Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 203–208*

Steiner triple (quadruple) systems of small ranks embedded into perfect (extended perfect) binary codes[1]

Darya I. Kovalevskaya daryik@rambler.ru
Sobolev Institute of Mathematics, Russia
Elena S. Filimonova FilimonovaES@yandex.ru
Faina I. Solov'eva sol@math.nsc.ru
Sobolev Institute of Mathematics, Novosibirsk State University, Russia

Abstract. It is shown that a class of Steiner triple systems of order 2^r-1, obtained by some special switchings from the Hamming Steiner triple system, is embedded into some perfect code, constructed by known switchings of ijk-components from the binary Hamming code. The number of Steiner triple systems of order n and rank less or equal $n - log(n+1) + 2$, embedded into perfect binary codes of length n, is given. Similar results are obtained for Steiner quadruple systems.

1 Introduction

There are a lot of open problems concerning Steiner triple (quadruple) systems, including the problem of embedding of any Steiner triple (quadruple) system of order $n = 2^r - 1$ into some perfect (extended perfect) binary code of length n.

Let $\bar{C}$ be any *extended perfect code* of length $N = 2^r$, obtained from a perfect code C of length $n = 2^r - 1$, $r \geq 2$, by parity checking. Further we will only consider perfect and extended perfect binary codes, containing the all-zero vector. It is known that the set of all vectors of weight 3 in the code C defines a Steiner triple system of order $2^r - 1$ (briefly $STS(2^r - 1)$), and the set of all vectors of weight 4 in the code $\bar{C}$ defines a Steiner quadruple system of order 2^r (briefly $SQS(2^r)$). A Steiner triple (quadruple) system of order n (N), corresponding to a binary (extended) Hamming code $\mathcal{H}^n$ ($\mathcal{H}^N$), is called *Hamming Steiner triple system* $STS(\mathcal{H}^n)$ (*Hamming Steiner quadruple system* $SQS(\mathcal{H}^N)$). It is proved in [1] that only 33 among 80 nonisomorphic Steiner triple systems of order 15 are embedded into perfect binary codes, and only 15590 among 1054163 Steiner quadruple systems of order 16 are embedded into extended perfect binary codes.

A code $C' = (C \backslash M) \cup M'$ is obtained by a *switching* of some set M with a set M' in a binary code C, see [2], if the code C' has the same parameters

[1]The work was supported by the Grant of the President of Russian Federation for young Russian Researchers (project no. MK-1700.2011.1) and partially supported by the Grants of RFBR 10-01-00424-a and 12-01-00631-a.

as C. Such set M is called a *component* of C. If $M' = M \oplus e_i$ for some $i \in \{1, 2, \ldots, n\}$, where e_i is the vector of weight 1 with the ones only in the i-th coordinate, then the set M is called an *i-component* of the code C of length n. Let α be a subset of the set $\{1, \ldots, n\}$. The set M is called an *α-component* of the code C, if it is an i-component for every $i \in \alpha$, see [2]. A notion of switching for t-$(v, k, 1)$-design is defined in a similar way. Two sets R and R', composed of k-element subsets of the set V, $|V| = v$, are called *balanced with each other*, if every t-element unordered set from the k-element subsets of the first set can also be found in the k-element subsets of the second set. It is said that a t-$(v, k, 1)$-design $A' = (A \backslash R) \cup R'$ is obtained by a *switching* of a block set R with a block set R' in a t-$(v, k, 1)$-design A, if the sets R and R' are balanced with each other (see, for example, [3]). The set R (and also R') is also called a *component*, see [4].

The *rank* of a code C in the vector space F^n is the dimension of the subspace $< C >$ spanned by the code C. Analogously we define the rank for any $STS(n)$. Tonchev [5] presented the description of all Steiner triple systems of order $n = 2^r - 1,\ r > 3$ and of rank $n - \log(n + 1) + 1$. He gave the number of different $STS(2^r - 1)$ of rank $2^r - r$, which is one more than the (minimum possible) rank of the Hamming code of length 2^r. Similar results for SQS were obtained in [6].

V. Zinoviev and D. Zinoviev [7] gave constructions which define all the different Steiner quadruple systems of order $N = 2^r$ of rank at most $2^r - r + 1$; the number of all such different Steiner quadruple systems, built with the help of these constructions from a Steiner quadruple system of order $N/4$, equals to

$$\frac{2^{N+2} \cdot N! \cdot (N/4)! \cdot 6^{N(N-4)/2^5} \cdot 55296^{N(N-4)(N-8)/(3 \cdot 2^9)}}{24^{N/4} \cdot N(N-4)(N-8)\ldots(N-N/2)}. \tag{1}$$

2 Steiner triple systems embedded into perfect codes

In this section, we develop a switching construction of Steiner triple systems, embedded into perfect binary codes obtained by the switching method of ijk-components. The construction is based on the following iterative method.
Let $M = \{1, 2, 3, \ldots, m\},\ m \equiv 1, 3 (mod\ 6),\ m > 1$. Consider $STS(m)$ of order m with the ground set M. Let $\{i, j, k\}$ be such a set that $M \cap \{i, j, k\} = \emptyset$. Using Table 1 (denoted by T) and its elements we construct a set of triples $S(T, n)$ (see rules **A**, **B** below). Then we prove that $S(T, n)$ is a Steiner triple system of order $n = 4m + 3$.
Rule A. For any element a from the set M we consider the set of all elements from its column $(a\ i_a\ j_a\ k_a)^T$ in T and the set $\{i, j, k\}$. It is easy to see that the set of 6 triples

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

Table 1:

	1	2	...	a	...	m
i	i_1	i_2	...	i_a	...	i_m
j	j_1	j_2	...	j_a	...	j_m
k	k_1	k_2	...	k_a	...	k_m

together with the triple (i, j, k) define a Steiner triple system $STS(7)$ of order 7, also known as the Fano plane. The set (2) contains 3 Pasch configurations $\{(i, j_a, k_a), (i, a, i_a), (j, a, j_a), (j, i_a, k_a)\}$; $\{(i, j_a, k_a), (i, a, i_a), (k, i_a, j_a), (k, a, k_a)\}$;

$$\{(j, a, j_a), (j, i_a, k_a), (k, i_a, j_a), (k, a, k_a)\}. \tag{3}$$

These Pasch configurations allow the known switchings $i \leftrightarrow j$, $i \leftrightarrow k$, $j \leftrightarrow k$ respectively. We include into $S(T, n)$ either the set (2) or the set obtained from (2) by a switching of one of the sets from (3). Since a is any element from the set M and $|M| = m$ we choose $6m$ triples to include them into the set $S(T, n)$.

Rule B. For each triple $(a, b, c) \in STS(m)$ we consider the set of all elements from $(a\ i_a\ j_a\ k_a)^T$, $(b\ i_b\ j_b\ k_b)^T$, $(c\ i_c\ j_c\ k_c)^T$ and construct 16 triples:

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

For each element from the set $\{i, j, k\}$ we associate rows, columns and transversals from (4) by the rule: the element i corresponds to columns, the element j corresponds to rows, the element k corresponds to the next transversals:

$$\begin{gathered}\{(a, b, c), (a, k_b, k_c), (k_a, b, k_c), (k_a, k_b, c)\};\\ \{(a, j_b, j_c), (a, i_b, i_c), (k_a, j_b, i_c), (k_a, i_b, j_c)\};\\ \{(j_a, b, j_c), (j_a, k_b, i_c), (i_a, b, i_c), (i_a, k_b, j_c)\};\\ \{(j_a, j_b, c), (j_a, i_b, k_c), (i_a, j_b, k_c), (i_a, i_b, c)\}.\end{gathered} \tag{5}$$

After that we follow to one of the next two variants:

B1. Choose an element i, j or k and consider the set of triples (4). Every row and every column in (4) is a Pasch configuration and allows switchings. For example, for the rows we can apply the switchings $a \leftrightarrow j_a$, $a \leftrightarrow j_a$, $i_a \leftrightarrow k_a$, $i_a \leftrightarrow k_a$, for the columns we can apply the switchings $a \leftrightarrow i_a$, $a \leftrightarrow i_a$, $j_a \leftrightarrow k_a$, $j_a \leftrightarrow k_a$, respectively. Moreover, 4 special transversals (5) also give Pasch

configurations, which allow the switchings $a \leftrightarrow k_a$, $a \leftrightarrow k_a$, $j_a \leftrightarrow i_a$, $j_a \leftrightarrow i_a$. It is easy to see that all the switchings give different triples. Therefore, we have 16 triples, partitioned into the subsets having 4 triples, in three different ways. Each of that 4 triples define a Pasch configuration allowing a switching.
B2. Take an element i, j or k (for example, j) and apply the acceptable switchings (from **B1**) first to all of the blocks corresponding to this element (to the rows, in our case), after that – to some of the blocks, corresponding to one of the other two elements from the set $\{i, j, k\}$ (to the columns or transversals, in our case). As a result, we get a set which is balanced with the initial set of triples (4). We can similarly operate with the element i (k), i.e. with the columns (transversals) of (4), applying the acceptable switchings first to all of them, after that – to some of the rows or transversals (rows or columns, respectively). As a result we get a balanced set with the initial set of triples (4).

Since $|STS(m)| = m(m-1)/6$, choosing one of these two possible ways of switchings for any triple $(a, b, c) \in STS(m)$ to be included into $S(T, n)$, we get $16 \times m(m-1)/6$ triples. We also include the triple (i, j, k) into $S(T, n)$. From the construction of the set $S(T, n)$ we can see that $|S(T, n)| = n(n-1)/6$ and all the triples in $S(T, n)$ are different, so the next theorem is true.

Theorem 1. *The set $S(T, n)$ is a Steiner triple system of order $n = 4m + 3$.*

Corollary 1. *Let $STS(m)$ be the Hamming Steiner triple system. Then the Steiner triple system $S(T, n)$ of order $n = 4m + 3$, built by the rules* **A** *and* **B** *taking the triples (2) and (4), is the Hamming Steiner triple system.*

In [2], the method of ijk-components, letting us to do switchings of the binary Hamming code, is adduced, and it is true the following

Theorem 2. *(see [2]) Every binary Hamming code of length n can be presented as an union of disjoint ijk-components R^t_{ijk}. Each of them can be represented as an union of disjoint i-components R^{pt}_i:*
$\mathcal{H}^n = \bigcup_{t=1}^{N_2} R^t_{ijk} = \bigcup_{t=1}^{N_2} \bigcup_{p=1}^{N_1} R^{pt}_i$, *where* $N_1 = 2^{(n-3)/4}$, $N_2 = 2^{(n+5)/4 - log(n+1)}$.

On the basis of the above-mentioned construction and Theorem 2, we obtain

Theorem 3. *The class of Steiner triple systems of order $n = 4m + 3$, obtained by the switching construction of Theorem* 1 *using the Hamming Steiner triple system $STS(\mathcal{H}^m)$ of order m, is embedded into the class of perfect binary codes, constructed by the method of ijk-components from the binary Hamming code.*

The rank of a perfect binary code of length n, constructed by switchings of ijk-components from the binary Hamming code, is not more than $n - log(n + 1) + 2$, see [2]. Therefore, the rank of a $STS(n)$, constructed by the switching method of ijk-components from $STS(\mathcal{H}^n)$, is not more than $n - log(n + 1) + 2$.

Theorem 4. *The number $R'(n)$ of different Steiner triple systems of order $n = 4m+3$ of rank not more than $n-log(n+1)+2$, embedded into perfect binary codes, equals to $R'(n) = 4^{(n-3)/4} \cdot 130^{(n-3)(n-7)/3 \cdot 2^5} \cdot n(n-1)/6 \cdot R(\mathcal{H}, (n-3)/4)$, where $R(H, m) = m!/(m(m-1)(m+1-2^2)(m+1-2^3) \cdot \ldots \cdot (m+1)/2)$ is the number of different $STS(\mathcal{H}^m)$ of order m.*

Theorem 5. *Any $STS(n)$ of rank $n-log(n+1)+1$ is embedded in some perfect code of length n with the same rank, the code is given by Vasil'ev construction from the Hamming code of length $(n-1)/2$.*

The number of such different $STS(n)$ is according to [5]: $(2^{|STS(\frac{n-1}{2})|-\frac{n-1}{2}} - \frac{2}{n+1}) \cdot n!/|Sym(\mathcal{H}^{\frac{n-1}{2}})|$, where $|Sym(\mathcal{H}^{\frac{n-1}{2}})| = |GL(log(\frac{n+1}{2}), 2)|$.

There were found additional switchings of the above construction, letting us to obtain Steiner triple systems which are not embedded into perfect codes constructed by the method of ijk-components from the Hamming code.

Theorem 6. *The number $R^*(n)$ of different Steiner triple systems $STS(n)$ of order $n = 4m+3$, which are not embedded into perfect binary codes constructed by the method of ijk-components from the binary Hamming code, is at least $R^*(n) \geq ((3(n-3)/4)! - 6^{(n-3)/4}) \cdot ((n+1) \cdot 4^{(n-7)/4} + n - 3) \cdot 310^{(n-3)(n-7)/3 \cdot 2^5} \cdot \cdot n(n-1)/6 \cdot R((n-3)/4) - R'(n)$, where $R((n-3)/4)$ is the number of different $STS((n-3)/4)$.*

3 Steiner quadruple systems embedded into extended perfect binary codes

The direct extention of the above switching construction of Steiner triple systems to Steiner quadruple systems is possible, but does not let us to enumerate perfectly all the Steiner quadruple systems, corresponding to extended perfect binary codes, constructed by the method of $ijkl$-components from the extended binary Hamming code. To find out properly what kind of Steiner quadruple systems are embedded into extended perfect binary codes, constructed by the method of $ijkl$-components from the extended binary Hamming code, a construction Q_N of $SQS(N)$ of order $N = 4m$ was considered. This construction is built from some $SQS(m)$ and is a switching one, based on the well-known Lindner construction [8]. Let us call this construction as *the switching method of $ijkl$-components* for SQS. It follows from the construction that some of such $SQS(4m)$ are embedded into extended perfect binary codes. Because the principles of building such Steiner triple and quadruple constructions have a lot in common, and for brevity, we announce the obtained results without details.

It follows from [2] that the method of $ijkl$-components, as well as the analogue of Theorem 2, are correct for extended perfect binary codes. On the basis of these results and derived construction, one can get the following

Theorem 7. *The Steiner quadruple system, constructed by the switching method of $ijkl$-components from the Hamming Steiner quadruple system $SQS(\mathcal{H}^N)$, is embedded into some extended perfect binary code, constructed by the method of $ijkl$-components from the extended binary Hamming code.*

Theorem 8. *The number $R(N)$ of different Steiner quadruple systems $SQS(N)$ of order N of rank not more than $N - logN + 1$, embedded into perfect extended binary codes, constructed by the method of $ijkl$-components from the extended binary Hamming code, is at least*

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

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

This bound is less than (1), and the question if all of Steiner quadruple systems from [7] are embedded into extended perfect binary codes, is still open.

References

[1] P. R. Östergård, O. Pottonen, The Perfect Binary One-Error-Correcting Codes of Length 15: Part 1 – Classification, *IEEE Trans. Inform. Theory,* **55**, 4657–4660, 2009.

[2] S. V. Avgustinovich, F. I. Solov'eva, Construction of perfect binary codes by sequential translations of an $\tilde{\alpha}$-components, *Probl. Inform. Transm.,* **33** (3), 15–21, 1997.

[3] A. Ya. Petrenyuk, Nonisomorphy markers of Steiner triple systems, *Ukr. Math. Journ.,* **24** (6), 772–780, 1972.

[4] V. A. Zinoviev, D. V. Zinoviev, Steiner systems $S(v, k, k-1)$: Components and rank, *Probl. Inform. Transm.,* **47** (2), 52–71, 2011.

[5] V. D. Tonchev, A mass formula for Steiner triple systems $STS(2^n - 1)$ of 2-rank $2^n - n$, *Journal of Combin. Theory,* **A** (95), 197–208, 2001.

[6] V. D. Tonchev, A formula for the number of Steiner quadruple systems on 2^n points of 2-rank $2^n - n$, *Journal of Combin. Designs,* **11**, 260–274, 2003.

[7] V. A. Zinoviev, D. V. Zinoviev, On resolvability of Steiner systems $S(v = 2^m, 4, 3)$ of rank $r \leq v - m + 1$ over F^2, *Probl. Inform. Transm.,* **43** (1), 39–55, 2007.

[8] C. C. Lindner, On the construction of nonisomorphic Steiner quadruple systems, *Colloq. Math.,* **29**, 303–306, 1974.