

Steiner quadruple systems with abelian regular automorphism group

東北大学大学院情報科学研究科 宗政昭弘 (Akihiro Munemasa)

Graduate School of Information Sciences,

Tohoku University

1 Introduction

The contents of this talk is based on a joint work with Masanori Sawa [7]. Steiner systems originated from a problem posed by Steiner (1853), but it had already been solved by Kirkman (1847). The concept itself was also introduced by Woolhouse (1844). We refer the reader to van Lint–Wilson [5] for early history of the subject.

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} is a set of v “points,”
- \mathcal{B} is a family of k -subsets of \mathcal{P} , called “blocks,” “lines,” “planes,” etc

such that

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

When $t = 2$, the condition above can be expressed intuitively as follows:

any two distinct points are contained in exactly one line, and
every line consists of k points.

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

The affine space over \mathbb{F}_q is an example of a Steiner 2-design. Let $\mathcal{P} = \mathbb{F}_q^n$, $\mathcal{B} = \{\text{lines in } \mathbb{F}_q^n\}$. Then any two distinct points are contained in exactly one line, and every line consists of q points. The total number of points is $v = |\mathcal{P}| = q^n$. This means that we have an $S(2, q, q^n)$.

If we try to state the condition again in a geometrical language for $t = 3$, then one may realize that it is not natural. This is because, generally speaking, there are two kinds of sets of three points, namely, collinear sets of

points and non-collinear sets of points. However, the former does not occur if $q = 2$, hence every triple of points in an affine space over \mathbb{F}_2 determines a unique plane. This leads to an $S(3, 4, 2^n)$.

The situation is quite different for $t \geq 4$. In fact, there are only finitely many $S(t, k, v)$ known for $t \geq 4$, and it is not known whether there are infinitely many. The most famous $S(t, k, v)$'s with $t \geq 4$ are those associated to the Mathieu groups: $S(4, 5, 11)$, $S(5, 6, 12)$, $S(4, 7, 23)$ and $S(5, 8, 24)$. The uniqueness of these designs was proved by Witt [12] in 1938.

Multiple transitivity of the Mathieu groups could be considered to be the reason for the existence of these designs. However, as a consequence of the classification of finite simple groups, there are no other nontrivial 4-transitive groups, so one cannot expect any more 4-designs arising in this way.

If we are to prove there are infinitely many (too ambitious), we need a unified algebraic approach. For $t = 2$, the construction of the affine space over \mathbb{F}_q can be regarded as a unified construction, but analogous construction is not known for $t > 3$. So let us try to be modest. First understand completely the known algebraic construction of $S(3, k, v)$, and hope to see why $t > 3$ is so different from $t \leq 3$. Among $S(3, k, v)$'s, the smallest possible value of k is 4, so let us first understand completely the known algebraic construction of $S(3, 4, v)$ (called a Steiner quadruple system, denoted $\text{SQS}(v)$).

Theorem 1 (Hanani, 1963). There exists an $\text{SQS}(v)$ if and only if $v \equiv 2$ or $4 \pmod{6}$.

Though best possible and beautiful, the proof of this theorem [3] does not seem to give a unified algebraic construction for all of the $\text{SQS}(v)$'s.

In the following, we try to set up a unified construction based on a geometric consideration which is then turned to an algebraic one. A major disadvantage is that one cannot obtain $\text{SQS}(v)$ for some v 's, but for infinitely many other v 's, an $\text{SQS}(v)$ will be constructed. After all, there may not exist a unified construction which works for all v 's. It is our strategy that the nicest method is the one we should first investigate for a possible generalization for higher values of t in the future.

A Steiner quadruple system $\text{SQS}(v)$ whose set of points is $\mathcal{P} = \{\xi \in \mathbb{C} \mid \xi^v = 1\}$ can be conveniently described by polygons on the unit circle. There

are three kinds of triangles:

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

Then, a Steiner quadruple system can be constructed if we supply with a family of quadrangles \mathcal{B} such that

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

Every isosceles triangle and every right triangle are contained in a unique kite, and every ordinary triangle (other than isosceles and right triangles) is contained in some trapezoids not containing a diameter. So it seems reasonable to take $\mathcal{B} = \{\text{all kites}\} \cup \{\text{some trapezoids}\}$, but how to choose an appropriate set of trapezoids is not clear at the moment.

Example 2. For $v = 10$, taking *all* trapezoids not containing a diameter gives an $\text{SQS}(10)$.

When we take the set of points to be $\mathcal{P} = \{\xi \in \mathbb{C} \mid \xi^v = 1\}$ then we have implicitly assumed symmetry under the dihedral group D_v of order $2v$. Does there exist an $\text{SQS}(v)$ invariant under D_v ? No such $\text{SQS}(8)$ exists, but certainly there exists an $\text{SQS}(8)$ on \mathbb{F}_2^3 which is the 3-dimensional affine space over \mathbb{F}_2 . So, it may not be a good idea to stick to *cyclic* groups or *dihedral* groups for assumed symmetry. We note that quite a lot of work has been done for the cyclic case, nevertheless.

Formally, the definition of a Steiner quadruple system can be expressed in terms of $(0, 1)$ -solution of a system of linear equations whose coefficient is the “inclusion matrix,” which is the matrix whose rows and columns are indexed by $\binom{\mathcal{P}}{3}$, $\binom{\mathcal{P}}{4}$, respectively, and (T, B) -entry is 1 or 0 according as $T \subset B$ or not.

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

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

A permutation group G on \mathcal{P} allows to *collapse* the matrix, and we are to seek for a solution which is the characteristic vector of a union of some orbits of G on $\binom{\mathcal{P}}{4}$.

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

Let us consider the special case where $\mathcal{P} = \{\xi \in \mathbb{C} \mid \xi^v = 1\}$ and G is the dihedral group of order $2v$. If we group the rows (resp. columns) according to the shape of a triangle (resp. a quadruple), then

$$\left(\begin{array}{c} P \\ 3 \end{array} \right) \left\{ \begin{array}{l} \text{isos.} \\ \text{right} \\ \text{ordinary} \end{array} \right. \left[\begin{array}{c|c|c} 0 \cdots 1 \cdots 0 & 0 \cdots 0 & * \\ \dots & \vdots & \vdots \\ 10 \cdots \cdots 0 & 0 \cdots 0 & * \\ \dots & \vdots & \vdots \\ 0 & * & * \end{array} \right] \left[\begin{array}{c} 1 \\ 0 \\ or \\ 1 \\ 0 \end{array} \right] = \left[\begin{array}{c} 1 \\ \vdots \\ 1 \\ \vdots \\ 1 \end{array} \right]$$

Here the first set of columns correspond to kites, the second set to trapezoids not containing a diameter, and the third to the remaining quadrangles. From now on, by a trapezoid we always mean a trapezoid not containing a diameter. We seek for solutions which has 1's in the first set of coordinates, 0's in the third sets. This is to assume that the set of blocks contains all kites, and contains no quadrangles other than kites or trapezoids. Then it is clear that the only nontrivial part of the equations is how to choose trapezoids which cover ordinary triangles evenly. Since these geometrical concepts are invariant under the action of the dihedral group D_v of order $2v$, we may collapse the coefficient matrix and seek for a solution which is invariant under D_v . We denote by K the matrix obtained from the submatrix of the inclusion matrix corresponding to rows of ordinary triangles and columns of trapezoids, by collapsing under the action of D_v .

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

The matrix K has the following properties:

- K has *at most* three 1's in each row. This is because every ordinary triangle is contained in at most three trapezoids up to congruence,
- K has exactly two 1's in each column. This is because every trapezoid contains exactly two ordinary triangles up to congruence.

Therefore, K can be regarded as an incidence matrix of a *graph*. The set of vertices are the rows of K which are the congruence classes of ordinary triangles, and the set of edges are the columns of K which are the congruence classes of trapezoids. Then the above system of linear equations reduces to the following.

$$\left[\begin{array}{c} K \end{array} \right] \left[\begin{array}{c} 0 \\ \text{or} \\ 1 \end{array} \right] = \left[\begin{array}{c} 1 \\ \vdots \\ 1 \end{array} \right]$$

A solution to such a system of equations (i.e., K is the vertex-edge incidence matrix of a graph), is the characteristic vector of a *1-factor* of the graph. More precisely, a 1-factor of a graph is a subset of edges covering every vertex exactly once.

To summarize, we have realized that the importance of the graph defined by its incidence matrix K which can be constructed as follows:

- $\mathcal{T} = \{ \text{ordinary triangles} \subset \mathcal{P} \}/\text{cong.: vertices}$
- $\mathcal{E} = \{ \text{trapezoids } \not\supset \text{diam.} \}/\text{cong.: edges}$
- K : its incidence matrix, where the incidence is defined by inclusion of representatives.

We call the resulting graph $(\mathcal{T}, \mathcal{E})$ the *Köhler graph*, denoted $\mathcal{G}(\mathbb{Z}_v)$, since Köhler [4] was the first to state the above observation formally.

Theorem 3 (Köhler). If there exists a 1-factor in $\mathcal{G}(\mathbb{Z}_v)$, then there exists an $\text{SQS}(v)$ invariant under D_v .

A picture of a Köhler graph appeared much earlier. Already in 1915, Fitting [2] seems to have noticed Köhler's method. Piotrowski [9] proved the following:

- there exists a 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 $v = 2p$, where p is an odd prime.

Still an open problem is to determine v such that there exists a 1-factor in $\mathcal{G}(\mathbb{Z}_v)$. This leads to a number theoretic problem. See Siemon [10, 11] for details.

In this talk, we generalize Köhler's method to arbitrary finite abelian groups. In the next section, we let A be an abelian group of order v , and

- define “isosceles”, “right” triangles in $\binom{A}{3}$,
- define “kite”, “trapezoid” in $\binom{A}{4}$,
- define the Köhler graph $\mathcal{G}(A)$ of A .

Then we have the following result.

Theorem 4 (joint work with M. Sawa). If there exists a 1-factor in $\mathcal{G}(A)$, then there exists an $\text{SQS}(v)$ invariant under A .

2 The Köhler graph of an abelian group

Throughout this section, we let A be an abelian group of order v . We regard A as a permutation group acting on A regularly, and form the semidirect product $\hat{A} = A \rtimes \langle \sigma \rangle$, where σ is the automorphism of A defined by $a^\sigma = -a$. The group \hat{A} is a permutation group on A . For distinct nonzero elements a, b of A , we denote by $[a, b]$ the orbit of $\{0, a, b\}$ under the action of \hat{A} . We define isosceles, right, and ordinary triangles formally as follows:

$$\begin{aligned}\mathcal{T}_1 &= \{[a, -a] \mid a \in A, 2a \neq 0\}, \\ \mathcal{T}_2 &= \{[a, b] \mid a \in A \setminus \{0\}, b \in A \setminus \{0, a\}, 2b = 0\}, \\ \mathcal{T} &= \{[a, b] \mid \{0, a, b\} \in \binom{A}{3}, [a, b] \notin \mathcal{T}_1 \cup \mathcal{T}_2\}\end{aligned}$$

$$= \{[a, b] \mid a \neq \pm b, 2a \notin \{0, b, 2b\}, 2b \notin \{0, a, 2a\}\}.$$

If $A = \{\xi \in \mathbb{C} \mid \xi^v = 1\}$, then \mathcal{T}_1 is the congruence classes of isosceles triangles, and \mathcal{T}_2 is the congruence classes of right triangles.

We aim to define a graph on \mathcal{T} by adjacency induced by trapezoids. One could define edges by properly defining trapezoids, but it is somewhat complicated, so we define neighbors instead.

The Köhler graph $\mathcal{G}(A)$ has \mathcal{T} as the set of its vertices, and a vertex $[a, b]$ is adjacent to

$$[a, a+b], [a, b-a], [b, a-b] \quad (1)$$

provided they belong to \mathcal{T} . It is important to note that even if $[a, b]$ belongs to \mathcal{T} , some or all of $[a, a+b], [a, b-a], [b, a-b]$ may not belong to \mathcal{T} . So the degree of a vertex $[a, b]$ is at most 3, and it can be less than 3 in general.

Example 5. If $A = \mathbb{Z}_4 \times \mathbb{Z}_4$, then the graph $\mathcal{G}(A)$ is the cube. If $A = \mathbb{Z}_{20}$, then the graph $\mathcal{G}(A)$ is isomorphic to the union of a 6-cycle and three isolated edges.

In Example 5, the graph $\mathcal{G}(A)$ obviously has a 1-factor. The following lemma is immediate from the definition of the neighbors (1).

Lemma 6. Suppose that $[a, b] \in \mathcal{T}$ and $[c, d] \in \mathcal{T}$ belong to the same connected component of \mathcal{G} . Then $\langle a, b \rangle = \langle c, d \rangle$.

Lemma 7. Let A' be a subgroup of A . Then the Köhler graph of A' is isomorphic to a union of connected components of \mathcal{G} .

It follows from Lemmas 6 and 7 that every connected component of the Köhler graph of A is isomorphic to a connected component of the Köhler graph of a subgroup of A generated by two elements. In particular, by Example 5, we see that there exists a 1-factor in the Köhler graph of A whenever A is an abelian 2-group of exponent 4. Note that if A is an elementary abelian 2-group of order v , then the Köhler graph is empty, and we always have an $\text{SQS}(v)$ as the affine space over \mathbb{F}_2 .

In view of Theorem 4, our aim now is to show the existence of a 1-factor in the graph $\mathcal{G}(A)$ for as many classes of abelian groups A as possible.

As one can guess from the definition of the neighbors (1), in majority of cases, the elements (1) are distinct and all belong to \mathcal{T} . In such a case, the vertex $[a, b]$ has degree exactly 3. In fact, a careful analysis reveals the following.

Lemma 8. The degree of a vertex $[a, b] \in \mathcal{T}$ is 3 if and only if

$$0 \notin \{2a + b, a + 2b, 2a + 2b, 3a - b, 3a - 2b, 4a - 2b, 3b - a, 3b - 2a, 4b - 2a\}.$$

A direct consequence of this lemma and Lemma 6 is the following.

Proposition 9. Suppose $[a, b] \in \mathcal{T}$. If $\langle a, b \rangle$ is not cyclic, $|\langle a, b \rangle| \not\equiv 0 \pmod{3}$ and the Sylow 2-subgroup is either cyclic or contains $\mathbb{Z}_4 \times \mathbb{Z}_4$, then the connected component of the Köhler graph containing the vertex $[a, b]$ is 3-regular.

Proof. Suppose that the degree of the vertex $[a, b]$ is less than 3. Since $\langle a, b \rangle$ is not cyclic and $|\langle a, b \rangle| \not\equiv 0 \pmod{3}$, Lemma 8 implies

$$0 \in \{2a + 2b, 4a - 2b, 4b - 2a\}.$$

In other words, one of $a + b$, $2a - b$, $2b - a$ is an involution. This implies that $\langle a, b \rangle$ is generated by an involution c together with an element $d \in \{a, b\}$ and, as $\langle a, b \rangle$ is not cyclic, d has an even order. Thus the Sylow 2-subgroup of $\langle a, b \rangle$ is not cyclic, and $\langle a, b \rangle \cong \langle c \rangle \oplus \langle d \rangle$ does not contain $\mathbb{Z}_4 \times \mathbb{Z}_4$. \square

In some cases, the connected component of the Köhler graph containing a vertex $[a, b]$ is not only 3-regular, but also bridgeless, that is, the removal of an edge does not disconnect the graph. It is well known in graph theory ([8], see also [6, p.59]) that any bridgeless 3-regular graph has a 1-factor.

We conclude our report by indicating a possible group theoretical approach. Let D_6 denote the following subgroup of $\mathrm{GL}_2(\mathbb{Z})$:

$$D_6 = \left\langle \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle.$$

The group D_6 is isomorphic to the dihedral group of order 12. Note that $\mathrm{GL}_2(\mathbb{Z})$ acts on $A \times A$ (from the right), and so does D_6 .

If $\{0, a, b\} \in \binom{A}{3}$, then

$$(a, b)D_6 = \{(c, d) \in A \times A \mid \{0, c, d\} \in [a, b]\}.$$

This means that we can identify $(a, b)D_6$ with $[a, b]$, so we have an embedding

$$\mathcal{T} \subset \binom{A}{3}/\hat{A} \hookrightarrow A \times A/D_6.$$

The definition of the neighbors (1) implies that the neighbors of $(a, b)D_6$ are

$$(a, b)x D_6 \quad \left(x \in \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \right\} \right). \quad (2)$$

Note that $\mathrm{GL}_2(\mathbb{Z})$ is generated by D_6 together with the three matrices in (2), which can be seen from a well known set of generators for $\mathrm{SL}_2(\mathbb{Z})$, see [1, Exercise 1.1.1, p.7]. This might suggest that the connected component of the Köhler graph containing a given vertex $(a, b)D_6$ can be identified with the double coset $H \backslash \mathrm{GL}_2(\mathbb{Z}) / D_6$, where H is the stabilizer of (a, b) in $\mathrm{GL}_2(\mathbb{Z})$. However, this is not true in general, since some element $(a, b)x$ with $x \in \mathrm{GL}_2(\mathbb{Z})$ may not belong to \mathcal{T} . One can think of those outside \mathcal{T} as “singular points,” because these points make the structure of the graph irregular.

References

- [1] F. Diamond and J. Shurman, A First Course in Modular Forms, Springer, 2005.
- [2] F. Fitting, Zyklische Lösung des Steinerschen Problems, Nieuw. Arch. Wisk., **11** (1915), 140–148.
- [3] H. Hanani, On some tactical configurations, Canad. J. Math., **15** (1963), 705–722.
- [4] E. Köhler, Zyklische Quadrupelsysteme, Abh. Math. Sem. Univ. Hamburg, **48** (1979), 1–24.
- [5] J. H. van Lint and R. M. Wilson, A Course on Combinatorics, 2nd ed., Cambridge University Press, 2001.
- [6] L. Lovász, Combinatorial Problems and Exercises, 2nd ed., North-Holland, 1993.
- [7] A. Munemasa and M. Sawa, Steiner quadruple systems with point-regular abelian automorphism groups, preprint.
- [8] J. Petersen, Die Theorie der regulären graphs, Acta Math., **15** (1891), 193–220.

- [9] W. Piotrowski, Untersuchungen über S-zyklische Quadrupelsysteme, Diss. Univ. Hamburg, 1985.
- [10] H. Siemon, A number-theoretic conjecture and the existence of S -cyclic Steiner quadruple systems, Des. Codes Cryptogr., **13** (1998), 63–94.
- [11] H. Siemon, Some remarks on the construction of cyclic Steiner quadruple systems, Arch. Math. (Basel), **49** (1987), 166–178.
- [12] E. Witt, Über Steinersche systeme, Abh. Math. Sem. Univ. Hamburg, **12** (1938), 265–275.