On Butson Hadamard matrices and
an extension of difference matrices

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

1 Introduction

Definition 1.1. Let $U$ be a group of order $u$ and $k, \lambda$ positive integers. In this note, we often identify a subset $S$ of $U$ with the group ring element $\sum_{x \in S} x \in \mathbb{Z}[U]$.

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 $(u, k, \lambda)$-difference matrix over $U$ (for short, a $(u, k, \lambda)$-DM over $U$) if
$$d_{i,1}d_{\ell,1}^{-1}+\cdots+d_{i,u\lambda}d_{\ell,u\lambda}^{-1} = \lambda U$$
for any $i, \ell$ $(1 \leq i \neq \ell \leq k)$.

Example 1.2. \begin{bmatrix} 1 & 1 & 1 \\ 1 & a & a^2 \\ 1 & a^2 & a \end{bmatrix} is a $(3, 3, 1)$-DM over $\langle a \rangle \simeq \mathbb{Z}_3$.

The following result on difference matrices is well known.

Result 1.3. (D. Jungnickel [6]) If there exists $(u, k, \lambda)$-DM, then $k \leq u\lambda$.

A $(u, u\lambda, \lambda)$-DM is called a GH$(u, \lambda)$ matrix (a generalized Hadamard matrix).

The following conjecture is well known.

Conjecture. If there exists a GH$(u, \lambda)$ matrix over a group $G$, then $G$ is a $p$-group for some prime $p$.

The following are well known construction methods for difference matrices

Result 1.4. (M. Buratti [1]) Let $G = \mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_t}}$, where $p$ is a prime. Set $e = \sum n_i$ and $f = \lceil e/\max\{n_1, \cdots, n_t\} \rceil$. Then there exists a $(p^e, p^f, 1)$-DM over $G$. 


Result 1.5. (M. Buratti [1]) If $G > N$ and there exist a $(|G/N|, k, \lambda)$-DM over $G/N$ and a $(|N|, k, \mu)$-DM over $N$, then there exists a $(|G|, k, \lambda\mu)$-DM over $G$.

Result 1.6. (Kronecker product) Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be a $(u, k_1, \lambda_1)$-DM over $G$ and $(u, k_2, \lambda_2)$-DM over $G$, respectively. Then $A \otimes B = [a_{ij}b_{ij}]$ is a $(u, k_1k_2, u\lambda_1\lambda_2)$-DM over $G$.

Result 1.7. (W. de Launey, [8]) Let $G$ be any $p$-group of order $q = p^n$. Then there exists a $(q, q^{2t}, q^{2t-1})$-DM over $G$ for any positive integer $t$.

There is a relation between difference matrices and orthogonal arrays.

Definition 1.8. A $k \times u^2\lambda$ array $A$ over a $u$-set $U$ is called an OA$_\lambda(k,u)$ (orthogonal array) if any $2 \times u^2\lambda$ subarray of $A$ contains each $2 \times 1$ column vector exactly $\lambda$ times.

An OA$_\lambda(k,u)$ $A_D$ obtained from a $(u, k, \lambda)$-DM $D$ over $U$ is as follows:

$A_D := [Dg_1, \ldots, Dg_u]$, where $U = \{g_1, \ldots, g_u\}$ [3].

The above array can be extended to OA$_\lambda(k+1,u)$ in the following way : [3]:

Let $D = [D_1, \ldots, D_u]$ ($\forall D_j : k \times \lambda$ matrix) be a division of $(u, k, \lambda)$-DM $D$ and set $J := J_\lambda(= [1, \ldots, 1])$. Then the following is an OA$_\lambda(k+1,u)$.

$M = \begin{bmatrix} D_1g_1 & \cdots & D_1g_u & \cdots & D_2g_1 & \cdots & D_2g_u & \cdots & D_u\lambda g_1 & \cdots & D_u\lambda g_u \\ Jg_1 & \cdots & Jg_u & \cdots & Jg_2 & \cdots & Jg_u & \cdots & Jg_1 & \cdots & Jg_u \end{bmatrix}$

We note that $U$ does not act on $M$ as a class regular automorphism group of $M$. Therefore $D$ can not, in general, be extended to a $(u, k+1, \lambda)$-DM over $U$.

We consider following problem.

Problem. Given a group $U$ of order $u$ and an integer $\lambda > 0$, what can we say about $k$ for which a $(u, k, \lambda)$-DM over $U$ exists ?

Definition 1.9. Let $M$ be a $(u, k, \lambda)$-DM over a group $U$ of order $u$ and set $d_M = u\lambda - k$. We call $d_M$ the deficiency of $M$.

Result 1.10. (Drake, [5]) Assume that $\lambda$ is odd and a group $U$ has a nontrivial cyclic Sylow 2-subgroup. If there exists $(u, k, \lambda)$-DM, then $k \leq 2$.

Result 1.11. (Lampio-Ostergard, [7]) The following holds.

(i) $\max\{k \mid 3(3, k, 5)$-DM over $\mathbb{Z}_3\} = 9$.

(ii) $\max\{k \mid 5(5, k, 3)$-DM over $\mathbb{Z}_5\} = 8$.

(iii) $\max\{k \mid 6(6, k, 2)$-DM over $\mathbb{Z}_6\} = 6$.

2 Examples of maximal difference matrices

Example 2.1. (Drake [5]) Let $G = \{g_1 = 1, \ldots, g_{2n}\}$ be a group of order $2n$ with a cyclic Sylow 2-subgroup. If $2 \nmid \lambda$, then the following is a maximal $(2n, 2, \lambda)$-DM over $G$

$M_{2n} = \begin{bmatrix} 1 & \cdots & 1 & \cdots & 1 & \cdots & 1 \\ g_1 & \cdots & g_1 & \cdots & g_{2n} & \cdots & g_{2n} \end{bmatrix}$
Example 2.2. Let $p$ be a prime and set $a_{ij} = ij \pmod p$ $(i, j \in \mathbb{Z}_p)$. Then $D_p = [a_{ij}]_{0 \leq i,j \leq p-1}$ is a $(p,p,1)$-DM over $\mathbb{Z}_p$. When $p = 3, 5$, we can verify that $D_p$ is the only maximal $(p,k,1)$-DM. Therefore, any $(p,k,1)$-DM with $p \in \{3, 5\}$ can be extended to $(p,p,1)$-DM. However, when $p = 7$, the following is also a maximal $(7,3,1)$-DM:

\[
M = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 3 & 4 & 5 & 6 \\
0 & 2 & 5 & 1 & 6 & 4 & 3
\end{bmatrix}, \quad \text{where } d_M = 4.
\]

Example 2.3. The following is a maximal $(3,3,2)$-DM over $\mathbb{Z}_3$.

\[
M = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 2 & 2 \\
0 & 0 & 2 & 2 & 1 & 1
\end{bmatrix}, \quad \text{where } d_M = 3.
\]

However, there exists a $(3,6,2)$-DM.

Example 2.4. The following is a unique maximal $(8,k,1)$-DM over $\langle a, b \rangle \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$.

\[
M = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & a & a^2 & a^3 & b & ab & a^2b & a^3b \\
1 & a^2 & b & a^2b & a & ab & a^2 & a \\
1 & a^3 & a^2b & ab & a^3b & a^2 & a & b
\end{bmatrix}, \quad \text{where } d_M = 4.
\]

We note that there exists a $(p^3,p,1)$-DM over $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ for any prime $p$ by a result of Buratti [1].

Concerning Example 2.4 we would like to raise the following question.

Question. Does there exist a $(p^3,p,1)$-DM over $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ for a prime $p$?

Example 2.5. The following is the only maximal $(9,k,1)$-DM over $\mathbb{Z}_9$.

\[
M = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
0 & 2 & 1 & 6 & 8 & 7 & 3 & 5 & 4
\end{bmatrix}, \quad \text{(d}_M = 6)
\]

Let $U = \langle a \rangle \simeq \mathbb{Z}_{p^2}$. As $U/\langle a^p \rangle \simeq \langle a^p \rangle \simeq \mathbb{Z}_p$, by a result of Buratti [1], the exists a $(p^2,p,1)$-DM over $\mathbb{Z}_{p^2}$ for any prime $p$.

Concerning Example 2.5 we would like to raise the following question.

Question. Is a $(p^2,p,1)$-DM the only maximal DM over $\mathbb{Z}_{p^2}$?

Example 2.6. The following is a unique maximal $(4,k,2)$-DM over $\mathbb{Z}_4$.

\[
M = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 2 & 2 & 3 & 3 \\
0 & 0 & 2 & 3 & 1 & 3 & 1 & 2 \\
0 & 0 & 3 & 2 & 3 & 1 & 2 & 1
\end{bmatrix}, \quad \text{(d}_M = 4)
\]

Example 2.7. The following are maximal $(4,k,2)$-DMs $M$ over $\{0,a,b,c\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

\[
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & a & a & b & b & c & c \\
0 & 0 & b & b & c & c & a & a \\
0 & 0 & c & c & a & a & b & b
\end{bmatrix}, \quad \text{a maximal $(4,4,2)$-DM with } d_M = 4
\]
We give an infinite family of maximal difference matrices.

**Proposition 2.8.** Let $p$ be a prime with $p^n \nmid \lambda$ and let $L$ be the multiplication table of $K = GF(p^n)$. Set $J = J_{\lambda} = (1, \cdots , 1)$. Then $M = L \otimes J$ is a maximal $(p^n, p^n, \lambda)$-DM over $\mathbb{Z}_p^n$.

**Proof.** Set $K = \{k_0 = 0, k_1, k_2, \cdots , k_s\}$, $s = p^n - 1$. Then the following is a $(p^n, p^n, \lambda)$-DM over $(K, +)$.

$$M = \begin{bmatrix}
    k_0k_0J & k_0k_1J & \cdots & k_0k_sJ \\
    k_1k_0J & k_1k_1J & \cdots & k_1k_sJ \\
                   & \cdots & \cdots & \cdots \\
    k_sk_0J & k_sk_1J & \cdots & k_sk_sJ
\end{bmatrix}$$

Assume that we can obtain $(p^n, p^n + 1, \lambda)$-DM $\widehat{M} = [m_{ij}](0 \leq i \leq s + 1, 0 \leq j \leq p^n\lambda - 1)$ by adding the $s + 2$ ($= p^n + 1$)-th row, say $w$ to $M$. Let $w = (m_{s+1,0}, m_{s+1,1}, \cdots , m_{s+1,p^n\lambda - 1})$ and $m = \#\{(i,j) \mid m_{i,j} = m_{s+1,j}, 0 \leq i \leq s, 0 \leq j \leq p^n\lambda - 1\}$. We count $N = \#\{i \mid m_{i,j} = m, 0 \leq i \leq \lambda - 1\}$ in two ways. Then we have $ap^n + (p^n\lambda - \lambda) \cdot 1 = \lambda p^n$. Thus $ap^n = \lambda$, contrary to $p^n \nmid \lambda$. \square

The following is a table of $k$ for which there exists a maximal $(u, k, \lambda)$-DM over an abelian group $U$ with $2 \leq u\lambda \leq 12$.

<table>
<thead>
<tr>
<th>$u$</th>
<th>$U$</th>
<th>$\lambda$</th>
<th>$k$</th>
<th>$u\lambda$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$\mathbb{Z}_2$</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>$\mathbb{Z}_3$</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>$\mathbb{Z}_4$</td>
<td>1</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_2$</td>
<td>1</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>$\mathbb{Z}_5$</td>
<td>1</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>$\mathbb{Z}_2$</td>
<td>3</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>$\mathbb{Z}_3$</td>
<td>2</td>
<td>3,6</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>$\mathbb{Z}_6$</td>
<td>1</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>$\mathbb{Z}_7$</td>
<td>1</td>
<td>3,7</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_4$</td>
<td>1</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>$\mathbb{Z}_8$</td>
<td>1</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>$\mathbb{Z}_2$</td>
<td>4</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>$\mathbb{Z}_4$</td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_2$</td>
<td>2</td>
<td>4,6,8</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$u$</th>
<th>$U$</th>
<th>$\lambda$</th>
<th>$k$</th>
<th>$u\lambda$</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>$\mathbb{Z}_8$</td>
<td>1</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$</td>
<td>1</td>
<td>4,8</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>$\mathbb{Z}_9$</td>
<td>1</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>$\mathbb{Z}_3 \times \mathbb{Z}_3$</td>
<td>1</td>
<td>4,6</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>$\mathbb{Z}_3$</td>
<td>3</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>10</td>
<td>$\mathbb{Z}_{10}$</td>
<td>1</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>$\mathbb{Z}_5$</td>
<td>2</td>
<td>4,5,6,10</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>$\mathbb{Z}_2$</td>
<td>5</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>11</td>
<td>$\mathbb{Z}_{11}$</td>
<td>1</td>
<td>3,4,5,11</td>
<td>11</td>
</tr>
<tr>
<td>12</td>
<td>$\mathbb{Z}_{12}$</td>
<td>1</td>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>2</td>
<td>$\mathbb{Z}_2$</td>
<td>6</td>
<td>4,12</td>
<td>12</td>
</tr>
<tr>
<td>3</td>
<td>$\mathbb{Z}_3$</td>
<td>4</td>
<td>6,9,12</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_2$</td>
<td>3</td>
<td>4,5,6,12</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>$\mathbb{Z}_4$</td>
<td>3</td>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>6</td>
<td>$\mathbb{Z}_6$</td>
<td>2</td>
<td>4,5,6</td>
<td>12</td>
</tr>
</tbody>
</table>
From the table, it is conceivable that $d_M \geq 2$ except for GH matrices. From this, we would like to propose the following conjecture (see [4]).

**Conjecture.** Any $(u, u\lambda - 1, \lambda)$-DM over a group $U$ can be extended to a $(u, u\lambda, \lambda)$-DM over $U$ (i.e. GH$(u, \lambda)$ matrix).

The following two results might be relevant to this.

**Result 2.9.** (W. de Launey, [8]) Assume that $2 \nmid u\lambda$ and there exists a $(u, u\lambda, \lambda)$-DM over $G$. Let $p$ be a prime divisor of $u$ and $m$ a divisor of the square free part of $\lambda$. Then $\text{Ord}_p(m) \equiv 1 \pmod{2}$.

**Result 2.10.** (A. Winterhof, 2002) Assume that $2 \nmid u\lambda$ and there exists a $(u, u\lambda - 1, \lambda)$-DM over $G$. Let $p$ be a prime divisor of $u$ and $m$ a divisor of the square free part of $\lambda$. Then $\text{Ord}_p(m) \equiv 1 \pmod{2}$.

We note that though the conditions of the above two results are different, the conclusions are the same.

3 An extension to GH matrices and BH matrices

Concerning the above conjecture we prove the following.

**Theorem 3.1.** Let $p$ be a prime and $G$ an abelian group of order $q(= p^n)$. Then $(q, q\lambda - 1, \lambda)$-DM over $G$ can be extended to a $\text{GH}(q, \lambda)$ matrix over $G$.

To show this we use the following well known result on characters.

**Result 3.2.** (inversion formula) Let $\hat{G}$ be the set of characters of an abelian group $G$ and let $f = \sum_{g \in G} a_g g \in \mathbb{C}[G]$. Then, $a_g = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(f) \chi(g^{-1})$, In particular, if $\chi(f) = 0$ for any $\chi \in \hat{G}$, $\chi \neq \chi_0$, then $f = \chi_0(f) \sum_{g \in G} g$.

Assume that a $(q, q\lambda - 1, \lambda)$-DM $N$ over abelian group $G$ is extended to $\text{GH}(q, \lambda)$ matrix over $G$, say $M$ ($M_{ij} \in G$). Let $\chi \neq \chi_0$ be any character of $G$ and define $\chi(M) := [\chi(M_{ij})]$. Let $p^e$ be the exponent of $G$. Then $\chi(M_{ij}) \in \langle \zeta_{p^e} \rangle$, where $\zeta_{p^e}$ is a primitive $p^e$th root of unity. As $M_{i,1} M_{\ell,1}^{-1} + \cdots + M_{i,u\lambda} M_{\ell,u\lambda}^{-1} = \lambda G$, for any $i, \ell$ with $i \neq \ell$, $\chi(M)$ satisfies the following.

$$\chi(M) \chi(M)^* = m I \quad (I = I_m, \ m = u\lambda). \quad (1)$$

Similarly, $\chi(N)$ is an $(m - 1) \times m$ matrix satisfying

$$\chi(N) \chi(N)^* = m I_{m-1}. \quad (2)$$

A matrix with the property (1) is defined in [2].
Definition 3.3. A matrix $B$ of degree $m$ is called a Butson Hadamard matrix $BH(m, s)$ if $B_{ij} \in \langle \zeta_{s} \rangle$ for all $i, j$ and $B$ satisfies $BB^{*} = mI_{m}$.

In this note we define a matrix with the property (2) as follows.

Definition 3.4. We call a $(m - 1) \times m$ $(m \geq 3)$ matrix $A$ a near Butson Hadamard matrix and denote it by $NBH(m, s)$ if $A_{ij} \in \langle \zeta_{s} \rangle$ and $A$ satisfies $AA^{*} = mI_{m-1}$.

Example 3.5. The following is a $BH(6, 6)$.

$$M = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & -1 \\
1 & -\omega & \omega^{2} & -1 & \omega & -\omega^{2} \\
1 & 1 & \omega & \omega^{2} & \omega & \omega^{2} \\
1 & \omega & \omega^{2} & 1 & \omega & \omega^{2} \\
1 & -1 & \omega & -\omega & \omega^{2} & -\omega^{2}
\end{bmatrix}, \quad \omega = \zeta_{3}$$

The above conjecture gives rise to the problem of the extension of $NBH(m, s)$ to $BH(m, s)$.

Problem. Can $NBH(m, s)$ be extended to $BH(m, s)$?

Concerning this we show that $NBH(m, s)$ can be extended $BH(m, s)$ under the condition that $m$ is a power of a prime.

Proposition 3.6. Let $p$ be a prime and set $\theta = \zeta_{p^{n}}$. Let $A = [v_{ij}]$ be a $NBH(m, p^{n})$ matrix such that $v_{11} = v_{21} = \cdots = v_{m-1, 1} = 1$.

$$M = \begin{bmatrix}
1 & v_{12} & \cdots & v_{1,m} \\
1 & v_{22} & \cdots & v_{2,m} \\
\vdots & \vdots & \ddots & \vdots \\
1 & v_{m-1, 2} & \cdots & v_{m-1,m}
\end{bmatrix}$$

Set $v_{i} = (v_{i1}, \cdots, v_{im})$ $(1 \leq i \leq m - 1)$. Then,

(i) $p \mid m$,

(ii) Set $v = (m, 0, \cdots, 0) - (v_{1} + \cdots + v_{m-1})$. Then each entry of $v$ is an element of $\langle \theta \rangle$. In particular, each column sum of $M$ is $m - 1$ or an element of $-\langle \theta \rangle$, and

(iii) Let $\tilde{A}$ be a matrix of degree $m$ adding $v$ to $M$ as a row. Then $\tilde{A}$ is a $BH(m, p^{n})$ matrix.

To show the proposition we use the following lemma.

Lemma 3.7. Let $p$ be a prime and set $\theta = \zeta_{p^{n}}$. For $a_{0}, \cdots, a_{p^{n}-1} \in \mathbb{Q}$, assume that $(\ast)$ $a_{0} + a_{1}\theta + \cdots + a_{p^{n}-1}\theta^{p^{n}-1} = 0$. Then,

(i) $a_{i} = a_{j}$ whenever $i \equiv j \pmod{p^{n-1}}$ and

(ii) if $a_{0}, \cdots, a_{p^{n}-1} \in \mathbb{Z}$, then $\sum_{0 \leq i \leq p^{n}-1} a_{i} \equiv 0 \pmod{p}$.

Sketch of the proof

The cyclotomic polynomial $\Phi_{p^{n}}(x) = \frac{x^{p^{n}-1} - 1}{x^{p^{n-1}} - 1}$ is a minimal polynomial of $\theta$ over $\mathbb{Q}$. As $\Phi_{p^{n}}(x) = x^{(p-1)p^{n-1}} + x^{(p-2)p^{n-1}} + \cdots + x^{p^{n-1}} + 1,$
\[ (**) \quad \theta^{(p-1)p^{n-1}} + \theta^{(p-2)p^{n-1}} + \cdots + \theta^{p^{n-1}} + 1 = 0. \]

Hence \( \theta^{(p-1)p^{n-1}+t} = -\theta^{(p-2)p^{n-1}+t} - \cdots - \theta^{p^{n-1}+t} - p^t \) for any \( t \) with \( 0 \leq t \leq p^{n-1} - 1 \). Substituting these into (*) and using the minimality of (**) we can obtain the lemma.

**Proof of Proposition 3.6**

Set \( I = \{0, 1, \ldots, p^n - 1\} \). Let \( c_i \) be the number of \( \theta^i \) contained in the multiset \( \{v_{11}v_{21}, v_{12}v_{22}, \ldots, v_{1m}v_{2m}\} \). As \( v_{11}v_{21}^T = 0 \), \( \sum_{i \in I} c_i \theta^i = 0 \) and \( \sum_{i \in I} c_i = m \). Therefore \( p \mid m \) by (ii) of Lemma 3.7.

As \( v = (m, 0, \ldots, 0) - (v_1 + \cdots + v_{m-1}) \), \( v \cdot v_i = m - v_1 \cdot v_i = 0 \). Hence \( v \perp v_1, \ldots, v_{m-1} \). On the other hand, setting \( \alpha_t = \sum_{1 \leq i \leq m-1} v_{it} \) \( (2 \leq t \leq m) \), we have \( v = (1, -\alpha_2, \ldots, -\alpha_m) \). Moreover \( v_1 + \cdots + v_{m-1} = (m-1, \alpha_2, \ldots, \alpha_m) \). From this, \( 0 = (v_1 + \cdots + v_{m-1}, v) = m - 1 - \alpha_2\alpha_2 - \cdots - \alpha_m\alpha_m \). Thus \( \alpha_2\alpha_2 + \cdots + \alpha_m\alpha_m = m - 1 \). Let \( a_{ij} \) \( (0 \leq j \leq p^n - 1) \) be the number of the value \( \theta^j \) appeared in the multiset \( \{v_{1,t}, v_{2,t}, \ldots, v_{m-1,t}\} \). As \( \alpha_t = \sum_{1 \leq i \leq m-1} v_{it} \), it follows that

\[
\alpha_t = a_{t,0} + a_{t,1}\theta + a_{t,2}\theta^2 + \cdots + a_{t,p^n-1}\theta^{p^n-1}
\]

\[
a_{t,0} + a_{t,1} + \cdots + a_{t,p^n-1} = m - 1 \quad (3)
\]

As \( \alpha_i\alpha_i = \sum_{j,k \in I} a_{ij}a_{ik}\theta^{j-k} = \sum_{r \in I} \left( \sum_{k \in I} a_{i,k+r}a_{i,k} \right) \theta^r \), we have

\[
\sum_{r \in I} \left( \sum_{2 \leq i \leq m} \sum_{k \in I} a_{i,k+r}a_{i,k} \right) \theta^r = m - 1 \quad (4)
\]

Comparing the coefficients of \( \theta^{sp^n-1} \) \( (0 \leq s \leq p - 1) \) in (4) and applying the lemma, we have

\[
\sum_{2 \leq i \leq m} \sum_{0 \leq k \leq p^n-1} (a_{i,k+sp^n-1} - a_{i,k})^2 = 2(m - 1).
\]

From this, \( \sum_{2 \leq i \leq m} \sum_{0 \leq k \leq p^n-1} (a_{i,k+sp^n-1} - a_{i,k})^2 = 2(m - 1) \).

Thus, by (3), \( \sum_{0 \leq k \leq p^n-1} (a_{i,k+sp^n-1} - a_{i,k})^2 = 2 \) \( (2 \leq i \leq m - 1) \).

It follows that, for each \( i \), there exists a unique \( \ell \) \( (0 \leq \ell \leq p^n-1 - 1) \) such that

\[
\{a_{i,k}, a_{i,k+sp^n-1}, \ldots, a_{i,k+(p-1)p^n-1}\}
\]

\[
= \begin{cases} 
\{c_\ell, \ldots, c_\ell, c_\ell - 1\} & \text{if } k = \ell \\
\{c_k, \ldots, c_k, c_k\} & \text{otherwise}
\end{cases}
\]

as multisets.
Hence, for each $i$, there exists $d_i \geq 0$ such that
\[
\alpha_i = a_{i,0} + a_{i,1}\theta + a_{i,2}\theta^2 + \cdots + a_{i,p^n-1}\theta^{p^n-1} = -\theta^{d_i}.
\]
Thus
\[
v = (1, -\alpha_2, \cdots, -\alpha_m) = (1, \theta^{d_2}, \cdots, \theta^{d_m})
\]
and so the proposition holds. $\Box$

By the proposition, we have

**Theorem 3.8.** Let $q = p^n$ with $p$ a prime. Then every $NBH(m, q)$ matrix can be extended to $BH(m, q)$ matrix.

We now prove the main theorem.

4 An extension to GH matrices

Let $G$ be an abelian group. For an element $f = \sum_{x \in G}a_x x \in \mathbb{Z}[G]$, we set
\[
f(-1) = \sum_{x \in G}a_x x^{-1}.
\]
Moreover, we set $\hat{G} = \sum_{x \in G}x \in \mathbb{Z}[G]$, and $R = \mathbb{Z}[G]/\mathbb{Z}[\hat{G}]$. For $u = (u_1, \cdots, u_m), v = (v_1, \cdots, v_m) \in V := R^m, (u_i, v_j \in R)$ we define the product of $u$ and $v$ in the following way:
\[
u \cdot v = u_1v_1^{-1} + \cdots + u_mv_m^{-1}
\]
Then, for $v = (g_1, \cdots, g_m), w = (h_1, \cdots, h_m) (g_i, h_j \in G)$,
\[
v \perp w = 0 \iff v_1w_1^{-1} + \cdots + v_mw_m^{-1} = (m/|G|)\hat{G}
\]
We now prove the following.

**Theorem 4.1.** Let $G$ be an abelian group of order $q = p^n$ with $p$ a prime. Then every $(q, q\lambda - 1, \lambda)$-DM over $G$ can be extended to a $GH(u, \lambda)$ matrix over $G$.

To prove the theorem it suffices to show the following.

**Proposition 4.2.** Let $G$ be an abelian group of order $q = p^n$ with $p$ a prime and $M = [g_{ij}]$ a $(q, q\lambda - 1, \lambda)$-DM over $G$ such that $m_{i1} = 1$ for each $i$:
\[
M = \begin{bmatrix}
1 & g_{12} & \cdots & g_{1,m} \\
1 & g_{22} & \cdots & g_{2,m} \\
\vdots & \vdots & \ddots & \vdots \\
1 & g_{m-1,2} & \cdots & g_{m-1,m}
\end{bmatrix}, \text{ where } m = q\lambda.
\]
Define $g_{mj}$ ($1 \leq j \leq m$) by
\[
g_{m1} = 1, \quad g_{m2} = \lambda G - \sum_{i=1}^{m-1}g_{i2}, \quad \cdots, \quad g_{mm} = \lambda G - \sum_{i=1}^{m-1}g_{im}.
\]
Then the following holds.

(i) $g_{mj} \in G$.

(ii) $\tilde{M} = [g_{ij}]$ is a $GH(q, \lambda)$ matrix over $G$. 

Proof of Proposition 4.2

Set $R = \mathbb{Z}[G] / \mathbb{Z} \hat{G}$, $V = R^m$, where $m = q\lambda$. We identify the $i$th row $v_i$ of $M$ with an element of $V$. By definition of a difference matrix

$$v_i \cdot v_j = 0 \ (i \neq j) \ and \ v_i \cdot v_i = m.$$ 

Then $v \cdot v_i = m - v_i \cdot v_i = 0 \ (1 \leq i \leq m - 1)$ and so $v \perp v_i$. Hence, setting $I = \{1, \cdots, m-1\}$, we have $v = (1, -\sum_{i \in I} g_{i1}, \cdots, -\sum_{i \in I} g_{im})$ and $v \perp v_1 + v_2 + \cdots + v_{m-1}$. Set $z_j = \sum_{i \in I} g_{i,j}$ ($j = 2, \cdots, m)$. Then $v = (1, -z_2, \cdots, -z_m)$ and $0 = v \cdot (v_1 + \cdots + v_{m-1}) = m - 1 - (z_2 z_2^{-1} + \cdots + z_m z_m^{-1})$.

Therefore

$$m - 1 = z_2 z_2^{-1} + \cdots + z_m z_m^{-1} \ in \ R$$

Let $p^e$ be the exponent of $G$ and set $G = \{h_0, \cdots, h_{q-1}\}$. Let $\{\chi_0, \chi_1, \cdots, \chi_{q-1}\}$ be the set of characters of $G$. Fix $z_j (2 \leq j \leq m-1)$ and consider each character $\chi_u \neq \chi_0$ of $G$.

Clearly $\chi_u(M)$ is a NBH $(m, p^e)$ matrix and each entry of its first column is 1. Applying Proposition 3.6, $\chi_u(z_j) = -\theta^{i_u}$, for some $i_u \in \mathbb{N} \cup \{0\}$. Set $z_j = a_0 h_0 + \cdots + a_{q-1} h_{q-1}$ ($a_0, \cdots, a_{q-1} \in \mathbb{N} \cup \{0\}$). Then

$$a_0 + a_1 + \cdots + a_{q-1} = m - 1$$

and

$$a_i = (1/q)(m - 1 - \chi_1(h_i) \theta^{i_1} + \cdots + \chi_{q-1}(h_i) \theta^{i_{q-1}}).$$ 

Hence $a_i = (1/q)(m - 1 - (\chi_1(h_i) \theta^{i_1} + \cdots + \chi_{q-1}(h_i) \theta^{i_{q-1}}))$. As $m = q\lambda$,

If (1) occurs, then $\chi_s(h_i) = \theta^{i_s} \ (1 \leq s \leq q - 1)$ and $a_i = \lambda - 1$. If (2) occurs, then clearly $a_i = \lambda$.

On the other hand, $\sum_{0 \leq i \leq q-1} a_i = m - 1 = q\lambda - 1$. Therefore, as a multiset,

$$\{a_0, a_1, \cdots, a_{q-1}\} = \{\lambda - 1, \lambda, \cdots, \lambda\}. \ Thus \ there \ exists \ a \ unique \ r_j \ such \ that \ \chi_1(h_{r_j}) = \theta^{i_1}, \ \chi_2(h_{r_j}) = \theta^{i_2}, \ \cdots, \ \chi_{q-1}(h_{r_j}) = \theta^{i_{q-1}} \ by \ (1).$$

Hence $\chi_u(z_j) = -\theta^{i_u} = -\chi_u(h_{r_j})$ for any $u \neq 0$. It follows that $\chi_u(z_j + h_{r_j}) = 0$ for any $u \neq 0$ and $z_j + h_{r_j} = c\hat{G}$ for some $c$. In particular, $c = m/q = \lambda$. Hence $z_j = \lambda\hat{G} - h_{r_j}$ for each $j \in \{2, \cdots, m\}$. Thus $v = (1, -\lambda\hat{G} + h_{r_2}, \cdots, -\lambda\hat{G} + h_{r_m})$ Therefore $(1, h_{r_2}, \cdots, h_{r_m}) \perp v_t \ (1 \leq t \leq m - 1)$ holds. \ 

We would like to raise the following question.

**Question.** Can an $(u, u\lambda - 1, \lambda)$-DM over $G$ be extended to $GH(u, \lambda)$ matrix even if $G$ is non-abelian $p$-group?
References


