Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 199-204*

Steiner quadruple systems $S(n, 4, 3)$ of a fixed corank[1]

D. V. Zinoviev dzinov@iitp.ru
V. A. Zinoviev zinov@iitp.ru
A.A. Kharkevich Institute for Problems of Information Transmission,
Russian Academy of Sciences, Moscow, RUSSIA

Dedicated to the memory of Professor Stefan Dodunekov

Abstract. Steiner systems $S(2^m, 4, 3)$ of rank $2^m - m - 1 + s$, $s \geq 0$ is fixed, over the field $\mathbb{F}_2$ are considered. We provide the construction of all such different systems and derive the estimate of the number of all such different systems.

1 Introduction

A Steiner System $S(v, k, t)$ is a pair (X, B) where X is a set of v elements and B is a collection of k-subsets (blocks) of X such that every t-subset of X is contained in exactly one block of B. A system $S(v, 4, 3)$ is called a Steiner quadruple system (briefly SQS(v)) (see [1-3] for more information).

Tonchev [5] enumerated all different Steiner quadruple systems SQS(2^m) with 2-rank (i.e. rank over the field $\mathbb{F}_2$), equal to $2^m - m$.

In [6], the authors enumerated all different Steiner quadruple systems SQS(2^m) with 2-rank $r \leq 2^m - m + 1$.

The goal of the present work is to enumerate all different Steiner quadruple systems SQS(2^m) of the 2-rank $2^m - m - 1 + s$, where $s \geq 0$ is fixed. We provide a recursive construction of such systems, which in particular, allows us to construct all different systems of order $v = 2^m$ of 2-rank not greater than $2^m - m - 1 + s$ over $\mathbb{F}_2$. Moreover, we estimate the total number of such different systems.

Let E_q be an alphabet of size q: $E_q = \{0, 1, \ldots, q-1\}$, in particular, $E = \{0, 1\}$. Denote a q-ary code C of length n with the minimum (Hamming) distance d and cardinality N as an $(n, d, N)_q$-code (or an (n, d, N)-code for $q = 2$). Denote by $\mathrm{wt}(\boldsymbol{x})$ the Hamming weight of vector $\boldsymbol{x}$ over E_q, and by $d(\boldsymbol{x}, \boldsymbol{y})$ the Hamming distance between the vectors $\boldsymbol{x}, \boldsymbol{y} \in E_q^n$. For a binary code C denote by $\langle C \rangle$ the linear envelope of words of C over the Galois Field $\mathbb{F}_2$. The dimension of space $\langle C \rangle$ is the *rank* of code C over $\mathbb{F}_2$ denoted by $\mathrm{rk}\,(C)$.

[1]This work has been partially supported by the Russian fund of fundamental researches (under the project No. 12 - 01 - 00905).

Denote by (n, w, d, N) a constant weight (n, d, N)-code, whose codewords have the same fixed weight w.

Let $J = \{1, 2, \dots, n\}$ be the set of coordinate positions E_q^n. Denote by $\mathrm{supp}(\boldsymbol{v}) \subseteq J$ the support of a vector $\boldsymbol{v} = (v_1, \dots, v_n) \in E^n$, $\mathrm{supp}(\boldsymbol{v}) = \{i : v_i \neq 0\}$. For an arbitrary set $X \subseteq E^n$ define

$$\mathrm{supp}(X) = \bigcup_{\boldsymbol{x} \in X} \mathrm{supp}(\boldsymbol{x}).$$

A binary (n, d, N)-code C, which is a linear k-dimensional space over $\mathbb{F}_2$, is denoted as $[n, k, d]$-code. Let $(\boldsymbol{x} \cdot \boldsymbol{y}) = x_1 y_1 + \cdots + x_n y_n$ be the scalar product over $\mathbb{F}_2$ of the binary vectors $\boldsymbol{x} = (x_1, \dots, x_n)$ and $\boldsymbol{y} = (y_1, \dots, y_n)$. For any (linear, non-linear or constant weight) code C of length n let $C^\perp$ be its dual code: $C^\perp = \{\boldsymbol{v} \in \mathbb{F}_2^n : (\boldsymbol{v} \cdot \boldsymbol{c}) = 0, \ \forall \ \boldsymbol{c} \in C\}$. It is clear that $C^\perp$ is a $[n, n-k, d^\perp]$-code with minimum distance $d^\perp$, and where $k = \mathrm{rk}\,(C)$.

Denote by K a q-ary MDS $(4, 2, q^3)_q$-code and by Γ_K denote the number of different such codes K.

Lemma 1. *[4] When $q = 2^s$, we have the following estimates:*

$$\Gamma_K \geq (2)^{(q/2)^3}.$$

Define the mapping φ of E_q^n into E^{qn} setting for $\boldsymbol{c} = (c_1, \dots, c_n)$: $\varphi(\boldsymbol{c}) = (\varphi(c_1), \dots, \varphi(c_n))$, where $\varphi(0) = (1, 0, \dots, 0)$, $\varphi(1) = (0, 1, \dots, 0)$,..., $\varphi(q-1) = (0, 0, \dots, 1)$.

For a given code $(4, 2, q^3)_q$-code K, define the constant weight $(4q, 4, 4, q^3)$-code $C(K)$:

$$C(K) = \{\varphi(\boldsymbol{c}) : \ \boldsymbol{c} \in K\}.$$

Every codeword $\boldsymbol{c}$ of the code $C(K)$, is split into blocks of length q so that $\boldsymbol{c} = (\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3, \boldsymbol{c}_4)$ and $\mathrm{wt}(\boldsymbol{c}_i) = 1$ for $i = 1, 2, 3, 4$. We say that $C(K)$ has *the block structure*. For a code $C(K)$ and a vector $\boldsymbol{x} = (x_1, \dots, x_u)$ of weight 4 with support $\mathrm{supp}(\boldsymbol{x}) = \{i_1, i_2, i_3, i_4\}$ define the following code $C(K; \boldsymbol{x}) = C(K; i_1, i_2, i_3, i_4)$ of length qu with block structure:

$$\{(\boldsymbol{c}_1, \dots, \boldsymbol{c}_u) : \ (\boldsymbol{c}_{i_1}, \boldsymbol{c}_{i_2}, \boldsymbol{c}_{i_3}, \boldsymbol{c}_{i_4}) \in C(K), \text{and } \boldsymbol{c}_j = (0, 0, \cdots, 0), \text{if } j \neq i_1, i_2, i_3, i_4\}.$$

For a given set X of vectors of length u and weight 4, define

$$C(K; X) = \{C(K; \boldsymbol{x}) : \ \boldsymbol{x} \in X\}.$$

Define the mapping $\psi(\cdot)$ from E^u into E^{qu}, so that for every vector $\boldsymbol{x} = (x_1, x_2, \dots, x_u)$ we have:

$$\psi(\boldsymbol{x}) = (x_1, \dots, x_1, x_2, \dots, x_2, \dots, x_u, \dots, x_u).$$

Let V be the set of all words of weight 2 and length $q = 2^s$. Then V can be split into $q-1$ trivial codes V_i, $i = 1, \dots, q-1$ with parameters $(q, 2, 4, q/2)$. Let $\Gamma_V(q)$ be the number of different partitions $V^{(j)} = \{V_1^{(j)}, \dots, V_{q-1}^{(j)}\}$, $j = 1, \dots, \Gamma_V(q)$ of V.

Lemma 2. *[7] The following equality is valid:*

$$\Gamma_V(q) \geq \exp\{\frac{(q-1)^2}{12}(\log(q-1) - 5)\},$$

where $q = 2u$ and $u \equiv 1$ or $2 \pmod 3$.

We finally need constant weight codes W with parameters $(2q, 4, 4, q^2(q-1)/4)$, where the codewords can be split into blocks of length q and each block has weight 0 or 2. The different codes are $W^{(j)}$, $j = 1, \dots, \Gamma_W$, where $\Gamma_W = \Gamma_W(q)$ is the number of such different codes.

Lemma 3. *We have the following equality:*

$$\Gamma_W(q) \; = \; (q-1)! \cdot \Gamma_V^2.$$

2 Main results

Suppose $S_v = S(v, 4, 3)$ is a Steiner quadruple system of order $v = 2^m$ and of 2-rank $r \leq 2^m - m - 1 + s$. That means that the dual code $S_v^\perp$ contains a subcode $[v, m+1-s, v/2]$, denoted by $\mathcal{A}_m$ with minimum distance $d^\perp = v/2 = 2^{m-1}$ [6]. More precisely, $\mathcal{A}_m$ contains one word of weight v and the all other nonzero words have the same weight 2^{m-1}, i.e. the code is a subcode of a well known linear biorthogonal code and can be generated by the following matrix:

$$G(\mathcal{A}_m) \; = \; \left[\begin{array}{ccccccccc} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \dots & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \dots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \dots & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \end{array} \right], \qquad (1)$$

where $\mathbf{1} = (1, \dots, 1)$ and $\mathbf{0} = (0, \dots, 0)$ are binary words of length $q = 2^s$. Every word $\boldsymbol{c} \in S_v$ has the block srtucture: $\boldsymbol{c} = (\boldsymbol{c}_1, \boldsymbol{c}_2, \dots |, \boldsymbol{c}_u)$ with blocks of length q, where $u = v/q = 2^{m-s}$. Define the following subsets J_i of size q of the coordinate set J, which correspond to the blocks of length q:

$$J_i = \{q(i-1)+1, q(i-1)+2, \dots, q\,i\}, \;\; i = 1, 2, \dots u.$$

Define the coordinate set $J(u) = \{1, 2, \dots, u\}$ of block indices. Since the codewords of $\mathcal{A}_m$ are orthogonal to our system S_v, its words can be divided naturally into three subsets $S^{(1,1,1,1)}$, $S^{(2,2)}$ and $S^{(4)}$:

- $S^{(1,1,1,1)} \;=\; \{\boldsymbol{c} \in S:\; |\text{supp}(\boldsymbol{c}) \cap J_i| \in \{0,1\},\, i = 1,\dots,u\}.$
- $S^{(2,2)} \;=\; \{\boldsymbol{c} \in S:\; |\text{supp}(\boldsymbol{c}) \cap J_i| \in \{0,2\},\, i = 1,\dots,u\}.$
- $S^{(4)} \;=\; \{\boldsymbol{c} \in S:\; |\text{supp}(\boldsymbol{c}) \cap J_i| \in \{0,4\},\, i = 1,\dots,u\}..$

For any $\boldsymbol{c} \in S^{(1,1,1,1)}$ with support $\text{supp}(\boldsymbol{c}) = \{i_1, i_2, i_3, i_4\}$ define its block support $\text{supp}_q(\boldsymbol{c})$ as a set of indices of its nonzero blocks (i.e. if $i \in \text{supp}(\boldsymbol{c})$ then $j = \lfloor (i+q-1)/q \rfloor \in \text{supp}_q(\boldsymbol{c})$).

Lemma 4. *Let $S_v = S(v,4,3)$ be a Steiner system of order $v = 2^m$ with 2-rank $r_v \leq v - m - 1 + s$. Let $S_v^{\perp}$ be a dual to S_v code which contains a subcode $\mathcal{A}_m$ with parameters $[v, s, v/2]$. Suppose the system S_v splits into subsets $S^{(1,1,1,1)}$, $S^{(2,2)}$, $S^{(4)}$. Then we have*

- *$S^{(1,1,1,1)}$ is a set of codes $C(K_i, \mathbf{c}^{(i)})$, where the set of indices $j_1, j_2, j_3, j_4 \in J(u) = \{1, 2, \dots, u\}$, $u = 2^{m-s}$, $\{j_1, j_2, j_3, j_4\} = \text{supp}_q(\boldsymbol{c}^{(i)})$, forms a Steiner system $S_u = S(u,4,3)$ on the coordinate set $J(u)$ when $\mathbf{c}^{(i)}$ runs over $S^{(1,1,1,1)}$.*
- *The Steiner quadruple system S_u has the minimal 2-rank: $r_u = u - log(u) - 1$, i.e. it is a Boolean system.*
- *The set $S^{(2,2)}$ is a set of arbitrary codes $W^{(j)}(i_1, i_2)$, where i_1 and i_2 take all different values from $\{1, \dots, u\}$ and j takes values from $\{1, 2, \dots, \Gamma_W\}$.*
- *The set $S^{(4)}$ is a set of arbitrary Steiner systems $S_q(j) = S(q,4,3)$, where $\text{supp}(S_q(j)) = J_j$.*

The structure of the Steiner quadruple systems SQS(v) of order $v = uq$ and 2-rank $v - m - 1 + s$ that we described above, induce the following recursive construction of SQS(v) of order v for a given SQS(u) of an arbitrary order u (i.e. $u \equiv 2$ or $4 \pmod 6$).

Construction $II(s)$**.** Let $q = 2^s$ and $S_u = S(u,4,3)$ be a Steiner system of rank r_u, whose words $\mathbf{c}^{(s)}$ are ordered by a fixed enumeration $s = 1, 2, \dots, h$, where $h = u(u-1)(u-2)/24$. Suppose, we have a family of arbitrary q-ary codes $K_1, K_2, \dots, K_h$ with parameters $(4, 2, q^3)_q$. Suppose we have u arbitrary Steiner systems $S_q(j) = S(q,4,3)$, $j = 1, \dots, u$. Assume that for any pair i_1, i_2, where $i_1 < i_2$, run through all possible values from $\{1, 2, \dots, u\}$, there is an arbitrary $(2q, 4, 4, q^2(q-1)/4)$-code $W(i_1, i_2)$. Let $J(u)$ be the coordinate set of the system S_u. Define the new coordinate set $J(v)$ of size $v = u \cdot q$, obtained from $J(u)$ as follows: every index $j \in J(u)$ is associated with the set J_j, of q elements, namely $J_j = \{q(j-1)+1, \dots, q\,j\}$. Define the coordinate set $J(v)$ as the union:

$$J(v) = J_1 \cup \dots \cup J_u.$$

Every word $\boldsymbol{c}^{(i)}$ of S_u with support $\text{supp}(\boldsymbol{c}^{(i)}) = \{j_1, j_2, j_3, j_4\}$ and a code K_i define the constant weight code $C(K_i; \boldsymbol{c}^{(i)}) = C(K_i; j_1, j_2, j_3, j_4)$. Define the following three sets:

$$S^{(1,1,1,1)} \;=\; \bigcup_{i=1}^{h} C(K_i; j_1, j_2, j_3, j_4), \quad \text{supp}(\boldsymbol{c}^{(i)}) = \{j_1, j_2, j_3, j_4\},$$

i.e. the supports of all words of $C(K_i; j_1, j_2, j_3, j_4)$ belong to the set $J_{j_1} \cup J_{j_2} \cup J_{j_3} \cup J_{j_4}$;

$$S^{(2,2)} = \bigcup_{i_1 \neq i_2 \in \{1,2,\ldots,u\}} W(i_1, i_2);$$

i.e. the supports of all vectors of $W(i_1, i_2)$ is always contained in two blocks with numbers i_1 and i_2;

$$S^{(4)} = \bigcup_{j=1}^{u} \{\boldsymbol{c} \in S_q(j)\}, \;\; \text{supp}(S_q(j)) = J_j.$$

Theorem 1. *Let $S_u = S(u, 4, 3)$ be a Steiner system, let $q = 2^s \geq 4$, and let $\boldsymbol{c}^{(i)}$, $i = 1, 2, \ldots, h$ be the words of this system, where $h = u(u-1)(u-2)/24$. Let $S^{(1,1,1,1)}$, $S^{(2,2)}$ and $S^{(4)}$ be the sets, obtained by construction $II(s)$, based on the families of the $(4, 2, q^3)_q$-codes $K_1, K_2, \ldots, K_h$, the family of $u(u-1)/2$ constant weight $(2q, 4, 4, q^2(q-1)/4)$-codes $W(i_1, i_2)$, where i_1 and i_2, $i_1 \neq i_2$ run through all possible values from $\{1, 2, \ldots, u\}$ and u Steiner systems $S_q(j) = S(q, 4, 3)$. Let*

$$S \;=\; S^{(1,1,1,1)} \cup S^{(2,2)} \cup S^{(4)}. \qquad (2)$$

Then, for any choice of S_u, the codes $K_1, K_2, \ldots, K_h$, codes $W(i_1, i_2)$ and systems $S_q(j)$:

- *The set S is the Steiner system $S_v = S(v, 4, 3)$, $v = u \cdot q$.*
- *The rank of the new system S_v satisfies*

$$u(q-1) + \text{rk}(S_u) - s \;\leq\; \text{rk}(S_v) \;\leq\; u(q-1) + \text{rk}(S_u).$$

From this bound it follows, in particular, that if the original system $S(u, 4, 3)$ has the full rank $r_u = u - 1$, then according to Theorem 1, the resulting system $S(v, 4, 3)$ of order $v = u \cdot 2^s$, in general, can also be of the full rank $r_v = v - 1$.

Theorem 2. *Suppose $S_v = S(v, 4, 3)$ is a Steiner system of order $v = 2^m$. Suppose that its 2-rank satisfies $\text{rk}(S_v) \leq 2^m - m - 1 + s$. Then the system S_v is obtained from the Boolean (i.e. of the minimal rank) Steiner quadruple system $S_u = S(u, 4, 3)$ of order $u = 2^{m-s}$ using construction $II(s)$, described above.*

So, we know the structure of all quadruple Steiner systems $S_v = S(v, 4, 3)$ of order $v = 2^m$ and of 2-rank not greater than $v - 1 - m + s$. Now we can estimate the number of all such different systems, which we denote by $\Gamma_S(v, s)$.

Theorem 3. *The number $\Gamma_S(v, s)$ of different Steiner systems $S_v = S(v, 4, 3)$ of order $v = 2^m$ of rank not greater than $v - 1 - m + s$ satisfies the following equality:*

$$\begin{aligned} \Gamma_S(v, s) &= \Gamma_S(u, 0) \cdot (\Gamma_K)^{u(u-1)(u-2)/24} \cdot (\Gamma_W)^{u(u-1)/2} \cdot (\Gamma_S(q, s))^u \\ &> (2)^{c \cdot \frac{v^3}{24}}, \end{aligned}$$

where $c < 1/8$ and $c \to 1/8$ when q is fixed and $u \to \infty$.

Here $\Gamma_S(u, 0)$ is the number of different Boolean quadruple systems $S_u = S(u, 4, 3)$, and $\Gamma_S(q, s)$ is the number of different quadruple systems of order q, where $q = 2^s$, $u = 2^\ell$, and $\ell = m - s$. Recall that the best lower bound for the number $\Gamma_S(v)$ (i. e. of arbitrary ranks) looks as [8]:

$$\Gamma_S(v) > (2)^{\frac{v^3}{24}}.$$

References

[1] J. Doyen, X. Hubaut, M. Vandensavel, Ranks of incidence matrices of Steiner triple systems, *Mathem. Zeitschr.* 163, 1978, 251-259.

[2] E. F. Assmus, Jr., On 2-ranks of Steiner triple systems, *The Electr. J. Combin.* 1995, V. 2. Paper R9.

[3] A. Hartman, K. T. Phelps, Steiner quadruple systems, In: Contemporary Design Theory: A Collection of Surveys. Dinitz J.H., Stinson D.R., Eds. John Wiley & Sons. 1992. Ch. 6. P. 205-240.

[4] V. N. Potapov, D. S. Krotov, P. V. Sokolova, On reconstructing reducible n-ary quasigroups and switching subquasigroups, *Quasigroups Relat. Syst.* 16, 2008, 55-67.

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

[6] V. A. Zinoviev, D. V. Zinoviev, On resolvability of Steiner systems $S(2^m, 4, 3)$ of rank $r \leq 2^m - m + 1$ over F_2, *Probl. Inform. Transmission* 43, No. 1, 2007, 39-55.

[7] C. C. Lindner, E. Mendelsohn, A. Rosa, On the number of 1-factorizations of the complete graph, *J. Combin. Theory* (B) 20, 1976, 265-282.

[8] J. Doyen, M. Vandensavel, Nonisomorphic Steiner quadruple systems, *Bull. Soc. Math. Belg.* 23, 1971, 393-410.