

Classification of Steiner quadruple systems of order 16 and rank 14. *

V. A. Zinoviev and D. V. Zinoviev
Institute for Problems of Information Transmission
Russian Academy of Sciences
Bol'shoi Karetnyi, 19, GSP-4, Moscow, 101447, Russia

Abstract

A Steiner quadruple system $S(v, 4, 3)$ of order v is a 3-design $T(v, 4, 3, \lambda)$ with $\lambda = 1$. In the previous paper [1] we classified all such Steiner systems $S(16, 4, 3)$ of order 16 with rank 13 or less over \mathbb{F}_2 . In particular, we have proved that there is one $S(16, 4, 3)$ of rank 11 (the points and planes of affine geometry $AG(4, 2)$), fifteen systems $S(16, 4, 3)$ of rank 12 and 4131 systems of rank 13. In this paper we describe all non-isomorphic $S(16, 4, 3)$ of rank 14 over \mathbb{F}_2 . All these Steiner systems $S(16, 4, 3)$ can be obtained by the generalized doubling construction, which we give here. Our main result is that there are exactly 684764 non-isomorphic Steiner quadruple systems $S(16, 4, 3)$ of order 16 with rank 14. We found all non-isomorphic homogenous systems with rank 14 over \mathbb{F}_2 .

*The paper has been written under the partial financial support of the Russian fund for the fundamental research (the number of project 03 - 01 - 00098)

§ 1. Introduction

A Steiner system $S(n, k, t)$ is a pair (X, B) where X is a v -set and B is a collection of k -subsets of X such that every t -subset of X is contained in exactly one member of B .

A system $S(v, 3, 2)$ is called a Steiner triple system (briefly STS(v)) and a system $S(v, 4, 3)$ is called a Steiner quadruple system (briefly SQS(v)). The necessary condition for existence of an SQS(v) is that $v \equiv 2$ or $4 \pmod{6}$. Hanani [2] proved that the necessary condition $v \equiv 2$ or $4 \pmod{6}$ for the existence of an $S(v, 4, 3)$ is also sufficient.

Two systems SQS(X, B) and SQS(X', B') are *isomorphic*, if there is a bijection $\alpha : X \rightarrow X'$ that maps the quadruples of B to those of B' . An *automorphism* of SQS(X, B) is an isomorphism of (X, B) to itself. The determination of number of the non-isomorphic SQS(v), which we will denote by $N(v)$, is the major problem in this area. Barrau [3] proved that $N(v) = 1$ for $v \leq 10$ and Mendelson and Hung [4] derived with the help of a computer that $N(14) = 4$.

In [5] it was shown that $N(16) \geq 8$. Using computer assisted computations, Gibbons, Mathon and Corneil [6] proved that $N(16) \geq 282$. The knowledge of all non-isomorphic 1-factorizations of K_8 (the complete graph on 8 vertices) together with their automorphism groups allowed Lindner and Rosa [7], using the classical doubling construction, obtained the bound $N(16) \geq 31021$ (for the number of systems with rank exactly 14 over \mathbb{F}_2). They slightly improved this bound in [8]: $N(16) \geq 31301$ (adding systems with rank less or equal 13 over \mathbb{F}_2). No progress has been made in this regard since this result of Lindner and Rosa (see [9], [10]).

Our result of [1] can be formulated as follows. *Among the non-isomorphic Steiner systems $S(16, 4, 3)$ of order $v = 16$ there are:*

- one $S(16, 4, 3)$ of rank 11 (the points and planes of 4-dimensional affine geometry $AG(4, 2)$ over \mathbb{F}_2);
- 15 systems $S(16, 4, 3)$ of rank 12;
- 4131 systems $S(16, 4, 3)$ of rank 13.

This paper is a natural continuation of our previous paper [1] where we started the systematic investigation of Steiner systems $S(16, 4, 3)$ of order 16 with given rank over the field \mathbb{F}_2 . Here we classified all Steiner systems $S(16, 4, 3)$ of order 16 with rank 14 over the field \mathbb{F}_2 . All such systems can be obtained by the generalized doubling construction, which we introduce here.

Our main result here can be formulated as follows. *Among the non-isomorphic Steiner systems $S(16, 4, 3)$ of order $v = 16$ there are:*

- 684764 systems $S(16, 4, 3)$ of rank 14 over \mathbb{F}_2 .

The paper is organized as follows. Preliminary results and terminology are given in § 2. In § 3 we describe the classical doubling construction of SQS($2n$) using given SQS(n). In § 4 we consider the general properties of SQS(n) with rank $n-2$ over \mathbb{F}_2 . Section § 5 is dedicated to the generalized doubling construction of Steiner systems $S(n, 4, 3)$ of arbitrary order n . The paragraph § 6 contains the main result of the paper: classification of all non-isomorphic Steiner systems $S(16, 4, 3)$ with rank 14 over \mathbb{F}_2 . In § 7 we give some results concerning the Steiner triple systems $S(15, 3, 2)$ which occur as derivative of all these non-isomorphic

$S(16, 4, 3)$ with rank 14. In particular, we found only such triple systems with numbers $1, 2, \dots, 22$ and 62 . We also found all homogeneous Steiner systems $S(16, 4, 3)$ of rank 14 (and from [1] we know such systems with ranks 11, 12 and 13). We give also the distribution of the number β (the number of non-somorphic derivative $S(15, 3, 2)$ of given $S(16, 4, 3)$) over all these systems $S(16, 4, 3)$ with rank 14.

§ 2. Preliminary results

Let E be a binary alphabet of size 2 : $E = \{0, 1\}$. A binary code of length n is an arbitrary subset of E^n . Denote such binary code C with length n , with the minimal distance d and cardinality N as (n, d, N) -code. Denote by $\text{wt}(\mathbf{x})$ the Hamming weight of vector \mathbf{x} over E . For a (binary) code C denote by $\langle C \rangle$ the linear envelope of words of C over \mathbb{F}_2 . The dimension of space $\langle C \rangle$ is called the *rank* of C over \mathbb{F}_2 and is denoted $\text{rank}(C)$.

Denote by (n, w, d, N) a binary constant weight code W of length n , with weight of all codewords w , with minimal distance d and cardinality N .

For any two subsets Y and Z of E^n denote by $d(Y, Z)$ the minimal distance between Y and Z :

$$d(Y, Z) = \min\{d(\mathbf{y}, \mathbf{z}) : \mathbf{y} \in Y, \mathbf{z} \in Z\}.$$

For vector $\mathbf{v} = (v_1, \dots, v_n) \in E^n$ denote by $\text{supp}(\mathbf{v})$ its support, i.e. the set of indices with nonzero positions:

$$\text{supp}(\mathbf{v}) = \{i : v_i \neq 0\}.$$

Denote by $\bar{\mathbf{v}}$ a vector, which is a complementary to \mathbf{v} , i.e. $\bar{v}_i = v_i + 1$.

If $E = \mathbb{F}_2$ is a field of order 2, the binary (n, d, N) -code A which is a linear k -dimensional space over \mathbb{F}_2 is denoted by $[n, k, d]$ -code. For binary vectors $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$ denote by $(\mathbf{x} \cdot \mathbf{y}) = x_1y_1 + \dots + x_ny_n$ their inner product over \mathbb{F}_2 . For a linear $[n, k, d]$ -code A denote by A^\perp its dual code:

$$A^\perp = \{\mathbf{v} \in \mathbb{F}_2^n : (\mathbf{v} \cdot \mathbf{c}) = 0, \forall \mathbf{c} \in A\}.$$

It is clear that A^\perp is a linear $[n, n - k, d^\perp]$ code with some minimal distance d^\perp .

Denote by E_2^n the set of all binary vectors of length n of weight 2. Let $J_n = \{1, 2, \dots, n\}$ be the coordinate set of E^n and let S_n be the full group of permutations of n elements. For any $i \in J_n$ and $\pi \in S_n$, define the image of i under the action of π by $\pi(i)$. For any set X of E^n and any $\pi \in S_n$ denote $\pi X = \{\pi(\mathbf{x}) : \mathbf{x} \in X\}$.

A binary incidence matrix of a Steiner system $S(v, 4, 3)$ is the binary constant weight code $(v, 4, 4, v(v-1)(v-2)/24)$, denoted by S which is strongly optimal [15]. In our notation the connection between the system (X, B) and the code S looks as follows:

$$B = \{\text{supp}(\mathbf{v}) \subset X : \mathbf{v} \in S\}.$$

For any Steiner system $S(v, 4, 3)$ denote by $\mu_s(\mathbf{c})$, where $\mathbf{c} \in S$ and $s \in \{0, 1, 2\}$, the number of codewords $\mathbf{x} \in S$ with distance $2(k - s)$ at \mathbf{c} , i.e.

$$\mu_s(\mathbf{c}) = |\{\mathbf{x} \in S : |\text{supp}(\mathbf{c}) \cap \text{supp}(\mathbf{x})| = s\}|, \quad s \in \{0, 1, 2\}.$$

The numbers $\mu_s(\mathbf{c})$ do not depend on the choice of \mathbf{c} and can be computed explicitly (see Theorem 5 in [15]). In particular, for $S(16, 4, 3)$ we have:

$$\mu_0 = 39, \quad \mu_1 = 64, \quad \mu_2 = 36. \quad (1)$$

For the case of Steiner systems the definition of equivalence can be formulated as follows.

Definition 1 *Two Steiner systems (X, B) and (X', B') of order 16 are isomorphic, if their incidence matrices S and S' are equivalent as constant weight codes, i.e. if there exists some permutation $\tau \in S_{16}$ such that S and $\tau S'$ coincide up to the permutation of rows.*

§ 3. SQS(2n) obtained by the doubling construction from SQS(n)

In this section, we describe the classical doubling construction of SQS(2n) from given SQS(n). Both constructions were described in [8], which we give here almost without changes. Denote by $F = F_1, F_2, \dots, F_{n-1}$ a full partition of E_2^n into subcodes with distance 4, i.e. for any $i, i = 1, \dots, n-1$ the set F_i is a constant weight $(n, 2, 4, n/2)$ -code. Let F and H be any such partitions of E_2^n , where $H = H_1, \dots, H_{n-1}$.

Construction A^* . Let (X, A) and (Y, B) be any two Steiner systems $S(n) = S(n, 4, 3)$ where $X \cap Y = \emptyset$. Let F and H where $F = F_1, \dots, F_{n-1}$ and $H = H_1, \dots, H_{n-1}$ be any full partitions of E_2^n and let α be any permutation from S_n . Define a constant weight code S on coordinate set $Q = X \cup Y$ as follows:

- (1) Any codeword belonging to A or B belongs to S ;
- (2) if $i_1, i_2 \in X$ and $j_1, j_2 \in Y$ then \mathbf{c} with $\text{supp}(\mathbf{c}) = \{i_1, i_2, j_1, j_2\}$ is a codeword of C , if and only if $\mathbf{f} \in F_{i_1}$ with $\text{supp}(\mathbf{f}) = \{i_1, i_2\}$, $\mathbf{h} \in H_{j_1}$ with $\text{supp}(\mathbf{h}) = \{j_1, j_2\}$ and $\alpha(i) = j$.

Proposition 1 [8] *Under construction, described above the set (Q, S) is a Steiner system $S(2n, 4, 3)$.*

In [7] these authors, using this construction and knowledge of all automorphisms groups of these partitions, derived the lower bound for $N(16) \geq 31021$.

Denote by F_1, F_2, \dots, F_6 the all non-isomorphic 1-partitions of E_2^8 , obtained in [22,23]. Agree that F_5 and F_6 are two partitions, not containing a sub-partitions of index 2 (see [24]), i.e. subcodes of partitions F_5 (respectively, F_6) do not form a partition of E_2^4 for any choice of 4 positions from E_2^8 .

Denote by $\{F_i\}$ the orbit by action of S_8 on F_i :

$$\{F_i\} = \text{Orb}_{S_8}(F_i), \quad i = 1, \dots, 6.$$

Simple arguments show that [7] for any two fixed $S(8, 4, 3)$ systems (X, A) and (Y, B) there are at least $|\{F_i\}| \cdot |\{F_j\}| \cdot 7!$ distinct $S(16, 4, 3)$ obtained by Construction A^* by taking any $F_i \in \{F_i\}$ for F and any $F_j \in \{F_j\}$ for G with $j \in \{5, 6\}$ and $i \neq j$. In addition, every such $S(16, 4, 3)$ has exactly two subsystems $S(8, 4, 3)$, namely (X, A) and (Y, B) . It follows [7] that there are at least

$$N_{A^*} = \frac{7!}{1344^2} \left(\sum_{i=1}^5 |\{F_i\}| \cdot |\{F_6\}| + \sum_{i=1}^4 |\{F_i\}| \cdot |\{F_5\}| \right).$$

By this construction it can be seen [7] that all resulting systems $S(16, 4, 3)$ have rank exactly 14 over \mathbb{F}_2 . The exact computation shows [7] that $N_{A^*} = 31021$. Using 280 systems found in [25], for which the number of sub-systems $S(8, 4, 3)$ different from two (which means that these 280 systems $S(16, 4, 3)$ have the rank less or equal to 13 over \mathbb{F}_2), one can get [7] that $N(16) \geq 31301$.

§ 4. General properties of SQS(16) with rank 14 over \mathbb{F}_2

Let S be an arbitrary Steiner system $S(16, 4, 3)$ of rank 14 over \mathbb{F}_2 . We consider the general properties of such system.

Applying the appropriate permutation of coordinates, S can be presented in the form, when the $[16, 8, 2]$ -code S^\perp , dual to S , looks as follows:

$$S^\perp = \{\mathbf{u}_0, \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_1 + \mathbf{u}_2\}, \quad (2)$$

where \mathbf{u}_0 is the zero vector, $\mathbf{u}_1 = (1111111100000000)$, and $\mathbf{u}_2 = (0000000011111111)$. Thus we split coordinates of S into two blocks of eight coordinates such that any $\mathbf{c} \in S$ consists of two vectors $\mathbf{c} = (\mathbf{c}_1 | \mathbf{c}_2)$ where each vector \mathbf{c}_i satisfies to the overall parity checking:

$$\text{wt}(\mathbf{c}_i) \equiv 0 \pmod{2}, \quad i = 1, 2$$

(we call it a *parity rule*).

Definition 2 Let S be a Steiner system $(16, 4, 3)$ of rank 14 over \mathbb{F}_2 with dual code (2). Define the subset S_{uv} of S where $u, v \in \{0, 2, 4\}$ as follows:

$$S_{uv} = \{\mathbf{c} = (\mathbf{a} | \mathbf{b}) \in S : \text{wt}(\mathbf{a}) = u, \text{wt}(\mathbf{b}) = v\}.$$

These words are called (u, v) -words.

Lemma 1 Let S be a Steiner system $(16, 4, 3)$ of rank 14 over \mathbb{F}_2 with dual code (2). Then S is a union of three subsets

$$S = S_{40} \cup S_{04} \cup S_{22}$$

where S_{40} (respectively S_{04}) is a Steiner system $S(8, 4, 3)$ and S_{22} has cardinality 112.

Proof. Follows from definition of Steiner system $S(16, 4, 3)$. \blacktriangle

The group (subgroup of S_{16}) of two elements which permutes the blocks is identified with S_2 . An element $\tau_1 \times \tau_2 \in S_8 \times S_8 \subset S_{16}$ acts on $(\mathbf{x} | \mathbf{y})$ in the natural way:

$$(\tau_1 \times \tau_2)(\mathbf{x} | \mathbf{y}) = (\tau_1(\mathbf{x}) | \tau_2(\mathbf{y})).$$

We have the following statement.

Lemma 2 *Let S be an arbitrary Steiner system $S(16, 4, 3)$ of rank 14 over \mathbb{F}_2 with dual code (2). Suppose there exists a permutation $\sigma \in S_{16}$ so that σS satisfies the parity rule. Then $\sigma \in S_2 \times (S_8 \times S_8)$.*

Proof. Since S satisfies parity rule, we have that

$$(\mathbf{x} \cdot \mathbf{u}_1) = 0, \quad (3)$$

for any $\mathbf{x} \in S$. Similarly, since σS satisfies the parity rule, we have that

$$(\sigma(\mathbf{x}) \cdot \mathbf{u}_1) = 0, \quad \text{for any } \mathbf{x} \in S.$$

Multiplying both vectors $\sigma(\mathbf{x})$ and \mathbf{u}_1 by σ^{-1} , we obtain

$$(\mathbf{x} \cdot \sigma^{-1}(\mathbf{u}_1)) = 0, \quad \text{for any } \mathbf{x} \in S. \quad (4)$$

Let $\mathbf{u}' = \mathbf{u}_1 + \sigma^{-1}(\mathbf{u}_1)$. From (3) and (4) we have that

$$(\mathbf{x} \cdot \mathbf{u}') = 0, \quad \text{for any } \mathbf{x} \in S.$$

Thus $\mathbf{u}' \in S^\perp$ and consequently (recall that S^\perp is a vector space) $\sigma^{-1}(\mathbf{u}_1) \in S^\perp$. Taking into account that $\sigma^{-1}(\mathbf{u}_1)$ is of weight 8, we obtain that $\sigma^{-1}(\mathbf{u}_1)$ is equal to either \mathbf{u}_1 or \mathbf{u}_2 . So $\sigma(\mathbf{u}_1) = \mathbf{u}_1$ or $\sigma(\mathbf{u}_2) = \mathbf{u}_1$, in other words, σ either stabilizes the blocks or permutes them.

▲

Recall that E_2^8 is the subset of E^8 , formed by the all vectors of weight 2. Denote any codeword of S by $\mathbf{c} = (\mathbf{a} | \mathbf{b})$.

Definition 3 *Let S be a Steiner system $(16, 4, 3)$ of rank 14 over \mathbb{F}_2 with dual code (2). Let $\mathbf{c} = (\mathbf{a} | \mathbf{b})$ be any codeword of S such that $\text{wt}(\mathbf{a}) = \text{wt}(\mathbf{b})$. Denote by $A_l(\mathbf{b})$ (respectively, by $A_r(\mathbf{a})$) the sets obtained by fixing vector \mathbf{b} (respectively \mathbf{a}):*

$$A_r(\mathbf{a}) = \{\mathbf{b} : (\mathbf{a} | \mathbf{b}) \in S\}, \quad A_l(\mathbf{b}) = \{\mathbf{a} : (\mathbf{a} | \mathbf{b}) \in S\}.$$

Lemma 3 *Suppose the conditions of lemma 2 are satisfied. Let $\mathbf{c} = (\mathbf{a} | \mathbf{b})$ be any codeword of S such that $\text{wt}(\mathbf{a}) = \text{wt}(\mathbf{b})$. Then the set $A_l(\mathbf{b})$ (respectively $A_r(\mathbf{a})$) is a Steiner system $S(8, 2, 1)$ (or, equivalently, a constant weight $(8, 2, 4, 4)$ code).*

Proof. The fact that $A_l(\mathbf{b})$ (respectively, $A_r(\mathbf{a})$) is a constant weight code $(8, 2, 4, N_l(\mathbf{b}))$ with minimal distance 4 follows from definition of such set. Indeed, any two words of S have distance not less than 4, implying that any two distinct words \mathbf{x} and \mathbf{x}' of $A_l(\mathbf{b})$ have distance not less than 4. From the other side, since S is a 3-design, nonzero positions of vectors \mathbf{x} from $A_l(\mathbf{b})$ should cover all 8 positions of the first coordinate block of S . This means that for any $\mathbf{b} \in E_2^8$ the set $A_l(\mathbf{b})$ is a 1-design or $S(8, 2, 1)$. This follows also from counting arguments. In average, over all $\mathbf{b} \in E_2^8$, we have that

$$|\bar{A}_l| = \frac{1}{|E_2^8|} \times \sum_{\mathbf{b} \in E_2^8} |A_l(\mathbf{b})| = \frac{|C_{(2)}|}{|E_2^8|} = 4.$$

From the other side, $|A_l(\mathbf{b})|$ can not be more than 4 for any $\mathbf{b} \in E_2^8$. Thus $|A_l(\mathbf{b})| = 4$. Similarly, the same equality is valid for $|A_r(\mathbf{a})|$. ▲

Definition 4 Define the sphere $W_i \subset E_2^8$, $i = 1, 2, \dots, 8$ of radius two as a set of seven vectors $\mathbf{e}_1(i), \dots, \mathbf{e}_7(i)$ from E_2^8 , which satisfy to the following properties:

- 1). $\{i\} \in \text{supp}(\mathbf{e}_j(i))$, $j = 1, \dots, 7$.
- 2). $d(\mathbf{e}_j(i), \mathbf{e}_s(i)) = 2$, for any $j \neq s$.

For example, the sphere W_8 , which we use very often, consists of the following vectors, which we denote for short $\mathbf{e}_s(8) = \mathbf{e}_s$:

$$\begin{aligned} \mathbf{e}_1 &= (00000011), & \mathbf{e}_2 &= (00000101), \\ \mathbf{e}_3 &= (00001001), & \mathbf{e}_4 &= (00010001), \\ \mathbf{e}_5 &= (00100001), & \mathbf{e}_6 &= (01000001), \\ \mathbf{e}_7 &= (10000001). \end{aligned}$$

Note that the stabilizer of W_8 in S_8 fixes the last nonzero coordinate of $\mathbf{e}_i(8)$ and is isomorphic to S_7 .

Lemma 4 Suppose we are in conditions of lemma 2 and let $(\mathbf{a}_1 | \mathbf{b}_1)$ and $(\mathbf{a}_2 | \mathbf{b}_2)$ be any two codewords of $C_{(2)}$. Let \mathbf{a}_1 and \mathbf{a}_2 (respectively, \mathbf{b}_1 and \mathbf{b}_2) be such that $d(\mathbf{a}_1, \mathbf{a}_2) = 2$ (respectively, $d(\mathbf{b}_1, \mathbf{b}_2) = 2$). Then the corresponding codes $A_r(\mathbf{a}_1)$ and $A_r(\mathbf{a}_2)$ (respectively, $A_l(\mathbf{b}_1)$ and $A_l(\mathbf{b}_2)$) do not intersect each other, i.e. $A_r(\mathbf{a}_1) \cap A_r(\mathbf{a}_2) = \emptyset$ (respectively, $A_l(\mathbf{b}_1) \cap A_l(\mathbf{b}_2) = \emptyset$).

Proof. In contrary, assume that there is \mathbf{x} such that $\mathbf{x} \in A_r(\mathbf{a}_1) \cap A_r(\mathbf{a}_2)$. Then we have

$$d((\mathbf{a}_1 | \mathbf{x}), (\mathbf{a}_2 | \mathbf{x})) = d(\mathbf{a}_1, \mathbf{a}_2) = 2,$$

i.e. a contradiction, since $(\mathbf{a}_1 | \mathbf{x})$ and $(\mathbf{a}_2 | \mathbf{x})$ are distinct codewords of C . The proof of the second statement is similar. \blacktriangle

Lemma 5 Suppose we are in conditions of lemma 2 and let $W_i = \{\mathbf{e}_1(i), \dots, \mathbf{e}_7(i)\}$ be any sphere, $i = 1, 2, \dots, 8$. Then the set of codes $A_l(\mathbf{e}_1(i))$, $A_l(\mathbf{e}_2(i))$, ..., $A_l(\mathbf{e}_7(i))$ forms a partition of E_2^8 .

Proof. Since

$$|W_i| \times |A_l(\mathbf{e}_s(i))| = |E_2^8| = 28,$$

we have to check only that any two distinct codes $A_l(\mathbf{e}_j(i))$ and $A_l(\mathbf{e}_s(i))$ where $j \neq s$ and $j, s \in \{1, \dots, 7\}$ have empty intersection. But this follows from lemma 4, since for any $\mathbf{e}_j(i), \mathbf{e}_s(i)$ from W_i we have that $d(\mathbf{e}_j(i), \mathbf{e}_s(i)) = 2$. \blacktriangle

Remark 1 It is easy to see that the results above, which we derived for Steiner system $S(16, 4, 3)$ of rank 14 over \mathbb{F}_2 , are valid for any $S(n, 4, 3)$ of arbitrary order $n \geq 16$ with rank $n - 2$ over \mathbb{F}_2 such that $n/2 \equiv 2$ or $4 \pmod{6}$.

§ 5. Generalized doubling construction of $S(16, 4, 3)$ with rank 14 over \mathbb{F}_2

Now we describe the general doubling construction of Steiner systems $S(16, 4, 3)$ with rank 14 over \mathbb{F}_2 . This construction is induced by the general doubling construction of the extended binary perfect nonlinear $(16, 4, 2^{11})$ -codes of rank 14 over \mathbb{F}_2 , which we described in [15]. Indeed, the set of codewords of weight four of any such $(16, 4, 2^{11})$ -code with zero codeword forms a Steiner system $S(16, 4, 3)$.

It is convenient for us to present such a system $S(16, 4, 3)$ by the corresponding constant weight $(16, 4, 4, 140)$ code, which uniquely defines this system [16], and which we denote here by S . Denote by \mathcal{S} the set of all such distinct $(16, 4, 4, 140)$ codes S . Our purpose now is to parameterize all these Steiner systems, using the canonical partitions of E_2^8 . We can do it using the special subsets of S , called headings, formed by the two partitions, connected with the two spheres $W_8 = \{\mathbf{e}_s : s = 1, \dots, 7\}$ which occur on the left and right hand sides (the first and the second blocks) of the codewords. We start with the definition of *heading* of a code. Clearly when $\mathbf{c} = (\mathbf{a} | \mathbf{b})$ runs over S , each of two vectors \mathbf{a} and \mathbf{b} run over the set E_2^8 . In particular, when \mathbf{a} runs over the sphere W_8 the corresponding codes $A_r(\mathbf{a})$ form a partition of E_2^8 ,

$$E_2^8 = \bigcup_{\mathbf{a} \in W_8} A_r(\mathbf{a}) = \bigcup_{s=1}^7 A_r(\mathbf{e}_s).$$

Similarly, when \mathbf{b} runs over the set W_8 , the codes $A_l(\mathbf{b})$ also form a partition of E_2^8 .

Denote by Ω the set of all distinct partitions $L_i = (L_{i,1}, L_{i,2}, L_{i,3}, L_{i,4})$ of E_2^8 into (binary constant weight) $(8, 2, 4, 4)$ codes $L_{i,s}$, $s = 1, 2, 3, 4$. Moreover the following result holds.

Proposition 2 (*Computational result*). *There exist exactly 6240 different partitions of E_2^8 which can be arranged under action of S_8 into six orbits $\text{Orb}_{S_8}(L_i)$, ordered according to the indices i of $\text{Orb}_{S_8}(L_i)$.*

We assume that the unique Steiner system $S(8, 4, 3)$ is formed by the following vectors (in addition to words of all zeroes and ones):

$$\begin{array}{ll} (1111|0000), & (0000|1111), \\ (1100|1100), & (0011|0011), \\ (1100|0011), & (0011|1100), \\ (1010|0110), & (0101|1001), \\ (1010|1001), & (0101|0110), \\ (1001|1010), & (0110|0101), \\ (1001|0101), & (0110|1010). \end{array}$$

Denote by P its stabilizer in S_8 and by P' its stabilizer in the group S_7 .

Definition 5 *Define the group:*

$$G = S_2 \times (P \times P) \subset S_{16}$$

It is known (see, for example, [8]) that $|P| = 1344$. Recall Lemma 1 that any system S of rank 14 (with dual code S^\perp given by (2)) is partitioned into three subsets S_{40} , S_{04} and S_{22} . Without loss of generality, we can assume from now that all our systems S from \mathcal{S} are such that the subsets $S_{40} = A_l(\mathbf{0})$ and $S_{04} = A_r(\mathbf{0})$ of 14 elements are obtained from the Steiner system given above. This condition increases the number of non-equivalent partitions of E_2^8 since we consider the P -equivalence and P' -equivalence.

Proposition 3 (*Computational result*). *Let Ω be the set of all 6240 different partitions of E_2^8 into $(8, 2, 4, 4)$ codes. Then Ω splits into 43 P -orbits $\text{Orb}_P(L_i)$ ($i = 1, \dots, 43$) and 62 P' -orbits $\text{Orb}_{P'}(L'_i)$. We assume that the 62 non-equivalent partitions L'_i are chosen so that $L_i = L'_i$, where $i = 1, \dots, 43$.*

We denote L'_i via L_i , $i = 1, \dots, 62$ and call them *canonical partitions* of E_2^8 .

For any such canonical partition L_i , denote by $\text{Stab}_P(L_i)$ the stabilizer of L_i in the group P and by $Q_i \subset S_7$ a group of permutations of its seven components $L_{i,1}, L_{i,2}, \dots, L_{i,7}$ induced by the automorphisms of P :

$$Q_i = \{\pi \in S_7 : \exists \mathbf{g} \in \text{Stab}_P(L_i) : \mathbf{g}L_{i,s} = L_{i,\pi^{-1}(s)}, i = 1, \dots, 7\}.$$

For an element $\mathbf{a} \in E^8$ and set $X \subseteq E^8$ denote:

$$\mathbf{a} \times X = \{(\mathbf{a} | \mathbf{x}) : \mathbf{x} \in X\}, \quad X \times \mathbf{a} = \{(\mathbf{x} | \mathbf{a}) : \mathbf{x} \in X\}.$$

Definition 6 *Let S be a $(16, 4, 4, 140)$ code with rank 14 over \mathbb{F}_2 . Define the following subset $F = F(S)$ of S (of 56 words), consisting of two partitions (with 7 common words counted twice)*

$$F(S) = \bigcup_{s=1}^7 \{(e_s | \mathbf{y}) : \mathbf{y} \in A_r(e_s)\} \cup \bigcup_{s=1}^7 \{(\mathbf{x} | e_s) : \mathbf{x} \in A_l(e_s)\}. \quad (5)$$

We say that S has a heading F and for the sake of simplicity write as:

$$F = \bigcup_{s=1}^7 e_s \times A_r(e_s) \cup \bigcup_{s=1}^7 A_l(e_s) \times e_s.$$

Assume that the partition $A_l(e_1), \dots, A_l(e_7)$ is equivalent to L_i for some i , $i = 1, \dots, 43$ and the partition $A_r(e_1), \dots, A_r(e_7)$ is equivalent to L_j for some j , $j = 1, \dots, 62$. Recall that L_i (respectively, L_j) are among of the 43 (respectively 62) canonical (non-equivalent) partitions, given by proposition 3. All these partitions L_i , $i = 1, \dots, 62$ are ordered, according to the vectors \mathbf{e}_s of the ball W_8 :

$$L_i = (L_{i,1}, \dots, L_{i,7}) \quad \text{where } \mathbf{e}_s \in L_{i,s} \quad \text{for } s = 1, \dots, 7.$$

Without loss of generality we can assume that $i \leq j$ (if not we can consider the Steiner system S' obtained from S by switching the sides). Furthermore, by the corresponding permutation of coordinates we can obtain the following ordering of L_i :

$$L_i = (L_{i,1}, \dots, L_{i,7}), \quad L_{i,s} = A_l(\mathbf{e}_s), \quad (6)$$

where the vectors \mathbf{e}_s ($s = 1, \dots, 7$) are given by definition 4. In such way we arrive to the following natural *canonical heading*.

Definition 7 (*Canonical (i, j, k) heading*). Let $1 \leq i \leq 43$ and $i \leq j \leq 62$ and L_i, L_j are two canonical partitions. Define the set of 56 (where 7 words are counted twice) elements as follows:

$$\begin{aligned} F_{i,j}^{(k)} &= \bigcup_{s=1}^7 L_{i,\pi(s)} \times \mathbf{e}_s \cup \bigcup_{s=1}^7 \mathbf{e}_{\pi(s)} \times L_{j,s} \\ &= \bigcup_{s=1}^7 \{(\mathbf{x} | \mathbf{e}_s) : \mathbf{x} \in L_{i,\pi(s)}\} \cup \bigcup_{s=1}^7 \{(\mathbf{e}_{\pi(s)} | \mathbf{y}) : \mathbf{y} \in L_{j,s}\}. \end{aligned}$$

where $\pi = \pi_k^{-1}$, $k = 1, 2, \dots, m(i, j)$, and

$$\{\pi_1, \pi_2, \dots, \pi_{m(i,j)}\}$$

is a fixed set of the $(Q_j - Q_i)$ -double-coset representatives of S_8 .

We know all canonical headings (i, j, k) .

Proposition 4 (*Computational result*). There exist 339716 different canonical headings (i, j, k) .

Using canonical headings, now we can define *canonical Steiner systems* C .

Definition 8 (*Canonical Steiner system*). Let S be any Steiner system from \mathcal{S} . We say that S is a canonical (i, j, k) code, denoted by $S_{i,j}^{(k)}$ if S has a canonical heading

$$F(S_{i,j}^{(k)}) = F_{i,j}^{(k)}.$$

Now the important question is does any system S from \mathcal{S} equivalent to a canonical one $S_{i,j}^{(k)}$?

Proposition 5 Let $S \in \mathcal{S}$ and let $F = F(S)$ be the heading of S . Then S is G -equivalent to a canonical Steiner system $S_{i,j}^{(k)} \in \mathcal{S}$ with heading $F_{i,j}^{(k)}$, where $1 \leq i \leq 43$ and $i \leq j \leq 62$ and where the permutation π_k is defined by definition 7.

Proof. Let S be any Steiner system from \mathcal{S} . Define the following subset of S

$$Y_2 = \bigcup_{s=1}^7 A_l(\mathbf{e}_s) \times \mathbf{e}_s = \{(\mathbf{y} | \mathbf{e}_s) : \mathbf{e}_s \in W_8, \mathbf{y} \in A_l(\mathbf{e}_s)\}, \quad (7)$$

where $A_l(\mathbf{e}_s)$, $s = 1, \dots, 7$ is a partition A_l of E_2^8 . Assume that A_l is P -equivalent to L_i for some i . Thus there exists a permutation $\tau_2 \in P$ such that $\tau_2 A_l = L_i$ and in particular

$$\tau_2 A_l(\mathbf{e}_s) = L_{i, \tau_2^{-1}(s)}. \quad (8)$$

Let 1_8 be the identity element of S_8 . Applying the element $\tau_2 \times 1_8$ to S , its subset defined (7), and taking into account (8), we have

$$\begin{aligned} (\tau_2 \times 1_8)Y_2 &= (\tau_2 \times 1_8) \left\{ \bigcup_{s=1}^7 A_l(\mathbf{e}_s) \times \mathbf{e}_s \right\} \\ &= \bigcup_{s=1}^7 (\tau_2 A_l(\mathbf{e}_s)) \times \mathbf{e}_s \\ &= \bigcup_{s=1}^7 L_{i, \tau_2^{-1}(s)} \times \mathbf{e}_s \\ &= \bigcup_{s=1}^7 L_{i, s} \times \mathbf{e}_{\tau_2(s)}. \end{aligned}$$

Set $S' = (\tau_2 \times 1_8)S$, and define the following subset of S'

$$Y_1 = \bigcup_{s=1}^7 \mathbf{e}_s \times A_r(\mathbf{e}_s) = \{(\mathbf{e}_s | \mathbf{y}) : \mathbf{e}_s \in W_8, \mathbf{y} \in A_r(\mathbf{e}_s)\},$$

where $A_r(\mathbf{e}_s)$, $s = 1, \dots, 7$ is a partition A_r of E_2^8 . Assume that A_r is P' -equivalent to L_j for some j . Thus there exists an element $\tau_1 \in P'$ such that $\tau_1 A_r = L_j$ and $\tau_1 W_8 = W_8$. In particular

$$\tau_1 A_r(\mathbf{e}_s) = L_{j, \tau_1^{-1}(s)}. \quad (9)$$

Applying the element $1_8 \times \tau_1$ to S' , its subset Y_1 , and taking into account (9), we have

$$\begin{aligned} (1_8 \times \tau_1)Y_1 &= (1_8 \times \tau_1) \left\{ \bigcup_{s=1}^7 \mathbf{e}_s \times A_r(\mathbf{e}_s) \right\} \\ &= \bigcup_{s=1}^7 \mathbf{e}_s \times (\tau_1 A_r(\mathbf{e}_s)) \\ &= \bigcup_{s=1}^7 \mathbf{e}_s \times L_{j, \tau_1^{-1}(s)}. \end{aligned}$$

Moreover, we have

$$\begin{aligned} (1_8 \times \tau_1) \left\{ \bigcup_{s=1}^7 L_{i,s} \times \mathbf{e}_{\tau_2(s)} \right\} &= \bigcup_{s=1}^7 L_{i,s} \times \tau_1(\mathbf{e}_{\tau_2(s)}) \\ &= \bigcup_{s=1}^7 L_{i,s} \times \mathbf{e}_{\tau_3(s)}, \end{aligned}$$

for some permutation $\tau_3 \in S_7$. Since $\mathbf{e}_{\tau_3(s)} \in L_{j,\tau_1^{-1}(s)}$ we conclude that $\tau_3 = \tau_1^{-1}$. Set $S'' = (1_8 \times \tau_1)S'$. Then S'' is equivalent to S and its heading by definition is equal to

$$\bigcup_{s=1}^7 L_{i,s} \times \mathbf{e}_{\tau_1^{-1}(s)} \cup \bigcup_{s=1}^7 \mathbf{e}_s \times L_{j,\tau_1^{-1}(s)}.$$

Without loss of generality we can always assume that $i \leq j$ (if not apply the permutation of S_2 from the definition of G , i.e. switch the blocks of coordinates). \blacktriangle

It is clear that a Steiner system S can have different headings as well as different Steiner systems may have the same heading.

Now we want to describe the general doubling construction of Steiner systems $S(16, 4, 3)$ of rank 14 over \mathbb{F}_2 .

Definition 9 Let \mathcal{M}_s , $s = 1, 2, \dots, 7$ be the set of constant weight $(8, 2, 4, 4)$ codes containing e_s . Let

$$\mathcal{M} = \bigcup_{s=1}^7 \mathcal{M}_s$$

be the set of all constant weight $(8, 2, 4, 4)$ codes.

It is easy to check that there are 15 codes in every set \mathcal{M}_s so that the total number of $(8, 2, 4, 4)$ codes is 105. We consider functions from E_2^8 to \mathcal{M} .

Definition 10 (*Admissible function*) We say that a function $\Lambda: E_2^8 \rightarrow \mathcal{M}$ is admissible if there exist $1 \leq i \leq 43$, $i \leq j \leq 62$, and a permutation π_k such that:

- 1). $\Lambda(\mathbf{e}_{\pi^{-1}(s)}) = L_{j,s}$, for $s = 1, \dots, 7$.
 - 2). $\Lambda(\mathbf{x}) = M \in \mathcal{M}_s$, where $\mathbf{x} \in L_{i,\pi^{-1}(s)}$ and $s = 1, \dots, 7$.
- Such function will be called an (i, j, k) -admissible function.

Admissible functions are used to parameterize canonical Steiner systems. Indeed for any canonical Steiner system $S = S_{i,j}^{(k)}$, and any $\mathbf{x} \in E_2^8$, set $\Lambda(\mathbf{x}) = A_r(\mathbf{x})$ (see Definition 3). Then

$$S_{22} = \bigcup_{\mathbf{x} \in E_2^8} \mathbf{x} \times \Lambda(\mathbf{x}),$$

where Λ is (i, j, k) -compatible by definition.

§ 6. Derived triple systems

For an SQS(v), given by the pair of sets (X, B) , a derived triple system (briefly DTS($v - 1$)) of (X, B) is a pair (X_a, B_a) , where $X_a = X \setminus \{a\}$ and $B_a = \{b \setminus \{a\} : a \in b \in B\}$. It is obvious, that every derived triple system is a Steiner triple system $S(v - 1, 3, 2)$. For $v = 16$ we obtain a system $S(15, 3, 2)$. It is known [19] from 1917 that there are exactly 80 non-isomorphic systems $S(15, 3, 2)$. There is a standard numbering of these systems by the indices from 1 to 80, related to the number of Pasch configurations (see [1]).

Given a Steiner system $S = S(v, 4, 3)$, let $\beta = \beta(S)$ denote the number of its pairwise non-isomorphic DTS($v - 1$). Clearly $1 \leq \beta \leq v$ for any SQS(v). A system SQS(v) is said to be *homogeneous* (respectively, *heterogeneous*), if $\beta = 1$ (respectively, $\beta = v$). Among all Steiner systems SQS(16) of rank at most thirteen, the only derived systems DTS(15) that we found are those with numbers 1, 2, 3, 4, 5, 6, 7. All Steiner triple systems with these numbers occur as the DTS(15) in the homogeneous SQS(16).

Denote by $N_{hom}(i)$ the number of non-isomorphic homogeneous systems SQS(16) with rank at most thirteen, whose derived systems are DTS(15) with number i , where $i \in \{1, 2, \dots, 7\}$. Denote by $N(\beta)$ the number of such non-isomorphic systems SQS(16) with rank at most thirteen with given β . Denote by $N(\mu(i_1), \mu(i_2), \dots, \mu(i_\beta))$ the number of non-isomorphic systems SQS(16) with rank at most thirteen which have $\mu(i_s) > 0$ derived systems with number i_s , where $i_s \in \{1, 2, \dots, 7\}$ for $s = 1, \dots, \beta$, i.e. in our notation $N_{hom}(i) = N(\mu(i) = 16)$.

§ 7. Non-isomorphic Steiner systems SQS(16) of rank 14 over \mathbb{F}_2

Theorem 1 *There exists 684764 non-equivalent Steiner systems $S(16, 4, 3)$ of length 16 and rank 14.*

Proof. Computational result. First, we construct all different Steiner systems using (i, j, k) -admissible functions Λ . Then to any Steiner system SQS(16) we associate a set of 16 indices of the derived triple systems. We note that if the two sets that correspond to an arbitrary two SQS(16) systems are different these systems are non-equivalent. Thus all different Steiner systems are arranged into lists which correspond to the same set of 16 indices. The lists are pair-wise non-equivalent, i.e. two systems belong to the different lists are non-equivalent. ▲

§ 8. Resolvability

The general *resolvability* problem for SQS(v) can be stated as follows. A Steiner system $S(v, 4, 3)$ is called (t, λ) -*resolvable* if its block set B can be partitioned into r subsets B_1, B_2, \dots, B_r such that (S, B_i) is a t -design $T(v, 4, t, \lambda)$ for all i . It is clear that

$$\frac{|B|}{r} = \frac{\binom{v}{t}}{\binom{4}{t}} \cdot \lambda.$$

For the case of systems $S(v, 4, 3)$ there are two possibilities: $t = 1$ or $t = 2$. Denote (t, λ) -resolvable SQS(v) by RSQS(t, λ, v). If $(t, \lambda) = (1, 1)$ such SQS(v) is also called *resolvable*, and if SQS(v) is $((t, 1)$ -resolvable simultaneously for $t = 1$ and 2 it is also called *double resolvable*. The first infinite family of double resolvable SQS(v) for all $v = 4^m$ was given in [21] (see also [11] and references there). Next, we would like to show that all systems SQS(16) of rank 14 over \mathbb{F}_2 are resolvable.

REFERENCES

1. *Zinoviev V.A., Zinoviev D.V.* Classification of Steiner quadruple systems of order 16 and rank at most thirteen// Problems of Information Transmission. 2004. V. 40. N° 4. P. 48–67.
2. *Hanani H.* On quadruple systems// Canad. J. Math. 1960. V. 12. P. 145-157
3. *Barrau J.A.* On the combinatory problem of Steiner // K. Akad. Wet. Amst. Proc. Sect. Sci. 1908. V. 11. P. 352-360.
4. *Mendelsohn N.S., Hung S.H.Y.* On the Steiner Systems $S(3, 4, 14)$ and $S(4, 5, 15)$ // Utilitas Math. 1972. V. 1. P. 5-95.
5. *Doyen J., Vandensavel M.* Non-isomorphic Steiner quadruple systems// Bull. Soc. Math. Belg. 1971. V. 23. P. 393-410.
6. *Gibbons P.B., Mathon R., Corneil D.G.* Steiner quadruple systems on 16 symbols// In: Proc. 6-th Southeastern Conf. Combinatorics, Graph Theory and Computing, Boca Raton. 1975. Congressus Numerantium XIV (Utilitas Math. Publ. Winnipeg. 1975). P. 345-365.
7. *Lindner C.C., Rosa A.* There are at least 31021 nonisomorphic Steiner quadruple systems of order 16// Utilitas Math. 1976. V. 10. P. 61-64.
8. *Lindner C.C., Rosa A.* Steiner quadruple systems – A survey// Discrete Mathematics. 1978. V. 21. P. 147-181.
9. *Hartman A., Phelps K.T.* 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.
10. *C.J. Colbourn C.J., J.H. Dinitz J.H.* The CRC Handbook of Combinatorial Designs. Boca Raton, FL: CRC Press, 1996.
13. *Zinoviev V.A., Zinoviev D.V.* Classification of Steiner quadruple systems of order 16 and rank at most thirteen// Proc. Ninth Int. Workshop on Algebraic and Combinatorial Coding Theory. Kranevo, Bulgaria (June 19-25), 2004, P. 399-403.
14. *Zinoviev V.A., Zinoviev D.V.* Binary extended perfect codes of length 16 by generalized concatenated construction// Problems of Information Transmission. 2002. V. 38. N° 4. P. 56–84.
15. *Zinoviev V.A., Zinoviev D.V.* Binary extended perfect codes of length 16 and rank 14// Problems of Information Transmission. 2004. submitted.
16. *Semakov N.V., Zinoviev V.A.* Constant weight codes and tactical configurations// Problems of Information Transmission. 1969. V. 5. N° 3. P. 29–38.

17. *Zinoviev V.A., Lobstein A.* On generalized concatenated constructions of perfect binary nonlinear codes// Problems of Information Transmission. 2000. V. 36. N° 4. P. 59–73.
18. *Doyen J., Hubaut X., Vandensavel M.* Ranks of Incidence Matrices of Steiner Triple Systems// Mathem. Zeitschr. 1978. V. 163. P. 251-259.
19. *MacWilliams F.J., N.J.A. Sloane N.J.A., The theory of Error Correcting Codes,* North-Holland, 1986.
20. *Cole F.N., Cummings L.D., White H.S.* The complete enumeration of trial systems in 15 elements// Proc. Nat. Acad. Sci. USA. 1917. V. 3. P. 197-199.
21. *de Vries H.L.* Some Steiner quadruple systems $S(3, 4, 16)$ such that all 16 derived triple systems $S(2, 3, 15)$ are isomorphic// Ars Combin. 1987. V. 24A. P. 107–129.
22. *Zaitsev G.V., Zinoviev V.A., Semakov N.V.* Interrelation of Preparata and Hamming codes and extension of Hamming codes to new double-error-correcting codes, in: "2nd International Symposium on Information Theory, Tsahkadzer, Armenia, USSR, 1971," Akademiai Kiado-Budapest. 1973. P. 257-263.
23. *Dickson L.E., Safford F.H.* Solution to Problem 8 (Group Theory)// Am. Math. Monthly. 1906. V. 13. P. 150–151.
24. *Wallis W.D.* On one-factorizations of complete graphs// J. Austral. Math. Soc. 1973. V. 16. P. 167–171.
25. *Lindner C.C., Mendelsohn E., Rosa A.* On the number of 1-factorizations of the complete graph// J. Combinatorial Theory. B. 1976. V. 20. P. 265–282.
26. *Gibbons P.B.* Computing techniques for the construction and analysis of block designs// Ph.D Thesis. University of Toronto. 1976.

Zinoviev Victor Alexandrovich

Zinoviev Dmitrii Victorovich

Institute for Information Transmission Problems, Russian Academy of Sciences

zinov@iitp.ru

dzinov@iitp.ru