Steiner triple and quadruple systems of low 2-rank

Vladimir D. Tonchev

Department of Mathematical Sciences

Michigan Technological University

Houghton, MI 49931, USA

tonchev@mtu.edu, www.math.mtu.edu/∼tonchev

Overview

- Steiner systems $STS(v)$ and $SQS(v)$
- The code of a Steiner system
- The theorems of Assmus
- Formulas for Steiner systems of low rank
- Enumeration of Steiner systems
- New developments

Steiner Triple Systems

S=STS(v): $S=(X, \mathcal{B})$

$X = \{x_i\}_{i=1}^{v}$ points

$\mathcal{B}=\{B_j\}_{j=1}^{b}$ blocks

- $B_j \subset X,\ |B_j| = 3$;
- every pair of points is in exactly one block;
- every point is in $(v-1)/2$ blocks;
- there are $b = v(v-1)/6$ blocks.

Steiner Quadruple Systems

A Steiner Quadruple System $SQS(v)$ is a set of v points and a collection of 4-subsets called blocks such that every three points are contained in exactly one block.

Note. The blocks through a point x of an $SQS(v)$ after deleting x form an $STS(v-1)$.

Isomorphisms and Automorphisms

Two systems $S' = (X, \mathcal{B}')$, $S'' = (X, \mathcal{B}'')$ are distinct if $\mathcal{B}' \neq \mathcal{B}''$.

Two systems $S' = (X, \mathcal{B}')$, $S'' = (X, \mathcal{B}'')$ are isomorphic if there is a permutation of X that maps $\mathcal{B}'$ to $\mathcal{B}''$.

An automorphism of $S = (X, \mathcal{B})$ is a permutation of X that preserves $\mathcal{B}$.

Existence and Examples

An $STS(v)$ exists if and only if $v \equiv 1, 3 \pmod 6$.

An $SQS(v)$ exists if and only if $v \equiv 2, 4 \pmod 6$.

The Classical $STS(2^n - 1)$ has the lines in $PG(n-1, 2)$ as blocks.

The Classical $SQS(2^n)$ has the planes in $AG(n, 2)$ as blocks.

Small $STS(v)$ and $SQS(v)$

The number $N(v)$ of non-isomorphic $STS(v)$'s:

v	$N(v)$
3	1
7	1
9	1
13	2
15	80
19	11,084,874,829

The number $N(v)$ of non-isomorphic $SQS(v)$'s:

v	$N(v)$
4	1
8	1
10	1
14	4
16	1,054,163

$STS(v)$ with large v

Theorem (Richard Wilson, 1974):

$$N(v) \geq \left(\frac{v}{e^5}\right)^{\frac{v^2}{6}}.$$

The Incidence Matrix

$$A = (a_{ij})_{b \times v} :$$

$$a_{i,j} = 1 \text{ is } x_j \in B_i,\ a_{i,j} = 0 \text{ if } x_j \notin B_i.$$

The Code C of an $STS(v)$

$$C \leq GF(2)^v$$

is the linear span of the incidence matrix A over $GF(2)$.

Note: $dim(C) = rank_2 A$.

Theorem. (Doyen, Hubaut, Vandensavel, 1978):

(i) $rank_2 A = v - \log_2(m+1)$,

where m is the number of maximal subsystems.

(ii) If $v = 2^n - 1$ then $rank_2 A \geq 2^n - n - 1$,

with equality if and only if $S \simeq PG(n-1, 2)$.

Subsystems

A subsystem $S' = STS(v')$:
$D' = (X', \mathcal{B}')$

Note: $v' \leq (v-1)/2$.

A subsystem S' is maximal if

$$v' = (v-1)/2.$$

The point and block codes of small S

Theorem. (R. Weishaar 1993).

(i) The binary codes spanned by the point by block (transposed) incidence matrices (or point codes) of non-isomorphic Steiner systems $STS(v)$ with $v \leq 15$ are inequivalent.
(ii) The binary codes of the block by point incidence matrices of non-isomorphic Steiner systems $STS(v)$ with $v \leq 15$ having the same 2-rank are equivalent.

Theorem. (Kaski and Ostergard 2004).

There exist nonisomorphic $STS(19)$ that have equivalent point codes.

Assmus' Theorem

Theorem. (E.F. Assmus, Jr., 1995):

- The codes of two $STS(v)$'s, $S_1,\ S_2$ are equivalent if and only if $rank_2(S_1) = rank_2(S_2)$.
- For every admissible 2-rank $r \leq v$ there is a unique code that contains representatives of all $STS(v)$ of 2-rank r.
- If $v = 2^n - 1$ and $rank_2 S = 2^n - n$, the code of S is spanned by the incidence matrix of the classical $STS(2^n - 1)$ in $PG(n-1, 2)$ and a vector of weight 1.

A formula for $STS(2^n-1)$

Theorem.

(i) The total number of distinct $STS(2^n-1)$ of 2-rank 2^n-n is

$$\frac{(2^n-1)!(2^{\frac{(2^{n-1}-1)(2^{n-2}-1)}{3}}-2^{2^{n-1}-n})}{2^{2^{n-1}-1}(2^{n-1}-1)(2^{n-1}-2)\dots(2^{n-1}-2^{n-2})}.$$

(ii) If $D_1,\dots,D_s$ is a complete set of nonisomorphic $STS(2^n-1)$'s of 2-rank 2^n-n, then

$$2^{\frac{(2^{n-1}-1)(2^{n-2}-1)}{3}}-2^{2^{n-1}-n}=\Sigma_{i=1}^{s}\frac{|Aut(C)|}{|Aut(D_i)|}.$$

A Lower Bound

Corollary.
The number $N(v)$ of nonisomorphic $STS(v)$, $v = 2^n - 1$, of 2-rank $2^n - n$ is not less than

$$\frac{2^{\frac{(2^{n-1}-1)(2^{n-2}-1)}{3}} - 2^{2^{n-1}-n}}{2^{2^{n-1}-1}(2^{n-1}-1)(2^{n-1}-2)\dots(2^{n-1}-2^{n-2})}.$$

In particular, if $n = 5,\ N(31) \geq 53$.

Theorem. (Octavio Paez Osuna, 2005):
There are exactly 1239 STS(31) of 2-rank 27:
$N(31) = 1239$.

The Proof

A quadrilateral (or Pasch configuration) in an $STS(v)$:
A collection of four blocks and six points such that

- every point is in two blocks;
- every two blocks meet in one point.

Main Observation:

Every $STS(2^n - 1)$ of 2-rank $2^n - n$ can be obtained from the classical one by replacing quadrilaterals in $PG(n-1, 2)$ with quadrilaterals of truncated planes in $AG(n, 2)$.

$SQS(2^n)$ of 2-rank $2^n - n$

Theorem. (Teirlinck 1980)
The 2-rank of an $S = SQS(2^n)$ is greater than or equal to $2^n - n - 1$, with equality if and only if S is isomorphic to the classical $SQS(2^n)$ of the planes in $AG(n, 2)$.

Theorem. (Assmus 1995)
(i) Distinct $SQS(v)$ having the same 2-rank have equivalent codes.
(ii) The code C_n of length 2^n spanned by the classical $SQS(2^n)$ and a vector of weight 2, contains representatives of all nonisomorphic $SQS(2^n)$ of 2-rank $2^n - n$.

Counting $SQS(2^n)$ of 2-rank $2^n - n$

Lemma 1. The vectors of weight 4 in the code C_n are supported by either (a) affine planes, or (b) quadruples of four affine points with constant sum $\bar{1} = (0, 0, \ldots, 1)$.

Lemma 2. (i) The set of codewords of weight 4 of type (a) can be partitioned in a unique way into groups of size 8, each group being a Clifford configuration.
(ii) The set of codewords of weight 4 of type (b) can be partitioned in a unique way into 8-subsets as in Table 1.
(iii) Every 8-set of type (a) forms a matching pair with exactly one set of type (b).

The Clifford 8-configuration

- A collection of 8 points and 8 blocks.
- Every point is in 4 blocks, and every block contains 4 points.
- Every two blocks share an even number of points.
- The configuration is symmetric.

Note. The Clifford configuration consists of 8 blocks of an $STS(8)$.

Table 1

ϕ	$\alpha+\phi$	$\beta+\phi$	$\alpha+\beta+\phi$
ϕ	$\alpha+\phi+\bar{1}$	$\beta+\phi+\bar{1}$	$\alpha+\beta+\phi$
ϕ	$\alpha+\phi+\bar{1}$	$\beta+\phi$	$\alpha+\beta+\phi+\bar{1}$
ϕ	$\alpha+\phi$	$\beta+\phi+\bar{1}$	$\alpha+\beta+\phi+\bar{1}$
$\phi+\bar{1}$	$\alpha+\phi+\bar{1}$	$\beta+\phi+\bar{1}$	$\alpha+\beta+\phi+\bar{1}$
$\phi+\bar{1}$	$\alpha+\phi$	$\beta+\phi$	$\alpha+\beta+\phi+\bar{1}$
$\phi+\bar{1}$	$\alpha+\phi$	$\beta+\phi+\bar{1}$	$\alpha+\beta+\phi$
$\phi+\bar{1}$	$\alpha+\phi+\bar{1}$	$\beta+\phi$	$\alpha+\beta+\phi$

A formula for $SQS(2^n)$

Theorem.

The code C_n contains exactly

$$2^{\frac{2^{n-3}(2^{n-1}-1)(2^{n-2}-1)}{3}}$$

distinct $SQS(2^n)$.

Theorem.

The total number of distinct $SQS(2^n)$'s of 2-rank $2^n - n$ is given by

$$\frac{(2^n)!(2^{\frac{2^{n-3}(2^{n-1}-1)(2^{n-2}-1)}{3}} - 2^{2^{n-1}-n})}{2^{2^{n-1}+\frac{n(n-1)}{2}}(2^{n-1}-1)(2^{n-2}-1)\dots(2^2-1)}.$$

A mass formula for $SQS(2^n)$'s

Theorem.

If D_i, $1 \leq i \leq s$ are representatives of all isomorphism classes of $SQS(2^n)$'s of 2-rank $2^n - n$, then

$$2^{\frac{2^{n-3}(2^{n-1}-1)(2^{n-2}-1)}{3}} - 2^{2^{n-1}-n} = \Sigma_{i=1}^{s} \frac{|Aut(C_n)|}{|Aut(D_i)|}.$$

$SQS(16)$ of 2-rank 12

No.	$\lvert Aut\rvert$	# Distinct in C_4	Weights
1	21504	16	35(16), 48(7), 56(128)
2	3072	112	16(1), 35(16), 43(16)
3	3072	112	32(3), 35(16), 51(48)
4	1536	224	8(1), 35(24), 43(8)
5	1536	224	35(16), 40(3), 48(4)
6	768	448	24(1), 32(2), 35(20)
7	768	448	24(1), 35(16), 43(12)
8	768	448	32(2), 35(16), 40(4)
9	768	448	35(16), 40(4), 48(6)
10	256	1344	16(1), 35(20), 40(2)
11	256	1344	24(1), 35(16), 40(2)
12	256	1344	32(1), 35(16), 40(2)
13	128	2688	32(2), 35(16) 40(2)
14	96	3584	24(1), 32(1), 35(18)
15	96	3584	32(1), 35(16), 40(3)

The Counting Formula

$$2^{14} - 2^4 = 16368 =$$

$$= 344064\left(\frac{1}{21504} + \frac{2}{3072} + \frac{2}{1536} + \frac{4}{768} + \frac{3}{256} + \frac{1}{128} + \frac{2}{96}\right).$$

$SQS(2^n)$ of 2-rank $2^n - n + 1$

Theorem. (V. Zinoviev and D. Zinoviev, 2006).

(i) Every $SQS(2^n)$ of 2-rank $\leq 2^n - n + 1$ is resolvable.

(ii) The resolvable $SQS(2^n)$ of 2-rank $\leq 2^n - n + 1$ can be counted.

References

E.F. Assmus, Jr., On 2-ranks of Steiner triple systems, *Electronic J. Combinatorics* **2** (1995) paper R9.

Octavio Páez Osuna, There are 1239 Steiner triple systems $STS(31)$ of 2-rank 27, *Designs, Codes and Cryptography* **40** (2006), 187-190.

V. D. Tonchev, A mass formula for Steiner triple systems $STS(2^n-1)$ of 2-rank 2^n-n, *J. Combinatorial Theory*, Ser. A 97 (2001), 197-208.

V. D. Tonchev, A formula for the number of Steiner quadruple systems on 2^n points of 2-rank 2^n-n, *J. Combinatorial Designs* **11** (2003), 260-274.

V.A. Zinoviev and D.V. Zinoviev, On the resolvability of Steiner systems $S(v=2^m,4,3)$ of rank $r \leq v-m+1$ over

MUCHAS GRACIAS!