On the non-existence of maximal difference matrices of deficiency 1

Yutaka Hiramine
Department of Mathematics, Faculty of Education, Kumamoto University, Kurokami, Kumamoto, Japan

hiramine@kumamoto-u.ac.jp

Abstract. A $k \times u\lambda$ matrix $M = [d_{ij}]$ with entries from a group U of order u is called a (u, k, λ)-difference matrix over U if the list of quotients ${d_{i\ell}d_{j\ell}}^{-1}, 1 \leq \ell \leq u\lambda$, contains each element of U exactly λ times for all $i \neq j$. D. Jungnickel has shown that $k \leq u\lambda$ and it is conjectured that the equality holds only if U is a p-group for a prime p. On the other hand, A. Winterhof has shown that some known results on the non-existence of $(u, u\lambda, \lambda)$-difference matrices are extended to $(u, u\lambda - 1, \lambda)$-difference matrices. This fact suggests us that there is a close connection between these two cases. In this article we show that any $(u, u\lambda - 1, \lambda)$-difference matrix over an abelian p-group can be extended to a $(u, u\lambda, \lambda)$-difference matrix.

Keywords: difference matrix; generalized Hadamard matrix; Butson Hadamard matrix

MSC 2010 Code: 05B20

1 Introduction

Definition 1.1. Let U be a group of order u and k, λ positive integers. In this article, 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 $M = [d_{ij}]$ with entries from U is called a (u, k, λ)-difference matrix over U (for short, a (u, k, λ)-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, ℓ with $1 \leq i \neq \ell \leq k$. M is said to be maximal if it cannot be extended to a $(u, k+1, \lambda)$-DM over U. In this case we call $d_M := u\lambda - k$ the deficiency of M.

If there exists a (u, k, λ)-DM, then $k \leq u\lambda$ by D. Jungnickel [4]. If the equality holds, the matrix is called a GH(u, λ) matrix (a generalized Hadamard matrix). In Section 2 we will see that there exists a maximal difference matrix with the deficiency 2. However, no example of a maximal difference matrix with the deficiency 1 is known as far as the author knows. As we will see in Section 2 there is no maximal (u, k, λ)-DM M satisfying $d_M = 1$ when $u\lambda \leq 12$.

We are interested in the following problem.

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

In this article we study the case that $d_M = 1$ and show 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, λ) matrix over G.

Our result is best possible since there exist maximal $(4, 2, 1)$- and $(4, 6, 2)$-difference matrices (see Table 1 in Section 2).

2 Examples of maximal difference matrices

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

$$M_{2n} = \begin{bmatrix} 1 & \cdots & 1 & \cdots & \cdots & 1 & \cdots & 1 \\ g_1 & \cdots & g_1 & \cdots & \cdots & g_{2n} & \cdots & g_{2n} \end{bmatrix}$$

We now give an infinite family of maximal difference matrices over the additive group of $GF(p^n)$.

Proposition 2.2. *Let p be a prime with $p^n \nmid \lambda$ and let L be the multiplication table of $K = GF(p^n)$. Set $J = J_\lambda (= (1, \cdots, 1) \in K^\lambda)$. Then $M = L \otimes J$ is a maximal (p^n, p^n, λ)-DM over $(K, +)(\simeq \mathbb{Z}_p^n)$ with $d_M = (\lambda - 1)p^n$.*

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, λ)-DM over $(K, +)$.

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

We note that each entry of 0th, $\cdots$, $(\lambda - 1)$th column of M is 0, and each ith column with $\lambda \le i \le \lambda p^n - 1$ contains any element of K exactly one time.
Assume that we can obtain $(p^n, p^n + 1, \lambda)$-DM $\widehat{M} = [m_{ij}](0 \le i \le s + 1, 0 \le j \le p^n\lambda - 1)$ by adding the $s + 1$ $(= p^n)$-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 $a = \#\{i \mid m_{s+1,i} = 0, \ \ 0 \le i \le \lambda - 1\}$. We count $N = \#\{(i, j) \mid m_{i,j} = m_{s+1,j}, 0 \le i \le s, \ \ 0 \le j \le p^n\lambda - 1\}$ in two ways. Then we have $ap^n + (p^n\lambda - \lambda) \cdot 1 = \lambda p^n$ as $\widehat{M}$ is a $(p^n, p^n + 1, \lambda)$-DM. Thus $ap^n = \lambda$, contrary to $p^n \nmid \lambda$. □

Example 2.3. The following is a maximal $(4, 6, 2)$-DM over $U = \{0, a, b, c\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ with $d_M = 2$:

$$M = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a & 0 & a & b & c & c & b \\ 0 & b & a & c & 0 & b & c & a \\ 0 & c & a & b & b & a & 0 & c \\ 0 & 0 & b & b & c & c & a & a \\ 0 & 0 & c & c & a & a & b & b \end{bmatrix}.$$ The set of the first four rows of M forms a subgroup of the direct product group U^8. Hence we can easily verify that $M = [m_{ij}]$ is a $(4, 6, 2)$-DM. Assume that M can be extended to $(4, 7, 2)$-DM by adding a row say $(d_1, d_2, \cdots, d_8)$ to M. As $|\{(i, j)\ |d_j - m_{ij} = d_1\}| \geq 6 + 1 \cdot (8 - 1) = 13 > 6 \cdot 2$, we have a contradiction. Thus M is maximal.

By a computer search we obtain the following table of k for which there exists a maximal (u, k, λ)-DM over an abelian group U of order u with $2 \leq u\lambda \leq 12$.

Table 1

u	U	λ	k	$u\lambda$
2	$\mathbb{Z}_2$	1	2	2
3	$\mathbb{Z}_3$	1	3	3
4	$\mathbb{Z}_4$	1	2	4
4	$\mathbb{Z}_2 \times \mathbb{Z}_2$	1	4	4
2	$\mathbb{Z}_2$	2	4	4
5	$\mathbb{Z}_5$	1	5	5
2	$\mathbb{Z}_2$	3	2	6
3	$\mathbb{Z}_3$	2	3,6	6
6	$\mathbb{Z}_6$	1	2	6
7	$\mathbb{Z}_7$	1	3,7	7
8	$\mathbb{Z}_2 \times \mathbb{Z}_4$	1	4	8
8	$\mathbb{Z}_8$	1	2	8
2	$\mathbb{Z}_2$	4	4	8
4	$\mathbb{Z}_4$	2	4	8
4	$\mathbb{Z}_2 \times \mathbb{Z}_2$	2	4,6,8	8

u	U	λ	k	$u\lambda$
8	$\mathbb{Z}_8$	1	2	8
8	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	1	4,8	8
9	$\mathbb{Z}_9$	1	3	9
9	$\mathbb{Z}_3 \times \mathbb{Z}_3$	1	4,6	9
3	$\mathbb{Z}_3$	3	9	9
10	$\mathbb{Z}_{10}$	1	2	10
5	$\mathbb{Z}_5$	2	4,5,6,10	10
2	$\mathbb{Z}_2$	5	2	10
11	$\mathbb{Z}_{11}$	1	3,4,5,11	11
12	$\mathbb{Z}_{12}$	1	2	12
12	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$	1	3,4,5,6	12
2	$\mathbb{Z}_2$	6	4,12	12
3	$\mathbb{Z}_3$	4	6,9,12	12
4	$\mathbb{Z}_2 \times \mathbb{Z}_2$	3	4,5,6,12	12
4	$\mathbb{Z}_4$	3	2	12
6	$\mathbb{Z}_6$	2	4,5,6	12

From the table, it is conceivable that $d_M \geq 2$ except for GH matrices.

On the other hand, the following two results suggest us that there is a close connection between $(u, u\lambda - 1, \lambda)$-DMs and $(u, u\lambda, \lambda)$-DMs.

Result 2.4. (W. de Launey [5]) 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 λ. Then $\mathrm{Ord}_p(m) \equiv 1 \pmod 2$.

Result 2.5. (A. Winterhof [8]) 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 λ. Then $\mathrm{Ord}_p(m) \equiv 1 \pmod 2$.

From these facts, we would like to propose the following conjecture.

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. a GH(u, λ) matrix).

3 An extension of near BH matrices

Concerning the above conjecture we prove that it is true under the condition that the corresponding group is an abelian p-group in Section 4 (Theorem 4.1). To show this we use the following well known result on characters.

Result 3.1. (Fourier inversion formula, see [7]) Let $\widehat{G}$ 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,

(i) $a_g = \dfrac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(f)\chi(g^{-1})$ and

(ii) if $\chi(f) = 0$ for any $\chi \in \widehat{G}, \chi \neq \chi_0$, then $f = \dfrac{\chi_0(f)}{|G|} \sum_{g \in G} g$, where χ_0 is the principal character of G.

Assume that a $(u, u\lambda - 1, \lambda)$-DM N over abelian group G of order u is extended to a GH(u, λ) matrix over G, say $M = [m_{ij}]$ $(m_{ij} \in G)$. Let $\chi \neq \chi_0$ be any character of G and define $u\lambda \times u\lambda$ matrix $\chi(M)$ over $\mathbb{C}$ by $\chi(M) = [\,\chi(m_{ij})]$. Let s be the exponent of G. Then $\chi(m_{ij}) \in \langle \zeta_s \rangle$, where ζ_s is a primitive sth 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, ℓ with $i \neq \ell$, $\chi(M)$ satisfies the following.

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

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

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

A matrix with the property (1) is defined in [1].

Definition 3.2. A matrix $B = [b_{ij}]$ 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 article we define a matrix with the property (2) as follows.

Definition 3.3. We call an $(m-1) \times m$ matrix $A = [a_{ij}]$ a *near Butson Hadamard matrix* and denote it by NBH(m, s) if $m \geq 3$, $a_{ij} \in \langle \zeta_s \rangle$ and A satisfies $AA^* = mI_{m-1}$.

The conjecture mentioned in Section 2 gives rise to the following problem of the extension of a NBH(m, s) to a BH(m, s).

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

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

Proposition 3.4. *Let p be a prime and set $\theta = \zeta_{p^n}$. Let $A = [v_{ij}]$ be a NBH(m, p^n) matrix such that $v_{11} = v_{21} = \cdots = v_{m-1,1} = 1$ and $m \geq 3$. 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 A is $m-1$ or an element of $-\langle\theta\rangle$, and*

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

To show the proposition we use the following lemma.

Lemma 3.5. *Let p be a prime and set $\theta = \zeta_{p^n}$. For $a_0, \cdots, a_{p^n-1} \in \mathbb{Q}$, assume that $(*)$ $a_0 + a_1\theta + \cdots + a_{p^n-1}\theta^{p^n-1} = 0$. 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 $\sum_{0 \leq s \leq p-1} a_{p^{n-1}s+t} \equiv 0 \pmod{p}$ for any fixed t with $0 \leq t \leq p^{n-1} - 1$.*

Proof. The cyclotomic polynomial $\Phi_{p^n}(x) = \frac{x^{p^n}-1}{x^{p^{n-1}}-1}$ is a minimal polynomial of θ over $\mathbb{Q}$. As $\Phi_{p^n}(x) = x^{(p-1)p^{n-1}} + x^{(p-2)p^{n-1}} + \cdots + x^{p^{n-1}} + 1$,

$$\theta^{(p-1)p^{n-1}} + \theta^{(p-2)p^{n-1}} + \cdots + \theta^{p^{n-1}} + 1 = 0. \tag{3}$$

Hence

$$\theta^{(p-1)p^{n-1}+t} = -\theta^{(p-2)p^{n-1}+t} - \cdots - \theta^{p^{n-1}+t} - \theta^t \ (0 \leq t \leq p^{n-1} - 1). \tag{4}$$

As $a_0 + a_1\theta + \cdots + a_{p^n-1}\theta^{p^n-1} = \sum_{s=0}^{p-1} \sum_{t=0}^{p^{n-1}-1} a_{p^{n-1}s+t}\theta^{p^{n-1}s+t}$, we have

$$\sum_{t=0}^{p^{n-1}-1} a_{p^{n-1}(p-1)+t}\theta^{p^{n-1}(p-1)+t} + \sum_{s=0}^{p-2} \sum_{t=0}^{p^{n-1}-1} a_{p^{n-1}s+t}\theta^{p^{n-1}s+t} = 0. \tag{5}$$

Substituting (4) into (5) we have

$$\sum_{t=0}^{p^{n-1}-1} \sum_{s=0}^{p-2} (a_{p^{n-1}s+t} - a_{p^{n-1}(p-1)+t})\theta^{p^{n-1}s+t} = 0.$$

By the minimality of (3) we have $a_{p^{n-1}s+t} = a_{p^{n-1}(p-1)+t}$ for any s, t with $0 \leq s \leq p-2$ and $0 \leq t \leq p^{n-1} - 1$. Hence $a_{p^{n-1}(p-1)+t} = a_{p^{n-1}(p-2)+t} = \cdots = a_{p^{n-1}\cdot 1+t} = a_t$ for any t with $0 \leq t \leq p^{n-1} - 1$. Thus the lemma holds. □

Proof of Proposition 3.4

Set $I = \{0, 1, \cdots, p^n - 1\}$. As $m - 1 \geq 2$, we can consider a multiset $S = \{v_{11}\overline{v_{21}}, v_{12}\overline{v_{22}}, \cdots, v_{1m}\overline{v_{2m}}\}$. Let $c_i (\geq 0)$ be the number of θ^i contained in S for $i \in I$. As $v_1\overline{v_2}^T = 0$, $\sum_{i\in I} c_i\theta^i = 0$ and $\sum_{i\in I} c_i = m$. Therefore $p \mid m$ by (ii) of Lemma 3.5.
As $v = (m, 0, \cdots, 0) - (v_1 + \cdots + v_{m-1})$, $v \cdot v_i = m - v_i \cdot v_i = 0$. Hence $v \perp v_1, \cdots, v_{m-1}$. On the other hand, setting $\alpha_t = \sum_{1\leq i\leq m-1} v_{it}$ $(2 \leq t \leq m)$, we have $v_1 + \cdots + v_{m-1} = (m - 1, \alpha_2, \cdots, \alpha_m)$ and so $v = (1, -\alpha_2, \cdots, -\alpha_m)$. From this, $0 = (v_1 + \cdots + v_{m-1}, v) = m - 1 - \alpha_2\overline{\alpha_2} - \cdots - \alpha_m\overline{\alpha_m}$. Thus $\alpha_2\overline{\alpha_2} + \cdots + \alpha_m\overline{\alpha_m} = m - 1$. Let a_{tj} $(0 \leq j \leq p^n - 1)$ be the number of the value θ^j contained in the multiset $\{v_{1,t}, v_{2,t}, \cdots, v_{m-1,t}\}$. As $\alpha_t = \sum_{1\leq i\leq m-1} v_{it}$, it follows that

$$\begin{aligned} &\alpha_t = a_{t,0} + a_{t,1}\theta + a_{t,2}\theta^2 + \cdots + a_{t,p^n-1}\theta^{p^n-1} \\ &a_{t,0} + a_{t,1} + \cdots + a_{t,p^n-1} = m - 1 \end{aligned} \tag{6}$$

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

$$\sum_{r\in I}\Big(\sum_{2\leq i\leq m}\sum_{k\in I} a_{i,k+r}a_{i,k}\Big)\theta^r = m - 1 \tag{7}$$

We note that the addition of indices is computed modulo p^n. Comparing the coefficients of $\theta^{sp^{n-1}}$ $(0 \leq s \leq p-1)$ in (7) and applying Lemma 3.5(i), we have

$$\begin{aligned} &\sum_{2\leq i\leq m} (a_{i,0}^2 + \cdots + a_{i,p^n-1}^2) - (m - 1) \\ &= \sum_{2\leq i\leq m}\sum_{0\leq k\leq p^n-1} a_{i,k+sp^{n-1}}\, a_{i,k} \quad (1 \leq \forall s \leq p - 1). \end{aligned}$$

From this, $\sum_{2\leq i\leq m}\sum_{0\leq k\leq p^n-1} (a_{i,k+sp^{n-1}} - a_{i,k})^2 = 2(m - 1)$. We note that $\sum_{0\leq k\leq p^n-1} (a_{i,k+sp^{n-1}} - a_{i,k})^2 \geq 2$ by (6). Thus $\sum_{0\leq k\leq p^n-1} (a_{i,k+sp^{n-1}} - a_{i,k})^2 = 2$ for i with $2 \leq i \leq m - 1$. It follows that, for each i, there exists a unique ℓ $(0 \leq \ell \leq p^{n-1} - 1)$ such that

$$\begin{aligned} &\{a_{i,k},\ a_{i,k+sp^{n-1}},\ \cdots,\ a_{i,k+(p-1)sp^{n-1}}\} \\ &= \begin{cases} \{c_\ell,\ \cdots,\ c_\ell,\ c_\ell - 1\} & \text{if } k = \ell \text{ and } p > 2 \\ \{c_\ell,\ \cdots,\ c_\ell,\ c_\ell \pm 1\} & \text{if } k = \ell \text{ and } p = 2 \\ \{c_k,\ \cdots,\ c_k,\ c_k\} & \text{otherwise} \end{cases} \end{aligned}$$

as multisets.

Hence, for each i, there exists $d_i \geq 0$ such that

$$\alpha_i = a_{i,0} + a_{i,1}\theta + a_{i,2}\theta^2 + \cdots + a_{i,p^n-1}\theta^{p^n-1} = \begin{cases} -\theta^{d_i} & \text{if } p > 2 \\ \pm\theta^{d_i} & \text{if } p = 2. \end{cases}$$

We note that $+\theta^{d_i} = -\theta^{d_i+2^{n-1}}$ when $p = 2$. Hence, in this case we rewrite $\theta^{d_i+2^{n-1}}$ as θ^{d_i}. Thus we have $v = (1, -\alpha_2, \cdots, -\alpha_m) = (1, \theta^{d_2}, \cdots, \theta^{d_m})$ and so the proposition holds.

By Proposition 3.4, we have

Theorem 3.6. *Let $q = p^n$ with p a prime. Then every NBH(m, q) matrix can be extended to a BH(m, q) matrix.*

We now prove our 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 $\widehat{G} = \sum_{x\in G} x \in \mathbb{Z}[G]$ and $R = \mathbb{Z}[G]/\mathbb{Z}[\widehat{G}]$. For $u = (u_1, \cdots, u_m)$, $v = (v_1, \cdots, v_m) \in R^m$, $(u_i, v_j \in R)$ we define the product of u and v in the following way :

$$u \cdot v = u_1 {v_1}^{(-1)} + \cdots + u_m {v_m}^{(-1)} \ (\in R).$$

Let g_i and h_j be elements of G for $i, j \in \{1, 2, \cdots m\}$. Then, for $v = (g_1, \cdots, g_m)$ and $w = (h_1, \cdots, h_m)$

$$v \perp w \text{ in } R \iff g_1 {h_1}^{-1} + \cdots + g_m {h_m}^{-1} = (m/|G|)\widehat{G}.$$

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, λ) 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 $g_{i1} = 1$ for each i :*

$$M = \begin{bmatrix} 1 & g_{12} & \cdots & g_{1,m} \\ 1 & g_{22} & \cdots & g_{2,m} \\ \vdots & \cdots & \cdots & \cdots \\ 1 & g_{m-1,2} & \cdots & g_{m-1,m} \end{bmatrix}, \text{ where } m = q\lambda.$$

Define g_{mj} $(1 \le j \le m)$ 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) $\tilde{M} = [g_{ij}]_{1\le i,j\le m}$ *is a GH(q, λ) matrix over G.*

Proof of Proposition 4.2

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

$v_i \cdot v_j = 0$ $(i \neq j)$ and $v_i \cdot v_i = m$. Set $v = (m, 0, \cdots, 0) - (v_1 + \cdots + v_{m-1})$. 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 $v = (1, -\sum_{i\in I} g_{i2}, \cdots, -\sum_{i\in I} g_{im})$ 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

$$z_2 z_2^{(-1)} + \cdots + z_m z_m^{(-1)} = m - 1 \quad \text{in } R$$

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 3.4, $\chi_u(z_j) = -\theta^{i_u}$, 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

$$\begin{bmatrix} \chi_0(h_0) & \chi_0(h_1) & \cdots & \chi_0(h_{q-1}) \\ \chi_1(h_0) & \chi_1(h_1) & \cdots & \chi_1(h_{q-1}) \\ \cdots & \cdots & \cdots & \cdots \\ \chi_{q-1}(h_0) & \chi_{q-1}(h_1) & \cdots & \chi_{q-1}(h_{q-1}) \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{q-1} \end{bmatrix} = \begin{bmatrix} m-1 \\ -\theta^{i_1} \\ \vdots \\ -\theta^{i_{q-1}} \end{bmatrix}$$

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

(1) $\overline{\chi_1(h_i)}\theta^{i_1} = \cdots = \overline{\chi_{q-1}(h_i)}\theta^{i_{q-1}} = 1$ or

(2) $1 + \overline{\chi_1(h_i)}\theta^{i_1} + \cdots + \overline{\chi_{q-1}(h_i)}\theta^{i_{q-1}} = 0$.

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

$$\chi_1(h_{r_j}) = \theta^{i_1}, \quad \chi_2(h_{r_j}) = \theta^{i_2}, \quad \cdots, \chi_{q-1}(h_{r_j}) = \theta^{i_{q-1}} \text{ by (1).}$$

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 so $z_j + h_{r_j} = c\hat{G}$ for some c by Result 3.1. 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 a GH(u, λ) matrix even if G is a non-abelian p-group ?

In the rest of this section, we give an application to difference matrices of coset type.

Definition 4.3. ([6], [3]) Let H be a (u, k, λ)-DM over a group U of order u. Let R be the set of rows of H. We regard R as a subset of the direct product group $U^{u\lambda}$. We say H is of *coset type* with respect to a row $w \neq (1, \cdots, 1)$ of H if $rw \in R$ for all $r \in R$.

Remark 4.4. We note that the (p^n, p^n, λ)-DM over the additive group of K in Proposition 2.2 is of coset type with respect to any row except for the first one.

We prove the following as an application of Theorem 4.1.

Corollary 4.5. *Let p be a prime and let H be a $(p, p\lambda - p; \lambda)$-DM of coset type over a group $U = \langle a \rangle$ of order p with respect to a row of H. If $\lambda \geq 3$, then H can be extended to a GH(p, λ) matrix of coset type over U.*

To show the corollary, we use the following result [3].

Result 4.6. ([3]) Let p be a prime and k an integer with $k > p$. Let H be a (p, k, λ)-DM of coset type over a group $U = \langle a \rangle$ of order p with respect to a row of H. Then $p \mid \lambda$ and there exist p normalized $(p, k/p, \lambda/p)$-DMs $H_0, H_1, \ldots, H_{p-1}$ over U such that H is equivalent to the following standard form.

$$M([H_0, H_1, \ldots, H_{p-1}], w) := \begin{bmatrix} (H_0, H_1, \ldots, H_{p-1}) \\ (H_0, H_1, \ldots, H_{p-1})w \\ \vdots \\ (H_0, H_1, \ldots, H_{p-1})w^{p-1} \end{bmatrix}$$

where $w = (J, Ja, \ldots, Ja^{p-1}) \in U^{p\lambda}$, $J = (1, \ldots, 1) \in U^{\lambda}$.

Proof of Corollary 4.5

By assumption $p\lambda - p > p$. Hence, applying Result 4.6, we have $p \mid \lambda$ and there exist p normalized $(p, \lambda - 1, \lambda/p)$-DMs $H_0, H_1, \ldots, H_{p-1}$ over U such that H is equivalent to the following standard form :

$$M = M([H_0, H_1, \ldots, H_{p-1}], w).$$

By Theorem 4.1, each H_i can be extended to a GH$(p, \lambda/p)$ matrix, say L_i. Hence we obtain a GH(p, λ) matrix $L = M([L_0, L_1, \ldots, L_{p-1}], w)$. Clearly L is an extension of M and of coset type with respect to w.

Remark 4.7. In the proof of Proposition 2.2, assume $n = 1, \lambda = 2$ and $p > 2$. Then M is a $(p, 2p - p, 2)$-DM of coset type by Remark 4.4. But, it can not be extended to a GH$(p, 2)$ by Proposition 2.2.

References

[1] A. T. Butson, Generalized Hadamard matrices. Proc. Amer. Math. Soc. 13 (1962) 894-898.

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

[3] Y. Hiramine and C. Suetake, On difference matrices of coset type, Journal of Combinatorial Theory, Series A 120 (2013) 266-274

[4] D. Jungnickel, On difference matrices, resolvable transversal designs and generalised Hadamard matrices, Math. Z., Vol. 167 (1979), 49-60.

[5] W. de Launey, On the non-existence of generalized Hadamard matrices, Journal of Statistical Planning and Inference (1984), Vol.10, 385-396.

[6] T.P. McDonough, V.C. Mavron and C.A. Pallikaros, Generalised Hadamard matrices and translations, Journal of Statistical Planning and Inference, Vol. 86 (2000), 527-533.

[7] B. Schmidt, "Characters and cyclotomic Fields in Finite Geometry", Lecture Notes in Mathematics, vol. 1797, Springer, 2002.

[8] A. Winterhof, On the non-existence of $(g, g\lambda-1, \lambda)$-difference matrices, Ars Combinatoria Vol. 64 (2002), 265-269