数理解析研究所講究録
第 1965 巻 2015 年 112-120



# On SCT automorphism groups of divisible designs

熊本大学・教育学部 平峰 豊
Yutaka Hiramine
Department of Mathematics, Faculty of Education,
Kumamoto University,
Kurokami, Kumamoto, Japan

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

§1 Divisible Designs and class regularity

A *divisible design* $(m, u, k, \lambda)$-DD is an incidence structure $(\mathbb{P}, \mathbb{B})$, where

(i) $\mathbb{P}$ is a set of $mu$ points partitioned into $m$ classes $\mathscr{C}$ (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 $\lambda$ blocks.

We can show the following : $|\mathbb{P}| = mu,\ |\mathbb{B}| = u^2m(m-1)\lambda/k(k-1)$

An $(m, u, k, \lambda)$-DD with $k = m$ is called a *transversal design* and denoted by $\mathrm{TD}_\lambda(k, u)$. A $\mathrm{TD}_\lambda(k, u)$ is called a *symmetric transversal design* and denoted by $\mathrm{STD}_\lambda(k, u)$ with $k = u\lambda$ if its dual is also a $\mathrm{TD}_\lambda(k, u)$. We note that an $(m, 1, k, \lambda)$-DD is just a 2-$(m, k, \lambda)$ design.

### Partial difference matrices

**Definition.** (Jungnickel [2]) Let $U$ be a group of order $u$. An $m \times t$ matrix $D = [d_{ij}]$ with entries from $U \cup \{0\}$ is called an $(m, u, k, \lambda)$-*partial difference matrix* (PDM) over $U$ if the following conditions are satisfied :

(i) Each column of $D$ has exactly $k$ nonzero entries.

(ii) $\displaystyle\sum_{1\leq j\leq t} d_{ij}{d_{\ell j}}^{-1} = \lambda U,\ \forall i \neq \ell,$ where $0^{-1} = 0,\ 0 \cdot g = g \cdot 0 = 0\ \ \forall g \in U$ and $t = |\mathbb{B}|/|G| = m(m-1)u\lambda/k(k-1))$.

An $(m,u,k,\lambda)$-PDM with $m = k$ over a group $U$ of order $u$ is called a $(u,k,\lambda)$-*difference matrix* (DM). Moreover, a $(u,u\lambda,\lambda)$-DM, denoted by $\mathrm{GH}(u,\lambda)$, is called *a generalized Hadamard matrix.*

**Example.** Set $U = \langle a \rangle \simeq \mathbb{Z}_3$.

$$\underset{(5,3,4,1)\text{-PDM}}{\begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & a & 0 & a^2 \\ 1 & a & 1 & a^2 & 0 \\ a & 1 & 0 & a^2 & a \\ 1 & 0 & a^2 & 1 & a \end{bmatrix}}, \quad \underset{(3,3,2)\text{-DM}}{\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & a & a & a^2 & a^2 \\ 1 & 1 & a^2 & a^2 & a & a \end{bmatrix}}, \quad \underset{\mathrm{GH}(3,1)}{\begin{bmatrix} 1 & 1 & 1 \\ 1 & a & a^2 \\ 1 & a^2 & a \end{bmatrix}}$$

**Class regularity**

Following results are known.

**Result.** (D. Jungnickel [3]) The existence of an $(m,u,k,\lambda)$-DD admitting a class regular automorphism group $U$

$\Longleftrightarrow$ The existence of a $(m,u,k,\lambda)$-partial difference matrix over $U$

**Result.** (D.A. Drake [2]) Assume $U$ is a group of even order $u$ and $2 \nmid \lambda$. If a Sylow 2-subgroup of $U$ is cyclic then there exists no $(u,k,\lambda)$-DM over $U$ for $k \geq 3$.

We now consider *the regular action* of a subgroup $G$ of $\mathrm{Aut}(\mathcal{D})$ on the set of point classes $\mathscr{C} = \{\mathcal{C}_i \mid i \in I_m\}$, where $I_m = \{1, 2, \cdots, m\}$.

## §2 SCT groups and SCT matrices

Let $(\mathbb{P},\mathbb{B})$ be a $(m,u,k,\lambda)$-DD and $G \leq \mathrm{Aut}(\mathbb{P},\mathbb{B})$. We say $G$ is an *SCT*$(m,u,k,\lambda)$ *group* if $G$ is semiregular on $\mathbb{P} \cup \mathbb{B}$ and regular on the set of point classes $\mathscr{C} = \{\mathcal{C}_1, \cdots, \mathcal{C}_m\}$. (Note that $|G| = m$.)

Assume that $G$ is an SCT$(m,u,k,\lambda)$ group of a $(m,u,k,\lambda)$-DD $\mathcal{D}(= (\mathbb{P},\mathbb{B}))$. Choose a point class $\mathcal{C} = \{p_1, \cdots, p_u\} \in \mathscr{C}$. Then $\mathbb{P} = \bigcup_{i \in I_u} {p_i}^G$ and $\mathbb{B} = \bigcup_{j \in I_s} {B_j}^G$, where $s = |\mathbb{B}|/|G|$.

A $u \times s$ matrix $M_\mathcal{D} = [D_{ij}]$ $(D_{ij} \subset G)$ over $G$ is defined by

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

**Theorem 1.** The following holds.

$$\sum_{j \in I_s} D_{ij} {D_{\ell j}}^{(-1)} = \begin{cases} \rho + \lambda(G-1) & \text{if } i = \ell, \\ \lambda(G-1) & \text{otherwise,} \end{cases}$$

where $\rho = (m-1)u\lambda/(k-1)$.

$$\sum_{i \in I_u} |D_{ij}| = k \qquad \forall j \in I_s$$

**Definition.** Let $G$ be a group of order $m$. Let $u, s \in \mathbb{N}$. For subsets $D_{ij} \subset G$ $(i \in I_u, j \in I_s)$ we call a $u \times s$ matrix $\begin{bmatrix} D_{11} & \cdots & D_{1s} \\ \vdots & \vdots & \vdots \\ D_{u1} & \cdots & D_{us} \end{bmatrix}$ an SCT$(m,u,k,\lambda)$-

matrix over $G$ if it satisfies the following for some $\rho \in \mathbb{N}$.

$$\sum_{j \in I_s} D_{ij} D_{\ell j}{}^{(-1)} = \begin{cases} \rho + \lambda(G-1) & \text{if } i = \ell, \\ \lambda(G-1) & \text{otherwise,} \end{cases}$$

$$\sum_{i \in I_u} |D_{ij}| = k \qquad \forall j \in I_s$$

**Remark.** (i) $s = (m-1)u^2\lambda/k(k-1), \quad \rho = (m-1)u\lambda/(k-1)$
(ii) An SCT$(m, 1, k, \lambda)$-matrix is just an $(m, k, \lambda)$-difference family.

$\star$ An incidence structure $\mathcal{D}(\mathbb{P}, \mathbb{B})$ defined by the following is an $(m, u, k, \lambda)$-DD admitting $G$ as an SCT group under the action $(i, w)g = (i, wg)$ for $i \in \{1, \cdots, u\}$ and $w, g \in G$.
$\mathbb{P} = \{1, 2, \cdots, u\} \times G$

$$\mathbb{B} = \{B_{j,g} \mid j \in I_s,\ g \in G\}, \text{ where } B_{j,g} = \bigcup_{i \in I_u} (i, D_{ij}g)$$

$\star$ $(m, u, k, \lambda)$-DD with SCT-group $\Longleftrightarrow$ SCT$(m, u, k, \lambda)$-matrix

**Example.** (i) The following is an SCT$(9, 2, 9, 9)$ matrix over $G := \langle a, b \rangle \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$ :

$$\begin{bmatrix} \langle a \rangle & \langle b \rangle & G - \langle ab \rangle & G - \langle ab^2 \rangle \\ G - \langle a \rangle & G - \langle b \rangle & \langle ab \rangle & \langle ab^2 \rangle \end{bmatrix}$$

This matrix gives a $\mathrm{TD}_9(9, 2)$, which is not obtained from any difference matrix by Drake's result.

(ii) The following is an SCT$(12, 5, 11, 2)$ matrix over Alt$(4) = N \rtimes H$, $N = \{1, a, b, c\} \simeq E_4$, $H = \{1, d, d^2\} \simeq \mathbb{Z}_3$ :

$$\begin{bmatrix} 0 & \alpha & \beta & \gamma & \delta \\ \alpha & \beta & \gamma & \delta & 0 \\ \beta & \gamma & \delta & 0 & \alpha \\ \gamma & \delta & 0 & \alpha & \beta \\ \delta & 0 & \alpha & \beta & \gamma \end{bmatrix}, \text{ where } \begin{cases} \alpha = ad + cd^2 \\ \beta = d + bd^2 + d^2 + cd \\ \gamma = b + c \\ \delta = ad^2 + bd + a \end{cases}$$

From this we obtain a $(12, 5, 11, 2)$-DD with the full automorphism group isomorphic to Alt$(5)$ ($\geq$ Alt$(4) \simeq N \rtimes H$). This DD is not class regular, hence not obtained from any partial difference matrix.

**Relations among SCT aut. , Class regular aut. and RDS**

$$\begin{array}{lcl} \exists\ \text{SCT aut.} \Longleftrightarrow \exists\ \text{SCT mat.} & & \\ \qquad\qquad\qquad\quad \Downarrow & & \\ \qquad\qquad \text{Divisible design} \supset \text{Transversal design} & & \\ \qquad\qquad\qquad\quad \Uparrow \qquad\qquad\quad \Uparrow & & \\ \exists\ \text{class regular aut.} \Longleftrightarrow \exists\ \text{partial DM} \supset \text{DM} \supset \text{GH mat.} & & \end{array}$$

$\exists$ SCT aut. & $\exists$ class regular aut. $\Longleftrightarrow$ $\exists$ splitting relative difference set

### Difference families and SCT matrices

A family of $k$-subsets $\{D_1, \cdots, D_n\}$ of a group $G$ of order $v$ is called an $n$-$(v, k, \lambda)$ *difference family* if

$$D_1 D_1{}^{(-1)} + \cdots + D_n D_n{}^{(-1)} = kn + \lambda(G - 1).$$

From an $n$-$(v, k, \lambda)$ difference family in a group $G$ we obtain a 2-$(v, k, \lambda)$ design $(\mathbb{P}, \mathbb{B}) : \mathbb{P} = G, \ \ \mathbb{B} = \{D_i x \mid i \in I_n, \ x \in G\}$. In the following we give a relation between difference families and SCT matrices with $u = 2$.

**Theorem 2.** Let $\{D_1, \cdots, D_{4d}\}$ be a $4d$-$(m, k, d(4k - m))$ difference family in a group $G$ of order $m$. Set $C_i = G - D_i$ for $i \in I_{4d}$. Then the following is an SCT$(m, 2, m, dm)$ matrix corresponding to a TD$_{dm}(m, 2)$.

$$M = \begin{bmatrix} D_1 & \cdots & D_{2d} & C_{2d+1} & \cdots & C_{4d} \\ C_1 & \cdots & C_{2d} & D_{2d+1} & \cdots & D_{4d} \end{bmatrix}$$

$$\begin{aligned} \because \ C_i C_i{}^{(-1)} &= D_i D_i{}^{(-1)} + (m - 2k)G \\ D_i C_i{}^{(-1)} &= C_i D_i{}^{(-1)} = kG - D_i D_i{}^{(-1)} \end{aligned}$$

### Some theorems on difference families

The following results on difference families are known.

**Result.** (Leung-Ma-Schmidt [4]) Let $q$ be a prime power and $d > 0$ an integer. Suppose, either (i) $q \equiv 2d - 1 \pmod{4d}$ and $2 \nmid d$ or (ii) $q \equiv 4d - 1 \pmod{8d}$. Then there exists a $4d$-$(q^2, (q^2 - q)/2, dq^2 - 2dq)$ difference family in $(GF(q^2), +)$.

**Result.** (Q. Xiang [6]) Let $q$ be a power of a prime and $b, c$ positive integers such that $q + 1 = 2^c b$ and $c \geq 2$ with $2 \nmid b$. Then there exists a $2^c$-$(q^2, (q^2 - q)/2, 2^{c-2}(q^2 - 2q))$ difference family in $(GF(q^2), +)$.

**Remark.** Set $d = 2^{c-2}$ in the above result. Then $2^c$-$(q^2, (q^2 - q)/2, 2^{c-2}(q^2 - 2q))$ is identical with $4d$-$(q^2, (q^2 - q)/2, dq^2 - 2dq)$.

We now apply Theorem 2 to the above results for $m = q^2, k = (q^2 - q)/2$.

### TD$_{dq^2}(q^2, 2)$s admitting SCT groups

**Proposition.** Let $q$ be a power of a prime and $d$ a positive integer satisfying one of the following :

(i) $q \equiv 2d - 1 \pmod{4d}$.
(ii) $q \equiv 4d - 1 \pmod{8d}$.
(iii) $4d \mid q + 1, 8d \nmid q + 1$ with $d$ a power of 2.

Then, there exists an SCT$(q^2, 2, q^2, dq^2)$ matrix over $(GF(q^2), +)$ and the resulting TD$_{dq^2}(q^2, 2)$ admits an SCT automorphism group of order $q^2$.

**Remark.** If $2 \nmid dq$, then no TD$_{dq^2}(q^2, 2)$s are obtained from difference matrices by Drake's result.

## §3 Direct product RDSs and SCTs

Let $\mathcal{G}$ be a group of order $um$ and $U$ its (not necessarily normal) subgroup of order $u$. A $k$-subset $D$ of $\mathcal{G}$ is called an $(m, u, k, \lambda)$-*relative difference set* (or, RDS for short) relative to $U$ if $DD^{(-1)} = k + \lambda(\mathcal{G} - U)$. Usually $U$ is called the forbidden subgroup.

An $(m, u, k, \lambda)$-divisible design $\mathcal{D} = (\mathbb{P}, \mathbb{B})$ is obtained from $(m, u, k, \lambda)$-RDS in the following way : the set $\mathbb{P}$ of points are elements of $\mathcal{G}$ and the set of blocks $\mathbb{B}$ are subsets $Dx (x \in \mathcal{G})$. We note that the set of point classes are $\{Ug \mid g \in \mathcal{G}\}$.

We say $\mathcal{G}$ is *splitting* (over $U$) if there exists a subgroup $G$ of $\mathcal{G}$ of order $m$ such that $\mathcal{G} = GU$ and $G \cap U = 1$. In this case $G$ is an SCT$(m, u, k, \lambda)$ group of $\mathcal{D}$.

From now on we consider an SCT matrix obtained from a splitting abelian RDS ; $\mathcal{G} = G \times U$.

**Hypothesis 3.** Let $G = \{g_1, \cdots, g_m\}$ and $U = \{w_1, \cdots, w_u\}$ be abelian groups of order $m$ and $u$, respectively. Suppose $D$ is an $(m, u, k, \lambda)$-RDS in the group $\mathcal{G} = G \times U$ relative to $U$. Set $\mathbb{P} = \mathcal{G} = \{w_i g_j \mid i \in I_u, j \in I_m\}$ and $\mathbb{B} = \{Dw_i g_j \mid i \in I_u, j \in I_m\}$. Then $\mathcal{D}_{D,\mathcal{G}} := (\mathbb{P}, \mathbb{B})$ is a $(m, u, k, \lambda)$-DD with the set $\mathscr{C} := \{Ug_1, \cdots, Ug_m\}$ of point classes.

We now consider the action of $G$ on $(\mathbb{P}, \mathbb{B})$ as an SCT group.

$\{w_i G \mid i \in I_u\}$ : the set of $G$-orbits on $\mathbb{P}$,

$\{Dw_i G \mid i \in I_u\}$ : the set of $G$-orbits on $\mathbb{B}$,

$D = G_{w_1} w_1 \cup \cdots \cup G_{w_u} w_u \quad (\exists G_{w_1}, \cdots, \exists G_{w_u} \subset G)$.

We choose a point class $\mathcal{C} = \{w_1, \cdots, w_u\} (\in \mathscr{C})$ as a set of representatives of $G$-orbits on $\mathbb{P}$ and $\{Dw_1, \cdots, Dw_u\} (\subset \mathbb{B})$ as a set of representatives of $G$-orbits on $\mathbb{B}$.

**Direct product RDSs and SCTs**

Under Hypothesis 3, the corresponding $u \times u$ SCT matrix $[D_{ij}]$ is given by

$$D_{ij} = \{g \in G \mid (w_i)g \in Dw_j\} = G \cap Dw_i^{-1} w_j.$$

As $D = G_{w_1} w_1 \cup \cdots \cup G_{w_u} w_u \quad (G_{w_1}, \cdots, G_{w_u} \subset G)$,
we have $[D_{ij}] = [G_{w_i w_j^{-1}}]$, which we call *an SCT matrix of standard form with respect to* $\{D, G \times U\}$.

Similarly, if we choose a point class $\mathcal{C} = \{w_1 g, \cdots, w_u g\} \in \mathscr{C}$ $(g \in G)$ and $\{Dw_1 g_{n_1}, \cdots, Dw_u g_{n_u}\} \subset \mathbb{B}$ $(n_1, \cdots, n_u \in I_m)$ as sets of representatives of $G$-orbits on $\mathbb{P}$ and $\mathbb{B}$, respectively, then we have the following.

**Lemma 4.** Under Hypothesis 3, set $D = G_{w_1} w_1 \cup \cdots \cup G_{w_u} w_u$, where $G_{w_1}, \cdots, G_{w_u} \subset G$. Then a $u \times u$ matrix $[G_{w_i w_j^{-1}} g^{-1} g_{n_j}]$ is an SCT$(m, u, k, \lambda)$ matrix.

Let notations be as in Lemma 4. Then we have the following.

**Proposition 5.** Set $M = [G_{w_i w_j^{-1}}]$, the SCT matrix of standard form with respect to $\{D, G \times U\}$. Then,

(i) any SCT matrix is obtained from $M$ by multiplication of any column by an element of $G$ and any permutation of rows and columns;

(ii) $M$ is circulant if $u$ is a prime and $w_i = w^{i-1}$ for $i \in I_u$, where $U = \langle w \rangle$.

## §4 Spreads and SCTs

**Theorem 6.** Let $q = p^e$ be a power of a prime $p$ and let $G$ be an elementary abelian $p$-group of order $q^2$. Let $\{H_1, \cdots, H_{q+1}\}$ be a spread of $G$ (i.e. $|H_i| = q, |H_i \cap H_j| = 1,\ \forall i \neq j$). Set $q_0 = q/p^m\ (= p^{e-m})$ and

$A_i = H^*_{iq_0+1} + H^*_{iq_0+2} + \cdots + H^*_{(i+1)q_0} \quad (0 \leq i \leq p^m - 2),$

$A_{p^m-1} = H^*_{(p^m-1)q_0+1} + H^*_{(p^m-1)q_0+2} + \cdots + H^*_{p^m \cdot q_0} + H^*_{p^m \cdot q_0+1} + 1$

Let $L = [n_{ij}]$ be a Latin square of order $p^m$ with entries from $\{0, 1, \cdots, p^m - 1\}$. Then the following is an SCT$(p^{2e}, p^m, p^{2e}, p^{2e-m})$ matrix, which gives an STD$_{q^2/p^m}(p^{2e}, p^m)$.

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

Sketch of proof : (1) $\sum_{i \in I_{p^m}} A_i A_i^{(-1)} = q^2 + qq_0(G-1) \quad (\forall i \in I_{p^m})$.

(2) If $\{n_{i1}, \cdots, n_{ip^m}\} = \{n_{\ell 1}, \cdots, n_{\ell p^m}\} = I_{p^m}$ and $n_{i,1} \neq n_{\ell,1}, \cdots, n_{ip^m} \neq n_{\ell p^m}$, then

$$A_{i1} A_{\ell 1}{}^{(-1)} + \cdots + A_{ip^m} A_{\ell p^m}{}^{-1} = q_0 q(G-1)$$

### An equivalence class in Latin squares of order $n$

We show that some of the STDs obtained in Theorem 6 admit no class regular automorphism groups. This implies that these STDs are never obtained from generalized Hadamard matrices. In order to prove this we need a lemma on the set of Latin squares.

**Definition.** Let $e_1 = (1, 0, 0, \cdots, 0), e_2 = (0, 1, 0, \cdots, 0), \cdots$ be vectors of $\mathrm{V}(n, \mathbb{C})$. For a permutation $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ of $\Omega := \{1, 2, \cdots, n\}$, a permutation matrix $P_\sigma$ is defined by $e_i P_\sigma = e_{r_i}$ for each $i \in I_n$. Let $N$ be the group of permutation matrices of order $n$ and $\mathscr{L}$ the set of Latin squares on $\Omega$. We say Latin squares $L_1$ and $L_2$ in $\mathscr{L}$ are equivalent if $L_2 = PL_1Q$ for some $P, Q \in N$. Let $H := N \times N$ be the direct product and define the action of $H$ on $\mathscr{L}$ by $L(P, Q) = P^T LQ$ for $L \in \mathscr{L}$ . Then $H$ is a permutation group on $\mathscr{L}$.

### The number of Latin squares of order $n$

Let $\mathscr{L}_n$ be the set of Latin squares of order $n$ on $\{1, \cdots, n\}$.
By Theorem III.1.19 of [1],

$|\mathscr{L}_n| > f(n) := (n!)^{2n}/n^{n^2}$ for $n > 1$.

$|\mathscr{L}_2| = (2-1)!2! > \lceil f(2) \rceil = 1,$
$|\mathscr{L}_3| = (3-1)!3! > \lceil f(3) \rceil = 2,$
$|\mathscr{L}_4| = 4(4-1)!4! > \lceil f(4) \rceil = 25,$
$|\mathscr{L}_5| = 56(5-1)!5! = 161280 > \lceil f(5) \rceil = 2077$

$$\vdots$$

### Latin squares equivalent to a circulant one

$\mathscr{L}$ = the set of Latin squares on $\Omega := \{1, 2, \cdots, n\}$
$N$ = the group of permutation matrices of order $n$
$N \times N$ = the permutation group on $\mathscr{L}$ defined by $L(P,Q) = P^T LQ$

**Lemma.** Let $C$ be a circulant matrix of order $n$ whose first row is $(a_1, a_2, \cdots, a_n)$ with $\{a_1, a_2, \cdots, a_n\} = \Omega$. Let $T \in N$ be a circulant permutation matrix whose first row is $(0, 1, 0, \cdots, 0)$. If $Q, R \in N$ and $QC = CR$ then $Q = R$ and $Q \in \langle T \rangle$.

**Lemma 7.** Assume $C \in \mathscr{L}$ and $C$ is circulant. Then,

(i) The number of Latin squares in $\mathscr{L}$ equivalent to $C$ is $(n!)^2/n$;

(ii) If $n \geq 4$, then there exists a Latin square of $\mathscr{L}$ not equivalent to circulant one.

$\because$ By Theorem III.1.19 of [1], $|\mathscr{L}_n| > (n!)^{2n}/n^{n^2}$.
As $(n!)^{2n}/n^{n^2} > (n-1)!(n!)^2/n$, $(n \geq 4)$, the lemma holds.

### Non class regular STDs

**Theorem.** Let $p > 3$ be a prime and $A_L$ the $\mathrm{SCT}(p^{2e-1}, p^{2e}, p, p^{2e})$ matrix defined in Theorem 6. Then the $\mathrm{STD}_{p^{2e-1}}(p^{2e}, p)$ obtained from $A_L$ is not class regular.

*Proof.* By Lemma 7, there exists a Latin square $L$ not equivalent to a circulant one. Let $(\mathbb{P}, \mathbb{B})$ be the $\mathrm{STD}_{p^{2e-1}}(p^{2e}, p)$ obtained from $A_L$ and let $G$ be the $\mathrm{SCT}(p^{2e-1}, p^{2e}, p, p^{2e})$ automorphism group of order $p^{2e}$. Suppose false and let $U$ be a class regular automorphism group of $(\mathbb{P}, \mathbb{B})$. Then, as $G$ normalizes $U$ and $|U| = p$, $G$ centralizes $U$. The direct product $\mathcal{G} := G \times U$ contains a $(p^{2e}, p, p^{2e}, p^{2e-1})$-RDS corresponding to $(\mathbb{P}, \mathbb{B})$. By Proposition 5, $L$ must be equivalent to a circulant Latin square, a contradiction.

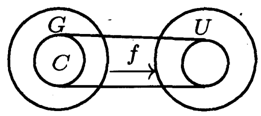
## §5 RDS and $\lambda$-planar functions

In this section we define a $\lambda$-planar function as a generalization of planar functions.

**Theorem.** Let $\mathcal{G} = GU$ be a group of order $mu$ and $G, U$ its subgroups with $|G| = m, |U| = u$ and $\mathcal{G} \rhd U$. Let $D$ be a $(m, u, k, \lambda)$-RDS in $\mathcal{G}$ relative to $U$. Then there exists a $k$-subset $C$ of $G$ and a function $f : C \longrightarrow U$ satisfying the following.

(i) $D = \{xf(x) \mid x \in C\}$

(ii) $\#\{x \in C \mid ax \in C,\ f(ax)^a f(x)^{-1} = b\} = \lambda$
for any $a \in G \setminus \{1\}$ and $b \in U$.




**Proposition.** Let $G, U$ be groups of order $m, u$, respectively. Let $\varphi$ be a homomorphism from $G$ to $\mathrm{Aut}(U)$ and $f$ a function form $C$ to $U$ for a $k$-subset $C$ of $G$. Assume that for any $a \in G \setminus \{1\}$ and $b \in U$

$$(\star)\quad \#\{x \in C \mid ax \in C,\ f(ax)^{\varphi(a)} f(x)^{-1} = b\} = \lambda.$$

Then $D = \{xf(x) \mid x \in C\}$ is a $(m, u, k, \lambda)$-RDS in a semi-direct product $\mathcal{G} = GU$ of $G$ by $U$ with respect to $\varphi$.

**Definition.** Let $G$ and $U$ be groups. Let $C$ be a subset of $G$ and $\varphi \in \mathrm{Hom}(G, \mathrm{Aut}(U))$. We call a function $f : C \longrightarrow U$ a **$\lambda$-planar function** relative to $(C, U, \varphi)$ if $f$ satisfies $(\star)$. If $\varphi$ is a trivial homomorphism, we say $f$ is a $\lambda$-planar function relative to $(C, U)$. We note that a 1-planar function relative to $(G, U)$ is just a planar function in the usual sense (see Pott [5]).

**Example.** Let $q = p^e$ be a power of a prime $p$ and set $G = F = (GF(q^2), +) \supset U = K = (GF(q), +)$. Then a function
$f(x) = x^{q+1}$ from $G$ to $U$ is a $q$-planar function relative to $(G, U)$.

$\because$ Let $0 \neq a \in G$ and $b \in U$. Then,

$$\begin{aligned} f(a+x) - f(x) = b &\iff (a^q + x^q)(a+x) - x^{q+1} = b \\ &\iff ax^q + a^q x = b - a^{q+1} \qquad (\star\star). \end{aligned}$$

As $ax^q + a^q x = ax^q + (ax^q)^q = \mathrm{Tr}_{F/K}(ax^q)$, $(\star\star)$ has exactly $q$ solutions in $G$. Thus $f$ is a $q$-planar function relative to $(G, U)$.

**$\lambda$-planar functions, SCTs, and RDSs**

**Theorem 8.** Let $G$ be a group of order $m$ and $U$ a group of order $u$. Let $D_y$ be subsets of $G$ for each $y \in U$. If a $u \times u$ matrix $D = [D_{yz^{-1}}]_{y,z \in U}$ over $\mathbb{Z}[G]$ is an SCT$(m, u, k, \lambda)$ matrix, then the following holds.

(i) Set $C = \bigcup_{y \in U} D_y (\subset G)$. Then $|C| = k, G = \langle C \rangle$ and a function $f : C \longrightarrow U$ defined by $f(D_y) = y \ \ (y \in U)$ is a $\lambda$-planar function relative to $(C, U)$.

(ii) Set $D = \{(x, f(x) \mid x \in C\}$. Then $D$ is an $(m, u, k, \lambda)$-RDS in $G \times U$ relative to $1 \times U$.

**Remark.** A $(u\lambda, u, u\lambda, \lambda)$-RDS is called semiregular. It is conjectured that any forbidden subgroup of a semiregular RDS is a $p$-group for a prime $p$. Concerning this we can show the following as an application of Theorems 6 and 8.

**Theorem.** *Any $p$-group can be a forbidden subgroup of a semiregular RDS.*

As a corollary we have the following, which gives another proof of de Launey's result on generalized Hadamard matrices (cf. [1], Theorem 5.9).

**Corollary** There exists a GH$(p^m, p^{2e-m})$ matrix over *any group of oder $p^m$* whenever $e \geq m$.

## References


[1] C. J. Colbourn and J. H. Dinitz, "The CRC Handbook of Combinatorial Designs", Second Edition, Chapman & Hall/CRC Press, Boca Raton, 2007.

[2] D.A. Drake, Partial $\lambda$-geometries and generalized Hadamard matrices over groups, Canad. J. Math. 31 (1979) 617-627.

[3] D. Jungnickel, On automorphism groups of divisible designs, Canad. J. Math. 34 (1982), 257-297.

[4] K. H. Leung, S. L. Ma and B. Schmidt, New Hadamard matrices of order $4p^2$ obtained from Jacobi sums of order 16, J. Combin. 113 (2006) 822-838.

[5] A. Pott, "Finite Geometry and Character Theory", Lecture Notes in Mathematics, vol. 1601, Springer, 1995.

[6] Q. Xiang, Difference families from lines and half lines, Europ. J. Combin. 19 (1998), 395-400