Journal of Combinatorial Theory, Series A 120 (2013) 266–274

Contents lists available at SciVerse ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

On difference matrices of coset type

Yutaka Hiramine [a], Chihiro Suetake [b]

[a] Department of Mathematics, Faculty of Education, Kumamoto University, Kurokami, Kumamoto, Japan
[b] Department of Mathematics, Faculty of Engineering, Oita University, Oita, 870-1192, Japan

ARTICLE INFO

Article history:
Received 25 October 2011
Available online 27 August 2012

Keywords:
Difference matrix
Generalized Hadamard matrix
Transversal design

ABSTRACT

A $(u,k;\lambda)$-difference matrix H over a group U is said to be of coset type with respect to one of its rows, say w, whose entries are not equal, if it has the property that rw is also a row of H for any row r of H. In this article we study the structural property of such matrices with $u(<k)$ a prime and show that $u|\lambda$ and, moreover, H contains u $(u,k/u;\lambda/u)$-difference submatrices and is equivalent to a special kind of extension using them. Conversely, we also show that any set of u $(u,k';\lambda')$-difference matrices over U yields a $(u,uk';u\lambda')$-difference matrix of coset type over U.

1. Introduction

Let U be a group of order u and $k,\lambda \in \mathbb{N}$. A $k \times u\lambda$ matrix $H = [d_{ij}]$ over U is called a $(u,k;\lambda)$-difference matrix if $d_{ij} \in U$ for all i, j and satisfies $\sum_{1 \leqslant j \leqslant u\lambda} d_{i_1 j} d_{i_2 j}{}^{-1} = \lambda \widehat{U} \in \mathbb{Z}[U]$ $(1 \leqslant i_1 \neq i_2 \leqslant k)$, where $\widehat{U} = \sum_{x \in U} x$.

C.J. Colbourn and D.L. Kreher [3] gave various construction methods for difference matrices associated with pairwise balanced designs or finite fields. Recently, P.H.J. Lampio and P.R.J. Östergard [7] determined the largest number of k for which a $(u,k;\lambda)$-difference matrix exists for some small u, λ.

By a result of [6], $k \leqslant u\lambda$. A $(u,u\lambda;\lambda)$-difference matrix over a group U achieving this equality is called a generalized Hadamard matrix and denoted by $\mathrm{GH}(u,\lambda)$. This paper is motivated by a result of [8], which states that if a $\mathrm{GH}(u,\lambda)$ matrix H over a group U has a row w, whose entries are not equal, with the property that rw is also a row of H for any row r of H, then U is an elementary abelian p-group for a prime p. This implies that the set of rows of H is a union of some left cosets of $\langle w \rangle$ in the direct product group $U^{u\lambda}$.

In this paper we study the structure of $(u,k;\lambda)$-difference matrices of coset type over a group U. Concerning the parameter λ we show that the exponent of U is a divisor of λ if $k = u\lambda$ and $\lambda \neq 1$

E-mail addresses: hiramine@gpo.kumamoto-u.ac.jp (Y. Hiramine), suetake@csis.oita-u.ac.jp (C. Suetake).

0097-3165/$ – see front matter
http://dx.doi.org/10.1016/j.jcta.2012.08.008

(Theorem 3.4), while this is not true in general if $k \neq u\lambda$ (see an example just after the proof of Theorem 3.4). We mainly concentrate on the structure of $(p, k; \lambda)$-difference matrices H of coset type over a group U of prime order p. We show that H contains p $(p, k/p; \lambda/p)$-difference submatrices and H is equivalent to some kind of extension using them (Theorem 4.8). We show that some of the known Hadamard matrices are of this type (Example 4.12) and also present a construction method for $(p, p^m r, p^m \mu)$-matrices of coset type with respect to a group isomorphic to $\mathbb{Z}_p^m$ for given (p, r, μ)-matrices over $\mathbb{Z}_p$ (Proposition 4.10).

2. Difference matrices with respect to cosets

Let U be a group of order u and $k, \lambda \in \mathbb{N}$. For a subset S of U, we identify it with the group ring element $\widehat{S} = \sum_{x \in S} x \in \mathbb{Z}[U]$ and denote it again by S throughout this article.

A $k \times u\lambda$ matrix $H = [d_{ij}]$ over U is called a $(u, k; \lambda)$-difference matrix if $d_{ij} \in U$ for all i, j with $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant u\lambda$ and satisfies the following:

$$\sum_{1 \leqslant j \leqslant u\lambda} d_{i_1 j} {d_{i_2 j}}^{-1} = \lambda U \in \mathbb{Z}[U] \quad (1 \leqslant i_1 \neq i_2 \leqslant k).$$

Definition 2.1. Let H be a $(u, k; \lambda)$-difference matrix 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 $W (\subset U^{u\lambda})$ if the following conditions are satisfied:

(i) $W \subset R$ and W is a nontrivial subgroup of $U^{u\lambda}$.
(ii) If $w \in W$ and $r \in R$, then $rw \in R$.

If H is of coset type with respect to $\langle w \rangle$, we say shortly that it is of coset type with respect to w.

Remark 2.2. Let U, H, R and W be as in Definition 2.1 and let $1_{u\lambda}$ be the identity of $U^{u\lambda}$. Then the following holds:

(i) R is a union of some left cosets gW $(g \in U^{u\lambda})$.
(ii) As $w, w^2, \ldots \in R$, it follows that $1_{u\lambda} \in R$. There exists an integer n such that the order of w^n is a prime, say p. Clearly each entry of w^n is an element of U of order 1 or p. As $w^n, 1_{u\lambda} \in R$, it follows from the definition of a difference matrix that U is a p-group of exponent p and each row $(\neq 1_{u\lambda})$ contains each element of U exactly λ times.

The following is an example of difference matrices of coset type.

Example 2.3. Let $U = \{1, a, b, c\}$ be a group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Then we can verify that the following is a $(4, 8; 6)$-difference matrix over U:

$$\begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \\ h_4 \\ h_5 \\ h_6 \\ h_7 \end{bmatrix} = \begin{bmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&a&a&a&a&a&a&b&b&b&b&b&b&c&c&c&c&c&c\\
1&a&b&1&a&b&a&c&c&a&c&c&a&b&c&a&b&c&1&1&b&1&1&b\\
1&a&b&1&a&b&1&b&b&1&b&b&c&1&a&c&1&a&c&c&a&c&c&a\\
1&1&a&b&b&c&a&b&b&c&1&a&c&c&1&a&b&c&1&a&a&b&c&1\\
1&1&a&b&b&c&1&c&c&b&a&1&a&a&b&c&1&a&c&b&b&a&1&c\\
1&a&c&b&c&a&1&a&a&b&c&b&b&a&c&1&1&1&1&a&c&b&c&b\\
1&a&c&b&c&a&a&1&1&c&b&c&1&c&a&b&b&b&c&b&1&a&1&a
\end{bmatrix}.$$

We note that $W := \{h_0, h_1, h_2, h_3\}$ is a subgroup of U^{24} and $h_4 W = \{h_4, h_5, h_6, h_7\}$ is a coset of W in U^{24}.

Let notations be as in Definition 2.1. W. de Launey considered the case that $R = W$ and $k = u\lambda$ and called H a group Hadamard matrix [4]. T.P. McDonough, V.C. Mavron and C.A. Pallikaros studied $\mathrm{GH}(u,\lambda)$ matrices H over a group U of coset type with respect to some row of H and showed that U is an elementary abelian p-group for a prime p [8].

Example 2.4. Let p be a prime and let $U = \{g_1 = 1, \ldots, g_q\}$ be any p-group of order q and exponent p. Then it is obvious that a $(q, p; \lambda)$-difference matrix H of coset type with respect to a row is equivalent to the following:

$$H = [\, w^0 \quad w^1 \quad \cdots \quad w^{p-1} \,]^T$$

where $w = (Jg_1, Jg_2, \ldots, Jg_q)$, $J = (1, \ldots, 1) \in U^{\lambda}$. We note that λ is arbitrary in this example.

Let H be a $(p^m, k; \lambda)$-difference matrix of coset type, where p is a prime. If $k = p$, λ can be any positive integer as we have seen in Example 2.4. What can we say about the parameter λ when $k > p$? In the next section we will consider the case that $k = u\lambda$ concerning this question.

3. An automorphism corresponding to coset type

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

(i) $\mathbb{P}$ is a set of ku points partitioned into k classes $\mathcal{C}_0, \ldots, \mathcal{C}_{k-1}$ (called *point classes*), each of size u,
(ii) $\mathbb{B}$ is a collection of k-subsets of $\mathbb{P}$ (called blocks) and
(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 λ blocks.

A $\mathrm{TD}_{\lambda}(k,u)$ is obtained from a difference matrix [1].

Definition 3.1. Let $H = [h_{ij}]_{\substack{0 \leqslant i \leqslant k-1 \\ 0 \leqslant j \leqslant n-1}}$ be a $(u, k; \lambda)$-difference matrix over a group U of order u, where $n = u\lambda$. For i with $0 \leqslant i \leqslant k-1$, set $h_i = (h_{i,0}, \ldots, h_{i,n-1}) (\in U^n)$. An incidence structure $\mathcal{D}_H(\mathbb{P}, \mathbb{B})$ obtained from H is defined by

$$\text{the set of points:} \quad \mathbb{P} = \bigl\{(i,x) \bigm| 0 \leqslant i \leqslant k-1,\ x \in U\bigr\}, \qquad |\mathbb{P}| = ku,$$

$$\text{the set of blocks:} \quad \mathbb{B} = \{B_{j,y} \bigm| 0 \leqslant j \leqslant n-1,\ y \in U\}, \quad \text{where}$$

$$B_{j,y} = \bigl\{(0, h_{0j}y), (1, h_{1j}y), \ldots, (k-1, h_{k-1,j}y)\bigr\},$$

$$\text{incidence:} \quad (i,a) \in B_{j,b} \quad (\Longleftrightarrow \quad a = h_{ij}b).$$

We note that each block in $\mathbb{B}$ is defined by using a column of H or its translate.

The following lemma is well known [1]:

Lemma 3.2. *Let notations be as in Definition 3.1. Set $\mathcal{C}_i = \{i\} \times U$ $(0 \leqslant i \leqslant k-1)$ and $\mathcal{B}_j = \{B_{j,y} \mid y \in U\}$ $(0 \leqslant j \leqslant n-1)$. Then,*

(i) *$\mathcal{D}_H(\mathbb{P}, \mathbb{B})$ is a $\mathrm{TD}_{\lambda}(k,u)$ with a set of point classes $\mathcal{C}_i$'s and a set of block classes $\mathcal{B}_j$'s.*
(ii) *The action of U on $(\mathbb{P}, \mathbb{B})$ defined by $(i,a)^{\rho(x)} = (i, ax)$ and ${B_{j,b}}^{\rho(x)} = B_{j,bx}$ for each $x \in U$ induces an element of $\mathrm{Aut}(\mathbb{P}, \mathbb{B})$.*
(iii) *$\rho(U)$ is a subgroup of $\mathrm{Aut}(\mathbb{P}, \mathbb{B})$ and acts regularly on each $\mathcal{C}_i$ and $\mathcal{B}_j$.*

We consider a special kind of automorphism corresponding to difference matrices of coset type.

Lemma 3.3. *Let $H = [h_{ij}]$ be a $(u,k;\lambda)$-difference matrix over a group U and set $H = [\,h_0 \quad h_1 \quad \cdots \quad h_{k-1}\,]^T$. Assume H is of coset type with respect to a row h_m of H and define the action $\theta(h_m)$ on $\mathcal{D}_H(\mathbb{P},\mathbb{B})$ by*

$$(i,a)^{\theta(h_m)} = (\ell,a) \quad \text{and} \quad {B_{j,b}}^{\theta(h_m)} = B_{j,h_{mj}^{-1}b}, \quad \text{where } h_\ell = h_i h_m.$$

Then the following holds:

(i) *$\theta(h_m) \in \mathrm{Aut}(\mathbb{P},\mathbb{B})$ and $\theta(h_m)$ leaves each parallel class $\mathcal{B}_j$ invariant and acts semiregularly on $\mathbb{P}$.*
(ii) *$\theta(h_m)$ fixes each block of $\mathcal{B}_j$ if $h_{mj} = 1$, and no blocks of $\mathcal{B}_j$ otherwise.*
(iii) *$[\rho(U), \langle\theta(h_m)\rangle] = 1$ and $\rho(U) \times \langle\theta(h_m)\rangle$ acts semiregularly on $\mathbb{P}$.*

Proof. Clearly $\theta(h_m)$ induces a permutation on $\mathbb{P}$ and $\mathbb{B}$. Let $(i,a) \in \mathbb{P}$ and $B_{j,b} \in \mathbb{B}$ and assume $(i,a) \in B_{j,b}$. Then $a = h_{ij}b$ by definition and $h_\ell = h_i h_m$ for some ℓ. Hence $(i,a)^{\theta(h_m)} = (\ell,a)$ and $B_{j,b}^{\theta(h_m)} = B_{j,h_{mj}^{-1}b}$. On the other hand $h_{\ell j} = h_{ij}h_{mj}$ as $h_\ell = h_i h_m$. Hence $h_{ij} = h_{\ell j}h_{mj}^{-1}$ and so $a = h_{\ell j}h_{mj}^{-1}b$ as $a = h_{ij}b$. This implies that $(\ell,a) \in B_{j,h_{mj}^{-1}b}$. Thus (i) holds.

As $B_{j,b}^{\theta(h_m)} = B_{j,b}$ if and only if $B_{j,h_{mj}^{-1}b} = B_{j,b}$, it follows that $\theta(h_m)$ fixes $B_{j,b}$ if and only if $h_{mj}^{-1} = 1$. Thus (ii) holds.

Let $x \in U$. Then $(i,a)^{\rho(x)\theta(h_m)} = (i,ax)^{\theta(h_m)} = (\ell,ax)$, where $h_\ell = h_i h_m$. Similarly, $(i,a)^{\theta(h_m)\rho(x)} = (\ell,a)^{\rho(x)} = (\ell,ax)$. Thus $\rho(x)$ and $\theta(h_m)$ commute. By Remark 2.2(ii), the order of $\theta(h_m)$ is p for a prime p. Let $n \in \{0,1,\dots,p-1\}$. Then $h_i(h_m)^n = h_\ell$ for some ℓ. Then $(i,a)^{\rho(x)(\theta(h_m))^n} = (\ell,ax)$. Hence $\rho(x)(\theta(h_m))^n$ fixes (i,a) if and only if $x = 1$ and $h_i = h_i(h_m)^n$. This is equivalent to $x = 1$ and $n = 0$, which implies the second half of (iii). $\square$

Concerning the parameter λ of a $(u,u\lambda;\lambda)$-difference matrix of coset type, we can prove the following as an application of Lemma 3.3.

Theorem 3.4. *Assume H is a $(u,u\lambda;\lambda)$-difference matrix over a group U. If H is of coset type with respect to a row of H, then either $\lambda = 1$ or $\exp(U)|\lambda$.*

Proof. Let $\mathbb{P}$, $\mathbb{B}$ and $\mathcal{B}_j$ $(0 \leqslant j \leqslant u\lambda - 1)$ be as in Lemmas 3.2 and 3.3 and assume that $k = u\lambda$. By Theorem 3.2 of [6], $(\mathbb{P},\mathbb{B})$ is a symmetric transversal design. Assume that $\lambda > 1$ and that H is of coset type with respect to a row w of H. By Remark 2.2(ii), $\mathrm{o}(w)$ is a prime. Set $p = \mathrm{o}(w)$. By Lemma 3.3, $\mathrm{o}(\theta(w)) \neq 1$ and so $\mathrm{o}(\theta(w)) = p$. Moreover, as $\lambda > 1$, it follows from Remark 2.2(ii) and Lemma 3.3(ii) that we can choose two distinct block classes $\mathcal{B}_i, \mathcal{B}_j$ such that $\theta(w)$ fixes each block in $\mathcal{B}_i \cup \mathcal{B}_j$. Let $B \in \mathcal{B}_i$ and $C \in \mathcal{B}_j$. Then $\langle\theta(w)\rangle$ acts semiregularly on $B \cap C$ by Lemma 3.3(iii). Thus $p = \mathrm{o}(\theta(w)) \,|\, |B \cap C| = \lambda$. $\square$

We note that the following is a $(4,4;3)$-difference matrix over $U = \{1,a,b,c\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ of coset type with respect to the second row. However $2 \nmid \lambda = 3$, which shows that the condition $k = u\lambda$ in Theorem 3.4 is essential to the argument

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & a & a & a & b & b & b & c & c & c \\ 1 & 1 & 1 & b & b & b & c & c & c & a & a & a \\ 1 & 1 & 1 & c & c & c & a & a & a & b & b & b \end{bmatrix}.$$

Example 3.5. (i) Let $F = GF(p^n)$. Set $F = \{k_0(=0), k_1(=1), \dots, k_{q-1}\}$. It is well known that a $q \times q$ matrix $H = [h_{ij}]_{0 \leqslant i,j \leqslant q-1}$ with entries from F defined by $h_{ij} = k_i k_j$ is a $(q,q;1)$-difference matrix over the additive group $(F,+)$. H is one of the group Hadamard matrices defined by W. de Launey [4] and therefore it is of coset type such that $p \nmid \lambda = 1$.

(ii) The following matrix H is a $(3,18;6)$-difference matrix over $U=\langle a\rangle(\simeq\mathbb{Z}_3)$ of coset type with respect to the second row w of H. Clearly $3\lambda=6$. Moreover, we can verify that for each $i\in\{0,1,2,3,4,5\}$, the $(3i+1)$th, $(3i+2)$th and $(3i+3)$th rows of H form a coset of the subgroup $\langle w\rangle$ in U^{18}

$$H=\left[\begin{array}{cccccc|cccccc|cccccc}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&a&a&a&a&a&a&a^2&a^2&a^2&a^2&a^2&a^2\\
1&1&1&1&1&1&a^2&a^2&a^2&a^2&a^2&a^2&a&a&a&a&a&a\\
\hline
1&1&a&a^2&a&a^2&1&a^2&a^2&a&a&1&1&a&1&a&a^2&a^2\\
1&1&a&a^2&a&a^2&a&1&1&a^2&a^2&a&a^2&1&a^2&1&a&a\\
1&1&a&a^2&a&a^2&a^2&a&a&1&1&a^2&a&a^2&a&a^2&1&1\\
\hline
1&a^2&a^2&a&a&1&1&a&1&a&a^2&a^2&1&1&a&a^2&a&a^2\\
1&a^2&a^2&a&a&1&a&a^2&a&a^2&1&1&a^2&a^2&1&a&1&a\\
1&a^2&a^2&a&a&1&a^2&1&a^2&1&a&a&a&a&a^2&1&a^2&1\\
\hline
1&a&1&a&a^2&a^2&1&1&a&a^2&a&a^2&1&a^2&a^2&a&a&1\\
1&a&1&a&a^2&a^2&a&a&a^2&1&a^2&1&a^2&a&a&1&1&a^2\\
1&a&1&a&a^2&a^2&a^2&a^2&1&a&1&a&a&1&1&a^2&a^2&a\\
\hline
1&a&a^2&a^2&1&a&1&a&a^2&a^2&1&a&1&a&a^2&a^2&1&a\\
1&a&a^2&a^2&1&a&a&a^2&1&1&a&a^2&a^2&1&a&a&a^2&1\\
1&a&a^2&a^2&1&a&a^2&1&a&a&a^2&1&a&a^2&1&1&a&a^2\\
\hline
1&a^2&a&1&a^2&a&1&a^2&a&1&a^2&a&1&a^2&a&1&a^2&a\\
1&a^2&a&1&a^2&a&a&1&a^2&a&1&a^2&a^2&a&1&a^2&a&1\\
1&a^2&a&1&a^2&a&a^2&a&1&a^2&a&1&a&1&a^2&a&1&a^2
\end{array}\right].$$

(iii) By Theorem 3.4, any $\mathrm{GH}(p,\lambda)$ matrix with $\lambda\in\{2,4\}$ (see Table 5.10 of [2]) is not of coset type with respect to any of its rows when p is an odd prime.

4. $(p,k;\lambda)$-difference matrices of coset type with p a prime

We now consider the case that U is of prime order.

Notation 4.1. Let p be a prime and let $U=\langle a\rangle$ be a group of order p. Set $N=U^\lambda$ and $G=N^p$ and identify G with $U^{p\lambda}$. Set $J=(1,\dots,1)\in U^\lambda$ and $w=(J,Ja,\dots,Ja^{p-1})\in G$, where $(x_1,\dots,x_\lambda)x=(x_1x,\dots,x_\lambda x)$ for $(x_1,\dots,x_\lambda)\in N$ and $x\in U$. Let m be a positive integer. For $z=(z_1,\dots,z_m)\in U^m$, we set $\widehat{z}=z_1+\cdots+z_m\in\mathbb{Z}[U]$.

Remark 4.2. Let H be a $(p,k;\lambda)$-difference matrix over U. Assume that H is of coset type with respect to a row w of H. By Remark 2.2(ii), $1_{p\lambda}$ is a row of H and $\widehat{w}=\lambda U$. Hence, by permuting columns of H if necessary, we may assume that $w=(J,Ja,\dots,Ja^{p-1})$. Moreover, by Remark 2.2(i), $p|k$ and so $k=pr$ for an integer r.

Throughout the rest of this section we assume the following:

Hypothesis 4.3.

(i) H is a $(p,k;\lambda)$-difference matrix over a group $U(=\langle a\rangle)$ of order p with p a prime.
(ii) H is of coset type with respect to a row w of H and $k=pr$, $r>1$.
(iii) $w=(J,Ja,\dots,Ja^{p-1})\in U^{p\lambda}$, where $J=(1,\dots,1)\in U^\lambda$. According to the form of w, we write each row v of H in the form

$$v=(v_0,v_1,\dots,v_{p-1})\in\left(U^\lambda\right)^p,\quad\text{where } v_i\in U^\lambda.$$

We call v_i the ith part of v.

We also use the following notations in the rest of this section.

Notation 4.4. Let p be a prime and H a $(u,k;\lambda)$-difference matrix over $U=\langle a\rangle \simeq \mathbb{Z}_p$ of coset type with respect to a row w of H. Let R be the set of rows of H. As $R=h_0\langle w\rangle \cup h_1\langle w\rangle \cup \cdots \cup h_{r-1}\langle w\rangle$ for some rows $h_0,h_1,\ldots,h_{r-1}$ of H, where $h_0=(1,\ldots,1)\in U^{p\lambda}$, we may assume the following:

$$H=[\,M \quad Mw \quad \cdots \quad Mw^{p-1}\,]^T, \quad \text{where } M=[\,h_0 \quad h_1 \quad \cdots \quad h_{r-1}\,]^T. \tag{1}$$

If $w=(J,Ja,\ldots,Ja^{p-1})$ with $J=1_\lambda \in U^\lambda$, we say H in (1) is a *standard* $(p,k;\lambda)$-difference matrix over U of coset type with respect to w. We note that $\widehat{h_j w^i}=\lambda U$ $((i,j)\neq(0,0))$ by Remark 2.2.

Lemma 4.5. *Let notations be as in Notation 4.4 and set $v=(v_0,v_1,\ldots,v_{p-1})=h_{i_1}h_{i_2}^{-1}$ for distinct $i_1\neq i_2$, where $v_i\in U^\lambda$. Set $\widehat{v_i}=m_{i,0}1+m_{i,1}a+m_{i,2}a^2+\cdots+m_{i,p-1}a^{p-1}$ $(i\in\mathbb{Z}_p)$, where each m_{ij} is a non-negative integer. Then the following holds*:

(i) $\widehat{vw^t}=\lambda U$ *for all* $t\in\mathbb{Z}$.
(ii) $m_{i,0}+m_{i,1}+\cdots+m_{i,p-1}=\lambda$ $(0\leqslant i\leqslant p-1)$.
(iii) $m_{0,s}+m_{1,s-t}+m_{2,s-2t}+\cdots+m_{p-1,s-(p-1)t}=\lambda$ $(s,t\in\mathbb{Z}_p)$.

Proof. For $t\in\mathbb{Z}$, as $vw^t=h_{i_1}(h_{i_2}w^{-t})^{-1}$ and $h_{i_2}w^{-t}\in R$, we have (i). As v_i has exactly λ components, (ii) is clear. Since the ith part of w^t is $(Ja^i)^t=(a^{it},\ldots,a^{it})$, by (i) we have $\lambda U=\widehat{vw^t}=\sum_{0\leqslant i\leqslant p-1}\sum_{0\leqslant j\leqslant p-1}(m_{i,j}a^j)a^{it}=\sum_{0\leqslant i,j\leqslant p-1}m_{i,j}a^{j+it}$. Moreover, as $j+it\equiv s \pmod p$ if and only if $j\equiv s-it \pmod p$, we have $\sum_{0\leqslant i\leqslant p-1}m_{i,s-it}=\lambda$ $(s,t\in\mathbb{Z}_p)$, which implies (iii). □

Lemma 4.6. *Fix $i_0,j_0\in\mathbb{Z}_p$ and set $S_a=\{(i,j)\in\mathbb{Z}_p\times\mathbb{Z}_p \mid ia+j=i_0a+j_0\}$ for $a\in\mathbb{Z}_p$. Then the following holds*:

(i) $|S_a|=p$, $S_a\cap S_b=\{(i_0,j_0)\}$ $(a,b\in\mathbb{Z}_p,\ a\neq b)$.
(ii) $S_a\cap\{i_0\}\times\mathbb{Z}_p=S_a\cap\mathbb{Z}_p\times\{j_0\}=\{(i_0,j_0)\}$ *for any* $a\neq 0$.
(iii) *If $i\neq i_0$ and $j\neq j_0$, then there exists a unique $a(\neq 0)\in\mathbb{Z}_p$ such that $(i,j)\in S_a$.*

Proof. Clearly $|S_a|=p$ for any $a\in\mathbb{Z}_p$. Let $(i,j)\in S_a\cap S_b$. Then $it+j=i_0t+j_0$ for $t\in\{a,b\}$. Hence, $i(a-b)=i_0(a-b)$. As $a\neq b$, we have $i=i_0$ and so $j=j_0$. Thus (i) holds. Assume $i\neq i_0$ and $j\neq j_0$. Then, $a=(i-i_0)^{-1}(j-j_0)\in\mathbb{Z}_p\setminus\{0\}$, hence (iii) holds and (ii) is obvious. □

Solving a system of p^2+p linear equations given by Lemma 4.5 with p^2 variables m_{ij}'s, we can show the following:

Lemma 4.7. *Let notations be as in Lemma 4.5. Then p divides λ and $\widehat{v_i}=(\lambda/p)U$ $(0\leqslant i\leqslant p-1)$.*

Proof. Let $i_0,j_0\in\{0,1,\ldots,p-1\}$. We show that $m_{i_0,j_0}=\lambda/p$.

As $S_a=\{(i,j_0-(i-i_0)a)\mid i\in\mathbb{Z}_p\}=\{(i,j_0-ia)\mid i\in\mathbb{Z}_p\}$, using Lemma 4.5(iii), we have $\sum_{(i,j)\in S_a}m_{i,j}=\lambda$. Hence $\sum_{1\leqslant a\leqslant p-1}(\sum_{(i,j)\in S_a}m_{ij})=(p-1)\lambda$. Thus the following holds by Lemma 4.6(i)(ii):

$$(p-1)m_{i_0,j_0}+\sum_{i\neq i_0,\,j\neq j_0}m_{ij}=(p-1)\lambda.$$

Adding $\sum_{j\in\mathbb{Z}_p}m_{i_0,j}(=\lambda)$ and $\sum_{i\in\mathbb{Z}_p}m_{i,j_0}(=\lambda)$ to both sides of the above equation, we obtain $pm_{i_0,j_0}+\sum_{i,j\in\mathbb{Z}_p}m_{ij}=(p+1)\lambda$ by Lemma 4.6(iii). Therefore $m_{i_0,j_0}=\lambda/p$ and the lemma holds. □

A difference matrix over a group U is said to be *normalized* if each entry of its first row is identity of U. In the following, we determine the structure of $(p,k;\lambda)$-difference matrices of coset type over a group of prime order.

Theorem 4.8. *Let p be a prime and assume k is an integer with $k > p$. Let H be a $(p, k; \lambda)$-difference matrix of coset type over a group U of order p with respect to a row of H. Then $p|\lambda$ and there exist p normalized $(p, k/p; \lambda/p)$-difference matrices $H_0, H_1, \dots, H_{p-1}$ over U such that H is equivalent to the following standard form*:

$$\begin{bmatrix} (H_0, H_1, \dots, H_{p-1}) \\ (H_0, H_1, \dots, H_{p-1})w \\ \vdots \\ (H_0, H_1, \dots, H_{p-1})w^{p-1} \end{bmatrix}, \tag{2}$$

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

Proof. We may assume that H is of standard form defined in Notation 4.4. By Lemma 4.7, $p|\lambda$ and so set $\mu = \lambda/p \in \mathbb{N}$. Set $r = k/p \in \mathbb{N}\setminus\{1\}$ (see Remark 4.2) and $h_i = (h_{i,0}, h_{i,1}, \dots, h_{i,p-1})$, where $h_{i,j} \in U^{\lambda}$ $(0 \leqslant i \leqslant r-1)$. Moreover, set $v = h_{i_1} h_{i_2}^{-1}$ for any i_1, i_2 with $0 \leqslant i_1 \neq i_2 \leqslant r-1$. For each $j \in \mathbb{Z}_p$, set $v_j = h_{i_1,j} h_{i_2,j}^{-1}$. Then, by Lemma 4.7, $\widehat{v_j} = \mu U$ and so $H_j := [\, h_{0,j} \ \ \cdots \ \ h_{r-1,j} \,]^T$ $(0 \leqslant j \leqslant p-1)$ is a $(p, r; \mu)$-difference matrix over U. Thus the theorem holds. $\square$

Example 4.9. Let H be the GH(3, 6) matrix over $U = \langle a \rangle \simeq \mathbb{Z}_3$ in Example 3.5(ii). If we arrange H according to the method of Theorem 4.8, we obtain three GH(3, 2) submatrices of H

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & a & a^2 & a & a^2 \\ 1 & a^2 & a^2 & a & a & 1 \\ 1 & a & 1 & a & a^2 & a^2 \\ 1 & a & a^2 & a^2 & 1 & a \\ 1 & a^2 & a & 1 & a^2 & a \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a^2 & a^2 & a & a & 1 \\ 1 & a & 1 & a & a^2 & a^2 \\ 1 & 1 & a & a^2 & a & a^2 \\ 1 & a & a^2 & a^2 & 1 & a \\ 1 & a^2 & a & 1 & a^2 & a \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a & 1 & a & a^2 & a^2 \\ 1 & 1 & a & a^2 & a & a^2 \\ 1 & a^2 & a^2 & a & a & 1 \\ 1 & a & a^2 & a^2 & 1 & a \\ 1 & a^2 & a & 1 & a^2 & a \end{bmatrix},$$

which we denote by H_0, H_1, H_2, respectively. We note that $M := [H_0, H_1, H_2]$ is the submatrix consisting of the $(3s+1)$th rows $(0 \leqslant s \leqslant 5)$ of H in Example 3.5(ii) and H is equivalent to $\tilde{H} = [\, M \ \ Mw \ \ Mw^2 \,]^T$, where $w = (J, Ja, Ja^2) \in U^{18}$ and $J = (1, \dots, 1) \in U^6$. Clearly $\tilde{H}$ is a GH(3, 6) matrix over $\mathbb{Z}_3$ of coset type with respect to the 7th row w of $\tilde{H}$.

We note that the converse of Theorem 4.8 is also true. Let $H_0, H_1, \dots, H_{p-1}$ be normalized $(p, r; \mu)$-difference matrices over $U = \langle a \rangle (\simeq \mathbb{Z}_p)$. Set $H_j = [\, v_{0,j} \ \ \cdots \ \ v_{r-1,j} \,]^T$ and $M = [v_{ij}]_{\substack{0 \leqslant i \leqslant r-1 \\ 0 \leqslant j \leqslant p-1}}$. Then $H = [\, M \ \ Mw \ \ \cdots \ \ Mw^{p-1} \,]^T$ is a $(p, rp; \mu p)$-difference matrix over U of coset type with respect to $\langle w \rangle$, where $w = (J, Ja, \dots, Ja^{p-1})$, $J = (1, \dots, 1) \in U^{p\mu}$. In general, the following holds:

Proposition 4.10. *Let $U = \langle a \rangle$ be a group of prime order p. Let m, s and μ be integers with $m \geqslant 0$ and $s, \mu > 0$. Assume that there exist normalized $(p, s; \mu)$-difference matrices H_j over U of coset type with respect to its p^m rows $W_j \simeq \mathbb{Z}_p^m$ $(0 \leqslant j \leqslant p-1)$. Then there exists a $(p, rp; \mu p)$-difference matrix H over U of coset type with respect to its p^{m+1} rows $W \simeq (\mathbb{Z}_p)^{m+1}$ such that every H_j is a submatrix of H.*

Proof. Set $s = r/p^m (\in \mathbb{N})$. By assumption, we may assume that for each $j \in \{0, \dots, p-1\}$ there exists a $p^m \times p\mu$ submatrix G_j of H_j such that W_j is the set of rows of G_j isomorphic to $\mathbb{Z}_p^m$ and there exist $v_{ij}, g_{ij} \in U^{p\mu}$ such that $v_{0,j} = g_{0,j} = (1, \ldots, 1) \in U^{p\mu}$ and $H_j = [\, G_j v_{0,j} \quad \cdots \quad G_j v_{s-1,j} \,]^T$, $G_j = [\, g_{0,j} \quad \cdots \quad g_{p^m-1,j} \,]^T$. Since G_j's are isomorphic, changing the order of the rows, we may assume that the rows of a $p^m \times p^2\mu$ matrix $[G_0, \ldots, G_{p-1}]$ form a subgroup of $U^{p^2\mu}$ isomorphic to $\mathbb{Z}_p^m$. Set $w = (J, Ja, \ldots, Ja^{p-1}) \in U^{p^2\mu}$, where $J = (1, \ldots, 1) \in U^{p\mu}$ and define an $sp^{m+1} \times p^2\mu$ matrix H over U in the following way:

$$H = [\, M \quad Mw \quad \cdots \quad Mw^{p-1} \,]^T, \quad M = \begin{bmatrix} G_0 v_{0,0} & G_1 v_{0,1} & \cdots & G_{p-1} v_{0,p-1} \\ G_0 v_{1,0} & G_1 v_{1,1} & \cdots & G_{p-1} v_{1,p-1} \\ \vdots & \vdots & \cdots & \vdots \\ G_0 v_{s-1,0} & G_1 v_{s-1,1} & \cdots & G_{p-1} v_{s-1,p-1} \end{bmatrix}.$$

We note that any row of H is of the form $(g_{i,0} v_{k,0}, g_{i,1} v_{k,1}, \ldots, g_{i,p-1} v_{k,p-1}) w^t$ for some i, k, t with $0 \leqslant i \leqslant p^m - 1$, $0 \leqslant k \leqslant s - 1$, $0 \leqslant t \leqslant p - 1$. Clearly the set W of the rows of $[G_0, \ldots, G_{p-1}] \cup [G_0, \ldots, G_{p-1}]w \cup \cdots \cup [G_0, \ldots, G_{p-1}]w^{p-1}$ forms a subgroup of $U^{p^2\mu}$ isomorphic to $\mathbb{Z}_p^{m+1}$. We show that the conclusion of the proposition holds for H. Let z_1 and z_2 be distinct rows of H. Then, there exist (i_1, k_1, t_1) and (i_2, k_2, t_2) $(0 \leqslant i_1, i_2 \leqslant s - 1,\ 0 \leqslant k_1, k_2 \leqslant p^m - 1,\ 0 \leqslant t_1, t_2 \leqslant p - 1)$ such that

$$z_1 = (g_{i_1,0} v_{k_1,0}, g_{i_1,1} v_{k_1,1}, \ldots, g_{i_1,p-1} v_{k_1,p-1}) w^{t_1} \quad \text{and}$$
$$z_2 = (g_{i_2,0} v_{k_2,0}, g_{i_2,1} v_{k_2,1}, \ldots, g_{i_2,p-1} v_{k_2,p-1}) w^{t_2}.$$

Then jth $(0 \leqslant j \leqslant p - 1)$ part of $z_1 z_2^{-1}$ is

$$g_{i_1,j} v_{k_1,j} J a^{jt_1} \left(g_{i_2,j} v_{k_2,j} J a^{jt_2} \right)^{-1} = g_{i_1,j} v_{k_1,j} (g_{i_2,j} v_{k_2,j})^{-1} J a^{j(t_1 - t_2)}. \tag{3}$$

First assume that $(i_1, k_1) \neq (i_2, k_2)$ and set $f = g_{i_1,j} v_{k_1,j} (g_{i_2,j} v_{k_2,j})^{-1}$. Then $g_{i_1,j} v_{k_1,j}$ and $g_{i_2,j} v_{k_2,j}$ are distinct rows of H_j. Hence $\widehat{f} = p\mu U$ and so $\widehat{f J a^{j(t_1 - t_2)}} = p\mu U$ for any j. It follows that $\widehat{z_1 z_2^{-1}} = p^2\mu U$.

Next we assume that $(i_1, k_1) = (i_2, k_2)$. As $z_1 \neq z_2$, $t_1 \neq t_2$ and so the jth part of $z_1 z_2^{-1}$ is $J a^{j(t_1 - t_2)}$, where $t_1 - t_2 \not\equiv 0 \pmod{p}$. Hence $\widehat{z_1 z_2^{-1}} = p^2\mu U$. Hence H is a $(p, rp; \mu p)$-difference matrix over U of coset type with respect to $W \simeq \mathbb{Z}_p^{m+1}$. Thus the proposition holds. $\square$

By repeated application of Proposition 4.10 we have the following:

Corollary 4.11. *Let $H_0, \ldots, H_{p-1}$ be $(p, r; \mu)$-difference matrices over a group U of prime order p. Then there exists a $(p, p^n r; p^n\mu)$-difference matrix H over U of coset type with respect a subgroup $W (\simeq \mathbb{Z}_p^n \subset U^{p^{n+1}\mu})$ consisting of its p^n rows and H_i's are submatrices of H.*

The following is an application of Proposition 4.10:

Example 4.12. Let $p = 2$ and let H_1 and H_2 be any normalized Hadamard matrices of order n over $\{\pm 1\}$. Then $H = \left[\begin{smallmatrix} H_1 & H_2 \\ H_1 & -H_2 \end{smallmatrix}\right]$ is also a Hadamard matrix of order $2n$ with respect to the $(n+1)$th row $(1, \ldots, 1, -1, \ldots, -1)$ of H. The five Hadamard matrices of order 16 given by Todd (1933) are of this type (see Table 7.3 of [5]).

Concerning Theorem 4.8, we would like to raise the following question:

Question 4.13. If $|U| = p^n > p$, what can we say about the structure of a $(p^n, k; \lambda)$-difference matrix of coset type over U?

References

[1] T. Beth, D. Jungnickel, H. Lenz, Design Theory, vol. I, second edition, Cambridge University Press, 1999.
[2] C.J. Colbourn, J.H. Dinitz, The CRC Handbook of Combinatorial Designs, second edition, Chapman & Hall/CRC Press, Boca Raton, 2007.
[3] C.J. Colbourn, D.L. Kreher, Concerning difference matrices, Des. Codes Cryptogr. 9 (1996) 61–70.
[4] W. de Launey, Generalized Hadamard matrices whose rows and columns form a group, in: L.R.A. Casse (Ed.), Combinatorial Mathematics X, in: Lecture Notes in Math., Springer, Berlin, 1983.
[5] A.S. Hedayat, N.J.A. Sloane, J. Stufken, Orthogonal Arrays, Springer, New York, 1999.
[6] D. Jungnickel, On difference matrices, resolvable transversal designs and generalised Hadamard matrices, Math. Z. 167 (1979) 49–60.
[7] P.H.J. Lampio, P.R.J. Östergard, Classification of difference matrices over cyclic groups, J. Statist. Plann. Inference 141 (2011) 1194–1207.
[8] T.P. McDonough, V.C. Mavron, C.A. Pallikaros, Generalised Hadamard matrices and translations, J. Statist. Plann. Inference 86 (2000) 527–533.