_a$	$j \leftrightarrow k_b$	$j \leftrightarrow j_b$
$ki_ak_bi_c$	ki_aj_bc	$j_bk_bci_c$	$k \leftrightarrow j_b$	$k \leftrightarrow k_b$
$jabj_c$	jai_bk_c	$jkai_a$	$a \leftrightarrow k_c$	$a \leftrightarrow j_c$
ji_abk_c	$ji_ai_bj_c$	jkj_ck_c	$i_a \leftrightarrow j_c$	$i_a \leftrightarrow k_c$
kai_bj_c	$kabk_c$	ai_abi_b	$j \leftrightarrow i_b$	$j \leftrightarrow b$
$ki_ai_bk_c$	ki_abj_c	$bi_bj_ck_c$	$k \leftrightarrow b$	$k \leftrightarrow i_b$
lj_aj_bc	$lj_ak_bi_c$	lij_ak_a	$j_a \leftrightarrow i_c$	$j_a \leftrightarrow c$
$lk_aj_bi_c$	lk_ak_bc	$lici_c$	$k_a \leftrightarrow c$	$k_a \leftrightarrow i_c$
ij_ak_bc	$ij_aj_bi_c$	$j_ak_aj_bk_b$	$l \leftrightarrow k_b$	$l \leftrightarrow j_b$
$ik_ak_bi_c$	ik_aj_bc	$j_bk_bci_c$	$i \leftrightarrow j_b$	$i \leftrightarrow k_b$
lj_abj_c	$lj_ai_bk_c$	lij_ak_a	$j_a \leftrightarrow k_c$	$j_a \leftrightarrow j_c$
lk_abk_c	$lk_ai_bj_c$	lij_ck_c	$k_a \leftrightarrow j_c$	$k_a \leftrightarrow k_c$
$ij_ai_bj_c$	ij_abk_c	$j_ak_abi_b$	$l \leftrightarrow i_b$	$l \leftrightarrow b$
$ik_ai_bk_c$	ik_abj_c	$bi_bj_ck_c$	$i \leftrightarrow b$	$i \leftrightarrow i_b$
laj_bj_c	lak_bk_c	$liai_a$	$a \leftrightarrow k_c$	$a \leftrightarrow j_c$
$li_aj_bk_c$	$li_ak_bj_c$	lij_ck_c	$i_a \leftrightarrow j_c$	$i_a \leftrightarrow k_c$
iak_bj_c	iaj_bk_c	$ai_aj_bk_b$	$l \leftrightarrow k_b$	$l \leftrightarrow j_b$
$ii_ak_bk_c$	$ii_aj_bj_c$	$j_bk_bj_ck_c$	$i \leftrightarrow j_b$	$i \leftrightarrow k_b$
$jj_aj_bj_c$	$jj_ak_bk_c$	jkj_ak_a	$j_a \leftrightarrow k_c$	$j_a \leftrightarrow j_c$
$jk_aj_bk_c$	$jk_ak_bj_c$	jkj_ck_c	$k_a \leftrightarrow j_c$	$k_a \leftrightarrow k_c$
$kj_ak_bj_c$	$kj_aj_bk_c$	$j_ak_aj_bk_b$	$j \leftrightarrow k_b$	$j \leftrightarrow j_b$
$kk_ak_bk_c$	$kk_aj_bj_c$	$j_bk_bj_ck_c$	$k \leftrightarrow j_b$	$k \leftrightarrow k_b$

Table 4.

R^{rabcl}_{1il}	R^{rabcl}_{2il}	R^3_{ril}	switchings $R^{rabcl}_{1il} \cup R^3_{ril}$	switchings $R^{rabcl}_{2il} \cup R^3_{ril}$
$labc$	lai_bi_c	$liai_a$	$a \leftrightarrow i_b$	$a \leftrightarrow b$
li_ai_bc	li_abi_c	$libi_b$	$i_a \leftrightarrow b$	$i_a \leftrightarrow i_b$
$iabi_c$	iai_bc	aci_ai_c	$l \leftrightarrow i_c$	$l \leftrightarrow c$
$ii_ai_bi_c$	ii_abc	bci_bi_c	$i \leftrightarrow c$	$i \leftrightarrow i_c$
jj_abc	$jj_ai_bi_c$	jkj_ak_a	$j_a \leftrightarrow i_b$	$j_a \leftrightarrow b$
jk_ai_bc	jk_abi_c	$jkbi_b$	$k_a \leftrightarrow b$	$k_a \leftrightarrow i_b$
kj_abi_c	kj_ai_bc	$j_ak_aci_c$	$j \leftrightarrow i_c$	$j \leftrightarrow c$
$kk_ai_bi_c$	kk_abc	bi_bci_c	$k \leftrightarrow c$	$k \leftrightarrow i_c$
jaj_bc	jak_bi_c	$jkai_a$	$a \leftrightarrow k_b$	$a \leftrightarrow j_b$
ji_ak_bc	$ji_aj_bi_c$	jkj_bk_b	$i_a \leftrightarrow j_b$	$i_a \leftrightarrow k_b$
kaj_bi_c	kak_bc	ai_aci_c	$j \leftrightarrow i_c$	$j \leftrightarrow c$
$ki_ak_bi_c$	ki_aj_bc	$j_bk_bci_c$	$k \leftrightarrow c$	$k \leftrightarrow i_c$
$jabj_c$	jai_bk_c	$jkai_a$	$a \leftrightarrow i_b$	$a \leftrightarrow b$
$ji_ai_bj_c$	ji_abk_c	$jkbi_b$	$i_a \leftrightarrow b$	$i_a \leftrightarrow i_b$
$kabk_c$	kai_bj_c	$ai_aj_ck_c$	$j \leftrightarrow k_c$	$j \leftrightarrow j_c$
$ki_ai_bk_c$	ki_abj_c	$bi_bj_ck_c$	$k \leftrightarrow j_c$	$k \leftrightarrow k_c$
lj_aj_bc	$lj_ak_bi_c$	lij_ak_a	$j_a \leftrightarrow k_b$	$j_a \leftrightarrow j_b$
lk_ak_bc	$lk_aj_bi_c$	lij_bk_b	$k_a \leftrightarrow j_b$	$k_a \leftrightarrow k_b$
$ij_aj_bi_c$	ij_ak_bc	$j_ak_aci_c$	$l \leftrightarrow i_c$	$l \leftrightarrow c$
$ik_ak_bi_c$	ik_aj_bc	$j_bk_bci_c$	$i \leftrightarrow c$	$i \leftrightarrow i_c$
lj_abj_c	$lj_ai_bk_c$	lij_ak_a	$j_a \leftrightarrow i_b$	$j_a \leftrightarrow b$
$lk_ai_bj_c$	lk_abk_c	$libi_b$	$k_a \leftrightarrow b$	$k_a \leftrightarrow i_b$
ij_abk_c	$ij_ai_bj_c$	$j_ak_aj_ck_c$	$l \leftrightarrow k_c$	$l \leftrightarrow j_c$
$ik_ai_bk_c$	ik_abj_c	$bi_bj_ck_c$	$i \leftrightarrow j_c$	$i \leftrightarrow k_c$
laj_bj_c	lak_bk_c	$liai_a$	$a \leftrightarrow k_b$	$a \leftrightarrow j_b$
$li_ak_bj_c$	$li_aj_bk_c$	lij_bk_b	$i_a \leftrightarrow j_b$	$i_a \leftrightarrow k_b$
iaj_bk_c	iak_bj_c	$ai_aj_ck_c$	$l \leftrightarrow k_c$	$l \leftrightarrow j_c$
$ii_ak_bk_c$	$ii_aj_bj_c$	$j_bk_bj_ck_c$	$i \leftrightarrow j_c$	$i \leftrightarrow k_c$
$jj_aj_bj_c$	$jj_ak_bk_c$	jkj_ak_a	$j_a \leftrightarrow k_b$	$j_a \leftrightarrow j_b$
$jk_ak_bj_c$	$jk_aj_bk_c$	jkj_bk_b	$k_a \leftrightarrow j_b$	$k_a \leftrightarrow k_b$
$kj_aj_bk_c$	$kj_ak_bj_c$	$j_ak_aj_ck_c$	$j \leftrightarrow k_c$	$j \leftrightarrow j_c$
$kk_ak_bk_c$	$kk_aj_bj_c$	$j_bk_bj_ck_c$	$k \leftrightarrow j_c$	$k \leftrightarrow k_c$

quadruples pairwise disjoint with α_t. Therefore, the first quadruple for a switching inside the component R^{abcl}_{ijkl} can be chosen among all $|\mathrm{SQS}(N/4)|$ quadruples, and the second quadruple, which has no common elements with the first one, can be chosen among $|\mathrm{SQS}(N/4)| - z - 1$ quadruples. The third quadruple, which has no common elements with the first and second quadruples, can be chosen among the rest of $|\mathrm{SQS}(N/4)| - 2(z+1)$ quadruples. Proceeding the process in this way, it is easy to see that we can find at least $N/64$ pairwise disjoint quadruples which do not have common elements. Then, there exist at least

$$|\mathrm{SQS}(N/4)| \cdot \big(|\mathrm{SQS}(N/4)| - (z+1)\big) \cdot \big(|\mathrm{SQS}(N/4)| - 2(z+1)\big) \times \ldots \times \big(|\mathrm{SQS}(N/4)| - (N/64-1)(z+1)\big) > |\mathrm{SQS}(N/4)| \cdot \left(\frac{N^2+16N-512}{32}\right)^{N/64-1}$$

variants of such collections of 64 quadruples. As far as, given an arbitrary quadruple, there exist at least 18912 different switchings and each of them transforms the initial component into an equilibrium set, there exist at least

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

different switchings transforming the initial SQS into different SQS(N)s. The resulting systems are different because the different subsets of the initial set of quadruples are involved in these switchings. As for the initial SQS($N/4$) we can take each of the Hamming quadruple systems of order $N/4$, the bound in the assertion becomes evident. Rank of these SQS(N)s depends on the rank of SQS($N/4$) and can exceed r_N.

In result of these switchings, neither il-, nor jl-, nor kl-component of the initial SQS changes completely. So, after applying the above switchings, the resultant systems do not coincide with the SQSs corresponding to the extended perfect codes obtained from the extended Hamming code by the switchings of $ijkl$-components.

The proof of Theorem 4 is complete. □

Corollary. *The rank* $r(\mathrm{SQS}(N))$ *of the system* SQS(N) *obtained by means of switchings in Theorem* 4 *from some* SQS($N/4$) *of rank* $r(\mathrm{SQS}(N/4))$ *satisfies*

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

The question about embedding of SQSs in Theorem 4 into the extended perfect codes is still open.

ACKNOWLEDGMENTS

The authors are grateful to N. Chumakova for useful remarks improving the paper representation.

The authors were partially supported by the Russian Foundation for Basic Research (project no. 12–01–00631–a) and the Federal Target Program "Research and Pedagogical Personnel for Innovative Russia" for 2009–2012 (Contract no. 8227).

REFERENCES

1. S. V. Avgustinovich and F. I. Solov'eva, "Constructing the Perfect Binary Codes by Sequential Switchings of $\tilde{\alpha}$-Components," Problemy Peredachi Informatsii **33** (3), 15–21 (1997).
2. I. Sh. o. Aliev, "Combinatorial Designs and Algebras," Sibirsk. Mat. Zh. **13** (3), 499–509 (1972) [Siberian Math. J. **13** (3), 341–348 (1972)].
3. Yu. L. Vasil'ev, "On Nongroup Densely Packed Codes," Problemy Kibernetiki No. 8, 337–339 (1962).
4. V. A. Zinov'ev and D. V. Zinov'ev, "About Vasil'ev Codes of Length $n = 2^m$ and Duplication of Steiner Systems $S(n, 4, 3)$ of Given Rank," Problemy Peredachi Informatsii **42** (1), 13–33 (2006).
5. V. A. Zinov'ev and D. V. Zinov'ev, "On Solvability of Steiner Systems $S(v = 2^m, 4, 3)$ of Rank $r \leq v - m + 1$ over $\mathbb{F}^2$," Problemy Peredachi Informatsii **43** (1), 39–55 (2007).

6. V. A. Zinov'ev and D. V. Zinov'ev, “Steiner Systems $S(v, k, k-1)$: Components and Rank,” Problemy Peredachi Informatsii **47** (2), 52–71 (2011).
7. D. I. Kovalevskaya and F. I. Solov'eva, “On the Steiner Quadruple Systems of Small Rank Embedable into Extended Perfect Binary Codes,” Diskretn. Anal. Issled. Oper. **19** (5), 47–62 (2012).
8. D. I. Kovalevskaya, F. I. Solov'eva, and E. S. Filimonova, “On the Steiner Triple Systems of Small Rank Embedded into Perfect Binary Codes,” Diskretn. Anal. Issled. Oper. **20** (3), 3–25 (2013) [J. Appl. Indust. Math. **7** (3), 380–395 (2013)].
9. D. S. Krotov and V. N. Potapov, “About Switching Equivalence of n-Dimensional Quasigroups of Order 4 and Perfect Binary Codes,” Problemy Peredachi Informatsii **46** (3), 22–28 (2010).
10. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1977; Svyaz', Moscow, 1979).
11. A. Ya. Petrenyuk, “Signs of Nonisomorphism of Steiner Triple Systems,” Ukrain. Mat. Zh **24** (6), 772–780 (1972).
12. F. I. Solov'eva and S. T. Topalova, “Perfect Binary Codes and Steiner Triple Systems with Maximal Orders of Automorphism Group,” Diskretn. Anal. Issled. Oper. Ser. 1, **7** (4), 101–110 (2000).
13. J. Doyen, X. Hubaut, and M. Vandensavel, “Ranks of Incidence Matrices of Steiner Triple Systems,” Math. **163**, 251–259 (1978).
14. J. Doyen and M. Vandensavel, “Nonisomorphic Steiner Quadruple Systems,” Bull. Soc. Math. Belg. **23**, 393–410 (1971).
15. H. Hanani, “On Quadruple Systems,” Can. J. Math. **12**, 145–157 (1960).
16. H. Hanani, “The Existence and Construction of Balanced Incomplete Block Designs,” Ann. Math. Stat. **32** (2), 361–386 (1961).
17. H. Lenz, “On the Number of Steiner Quadruple Systems,” Mitt. Math. Seminar Giessen. **169**, 55–71 (1985).
18. C. C. Lindner, “On the Construction of Nonisomorphic Steiner Quadruple Systems,” Colloq. Math. **29**, 303–306 (1974).
19. P. R. Östergård and O. Pottonen, “The Perfect Binary One-Error-Correcting Codes of Length 15. Part 1: Classification,” IEEE Trans. Inform. Theory **55**, 4657–4660 (2009).
20. F. I. Solov'eva, S. V. Avgustinovich, and O. Heden, “The Classification of Some Perfect Codes,” Des. Codes Cryptogr. **31** (3), 313–318 (2004).
21. V. D. Tonchev, “A Formula for the Number of Steiner Quadruple Systems on 2^n Points of 2-Rank $2^n - n$,” J. Comb. Des. **11**, 260–274 (2003).
22. V. A. Zinoviev and D. V. Zinoviev, "Steiner Triple Systems $S(2^m - 1, 3, 2)$ of Rank $2^m - m + 1$ over F_2," Problems Inform. Transmission **48** (2), 102–126 (2012).