ISSN 1990-4789, Journal of Applied and Industrial Mathematics, 2013, Vol. 7, No. 1, pp. 68–77. © Pleiades Publishing, Ltd., 2013.
Original Russian Text © D.I. Kovalevskaya, F.I. Solov'eva, 2012, published in Diskretnyi Analiz i Issledovanie Operatsii, 2012, Vol. 19, No. 5, pp. 47–62.

On the Steiner Quadruple Systems of Small Rank Which Are Embeddable into Extended Perfect Binary Codes

D. I. Kovalevskaya* and **F. I. Solov'eva****

Sobolev Institute of Mathematics, pr. Akad. Koptyuga 4, Novosibirsk, 630090 Russia

Received October 14, 2011; in final form, February 10, 2012

Abstract—The codewords of weight 4 of every extended perfect binary code that contains the all-zero vector are known to form a Steiner quadruple system. We propose a modification of the Lindner construction for the Steiner quadruple system of order $N = 2^r$ which can be described by special switchings from the Hamming Steiner quadruple system. We prove that each of these Steiner quadruple systems is embedded into some extended perfect binary code constructed by the method of switching of $ijkl$-components from the binary extended Hamming code. We give the lower bound for the number of different Steiner quadruple systems of order N with rank at most $N - \log N + 1$ which are embedded into extended perfect codes of length N.

DOI: 10.1134/S1990478913010079

Keywords: *Steiner quadruple system, extended perfect binary code, switching, ijkl-component, il-component*

INTRODUCTION

Let $\mathbb{F}^n$ be the n-dimensional metric space over the Galois field $GF(2)$ with the Hamming metric. A *binary code* of length n is an arbitrary subset of $\mathbb{F}^n$. The *parameters* of an arbitrary binary code C from $\mathbb{F}^n$ are denoted by $(n, |C|, d)$, where n is the length of codewords (the code elements), $|C|$ is the cardinality of the code, and d is the code distance (i.e., the minimal Hamming distance between all codewords). The *support* $\mathrm{supp}(x)$ of a vector x from $\mathbb{F}^n$ is the set of nonzero coordinate positions of x. A binary code C of length n with distance $d = 2d' + 1$ is called *perfect* if, for every $x \in \mathbb{F}^n$, there exists a unique x' from C such that the Hamming distance $d(x, x')$ is equal to $(d-1)/2$. It is known [7] that a nontrivial perfect binary code correcting one error (further referred as *perfect*) exists if and only if $n = 2^r - 1$ for some integer $r \geq 2$.

If V is a set of v elements then a t-(v, k, λ)-*design* is a set of blocks designed from elements of v such that each block contains exactly k different elements and each t-element subset from V appears exactly in λ blocks. A *Steiner triple system of order* v (denote it by $\mathrm{STS}(v)$) and a *Steiner quadruple system of order* v (denote it by $\mathrm{SQS}(v)$) are 2-$(v, 3, 1)$- and 3-$(v, 4, 1)$-designs correspondingly. Two Steiner quadruple systems are *isomorphic* if there is a bijection of the sets of v elements which maps all blocks of one system into the blocks of the other. It is known [10] that a Steiner quadruple system $\mathrm{SQS}(v)$ exists if and only if $v \equiv 2, 4 \pmod 6$; and the best lower [14] and upper [12] bounds for the number $N(v)$ of all nonisomorphic Steiner quadruple systems of order v has the form

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

Let $\overline{C}$ be an *extended perfect code*, obtained from the perfect code C of length $2^r - 1$, $r \geq 2$, by adding the total even parity (i.e., by adding a coordinate equal to the sum of other coordinates modulo 2). Further we consider only perfect (and hence, extended perfect as well) codes that contain the zero vector. It is known [7] that supports of all codewords of weight 3 in a code C form the Steiner triple system

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

$\mathrm{STS}(2^r-1)$, and supports of the codewords of weight 4 in the code $\overline{C}$ form the Steiner quadruple system $\mathrm{SQS}(2^r)$.

It is said [1] that the code $C' = (C\backslash M) \cup M'$ is obtained by *switching* of M to M' in a binary code C if C' has the same parameters as C. Such M is called a *component* of C. If $M' = M \oplus e_i$ for some $i \in \{1, 2, \dots, n\}$, where e_i is a vector of weight 1 with 1 in the ith coordinate position, then M is called the i-*component of* C of length n. Let $\alpha \subseteq \{1, \dots, n\}$. A set is called an α-*component* of a code C if it is the i-component for each $i \in \alpha$ [1].

Similarly we define the notion of switching for t-$(v, k, 1)$-design. Two sets R and R' that consist of k-element subsets of a set V are called *balanced to each other* if every unordered subset with t elements that can be found in the k-element subsets of one set appears also in the k-element subsets of the other one. It is said that the t-$(v, k, 1)$-design $A' = (A\backslash R) \cup R'$ is obtained by *switching* of the set of blocks R to the set of blocks R' in t-$(v, k, 1)$-design A if R and R' are the balanced sets [2, 6, 8] (see the definition of balanced sets in [8]). In [6], such set R (as well as a set R') is called a *component*.

There are many open questions concerning Steiner triple and quadruple systems including the problem of classification of these systems and the problem of an embeddability of a Steiner triple (quadruple) system into a perfect (extended perfect) code.

A question of a correspondence between different constructions for a Steiner triple (quadruple) systems and constructions for the perfect (extended perfect) binary codes is also of interest; e.g., connection between the switching and concatenation constructions for these objects.

In [16] it is proved that only 33 of 80 nonisomorphic Steiner triple systems of order 15 are embedded into perfect codes and only 15590 of 1054163 Steiner quadruple systems of order 16 are embedded into extended perfect codes.

The *rank* of a code C is the dimension of the linear subspace of $\mathbb{F}^n$, spanned by the vectors from C. It is known that the rank of a Steiner triple system $\mathrm{STS}(2^r-1)$ (a Steiner quadruple system $\mathrm{SQS}(2^r)$) is varied from $2^r - r - 1$, the rank of the Hamming code (the linear perfect code) of length $2^r - 1$ [11, 17], up to the full rank $2^r - 1$.

In [19], the number is found of different Steiner triple systems of order $2^r - 1$ with rank $2^r - r$ that exceeds the minimal possible rank by 1; and, in [18], a similar formula is obtained for the number of different Steiner quadruple systems of order 2^r with rank $2^r - r$.

Recall that a *parallel class* in 3-$(v, 4, 1)$-design, $v \equiv 0 \pmod 4$, is defined as a set of $v/4$ blocks that are pairwise disjoint (in other words, a parallel class is a trivial 1-$(v, 4, 1)$-design). The Steiner quadruple system in which the set of blocks can be divided into the $r = (v-1)(v-2)/6$ disjoint parallel classes is called *resolvable*. In [5], the constructions are given that provide all different Steiner quadruple systems of order $N = 2^r$ with rank at most $2^r - r + 1$. It is proved there that all these systems are resolvable, and the number is found of different resolvable Steiner quadruple systems that have one fixed parallel class:

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

Thereafter, taking it into account that there exist $N!/24^{N/4}$ such different parallel classes, we can easily find the number of all different Steiner quadruple systems provided by these constructions from the Steiner quadruple systems of order $N/4$ with rank at most $2^r - r + 1$:

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

In [4], it is shown that the class of Steiner triple systems of order $2^r - 1$, obtained by special switchings from the Hamming Steiner triple system, is embedded into the class of perfect codes constructed by the ijk-components method, and the lower bound is given for the number of the Steiner triple systems of order $2^r - 1$ with rank at most $2^r - r + 1$.

Our work addresses the following question: Which Steiner quadruple systems are embedded into the extended perfect binary codes constructed by the known $ijkl$-components method from the Hamming code? For this purpose we introduce a switching construction of the Steiner quadruple system $\mathrm{SQS}(N)$, constructed from an arbitrary Steiner quadruple system $\mathrm{SQS}(m)$, $N = 4m$, and based on the Lindner construction. It is shown that the partition $\mathrm{SQS}(N)$ for $N = 2^r$ into the subsets-components of a certain form corresponds to some partition of the extended perfect code into the $ijkl$-components and, moreover, such Steiner quadruple system is embedded into the extended perfect code constructed by the $ijkl$-components method. We obtain the lower bound on the number of different Steiner quadruple systems $\mathrm{SQS}(N)$ with rank at most $N - \log N + 1$ which are embedded into an extended perfect code.

1. STEINER QUADRUPLE SYSTEMS SQS(4m) EMBEDDABLE INTO AN EXTENDED PERFECT CODE

Consider a construction of a Steiner quadruple system $\mathrm{SQS}(N)$ of order $N = 4m$ which is built from the Steiner quadruple system $\mathrm{SQS}(m)$ of order m and is a switching construction based on the Lindner construction [15] which, in turn, is a generalization of the known Hanani construction [13]. By construction, some of these $\mathrm{SQS}(4m)$ are embedded into extended perfect codes.

For completeness we consider the Lindner construction [15].

Let $M = \{1, 2, 3, \dots, m\}$ be a set on which an arbitrary Steiner quadruple system $\mathrm{SQS}(m)$ is defined, where $m \equiv 2, 4 \pmod 6$. On the set of elements

$$M \cup \{i_1, \dots, i_m, j_1, \dots, j_m, k_1, \dots, k_m\}$$

we construct some quadruple system of order $4m$, which is further referred as Q_N, $N = 4m$, and we show that it is a Steiner quadruple system. For this purpose we consider the table

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

First, for clarity, we describe the construction of $\mathrm{SQS}(4m)$ in the particular case when $m = 4$. Let, for example, $\mathrm{SQS}(4) = \{(a, b, c, d)\}$. In this case, the Steiner quadruple system $\mathrm{SQS}(4m)$ has the order 16, and T_M takes the form

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

Denote this table by T_{abcd}. Constructing $\mathrm{SQS}(16)$, we do the following: Include into the set of quadruples being under construction all rows and columns from T_{abcd} as well as the quadruples obtained from each pair of rows and columns that can be schematically represented as follows:

(3)

For example, for the first pair of rows we get quadruples

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

We also include all minors of the second order, i.e., the quadruples

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

Also we add to this set all possible combinations of elements that are located in different rows and columns of T_{abcd} (all transversals of T_{abcd}), i.e., the set of quadruples of the form

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

Given the fact that the construction includes 4 rows, 4 columns, 6 quadruples of the form (3), applied to each of C_4^2 rows and C_4^2 columns of the table, $6 \cdot C_4^2$ minors, and 24 quadruples (transversals of the table T_{abcd}), the total number of obtained quadruples equals

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

i.e., coincides with the number of blocks in SQS(16). By the construction of quadruples, each unordered triple of elements is contained in a unique block. Thus, given SQS(4), we construct the system SQS(16).

Let m be an arbitrary number such that there exists SQS(m). Then we include into the constructed set of quadruples Q_N, where $N = 4m$, all columns and also, for each pair of columns, all minors of the form (4) and quadruples of the form (3). Thus, we obtain

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

quadruples. Then, given a quadruple (a, b, c, d) from SQS(m), consider a submatrix T_{abcd}. For this matrix, into the set Q_N we include (a, b, c, d), remaining rows, the quadruples of the form (3) applied to each pair of rows of T_{abcd}, and the quadruples of the form (5).

It is easy that $1 + 3 + 6 \cdot C_4^2 + 4 \cdot 6 = 64$ quadruples correspond to each matrix of the form T_{abcd} in Q_N. The number of the tables is equal to the number of the quadruples in SQS(m), i.e., $m(m-1)(m-2)/24$. Hence, the total number of quadruples in the construction equals

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

By construction of the set of quadruples, each unordered triple of elements appears exactly in one quadruple. Thus, the Steiner quadruple system Q_N of order $N = 4m$ is constructed from the Steiner quadruple system SQS(m) of order m and the following holds:

Theorem 1 [15]. *Given an arbitrary Steiner quadruple system of order m, it is possible to construct a Steiner quadruple system of order $4m$.*

Recall that, in the original Hanani construction [13], the system SQS$(2n)$ of order $2n$ is constructed from the system SQS(n) for every admissible n, and, in Lindner construction [15], system SQS$(n \cdot t)$ of order $n \cdot t$ is constructed from the two systems SQS(n) and SQS(t) for every admissible n and t. The Steiner quadruple system of order N that corresponds to the binary extended Hamming code $\mathcal{H}^N$ is called the *Hamming Steiner quadruple system* SQS$(\mathcal{H}^N)$. It is easy to show the following

Corollary 1. *If SQS(m) is a Hamming Steiner quadruple system then the quadruple system Q_N with $N = 4m$ is a Hamming Steiner quadruple system of order N.*

We introduce a special type of components for extended perfect codes and a quadruple system of the extended Hamming code. Let K be an i-component of the Hamming code of length $N-1$ with $N = 2^r$ and $r \geq 3$ [1]. A set $\overline{K}$ is called an *il-component of the extended Hamming code* of length N obtained from the Hamming code by adding parity checking to the lth coordinate position, $l \in \{1, \ldots, N\} \backslash i$. Similarly we can define jl-, kl-, and ij-, ik-, jk-components of the extended Hamming code. Let x denote an arbitrary codeword of the extended Hamming code such that $\mathrm{supp}(x) = \{i, j, k, l\}$. A set $\overline{M}$ is called *$ijkl$-component of the extended Hamming code* if $\overline{M}$ is $s_1 s_2$-component of the extended Hamming code for any different s_1 and s_2 from $\{i, j, k, l\}$. Note that il- and jk-, jl- and ik-, kl- and ij-component of the extended Hamming code are pairwise equal.

A set Q is called an *il-component of the Hamming Steiner quadruple system* $\mathrm{SQS}(\mathcal{H}^N)$ if Q is a subset of vectors of weight 4 from the il-component of the extended Hamming code $\mathcal{H}^N$ of length N. If an il-component of the Steiner quadruple system Q is also a jl-component and kl-component then Q is called the *$ijkl$-component of* $\mathrm{SQS}(\mathcal{H}^N)$.

Note that the definition of component in [6] is more general. The minimal components of order 8 and cardinality 8 studied there are equal to the s_1s_2-components of the Hamming Steiner quadruple system defined above, whereas the $ijkl$-components are not considered in [6].

Theorem 2 [1]. *Let $\{i,j,k,l\}$ denote the support of an arbitrary vector of weight 4 of any extended binary Hamming code $\mathcal{H}^N$ of length N. Then $\mathcal{H}^N$ can be represented as the union of the disjoint $ijkl$-components R^t_{ijkl}; and, moreover, each of them can be represented as the union of the disjoint il-components R^{pt}_{il}:*

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

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

These partitions allow us to perform switchings of the extended Hamming code and obtain a wide class of extended perfect codes as a result.

Further we consider the components of the Steiner quadruple system that correspond to the subsets of components R^0_{ijkl}, R^{p0}_{il}, $R^{\alpha_t}_{ijkl}$, and $R^{p\alpha_t}_{il}$ of the extended perfect code containing this quadruple system. We denote them by R_{ijkl}, R^p_{il}, $R^{\alpha_t}_{ijkl}$, and $R^{p\alpha_t}_{il}$ correspondingly.

Lemma 1. *Let $\{i,j,k,l\}$ be the support of any weight 4 vector of an extended Hamming binary code of length N. Then the Hamming Steiner quadruple system $SQS(\mathcal{H}^N)$ can be represented as the union of $1 + N(N-4)(N-8)/(3\cdot 2^9)$ disjoint $ijkl$-components; and, in turn, each of them is the union of either $N/4 + (N-4)(N-8)/2^5$ or 8 disjoint il-component.*

Proof. Without loss of generality, let some column of T_M corresponds to the quadruple (i,j,k,l) from $\mathrm{SQS}(\mathcal{H}^m)$.

By Theorem 2,

$$R_{ijkl} = \bigcup_{p=1}^{N_1} R^p_{il},$$

where R^1_{il} is the linear span of vectors with support $\{(i,a,i_a,l),(i,j,k,l),(i,j_a,k_a,l) \mid a \in M' = M\backslash l\}$. Further, $R_{il} = R^1_{il}$. We represent the remaining R^p_{il} with $p > 1$ as all possible cosets of R_{il}. Note that $(j,a,j_a,l) \in R_{ijkl}$ and $(j,a,j_a,l) \notin R_{il}$ for each $a \in M'$, while, for different elements a and b from M', $(j,a,j_a,l) \notin R_{il} + (j,b,j_b,l)$. Therefore, there exist $N/4-1$ cosets of R_{il} of the form $R_{il} + (j,a,j_a,l)$, where $a \in M'$. Further, it is easy that $(j,a,j_a,l)+(j,b,j_b,l) \in R_{ijkl}$ and $(j,a,j_a,l)+(j,b,j_b,l) \notin R_{il}$ for every different a and b from M', $(j,a,j_a,l)+(j,b,j_b,l) \notin R_{il} + (j,c,j_c,l)$ for every pairwise different a, b, and c from M', and $(j,a,j_a,l)+(j,b,j_b,l) \notin R_{il} + (j,c,j_c,l) + (j,d,j_d,l)$ for every pairwise different a, b, c, and d from M'. Therefore, there exist

$$C^2_{N/4-1} = (N/4-1)(N/4-2)/2 = (N-4)(N-8)/2^5$$

cosets of R_{il} of the form $R_{il} + (j,a,j_a,l) + (j,b,j_b,l)$, where a and b are different elements from M'.

By similar reasoning for the cosets of R_{il} of the form

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

taking into account that

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

we obtain

$R_{il}^p = R_{il} + (j, a, j_a, l)$ for all $a \in M'$ and $2 \le p \le N/4$;

$R_{il}^p = R_{il} + (j, a, j_a, l) + (j, b, j_b, l)$ for different elements a and b from M', where $1 + N/4 \le p \le N/4 + (N-4)(N-8)/2^5$;

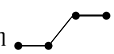
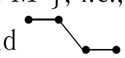
$R_{il}^p = R_{il} + (j, a, j_a, l) + (j, b, j_b, l) + (j, c, j_c, l)$ for different elements a, b, and c from M' for $1 + N/4 + (N-4)(N-8)/2^5 \le p \le N/4 + (N-4)(N-8)/2^5 + (N-4)(N-8)(N-12)/(3 \cdot 2^7)$;

$$R_{il}^{N_1} = R_{il} + (j, a, j_a, l) + (j, b, j_b, l) + \cdots + (j, m', j_{m'}, l), \qquad M' = \{a, b, \ldots, m'\}.$$

Therefore, for the Steiner quadruple system $\mathrm{SQS}(\mathcal{H}^N)$, the following holds: The component R_{ijkl} for $\mathrm{SQS}(\mathcal{H}^N)$ contains all columns of T_M as well as the minors (4) and the blocks of the form (3) for each pair of columns of the table.

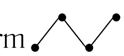
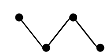
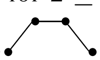
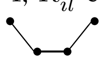
More specifically,

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

where $R_{il} = \{(i, j, k, l),\ (i, a, i_a, l),\ (i, j_a, k_a, l),\ (a, i_a, j_a, k_a),\ (a, i_a, j, k),\ (j, k, j_a, k_a)$ for all $a \in M'$; $(a, i_a, j_b, k_b),\ (a, b, i_a, i_b),\ (j_a, k_a, j_b, k_b)$ for every different a and b from $M'\}$; i.e., R_{il} contains all columns of the table, some minors and quadruples of the form  and  for each pair of columns of the table.

For all components of the form $R_{il}^p \subset R_{il} + (j, a, j_a, l)$ with $2 \le p \le N/4$ and all $a \in M'$, we have

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

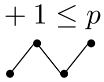
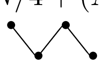
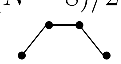
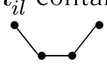
i.e., for $2 \le p \le 4$, R_{il}^p contains some minors and quadruples from (3) of the form   and   for the pair of columns (i, j, k, l) and $(a, i_a, j_a, k_a)^T$ and all $a \in M'$.

Since

$$R_{il}^p \subset R_{il} + (j, a, j_a, l) + (j, b, j_b, l), \qquad N/4 + 1 \le p \le N/4 + (N-4) \cdot (N-8)/2^5,$$

for every different $a, b \in M'$; therefore,

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

i.e., for $N/4 + 1 \le p \le N/4 + (N-4)(N-8)/2^5$, R_{il}^p contains some minors and quadruples from (3) of the form   and   for the pair of columns (a, i_a, j_a, k_a) and $(b, i_b, j_b, k_b)^T$ and every different a and b from M'.

Further, $R_{ijkl}^{\alpha_t} = R_{ijkl} + \alpha_t$, where $\alpha_t \in \mathrm{SQS}(m)$; therefore

$$R_{ijkl}^{\alpha_t} = \bigcup_{p=1}^{8} R_{il}^{p\alpha_t}.$$

Let us give an example of the partition for the component $R_{ijkl}^{\alpha_1} = R_{ijkl}^{abcl} = R_{ijkl} + (a, b, c, l)$ partition. The structures of the other components $R_{ijkl}^{\alpha_t}$ with $2 \le t \le m(m-1)/6$, where $\alpha_t \in \mathrm{SQS}(m)$, look similarly.

Consider the table

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

The first il-component consists of the first two rows (a, b, c, l) and (i, i_a, i_b, i_c) of this table, and also of the quadruples of form (3) built on these rows:

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

Remaining il-components are as follows:

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

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

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

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

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

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

The component $R_{il}^{8\alpha_1}$ consists of the two last rows (j, j_a, j_b, j_c) and (k, k_a, k_b, k_c) of T_{abcl}, and also of quadruples of the form (3) built on these rows:

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

For $R_{ijkl}^{\alpha_t}$ were $2 \le t \le N(N-4)(N-8)/(3 \cdot 2^9)$, we have

$$R_{ijkl}^{\alpha_t} = \bigcup_{p=1}^{8} R_{il}^{p\alpha_t};$$

at that, $R_{il}^{p\alpha_t}$ are constructed similarly to the previous case but each time for their own table T_{α_t}.

This completes the proof of Lemma 1. □

Theorem 3. *The Steiner quadruple system obtained from the system $SQS(\mathcal{H}^N)$ by the switching method of the $ijkl$-components is embedded into the extended perfect code obtained from the extended Hamming code $\mathcal{H}^N$ by the switching method of the $ijkl$-components.*

Proof. The proof of Lemma 1 implies immediately that the switchings of the components of the Steiner quadruple system $\mathrm{SQS}(\mathcal{H}^N)$ are completely defined by the switchings of the corresponding components of the extended Hamming code $\mathcal{H}^N$. Since il-, jl-, kl-, and $ijkl$-components of $\mathrm{SQS}(\mathcal{H}^N)$ are the subsets of the corresponding il-, jl-, kl-, and $ijkl$-components of $\mathcal{H}^N$; therefore, the Steiner quadruple system obtained by the switching method from the system $\mathrm{SQS}(\mathcal{H}^N)$ is embedded into the perfect code obtained by the switching method from $\mathcal{H}^N$.

The proof of Theorem 3 is complete. □

It should be noted that, according to [1], the rank of the extended perfect code of length N obtained from the extended binary Hamming code of length N by the switchings $ijkl$-components (and so the rank of the Steiner quadruple system of order N obtained by the switching method of $ijkl$-components from the Hamming Steiner quadruple system of order N) is at most $N - \log N + 1$.

Let us give the lower bound on the number of different Steiner quadruple systems of order N with rank at most $N - \log N + 1$ that are embedded into the extended perfect code of length N which is constructed by the switching method $ijkl$-components:

Theorem 4. *The number $R(N)$ of different Steiner quadruple systems $SQS(N)$ of order$N$ with rank at most $N - \log N + 1$ embedded into extended perfect codes is at least*

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

where $R^*(N/4) = (N/4)!/((N/4-1)(N/4-2)(N/4-2^2)\cdots(N/4)/2)$ is the number of different Hamming Steiner quadruple systems of order $N/4$.

Proof. Consider the Hamming Steiner quadruple system $\mathrm{SQS}(\mathcal{H}^N)$ constructed by the above approach (see Theorem 1), its component R^{abcl}_{ijkl} from Lemma 1, and the following table for this component:

$abcl$	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	$kk_aj_bj_c$
$ii_ai_bi_c$	$ii_ak_bk_c$	$ik_ai_bj_c$	$ik_ak_bi_c$	$ki_ai_bk_c$	$ki_ak_bi_c$	$kk_ai_bi_c$	$kk_ak_bk_c$

The rows correspond to the jl-components and the columns correspond to the il-components. Further we need the following diagonals of this table that correspond to the kl-components R^{abcl}_{ijkl}:

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

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

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

$$D_4 = \{(j_a, j_b, c, l),\ (j_a, i_b, k_c, l),\ (i_a, j_b, k_c, l),\ (i_a, i_b, c, l),\\ (k, j_a, j_b, k_c),\ (k, j_a, i_b, c),\ (k, i_a, j_b, c),\ (k, i_a, i_b, k_c)\},$$
$$D_5 = \{(i, a, b, i_c),\ (i, a, k_b, j_c),\ (i, k_a, b, j_c),\ (i, k_a, k_b, i_c),\\ (j, a, b, j_c),\ (j, a, k_b, i_c),\ (j, k_a, b, i_c),\ (j, k_a, k_b, j_c)\},$$
$$D_6 = \{(i, a, j_b, k_c),\ (i, a, i_b, c),\ (i, k_a, j_b, c),\ (i, k_a, i_b, k_c),\\ (j, a, j_b, c),\ (j, a, i_b, k_c),\ (j, k_a, j_b, k_c),\ (j, k_a, i_b, c)\},$$
$$D_7 = \{(i, i_a, b, c),\ (i, i_a, k_b, k_c),\ (i, j_a, b, k_c),\ (i, j_a, k_b, c),\\ (j, i_a, b, k_c),\ (j, i_a, k_b, c),\ (j, j_a, b, c),\ (j, j_a, k_b, k_c)\},$$
$$D_8 = \{(i, i_a, i_b, i_c),\ (i, i_a, j_b, j_c),\ (i, j_a, i_b, j_c),\ (i, j_a, j_b, i_c),\\ (j, i_a, i_b, j_c),\ (j, i_a, j_b, i_c),\ (j, j_a, i_b, i_c),\ (j, j_a, j_b, j_c)\}.$$

At that, for each of 1–4 and 5–8 rows, the switchings $l \leftrightarrow j$ and $i \leftrightarrow k$ are possible correspondingly. Note that the il-components are completely changed here.

If we first apply the corresponding given switchings to all rows of the table (i.e., for the $ijkl$-component R^{abcl}_{ijkl} of cardinality 64) then, for each of the resultant 1–4 and 5–8 columns or 1–4 and 5–8 diagonals, the additional switchings $j \leftrightarrow k$ and $l \leftrightarrow i$ or $i \leftrightarrow j$ and $l \leftrightarrow k$ are also feasible correspondingly.

Similarly, for each of the 1–4 and 5–8 columns (the 1–4 and 5–8 diagonals) of the table, the switchings $l \leftrightarrow i$ and $j \leftrightarrow k$ ($l \leftrightarrow k$ and $i \leftrightarrow j$) are possible correspondingly. In this case, the jl-components (the kl-components) are completely changed. If we apply the corresponding given switchings first to all columns (diagonals) of the table and then to each of the obtained 1–4 and 5–8 rows or 1–4 and 5–8 diagonals (1–4 and 5–8 rows or 1–4 and 5–8 columns), the additional switchings $i \leftrightarrow k$, $l \leftrightarrow j$ or $i \leftrightarrow j$, $l \leftrightarrow k$ ($i \leftrightarrow k$, $l \leftrightarrow j$ or $j \leftrightarrow k$, $l \leftrightarrow i$) are feasible correspondingly.

Thus, in each of 9 given cases of transformations of either only rows, columns, and diagonals (transformations of the s_1s_2-components) or their pairwise combinations (transformations of the $ijkl$- and corresponding s_1s_2-components), there can be 2^8 variants of switchings. Taking into account the arising duplications (e.g., the result of switching of all rows and then all columns of the table coincide with the result of switchings of all columns and then all rows of the table), we can conclude that there exist at least $9 \cdot 2^8 - 8$ variants of changing the component R^{abcl}_{ijkl}.

By similar arguments for every other component of the type $R^{\alpha_t}_{ijkl}$, we can find at least $9 \cdot 2^8 - 8$ variants of changing $R^{\alpha_t}_{ijkl}$. It should be noted that in result of these transformations the quadruples in $\mathrm{SQS}(\mathcal{H}^N)$ are changed, but the obtained system remains a Steiner quadruple system, though not Hamming.

Consider the component R_{ijkl}. For each of its il-, jl-, or kl-subcomponents of the form

$$R_{il} + (j, a, j_a, l),\ \ldots,\ R_{il} + (a, b, j_a, j_b),\ R_{jl} + (k, a, k_a, l),\ \ldots,\ R_{jl} + (a, b, k_a, k_b),$$

and

$$R_{kl} + (i, a, i_a, l),\ \ldots,\ R_{kl} + (a, b, i_a, i_b),$$

where $a, b \in M'$, the switchings $l \leftrightarrow i$, $a \leftrightarrow i_a$, $l \leftrightarrow j$, $a \leftrightarrow j_a$, $l \leftrightarrow k$, and $a \leftrightarrow k_a$ are possible correspondingly. Here the il-, jl-, or kl-components are also completely changed, and at least

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

variants of changing the component R_{ijkl} are possible.

In result, since we can take every quadruple of the system $\mathrm{SQS}(\mathcal{H}^N)$ as (i, j, k, l) and every of the $R^*(N/4)$ available different Hamming Steiner quadruple systems of order $N/4$ as the initial quadruple system $\mathrm{STS}(N/4)$; therefore, we obtain

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

possible switchings.

The proof of Theorem 4 is complete. □

Note that the above-obtained bound is less than (2). The question remains open: Whether all Steiner quadruple system from [5] are embedded into the extended perfect codes?

It should be also noted that the arguments, similar to those given in this work but much more complicated, can be developed for the α-components of the extended perfect codes when $|\alpha| > 4$.

ACKNOWLEDGMENTS

The first author was supported by the Grant of the President of the Russian Federation for Young Russian Scientists (project no. MK–1700.2011.1), and the second author, by the Russian Foundation for Basic Research (projects nos. 10–01–00424–a and 12–01–00631).

REFERENCES

1. S. V. Avgustinovich and F. I. Solov'eva, "Constructing the Perfect Binary Codes by Sequential Switching of $\tilde{\alpha}$-Components," Problemy Peredachi Informatsii **33** (3), 15–21 (1997).
2. I. Sh. Aliev, "Combinatoric Designs and Algebras," Sibirsk. Mat. Zh. **13** (3), 499–509 (1972).
3. Yu. L. Vasil'ev, "On Nongrouped Densely Packed Codes," Problemy Kibernetiki No. 8, 337–339 (1962).
4. E. S. Glukhikh, *Embeddability of the Steiner Triple Systems into Perfect Codes* (Novosib. Gos. Univ., Novosibirsk, 2005).
5. V. A. Zinov'ev and D. V. Zinov'ev, "On Resolvability 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. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (Elsevier/North-Holland, Amsterdam, 1977; Svyaz', Moscow, 1979).
8. A. Ya. Petrenyuk, "Signs of Nonisomorphism of Steiner Triple Systems," Ukrain. Mat. Zh. **24** (6), 772–780 (1972).
9. F. I. Solov'eva, *Introduction to Coding Theory* (Novosib. Gos. Univ., Novosibirsk, 2006) [in Russian].
10. M. Hall, *Combinatorics* (Mir, Moscow, 1970) [in Russian].
11. J. Doyen, X. Hubaut, and M. Vandensavel, "Ranks of Incidence Matrices of Steiner Triple Systems," Math. Z. **163** (3), 251–259 (1978).
12. J. Doyen and M. Vandensavel, "Nonisomorphic Steiner Quadruple Systems," Bull. Soc. Math. Belg. **23**, 393–410 (1971).
13. H. Hanani, "The Existence and Construction of Balanced Incomplete Block Designs," Ann. Math. Stat. **32** (2), 361–386 (1961).
14. H. Lenz, "On the Number of Steiner Quadruple Systems," Mitt. Math. Seminar Giessen. **169**, 55–71 (1985).
15. C. C. Lindner, "On the Construction of Nonisomorphic Steiner Quadruple Systems," Colloq. Math. **29**, 303–306 (1974).
16. 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).
17. Teirlinck L. "On Projective and Affine Hyperplanes," J. Comb. Theory Ser. A. **28** (3), 290–306 (1980).
18. 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** (4), 260–274 (2003).
19. V. D. Tonchev, "A Mass Formula for Steiner Triple Systems STS$(2^n - 1)$ of 2-Rank $2^n - n$," J. Comb. Theory Ser. A. **95** (2), 197–208 (2001).

null