

On transversal designs and their automorphism groups

熊本大学・教育学部 平峰 豊
Yutaka Hiramine

Department of Mathematics, Faculty of Education,
Kumamoto University,
Kurokami, Kumamoto, Japan
hiramine@kumamoto-u.ac.jp

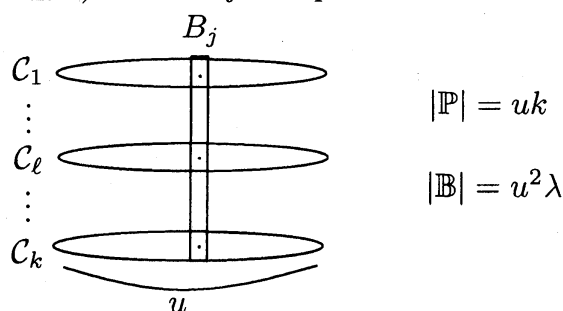
In this talk we consider automorphism groups SCTs of transversal designs acting regularly on the set of point classes and determine the relations among SCTs, RDSs and λ -planar functions.

1 Transversal Designs and Difference Matrices

Definition 1.1. A transversal design $\text{TD}_\lambda(k, u)$ ($u > 1$) is an incidence structure $\mathcal{D} = (\mathbb{P}, \mathbb{B})$, where

- (i) $\mathbb{P}$ is a set of uk points partitioned into k classes $\mathcal{C}_1, \dots, \mathcal{C}_k$ (called *point classes*), each of size u ,
- (ii) $\mathbb{B}$ is a collection of k -subsets of $\mathbb{P}$ (called *blocks*),
- (iii) Any two distinct points in the same point class are incident with no blocks and any two points in distinct point classes are incident with exactly λ blocks.

By definition, $|\mathbb{P}| = uk$, $|\mathbb{B}| = u^2\lambda$ and every block B_j of $\mathbb{B}$ intersects in each point class $\mathcal{C}_\ell$ ($1 \leq \ell \leq k$) in exactly one point.



Example 1.2. Set $F = GF(q)$. Then the following is a $\text{TD}_1(q, q)$.

$\mathbb{P} = F \times F$, $\mathbb{B} = \{y = ax + b \mid a, b \in F\}$, $\mathcal{C} = \{\mathcal{C}_i := \{i\} \times F \mid i \in F\}$.

Transversal designs and their automorphism groups

Let $\mathcal{D} = (\mathbb{P}, \mathbb{B})$ be a $\text{TD}_\lambda(k, u)$ with k point classes $\mathcal{C}_1, \dots, \mathcal{C}_k$ and let U be a subgroup of $\text{Aut}(\mathcal{D})$ acting regularly on each $\mathcal{C}_i$. Choose $p_i \in \mathcal{C}_i$ ($1 \leq i \leq k$) and let $B_1U, \dots, B_{u\lambda}U$ be the U -orbits on $\mathbb{B}$. Then a $k \times u\lambda$ matrix

$\begin{bmatrix} d_{1,1} & \cdots & d_{1,u\lambda} \\ \vdots & & \vdots \\ d_{k,1} & \cdots & d_{k,u\lambda} \end{bmatrix}$ defined by $p_i d_{ij} \in B_j$ ($d_{ij} \in U$) has the following property.

$$d_{i,1}d_{\ell,1}^{-1} + \cdots + d_{i,u\lambda}d_{\ell,u\lambda}^{-1} = \lambda U \quad (\in \mathbb{Z}[U]), \quad \forall i \neq \ell$$

Difference matrices

Definition 1.3. Let U be a group of order u and $k, \lambda \in \mathbb{N}$

A $k \times u\lambda$ matrix $\begin{bmatrix} d_{1,1} & \cdots & d_{1,u\lambda} \\ \vdots & & \vdots \\ d_{k,1} & \cdots & d_{k,u\lambda} \end{bmatrix}$ ($d_{ij} \in U$) is called a (u, k, λ) -**difference matrix** over U (a (U, k, λ) -**DM**) if

$$d_{i,1}d_{\ell,1}^{-1} + \cdots + d_{i,u\lambda}d_{\ell,u\lambda}^{-1} = \lambda U \in \mathbb{Z}[U] \quad (\forall i \neq \ell)$$

Example 1.4. The following is a $(3, 3, 1)$ -DM over $(\mathbb{Z}_3, +)$.

$$M = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix}$$

Transversal designs obtained from difference matrices

Definition 1.5. Let $D = [d_{ij}]$ be a (u, k, λ) -difference matrix over a group U of order u . A transversal design $\text{TD}_\lambda(k, u)$ $\mathcal{D}_D(\mathbb{P}, \mathbb{B})$ is obtained from D in the following way:

$$\mathbb{P} = \{1, \dots, k\} \times U$$

$$\mathbb{B} = \{ \{ (1, d_{1,j}g), (2, d_{2,j}g), \dots, (k, d_{k,j}g) \} \mid 1 \leq j \leq u\lambda, g \in U \}$$

We note that $\{1\} \times U, \dots, \{k\} \times U$ is the point classes of $(\mathbb{P}, \mathbb{B})$.

Example 1.6. The following is a $\text{TD}_1(3, 3)$ obtained from M in Example 1.4.

$$\mathbb{P} = \{1, 2, 3\} \times \mathbb{Z}_3,$$

$$\mathbb{B} = \left\{ \left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} (0) \right\}, \left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} (1) \right\}, \left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} (2) \right\}, \left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} (0) \right\}, \left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} (1) \right\}, \left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} (2) \right\}, \left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} (0) \right\}, \left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} (1) \right\}, \left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} (2) \right\} \right\},$$

$\mathfrak{C}$ (the point classes) : $\{1\} \times \mathbb{Z}_3, \{2\} \times \mathbb{Z}_3, \{3\} \times \mathbb{Z}_3$.

Difference matrices and orthogonal arrays

Let $U = \{g_1, \dots, g_u\}$ be a group of order u . A $k \times u\lambda$ (U, k, λ) -DM $D = [d_{ij}]$ is said to be *normalized* if each entry in its first row and column is equal to the identity of U .

Remark 1.7. Let notations be as mentioned above. Assume $[d_{ij}]$ is normalized. Then $(Dg_1, Dg_2, \dots, Dg_u)$ is an $OA_\lambda(k, u)$ ([13]) with entries from U . Denote by $d_i = (d_{i1}, \dots, d_{iu\lambda})$ the i -th row of $[d_{ij}]$. If $\lambda = 1$, then the following is a set of $k - 1$ mutually orthogonal Latin squares.

$$\begin{bmatrix} d_2 g_1 \\ \vdots \\ d_2 g_u \end{bmatrix}, \begin{bmatrix} d_3 g_1 \\ \vdots \\ d_3 g_u \end{bmatrix}, \dots, \begin{bmatrix} d_k g_1 \\ \vdots \\ d_k g_u \end{bmatrix}$$

The following results on difference matrices are well known.

Result 1.8. (D. Jungnickel ([6])) If there exist a (u, k, λ) -DM then $k \leq u\lambda$.

The above result says that the $TD_\lambda(k, u)$ obtained from a (u, k, λ) -DM must satisfy $k \leq u\lambda$. However, in general, the following holds.

Result 1.9. (Drake-Jungnickel [7]) If there exists a $TD_\lambda(k, u)$, then

$$(*) \quad k \leq (u^2\lambda - 1)/(u - 1).$$

Example 1.10. Examples are known satisfying the equality in $(*)$ ([13] Proposition I.7.10). For example, there actually exist a $TD_2(7, 2)$ and a $TD_3(11, 2)$.

Given $u > 0$ and $\lambda > 0$, the number of rows k of a (u, k, λ) -DM over a group U of order u depends on the group of U .

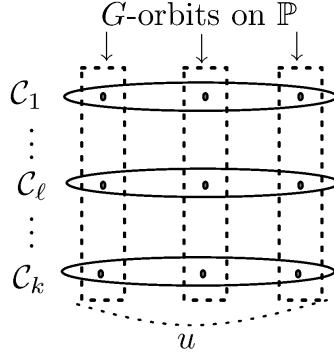
Result 1.11. (D. A. Drake [3]) Let U be any group of even order u with a cyclic Sylow 2-subgroup. If M is a (u, k, λ) -DM over U with $2 \nmid \lambda$, then $k \leq 2$.

For example, it is well known that no $(2, 2n, n)$ -DM (i. e. Hadamard matrix) exists for any odd integer $n > 1$. In general, if $2 \nmid \lambda$, there exists no $(2, k, \lambda)$ -DM for $k \geq 3$.

In what follows we use a notation $I_m = \{1, 2, \dots, m\}$ for positive integer m .

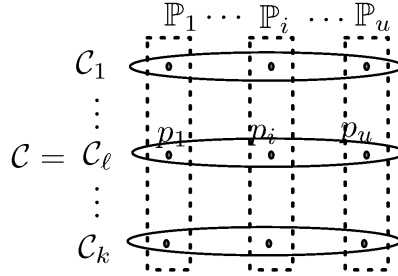
2 SCT groups

Definition 2.1. Let $\mathcal{D}(\mathbb{P}, \mathbb{B})$ be a transversal design $\text{TD}_\lambda(k, u)$ with the set of point classes $\mathfrak{C} = \{\mathcal{C}_i \mid i \in I_k\}$, where $|\mathbb{P}| = uk$, $|\mathbb{B}| = u^2\lambda$ and $|\mathcal{C}_i| = u, i \in I_k$. Let G be an automorphism group of $\mathcal{D}$. We say G is *class-transitive* if G is transitive on $\mathfrak{C}$. If G is a class-transitive group of order k and acts semi-regularly on $\mathbb{B}$, we say G is an *SCT*(u, k, λ) *group*. We note that G is semiregular on $\mathbb{P}$.



In the rest of this article we use the following notations.

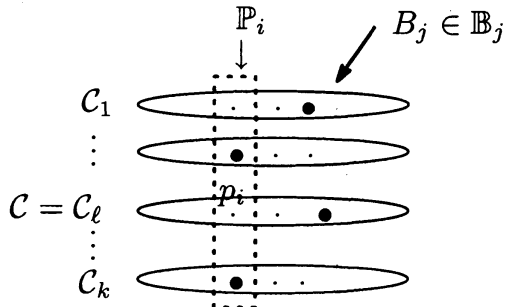
Notation 2.2. Let $\mathcal{D}(\mathbb{P}, \mathbb{B})$ be a transversal design $\text{TD}_\lambda(k, u)$, where $|\mathbb{P}| = uk$ and $|\mathbb{B}| = u^2\lambda$ with the set of point classes $\{\mathcal{C}_1, \dots, \mathcal{C}_k\}$. We fix a point class $\mathcal{C} \in \{\mathcal{C}_1, \dots, \mathcal{C}_k\}$ of $\mathcal{D}(\mathbb{P}, \mathbb{B})$. Assume a group $G (\leq \text{Aut}(\mathcal{D}))$ is an *SCT*(u, k, λ) group of $\mathcal{D}$. Let $\mathbb{P}_1, \mathbb{P}_2, \dots, \mathbb{P}_u$ be the G -orbits on $\mathbb{P}$ ($|\mathbb{P}|/|G| = u$) and set $\{p_i\} = \mathbb{P}_i \cap \mathcal{C}$ for each $i \in I_u$. Moreover, let $\mathbb{B}_1, \mathbb{B}_2, \dots, \mathbb{B}_r$ be the G -orbits on $\mathbb{B}$, where $r = |\mathbb{B}|/|G|$, and choose blocks $B_1 \in \mathbb{B}_1, B_2 \in \mathbb{B}_2, \dots$ and $B_r \in \mathbb{B}_r$.



A matrix obtained from an SCT group of $\text{TD}_\lambda(k, u)$

Hypothesis 2.3. Under Notation 2.2, we define a $u \times r$ matrix $M = [D_{ij}]$ ($D_{ij} \subset G$) over G of order k in the following manner.

$$D_{ij} = \{g \in G \mid p_i^g \in B_j\}, \quad i \in I_u, \quad j \in I_r,$$



$$M = \begin{bmatrix} D_{11} & D_{12} & \cdots & D_{1r} \\ \vdots & \cdots & \cdots & \vdots \\ D_{u1} & D_{u2} & \cdots & D_{ur} \end{bmatrix}$$

Theorem 2.4. Under Hypothesis 2.3, we have

- (i) $\sum_{i \in I_u} |D_{ij}| = k \quad \forall j \in I_r$ and
- (ii) $\sum_{j \in I_r} D_{ij} D_{\ell j}^{(-1)} = \begin{cases} u\lambda + \lambda(G-1) & \text{if } i = \ell, \\ \lambda(G-1) & \text{otherwise.} \end{cases}$

We define SCT matrices.

Definition 2.5. Let G be a group of order k and $M = [D_{ij}]$ a $u \times r$ matrix over $\mathbb{Z}[G]$, where $D_{ij} \subset G$ for $i \in I_u, j \in I_r$. We say M is an $SCT(u, k, \lambda)$ matrix over G if the following conditions are satisfied.

- (i) $\sum_{i \in I_u} |D_{ij}| = k \quad \forall j \in I_r$
- (ii) $\sum_{j \in I_r} D_{ij} D_{\ell j}^{(-1)} = \begin{cases} u\lambda + \lambda(G-1) & \text{if } i = \ell, \\ \lambda(G-1) & \text{otherwise.} \end{cases}$

Example 2.6. The following is an $SCT(2, 5, 5)$ over $\mathbb{Z}_5 = \langle a \rangle$.

$$\begin{bmatrix} 1 & 1+a & 1+a+a^3 & 1+a+a^2+a^3 \\ a+a^2+a^3+a^4 & a^2+a^3+a^4 & a^2+a^4 & a^4 \end{bmatrix}$$

We define an incidence structure corresponding to an $SCT(u, k, \lambda)$ matrix over a group G in the following manner.

Definition 2.7. Let $M = [D_{ij}]$ be a $u \times r$ $SCT(u, k, \lambda)$ matrix over a group G of order k . We define an incidence structure $\mathcal{D}_M = (\mathbb{P}, \mathbb{B})$ in the following manner.

$$\mathbb{P} = \{1, 2, \dots, u\} \times G, \quad \mathbb{B} = \{B_{j,g} \mid j \in I_r, g \in G\}$$

where $B_{j,g} = (B_j)g$ and $B_j = (1, D_{1j}) \cup (2, D_{2j}) \cup \dots \cup (u, D_{uj}) (\subset \mathbb{P})$.

The converse of Theorem 2.4 is true, as shown below.

Theorem 2.8. Let M be an $SCT(u, k, \lambda)$ matrix over a group $G = \{g_1, \dots, g_k\}$ of order k and $\mathcal{D}_M = (\mathbb{P}, \mathbb{B})$ the incidence structure defined in Definition 2.7. Then the following holds.

- (i) $\mathcal{D}_M$ is a $TD_\lambda(k, u)$ with the point classes $C_1 = I_u \times \{g_1\}, \dots, C_k = I_u \times \{g_k\}$,
- (ii) G acts on $\mathcal{D}_M$ as an $SCT(u, k, \lambda)$ group under the action $(i, w)g = (i, wg)$ for $i \in \{1, \dots, u\}$ and $w, g \in G$.

We now give a result on $SCT(2, k, \lambda)$ matrices with $k = \lambda$

Proposition 2.9. Let G be a group of order λ and let D_1, D_2, D_3, D_4 be subsets of G satisfying

$$(*) \quad D_1 D_1^{(-1)} + D_2 D_2^{(-1)} + D_3 D_3^{(-1)} + D_4 D_4^{(-1)} = \lambda + \lambda G$$

Then the following is a $SCT(2, \lambda, \lambda)$ matrix over G , from which we obtain a class transitive $TD_\lambda(\lambda, 2)$:

$$M = \begin{bmatrix} D_1 & D_2 & D_3 & D_4 \\ G - D_1 & G - D_2 & G - D_3 & G - D_4 \end{bmatrix}$$

Using some difference sets we can give $\text{SCT}(2, \lambda, \lambda)$ matrices.

Proposition 2.10. Let G be a group of order $v(= 4m^2)$ and D_i a (v, k_i, λ_i) difference set (DS) of order $n_i(= k_i - \lambda_i)$ in G for $i \in \{1, 2, 3, 4\}$. If $4m^2 = \sum \lambda_i = \sum n_i$, then $\{D_1, \dots, D_4\}$ satisfies the condition $(*)$ and we obtain a $\text{TD}_v(v, 2)$ admitting G as a $\text{SCT}(2, v, v)$ group.

For example, if we choose $D_1, \dots, D_4$ as $(4m^2, 2m^2 \pm m, m^2 \pm m)$ DSs (Hadamard DSs), then the condition is satisfied.

Remark 2.11. For each odd integer $n > 1$, there exists a $(4n^4, 2n^4 \pm n^2, n^4 \pm n^2)$ -difference set (an Hadamard difference set of order n^4) in an abelian group of order $4n^4$ (Haemer-Xiang[10]). From this we obtain an $\text{SCT}(2, 4n^4, 4n^4)$ group acting on a $\text{TD}_{4n^4}(4n^4, 2)$ applying Proposition 2.10.

Example 2.12. By computer search we can verify that there exists an $\text{SCT}(2, q, q)$ matrix for $q \in \{3, 5, 9, 11, 13, 17, 19\}$. From this we have a $\text{TD}_q(q, 2)$. We note that this is unable to obtain from difference matrices applying Drake's result. For example, the following is a $\text{SCT}(2, 19, 19)$ matrix over $\mathbb{Z}_{19} = \langle a \rangle$.

$$\begin{bmatrix} D_{11} & D_{12} & D_{13} & D_{14} \\ G - D_{11} & G - D_{12} & G - D_{13} & G - D_{14} \end{bmatrix}, \text{ where}$$

$$\begin{aligned} D_{11} &= 1 + a + a^2 + a^6 + a^{13} + a^{14}, \\ D_{12} &= 1 + a + a^2 + a^3 + a^4 + a^5 + a^6 + a^9 + a^{10} + a^{13}, \\ D_{13} &= 1 + a + a^2 + a^4 + a^5 + a^8 + a^{10} + a^{11} + a^{13} + a^{15}, \text{ and} \\ D_{14} &= 1 + a + a^2 + a^4 + a^5 + a^7 + a^9 + a^{11} + a^{12} + a^{14} + a^{15} + a^{17}. \end{aligned}$$

We also have the following result on $\text{SCT}(2, k, \lambda)$ matrices with $k = 2\lambda$.

Proposition 2.13. Let G be a group of order $4m^2$. If subsets A and B of G satisfies $(*)$ $AA^{(-1)} + BB^{(-1)} = 4m^2 + 2m^2(G - 1)$, then $\begin{bmatrix} A & B \\ G - A & G - B \end{bmatrix}$ is an $\text{SCT}(2, 4m^2, 2m^2)$ matrix over G .

Example 2.14. (i) Let G be a group of order $4m^2$ and let C and D be any $(4m^2, 2m^2 - m, m^2 - m)$ and $(4m^2, 2m^2 + m, m^2 + m)$ difference sets of G , respectively. Then we can verify that $CC^{(-1)} + DD^{(-1)} = 4m^2 + 2m^2(G - 1)$ and so by Proposition above we obtain an $\text{SCT}(2, 4m^2, 2m^2)$ matrix $\begin{bmatrix} C & D \\ G - C & G - D \end{bmatrix}$ over G . From this we have a $\text{TD}_{2m^2}(4m^2, 2)$ admitting G as an $\text{SCT}(2, 4m^2, 2m^2)$ automorphism group of order $4m^2$.

(ii) There are exactly 14 groups of order 16. Nine of them have $(16, 6, 2)$ -difference sets and so have $\text{SCT}(2, 16, 8)$ matrices by Proposition 2.13. On the other hand, five groups $\mathbb{Z}_{16}$, $\mathbb{Z}_2 \times \mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$ and D_{16} have no difference sets. However, we can verify that each of these contains subsets A and B satisfying the condition $(*)$ of Proposition 2.13. Hence there exists an $\text{SCT}(2, 16, 8)$ matrix over any group of order 16.

3 Spreads, SCT matrices and λ -planar functions

Definition 3.1. Let G be a group of order n^2 . A set of subgroups $\{H_1, \dots, H_{n+1}\}$ of G is called a **spread** of G if

- (1) $|H_1| = \dots |H_{n+1}| = n$ and
- (2) $G = H_i H_j$ ($1 \leq \forall i \neq \forall j \leq n+1$).

Remark 3.2. $G^* = H_1^* \cup H_2^* \cup \dots \cup H_{n+1}^*$ is a disjoint union.

By Theorems 4.4.9 and 4.9.14 of [15] we can show the following. A shorter proof was communicated to the author by N. Chigira [14].

Lemma 3.3. Let G be a group of order n^2 . If there exists a spread in G , Then G is an elementary abelian p -group for a prime p .

Example 3.4. Set $G = (V(2, q), +)$. Then the set of 1-dimensional $GF(q)$ -subspaces $H_1, \dots, H_{q+1}$ of $V(2, q)$ is a spread of G .

We can construct $SCT(p^m, q^2, q^2/p^m)$ matrices using a spread of an elementary abelian p -group of order q^2 .

Proposition 3.5. Let q be a power of a prime p and $G \simeq E_{q^2}$. For a spread $\mathcal{S} = \{H_1, \dots, H_{q+1}\}$ of G , set $r = q/p^m$ ($1 < p^m \leq q$) and $A_i = H_{ir+1}^* + H_{ir+2}^* + \dots + H_{(i+1)r}^*$ ($0 \leq i \leq p^m - 2$), $A_{p^m-1} = H_{(p^m-1)r+1}^* + H_{(p^m-1)r+2}^* + \dots + H_{p^m \cdot r}^* + H_{p^m \cdot r+1}^* + 1$.

Let $[n_{ij}]$ be any Latin square of order p^m with entries from $\{0, 1, \dots, p^m - 1\}$. Then the following is a $SCT(p^m, q^2, q^2/p^m)$ matrix, which gives a $TD_{q^2/p^m}(q^2, p^m)$.

$$\begin{bmatrix} A_{n_{1,1}} & A_{n_{1,2}} & \dots & A_{n_{1,p^m}} \\ A_{n_{2,1}} & A_{n_{2,2}} & \dots & A_{n_{2,p^m}} \\ \vdots & \vdots & \vdots & \vdots \\ A_{n_{p^m,1}} & \dots & A_{n_{p^m,p^m-1}} & A_{n_{p^m,p^m}} \end{bmatrix}$$

Definition 3.6. Let $\mathcal{G}$ be a group of order $u^2\lambda$ and $U(\triangleleft \mathcal{G})$ its normal subgroup of order u . A $u\lambda$ -subset D of $\mathcal{G}$ is called a $(u\lambda, u, u\lambda, \lambda)$ -relative difference set (RDS) relative to U if $DD^{(-1)} = u\lambda + \lambda(\mathcal{G} - U)$. The subgroup U is called a **forbidden subgroup**. We note that from U we obtain a $(u, u\lambda, \lambda)$ -difference matrix over U .

Remark 3.7. Denote by $\pi(n)$ the set of primes dividing an integer $n > 1$. In the known examples $\mathcal{G}$ satisfies $\pi(|\mathcal{G}|) \in \{\{p\}, \{3, 7\}, \{2, p\}\}$ for a prime p ([1],[4],[5],[8],[12]) and U is a p -group. Moreover, in most cases U is abelian.

We shall consider a relation between RDSs and $SCT(u, u\lambda, \lambda)$ matrices by generalizing the notion of planar functions.

Theorem 3.8. Let G be a group of order $u\lambda$ and U a group of order u . Let D_y ($y \in U$) be subsets of G . If a $u \times u$ matrix $D = [D_{yz^{-1}}]_{y,z \in U}$ over $\mathbb{Z}[G]$ whose rows and columns are indexed by the elements of U is a $\text{SCT}(u, u\lambda, \lambda)$ matrix, then the following holds.

- (i) $G = \sum_{y \in U} D_y$ (the disjoint union of u subsets D_y).
- (ii) A function $f : G \rightarrow U$ defined by $f(D_y) = y$ ($y \in U$) satisfies the following:
 $(\star) \quad \#\{x \in G \mid f(ax)f(x)^{-1} = b\} = \lambda \quad (\forall a \in G \setminus \{1\}, \forall b \in U)$

Definition 3.9. Let G and U be groups. We call a function $f : G \rightarrow U$ a λ -planar function if f satisfies $(\star)$.

Remark 3.10. (i) A 1-planar function is just a planar function in the usual sense (A. Pott [11]).

- (ii) We can show $|G| = |U|\lambda$ by counting the number of pairs $(x, f(tx)f(x)^{-1})$ with $x \in G$ in two ways.

Proof of Theorem 3.8

As D is an $\text{SCT}(u, u\lambda, \lambda)$ matrix over G , we have $\sum_{z \in U} D_{a_1 z^{-1}} D_{a_2 z^{-1}}^{(-1)} = \sum_{z \in U} D_{a_1 a_2^{-1}(a_2 z^{-1})} D_{a_2 z^{-1}}^{(-1)}$. Hence,

$$(\star) \quad \sum_{y \in U} D_{by} D_y^{(-1)} = \begin{cases} u\lambda + \lambda(G-1) & \text{if } b = 1, \\ \lambda(G-1) & \text{otherwise.} \end{cases}$$

Then, by $(\star)$, we have $\sum_{y \in G} |D_y| = u\lambda$ and $D_y \cap D_z = \emptyset$ ($y \neq z$) by putting $b = 1$ and $b \neq 1$, respectively. Thus we have (i).

Let $a \in G \setminus \{1\}$ and $b \in G$ and consider the equation $f(ax)f(x)^{-1} = b$. Set $y = f(x)$. Then $f(ax) = by$. Hence,

$$f(x) = y, f(ax) = by \iff x \in D_y, ax \in D_{by}.$$

By $(\star)$, there exist exactly λ distinct elements $(t_i, x_i) \in D_{by_i} \times D_{y_i}$ such that $a = t_i x_i^{-1}$ for $i \in \{1, \dots, \lambda\}$. As $t_i = ax_i$, $f(t_i) = by_i$ and $f(x_i) = y_i$, we have $f(ax_i)f(x_i)^{-1} = b$ and so (ii) holds. $\square$

We now show that relations among λ -planar functions, SCTs, and RDSs.

Theorem 3.11. Let G be a group of order $u\lambda$ and U a group of order u . If $f : G \rightarrow U$ is a λ -planar function, then the following holds.

- (i) A $u \times u$ matrix $D = [D_{y,z}]$ defined by $D_{y,z} = f^{-1}(yz^{-1})$ ($y, z \in U$) is an $\text{SCT}(u, u\lambda, \lambda)$ matrix.
- (ii) A subset $D = \{(x, f(x)) \mid x \in G\}$ of $\mathcal{G} := G \times U$ is a $(u\lambda, u, u\lambda, \lambda)$ relative difference set in a group $\mathcal{G}$ relative to U .

Proof. (i) Fix $a_1, a_2 \in U$ and let $y \in U$. Then, for any $t \in G$,

$$\begin{aligned} t \in D_{a_1, y} D_{a_2, y}^{(-1)} &\iff t = x_1 x_2^{-1}, \exists x_1 \in D_{a_1, y}, \exists x_2 \in D_{a_2, y} \\ &\iff x_1 = t x_2, f(t x_2) = a_1 y^{-1}, f(x_2) = a_2 y^{-1}, \exists x_2 \in D_{a_2, y} \\ &\iff t = x_1 x_2^{-1}, f(t x_2) f(x_2)^{-1} = a_1 a_2^{-1}, \exists x_2 \in D_{a_2, y}. \text{ Thus,} \end{aligned}$$

$$\sum_{y \in U} D_{a_1, y} D_{a_2, y}^{(-1)} = \begin{cases} |G| + \lambda(G - 1) & \text{if } a_1 = a_2, \\ \lambda(G - 1) & \text{otherwise.} \end{cases}$$

$$\begin{aligned} \text{(ii)} \quad (t, b) &\in (x_1, f(x_1))(x_2, f(x_2))^{-1}, \exists x_1, x_2 \in G \\ &\iff t = x_1 x_2^{-1}, f(x_1) f(x_2)^{-1} = b, \exists x_1, x_2 \in G \\ &\iff f(t x_2) f(x_2)^{-1} = b, x_1 = t x_2, \exists x_2 \in G. \quad \square \end{aligned}$$

Two Groups G, U corresponding to a λ -planar function f

Assume there exists a λ -planar function from G to U . Many examples are known where $|G|$ is not a power of a prime ([1],[4],[5],[8],[12]).

These satisfy $\pi(|G|) \in \{\{3, 7\}, \{2, p\}\}$.

However, every known example of U is a p -group for a prime p and in the most cases U is abelian. What is the possible group theoretic structure of G or U ?

When $\lambda = 1$, the following result is known.

Result 3.12. (Blokhuis-Jungnickel-Schmidt [9]) Let G and H be abelian groups of order n . If there exists a 1-planar function from G to H , then $n = p^e$ for a prime p and the p -rank of $G \times H$ is at least $e + 1$.

We now construct a λ -planar function with λ a prime power.

Theorem 3.13. Let p be a prime and U any group of order p^m . Let G be an elementary abelian p -group of order p^{2n} with $n \geq m$. Then there exists a p^{2n-m} -planar function from G to U .

Proof . Let $G, q, p^m, H_i (i \in I_{q+1})$ be as in Proposition 3.5 and consider an $\text{SCT}(p^m, p^{2n}, p^{2n-m})$ with $q = p^n$. Let U be any group of order p^m ($\leq q$) and $\cup_{y \in U} T_y$ a partition of the spread $\{H_1, \dots, H_{q+1}\}$ such that $|T_1| = r + 1$ and $|T_y| = r$ ($y \in U^*$), where $r = q/p^m$. Let D_y be the set of non-identity elements of T_y for $y \in U^*$ and D_1 the set of elements of T_1 . Then a matrix $L = [z_{y_1, y_2}]$ defined by $z_{y_1, y_2} = y_1 y_2^{-1}$ ($y_1, y_2 \in U$) is a Latin square of order p^m with entries from U . Hence, by Proposition 3.5, $[D_{y_1 y_2^{-1}}]_{y_1, y_2 \in U}$ is an $\text{SCT}(p^m, p^{2n}, p^{2n-m})$ matrix, which gives a p^{2n-m} -planar function from G to U by Theorem 3.8. $\square$

By Theorems 3.13 and 3.11, we have the following.

Theorem 3.14. Any p -group can be a forbidden subgroup of an RDS.

As a corollary we have the following, which gives another proof of de Launey's result on DMs (Corollary 2.8 of [2]).

Corollary 3.15. There exists a (p^m, p^{2n}, p^{2n-m}) -difference matrix over any group of order p^m whenever $n \geq m$.

References

- [1] J.A. Davis, J. Jedwab, M. Mowbray, New Families of Semi-Regular Relative difference Sets, DCC 13 (1998), 131-146.
- [2] W. de Launey, Square GBRDs over non-abelian groups, ARS Combinatoria 27 (1989), 40-49
- [3] D.A. Drake, Partial λ -geometries and generalized Hadamard matrices over groups, Canad. J. Math. 31 (1979), 617-727.
- [4] T. Feng and Q. Xiang, Semi-regular relative difference sets with large forbidden subgroups JCTA 115 (2008), 1456-1473.
- [5] T. Feng, Relative (pn, p, pn, n) -Difference sets With $\gcd(p, n) = 1$, Journal of Algebraic Combinatorics 29 (2009), 91-106.
- [6] D. Jungnickel, On Difference Matrices, Resolvable Transversal Designs and Generalized Hadamard Matrices, Math. Z. 167 (1979), 49-60.
- [7] D.A. Drake and D. Jungnickel, Klingenberg structures and partial designs II. Regularity and uniformity. Pacific J. Math. 77, 389-415 (1978)
- [8] K.H. Leung, S. Ling, S. L. Ma, Constructions of semi-regular relative difference sets, Finite Fields and Their Applications 7 (2001), 397-414
- [9] A. Blokhuis, D. Jungnickel and B. Schmidt, Proof of the prime power conjecture for projective planes of order n with abelian collineation groups of order n^2 , Proc. Amer. Math. Soc. 130 (2002), 1473-1476
- [10] W.H. Haemers and Q. Xiang, Strongly regular graphs with parameters $(4m^4, 2m^4 + m^2, m^4 + m^2, m^4 + m^2)$ exist for all $m > 1$.
- [11] A. Pott, "Finite Geometry and Character Theory", Lecture Notes in Mathematics, vol. 1601, Springer, 1995.
- [12] K. Akiyama, M. Ogawa and C. Suetake, On $\text{STD}_6[18, 3]$'s and $\text{STD}_7[21, 3]$'s admitting a semiregular automorphism group of order 9. Electron. J. Combin. 16 (2009), Research Paper 148, 21 pp
- [13] T. Beth, D. Jungnickel, H. Lenz, "Design Theory", Lecture Notes in Mathematics, vol. 1601, Cambridge Univ. Press, 2nd ed., 1999.
- [14] N. Chigira, Private communication.
- [15] D. R. Hughes and F. C. Piper, "Projective Planes" (1973), Springer-Verlag, Berlin-Heidelberg-New York.