Title
A construction for modified generalized Hadamard matrices using QGH matrices

Author(s)
Hiramine, Yutaka

Citation
Designs, Codes and Cryptography, 62(3): 279-288

Issue date
2012-03

Type
Journal Article

URL
http://hdl.handle.net/2298/33184
A construction for modified generalized Hadamard matrices using QGH matrices

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

Abstract. Let $G$ be a group of order $mu$ and $U$ a normal subgroup of $G$ of order $u$. Let $G/U = \{U_1, U_2, \cdots, U_m\}$ be the set of cosets of $U$ in $G$. We say a matrix $H = [h_{ij}]$ order $k$ with entries from $G$ is a quasi-generalized Hadamard matrix with respect to the cosets $G/U$ if

$$\sum_{1 \leq t \leq k} h_{it}h^{-1}_{jt} = \lambda h_{ij} U_1 + \cdots + \lambda h_{im} U_m \quad (\exists \lambda_{ij1}, \cdots, \exists \lambda_{ijm} \in \mathbb{Z})$$

for any $i \neq j$. On the other hand, in our previous article we defined a modified generalized Hadamard matrix $\text{GH}(s, u, \lambda)$ over a group $G$, from which a $\text{TD}_\lambda(u\lambda, u)$ admitting $G$ as a semiregular automorphism group is obtained. In this article, we present a method for combining quasi-generalized Hadamard matrices and semiregular relative difference sets to produce modified generalized Hadamard matrices.

Keywords: transversal design, generalized Hadamard matrix, semiregular relative difference set

1 Introduction

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

(i) $\mathcal{P}$ is a set of $uk$ points partitioned into $k$ classes (called point classes), each of size $u$,

(ii) $\mathcal{B}$ is a collection of $k$-subsets of $\mathcal{P}$ (called blocks),

(iii) Any two distinct points in the same point class are incident with no block and any two points in distinct point classes are incident with exactly $\lambda$ blocks.

A transversal design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is called symmetric (and often denoted by $\text{STD}_\lambda(k, u)$) if the dual structure $\mathcal{D}^*$ of $\mathcal{D}$ is also a transversal design with the same parameters as $\mathcal{D}$. If $\mathcal{D}$ is symmetric, the point classes of $\mathcal{D}^*$ are said to be the block classes of $\mathcal{D}$. A transversal design $\mathcal{D}$ is called class regular with respect to $U$ if $U$ is an automorphism group of $\mathcal{D}$ acting regularly on each point class.
Throughout the article all groups are assumed to be finite. Let $G$ be a group. A subset $S$ of $G$ is identified with a group ring element $\sum_{x \in S} x \in \mathbb{Z}[G]$ and $S^{(-1)}$ denotes the set of inverses of the elements of $S$. A matrix $M = [g_{ij}]$ of order $k(=u\lambda)$ with entries from $G$ is called a generalized Hadamard matrix over $G$ if it satisfies $\sum_{1 \leq t \leq k} g_{it}g_{it}^{-1} = \lambda G$ for any $i \neq \ell$, where $\lambda = k/|G|$. From a generalized Hadamard matrix we obtain a symmetric transversal design admitting $G$ as a class regular automorphism group ([3]). On the other hand a modified generalized Hadamard matrix $GH(s, u, \lambda)$ over a group is defined in [6] and from this one can construct a transversal design $TD_{\lambda}(u\lambda, u)$ admitting $G$ as a automorphism group (see Result 2.2).

Let $G$ be a group of order $mu$ and $U$ a normal subgroup of $G$ of order $u$. Let $S = \{U_1, \ldots, U_m\}$ be the set of cosets of $U$ in $G$. We say that a matrix $M = [d_{ij}]$ of order $k$ with entries from $G$ is a quasi-generalized Hadamard matrix with respect to $S$ if $\sum_{1 \leq j \leq t} d_{ij}d_{ij}^{-1} = \sum_{1 \leq s \leq m} \lambda_{is}sU_s(\lambda_{is} \in \mathbb{Z})$ for any $i \neq \ell$. In this article, we present a method for combining such matrices and semiregular relative difference sets to produce modified generalized Hadamard matrices (Theorem 4.1, Theorem 4.9).

2 Preliminaries

In [6] we introduced the notion of a modified generalized Hadamard matrix over a group. We first give a summary of the related results, which we will use in the later sections.

**Definition 2.1.** ([6]) Let $G$ be a group of order $su$, where $s$ is a divisor of $u\lambda$, and $u$ and $\lambda$ are positive integers. For subsets $D_{ij}$ $(1 \leq i, j \leq t, t = u\lambda/s)$ of $G$, we call a matrix

$$[D_{ij}] = \begin{bmatrix}
D_{11} & D_{12} & \cdots & D_{1t} \\
D_{21} & D_{22} & \cdots & D_{2t} \\
\vdots & \vdots & \ddots & \vdots \\
D_{t1} & D_{t2} & \cdots & D_{tt}
\end{bmatrix}$$

a modified generalized Hadamard matrix with respect to subgroups $U_i$ $(1 \leq i \leq t)$ of $G$ of order $u$ if the following conditions are satisfied:

$|D_{ij}| = s$ for all $i, j$, $1 \leq i, j \leq t$, and

$$\sum_{1 \leq j \leq t} D_{ij}D_{ij}^{(-1)} = \begin{cases}
u\lambda + \lambda(G - U_i) & \text{if } i = \ell, \\
\lambda G & \text{otherwise.}
\end{cases} \quad (1)$$

For short, we say $[D_{ij}]$ is a $GH(s, u, \lambda)$ matrix with respect to $U_i$, $1 \leq i \leq t$. If $U_1 = \cdots = U_t = U$ for a subgroup $U$ of $G$, we simply say that $[D_{ij}]$ is a $GH(s, u, \lambda)$ matrix with respect to $U$. In this case, if $U$ is normal in $G$, then a $GH(u, \lambda)$ matrix over $U$ is obtained from the $GH(s, u, \lambda)$ matrix (see Proposition 6.3 of [6]).
We denote by $M_t(\mathbb{Z}[G])$ the set of matrices of order $t$ over the group ring $\mathbb{Z}[G]$. An incidence structure $(\mathcal{P}, \mathcal{B})$ is obtained from a GH$(s, u, \lambda)$ matrix $[D_{ij}] \in M_t(\mathbb{Z}[G])$ in the following way:

$$\mathcal{P} = \{1, 2, \cdots, t\} \times G, \quad \mathcal{B} = \{B_{jh} : 1 \leq j \leq t, \ h \in G\},$$

where $B_{jh} = \bigcup_{1 \leq i \leq t} (i, D_{ij} h) \ (= \bigcup_{1 \leq i \leq t} \{(i, dh) : 1 \leq i \leq t, \ d \in D_{ij}\})$.

Moreover, the action of $G$ on $(\mathcal{P}, \mathcal{B})$ is defined by $(i, c)x = (i, cx)$, $(B_{jh})x = B_{jhx}$.

Then, by [6] we have

**Result 2.2.** ([6]) Let $[D_{ij}] \in M_t(\mathbb{Z}[G])$ be a GH$(s, u, \lambda)$ matrix over a group $G$ of order $su$ with respect to subgroups $U_i$ $(1 \leq i \leq t)$, where $t = u\lambda/s$. If we define $\mathcal{P}$ and $\mathcal{B}$ by (2), then the following holds.

(i) $(\mathcal{P}, \mathcal{B})$ is a transversal design $TD_{\lambda}(k, u)$, where $k = u\lambda$.

(ii) $G$ is an automorphism group of $(\mathcal{P}, \mathcal{B})$ acting semiregularly both on $\mathcal{P}$ and $\mathcal{B}$.

(iii) For any $i (1 \leq i \leq t)$ and $x \in G$, $P_i U_i x$ is a point class of $(\mathcal{P}, \mathcal{B})$, on which $x^{-1}U_i x$ acts regularly.

Using Result 2.2 we can obtain transversal designs by constructing modified generalized Hadamard matrices. Transversal designs obtained from GH$(s, u, \lambda)$ matrices are not always symmetric (see Example 5.3 of [6]) and do not always admit class regular automorphism groups even if they are symmetric (see [7]).

The following gives a criterion for the resulting transversal design to be symmetric.

**Result 2.3.** (Theorem 3.10 and Corollary 3.11 of [6]) Let $[D_{ij}] \in M_t(\mathbb{Z}[G])$ be a GH$(s, u, \lambda)$ matrix over a group $G$ with respect to subgroups $U_i$ $(1 \leq i \leq t)$, where $t = u\lambda/s$. Then the transversal design $TD_{\lambda}(k, u)$, $k = u\lambda$, corresponding to $[D_{ij}]$ is symmetric if and only if the matrix

$$[D_{ij}^{(-1)}]^T = \begin{bmatrix}
D_{11}^{(-1)} & D_{21}^{(-1)} & \cdots & D_{1t}^{(-1)} \\
D_{12}^{(-1)} & D_{22}^{(-1)} & \cdots & D_{2t}^{(-1)} \\
\vdots & \cdots & \vdots & \vdots \\
D_{1t}^{(-1)} & D_{2t}^{(-1)} & \cdots & D_{tt}^{(-1)}
\end{bmatrix}$$

is a GH$(s, u, \lambda)$ matrix over $G$ with respect to suitable subgroups $V_i$ of $G$, $1 \leq i \leq t$, of order $u$. In particular, if $G \triangleright U_1 = \cdots = U_t$, then $[D_{ij}^{(-1)}]^T$ is also a GH$(s, u, \lambda)$ matrix over $G$.

Let $G$ be a group of order $u^2\lambda$ and $U$ a subgroup of $G$ of order $u$. A $u\lambda$-subset $D$ of $G$ is called a $(u\lambda, u, u\lambda, \lambda)$-difference set relative to $U$ if the list of quotients

3
with distinct elements \( d_1, d_2 \in D \) contains each element of \( G - U \) exactly \( \lambda \) times and no elements of \( U \):

\[
DD^{(-1)} = u\lambda + \lambda(G - U)
\]

We note that if \( D \) is a \((u\lambda, u, u\lambda, \lambda)\)-difference set relative to \( U \), then \([D]\) is a \(GH(u\lambda, u, \lambda)\) matrix of order 1 and the corresponding transversal design is not always symmetric (see Proposition 4.4 of [5]). A \((u\lambda, u, u\lambda, \lambda)\)-difference set is often called a semiregular relative difference set.

For an abelian group \( G \), we denote by \( G^* \) the set of (linear) characters of \( G \). Let \( \chi_0 \) be the principal character of \( G \). The following is a well known result on \( G^* \).

**Result 2.4.** ([12]) Let \( G \) be an abelian group and let \( z \in \mathbb{Z}[G] \). If \( \chi(z) = 0 \) for any character \( \chi \in G^* \), \( \chi \neq \chi_0 \), then \( z = cG \) for an integer \( c \).

The following is a slight modification of Result 2.4.

**Lemma 2.5.** Let \( U \) be a subgroup of an abelian group \( G \) and let \( z \in \mathbb{Z}[G] \). If \( \chi(z) = 0 \) for every character \( \chi \in G^* \) such that \( \chi|_U \neq \chi_0 \), then \( z = Uf \) for some \( f \in \mathbb{Z}[G] \).

**Proof.** It suffices to show that \( zg = z \) for every \( g \in U \). On the other hand, for any \( \chi \in G^* \) we have \( \chi(g - 1) = 0 \) or \( \chi(z) = 0 \) according as \( \chi|_U = \chi_0 \) or \( \chi|_U \neq \chi_0 \). Hence \( \chi(z(g - 1)) = 0 \). By Result 2.4 the lemma holds. (\( \blacksquare \))

### 3 Quasi-Generalized Hadamard Matrices with respect to cosets

In this section we give a modification of generalized Hadamard matrices from a different point of view to construct \(GH(s, u, \lambda)\) matrices that we have given in Definition 2.1.

**Definition 3.1.** Let \( N \) be a group of order \( mu \) and \( U \) a normal subgroup of \( N \) of order \( u \). Let \( N/U = \{U_1(=U), U_2, \ldots, U_m\} \) be the set of cosets of \( U \) in \( N \). We say a matrix \( H = [h_{ij}] \) of order \( k(=u\lambda) \) with entries from \( N \) is a quasi-generalized Hadamard matrix with respect to the cosets \( N/U \) (a QGH\((u, \lambda)\) matrix with respect to \( N/U \) for brevity) if there exist integers \( \lambda_{ijt} \geq 0 \) such that

\[
\sum_{1 \leq t \leq k} h_{it}h_{jt}^{-1} = \lambda_{i1}U_1 + \cdots + \lambda_{im}U_m,
\]

for any \( i, j (1 \leq i \neq j \leq k) \).

We note that the condition (4) is equivalent to the following:

\[
H(H^{(-1)})^T = \begin{bmatrix}
  k & U_{z12} & \cdots & U_{z1k} \\
  U_{z21} & k & \cdots & U_{z2k} \\
  \vdots & \ddots & \ddots & \vdots \\
  U_{zk1} & U_{zk2} & \cdots & k
\end{bmatrix}
\]
where $z_{ij} \in \mathbb{Z}[N]$ ($i \neq j$) and each coefficient of $z_{ij}$ is a non-negative integer and satisfies $\chi_0(z_{ij}) = \lambda$ for the principal character $\chi_0$ of $N$.

**Remark 3.2.**

(i) An ordinary GH($u, \lambda$) matrix over $U$ is a QGH($u, \lambda$) matrix with respect to $U/U$.

(ii) If $H = [h_{ij}]$ is a generalized Hadamard matrix over a group $U$, then $H$ is also a quasi-generalized Hadamard matrix with respect to the cosets $U/V$ for any normal subgroup $V$ of $U$. Hence, there always exists a QGH($p^s, p^m$) matrix of order $p^{s+m}$ over $(\mathbb{Z}_p)^s$ with respect to the cosets $(\mathbb{Z}_p)^s/(\mathbb{Z}_p)^t$ for any non-negative integers $m, s$ and $t(\leq s)$ (see Table 5.10 of [2]).

(iii) Let $U$ be a normal subgroup of a group $G$ and $N$ a subgroup of $G$ such that $N \geq U$. If $H$ is a QGH($u, \lambda$) matrix with respect to $N/U$, then $H$ can be regarded as a QGH($u, \lambda$) matrix with respect to $G/U$.

(iv) Since $u\lambda = (\lambda_{ij1} + \cdots + \lambda_{ijm})|U|$ by (4), we have

$$\lambda = \lambda_{ij1} + \cdots + \lambda_{ijm}$$

for any $i, j$ ($i \neq j$).

We give some examples of quasi-generalized Hadamard matrices with respect to cosets.

Let $p^n$ be any prime power and $r$ a positive integer. We denote by GR($p^n, r$) the Galois ring over $\mathbb{Z}_{p^n}$ (see [10]).

**Proposition 3.3.** Let $R = GR(p^n, r)$ be the Galois ring over $\mathbb{Z}_{p^n}$. We define a matrix $M = [m_{ij}]$ of degree $p^n$ over the additive group $(R, +)$ by $m_{ij} = ij$ for $i, j \in R$. Then $M$ is a QGH($p^n, p^{(n-1)r}$) matrix with respect to the cosets $R/I$, where $I = (p^{n-1})$ is the smallest non-zero ideal of $R$.

**Proof.** As $\bigcup_{j \in R}(m_{ij} - m_{ij}) = (i - \ell)\bigcup_{j \in R} j$. Assume $i \neq \ell$. Then, as a mapping $f(j) = (i - \ell)j$ from $R$ to the ideal $(i - \ell)R$ of $R$ is an epimorphism, $(i - \ell)\bigcup_{j \in R} j = dJ$, where $d$ is the order of the kernel of $f$ and $J = (i - \ell)R$.

We note that any nonzero ideal of $R$ is of the form $(p^s)(p^{n-1})$ for some $s (0 \leq s \leq n-1)$ (see [10] p.308). Set $J = (p^s)$ and $I = (p^{n-1})$. Then $\bigcup_{j \in R}(m_{ij} - m_{ij}) = dU_1 \cup dU_2 \cup \cdots \cup dU_t$, where $J/I = \{U_1(= I), U_2, \cdots, U_t\}$ and $t = p^{n-s-1}$. Thus the proposition holds.

**Example 3.4.** (i) In Proposition 3.3, set $n = 2$ and $r = 1$. Then $R = \mathbb{Z}_{p^2}$. Hence there exists a QGH($p, p$) matrix over $\langle a \rangle \simeq \mathbb{Z}_{p^2}$ with respect to the cosets $\langle a \rangle / \langle a^p \rangle$ for any prime $p$.

(ii) Set $N = \langle a, b \rangle \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$, $U = \langle b \rangle \simeq \mathbb{Z}_3$. Then $[\ell_{ij}]$ below is a QGH($3, 3$) matrix with respect to $N/U$. 

5
We can verify that \[ \sum_{1 \leq t \leq 9} \ell_it\ell_j^{-1} \in \{3U, 2U + Ua, 2U + Ua^2\} \quad (i \neq j). \]

**Example 3.5.** Let \( N = \langle a \rangle \simeq \mathbb{Z}_6 \) and \( U = \langle a^2 \rangle \simeq \mathbb{Z}_3 \). Then the following matrix \([h_{ij}]\) of degree 12 is a QGH(3, 4) matrix with respect to \( N/U \). We note that \[ \sum_{1 \leq t \leq 12} h_{it}h_j^{-1} \in \{4U, 3U + Ua, 2U + 2Ua\} \quad (i \neq j). \]

\[
[h_{ij}] = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & a & a^2 & a^4 & a^5 & 1 & a^2 & a^3 & a^4 & a^6 & a^7 \\
1 & 1 & a^4 & a^2 & 1 & a^2 & a^4 & 1 & a^4 & a^2 & a^6 & a^4 \\
1 & 1 & a^2 & a^4 & 1 & a^2 & a^4 & a^2 & 1 & a^2 & a^4 & a^2 \\
1 & a^4 & a & a^2 & a^3 & a & a^2 & a^3 & a^5 & a^5 & a^4 & a^4 \\
1 & a^4 & a^3 & a^4 & a^2 & a^5 & 1 & a & a^5 & a^3 & a^2 & a^4 \\
1 & a^4 & a^3 & a^2 & a & a^5 & a^4 & a^3 & a & a^5 & 1 & a^4 \\
1 & a^4 & a^5 & a^4 & 1 & a^4 & a^3 & a^2 & a^2 & a & 1 & a^4 \\
1 & a^2 & a^5 & a^2 & 1 & a^3 & 1 & a^4 & a^4 & a & a^4 & a^4 \\
1 & a^2 & a^3 & 1 & a^4 & a^5 & a^2 & a^4 & 1 & a^2 & 1 & a^2 \\
1 & a^2 & a^4 & 1 & a^3 & 1 & a^2 & a^5 & 1 & a^2 & a^4 & a^3 \\
1 & a^2 & a^5 & 1 & a^4 & a^2 & a & a^4 & a^4 & a^2 & a^4 & a^3 & a^1 & 1 \\
\end{bmatrix}
\]

By the definition of the Kronecker product the following holds.

**Proposition 3.6.** Let \( N \) be a group and \( U \) a normal subgroup of \( N \). If \( H_i(i = 1, 2) \) is a QGH\((u, \lambda_i)\) matrix with respect to \( N/U \) for \( i \in \{1, 2\} \), then \( H_1 \otimes H_2 \) is a QGH\((u, \lambda_1\lambda_2u)\) matrix with respect to \( N/U \).

We note that when \( N = U \) the assertion of the proposition coincides with that of Theorem 5.11 in [2].

**4 Semiregular relative difference sets and QGH\((u, \lambda)\) matrices with respect to cosets**

In this section we present a construction method for transversal designs by combining quasi-generalized Hadamard matrices with respect to cosets and semiregular relative difference sets.
Theorem 4.1. Let $G$ be a group of order $u^2 \mu$ and let $U$ and $N$ be subgroups of $G$ such that $N_G(U) \geq N \geq U$ and $|U| = u$. Let $H = [h_{ij}]$ be a QGH($u, \lambda$) matrix with respect to $N/U$ and let $D = (D_1, D_2, \cdots, D_k)$ ($k = u\lambda$) be a $k$-tuple of $(u\mu, u, u\mu, \mu)$-difference sets in $G$ relative to $U$. Then the following is a GH($u^2 \mu, u, u\lambda\mu$) matrix of order $k$ with respect to $U$ and the resulting $TD_{u\mu\lambda}(u^2 \mu, u)$ admits $G$ as a semiregular automorphism group.

$$M_{H,D} = \begin{bmatrix} h_{11}D_1 & h_{12}D_2 & \cdots & h_{1k}D_k \\ h_{21}D_1 & h_{22}D_2 & \cdots & h_{2k}D_k \\ \vdots & \vdots & \ddots & \vdots \\ h_{k1}D_1 & h_{k2}D_2 & \cdots & h_{kk}D_k \end{bmatrix} \quad (5)$$

Proof. Set $N/U = \{U_1(= U), U_2, \cdots, U_m\}$, where $m = [N : U]$. By assumption, for any $i, j$ ($1 \leq i \neq j \leq k$) there exist $\lambda_{ij} \geq 0$ ($1 \leq s \leq m$) satisfying

$$\sum_{1 \leq t \leq k} h_{it}h_{jt}^{-1} = \lambda_{ij1}U_1 + \lambda_{ij2}U_2 + \cdots + \lambda_{ijm}U_m \quad (6)$$

and

$$\lambda = \lambda_{ij1} + \cdots + \lambda_{ijm} \quad (7)$$

by Remark 3.2(iv). Moreover, by assumption,

$$D_tD_t^{(-1)} = u\mu + \mu(G - U) \quad (1 \leq t \leq k) \quad (8)$$

Set $M_{H,D} = [D_{ij}]$, where $D_{ij} = h_{ij}D_j$.

Assume $i \neq j$. Then we have

$$\sum_{1 \leq t \leq k} D_{it}D_{jt}^{(-1)} = \sum_{1 \leq t \leq k} h_{it}(u\mu + \mu(G - U))h_{jt}^{-1} \quad (by \ (8))$$

$$= \sum_{1 \leq t \leq k} h_{it}h_{jt}^{-1}(u\mu + \mu(G - U)) \quad (as \ N \triangleright U)$$

$$= \sum_{1 \leq s \leq m} \lambda_{ij}U_s(u\mu + \mu(G - U)) \quad (by \ (6))$$

$$= u\mu \sum_{1 \leq s \leq m} \lambda_{ij}U_s + \mu(\sum_{1 \leq s \leq m} \lambda_{ij}|U_s|)G$$

$$- \mu \sum_{1 \leq s \leq m} \lambda_{ij}|U_s|U_s$$

$$= \mu(\sum_{1 \leq s \leq m} \lambda_{ij}U_s)G = \mu uG \quad (by \ (7))$$

Assume $i = j$. Then, similarly we have

$$\sum_{1 \leq t \leq k} D_{it}D_{it}^{(-1)} = \sum_{1 \leq t \leq k} h_{it}(u\mu + \mu(G - U))h_{it}^{-1}$$

$$= ku\mu + k\mu(G - U)$$

7
It follows that
\[
\sum_{1 \leq i \leq k} D_{ii}D_{ji}(-1) = \begin{cases} 
  k\mu u + k\mu(G-U) & \text{if } i = j, \\
  k\mu G & \text{otherwise}.
\end{cases}
\]

Therefore the theorem holds. \(\square\)

**Remark 4.2.** (i) In Theorem 4.1, if there exists a \((\mu, u, u\mu, \mu)\)-difference set \(D\) in \(G\) relative to \(U\), then we may choose a \(k\)-tuple \(D = (D_g1, D_g2, \cdots, D_gk)\), where \(g_1, \cdots, g_k \in G\).

(ii) We note that \(U\) is not always a normal subgroup of \(G\) in Theorem 4.1 and so the transversal design corresponding to \(D\) might not admit a class regular automorphism group.

**Corollary 4.3.** Let \(G\) be a group of order \(u^2\mu\) and \(U\) a normal subgroup of \(G\) of order \(u\). Let \(H = [h_{ij}]\) be a QGH\((u, \lambda)\) matrix with respect to \(G/U\) and \(D = (D_1, D_2, \cdots, D_k) (k = u\lambda)\) an \(n\)-tuple of \((\mu, u, u\mu, \mu)\)-difference sets in \(G\) relative to \(U\). Then the matrix of order \(k\) defined by \((5)\) is a GH\((\mu u, u, u\lambda)\) matrix with respect to \(U\) and gives an STD\(_{\mu u, \lambda}(u^2\mu, u)\).

**Proof.** The corollary immediately follows from Result 2.3 and Theorem 4.1. \(\square\)

**Lemma 4.4.** Assume the existence of a \((p\mu, p, p\mu, \mu)\)-difference set in a group \(G\) relative to a subgroup \(U \simeq \mathbb{Z}_p\) of \(G\) for a prime \(p\). If \(p^2 \mid |C_G(U)|\), then there exists a TD\(_{2\mu, p}(p^2\mu, p)\) admitting \(G\) as a semiregular automorphism group.

**Proof.** By assumption, there exists a subgroup \(N\) of \(G\) such that \(U \leq N \simeq \mathbb{Z}_{p^2}\) or \(\mathbb{Z}_p \times \mathbb{Z}_p\). Let \(D = (D_1, \cdots, D_{p^2})\) be a \(p^2\)-tuple of \((\mu, u, u\mu, \mu)\)-difference sets in \(G\) relative to \(U\). It follows from Example 3.4(i) or Remark 3.2(ii) that there is a QGH\((p, p)\) matrix with respect to \(N/U\), say \(H\). Applying Theorem 4.1, \(M_{H,D}\) is a GH\((p\mu, p, p^2\mu)\) matrix with respect to \(U\) and we obtain a TD\(_{2\mu, p}(p^2\mu, p)\) from \(M_{H,D}\), which admits \(G\) as a semiregular automorphism group. Thus the lemma holds. \(\square\)

**Example 4.5.** (i) Set \(G = \langle a, b, c \mid a^7 = b^3 = c^3 = 1, ac = ca, bc = cb, b^{-1}ab = a^2 \rangle\) and let \(D\) be a \((21, 3, 21, 7)\)-difference set relative to \(U = \langle c \rangle \simeq \mathbb{Z}_7\) \(([1])\). By Lemma 4.4, there exists a TD\(_{2\mu, 7}(3^7\mu, 3)\) admitting \(G \simeq (\mathbb{Z}_7 \times \mathbb{Z}_3) \times \mathbb{Z}_3\) as a semiregular automorphism group.

(ii) Set \(G = \langle r, s \rangle \simeq \text{Sym}(3) \times \mathbb{Z}_6\), where \(r^2 = s^3 = r^6 = 1, [r, s] = [s, r] = 1\) and \(rsr = s^{-1}\) and let \(D\) be a \((12, 3, 12, 4)\)-difference set in \(G\) relative to a non-normal subgroup \(U = \langle s^2 \rangle\) \(([5])\). By Lemma 4.4, there exists a TD\(_{108, 3}(108\mu, 3)\) admitting \(G \simeq \text{Sym}(3) \times \mathbb{Z}_6\) as a semiregular automorphism group.

**Example 4.6.** Assume that there exists a \((3\mu, 3\mu, \mu)\)-difference set in a group \(G\) relative to a subgroup \(U \simeq \mathbb{Z}_3\) of \(G\) and that \(2 \mid |C_G(U)|\). Let \(D = (D_1, \cdots, D_{12})\) be a \(12\)-tuple of \((3\mu, 3\mu, \mu)\)-difference sets in \(G\) relative to \(U\). By assumption, there exists a subgroup \(N\) of \(G\) such that \(U \leq N \simeq \mathbb{Z}_6\). It follows from Example 3.5 that there is a QGH\((3, 4)\) matrix with respect to \(N/U\),
Lemma 4.7. Let $G$ be an abelian group of order $u^2\mu$ and let $D = (D_1, \cdots, D_k)$ be a $k$-tuple of $(u\mu, u, u\mu, \mu)$-difference sets in $G$ relative to a subgroup $U$ of $G$ of order $u$, where $k = u\lambda$ for some $\lambda \in \mathbb{Z}$. Let $h_{ij}(1 \leq i, j \leq k)$ be elements of $G$. Then a matrix $M = [h_{ij}D_j]$ of order $k$ is a $\text{GH}(u\mu, u, u\lambda u)$ matrix with respect to $U$ if and only if $H = [h_{ij}]$ is a $\text{QGH}(u, \lambda)$ matrix with respect to $G/U$. If this is the case, the resulting TD $u\lambda u(u^2\mu, u)$ is symmetric.

Proof. By definition, $M$ is a $\text{GH}(u\mu, u, u\lambda u)$ matrix if and only if

$$
\sum_{1 \leq j \leq k} h_{ij}D_j(h_{ij}D_j)^{(-1)} = \begin{cases} k\mu + k\mu(G - U) & \text{if } j = \ell, \\ \mu k G & \text{otherwise}. \end{cases}
$$

(9)

Since $G$ is abelian, $\sum_{1 \leq j \leq k} h_{ij}D_j(h_{ij}D_j)^{(-1)} = \sum_{1 \leq j \leq k} h_{ij}h_{ij}^{-1}D_jD_j^{(-1)} = (u\mu + \mu(G - U))\sum_{1 \leq j \leq k} h_{ij}h_{ij}^{-1}$. Hence, by Result 2.4, (9) is equivalent to

$$
\chi(u\mu - \mu\chi(U))\chi\left(\sum_{1 \leq j \leq k} h_{ij}h_{ij}^{-1}\right) = 0 \quad (i \neq \ell)
$$

(10)

for any character $\chi(\neq \chi_0)$ of $G$. Clearly (10) is equivalent to $\chi\left(\sum_{1 \leq j \leq k} h_{ij}h_{ij}^{-1}\right) = 0$ for any character $\chi$ of $G$ such that $\chi|_U \neq \chi_0$. Applying Lemma 2.5, this is equivalent to the condition that $H$ is a $\text{QGH}(u, \lambda)$ matrix with respect to the cosets $G/U$. If this is the case, the resulting TD $u\lambda u(u^2\mu, u)$ is symmetric by Result 2.3. Therefore the proposition holds. \qed

Example 4.8. Set $G = \langle a \rangle \times \langle b \rangle \simeq \mathbb{Z}_9 \times \mathbb{Z}_3, N = \langle a \rangle \simeq \mathbb{Z}_9$ and $U = \langle a^3 \rangle \simeq \mathbb{Z}_3$. Let $H = [h_{ij}]$ be a $\text{QGH}(3, 3)$ matrix with respect to $N/U$ in Example 3.4(i). As $G$ contains $(9, 3, 9, 3)$-difference sets relative to $U$ (see [9]), we can choose a 9-tuple $D = (D_1, \cdots, D_9)$ of $(9, 3, 9, 3)$-difference sets in $G$ relative to $U$. Then, by Theorem 4.1, $M_{H,D}$ is a $\text{GH}(9, 3, 27)$ matrix with respect to $U$. Moreover, by Lemma 4.7, the TD $D_{27}(81, 3)$ obtained from $M_{H,D}$ is symmetric.

When $D$ is a $(u\mu, u, u\mu, \mu)$-difference set in $G$ relative to $U$, $D$ is a complete set of right coset representatives of $U$ in $G$ by (3), but $D^{(-1)}$ is not so in general. If some $(u\mu, u, u\mu, \mu)$-difference set in $G$ satisfies this condition, then we have the following.

Theorem 4.9. Let $G$ be a group of order $u^2\mu$ and let $U$ and $N$ be subgroups of $G$ such that $|N| = mu, |U| = u$ and $N_G(U) \geq N \geq U$ and $|U| = u$. Let $H = [h_{ij}]$ $(h_{ij} \in N)$ be a $\text{QGH}(u, \lambda)$ matrix with respect to $N/U$ and let $D = (D_1, D_2, \cdots, D_k)$ $(k = u\lambda)$ be a $k$-tuple of $(u\mu, u, u\mu, \mu)$-difference sets in $G$. Assume at least $k - 1$ of $D_i$’s are complete sets of right and left coset
representatives of \( U \) in \( G \). Then the following matrix \( M'_{H,D} \) of order \( k \) is a GH\((u\mu, u, u\mu)\) matrix with respect to \( U \) and the resulting TD\(_{u\mu\lambda}(u^2\mu\lambda, u)\) admits \( G \) as a semiregular automorphism group.

\[
M'_{H,D} = \begin{bmatrix}
D_1h_{11} & D_1h_{12} & \cdots & D_1h_{1k} \\
D_2h_{21} & D_2h_{22} & \cdots & D_2h_{2k} \\
\vdots & \vdots & \ddots & \vdots \\
D_kh_{k1} & D_kh_{k2} & \cdots & D_kh_{kk}
\end{bmatrix}
\]

(11)

Proof. Set \( N/U = Ug_1 \cup \cdots \cup Ug_m \) \((g_1, \ldots, g_m \in N)\), where \( m = [N : U] \). By assumption,

\[
\sum_{1 \leq t \leq k} h_{it}h_{jt}^{-1} = \lambda_{ij1}Ug_1 + \cdots + \lambda_{ijm}Ug_m
\]

(12)

for some non-negative integers \( \lambda_{ij}s \) \((1 \leq i \neq j, 1 \leq s \leq m)\).

Set \( M'_{H,D} = [D_{ij}] \), where \( D_{ij} = D_i h_{ij} \). Then

\[
\sum_{1 \leq t \leq k} D_{it}D_{jt}^{(-1)} = \sum_{1 \leq t \leq k} D_i h_{it}h_{jt}^{-1} D_j^{(-1)}
\]

\[
= D_i \left( \sum_{1 \leq t \leq k} h_{it}h_{jt}^{-1} \right) D_j^{(-1)}
\]

Hence, by (12)

\[
\sum_{1 \leq t \leq k} D_{it}D_{jt}^{(-1)} = \begin{cases} 
ku\mu + k\mu(G - U) & \text{if } i = j, \\
D_i(\lambda_{ij1}Ug_1 + \cdots + \lambda_{ijm}Ug_m)D_j^{(-1)} & \text{otherwise}. 
\end{cases}
\]

Assume \( i \neq j \). By assumption, either \( D_i \) or \( D_j \) is a complete set of right and left coset representatives of \( U \) in \( G \) as \( i \neq j \). Hence we have either \( D_iU = G \) or \( UD_j^{(-1)} = G \). In either case, \( \sum_{1 \leq t \leq k} D_{it}D_{jt}^{(-1)} = \lambda u\mu G \) as \( N \triangleright U \). Thus

\[
\sum_{1 \leq t \leq k} D_{it}D_{jt}^{(-1)} = \begin{cases} 
ku\mu + k\mu(G - U) & \text{if } i = j, \\
k\mu G & \text{otherwise}. 
\end{cases}
\]

Therefore the theorem holds. \( \square \)

**Corollary 4.10.** Let \( G \) be a group of order \( u^2\mu \) and \( U \) a normal subgroup of \( G \) of order \( u \). Let \( H = [h_{ij}] \) be a QGH\((u, \lambda)\) matrix with respect to \( G/U \) and \( D = (D_1, D_2, \ldots, D_k) \) \((k = u\lambda)\) a \( k \)-tuple of \((u\mu, u, u\mu)\)-difference sets in \( G \) relative to \( U \). Then the matrix of order \( k \) defined by (11) is a GH\((u\mu, u, u\lambda\mu)\) matrix with respect to \( U \) and the resulting TD\(_{u\mu\lambda}(u^2\mu\lambda, u)\) admits \( G \) as a semiregular automorphism group.
Example 4.11. Many \((4n^2, 2n^2 - n, n^2 - n)\)-difference sets have been constructed in abelian groups of order \(4n^2\) and they are called Menon Hadamard difference sets ([8]). Let \(L\) be an abelian group of order \(4n^2\) containing a Menon Hadamard difference set \(A\). Assume that \(L\) is not an elementary abelian 2-group. We define a group \(G = L \langle t \rangle\) of order \(8n^2\), where an element \(t\) of \(G\) inverts \(L\). By a similar way as in Proposition 4.14 of [4], we can verify that \(D = A + (L - A^{(-1)})t\) is a \((4n^2, 2, 4n^2, 2n^2)\)-difference set in \(G\) relative to \(U = \langle t \rangle\). We choose \(A\) so that it satisfies \(A = A^{(-1)}\) (see Problem 2 in Chapter 4 of [8]). For \(g \in L\), \(Dg\) is a \((4n^2, 2, 4n^2, 2n^2)\)-difference set in \(G\) relative to \(U\). However, as \((Dg)^{(-1)}(Dg) = 4n^2 + 2n^2(G - \langle gt \rangle)\), \(Dg\) is not a complete set of left coset representatives of \(U\) in \(G\). Clearly \(C_G(t)\) contains a subgroup \(N\) of the form \(N = \langle t \rangle \times \langle s \rangle\) isomorphic to \(Z_2 \times Z_2\). Let \(H = [h_{ij}]\) be the following \(QGH(2, 2)\) matrix with respect to \(N/U\):

\[
H = \begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & t & s & st \\
1 & 1 & t & t \\
1 & t & st & s
\end{bmatrix}
\]

Set \(D = (D, D, D, Dg)\). Then, applying Theorem 4.9, \(M'_{H, D}\) is a \(GH(4n^2, 2, 8n^2)\) matrix with respect to \(U\) and the resulting \(TD_{8n^2}(16n^2, 2)\) admits \(G\) as a semiregular automorphism group.

Acknowledgment

The author would like to thank the referees for valuable suggestions and comments. The author also thanks one of the referees who showed him a shorter proof of Lemma 2.5.

References


