Steiner quadruple systems with abelian regular automorphism group

Akihiro Munemasa[1]

[1]Graduate School of Information Sciences
Tohoku University
(joint work with Masanori Sawa)

RIMS, Kyoto University, January 7, 2009

Steiner system

Steiner systems originated from a problem posed by Steiner (1853), solved by Kirkman (1847). The concept was already introduced by Woolhouse (1844).

A Steiner system (or a Steiner t-design), denoted $S(t, k, v)$, where $t < k < v$ are integers, is a pair $(\mathcal{P}, \mathcal{B})$ with

- $\mathcal{P}$: a set of v "points,"
- $\mathcal{B}$: a family of k-subsets of $\mathcal{P}$, "blocks," "lines," "planes," etc

such that

$$\forall T \in \binom{\mathcal{P}}{t}, \ \exists! B \in \mathcal{B}, \ T \subset B.$$

$t = 2$: $\forall 2$ distinct points $\subset \exists!$ line, every line consists of k points.

$S(t, k, v)$ denotes not necessarily a unique mathematical object. There may be many non-isomorphic $S(t, k, v)$'s for a fixed (t, k, v).

$S(t,k,v)$: $\forall T \in \binom{\mathcal{P}}{t}$, $\exists! B \in \mathcal{B}$, $T \subset B$

Affine space over $\mathbb{F}_q$: $\mathcal{P} = \mathbb{F}_q^n$, $\mathcal{B} = \{\text{lines in } \mathbb{F}_q^n\}$.
$\forall$2 distinct points $\subset \exists!$ line (has size q), $v = |\mathcal{P}| = q^n$

$$\Longrightarrow S(2, q, q^n).$$

$t = 3$: $\forall$3 distinct points $\subset \exists!$?

collinear	non-collinear
line	plane
does not occur if $q = 2$	

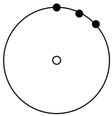
$$\Longrightarrow S(3, 4, 2^n).$$

$S(t,k,v)$: $\forall T \in \binom{\mathcal{P}}{t}$, $\exists! B \in \mathcal{B}$, $T \subset B$

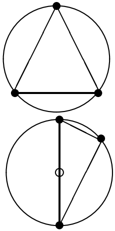
$t \geq 4$: Only finitely many $S(t,k,v)$ known.
Witt (1938): $S(4,5,11)$, $S(5,6,12)$, etc. (Mathieu groups)
Can't expect any more from 4-transitive groups (Mathieu groups are the only nontrivial 4-transitive ones, by CFSG)
If we are to prove there are infinitely many (too ambitious), we need a unified algebraic approach.
$t = 2$: affine space over $\mathbb{F}_q$ is a unified construction, but not clear for $t > 3$.
(Be modest): first understand completely known algebraic construction of $S(3,k,v)$. Hope to see why $t > 3$ is so different from $t \leq 3$.
(Be even more modest): first understand completely known algebraic construction of $S(3,4,v)$ (called a Steiner quadruple system, denoted SQS(v))

$\forall T \in \binom{\mathcal{P}}{3},\ \exists! B \in \mathcal{B},\ T \subset B$
Steiner quadruple systems SQS$(v) = S(3,4,v)$

Theorem (Hanani, 1963) $\exists$ SQS$(v) \iff v \equiv 2$ or $4 \pmod 6$.
Cyclic SQS(v): $\mathcal{P} = \{\xi \in \mathbb{C} \mid \xi^v = 1\}$.



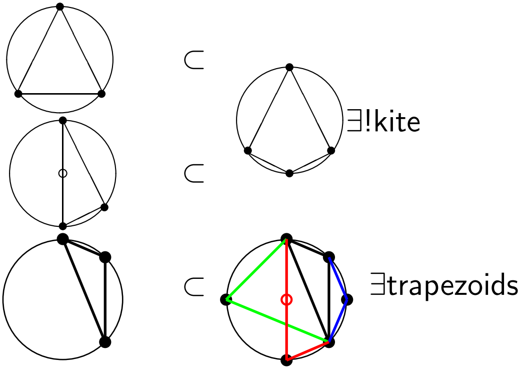
$$\binom{\mathcal{P}}{3} = \text{triangles} = \begin{cases} \text{isosceles} \\ \text{right} \\ \text{ordinary} \end{cases}$$



Find a family of quadrangles $\mathcal{B}$ such that

$$\forall T \in \binom{\mathcal{P}}{3},\ \exists! B \in \mathcal{B},\ T \subset B$$

$\mathrm{SQS}(v) = S(3,4,v)$ $v \equiv 2$ or $4 \pmod 6$
$\mathcal{P} = \{\xi \in \mathbb{C} \mid \xi^v = 1\}$, $\forall \triangle \subset \exists! \square \in \mathcal{B}$



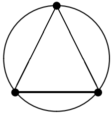
ordinary triangle$\not\subset$kite

isosceles, right triangle$\not\subset$trapezoid ($\not\supset$diameter)

$\mathcal{B} = \{$all kites$\} \cup \{$some trapezoids$\}$:

Example: $v = 10$. Take all trapezoids $\not\supset$ diam. $\implies$ SQS(10).

$\mathcal{P} = \{\xi \in \mathbb{C} \mid \xi^v = 1\}$, $\forall \triangle \subset \exists! \square \in \mathcal{B}$ triangle $\subset$ kite or trapezoid



- We have implicitly assumed symmetry under the dihedral group D_v of order $2v$.
- $\exists ?$ SQS(v) invariant under D_v
- No such SQS(8) (but $\exists$ SQS(8) on $\mathbb{F}_2^3$)
- It may not be a good idea to stick to cyclic groups or dihedral groups for assumed symmetry. (Quite a lot of work has been done for cyclic case, nevertheless)

SQS(v) as a $(0,1)$-solution to a linear equation

$$\begin{array}{cc} & B \in \binom{\mathcal{P}}{4} \supset \mathcal{B} \\ T \in \binom{\mathcal{P}}{3} & \left[\begin{cases} 1 & T \subset B \\ 0 & T \not\subset B \end{cases} \right] \end{array} \begin{bmatrix} 0 \\ \text{or} \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$$

A solution is the characteristic vector of a subset $\mathcal{B}$, forming SQS(v):

$$\forall T \in \binom{\mathcal{P}}{3},\ \exists! B \in \mathcal{B},\ T \subset B.$$

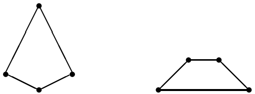
SQS(v) invariant under G acting on $\mathcal{P}$

$$
\begin{array}{cc}
 & B \in \binom{\mathcal{P}}{4} \\
T \in \binom{\mathcal{P}}{3} & \left[\begin{cases} 1 & T \subset B \\ 0 & T \not\subset B \end{cases} \right]
\end{array}
\begin{bmatrix} 0 \\ \text{or} \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}
$$

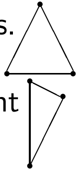
A permutation group G on $\mathcal{P}$ allows to collapse the matrix:

$$
\begin{array}{cc}
 & B \in \binom{\mathcal{P}}{4}/G \\
T \in \binom{\mathcal{P}}{3}/G & \left[\begin{cases} \geq 1 & T \subset B \\ 0 & T \not\subset B \end{cases} \right]
\end{array}
\begin{bmatrix} 0 \\ \text{or} \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}
$$

Collapsing $\binom{\mathcal{P}}{3} \times \binom{\mathcal{P}}{4}$ matrix by D_v



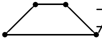
$\not\supset$diam.



$$\binom{\mathcal{P}}{3}\left\{\begin{array}{l}\text{isos.}\\ \\ \text{right}\\ \\ \text{ordinary}\end{array}\right. \left[\begin{array}{c|c|c} 0\cdots1\cdots0 & 0\cdots0 & * \\ \cdots & \vdots & \vdots \\ \hline 10\cdots\cdots0 & 0\cdots0 & * \\ \cdots & \vdots & \vdots \\ \hline 0 & * & * \end{array}\right] \left[\begin{array}{c} 1 \\ \hline \color{red}{0} \\ \color{red}{\text{or}} \\ \color{red}{1} \\ \hline 0 \end{array}\right] = \begin{bmatrix} 1 \\ \vdots \\ 1 \\ \vdots \\ 1 \end{bmatrix}$$

$$\begin{array}{c} \color{red}{\text{collapse}} \\ \Longrightarrow \\ \binom{\mathcal{P}}{3}/\color{red}{D_v} \end{array} \left[\begin{array}{c|c|c} 0\cdots1\cdots0 & 0\cdots0 & * \\ \cdots & \vdots & \vdots \\ \hline 10\cdots\cdots0 & 0\cdots0 & * \\ \cdots & \vdots & \vdots \\ \hline 0 & \color{red}{K} & * \end{array}\right] \left[\begin{array}{c} 1 \\ \hline \color{red}{0} \\ \color{red}{\text{or}} \\ \color{red}{1} \\ \hline 0 \end{array}\right] = \begin{bmatrix} 1 \\ \vdots \\ 1 \\ \vdots \\ 1 \end{bmatrix}$$

Collapsing $\binom{\mathcal{P}}{3} \times \binom{\mathcal{P}}{4}$ matrix by D_v

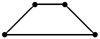


$\not\supset$ diam.

$$\begin{array}{rc} & \binom{\mathcal{P}}{4}/D_v \\ \begin{array}{r} \binom{\mathcal{P}}{3}/D_v \\ \\ \text{ordinary}\{ \end{array} & \left[\begin{array}{c|c|c} 0\cdots1\cdots0 & 0\cdots0 & * \\ \cdots & \vdots & \vdots \\ \hline 10\cdots\cdots0 & 0\cdots0 & * \\ \cdots & \vdots & \vdots \\ \hline 0 & K & * \end{array}\right] \left[\begin{array}{c} 1 \\ \hline 0 \\ \text{or} \\ 1 \\ \hline 0 \end{array}\right] = \left[\begin{array}{c} 1 \\ \vdots \\ 1 \\ \vdots \\ 1 \end{array}\right] \end{array}$$

- K has at most three 1's in each row
- K has exactly two 1's in each column (∀trapezoid⊃two triangles/ ≡)
- K can be regarded as an incidence matrix of a graph (columns=edges, rows=vertices)

Incidence matrix

 $\not\supset$ diam.

$$\begin{array}{cc} & \text{edges} \\ \text{vertices=ordinary} & \begin{bmatrix} & & \\ & K & \\ & & \end{bmatrix} \end{array} \begin{bmatrix} 0 \\ \text{or} \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$$

$$\begin{array}{cc} & \text{edges} \\ \text{vertices} & \begin{bmatrix} & & \\ & K & \\ & & \end{bmatrix} \end{array} \begin{bmatrix} 0 \\ \text{or} \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \iff \begin{array}{l} \text{1-factor} \\ \text{of the graph } K \end{array}$$

1-factor $\iff$ a subset of edges covering every vertex exactly once

Köhler (1979) $\mathcal{P} = \{\xi \mid \xi^v = 1\}$

- $v \equiv 2$ or $4 \pmod 6$
- $\mathcal{T} = \{$ ordinary triangles $\subset \mathcal{P}\}$/cong.: vertices
- $\mathcal{E} = \{$ trapezoids $\not\ni$diam.$\}$/cong.: edges
- The Köhler graph $\mathcal{G}(\mathbb{Z}_v)$ is $(\mathcal{T}, \mathcal{E})$, K: its incidence matrix

A solution to

$$\begin{bmatrix} & & \\ & K & \\ & & \end{bmatrix} \begin{bmatrix} 0 \\ \text{or} \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$$

corresponds to a subset $\mathcal{F}$ of edges with

$$\forall\text{vertex} \subset \exists!\text{member of } \mathcal{F}.$$

called a 1-factor.

Theorem (Köhler)

$\exists$1-factor in $\mathcal{G}(\mathbb{Z}_v) \implies \exists\,\mathrm{SQS}(v)$.

$\exists$1-factor in $\mathcal{G}(\mathbb{Z}_v) \implies \exists\,\mathrm{SQS}(v)$.

Piotrowski (1985)

- $\exists$1-factor in $\mathcal{G}(\mathbb{Z}_v)$ for infinitely many v
- existence of a 1-factor in $\mathcal{G}(\mathbb{Z}_v)$ reduces to the case $v = 2p$, p: odd prime

Still an open problem: Determine v such that $\exists$1-factor in $\mathcal{G}(\mathbb{Z}_v)$.

$\implies$ Leads to a number theoretic problem.

Our approach:

- A: abelian group of order v
- define "isosceles", "right" triangles in $\binom{A}{3}$
- define "kite", "trapezoid" in $\binom{A}{4}$
- define the Köhler graph $\mathcal{G}(A)$ of A

Theorem (joint work with M. Sawa)

$\exists$1-factor in $\mathcal{G}(A) \implies \exists\,\mathrm{SQS}(v)$.