The number of the non-full-rank Steiner triple systems

Minjia Shi*† Li Xu† Denis S. Krotov‡§

Abstract

The p-rank of a Steiner triple system B is the dimension of the linear span of the set of characteristic vectors of blocks of B, over $\mathrm{GF}(p)$. We derive a formula for the number of different Steiner triple systems of order v and given 2-rank $r_2 < v$ and the number of Steiner triple systems of order v and given 3-rank $r_3 < v-1$. We prove that there are no Steiner triple systems of 2-rank smaller than v and, at the same time, 3-rank smaller than $v-1$.

1. Introduction

A Steiner triple system $\mathrm{STS}(v)$ is a finite set S of cardinality v whose elements are called points, provided with a collection of 3-subsets called blocks such that every 2-subset of S is contained in one and only one block. We assume that $S = \{1, \ldots, v\}$ and do not distinguish a block b with its characteristic vectors, that is, the v-tuple of 0s and 1s having 1s in the coordinates numbered by the elements of b. E.g., $(0, 1, 0, 1, 1, 0, 0) = \{2, 4, 5\}$ $(v = 7)$. The dimension of the space over $\mathrm{GF}(p)$ spanned by the blocks (to be exact, by their characteristic vectors) of a Steiner triple system T is called the p-rank of T. As shown in [4], the p-rank of every $\mathrm{STS}(v)$ is v for all prime p except 2 and 3. The series of papers [1, 17, 13, 24, 25, 26, 23, 8, 6, 7] are devoted to the study of $\mathrm{STS}(v)$ of deficient 2- or 3-rank. In particular, in [17], [25], [23], there found formulas for the number of $\mathrm{STS}(2^m-1)$ of 2-rank 2^m-m, 2^m-m+1, 2^m-m+2, respectively. In a recent work [7], a formula for the number of STS dual to a fixed binary or ternary subspace was found.

In the current paper, we derive formulas for the number of $\mathrm{STS}(v)$ of arbitrary 2-rank smaller than v, see Theorem 4.6, or 3-rank smaller than $v-1$ (note that the 3-rank of STS cannot exceed $v-1$, as it is always orthogonal to the all-one vector $(1, 1, \ldots, 1)$ over $\mathrm{GF}(3)$), see Theorem 3.6. In particular, our result generalizes the formulas for 2-rank 2^m-m [17], 2^m-m+1 [25],MinGW32 and 2^m-m+2 [23], obtained before. The generalization is based on the Möbius transform, which makes possible to derive a common formula for different ranks and also to simplify some arguments. The formulas

*Key Laboratory of Intelligent Computing & Signal Processing, Ministry of Education, Anhui University No. 3 Feixi Road, Hefei Anhui Province 230039, P. R. China
†School of Mathematical Sciences, Anhui University, Anhui, 230601, P. R. China
‡Sobolev Institute of Mathematics, pr. Akademika Koptyuga 4, Novosibirsk 630090, Russia
§Novosibirsk State University, Pirogova 2, Novosibirsk 630090, Russia

are tight but conditional: they involve the numbers of objects of smaller order (Steiner triple systems, 1-factorizations of complete graph, and latin squares).

For partial cases where these numbers are known, we obtain explicit values. Namely, in addition to the results known before, we get the number of STS(3^k) of 3-rank $v-k$ and $v-k+1$, the number of STS($7\cdot 3^k$) of 3-rank $7\cdot 3^k-k-1$, and the number of STS($10\cdot 2^k-1$) of 2-rank $10\cdot 2^k-k-1$, for every k (Corollaries 3.7 and 4.7). In the other cases, our formulas can be combined with the asymptotic estimations of the number of Steiner triple systems [21, 10], 1-factorizations [3, 10, 22], and latin squares, see e.g. [18, Theorems 17.2, 17.3].

In the next section, we define necessary concepts and mention related facts. In Section 3, we describe the structure of STS(v) of 3-rank smaller than $v-1$ and of its dual space and derive a formula for the number of such systems. In Section 4, similar results are obtained for STS(v) of 2-rank smaller than v.

2. Definitions and notations

Orthogonality and duality. Two v-tuples $x=(x_1,\ldots,x_v)$ and $y=(y_1,\ldots,y_v)$ understood as vectors over GF(q) are said to be *orthogonal*, denoted $x\perp y$, if $x_1y_1+\ldots+x_vy_v=0$. Given a set B of vectors, the *dual space* $B^\perp$ is the set of all vectors orthogonal to each element of B. By $\langle B\rangle$, we denote the linear span of the vector set B.

To simplify the formulas, we will use the standard notation of q-factorial $[n]_q! = \prod_{s=1}^{n}\sum_{i=0}^{s-1}q^i$. Using this notation, the number $\prod_{t=1}^{n}(q^n-q^{t-1})$ of different bases in an n-dimensional space over GF(q) can be written as $q^{\frac{n(n-1)}{2}}(q-1)^n[n]_q!$.

Latin squares. A *latin square* of order n is a function $f:\{1,\ldots,n\}^2\to\{1,\ldots,n\}$ invertible in each argument. Traditionally, latin squares are represented by their value tables, whose rows and columns, by definition, contain all elements from 1 to n. (A system from the set $\{1,\ldots,n\}$ with a latin square operation f is known as a *quasigroup* of order n.) A latin square f is called *symmetric* if $f(x,y)\equiv f(y,x)$ (i.e., the corresponding quasigroup is commutative). A latin square f is called *totally symmetric* if $f(x,y)=z$ implies $f(y,x)=z$, $f(x,z)=y$, $f(z,x)=y$, $f(y,z)=x$, and $f(z,y)=x$. A latin square f is called *idempotent* if $f(x,x)\equiv x$. It is well known and obvious that the idempotent totally symmetric latin squares of order n are in one-to-one correspondence with the Steiner triple systems of order n.

Proposition 2.1. *Let $S=\{1,\ldots,n\}$. For every Steiner triple system (S,B), the function f defined as $f(x,x)\equiv x$ and $f(x,y)=z$ for every $\{x,y,z\}\in B$ is an idempotent totally symmetric latin square. Inversely, every idempotent totally symmetric latin square $f:S^2\to S$ induces the Steiner triple system (S,B), $B=\{\{x,y,z\}:x\neq y, f(x,y)=z\}$.*

Slightly less obvious but also well known is the following bijection.

Proposition 2.2. *For every odd n, there is a one-to-one correspondence between symmetric latin squares of order n and symmetric latin squares f of order $n+1$ such that $f(x,x)\equiv n+1$.*

Proof. Given symmetric latin square f of order $n+1$ such that $f(x,x) \equiv n+1$, the function $g : \{1,\ldots,n\}^2 \to \{1,\ldots,n\}$ defined by $g(x,x) = f(x,n+1)$, $g(x,y) = f(x,y)$ for every different x and y from $\{1,\ldots,n\}$ is straightforwardly a symmetric latin square.

$$\boxed{\begin{matrix} \mathbf{4} & 1 & 3 & \mathbf{2} \\ 1 & \mathbf{4} & 2 & \mathbf{3} \\ 3 & 2 & \mathbf{4} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{4} \end{matrix}} \longleftrightarrow \boxed{\begin{matrix} \mathbf{2} & 1 & 3 \\ 1 & \mathbf{3} & 2 \\ 3 & 2 & \mathbf{1} \end{matrix}}$$

To see the inverse, it is important to note that for a symmetric latin square g of odd order n, the set $\{g(x,x) : x \in \{1,\ldots,n\}\}$ coincides with $\{1,\ldots,n\}$ (indeed, for every x the number of the pairs (y,z) such that $g(y,z) = x$ is odd n, while the number of the pairs (y,z) such that $g(y,z) = x$ and $y \neq z$ is even, from the symmetry). Then we define the required f by the identities $f(x,x) = n+1$, $f(x,n+1) = f(n+1,x) = g(x,x)$, and $f(x,y) = g(x,y)$ for every $x,y \in \{1,\ldots,n\}$, $x \neq y$. ▲

Remark 1. The symmetric latin squares f of even order n such that $f(x,x) \equiv n$ are in a straightforward one-to-one correspondence with the ordered 1-factorizations of the complete graph on the vertex set $\{1,\ldots,n\}$ (i.e., the ordered partitions of the set of edges of this graph into $n-1$ sets of mutually disjoint edges; the number of the ordered partitions equals $(n-1)!$ times the number of unordered partitions, see [27]), with the tournament schedules for n teams, see e.g. [30], and with the resolutions of the complete system of pairs from $\{1,\ldots,n\}$, see e.g. [1]. Under these different names, but in the same context as in the current paper, the symmetric latin squares can be mentioned in the literature on combinatorial designs.

Möbius coefficients. For a prime power q, define the numbers $\mu_i^{(q)}$, $i = 0,1,2,\ldots$ by the following recursion: $\mu_i^{(q)} = 1$, and for an i-dimensional space S over GF(q), $i \geq 0$, and the set $\mathcal{S}$ of its subspaces,

$$\mu_i^{(q)} = -\sum_{C \in \mathcal{S}\setminus\{S\}} \mu_{\dim(C)}^{(q)}, \qquad \text{or, equivalently,} \qquad \sum_{C \in \mathcal{S}} \mu_{\dim(C)}^{(q)} = 0. \tag{1}$$

Remark 2. The numbers $\mu_i^{(q)}$ are related with the so-called Möbius function on the poset of spaces over GF(q). Namely, for two spaces U and V, the Möbius function $\mu_U(V)$ equals $\mu_{\dim(U)-\dim(V)}^{(q)}$ if $V \subseteq U$ and 0 otherwise.

Lemma 2.3 ([16, 3.10]). *For every prime power q, it holds $\mu_i^{(q)} = (-1)^i q^{\binom{i}{2}}$.*

3. Non-full-3-rank STS

Let $v \equiv 1,3 \bmod 6$; that is, there exist STS(v). By V^v, we denote the vector space of all v-tuples over GF(3). Denote by $\mathcal{D}$ the set of subspaces of V^v, each including the all-one vector and being orthogonal to at least one STS(v); denote

$$\mathcal{D}_i = \{D \in \mathcal{D} : \dim(D) = i+1\}.$$

The following lemma can be considered as a treatment of the results of [4, Sect. 4] in terms of the structure of a basis for the dual space of STS.

Lemma 3.1 ([8, Thm 5.1]). *Let M be a $(i+1)\times v$ generator matrix for $D\in\mathcal{D}_i$, and let the first row of M be the all-one vector. Then M consists of 3^i different columns, each occurring $v/3^i$ times.*

The prove given in [8] includes a proof of more deep mathematical result, a variation of Bonisoli's theorem. We give an independent simple prove.

Proof. Without loss of generality, we can assume that the first column of M is $(1,0,...,0)^{\mathrm{T}}$ (we can achieve this by subtracting the first row from some of the others).

Claim (*). *If a and b are columns of M, then $-a-b$ is also a column of M.* Consider an STS(v) orthogonal to the rows of M. Let a and b be the jth and kth columns of M, and let $\{j,k,l\}$ be the STS block containing j and k. Since all rows of M are orthogonal to the characteristic vector of this block, the lth column c satisfies $a+b+c=0$, i.e., $c=-a-b$. This proves (*).

Claim (**). *If c and d are columns of M, then $c+d-(1,0,...,0)^{\mathrm{T}}$ is also a column of M.* This is proved by applying (*) with $a=c$, $b=d$ first, and then with $a=-c-d$, $b=(1,0,...,0)^{\mathrm{T}}$.

The last claim means that the set of columns of the matrix M' obtained from M by removing the first row is closed under the addition. Since there are i linearly independent columns, this set contains all possible 3^i columns of height i.

It remains to prove that different columns a and b occur the same number of times in M. Let J and K be the sets of positions in which M has the columns a and b, respectively. And let l be a position of the column $-a-b$. For each j from J, there is k from K such that $\{j,k,l\}$ is a block of the STS. Moreover, different js correspond to different ks. This shows that $|J|\le|K|$. Similarly, $|K|\le|J|$. ▲

Example 1. If $v=27$, then a generator matrix for a subspace from $\mathcal{D}_2$ has the following form, up to permutation of the columns:

$$\begin{pmatrix} 111111111111111111111111111 \\ 000000000111111111222222222 \\ 000111222000111222000111222 \end{pmatrix}.$$

Lemma 3.2. *Let i and j be nonnegative integers such that $i\le j$. If $\mathcal{D}_j$ is not empty, then every subspace from $\mathcal{D}_i$ is contained in exactly $\Gamma_{v,i,j}$ subspaces from $\mathcal{D}_j$, where*

$$\Gamma_{v,i,j}=\left(\frac{v}{3^i}!\right)^{3^i}\Big/3^{\frac{(j+i+1)(j-i)}{2}}\left(\frac{v}{3^j}!\right)^{3^j}2^{j-i}[j-i]_3!. \tag{2}$$

In particular, $|\mathcal{D}_j|=\Gamma_{v,0,j}$.

Proof. Firstly, let us fix some D_i from $\mathcal{D}_i$ and construct all D_j from $\mathcal{D}_j$ that satisfy $D_i\subseteq D_j$. Let M_i be a generator matrix of D_i whose first row contains only 1s. According to Lemma 3.1, M_i divides the coordinates into 3^i "cells" such that each cell contains the same columns in it. Since $D_i\subseteq D_j$, so D_j has a generator matrix M_j that starts with the $i+1$ rows of M_i, and this matrix subdivides the cells into 3^j "subcells" of the same size. The number of such subdivisions is $A=\left(\frac{v}{3^i}!\right)^{3^i}/\left(\frac{v}{3^j}!\right)^{3^j}$.

Next, let us count the number of such matrices that generate the same code. Let M'_j be another generator matrix of D_j that also starts with $i+1$ rows of M_i; what is more, its ts row, $i+2 \le t \le j+1$, is a linear combination of the rows of M_j, but is not a linear combination of the rows above it in the matrix M'_j. So, we can get there are $3^{j+1}-3^{i+1}$ kinds of values for the row $i+2$, $3^{j+1}-3^{i+2}$ kinds of values for the row $i+3$ and so on. Therefore, the number of such matrices M'_j is $B = (3^{j+1}-3^{i+1})(3^{j+1}-3^{i+2})\dots(3^{j+1}-3^{j}) = 3^{\frac{(j-i)(j+i+1)}{2}}\prod_{s=1}^{j-i}(3^s-1)$. Finally, the number of different D_j that satisfy $D_i \subseteq D_j$ is $\Gamma_{v,i,j} = \frac{A}{B}$.

▲

Lemma 3.3 (the structure of non-full-3-rank STS[7]). *Given a subspace D from $\mathcal{D}_j$, the set of STS(v) orthogonal to D is in one-to-one correspondence with the collections of 3^j Steiner triple systems of order $v/3^j$ and $3^j(3^j-1)/6$ latin squares of order $v/3^j$.*

Proof (a sketch). According to Lemma 3.1, a generator matrix M of D divides the coordinates into 3^j *groups* of size $v/3^j$. It can be seen that every STS(v) orthogonal to D is divided into the $3^j + 3^j(3^j-1)/6$ following subsets:

- For each of 3^j groups, the triples with all 3 points in these group form STS($v/3^j$).
- For every 3 distinct groups $\{\alpha_1,\dots,\alpha_{v/3^j}\}$, $\{\beta_1,\dots,\beta_{v/3^j}\}$, $\{\gamma_1,\dots,\gamma_{v/3^j}\}$ corresponding to columns a, b, c with $a+b+c=0$, the triples with one point in each of these 3 groups have the form $\{\alpha_x,\beta_y,\gamma_{f(x,y)}\}$ for some latin square f of order $v/3^j$.

▲

Corollary 3.4 ([7]). *Given a subspace D from $\mathcal{D}_j$, the number $\Phi(D)$ of STS(v) orthogonal to D equals $\Phi_{v,j}$, where*

$$\Phi_{v,j} = \Psi_{v/3^j}^{3^j}\Lambda_{v/3^j}^{3^j(3^j-1)/6},$$

Ψ_u is the number of STS(u), and Λ_u is the number of latin squares of order u.

Now, given a subspace D from $\mathcal{D}_j$, we know the number $\Phi(D)$ of STS that are orthogonal to some subspace of D. To find the number of STS that are dual to D, we should apply to the function $\Phi(D)$ the Möbius transform on the poset of subspaces of D. This is essentially done in the next lemma.

Lemma 3.5. *Assume that v is divided by 3^k and k is the largest integer with this property. Let $i \in \{0,\dots,k\}$, and let D be in $\mathcal{D}_i$. The number of STS(v) with dual space D equals $\Upsilon_{v,i}$, where*

$$\Upsilon_{v,i} = \sum_{j=i}^{k}\Gamma_{v,i,j}\mu^{(3)}_{j-i}\Phi_{v,j}, \qquad (3)$$

where $\Gamma_{v,i,j}$ and $\Phi_{v,j}$ are from Lemma 3.2 and Corollary 3.4.

Proof. Utilizing the definition of $\Gamma_{v,i,j}$ and then expanding $\Phi_{v,j}$, we have

$$\sum_{j=i}^{k}\Gamma_{v,i,j}\mu^{(3)}_{j-i}\Phi_{v,j} = \sum_{j=i}^{k}\sum_{\substack{D'\in\mathcal{D}_j\\ D\subseteq D'}}\mu^{(3)}_{j-i}\Phi_{v,j} = \sum_{j=i}^{k}\sum_{\substack{D'\in\mathcal{D}_j\\ D\subseteq D'}}\sum_{B\in P(D')}\mu^{(3)}_{j-i},$$

where $P(D')$ is the set of STS(v) orthogonal to D'. We continue:

$$= \sum_{\substack{D'\in\mathcal{D}\\ D\subseteq D'}} \sum_{B\in P(D')} \mu^{(3)}_{\dim(D')-i} = \sum_{\substack{D'\in\mathcal{D}\\ D\subseteq D'}} \sum_{\substack{B\in P(D)\\ B\perp D'}} \mu^{(3)}_{\dim(D')-i} = \sum_{B\in P(D)} \sum_{\substack{D'\in\mathcal{D}\\ D\subseteq D',\, B\perp D'}} \mu^{(3)}_{\dim(D')-i}$$

$$= \sum_{B\in P(D)} \sum_{\substack{D'\in\mathcal{D}:\\ D\subseteq D'\subseteq B^\perp}} \mu^{(3)}_{\dim(D')-i} \overset{D^*=D'/D}{=} \sum_{B\in P(D)} \sum_{D^*\subseteq B^\perp/D} \mu^{(3)}_{\dim(D^*)}$$

$$\overset{(1)}{=} \sum_{B\in P(D)} (1 \text{ if } B^\perp = D;\ 0 \text{ otherwise}).$$

We see that the last formula meets the definition of $\Upsilon_{v,i}$. ▲

Theorem 3.6. *Assume that v is divided by 3^k and k is the largest integer with this property. Let $i \in \{0,\dots,k\}$. The total number of different STS(v) of 3-rank $v-i-1$ equals*

$$\Gamma_{v,0,i} \sum_{j=i}^{k} \Gamma_{v,i,j}\mu^{(3)}_{j-i}\Phi_{v,j}, \qquad \textit{where } \mu^{(3)}_l = (-1)^l 3^{\binom{l}{2}}, \quad \Phi_{v,j} = \Psi^{3^j}_{v/3^j}\Lambda^{3^j(3^j-1)/6}_{v/3^j},$$

$$\Gamma_{v,i,j} = \left(\frac{v}{3^i}!\right)^{3^i} \Big/ 3^{\frac{(j+i+1)(j-i)}{2}} \left(\frac{v}{3^j}!\right)^{3^j} \prod_{s=1}^{j-i}(3^s-1),$$

Ψ_u is the number of STS(u) (and also the number of idempotent totally symmetric latin squares of order u), and Λ_u is the number of latin squares of order u.

Proof. The number of STS(v) of 3-rank $v-i-1$ equals the number $\Upsilon_{v,i}$ of STS(v) of 3-rank $v-i-1$ orthogonal to a given subspace D from $\mathcal{D}_i$ multiplied by the number $\Gamma_{v,0,i}$ of such subspaces. Utilizing the formulas from Lemma 3.5 and Corollary 3.4, we get the result. ▲

Corollary 3.7. *The number of STS(v), $v=3^k$, of 3-rank $v-k-1$ is*

$$\frac{v!}{3^{\frac{k(k+1)}{2}} \cdot 2^k \cdot [k]_3!}.$$

The number of STS(v), $v=3^k$, of 3-rank $v-k$ is

$$\frac{v! \cdot (2^{v^2/27-4v/9+1} \cdot 3^{v^2/54-7v/18+k} - 1)}{2^k \cdot 3^{\frac{k(k+1)}{2}} \cdot [k-1]_3!}.$$

The number of STS(v), $v=3^k$, of 3-rank $v-k+1$ is

$$\frac{v!}{2^{k+2} \cdot 3^{\frac{k(k+1)}{2}-1} \cdot [k-2]_3!}$$

$$\times\left(\frac{(2^{35}\cdot 3^8 \cdot 5^2 \cdot 7^2 \cdot 5231 \cdot 3824477)^{\frac{v(v-9)}{486}}}{2^{4v/9-4}\cdot 3^{v/3-2k+1}} - 2^{v^2/27-4v/9+3}\cdot 3^{v^2/54-7v/18+k-1} + 1\right).$$

The number of STS(v), $v = 7 \cdot 3^k$, of 3-rank $v-k-1$ is

$$\frac{v! \cdot 61479419904000^{\frac{3^k(3^k-1)}{6}}}{2^k \cdot 3^{\frac{k(k+1)}{2}} \cdot 168^{3^k} \cdot [k]_3!}.$$

PROOF. According to [28], we have $\Lambda_1 = 1$, $\Lambda_3 = 12$, $\Lambda_7 = 61479419904000 = 2^{18} \cdot 3^5 \cdot 5^3 \cdot 7 \cdot 1103$ [14, 15], $\Lambda_9 = 5524751496156892842531225600 = 2^{35} \cdot 3^8 \cdot 5^2 \cdot 7^2 \cdot 5231 \cdot 3824477$ [2] (the last known value is Λ_{11} [12]). According to [29], we have $\Psi_1 = \Psi_3 = 1$, $\Psi_7 = 30$, $\Psi_9 = 840$ (the last known value is Ψ_{19} [9]). Applying the result of Theorem 3.6, we get the formulas. ▲

A computer-aimed classification of equivalence classes of STS(27) of 3-rank 24 is described in [6]. In particular, the total number of different systems with these parameters can be calculated from [6, Table 1] as the sum $\sum N_r 27!/|\mathrm{Aut}(\mathcal{S})|$ over the all rows of the table except the last one (corresponding to the 3-rank 23). This number coincides with the one given by our formula, 22 300 404 167 684 260 773 163 008 000 000.

4. Non-full-2-rank STS

In this section, to simplify the formulas, we denote the order of STS by $w-1$ instead of v. By $\dot{V}^{w-1}$, we denote the vector space of all $(w-1)$-tuples over GF(2). Denote by $\dot{\mathcal{D}}_i$ the set of i-dimensional subspaces of $\dot{V}^{w-1}$ orthogonal to at least one STS($w-1$). The following lemma can be considered as a treatment of the results of [4, Sect. 3] in terms of the structure of a basis for the dual space of STS.

Lemma 4.1 ([8, Thm 4.1]). *Let M be a $i \times (w-1)$ generator matrix for $D \in \dot{\mathcal{D}}_i$. Then each of the $2^i - 1$ nonzero columns of height i occurs $w/2^i$ times as a column of M, while the all-zero column occurs $w/2^i - 1$ times.*

PROOF. Claim (*). *If a and b are different nonzero columns of M, then $a + b$ is also a column of M.* The proof is similar to that of Claim (*) in the proof of Lemma 4.1.

Since the rank of M is i, it contains i linearly independent columns. It follows from (*) that it contains all $2^i - 1$ different nonzero columns of height i.

It remains to show that every nonzero column a occur $|K| + 1$ times, where K is the set of positions in which M has the all-zero column. Let J be the sets of positions in which M has the column a, and let $l \in J$. For each j from $J \backslash \{l\}$, there is k from K such that $\{j, k, l\}$ is a block of the STS. Moreover, different js correspond to different ks. This shows that $|J \backslash \{l\}| \le |K|$. Similarly, $|K| \le |J \backslash \{l\}|$. ▲

Example 2. If $w = 32$, then a generator matrix for a subspace from $\dot{\mathcal{D}}_3$ has the following form, up to permutation of the columns:

$$\begin{pmatrix} 0000000000000001111111111111111 \\ 0000000111111110000000011111111 \\ 0001111000011110000111100001111 \end{pmatrix}.$$

Lemma 4.2. *Let i and j be nonnegative integers such that $i \le j$. If $\dot{\mathcal{D}}_j$ is not empty,* *then every subspace from $\dot{\mathcal{D}}_i$ is contained in exactly $\dot{\Gamma}_{w,i,j}$ subspaces from $\dot{\mathcal{D}}_j$, where*

$$\dot{\Gamma}_{w,i,j} = \left(\frac{w}{2^i}!\right)^{2^i} \Big/ 2^{\frac{(j-i)(j+i+1)}{2}} \left(\frac{w}{2^j}!\right)^{2^j} [j-i]_2!. \qquad (4)$$

In particular, $|\dot{\mathcal{D}}_j| = \dot{\Gamma}_{w,0,j}$.

Proof. The proof is similar to that of Lemma 3.2. The difference is that the size of one cell, corresponding to the all-zero columns of the generator matrix, is one less than for each of the other cells; the same can be said for the subcells. So, totally we have

$$A = \left(\frac{w}{2^i}!\right)^{2^i-1} \left(\frac{w}{2^i}-1\right)! \Big/ \left(\frac{w}{2^j}!\right)^{2^j-1} \left(\frac{w}{2^j}-1\right)! = \left(\frac{w}{2^i}!\right)^{2^i} \Big/ 2^{j-i} \left(\frac{w}{2^j}!\right)^{2^j}$$

subdivisions. Dividing this number by the number $B = 2^{\frac{(j-i)(j+i-1)}{2}} \prod_{s=1}^{j-i}(2^s-1)$ of the matrices generating the same space, we get the result. ▲

The following lemma describes the structure of an arbitrary non-full-2-rank STS. It was proved in [26] for the partial case of STS(2^k-1) of rank 2^k+2; the arguments, however, are applicable to the general case. It should be also noted that Theorem 4.1 in [1] is close to this result, but the structure of the part of the block set connected with latin squares is not described there (with the exception of one partial example in Remark 6).

Lemma 4.3 (the structure of non-full-2-rank STS [7]). *Given a subspace D from $\dot{\mathcal{D}}_j$, the set of STS($w-1$) orthogonal to D is in one-to-one correspondence with the collections of one STS($w/2^j-1$), 2^j-1 symmetric latin squares of order $w/2^j-1$, and $(2^j-1)(2^j-2)/6$ latin squares of order $w/2^j$.*

Proof (a sketch). According to Lemma 3.1, a generator matrix M of D divides the coordinates into 2^j-1 groups of size $w/2^j$ and one group of size $w/2^j-1$ (the last group corresponds to the all-zero columns of M). It can be seen that the set of triples of every STS(v) orthogonal to D is divided into the $2^j+(2^j-1)(2^j-2)/6$ following subsets:

- The triples with all 3 points in the group of size $w/2^j-1$ form STS($w/2^j-1$).
- The triples with one points in the group $\{\gamma_1,\ldots,\gamma_{w/2^j-1}\}$ of size $w/2^j-1$ and two points in one of the 2^j-1 groups $\{\alpha_1,\ldots,\alpha_{w/2^j}\}$ of size $w/2^j$. Such triples have the form $\{\alpha_x,\alpha_y,\gamma_{f(x,y)}\}$ for some symmetric latin square f satisfying $f(x,x)\equiv w/2^j$. Proposition 2.2 relates f with a symmetric latin square of order $w/2^j-1$.
- For every 3 distinct groups $\{\alpha_1,\ldots,\alpha_{w/2^j}\}$, $\{\beta_1,\ldots,\beta_{w/2^j}\}$, $\{\gamma_1,\ldots,\gamma_{w/2^j}\}$ corresponding to columns a, b, c with $a+b+c=0$, the triples with one point in each of these 3 groups have the form $\{\alpha_x,\beta_y,\gamma_{f(x,y)}\}$ for some latin square f of order $v/2^j$.

▲

Corollary 4.4 ([7]). *Given a subspace D from $\dot{\mathcal{D}}_j$, the number $\dot{\Phi}(D)$ of STS($w-1$) orthogonal to D equals $\dot{\Phi}_{w-1,j}$, where*

$$\dot{\Phi}_{w-1,j} = \Psi_{w/2^j-1}\Pi_{w/2^j-1}^{2^j-1}\Lambda_{w/2^j}^{(2^j-1)(2^j-2)/6},$$

Ψ_u is the number of STS(u) (and the number of idempotent totally symmetric latin squares of order u), Π_u is the number of symmetric latin squares of order u, Λ_u is the number of latin squares of order u.

Lemma 4.5. *Assume that w is divided by 2^k and k is the largest integer with this property. Let $i \in \{0, \dots, k\}$, and let D be in $\dot{\mathcal{D}}_i$. The number of STS($w-1$) with dual space D equals $\dot{\Upsilon}_{w-1,i}$, where*

$$\dot{\Upsilon}_{w-1,i} = \sum_{j=i}^{k} \dot{\Gamma}_{w,i,j} \mu^{(2)}_{j-i} \dot{\Phi}_{w-1,j}, \tag{5}$$

where $\dot{\Gamma}_{w,i,j}$ and $\dot{\Phi}_{w-1,j}$ are from Lemma 3.2 and Corollary 3.4.

The proofs of the lemma and the following theorem are the same as those of Lemma 3.5, and we omit them.

Theorem 4.6. *Assume that w is divided by 2^k and k is the largest integer with this property. Let $i \in \{0, \dots, k\}$. The total number of different STS($w-1$) of 2-rank $w-i-1$ equals*

$$\dot{\Gamma}_{w,0,i} \sum_{j=i}^{k} \dot{\Gamma}_{w,i,j} \mu^{(2)}_{j-i} \dot{\Phi}_{w-1,j},$$

where $\mu^{(2)}_l = (-1)^l 2^{\binom{l}{2}}$, $\dot{\Phi}_{w-1,j} = \Psi_{w/2^j-1} \Pi^{2^j-1}_{w/2^j-1} \Lambda^{(2^j-1)(2^j-2)/6}_{w/2^j}$, Ψ_u is the number of STS(u) (and also the number of idempotent totally symmetric latin squares of order u), Π_u is the number of symmetric latin squares of order u (and also $u!$ times the number of 1-factorizations of the complete graph of order $u+1$), Λ_u is the number of latin squares of order u, and

$$\dot{\Gamma}_{w,i,j} = \left(\frac{w}{2^i}!\right)^{2^i} \Big/ 2^{\frac{(j-i)(j+i+1)}{2}} \left(\frac{w}{2^j}!\right)^{2^j} \prod_{s=1}^{j-i} (2^s - 1)$$

Corollary 4.7. *The number of STS($w-1$), $w = 2^k$, of 2-rank $w-k$ is*

$$w!(2^{w^2/24-3w/4+k+1/3} - 1)/2^{\frac{k(k+1)}{2}}[k-1]_2! \qquad \text{(see [17])}.$$

The number of STS($w-1$), $w = 2^k$, of 2-rank $w-k+1$ is

$$\frac{w!\left(3^{w^2/48-w/4+2/3} \cdot 2^{w^2/16-5w/4+2k-1} - 3 \cdot 2^{w^2/24-3w/4+k-2/3} + 1\right)}{3 \cdot 2^{\frac{(k+2)(k-1)}{2}} \cdot [k-2]_2!} \qquad \text{(see [25])}.$$

The number of STS($w-1$), $w = 2^k$, of 2-rank $w-k+2$ is

$$\frac{2^k!}{21 \cdot 2^{\frac{k(k+1)}{2}-3} \cdot [k-3]_2!}$$

$$\times \Big(780^{w/8-1} \cdot (2^{28} \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 1361291)^{w^2/384-w/16+1/3} \cdot 2^{3k-12}$$

$$-7\cdot 2^{w^2/16-5w/4+2k-3}\cdot 3^{w^2/48-w/4+2/3}+7\cdot 2^{w^2/24-3w/4-5/3+k}-1\Big) \qquad \textit{(see [23]).}$$

The number of STS$(10w-1)$, $w=2^k$, *of* 2*-rank* $10w-1-k$ *is*

$$\frac{(10w)!\cdot 122556672^{w-1}\cdot (2^{43}\cdot 3^{10}\cdot 5^4\cdot 7^2\cdot 31\cdot 37\cdot 547135293937)^{\frac{(w-1)(w-2)}{6}}}{2^{\frac{k(k+1)}{2}+5}\cdot 135\cdot [k]_2!}.$$

PROOF. To apply the formula from Theorem 4.6, in addition to the values considered in the proof of Corollary 3.7, we need $\Pi_1=1$, $\Pi_3=6$, $\Pi_7=31449600=7!\cdot 6240$ [19], $\Pi_9=444733651353600=9!\cdot 1225566720$ [5], see also [30],

$$\Lambda_2=2, \qquad \Lambda_4=576, \qquad \Lambda_8=108776032459082956800=2^{28}\cdot 3^5\cdot 5^2\cdot 7^2\cdot 1361291 \quad [20],$$
$$\Lambda_{10}=9982437658213039871725064756920320000=2^{43}\cdot 3^{10}\cdot 5^4\cdot 7^2\cdot 31\cdot 37\cdot 547135293937 \quad [11],$$

see also [28]. We also formally need the trivial values $\Pi_0=1$ and $\Phi_0=1$. ▲

Remark 3. Taking into account Propositions 2.1 and 2.2, we know that $\Psi(u-1)$ and $\Pi(u-1)$ are the numbers of latin squares of order u with certain restrictions. So, $\Psi(u-1)<\Pi(u-1)<\Lambda(u)$. It can be then noted that if $j\geq 3$, then the most valuable factor in the formulas for the number of $STS(v)$ of 2- or 3-rank at most $v-j$ is connected with the number of unrestricted latin squares.

5. Concluding remarks

As we see from the results of [7], the structure of the Steiner triple systems of deficient rank, either 2- or 3-rank, with fixed orthogonal subspace, is well understood, meaning that it can be described in terms of latin squares and Steiner triple systems of smaller order. The possibility to derive an explicit formula for the number of the non-full-rank STS (involving the number of latin squares and smaller STS) implies that this description is constructive even if we do not fix the orthogonal subspace of the systems. We finish the paper with a simple statement that shows that the privileges given by the knowledge of the structure of a Steiner triple system depending on the value of its 2-rank or the value of its 3-rank cannot be combined in the same system.

Proposition 5.1. *There is no a Steiner triple system of order v larger than 3 that is both non-full-2-rank and non-full-3-rank, i.e., of 2-rank less than v and 3-rank less than $v-1$.*

PROOF. Assume that S an a STS(v), $v>3$, which is (i) of 3-rank at most $v-2$ and (ii) 2-rank at most $v-1$, $v>3$. By Lemma 3.1, (i) means that there is a vector with $v/3$ zeros, $v/3$ ones, and $v/3$ twos that is orthogonal to S over GF(3); in particular, $v\equiv 0 \bmod 3$. Assumption (ii) means that S has a Steiner subsystem S' of order $(v-1)/2$, by Lemma 4.3. Since $v>3$ implies $(v-1)/2>v/3$, the system S' is orthogonal over GF(3) to a vector that is not all-0, all-1, or all-2. By Lemma 3.1, the order $(v-1)/2$ is an integer divisible by 3, and we get $v\equiv 1 \bmod 3$, a contradiction. ▲

6. Acknowledgements

The authors thank Vladimir Tonchev for the helpful discussion. This research is supported by the National Natural Science Foundation of China (61672036), Technology Foundation for Selected Overseas Chinese Scholar, Ministry of Personnel of China (05015133), Key projects of support program for outstanding young talents in Colleges and Universities (gxyqZD2016008), Excellent Youth Foundation of Natural Science Foundation of Anhui Province (No.1808085J20), and the Program of fundamental scientific researches of the Siberian Branch of the Russian Academy of Sciences No.I.1.1. (project No.0314-2016-0001).

References

1. E. F. Assmus, Jr. On 2-ranks of Steiner triple systems. *Electr. J. Comb.*, 2(R9):1–35, 1995.

2. S. E. Bammel and J. Rothstein. The number of 9×9 Latin squares. *Discrete Math.*, 11(1):93–95, 1975. DOI: 10.1016/0012-365X(75)90108-9.

3. P. J. Cameron. *Parallelisms of Complete Designs*, volume 23 of *Lond. Math. Soc. Lect. Note Ser.* Cambridge University Press, Cambridge etc., 1976. DOI: 10.1017/CBO9780511662102.

4. J. Doyen, X. Hubaut, and M. Vandensavel. Ranks of incidence matrices of Steiner triple systems. *Mathematische Zeitschrift*, 163(3):251–259, Oct. 1978. DOI: 10.1007/BF01174898.

5. E. N. Gelling and R. E. Odeh. On 1-factorizations of the complete graph and the relationship to round-robin schedules. *Congr. Numerantium*, 9:213–221, 1974.

6. D. Jungnickel, S. S. Magliveras, V. D. Tonchev, and A. Wassermann. The classification of Steiner triple systems on 27 points with 3-rank 24. *Des. Codes Cryptography*, 2018. DOI: 10.1007/s10623-018-0502-5.

7. D. Jungnickel and V. D. Tonchev. Counting Steiner triple systems with classical parameters and prescribed rank. *J. Comb. Theory, Ser. A*, 2018. To appear. `https://arxiv.org/abs/1709.06044`.

8. D. Jungnickel and V. D. Tonchev. On Bonisoli's theorem and the block codes of Steiner triple systems. *Des. Codes Cryptography*, 86(3):449–462, 2018. DOI: 10.1007/s10623-017-0406-9.

9. P. Kaski and P. R. J. Östergård. The Steiner triple systems of order 19. *J. Comb. Theory, Ser. A*, 73(248):2075–2092, 2004. DOI: 10.1090/S0025-5718-04-01626-6.

10. N. Linial and Z. Luria. An upper bound on the number of Steiner triple systems. *Random Struct. Alg.*, 43(4):399–406, 2013. DOI: 10.1002/rsa.20487. https://arxiv.org/abs/1108.5042

11. B. D. McKay and E. Rogoyski. Latin squares of order 10. *Electr. J. Comb.*, 2(N3):1–4, 1995.

12. B. D. McKay and I. M. Wanless. On the number of Latin squares. *Ann. Comb.*, 9(3):335–344, 2005. DOI: 10.1007/s00026-005-0261-7. https://arxiv.org/abs/0909.2101

13. O. P. Osuna. There are 1239 Steiner triple systems STS(31) of 2-rank 27. *Des. Codes Cryptography*, 40(2):187–190, Aug. 2006. DOI: 10.1007/s10623-006-0006-6.

14. A. Sade. Enumération des carrés latins. application au 7éme ordre. conjectures pour les ordres supérieurs. Privately published, 1948.

15. P. N. Saxena. A simplified method of enumerating Latin squares by MacMahon's differential operators, Part II, The 7×7 Latin squares. *J. Indian Soc. Agric. Stat.*, 3:24–79, 1951.

16. R. P. Stanley. *Enumerative Combinatorics, Volume I*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge Univ. Press, Cambridge, second edition, 2012. DOI: 10.1017/CBO9781139058520.

17. V. D. Tonchev. A mass formula for Steiner triple systems STS(2^n-1) of 2-rank 2^n-n. *J. Comb. Theory, Ser. A*, 95(2):197–208, Aug. 2001. DOI: 10.1006/jcta.2000.3161.

18. J. H. van Lint and R. M. Wilson. *A Course in Combinatorics*. Cambridge Univ. Press, Cambridge etc., second edition, 2001.

19. W. D. Wallis, A. P. Street, and J. S. Wallis. *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices*, volume 292 of *Lect. Notes Math.* Springer-Verlag, Berlin, 1972. DOI: 10.1007/BFb0069907.

20. M. B. Wells. The number of Latin squares of order eight. *J. Comb. Theory*, 3(1):98–99, 1967. DOI: 10.1016/S0021-9800(67)80021-8.

21. R. M. Wilson. Nonisomorphic Steiner triple systems. *Mathematische Zeitschrift*, 135(4):303–313, 1974. DOI: 10.1007/BF01215371.

22. D. V. Zinoviev. On the number of 1-factorizations of a complete graph. *Probl. Inf. Transm.*, 50(4):364–370, Oct. 2014. DOI: 10.1134/S0032946014040061 translated from Probl. Peredachi Inf. 50(4) (2014), 71-78.

23. D. V. Zinoviev. On the number of Steiner triple systems $S(2^m-1,3,2)$ of rank 2^m-m+2 over F_2. *Discrete Math.*, 339(11):2727–2736, Nov. 2016. Corrected formula: https://arxiv.org/abs/1512.00187

24. V. A. Zinoviev and D. V. Zinoviev. Steiner triple systems $S(2^m - 1, 3, 2)$ of rank $2^m - m + 1$ over F_2. *Probl. Inf. Transm.*, 48(2):102–126, Apr. 2012. DOI: 10.1134/S0032946012020020 translated from Probl. Peredachi Inf. 48(2) (2012), 21-47.

25. V. A. Zinoviev and D. V. Zinoviev. Remark on "Steiner triple systems $S(2^m - 1, 3, 2)$ of rank $2^m - m + 1$ over F_2" published in Probl. peredachi inf., 2012, no. 2. *Probl. Inf. Transm.*, 49(2):192–195, Apr. 2013. DOI: 10.1134/S0032946013020087 translated from Probl. Peredachi Inf. 49(2) (2013), 107-111.

26. V. A. Zinoviev and D. V. Zinoviev. Structure of Steiner triple systems $S(2^m - 1, 3, 2)$ of rank $2^m - m + 2$ over f_2. *Probl. Inf. Transm.*, 49(3):232–248, July 2013. DOI: 10.1134/S0032946013030034 translated from Probl. Peredachi Inf. 49(3) (2013), 40-56.

27. Sequence A000438 in The On-Line Encyclopedia of Integer Sequences. Published electronically at `http://oeis.org`, 2004. Number of 1-factorizations of complete graph K_{2n}.

28. Sequence A002860 in The On-Line Encyclopedia of Integer Sequences. Published electronically at `http://oeis.org`, 2004. Number of Latin squares of order n; or labeled quasigroups.

29. Sequence A030128 in The On-Line Encyclopedia of Integer Sequences. Published electronically at `http://oeis.org`, 2004. Steiner triple systems (STS's) on n elements.

30. Sequence A036981 in The On-Line Encyclopedia of Integer Sequences. Published electronically at `http://oeis.org`, 2001. (2n+1) X (2n+1) symmetric matrices each of whose rows is a permutation of 1..(2n+1).