Steiner triple systems $S(2^m - 1, 3, 2)$ of 2-rank $r \leq 2^m - m + 1$: construction and properties

D. V. Zinoviev dzinov@iitp.ru
V. A. Zinoviev zinov@iitp.ru
A.A. Kharkevich Institute for Problems of Information Transmission, Moscow, Russia

Abstract. Steiner systems $S(2^m - 1, 3, 2)$ of rank $2^m - m + 1$ over the field $\mathbb{F}_2$ are considered. The number of all such different systems is obtained. It is shown that all Steiner triple systems of rank $r \leq 2^m - m + 1$ are derived and Hamming.

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 $S(v, 3, 2)$ is called a Steiner triple system (briefly STS($v$)), and a system $S(v, 4, 3)$ is called a Steiner quadruple system (briefly SQS($v$)) (see [1-3] for more information).

Tonchev [4,5] enumerated all different Steiner triple systems STS($v$) and quadruple systems SQS($v+1$) of order $v = 2^m - 1$ and $v+1 = 2^m$, respectively, both with 2-rank (i.e. rank over the field $\mathbb{F}_2$), equal to $2^m - m$. In the previous paper [6] the authors enumerated all different Steiner quadruple systems SQS($v$) of order $v = 2^m$ and 2-rank $r \leq v - m + 1$.

The goal of the present work is to enumerate all different Steiner triple systems STS($v$) of order $v = 2^m - 1$ of the next rank $r = 2^m - m + 1$ over $\mathbb{F}_2$. It turns out that all such systems are derived, i.e. can be embedded into Steiner quadruple systems SQS($v+1$). Moreover, all such systems are Hamming, i.e. any such system can be embedded into a binary nonlinear perfect code of length $2^m - 1$.

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 $\text{wt}(x)$ the Hamming weight of vector $x$ over $E_q$, and by $d(x, y)$ the Hamming distance between the vectors $x, y \in E_q^n$. 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 rank$(C)$. Denote by $(n, w, d, N)$ a constant weight $(n, d, N)$-code, whose codewords have the same fixed weight $w$.

1This work has been partially supported by the Russian fund of fundamental researches (under the project No. 12 - 01 - 00905).
Let \( J = \{1, 2, \ldots, n\} \) be the set of coordinate positions \( E_q^n \). Denote by 
\[ \text{supp}(\mathbf{v}) \subseteq J \]
the support of a vector \( \mathbf{v} = (v_1, \ldots, v_n) \in E^n \), 
\( \text{supp}(\mathbf{v}) = \{i : v_i \neq 0\} \). For an arbitrary set \( X \subseteq E^n \) define
\[ \text{supp}(X) = \bigcup_{\mathbf{x} \in X} \text{supp}(\mathbf{x}). \]

A binary \((n, d, N)\)-code \( C \), which is a linear \( k \)-dimensional space over \( \mathbb{F}_2 \), is denoted as \([n, k, d]_2\)-code. Let \( (\mathbf{x} \cdot \mathbf{y}) = x_1y_1 + \cdots + x_ny_n \) be the scalar product over \( \mathbb{F}_2 \) of the binary vectors \( \mathbf{x} = (x_1, \ldots, x_n) \) and \( \mathbf{y} = (y_1, \ldots, y_n) \). For any (linear, non-linear or constant weight) code \( C \) of length \( n \) let \( C^\perp \) be its dual code: \( C^\perp = \{\mathbf{v} \in \mathbb{F}_2^n : (\mathbf{v} \cdot \mathbf{c}) = 0, \ \forall \mathbf{c} \in C\} \). It is clear that \( C^\perp \) is a \([n, n-k, d^\perp]_2\)-code with a minimal distance \( d^\perp \), and where \( k = \text{rank}(C) \).

We need the following two classes of the quaternary MDS codes: a \((3, 2, 4^2)\)_4-code, denoted by \( L \), and a \((4, 2, 4^3)\)_4-code, denoted by \( K \). The number \( \Gamma_L \) (respectively, \( \Gamma_K \)) of different codes \( L \) (respectively \( K \)) is \( \Gamma_L = (24)^2 \) (respectively, \( \Gamma_K = 55296 \) [4]).

Define the mapping \( \varphi \) of \( E_q^n \) into \( E^{3n} \) setting for \( \mathbf{c} = (c_1, \ldots, c_n) \): 
\[ \varphi(\mathbf{c}) = (\varphi(c_1), \ldots, \varphi(c_n)) \text{, where } \varphi(0) = (1 \ 0 \ 0 \ 0), \ \varphi(1) = (0 \ 1 \ 0 \ 0), \ \varphi(2) = (0 \ 0 \ 1 \ 0), \ \varphi(3) = (0 \ 0 \ 0 \ 1). \]

For a given code \((3, 2, 16)\)_4-code \( L \), define the constant weight \((12, 3, 4, 16)\)-code \( C(L) \):
\[ C(L) = \{\varphi(\mathbf{c}) : \mathbf{c} \in L\}. \]
Every codeword \( \mathbf{c} \) of the code \( C(L) \), is split into blocks of length four \( \mathbf{c} = (c_1, c_2, c_3) \), so that \( \text{wt}(c_i) = 1 \) for \( i = 1, 2, 3 \). We say that \( C(L) \) has the block structure. For a code \( C(L) \) and a vector \( \mathbf{x} = (x_1, \ldots, x_u) \) of weight 3 with support \( \text{supp}(\mathbf{x}) = \{i_1, i_2, i_3\} \) define the following code 
\[ C(L; \mathbf{x}) = C(L; i_1, i_2, i_3) \]
of length \( 4u \) with block structure:
\[ C(L; \mathbf{x}) = \{(c_1, \ldots, c_u) : (c_{i_1}, c_{i_2}, c_{i_3}) \in C(L), \text{ and } c_j = (0000), \text{ if } j \neq i_1, i_2, i_3\}. \]
For a given set \( X \) of vectors of length \( u \) weight 3, define
\[ C(L; X) = \{C(L; \mathbf{x}) : \mathbf{x} \in X\}. \]
Define the mapping \( \psi(\cdot) \) from \( E^u \) into \( E^{4^u} \), so that for every vector \( \mathbf{x} = (x_1, x_2, \ldots, x_u) \) we have:
\[ \psi(\mathbf{x}) = (x_1x_1x_1x_1, x_2x_2x_2x_2, \ldots, x_ux_ux_ux_u). \]
Define the following three trivial constant weight \((4, 2, 4, 2)\)-codes \( V(i) \):
\[ V(1) = \{(1100), (0011)\}, \ V(2) = \{(1010), (0101)\}, \ V(3) = \{(1001), (0110)\}. \]
2 Main results

Suppose \( S_v = S(v, 3, 2) \) is a Steiner triple system of order \( v = 2^m - 1 \) and of 2-rank \( r \leq 2^m - m + 1 \). That means that the dual code \( S_v^\perp \) contains a subcode \([v, m - 2, d]\), denoted by \( A_m \) with minimum distance \( d^\perp = (v + 1)/2 = 2^{m-1} \) \cite{6}. More precisely, \( A_m \) contains the non-zero words of the same weight \( 2^{m-1} \), i.e. the code is a subcode of a well known linear equidistant Hadamard code and can be generated by the following matrix:

\[
G(A_m) = \begin{bmatrix}
1111 & 1111 & 1111 & 1111 & \ldots & 0000 & 0000 & 0000 & 0000 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
1111 & 1111 & 0000 & 0000 & \ldots & 1111 & 1111 & 0000 & 0000 \\
1111 & 0000 & 1111 & 1111 & \ldots & 1111 & 0000 & 1111 & 1111 \\
\end{bmatrix} . \tag{1}
\]

Let \( J(v) = \{1, \ldots, v\} \) be the coordinate set of a system \( S_v \) and assume that the non-zero coordinate positions of the code \( A_m \) are the first \( v - 3 \) positions of \( S_v \). Define the following subsets \( J_i \) of \( J(v) \), which correspond to the block structures of the defined constant weight codes \( C(L; x) \) and \( C(K; y) \):

\[
J_i = \{4i-3, 4i-2, 4i-1, 4i\}, \quad i = 1, 2, \ldots, (v-3)/4, \quad J_{(v+1)/4} = \{v-2, v-1, v\}.
\]

Since the codewords of \( A_m \) are orthogonal to our system \( S_v \), its words can be divided naturally into three subsets \( S^{(1,1)}, S^{(2,1)} \) and \( S^{(3)} \):

\[
\begin{itemize}
\item \( S^{(1,1)} = \{ c \in S : \text{supp}(c) = \{j_1, j_2, j_3\}, j_s \in J_s, \text{ where } i_1 \neq i_2 \neq i_3 \neq i_1 \} \).
\item \( S^{(2,1)} = \{ c \in S : \text{supp}(c) = \{j_1, j_2, j_3\}, j_1, j_2 \in J_i, \text{ and } j_3 \in J_{(v+1)/4} \} \).
\item \( S^{(3)} = \{ c : \text{supp}(c) = J_{(v+1)/4} \} \).
\end{itemize}
\]

It is convenient to split the set \( S^{(2,1)} \) into three subsets \( S_j^{(2,1)} \), where the index \( j, j \in J_{(v+1)/4} \), is fixed:

\[
S_j^{(2,1)} = \{ c \in S^{(2,1)} : j \in \text{supp}(c) \}.
\]

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

\[
\begin{itemize}
\item The set \( S^{(1,1)} \) is a set of \((v - 3, 3, 4, 16)\)-codes \( C = C(j_1, j_2, j_3) \) of type \((1, 1, 1)\), where the set of triples of indices \( \{(j_1, j_2, j_3)\} \), \( j_1, j_2, j_3 \in J(u) = \{1, 2, \ldots, u\} \), is a Steiner triple system \( S_u = S(u, 3, 2) \) on coordinate set \( J(u) \) of order \( u = (v-3)/4 = 2^{m-2} - 1 \).
\end{itemize}
\]
• The 2-rank of a Steiner triple system $S_u$ is $r_u = u - m + 2$.

• Every code $C = C(j_1, j_2, j_3)$ induce a (4-ary) $(3, 2, 16)_4$-code $L = L(C) = \varphi^{-1}(C)$.

• For a fixed $j \in J_{(v+1)/4}$, the set obtained from $S_{v}^{(2,1)}$ removing $j$, is the set of codes $V(k_1), V(k_2), \ldots, V(k_u)$, where $\text{supp}(V(k_i)) = J_i$ and the indices $k_1, k_2, \ldots, k_u$ take their values in the set $\{1, 2, 3\}$.

• For the three sets $S_{v-2}^{(2,1)}, S_{v-1}^{(2,1)}$ and $S_v^{(2,1)}$ the corresponding three sets of indices $k_1, k_2, \ldots, k_u$, $k'_1, k'_2, \ldots, k'_u$ and $k''_1, k''_2, \ldots, k''_u$ are such that $\{k_j, k'_j, k''_j\} = \{1, 2, 3\}$ for every $j = 1, \ldots, u$.

• The set $S^{(3)}$ is made of one codeword $c$, with support $\text{supp}(c) = J_{(v+1)/4}$.

The structure of the Steiner triple systems $STS(v)$ of order $v = 4u + 3$ and 2-rank $v + m + 2$ that we described above, induce the following recursive construction of $STS(v)$ of order $v = 4u + 3$ for a given $STS(u)$ of an arbitrary order $u$ (i.e. $u \equiv 1$ or $3 \pmod{6}$).

Construction I. Let $S_u = S(u, 3, 2)$ be a Steiner system of rank $r_u$, whose words $c^{(s)}$ are ordered by a fixed enumeration $s = 1, 2, \ldots, k$, where $k = u(u - 1)/6$. Suppose, we have an arbitrary family of 4-ary codes $L_1, L_2, \ldots, L_k$ with parameters $(3, 2, 16)_4$ and with the possible repetitions. Let $V(1), V(2)$ and $V(3)$ be three binary constant weight $(4, 2, 4, 2)$-codes. Choose three arbitrary vectors $z_i = (z_{i,1}, \ldots, z_{i,u}), i = 1, 2, 3$, of length $u$ over the alphabet $\{1, 2, 3\}$ so that, for any $j$, $j = 1, \ldots, u$, the condition $\{z_{1,j}, z_{2,j}, z_{3,j}\} = \{1, 2, 3\}$ is satisfied. Let $J(u)$ be the coordinate set of the system $S_u$ and define the new coordinate set $J(v)$ of size $v = 4u + 3$, obtained from $J(u)$ as follows: every index $j \in J(u)$ is associated with the set $J_j$, of four elements, namely $J_j = \{4j - 3, 4j - 2, 4j - 1, 4j\}$. Also define the set $J_{u+1}$ of size three: $J_{u+1} = \{4u + 1, 4u + 2, 4u + 3\} = \{v - 2, v - 1, v\}$. Define the coordinate set $J(v)$ as the union:

$J(v) = J_1 \cup \cdots \cup J_u \cup J_{u+1}$.

Every word $c^{(s)}$ of $S_u$ with support $\text{supp}(c^{(s)}) = \{j_1, j_2, j_3\}$ and a code $L_s$ is associated the constant weight code $C(L_s; c^{(s)}) = C(L_s; j_1, j_2, j_3)$, based on this word $c^{(s)}$ and the code $L_s$, whose support belongs to the set $J(v)$:

$\text{supp}(C(L_s; j_1, j_2, j_3)) = J_{j_1} \cup J_{j_2} \cup J_{j_3}$.

Define the following three sets:

$S^{(1,1,1)} = \bigcup_{s=1}^k C(L_s; j_1, j_2, j_3), \quad \text{supp}(c^{(s)}) = \{j_1, j_2, j_3\}$,
i.e. the supports of all words of $C(L; j_1, j_2, j_3)$ belong to the set $J_{j_1} \cup J_{j_2} \cup J_{j_3}$:

$$S^{(2,1)} = S^{(2,1)}_{v-2} \cup S^{(2,1)}_{v-1} \cup S^{(2,1)}_v,$$

where

$$S^{(2,1)}_{v+1-t} = \bigcup_{t=1}^{u} \bigcup_{w \in V(z_{i,t})} \{ \mathbf{a} : \text{supp}(\mathbf{a}) = \text{supp}(\mathbf{w}) \cup \{v + 1 - i\}, \; i = 1, 2, 3\},$$

i.e. the supports of all vectors $\mathbf{a}$ contain a $(v + 1 - i)$-th coordinate position, and, for a given $t$, another two non-zero positions belong to $J_t$:

$$S^{(3)} = \{ \mathbf{c} : \text{supp}(\mathbf{c}) = \{v - 2, v - 1, v\}\}.$$

**Theorem 1.** Let $S_u = S(u, 3, 2)$ be a Steiner system of rank $r_u$ and $c^{(s)}$, $s = 1, 2, \ldots, k$ be the words of this system, where $k = u(u - 1)/6$. Let $S^{(1,1,1)}$, $S^{(2,1)}$ and $S^{(3)}$ be the sets, obtained by construction $I$, based on the families of $(3, 2, 16)_4$-codes $L_1, L_2, \ldots, L_k$ and the constant weight $(4, 2, 4, 2)$-codes $V(1)$, $V(2)$ and $V(3)$. Set

$$S = S^{(1,1,1)} \cup S^{(2,1)} \cup S^{(3)}.$$

Then, for any choice of the codes $L_1, L_2, \ldots, L_k$ and any triple of vectors $z_i = (z_{i,1}, \ldots, z_{i,u})$, $i = 1, 2, 3$, of length $u$ over the alphabet $\{1, 2, 3\}$ so that, $\{z_{1,j}, z_{2,j}, z_{3,j}\} = \{1, 2, 3\}$ for $j = 1, \ldots, u$, the set $S$ is the Steiner triple system $S_v = S(v, 3, 2)$ of order $v = 4u + 3$ with 2-rank $r_v$, such that

$$v - (u - r_u) - 2 \leq r_v \leq v - (u - r_u).$$

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

**Theorem 2.** Suppose $S_v = S(v, 3, 2)$ is a Steiner system of order $v = 2^m - 1 = 4u + 3$. Suppose that its 2-rank satisfies $r_v \leq v - m + 2$. Then this system $S_v$ is obtained from the Steiner triple system $S_u = S(u, 3, 2)$ of order $u = 2^{m-2} - 1$ on applying the construction $I$, described above.

Let $B_m$ be a $[2^{m-2} - 1, m - 2, 2^{m-2}]$-code, obtained via the map $\psi^{-1}$ from the code, which is, in turn, obtained from $A_m$ whose last three zero coordinate positions are removed.

**Theorem 3.** The following is true:
The number $M_v$ of all different Steiner triple systems $S(v, 3, 2)$ of order $v = 2^m - 1 = 4u + 3 \geq 15$, whose 2-rank $r_v \leq v - m + 2$, and whose dual code $A_m$ is given by (1), is equal to

$$M_v = M_u \cdot (2^6 \cdot 3^2)^k \times (6)^u, \quad k = u(u - 1)/6,$$

where $M_u$ is the number of different Steiner triple systems $S_u$ of order $u = 2^{m-2} - 1$, of 2-rank $r_u \leq u - m + 4$, whose dual code is $B_m$.

For large $m \geq 7$, the number $M_v$ of different Steiner triple systems $S(v, 3, 2)$ of order $v = 2^m - 1$ and of 2-rank $r_v \leq v - m + 2$, whose dual code $A_m$ is given by (1), can be bounded from below as

$$M_v \geq 2^{v^2 - c}, \quad c > (3 + \log_2(3)) \frac{1}{8} \cdot 1.0207004 > 0.5849841. \quad (2)$$

A Steiner triple system $S(v, 3, 2)$ is called derived (respectively, Hamming), if it can be embedded into a quadruple system $S(v+1, 4, 3)$ (respectively, into a binary non-linear perfect code of length $v$).

**Theorem 4.** Every Steiner triple system $S(v, 3, 2)$ of order $v = 2^m - 1$ and 2-rank $r_v \leq v - m + 2$ is derived and Hamming.

**References.**


[7]. Zinoviev V.A., Zinoviev D.V. On resolvability of Steiner systems $S(v = 2^m, 4, 3)$ of rank $r \leq v - m + 1$ over $F_2$// Problems of Information Transmission. 2007. V. 43. N° 1, P. 39 - 55.