On components of Steiner systems

Dimitrii Zinoviev
and
Victor Zinoviev

Institute for Problems of Information Transmission,
Moscow, Russia

Summary. For arbitrary Steiner systems $S(v, k, k-1)$ we introduce a concept of component, a subset of system, which can be switched (i.e. some positions can be permuted) without missing a property to be a Steiner system. Thus a component permits to build new Steiner systems (of the same orders) from the old ones. Two recursive constructions of such components for arbitrary systems $S(v, k, k-1)$ are derived. Components for the case $k = 3$ and $k = 4$ are considered in more details. In particular, for these cases new systems can have larger ranks. This approach permits to show that Steiner systems $S(v, k, k-1)$ with $k \geq 5$ have always maximum possible ranks over F_2.

1. Introduction. A Steiner system $S(n, k, t)$ is a pair (J, B) where J is a v-set and B is a collection of k-subsets (blocks) of J such that every t-subset of J is contained in exactly one block of B. A system $S(v, 3, 2)$ is called a Steiner triple system and a system $S(v, 4, 3)$ is called a Steiner quadruple system.

This paper is a natural continuation of our paper [ZZ] where we introduced a transformation of Steiner quadruple systems $S(v, 4, 3)$, which in fact was a *permutation of two positions in some subset of the system*, i.e. a typical switching construction. Here, for an arbitrary Steiner system $S(v, k, k-1)$, we introduce a concept of component, as a special small subset of vectors of a system, which can be slightly modified, for example, by some permutation of several positions, without missing a property to be a Steiner system.

2. Preliminary results. Let $E = \{0, 1\}$. A binary code of length n is an arbitrary subset of E^n. Denote a binary code C with length n, with minimum distance d and cardinality N as a (n, d, N)-code. Denote by $\mathrm{wt}(\boldsymbol{x})$ the Hamming weight of vector $\boldsymbol{x}$ over E. For a (binary) code C denote by $\langle C \rangle$ the linear envelope of words of C over F_2. The dimension of space $\langle C \rangle$ is called the *rank* of C over F_2 and is denoted $\mathrm{rank}(C)$.

Denote by (n, w, d, N) a binary constant weight code C of length n, with weight of all codewords w, with minimum distance d and cardinality N. Let $J = \{1, 2, \ldots, n\}$ be the coordinate set of E^n. For a vector $\boldsymbol{v} = (v_1, ..., v_n) \in E^n$ denote by $\mathrm{supp}(\boldsymbol{v})$ its support:

$$\mathrm{supp}(\boldsymbol{v}) = \{i : \; v_i \neq 0\}.$$

For any set $X \subseteq E^n$ define its support $\mathrm{supp}(X)$, as a set

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

For any (n, d, N)-code (linear, nonlinear, or constant weight) denote by $C^{\perp}$ its dual code:

$$C^{\perp} \; = \; \{\boldsymbol{v} \in F_2^n : \; (\boldsymbol{v} \cdot \boldsymbol{c}) = 0, \; \forall \; \boldsymbol{c} \in C\},$$

where $(\boldsymbol{v} \cdot \boldsymbol{c})$ is the inner product in F_2^n. Clearly $C^{\perp}$ is a linear $[n, n-k, d^{\perp}]$-code with some minimum distance $d^{\perp}$, where $k = \text{rank}(C)$.

For arbitrary sets $X \subset E^n$ and $Y \subset E^m$, define

$$X \times Y \; = \; \{(\boldsymbol{x} \,|\, \boldsymbol{y}) \; : \; \boldsymbol{x} \in X, \; \boldsymbol{y} \in Y\} \subset E^{n+m}.$$

A binary incidence matrix of a Steiner system $S(v, k, k-1)$ is a constant weight $(v, k, 4, N_{v,k})$-code C of cardinality

$$N_{v,k} = \frac{v(v-1)\cdots(v-k+2)}{k(k-1)\cdots 2}.$$

In our notation the connection between the system (X, B) and the code C is:

$$B = \{\mathrm{supp}(\boldsymbol{v}) \subset J : \ \boldsymbol{v} \in C\}.$$

Here the Steiner system $S(v, k, k-1)$ is identified with the constant weight $(v, k, 4, N_{v,k})$-code, which uniquely defines this system.

3. Components of $S(v,k,k-1)$. For any set $X \subset E^n$ of vectors of weight $l < n$, define by $D(X) \subset E^n$ the set of all vectors of weight $l-1$, which are covered by vectors from X. Clearly for two disjoint sets $X \subset E^n$ and $Y \subset E^n$

$$D\,(X \ \cup \ Y) = D(X) \ \cup \ D(Y).$$

If π is any permutation, then $D(\pi(X)) = \pi(D(X))$. Then for any two arbitrary sets $X \subset E^n$ and $Y \subset E^m$, we have

$$\begin{aligned} D(X \times Y) &= (D(X) \times Y) \ \cup \ (X \times D(Y)) \\ &= D(X) \times Y \ \cup \ X \times D(Y). \quad (1) \end{aligned}$$

Definition 1 . *Let $K = K(n,k,N) \subset E^n$ be a set of vectors of weight k and cardinality N, with minimum distance $d \geq 4$. Call K a component, if there exists another set $L \subset E^n$, such that*

$$D(K) \ = \ D(L), \ K \cap L = \varnothing.$$

Theorem 1 (*Component structure*). *Let $K \subset E^n$ be some component with words of weight k, $\pi = (1 \ldots r)$ be the cyclic permutation of the first r positions. Let K contain the subset*

$$\bigcup_{i=1}^{l} \boldsymbol{x}_i \times Y(\boldsymbol{x}_i),$$

for some $l > 0$, i.e. words of type

$$(\boldsymbol{x}_i | \boldsymbol{y}) \in E^r \times E^{n-r}$$

with weight $\mathrm{wt}(\boldsymbol{x}_i)$ equal to maximum value, $i = 1, \ldots, l$. Let

$$X = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_l\} \subset E^r.$$

Then:

1). *The set X, under action of π is partitioned into orbits, with length larger 1, which divides r.*

2). *If $\boldsymbol{x}' \in \mathrm{Orb}(\boldsymbol{x})$, then $D(Y(\boldsymbol{x})) = D(Y(\boldsymbol{x}'))$.*

4. Two recursive constructions.

Set

$$\boldsymbol{e}_1 = (10\ldots0), \boldsymbol{e}_2 = (01\ldots0), \ldots, \boldsymbol{e}_r = (00\ldots1),$$

and let π be a cyclic permutation $\pi = (1\ldots r)$ (which acts on the first r coordinates).

Theorem 2 (*Construction I*) *Let*

$$K_1 = K(n, k-1, , N), \ldots, K_r = K(n, k-1, N)$$

be r mutually disjoint components of order n cardinality N of words of weight $k-1$. Then the set L, where

$$L = \bigcup_{i=1}^{r} \boldsymbol{e}_i \times K_i = \bigcup_{i=1}^{r} \{(\boldsymbol{e}_i \,|\, \boldsymbol{x}) : \ \boldsymbol{x} \in K_i\},$$

is a component $K(n+r, k, rN)$ of order $n+r$ cardinality $r \cdot N$ of weight k, and

$$D(L) = D(\pi(L)).$$

Theorem 3 (*Construction II*). *Let*

$$Y_1 = K(n, k-2, N), \quad Y_2 = K(n, k-2, N)$$

be two disjoint components of order n *cardinality* N *of weight* $k-2$. *Let* r *be even. Let* X_1, X_2 *be two different parallel classes (cardinality* $r/2$*) of vectors of length* r *of weight* 2, *such that*

$$X_1 \cap X_2 = \emptyset, \quad \pi(X_1) = X_2 \text{ and } \pi(X_2) = X_1,$$

where $\pi \in \mathcal{S}_r$. *Then the set*

$$L = X_1 \times Y_1 \cup X_2 \times Y_2,$$

is a component $K(n+r, k, rN)$ *of order* $n+r$ *cardinality* $r \cdot N$ *of weight* k, *i.e.*

$$D(L) = D(\pi(L)).$$

4. Components of Steiner systems $S(v,3,2)$ and $S(v,4,3)$.

Definition 2 . *Let M_1 be a component of even order n such that*

$$M_2 = M_1 + \boldsymbol{e}, \quad \textit{where} \;\; \mathrm{wt}(\boldsymbol{e}) = 2.$$

Let $(\boldsymbol{e} \cdot \boldsymbol{x}) = 1$ for every $\boldsymbol{x} \in M_1$. Say that the components M_1 and M_2 are normal, if for any vector $\boldsymbol{u} \in M_1^{\perp}$, such that

$$(\boldsymbol{e} \cdot \boldsymbol{u}) = 1,$$

the following condition is satisfied:

$$\mathrm{wt}(\boldsymbol{u}) = n/2.$$

Direct application of Theorem 2 with the following initial parallel classes of vectors of weight 2:

$$\begin{array}{c} (1\,1\,0\,0\,\ldots\,0\,0\,0\,0) \\ (0\,0\,1\,1\,\ldots\,0\,0\,0\,0) \\ \ldots\ldots\ldots \\ (0\,0\,0\,0\,\ldots\,1\,1\,0\,0) \\ (0\,0\,0\,0\,\ldots\,0\,0\,1\,1) \end{array}, \qquad \begin{array}{c} (1\,0\,\ldots 0\,0\,1\,0\,\ldots\,0\,0) \\ (0\,1\,\ldots 0\,0\,0\,1\,\ldots\,0\,0) \\ \ldots\ldots\ldots\ldots \\ (0\,0\,\ldots 1\,0\,0\,0\,\ldots\,1\,0) \\ (0\,0\,\ldots 0\,1\,0\,0\,\ldots\,0\,1) \end{array},$$

covering all vectors of weight 1, gives the following components $K_1^{(i)}$ and $K_2^{(i)}$, $i = 1, 2, 3$ for Steiner triple systems $S(v, 3, 2)$:

$$K_1^{(1)} = \begin{array}{c} (1\,0\,|\,1\,1\,0\,0) \\ (1\,0\,|\,0\,0\,1\,1) \\ (0\,1\,|\,1\,0\,1\,0) \\ (0\,1\,|\,0\,1\,0\,1) \end{array} \quad K_2^{(1)} = \begin{array}{c} (0\,1\,|\,1\,1\,0\,0) \\ (0\,1\,|\,0\,0\,1\,1) \\ (1\,0\,|\,1\,0\,1\,0) \\ (1\,0\,|\,0\,1\,0\,1) \end{array}$$

$$K_1^{(2)} = \begin{array}{c} (1\,0\,|\,1\,1\,0\,0\,0\,0) \\ (1\,0\,|\,0\,0\,1\,1\,0\,0) \\ (1\,0\,|\,0\,0\,0\,0\,1\,1) \\ (0\,1\,|\,1\,0\,0\,1\,0\,0) \\ (0\,1\,|\,0\,1\,0\,0\,1\,0) \\ (0\,1\,|\,0\,0\,1\,0\,0\,1) \end{array} \quad K_2^{(2)} = \begin{array}{c} (0\,1\,|\,1\,1\,0\,0\,0\,0) \\ (0\,1\,|\,0\,0\,1\,1\,0\,0) \\ (0\,1\,|\,0\,0\,0\,0\,1\,1) \\ (1\,0\,|\,1\,0\,0\,1\,0\,0) \\ (1\,0\,|\,0\,1\,0\,0\,1\,0) \\ (1\,0\,|\,0\,0\,1\,0\,0\,1) \end{array}$$

and

$$K_1^{(3)} = \begin{array}{c} (1\,0\,|\,1\,1\,0\,0\,0\,0\,0\,0) \\ (1\,0\,|\,0\,0\,1\,1\,0\,0\,0\,0) \\ (1\,0\,|\,0\,0\,0\,0\,1\,1\,0\,0) \\ (1\,0\,|\,0\,0\,0\,0\,0\,0\,1\,1) \\ (0\,1\,|\,1\,0\,0\,0\,1\,0\,0\,0) \\ (0\,1\,|\,0\,1\,0\,0\,0\,1\,0\,0) \\ (0\,1\,|\,0\,0\,1\,0\,0\,0\,1\,0) \\ (0\,1\,|\,0\,0\,0\,1\,0\,0\,0\,1) \end{array}$$

$$K_2^{(3)} = \begin{array}{c} (0\,1\,|\,1\,1\,0\,0\,0\,0\,0\,0) \\ (0\,1\,|\,0\,0\,1\,1\,0\,0\,0\,0) \\ (0\,1\,|\,0\,0\,0\,0\,1\,1\,0\,0) \\ (0\,1\,|\,0\,0\,0\,0\,0\,0\,1\,1) \\ (1\,0\,|\,1\,0\,0\,0\,1\,0\,0\,0) \\ (1\,0\,|\,0\,1\,0\,0\,0\,1\,0\,0) \\ (1\,0\,|\,0\,0\,1\,0\,0\,0\,1\,0) \\ (1\,0\,|\,0\,0\,0\,1\,0\,0\,0\,1) \end{array} .$$

The components $K_1^{(1)}$ and $K_2^{(1)}$ are well known and were considered under the name of Pasch configurations by Fisher [F]. These components are contained in 79 out of all 80 non-isomorphic systems $S(15, 3, 2)$ [CCW]; the system, which does not contain such component, has number 80 [F]. Furthermore, the distribution of these components on coordinates is different for all 80 non-isomorphic systems $S(15, 3, 2)$ [F].

It is easy to see that the component $K_1^{(1)}$ can be switched by changing every vector $\boldsymbol{x} \in K_1^{(1)}$ by the complementary vector $\bar{\boldsymbol{x}}$, preserving the property of S to be a Steiner system. Under the action of this switching all 79 systems $S(15, 3, 2)$, which contain a Pasch configuration, form a single orbit [G]. Many papers were devoted to such switching of Steiner systems $S(v, 3, 2)$ (see [GGM] and references there).

It is interesting that components $K_1^{(2)}$ and $K_2^{(2)}$ are also contained almost in all systems $S(15,3,2)$, namely, in systems with numbers $11, 12$,$19, 20, \ldots 80$. These components $K_1^{(2)}$ and $K_2^{(2)}$ are also contained in systems $S(19,3,2)$.

Remark that the components $K_1^{(1)}$, $K_2^{(1)}$ and $K_1^{(3)}$, $K_2^{(3)}$ are normal.

Theorem 4 . *Let S be a Steiner system $S(v,3,2)$. Assume that S contains a normal component K_1 of even order n, $6 \leq n \leq (v+1)/2$, and the vector $\boldsymbol{e}$ of length v and weight 2 transforms K_1 to K_2, i.e. $K_2 = K_1 + \boldsymbol{e}$. Let*

$$S^* \;=\; (S \setminus K_1) \cup K_2$$

be a new system $S(v,3,2)$. If the initial system S has a rank $r \leq v-1$ over F_2, then the rank r^* of new system S^* increases by 1, i.e. $r^* = r+1$, if and only if the vector $\boldsymbol{e}$ does not belong to the linear envelope $\langle S \rangle$.

The following two normal components $M_1^{(1)}$ and $M_2^{(1)}$ of minimal order 8 and weight 4, obtained by Theorem 2 from components $K_1^{(1)}$ and $K_2^{(1)}$, were introduced in [ZZ]:

$$M_1^{(1)} = \begin{array}{c} (1\,0\,|\,1\,0\,|\,1\,1\,0\,0) \\ (1\,0\,|\,1\,0\,|\,0\,0\,1\,1) \\ (1\,0\,|\,0\,1\,|\,1\,0\,1\,0) \\ (1\,0\,|\,0\,1\,|\,0\,1\,0\,1) \\ (0\,1\,|\,0\,1\,|\,1\,1\,0\,0) \\ (0\,1\,|\,0\,1\,|\,0\,0\,1\,1) \\ (0\,1\,|\,1\,0\,|\,1\,0\,1\,0) \\ (0\,1\,|\,1\,0\,|\,0\,1\,0\,1) \end{array}$$

$$M_2^{(1)} = \begin{array}{c} (0\,1\,|\,1\,0\,|\,1\,1\,0\,0) \\ (0\,1\,|\,1\,0\,|\,0\,0\,1\,1) \\ (0\,1\,|\,0\,1\,|\,1\,0\,1\,0) \\ (0\,1\,|\,0\,1\,|\,0\,1\,0\,1) \\ (1\,0\,|\,0\,1\,|\,1\,1\,0\,0) \\ (1\,0\,|\,0\,1\,|\,0\,0\,1\,1) \\ (1\,0\,|\,1\,0\,|\,1\,0\,1\,0) \\ (1\,0\,|\,1\,0\,|\,0\,1\,0\,1) \end{array} .$$

The component, given above, occurs to be very useful for Steiner systems $S(16,4,3)$ [ZZ]. For example, all 708103 non-isomorphic systems $S(16,4,3)$ of rank 14 contain at least 295488 different components $M_1^{(1)}$. All possible different switching of these components give at least 314198 non-isomorphic systems $S(16,4,3)$ of rank 15 over F_2.

Theorem 5 *Let S be a Steiner system $S(v,4,3)$ of order $v \geq 16$. Assume that S contains a normal component M_1 of order n, where n is a multiple of 8 and $8 \leq n \leq v/2$, and the vector $\boldsymbol{e}$ of length v and weight 2 transforms M_1 to M_2, i.e. $M_2 = M_1 + \boldsymbol{e}$. Let*

$$S^* = (S \setminus M_1^{(1)}) \cup M_2^{(1)},$$

be a new Steiner system $S(v,4,3)$. If the initial system S has the rank $r \leq v-2$ over F_2, then the rank r^* of the new system S^* increases by 1, i.e. $r^* = r+1$, if and only if the vector $\boldsymbol{e}$ does not belong to the linear envelope $\langle S \rangle$.

If now apply Theorem 2 to components $K_1^{(2)}$ and $K_2^{(2)}$, then we obtain the following two components $M_1^{(2)}$ and $M_2^{(2)}$ of order 10 and cardinality 12:

$$M_1^{(2)} = \begin{array}{c} (1\,0\,|\,1\,0\,|\,1\,1\,0\,0\,0\,0) \\ (1\,0\,|\,1\,0\,|\,0\,0\,1\,1\,0\,0) \\ (1\,0\,|\,1\,0\,|\,0\,0\,0\,0\,1\,1) \\ (1\,0\,|\,0\,1\,|\,1\,0\,0\,1\,0\,0) \\ (1\,0\,|\,0\,1\,|\,0\,1\,0\,0\,1\,0) \\ (1\,0\,|\,0\,1\,|\,0\,0\,1\,0\,0\,1) \\ (0\,1\,|\,0\,1\,|\,1\,1\,0\,0\,0\,0) \\ (0\,1\,|\,0\,1\,|\,0\,0\,1\,1\,0\,0) \\ (0\,1\,|\,0\,1\,|\,0\,0\,0\,0\,1\,1) \\ (0\,1\,|\,1\,0\,|\,1\,0\,0\,1\,0\,0) \\ (0\,1\,|\,1\,0\,|\,0\,1\,0\,0\,1\,0) \\ (0\,1\,|\,1\,0\,|\,0\,0\,1\,0\,0\,1) \end{array},$$

$$M_2^{(2)} = \begin{array}{c}
(0\,1\,|\,1\,0\,|\,1\,1\,0\,0\,0\,0) \\
(0\,1\,|\,1\,0\,|\,0\,0\,1\,1\,0\,0) \\
(0\,1\,|\,1\,0\,|\,0\,0\,0\,0\,1\,1) \\
(0\,1\,|\,0\,1\,|\,1\,0\,0\,1\,0\,0) \\
(0\,1\,|\,0\,1\,|\,0\,1\,0\,0\,1\,0) \\
(0\,1\,|\,0\,1\,|\,0\,0\,1\,0\,0\,1) \\
(1\,0\,|\,0\,1\,|\,1\,1\,0\,0\,0\,0) \\
(1\,0\,|\,0\,1\,|\,0\,0\,1\,1\,0\,0) \\
(1\,0\,|\,0\,1\,|\,0\,0\,0\,0\,1\,1) \\
(1\,0\,|\,1\,0\,|\,1\,0\,0\,1\,0\,0) \\
(1\,0\,|\,1\,0\,|\,0\,1\,0\,0\,1\,0) \\
(1\,0\,|\,1\,0\,|\,0\,0\,1\,0\,0\,1)
\end{array}.$$

It is interesting that these components $M_1^{(2)}$ and $M_2^{(2)}$ are also contained in Steiner systems $S(16, 4, 3)$. In particular, about 1800 systems $S(16, 4, 3)$ of rank 14 contain the component $M_1^{(2)}$. The next components $M_1^{(3)}$ and $M_2^{(3)}$ of order 12 and cardinality 16, which are built by Theorem 2, are also contained in systems $S(16, 4, 3)$ of ranks 13 and 14.

6. Ranks of Steiner systems $S(v, k, k-1)$ for $k \geq 5$. The same approach, which was used for proofs of two previous theorems, permits to make conclusion on the value of rank of any Steiner systems $S(v, k, k-1)$ for values $k \geq 5$.

Theorem 6 . *Let S be a Steiner system $S(v, k, k-1)$ and let $k \geq 5$. Then this system has a full rank over F_2. Namely, if r is a rank of this system over F_2. Then:*

$$r = \begin{cases} v-1, & \textit{if} \quad k \geq 6 \quad \textit{even}, \\ v, & \textit{if} \quad k \geq 5 \quad \textit{odd}. \end{cases}$$

Note that this result has been obtained by Dehon [D1, D2]. Our proof seems to be simpler.

We thank Faina Solov'eva who pointed out papers [F] and [GGM].

[ZZ] *Zinoviev V.A., Zinoviev D.V.* On one transformation of Steiner systems $S(v, 4, 3)$// Probl. Inform. Transm., 2009, v. 45. n. 4, 26-42.

[F] *Fisher R.A.* An examination of the different possible solutions of a problem in incomplete blocks// Ann. Eugenics, 1940, v. 10, 52 - 75.

[CCW] *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, 197-199.

[G] *Gibbons P.D.* Computing Techniques for the Construction and Analysis of Block Designs// Ph.D. Dissertation, Univ. Toronto, Canada, 1976.

[GGM] *Grannel M.J., Griggs T.S., Murphy J.P.* Equivalence classes of Steiner triple systems// Congressus Numerantium, 1992. v. 86, 19-25.

[D1] *Dehon M.* Ranks of Incidence Matrices of t-Designs $S_\lambda(t, t+1, v)$// Europ. J. Comb. 1980. v. 1. 97-100.

[D2] *Dehon M.* Designs et hyperplans// J. Combinatorial Theory (A), 1977. v. 23. 264 - 274.