Constructions of Butson Hadamard Matrices Invariant Under Abelian p-Groups

Bernhard Schmidt
School of Physical & Mathematical Sciences
Nanyang Technological University
Singapore 637371, Republic of Singapore [*]

Dai Quan Wong
School of Physical & Mathematical Sciences
Nanyang Technological University
Singapore 637371, Republic of Singapore

Qing Xiang
Department of Mathematical Sciences
University of Delaware
Newark, Delaware 19716, USA

May 3, 2020

[*]This research is supported by the Ministry of Education, Singapore, under its Academic Research Fund Tier 1 (RG27/18)

Abstract

Let a and h be positive integers and let p be a prime. Let $q_1, \dots, q_t$ be the distinct prime divisors of h and write $\mathcal{Q}(h) = \left\{\sum_{i=1}^{t} c_i q_i : c_i \in \mathbb{Z}, c_i \geq 0\right\}$. We provide constructions of group invariant Butson Hadamard matrices $\mathrm{BH}(G, h)$ in the following cases.

1. $G = (\mathbb{Z}_p)^{2a}$ and at least one of the following conditions is satisfied.
   - $p^a \in \mathcal{Q}(h)$,
   - $p^a + 2 \in \mathcal{Q}(h)$ and h is even,
   - $p^a + 1 = (q_1 - 1)(q_2 - 1)$ where q_1 and q_2 are distinct prime divisors of h.
2. $G = \mathbb{Z}_{p^a} \times \mathbb{Z}_{p^a}$ and $p - 1, p \in \mathcal{Q}(h)$.
3. $G = (\mathbb{Z}_{p^2})^a$ and $p^b \in \mathcal{Q}(h)$ for some divisor b of a with $1 \leq b < a$.
4. $G = P \times \mathbb{Z}_p^a$ where P is any abelian group of order p^a and $p \in \mathcal{Q}(h)$.

1 Introduction

Let H be a square matrix of order n all of whose entries are complex roots of unity, let H^* denote the complex conjugate transpose of H, and let I be the identity matrix of order n. If $HH^* = nI$, then H is called a **Butson Hadamard matrix**. If all entries of H are complex hth roots of unity, we call H a **BH(n, h) matrix**. In particular, a Hadamard matrix of order n is a $\mathrm{BH}(n, 2)$ matrix.

Let G be an abelian group of order n which is written multiplicatively. An $n \times n$ matrix $A = (a_{g,k})_{g,k \in G}$, whose rows and columns are indexed by elements of G, is called ***G*-invariant** (or just **group-invariant**) if $a_{gl,kl} = a_{g,k}$ for all $g, k, l \in G$. A G-invariant $\mathrm{BH}(n, h)$ matrix is called a **BH(G, h) matrix**.

An overview of most known results on Butson Hadamard matrices is given in the Ph.D. thesis of Szöllősi [22]. More recent work on Butson Hadamard matrices and group-invariant Butson Hadamard matrices can be found in [12, 14, 16]. A survey of group-invariant Butson Hadamard matrices and related objects is provided in [21].

For an abelian group G, let $\exp(G)$ denote the least common multiple of the orders of the elements of G. It is well known [3] that group invariant $\mathrm{BH}(n, 2)$ matrices, i.e., group invariant Hadamard matrices, are equivalent to Hadamard difference sets. Thus the following is a consequence of the results of Turyn [23], Davis [8], and Kraemer [15] on Hadamard difference sets.

Result 1.1 (Turyn, Davis, Kraemer)**.** *Let G be an abelian group of order 2^{2a}. A $\mathrm{BH}(G,2)$ matrix exists if and only if $\exp(G) \leq 2^{a+1}$.*

The main purpose of this paper is a partial generalization of the existence part of Result 1.1 to abelian p-groups. It should be noted, however, that there is no chance to generalize Result 1.1 to $\mathrm{BH}(G,2)$ matrices with G being an abelian p-group of odd order, since Hadamard matrices of odd order larger than 1 do not exist. Instead, we are constructing $\mathrm{BH}(G,h)$ matrices with $h > 2$. Curiously, quite general constructions are known already for $\mathrm{BH}(G,h)$ matrices in the case where G is an abelian p-group and p divides h, see [2, 12, 21]. Very little is known, however, in the case where $\gcd(p,h) = 1$. It is this latter case that we focus on.

Our first few constructions are similar to the "big subgroup construction" of relative difference sets given in [9]. In fact, the subgroups we need are obtained from spreads of elementary abelian groups that correspond to translation planes. We use these subgroups as a foundation to build Butson Hadamard matrices in the form of group ring elements. More specifically, we create a group ring expression by assigning the same root of unity as coefficients to all elements of certain subgroups. If a group element is in more than one of the chosen subgroups, the coefficients assigned to these subgroups must add up to another root of unity. This requirement will determine the conditions under which our constructions work. For instance, we prove the following.

Theorem 1.2. *Let p be a prime and suppose there are complex hth roots of unity $\eta_0, \ldots, \eta_p$ such that $\sum_{i=0}^{p} \eta_i$ is a root of unity. Then there exists a $\mathrm{BH}(\mathbb{Z}_p \times \mathbb{Z}_p, h)$ matrix.*

It is interesting to note that Craigen and Szöllősi's construction of $\mathrm{BH}(p^2,6)$ matrices [22, Theorem 1.4.41] is as a special case of Theorem 1.2. In fact, suppose that p is an odd prime and set

$$\eta_0 = 1, \eta_p = \zeta_3 \text{ and } \eta_i = \left(\frac{i}{p}\right) \text{ for } i = 1, \ldots, p-1 \tag{1}$$

in Theorem 1.2, where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. Then we recover [22, Thm. 1.4.41]. This is not obvious at first glance, as [22, Thm. 1.4.41] uses Paley matrices and Kronecker products whereas our construction is described in the language of group rings. However, a direct comparison of the matrices shows that this is indeed the case.

In Section 4, we construct Butson Hadamard matrices invariant under $\mathbb{Z}_{p^a} \times \mathbb{Z}_{p^a}$ by exploiting the way the cyclic subgroups of these groups are "nested". A recursive construction of Butson Hadamard matrices invariant under $\mathbb{Z}_{p^a} \times (\mathbb{Z}_p)^a$ based on elementary properties of finite affine geometries is given in Section 5. In Section 6, Galois rings are employed to obtain a construction of $\mathrm{BH}(G,h)$ matrices for groups G of the form $\mathbb{Z}_{p^2}\times\cdots\times\mathbb{Z}_{p^2}$ for a prime p. Finally, in Section 7, we use non-homomorphic character sum preserving bijections between abelian groups that were introduced in [13] to extend our constructions to further classes of abelian p-groups.

For all our construction methods, vanishing sums of roots of unity play a crucial role. and we heavily use relevant results of Lam and Leung [17]. The following is the central result of [17] we need.

Result 1.3. *Let $h,k\geq 2$ be integers and let $q_1,\ldots,q_t$ be the distinct prime divisors of h. There are complex hth roots of unity $\eta_1,\ldots,\eta_k$ with $\eta_1+\cdots+\eta_k=0$ if and only if*

$$k=\sum_{i=1}^{t}a_iq_i \tag{2}$$

for some nonnegative integers a_i.

Note that, using the notation introduced in the abstract, condition (2) is equivalent to $k\in\mathcal{Q}(h)$.

2 Preliminaries

Throughout this paper, we write $\zeta_h=\exp(2\pi i/h)$ and

$$\mathcal{U}(h)=\{\zeta_h^i : i=0,\ldots,h-1\}.$$

Furthermore, $\mathbb{Z}_m$ denotes a cyclic group of order m.

2.1 Group Rings and Characters

We use the language of group rings to formulate our constructions. Let G be a multiplicatively written finite abelian group and let R be a ring. The elements of the group ring $R[G]$ have the form $X=\sum_{g\in G}a_gg$ with $a_g\in R$. The a_g's are called the **coefficients** of X and $\mathrm{supp}(X)=\{g\in G : b_g\neq 0\}$ is the **support** of X. Two elements $X=\sum_{g\in G}a_gg$ and $Y=\sum_{g\in G}b_gg$ of $R[G]$ are equal if and only if $a_g=b_g$ for all $g\in G$. A subset S of G is identified with the group ring element $\sum_{g\in S}g$. For the identity element 1_G of G and $\lambda\in R$, we write λ for the group ring element $\lambda 1_G$.

For our purposes, group rings $R[G]$ with $R=\mathbb{Z}[\zeta_h]$ will be useful. In this case, the elements of $R[G]$ have the form $X=\sum_{g\in G}a_gg$ with $a_g\in\mathbb{Z}[\zeta_h]$ and we write

$$X^{(-1)}=\sum_{g\in G}\overline{a_g}g^{-1},$$

where $\overline{a_g}$ is the complex conjugate of a_g.

We denote the group of complex characters of G by $\widehat{G}$. For $U \leq G$, write

$$U^{\perp} = \{\chi \in \widehat{G} : \chi(g) = 1 \text{ for all } g \in U\}.$$

Characters χ of G are extended to the group ring $R[G]$ by $\chi(X) = \sum_{g\in G} a_g \chi(g)$ for $X = \sum_{g\in G} a_g g \in R[G]$. The **trivial character** of G is the character that maps all elements of G to 1.

The following is a useful criterion for checking if group invariant matrices are Butson Hadamard matrices. For a proof, see [21, Lem. 2.1].

Result 2.1. *Let G be a finite abelian group, let h be a positive integer, and let $a_g \in \mathcal{U}(h)$ for all $g \in G$. Consider the element $D = \sum_{g\in G} a_g g$ of $\mathbb{Z}[\zeta_h][G]$. The G-invariant matrix $(a_{gk^{-1}})_{g,k\in G}$ is a $\mathrm{BH}(G, h)$ matrix if and only if*

$$DD^{(-1)} = |G|. \tag{3}$$

Moreover, (3) holds if and only if

$$|\chi(D)|^2 = |G| \text{ for all } \chi \in \widehat{G}.$$

For the rest of this paper, we identify the group ring elements D as in Result 2.1 with the corresponding group invariant matrices $(a_{gk^{-1}})_{g,k\in G}$. Hence, if (3) holds, we will just say that D is a $\mathrm{BH}(G, h)$ matrix.

For a proof of the following result, see [3, Chapter VI, Lemma 3.5], for instance.

Result 2.2. *Let G be a finite abelian group and $D = \sum_{g\in G} a_g g$ with $a_g \in \mathbb{C}$. Then*

$$a_g = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(Dg^{-1}) \text{ for all } g \in G.$$

2.2 Sums of Roots of Unity

Sums of roots of unity satisfying certain conditions will be an essential tool for all our constructions of Butson Hadamard matrices. We now state a number theoretic result determining precisely when these conditions can be satisfied. We defer the proof of this result to the appendix, since it is quite technical.

Let $h \geq 2$ be a integer and let $q_1, \ldots, q_t$ be the distinct prime divisors of h. We recall the following notation.

$$\mathcal{Q}(h) = \left\{ \sum_{i=1}^{t} a_i q_i : a_i \in \mathbb{Z}, a_i \geq 0 \right\},$$
$$\mathcal{U}(h) = \{\zeta_h^i : i = 0, \ldots, h-1\}.$$

Theorem 2.3. *Let h, m be positive integers.*

(a) There are $\eta_1, \ldots, \eta_m \in \mathcal{U}(h)$ with $\sum_{i=1}^m \eta_i = 0$ if and only if $m \in \mathcal{Q}(h)$.

(b) There are $\eta_1, \ldots, \eta_m \in \mathcal{U}(h)$ with

$$\sum_{i=1}^{m} \eta_i = 1 \tag{4}$$

if and only if one of the following conditions is satisfied.

(i) h is even and $m+1 \in \mathcal{Q}(h)$,

(ii) h is odd and $m-1 \in \mathcal{Q}(h)$,

(iii) h is odd, has at least two distinct prime divisors, and $m = (q_1-1)(q_2-1)$, where q_1, q_2, $q_1 \neq q_2$, are the two smallest prime divisors of h.

3 Construction from Finite Translation Planes

Let G be a finite group of order m^2. A collection $U_0, \ldots, U_m$ of subgroups of G with $|U_i| = m$ for all i, $U_iU_j = G$ for all $i \neq j$, and $\bigcup_{i=0}^m U_i = G$ is called a **spread** of G. By the fundamental work of André [1], there is a one-to-one correspondence between spreads in finite groups and finite translation planes. Moreover, there is a spread in a group G of order m^2 if and only if G is an elementary abelian p-group for some prime p.

Theorem 3.1. *Let $U_0, \ldots, U_m$ be a spread of a group G of order m^2 and let $\eta_0, \ldots, \eta_m$ be any complex roots of unity with $\sum_{i=0}^m \eta_i = 1$. Then*

$$X = \sum_{i=0}^{m} U_i \eta_i.$$

is a $\mathrm{BH}(G, h)$ matrix, where h is the least common multiple of the orders of the η_i's.

Proof. It follows from the definition of X that $X = \sum_{g \in G} a_g g$ with $a_g \in \mathbb{Z}[\zeta_h]$. We first show $a_g \in \mathcal{U}(h)$ for all $g \in G$. As $|U_i| = m$ for all i and $U_i \cap U_j = \{1\}$ for all $i \neq j$, every nonidentity element g of G is contained exactly one U_i. Hence $a_g = \eta_i \in \mathcal{U}(h)$. The coefficient of the identity element in X is $\sum_{i=0}^{m} \eta_i = 1$ by assumption. Thus $a_g \in \mathcal{U}(h)$ for all $g \in G$.

Now let χ be any nontrivial character of G. If χ was trivial on both U_i and U_j for some $i \neq j$, then it would be trivial on $U_i U_j = G$, a contradiction. Hence $|U_i^{\perp} \cap U_j^{\perp}| = 1$ for all $i \neq j$. This implies

$$\left| \bigcup_{i=0}^{m} U_i^{\perp} \right| = (m+1)m - m = m^2$$

and thus $\bigcup_{i=0}^{m} U_i^{\perp} = \hat{G}$. Hence every nontrivial character of G is trivial on exactly one U_i. Suppose χ is nontrivial on U_i. Then $\chi(X) = \chi(U_i)\eta_i = m\eta_i$ and thus $|\chi(X)| = m^2$. For the trivial character χ_0 of G, we have

$$\chi_0(X) = \sum_{i=0}^{m} |U_i| \eta_i = m \sum_{i=0}^{m} \eta_i = m$$

by assumption and thus $|\chi_0(X)| = m^2$. In summary, we have shown $|\chi(X)| = m^2$ for all characters χ of G. Hence $X \in \mathrm{BH}(G, h)$ by Result 2.1. □

Translation planes and thus spreads of elementary abelian groups exist in abundance; see the monograph [18], for instance. In particular, we have the following.

Corollary 3.2. *Let G be an elementary abelian group of order p^{2a} and let h be any positive integer such that at least one of the following conditions is satisfied.*

- $p^a \in \mathcal{Q}(h)$,
- $p^a + 2 \in \mathcal{Q}(h)$ *and h is even,*
- $p^a + 1 = (q_1 - 1)(q_2 - 1)$ *where q_1 and q_2 are distinct prime divisors of h.*

Then there is a $\mathrm{BH}(G, h)$ *matrix.*

Proof. It is well known [18] that there is a spread in G. Hence, by Theorem 3.1, it suffices to show that there are $\eta_1, \ldots, \eta_{p^a+1} \in \mathcal{Q}(h)$ with

$$\sum_{i=1}^{p^a+1} \eta_i = 1. \tag{5}$$

First suppose that $p^a \in \mathcal{Q}(h)$. If h is odd, then (5) follows from Theorem 2.3 (b), as condition (ii) of this theorem is satisfied. If h is even, then $p^a + 2 \in \mathcal{Q}(h)$, as we assume $p^a \in \mathcal{Q}(h)$ and 2 is a prime divisor of h. Hence condition (i) of Theorem 2.3 (b) holds and (5) follows.

If $p^a + 2 \in \mathcal{Q}(h)$ and h is even, then (5) directly follows from Theorem 2.3 (b). Finally, suppose $p^a + 1 = (q_1 - 1)(q_2 - 1)$ where q_1 and q_2 are distinct prime divisors of h. Then expanding the left hand side of $(\zeta_{q_1} + \cdots + \zeta_{q_1}^{q_1-1})(\zeta_{q_2} + \cdots + \zeta_{q_2}^{q_2-1}) = 1$ gives a solution of (5). □

Corollary 3.3. *Let h be a positive integer with at least two distinct prime divisors and let q_1 and q_2 be the two smallest prime divisors of h. For every elementary abelian group of order p^{2a} with $p^a \geq (q_1 - 1)(q_2 - 1) - 1$, there is a* $\mathrm{BH}(G, h)$ *matrix.*

Proof. If $p^a = (q_1 - 1)(q_2 - 1) - 1$, then a $\mathrm{BH}(G, h)$ matrix exists by Corollary 3.2. Hence we can assume $p^a \geq (q_1 - 1)(q_2 - 1)$. Then $p^a \in \mathcal{Q}(h)$ by [17, Lem. 5.1] and thus a $\mathrm{BH}(G, h)$ matrix exists by Corollary 3.2. □

Corollary 3.4. *A* $\mathrm{BH}(G, 6)$ *matrix exists for every elementary abelian group G of square order.*

Proof. This follows from Corollary 3.3, as $(q_1 - 1)(q_2 - 1) = 2$ for $h = 6$. □

4 Nested Cyclic Subgroups Construction

Throughout this section, G denotes the group $\mathbb{Z}_{p^a} \times \mathbb{Z}_{p^a}$, where p is a prime and a is a positive integer. Our next construction uses cyclic subgroups of G of order p^a as building blocks for $\mathrm{BH}(G, h)$ matrices. We start with a preliminary result. By $\mathcal{M}(b)$ we denote the set of cyclic subgroups of G of order p^b, $0 \leq b \leq a$.

Lemma 4.1. *Using the notation just introduced, we have the following.*

(i) $|\mathcal{M}(b)| = (p + 1)p^{b-1}$ *for* $1 \leq b \leq a$.

(ii) Suppose $1 \leq b \leq a - 1$. *Each subgroup in* $\mathcal{M}(b)$ *is contained in exactly* p *subgroups in* $\mathcal{M}(b + 1)$.

(iii) Let χ *be a character of* G *of order* p^b, $0 \leq b \leq a$. *Then there is* $T \in \mathcal{M}(a - b)$ *such that the following holds for every* $K \in \mathcal{M}(a)$.

$$K \leq \ker(\chi) \text{ if and only if } T \leq K.$$

Proof. Parts (i) and (ii) are well known, but we include a proof for the convenience of the reader. There are exactly $p^{2b} - p^{2b-2}$ elements of G of order p^b and each subgroup in $\mathcal{M}(b)$ has exactly $(p-1)p^{b-1}$ generators. Hence

$$|\mathcal{M}(b)| = (p^{2b} - p^{2b-2})/((p-1)p^{b-1}) = (p+1)p^{b-1}.$$

This proves (i).

Suppose $1 \leq b \leq a-1$. As $\mathrm{Aut}(G)$ is transitive on $\mathcal{M}(b)$, each subgroup in $\mathcal{M}(b)$ is contained in same number of subgroups in $\mathcal{M}(b+1)$. Since $|\mathcal{M}(b+1)|/|\mathcal{M}(b)| = p$ and each subgroup in $\mathcal{M}(b+1)$ contains exactly one subgroup in $\mathcal{M}(b)$, we conclude that (ii) holds.

We now prove (iii). It is straightforward to show that $\ker(\chi)$ contains an element of order p^a. Let g be such an element and let k be another element of order p^a of G such that $G = \langle g, k \rangle$. Since χ has order p^b and $\chi(g) = 1$, we have $\chi(k) = \zeta_{p^b}^t$ for some integer t coprime to p. Set $T = \langle g^{p^b} \rangle$.

Write $K = \langle g^i k^j \rangle$ for some integers i, j. Since K has order p^a, we have $T \leq K$ if and only if $(g^i k^j)^{p^b} \in T$, that is, $k^{jp^b} = 1$. This holds if and only if $j \equiv 0 \pmod{p^{a-b}}$. On the other hand, we have $K \leq \ker(\chi)$ if and only if $\chi(g^i k^j) = \zeta_{p^b}^{tj} = 1$, which also holds if and only if $j \equiv 0 \pmod{p^{a-b}}$. This proves (iii). □

Before we state our construction, we introduce some more notation. By $\mathcal{C}(G)$ we denote the set of all cyclic subgroups of G of order larger than 1. For each cyclic subgroup U of G with $1 \leq |U| \leq p^{a-1}$, let $\mathcal{S}(U)$ be the set of cyclic subgroups of G of order $p|U|$ that contain U. By Result 4.1, we have $|\mathcal{S}(U)| = p$ for all U with $p \leq |U| \leq p^{a-1}$ and $|\mathcal{S}(U)| = p+1$ if $|U| = 1$. Note that

$$\mathcal{C}(G) = \bigcup_U \mathcal{S}(U), \tag{6}$$

where U runs over all cyclic subgroups U of G with $1 \leq |U| \leq p^{a-1}$ and the right hand side of (6) is a partition of $\mathcal{C}(G)$ into pairwise disjoint subsets.

Theorem 4.2. *Let η_W, $W \in \mathcal{C}(G)$, be complex roots of unity such that*

$$\sum_{W \in \mathcal{S}(U)} \eta_W = \eta_U \tag{7}$$

for all cyclic subgroups U of G with $1 \leq |U| \leq p^{a-1}$. Then

$$X = \sum_{W \in \mathcal{M}(a)} \eta_W W$$

is a $\mathrm{BH}(G,h)$ *matrix, where* h *is the least common multiple of all the orders of* η_W*,* $W \in \mathcal{C}(G)$*.*

Proof. We first show that (7) implies

$$\sum_{\substack{W\in\mathcal{M}(a)\\ U\subseteq W}} \eta_W = \eta_U \tag{8}$$

for every cyclic subgroup U of G. We prove (8) by backward induction on $|U|$. For $|U| = p^a$, the only subgroup in $\mathcal{M}(a)$ containing U is U itself, so (8) holds. Now assume that (8) holds for all U with $|U| = p^b$ where $1 \le b \le a$. Let K be a cyclic subgroup of G of order p^{b-1}.

Since $|K'| = p^b$ for $K' \in \mathcal{S}(K)$, we have

$$\sum_{\substack{W\in\mathcal{M}(a)\\ K'\subseteq W}} \eta_W = \eta_{K'} \tag{9}$$

by the induction hypothesis. Note that a subgroup $W \in \mathcal{M}(a)$ contains K if and only if W contains exactly one of the subgroups in $\mathcal{S}(K)$, that is, we have

$$\{W \in \mathcal{M}(a) : K \subseteq W\} = \{W \in \mathcal{M}(a) : K' \subseteq W \text{ for exactly one } K' \in \mathcal{S}(K)\}.$$

Using this and (7), (9), we get

$$\sum_{\substack{W\in\mathcal{M}(a)\\ K\subseteq W}} \eta_W = \sum_{K'\in\mathcal{S}(K)} \sum_{\substack{W\in\mathcal{M}(a)\\ K'\subseteq W}} \eta_W = \sum_{K'\in\mathcal{S}(K)} \eta_{K'} = \eta_K.$$

This completes the proof of (8).

From the definition of X, it is clear that $X = \sum_{g\in G} a_g g$ with $g \in \mathbb{Z}[\zeta_h]$. We now show that $a_g \in \mathcal{U}(h)$ for all $g \in G$. Let g be any element of G and let U be the cyclic group generated by g. By the definition of X and (8), we have

$$a_g = \sum_{\substack{W\in\mathcal{M}(a)\\ U\subseteq W}} \eta_W = \mu_U$$

and thus $a_g \in \mathcal{U}(h)$ as required.

Finally, let χ be any character of G and let p^b be the order of χ. By Lemma 4.1, there is a cyclic subgroup T of G such that the following holds for every $W \in \mathcal{M}(a)$.

$$W \le \ker(\chi) \text{ if and only if } T \le W.$$

Moreover, note that $\chi(W) = p^a$ if $W \le \ker(\chi)$ and $\chi(W) = 0$ otherwise. Hence

$$\chi(X) = \sum_{\substack{W\in\mathcal{M}(a)\\ T\subseteq W}} p^a \eta_W = \eta_T p^a$$

by (8). Hence $|\chi(X)|^2 = p^{2a}$ for all characters χ of G. Thus X is a $\mathrm{BH}(G, h)$ matrix by Result 2.1. □

Corollary 4.3. *Let p be a prime and let a, h be positive integers such that $p-1, p \in \mathcal{Q}(h)$. Then there is a $\mathrm{BH}(\mathbb{Z}_{p^a} \times \mathbb{Z}_{p^a}, h)$ matrix.*

Proof. Write $G = \mathbb{Z}_{p^a} \times \mathbb{Z}_{p^a}$. By Theorem 4.2, it suffices to show that there are roots of unity $\eta_W \in \mathcal{U}(h)$, $W \in \mathcal{C}(G)$, such that

$$\sum_{W \in \mathcal{S}(U)} \eta_W = \eta_U \tag{10}$$

for all cyclic subgroups U of G with $1 \leq |U| \leq p^{a-1}$. Recall that $\mathcal{C}(G)$ is the union of the pairwise disjoint sets $\mathcal{S}(U)$, where U runs over all cyclic subgroups of G with $1 \leq |U| \leq p^{a-1}$. We construct the necessary roots of unity η_W recursively. For $U = \{1\}$, the set $\mathcal{S}(U)$ consists of the $p+1$ subgroups of G of order p. Let $W_1, \ldots, W_{p+1}$ denote these subgroups. We first show that there are $\eta_1, \ldots, \eta_{p+1} \in \mathcal{U}(h)$ with

$$\sum_{i=1}^{p+1} \eta_i = 1. \tag{11}$$

If h is odd, then (11) has a solution by Theorem 2.3 (b) (ii), since $p \in \mathcal{Q}(h)$ by assumption. If h is even, then $p + 2 \in Q(h)$, as $p \in \mathcal{Q}(h)$ and 2 is a prime divisor of h. Hence (11) has a solution by Theorem 2.3 (b) (i). This completes the proof of (11). Now set $\eta_{\{1\}} = 1$ and $\eta_{W_i} = \eta_i$ for $i = 1, \ldots, p+1$. This solves (10) for $U = \{1\}$.

Suppose that η_W's have been chosen such that (10) holds for all for all cyclic subgroups U of G with $1 \leq |U| \leq p^b$ and $b \leq a-2$. Recall that $p - 1 \in \mathcal{Q}(h)$ by assumption. In the same way as above, we see that there are $\mu_1, \ldots, \mu_p \in \mathcal{U}(h)$ with $\sum_{i=1}^{p} \mu_i = 1$. Now let U be any cyclic subgroup of G with $|U| = p^{b+1}$ and let $K_1, \ldots, K_p$ the subgroups in $\mathcal{S}(U)$. Setting $\eta_{K_i} = \mu_i \eta_U$ for $i = 1, \ldots, p$ solves (10) for U. Since the sets $\mathcal{S}(U)$ are pairwise disjoint, we can thus solve (10) for all cyclic subgroups U of G with $|U| = p^{b+1}$. This shows that (10) has a solution. □

5 Recursive Subspace Construction

The constructions in the previous sections, in particular, yield $\mathrm{BH}(\mathbb{Z}_p \times \mathbb{Z}_p, h)$ matrices for all primes p. We now use these matrices as an ingredient in a recursive construction that produces $\mathrm{BH}(\mathbb{Z}_{p^a} \times (\mathbb{Z}_p)^a, h)$ matrices for all primes p and positive integers a. A second essential ingredient will be subspaces of the maximal elementary abelian subgroup of $\mathbb{Z}_{p^a} \times (\mathbb{Z}_p)^a$, when viewed as an finite affine geometry $\mathrm{AG}(a+1,p)$.

We first fix some notation that we use throughout this section. Let p be a prime and let a be positive integer. Let G_a denote the group $\mathbb{Z}_{p^a} \times (\mathbb{Z}_p)^a$, and write

$$G_a = \langle \alpha \rangle \times \langle \beta \rangle \times \langle \gamma_1 \rangle \times \cdots \times \langle \gamma_{a-1} \rangle,$$

where the order of α is p^a and the orders of β, γ_i, for $i = 1, \ldots, a-1$, are all equal to p. The following elementary abelian subgroups of G_a will play a crucial role.

$$\begin{aligned}
W &= \langle \alpha^{p^{a-1}}, \beta, \gamma_1, \ldots \gamma_{a-1} \rangle, \\
U &= \langle \alpha^{p^{a-1}} \rangle, \\
R &= \langle \gamma_1, \ldots, \gamma_{a-1} \rangle, \\
S &= RU = \langle \alpha^{p^{a-1}}, \gamma_1, \ldots, \gamma_{a-1} \rangle.
\end{aligned}$$

Note that $\langle \alpha^p \rangle \times R \cong \mathbb{Z}_{p^{a-1}} \times \mathbb{Z}_p^{a-1} \cong G_{a-1}$. Hence we can identify G_{a-1} with $\langle \alpha^p \rangle \times R$. Moreover, $W \cong \mathbb{Z}_p^{a+1}$ is the maximal elementary abelian subgroup of G_a. We view W as an affine geometry $\mathrm{AG}(a+1,p)$ and S as a subgeometry of W. In particular, we call subgroups of W of order p^a **hyperplanes of W** and subgroups of S of order p^{a-1} **hyperplanes of S**. The following is well known and straightforward to prove.

Result 5.1. *Using the notation just introduced we have the following.*

(a) *There are exactly p^{a-1} hyperplanes of S that do not contain U and exactly p^a hyperplanes of W that do not contain U.*

(b) *For every hyperplane H of S that does not contain U, there are exactly p hyperplanes V of W with $H \le V$ and $U \not\le V$.*

(c) *Let χ be a character of G that is nontrivial on W. Then χ is trivial on exactly one hyperplane of W.*

Based on Result 5.1, we introduce some more notation.

- By $H_0, \ldots, H_{p^{a-1}-1}$ we denote the hyperplanes of S that do not contain U.
- For each i with $0 \le i \le p^{a-1}-1$, let $V_{i,0}, \ldots, V_{i,p-1}$ be the hyperplanes of W that contain H_i and do not contain U.

Suppose $V_{i,j} = V_{i',j'}$ with $i \neq i'$. Then $V_{i,j}$ contains both H_i and $H_{i'}$ and thus S. But this is impossible, since $U \leq S$ and $U \not\leq V_{i,j}$. This shows that the hyperplanes $V_{i,j}$, $i = 0, \ldots, p^{a-1} - 1$, $j = 0, \ldots, p - 1$, are pairwise distinct. Using Result 5.1 (a), we conclude that the $V_{i,j}$'s are all the hyperplanes of W that do not contain U.

Theorem 5.2. *We use the notation introduced above. Suppose that $\zeta_{i,j}$, $i = 0, \ldots, p^{a-1} - 1$, $j = 0, \ldots, p - 1$, are complex roots of unity satisfying*

$$\sum_{j=0}^{p-1} \zeta_{i,j} = 0 \text{ for } i = 0, \ldots, p^{a-1} - 1. \tag{12}$$

Moreover, suppose that $\eta_{i,g}$, $i = 0, \ldots, p^{a-1} - 1$, $g \in R$, are complex roots of unity such that

$$Y = \sum_{i=0}^{p^{a-1}-1} \sum_{g \in R} \eta_{i,g} g \alpha^{pi}$$

is a $\mathrm{BH}(G_{a-1}, h)$ matrix. Let $g_i \in R$, $i = 0, \ldots, p^{a-1} - 1$, be arbitrary and let k be any integer. Then

$$X = \sum_{i=0}^{p^{a-1}-1} \left(\sum_{j=0}^{p-1} \zeta_{i,j} V_{i,j} g_i + \sum_{g \in R} \eta_{i,g} U g \right) \alpha^i \beta^{ki} \tag{13}$$

is a $\mathrm{BH}(G_a, h)$ matrix, where h is the least common multiple of the orders of all $\zeta_{i,j}$'s and $\eta_{i,g}$'s.

Proof. We first show that all coefficients of X are in $\mathcal{U}(h)$. Fix any $i \in \{0, \ldots, p^{a-1} - 1\}$ and set

$$X_i = A_i + B_i \text{ where } A_i = \sum_{j=0}^{p-1} \zeta_{i,j} V_{i,j} g_i \text{ and } B_i = \sum_{g \in R} \eta_{i,g} U g.$$

Write $X_i = \sum_{x \in W} b_{x,i} x$ with $b_{x,i} \in \mathbb{Z}[\zeta_h]$. We show that $b_{x,i} \in \mathcal{U}(h)$ for all $x \in W$.

We have $V_{i,j} \cap S = H_i$ for $j = 0, \ldots, p-1$, as S and $V_{i,j}$ are distinct hyperplanes of W and thus intersect in a hyperplane of S. Hence the sets $V_{i,j} \setminus S$, $j = 0, \ldots, p-1$, are pairwise disjoint and the union of these sets covers exactly $p(|V_{i,j}| - |H_i|) = p(p^a - p^{a-1}) = p^{a+1} - p^a$ elements of $W \setminus S$. Since $|W \setminus S| = p^{a+1} - p^a$, we conclude $\bigcup_{j=0}^{p-1} (V_{i,j} \setminus S) = W \setminus S$. As $g_i \in R \leq S$, this implies

$$\bigcup_{j=0}^{p-1} (V_{i,j} g_i \setminus S) = W \setminus S \tag{14}$$

and the left hand side of (14) is a union of pairwise disjoint sets.

First suppose $x \in W \setminus S$. Note that $\mathrm{supp}(B_i) = S$. Hence all contributions to $b_{x,i}$ come from A_i. By (14), there is exactly one j such that $x \in V_{i,j} g_i$. Thus $b_{x,i} = \zeta_{i,j}$.

Next, suppose $x \in S \setminus H_i g_i$. As $g_i \in R \subset S$, we have $V_{i,j}g_i \cap S = V_{i,j}g_i \cap Sg_i = (V_{i,j} \cap S)g_i = H_i g_i$ for $j = 0, \dots, p-1$. As $x \notin H_i g_i$, this shows that A_i does not contribute to $b_{x,i}$. Moreover, since $\bigcup_{g \in R} Ug = S$, there is exactly one $g \in R$ with $x \in Ug$. This implies $b_{x,i} = \eta_{i,g}$.

Finally, let $x \in H_i g_i$. Then $x \in V_{i,j}g_i$ for $j = 0, \dots, p-1$ and thus the contribution of A_i to $b_{x,i}$ is $\sum_{j=0}^{p-1} \zeta_{i,j} = 0$ by (12). Furthermore, as $\bigcup_{g \in R} Ug = S$, there is exactly one $g \in R$ with $x \in Ug$. This implies $b_{x,i} = \eta_{i,g}$.

In summary, we have shown

$$b_{x,i} = \begin{cases} \zeta_{i,j} \text{ for some } j & \text{if } x \in W \setminus S, \\ \eta_{i,g} \text{ for some } g \in R & \text{otherwise.} \end{cases}$$

By the definition of h, this shows that $b_{x,i} \in \mathcal{U}(h)$ for all $x \in W$.

By (13), we have

$$X = \sum_{i=0}^{p^{a-1}-1} X_i \alpha^i \beta^{ki} = \sum_{i=0}^{p^{a-1}-1} \sum_{x \in W} b_{x,i} \alpha^i \beta^{ki} x.$$

Since $\beta \in W$ and $1, \alpha, \dots, \alpha^{p^{a-1}-1}$ represent each coset of W in G_a exactly once, the elements $\alpha^i \beta^{ki} x$, $i = 0, \dots, p^{a-1}-1$, $x \in W$, cover each element of G_a exactly once. As $b_{x,i} \in \mathcal{Q}(h)$ for all $x \in W$, this shows that all coefficients of X are in $\mathcal{U}(h)$.

Next, we prove that

$$|\chi(X)|^2 = p^{2a} \text{ for all } \chi \in \widehat{G}. \tag{15}$$

First suppose $\chi \in W^{\perp}$. Then χ is trivial on all $V_{i,j}$'s and on U. Furthermore, we have $\chi(\beta) = \chi(g) = 1$ for all $g \in R$ and $\chi(\alpha)$ is a root of unity of order dividing p^{a-1}. Using (12), we get

$$\begin{aligned} \chi(X) &= \sum_{i=0}^{p^{a-1}-1} \left(\sum_{j=0}^{p-1} \zeta_{i,j} |V_{i,j}| + \sum_{g \in R} \eta_{i,g} |U| \right) \chi(\alpha)^i \\ &= p^a \sum_{i=0}^{p^{a-1}-1} \sum_{j=0}^{p-1} \zeta_{i,j} + p \sum_{i=0}^{p^{a-1}-1} \sum_{g \in R} \eta_{i,g} \chi(\alpha)^i \qquad (16) \\ &= p \sum_{i=0}^{p^{a-1}-1} \sum_{g \in R} \eta_{i,g} \chi(\alpha)^i. \end{aligned}$$

Recall that $Y = \sum_{i=0}^{p^{a-1}-1} \sum_{g \in R} \eta_{i,g} g \alpha^{pi}$ is a BH(G_{a-1}, h) matrix by assumption. As the order of χ divides p^{a-1}, we have $\chi(\alpha) = \zeta_{p^{a-1}}^t$ for some integer t. Let τ be the character of $G_{a-1} = \langle \alpha^p \rangle \times R$ determined by $\tau(\alpha^p) = \zeta_{p^{a-1}}^t$ and $\tau(g) = 1$ for all $g \in R$. Using (16), we get

$$\tau(Y) = \sum_{i=0}^{p^{a-1}-1} \sum_{g \in R} \eta_{i,g} \zeta_{p^{a-1}}^{ti} = \sum_{i=0}^{p^{a-1}-1} \sum_{g \in R} \eta_{i,g} \chi(\alpha)^i = \frac{1}{p} \chi(X). \tag{17}$$

By Result 2.1, we have $|\tau(Y)|^2 = p^{2a-2}$ and hence (15) follows from (17).

Now, suppose that $\chi \in \widehat{G} \setminus W^\perp$. By Result 5.1, we have that χ is trivial on exactly one of the hyperplanes of W, say V. First suppose that $V = V_{i,j}$ for some i, j. Then χ is nontrivial on U since $UV = W$ and $\chi \notin W^\perp$. Hence $\chi(X) = |V_{i,j}| \zeta_{i,j} \chi(g_i \alpha^i \beta^{ki}) = p^a \zeta$, where $\zeta = \zeta_{i,j} \chi(g_i \alpha^i \beta^{ki})$ is a root of unity and thus (15).

Now assume $V \neq V_{i,j}$ for all i, j. Then χ is nontrivial on all $V_{i,j}$'s and thus $\chi(V_{i,j}) = 0$ for all i, j. Moreover, U is contained in V and thus χ is trivial on U. Hence the order of χ divides p^{a-1} and $\chi(\alpha\beta^k)$ is a root of unity of order dividing p^{a-1}. Let τ be the character of G_{a-1} defined by $\tau(\alpha^p) = \chi(\alpha\beta^k)$ and $\tau(g) = \chi(g)$ for all $g \in G$. Then

$$\chi(X) = \sum_{i=0}^{p^{a-1}-1} \sum_{g \in R} \eta_{i,g} |U| \chi(g) \chi(\alpha\beta^k)^i = p \sum_{i=0}^{p^{a-1}-1} \sum_{g \in R} \eta_{i,g} \tau(\alpha^{pi} g) = p\tau(Y).$$

Hence $|\chi(X)|^2 = p^2 |\tau(Y)| = p^{2a}$ by Result 2.1.

In summary, we have shown that all coefficients of X are in $\mathcal{U}(h)$ and that (15) holds. Hence is a $\mathrm{BH}(G_a, h)$ matrix by Result 2.1. □

Note that, by Result 1.3, there are roots of unity $\eta_{i,j}$ satisfying condition (12) $p \in \mathcal{Q}(h)$. Hence Corollary 3.2 and Theorem 5.2 imply the following.

Corollary 5.3. *Suppose that $p \in \mathcal{Q}(h)$. Then there exists a $\mathrm{BH}(G_a, h)$ matrix for all positive integers a.*

6 Construction of Butson Hadamard Matrices over $\mathbb{Z}_{p^2} \times \cdots \times \mathbb{Z}_{p^2}$

We now use Galois rings to construct $\mathrm{BH}(G, h)$ matrices with G of the form $\mathbb{Z}_{p^2} \times \cdots \times \mathbb{Z}_{p^2}$. We first introduce the necessary background on Galois rings. We refer the reader to [19] for background and proofs of the assertions made below.

Let p be a prime, let $\mathbb{F}_p$ denote the finite field of order p, and let d be a positive integer. For $h \in \mathbb{Z}_{p^2}[x]$, let $\bar{h} \in \mathbb{F}_p[x]$ be the polynomial that is obtained by reducing the coefficients of f modulo p. There is a monic polynomial $f \in \mathbb{Z}_{p^2}[x]$ of degree d such that

$\bar{f}$ is a primitive polynomial over $\mathbb{F}_p$ and f divides $x^{p^d} - 1$ in $\mathbb{Z}_{p^2}[x]$. The **Galois ring** of degree d over $\mathbb{Z}_{p^2}$ is defined as

$$\mathrm{GR}(p^2, d) = \mathbb{Z}_{p^2}[x]/(f).$$

Write $R = \mathrm{GR}(p^2, d)$. There is $g \in R$ with $g^{p^d-1} = 1$ and $g^i \neq 1$ for $1 \leq i \leq p^d - 2$. The additive group of R is isomorphic to $(\mathbb{Z}_{p^2})^d$ and the unique maximal ideal of R is $I = pR = \{0, p, pg, \ldots, pg^{p^d-2}\}$. The residue class field $K := \mathrm{GR}(p^2, d)/I = \{\bar{0}, \bar{1}, \bar{g}, \ldots, \bar{g}^{p^d-2}\}$ is a finite field of order p^d. The set $\mathcal{T} = \{0, 1, g, \ldots, g^{p^d-2}\}$ is called a **Teichmüller system**. Note that $\mathcal{T}$ is a complete system of representatives of cosets of I in R. An arbitrary element α of R can be expressed uniquely as $\alpha = \alpha_0 + p\alpha_1$ with $\alpha_0, \alpha_1 \in \mathcal{T}$ and α is a unit of R if and only if $\alpha_0 \neq 0$.

Let R^* be the set of units of R. Then $|R^*| = (p^d - 1)p^d$ and every element of R^* has a unique representation $g^i(1 + p\alpha)$ with $0 \leq i \leq p^d - 2$ and $\alpha \in \mathcal{T}$. As a multiplicative group, R^* is the direct product of $H = \langle g \rangle$ and $U = \{1 + p\alpha : \alpha \in \mathcal{T}\}$. Moreover, we have $H \cong \mathbb{Z}_{p^d-1}$ and $U \cong (\mathbb{Z}_p)^d$.

Define the absolute trace function $\mathrm{Tr} : K \to \mathbb{F}_p$ by

$$\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{d-1}}.$$

for $\alpha \in K$. Let f be any divisor of d and let F be the subfield of K of order p^f. The trace function of K relative to F is denoted by $\mathrm{Tr}_{d,f}$. Note that

$$\mathrm{Tr}_{d,f}(\alpha) = \alpha + \alpha^{p^f} + \cdots + \alpha^{p^{d-f}}.$$

By transitivity of trace, we have $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\mathrm{Tr}_{d,f})(\alpha))$ for all $\alpha \in K$.

We now define the ingredients of our construction. Recall that $H = \langle g \rangle$ is a subgroup of R^* of order $p^d - 1$. The elements of $U = \{1 + p\alpha : \alpha \in \mathcal{T}\}$ form a complete set of representatives of H in R^* and thus we can label the cosets of H in R^* as

$$E_{\bar{0}} = H \text{ and } E_{\bar{g}^i} = (1 + pg^i)H \text{ for } i = 0, \ldots, p^d - 2.$$

Note that $|E_{\bar{g}^i}| = |H| = p^d - 1$ for all i.

Let $f \geq 1$ be a proper divisor of d and let F be the subfield of K of order p^f. As $f < d$, there is $\bar{k} \in K$, $k \neq \bar{0}$, with $\mathrm{Tr}_{d,f}(\bar{k}) = 0$. Moreover,

$$V = \{\bar{x} \in K : \mathrm{Tr}_{d,f}(\bar{k}\bar{x}) = \bar{0}\}.$$

is a $(d/f-1)$-dimensional F-subspace of K. In particular, $|V| = p^{f(d/f-1)} = p^{d-f}$. It is straightforward to verify that, as an identity of subsets of the group R^* (not of group ring elements), we have $E_{\bar{x}} E_{\bar{y}} = E_{\bar{x}+\bar{y}}$ for all $\bar{x}, \bar{y} \in K$. This implies that

$$D = \bigcup_{\bar{x} \in V} E_{\bar{x}}$$

is a subgroup of R^*. Note that $|D| = p^{d-f}(p^d - 1)$. Let $D_0, \ldots, D_{p^f-1}$ be the cosets of D in R^* where $D_0 = D$. The following was proved in [7, p. 183–185].

Result 6.1. *Suppose that χ is an additive character of R.*

1. *If χ is the trivial character, then $\chi(I) = p^d$ and $\chi(D_i) = p^{d-f}(p^d - 1)$.*
2. *If χ has order p, then $\chi(I) = p^d$ and $\chi(D_i) = -p^{d-f}$.*
3. *If χ has order p^2, then $\chi(I) = 0$ and $\chi(D_i) = -p^{d-f}$ or $p^{d-f}(p^f - 1)$. Furthermore, for a fixed character χ of R of order p^2, there is a unique coset D_i such that $\chi(D_i) = p^{d-f}(p^f - 1)$.*

Theorem 6.2. *Let G be the additive group of $\mathrm{GR}(p^2, d)$ and let f be a divisor of d with $1 \le f < d$. Suppose that $\eta, \eta_0, \ldots, \eta_{p^f-1}$ are complex roots of unity such that*

$$\sum_{i=0}^{p^f-1} \eta_i = 0. \tag{18}$$

Then, using the notation introduced above,

$$X = \sum_{i=0}^{p^f-1} \eta_i D_i + \eta I$$

is a $\mathrm{BH}(G, h)$, where h is the least common multiple of the orders of all the η and η_i's

Proof. By definition, the cosets $D_0, \ldots, D_{p^f-1}$ partition R^* and we have G is the disjoint union of I and R^*. Hence all coefficients of X are in $\mathcal{U}(h)$. By Result 2.1, it remains to show that

$$|\chi(X)|^2 = |G| = p^{2d} \text{ for all } \chi \in \widehat{G}. \tag{19}$$

First suppose that the order of χ divides p. Then

$$\chi(X) = \sum_{i=0}^{p^f-1} \eta_i \chi(D_i) + \eta \chi(I) = \chi(D_0) \sum_{i=0}^{p^f-1} \eta_i + p^d \eta = p^d \eta$$

by Result 6.1 and (18). Thus (19) holds.

Now suppose that χ has order p^2. Then, by Result 6.1, there is a unique j with $0 \leq j \leq p^f - 1$, such that $\chi(D_j) = p^{d-f}(p^f - 1)$ and $\chi(D_i) = -p^{d-f}$ for all $i \neq j$. Moreover, we have $\chi(I) = 0$. Hence

$$\chi(X) = p^{d-f}(p^f - 1)\eta_j - \sum_{i \neq j}^{p^f - 1} p^{d-f}\eta_i = p^d\eta_j - p^{f-d}\sum_{i=0}^{p^f-1}\eta_i = p^d\eta_j,$$

by (18) and thus (19) holds. This completes the proof. □

From Result 1.3 and Theorem 6.2 we get the following.

Corollary 6.3. *Let p be a prime and let d, h be positive integers. Suppose there is divisor f of d with $1 \leq f < d$ such that $p^f \in \mathcal{Q}(h)$. Then there exists a $\mathrm{BH}((\mathbb{Z}_{p^2})^d, h)$ matrix.*

7 Folding Construction

It was shown in [13] that certain bijections between nonisomorphic groups preserve character sums (up to multiplication with roots of unity). We now use this idea to extend our constructions of group invariant Butson Hadamard matrices to further abelian p-groups.

As a preparation, we consider a useful property of character values of group ring elements.

Lemma 7.1. *Let p be a prime, let a be a positive integer, and $G = \mathbb{Z}_{p^a} \times H$ where H is an elementary abelian p-group. Let h be a positive integer with $p^2 \nmid h$ and $D \in \mathbb{Z}[\zeta_h][G]$. Let χ be a character of G order p^b, $1 \leq b \leq a$, and let W be the subgroup of $\mathbb{Z}_{p^a}$ of order p^{a-b+1}. Write $D = \sum_{i=0}^{p^{b-1}-1} D_i\alpha^i$ with $D_i \in \mathbb{Z}[\zeta_h][W \times H]$ where α is a generator of $\mathbb{Z}_{p^a}$.*

If $\chi(D) = \mu m$ where μ is a root of unity and m is an integer, then there is a j such that

$$\chi(D) = \chi(D_j\alpha^j) \text{ and } \chi(D_i) = 0 \text{ for all } i \neq j. \tag{20}$$

Proof. Note that $\chi(\alpha)$ is a primitive p^bth root of unity. Hence, without loss of generality, we can assume $\chi(\alpha) = \zeta_{p^b}$. Write $h = p^t k$ with $t \in \{0, 1\}$ and $(p, k) = 1$. As $\chi(D) \in \mathbb{Z}[\zeta_{p^b k}]$, we have $\mu \in \mathbb{Q}(\zeta_{p^b k})$ and thus $\mu = \pm\zeta_{p^b}^u\zeta_k^w$ for some integers u, w. Using the assumptions, we get

$$\sum_{i=0}^{p^{b-1}-1} \chi(D_i)\zeta_{p^b}^i = \sum_{i=0}^{p^{b-1}-1} \chi(D_i)\chi(\alpha)^i = \chi(D) = \mu m = (\pm\zeta_k^w m)\zeta_{p^b}^u. \tag{21}$$

Note that $\chi(D_i) \in \mathbb{Q}(\zeta_{pk})$ for all i, since the order of χ restricted to W is $p^b/(p^a/|W|) = p^{b-a+(a-b+1)} = p$ and H is elementary abelian. As $\pm\zeta_k^w m \in \mathbb{Q}(\zeta_{pk})$ and $\{1, \zeta_{p^b}, \dots, \zeta_{p^b}^{p^{b-1}-1}\}$

is independent over $\mathbb{Q}(\zeta_{pk})$, we conclude from (21) that $\chi(D_i) = 0$ whenever $i \not\equiv u \pmod{p^{b-1}}$. Hence $\chi(D) = \chi(D_j\alpha^i)$ by (21) where j is the unique index with $j \equiv u \ (\bmod\ p^{b-1})$. This completes the proof of (20). □

We now define the non-homomorphic bijections between groups that we will work with. Let p be prime and let a be a positive integer. Let P be an abelian group of order p^a and write $P = \mathbb{Z}_{p^{t_1}} \times \cdots \times \mathbb{Z}_{p^{t_s}}$ where $a = \sum_{i=1}^{s} t_i$ and $\mathbb{Z}_{p^{t_1}} = \langle \alpha_i \rangle$, $i = 1, \ldots, s$. Define a lexicographic order on P by

$$\alpha_1^{x_1} \cdots \alpha_s^{x_s} > \alpha_1^{y_1} \cdots \alpha_s^{y_s} \Leftrightarrow x_j > y_j \text{ for } j = \min\{i : x_i \neq y_i\},$$

where $0 \leq x_i, y_i \leq p^{t_i} - 1$ for all i.

Consider a cyclic group $\mathbb{Z}_{p^a} = \{1, \alpha, \ldots, \alpha^{p^a-1}\}$. For $n = 0, \ldots, p^a - 1$, let $f(\alpha^n)$ be the n^{th} element of P in the lexicographical order. We call the bijection $f : \mathbb{Z}_{p^a} \to P, \alpha^n \mapsto f(\alpha^n)$ a **folding** of $\mathbb{Z}_{p^a}$. For a group H and a folding f of $\mathbb{Z}_{p^a}$, we extend f to a map $\mathbb{Z}_{p^a} \times H \to P \times H$ by to G by $f(gh) = f(g)h$ for all $g \in P$ and $h \in H$ and call this map a **folding** of $\mathbb{Z}_{p^a} \times H$. Foldings are extended to bijections of group rings by linearity, that is, for $X = \sum_{g \in G} a_g g$ with $a_g \in \mathbb{Z}[\zeta_t]$, we set

$$f(X) = \sum_{g \in G} a_g f(g). \tag{22}$$

As above, let $P = \langle \alpha_1 \rangle \times \cdots \times \langle \alpha_s \rangle \cong \mathbb{Z}_{p^{t_1}} \times \cdots \times \mathbb{Z}_{p^{t_s}}$. We say that a subgroup U of P is **left full** if it has the form

$$U = \langle \alpha_1, ..., \alpha_{r-1}, \alpha_r^l \rangle$$

for some l and some $r \in \{1, ..., s\}$. The following is proved in [13, Lem. 4.1, 4.3].

Result 7.2. *Let p be a prime, let a be positive integer, and let α be a generator of $\mathbb{Z}_{p^a}$. Suppose that $f : \mathbb{Z}_{p^a} \times H \to P \times H$ is a folding.*

(a) Let U be a left full subgroup of P and let W be the subgroup of $\mathbb{Z}_{p^a}$ of order $|U|$. Then

$$f(\alpha^i w) = f(\alpha^i) f(w)$$

for $0 \leq i < p^a/|U|$ and all $w \in W$.

(b) Let χ be a character of $P \times H$ which is nontrivial on P and let U be the maximal left full subgroup of P contained in the kernel of χ. Let W be the subgroup of $\mathbb{Z}_{p^a}$ of order $p|U|$. Then there is a character τ of $\mathbb{Z}_{p^a} \times H$ such that

$$\tau(x) = \chi(f(x))$$

for all $x \in W \times H$ and τ has order $p^a/|U|$ when restricted to $\mathbb{Z}_{p^a}$.

Now we are ready to prove the main result of this section. The proof is similar to that of [13, Thm. 4.6], but we include it for the convenience of the reader, as the setting is slightly different.

Theorem 7.3. *Let p be a prime, let a, h be positive integers with $h \not\equiv 0 \pmod{p^2}$, and let $G = \mathbb{Z}_{p^a} \times H$ where H is an elementary abelian group of order p^a. Suppose that there exists a* $\mathrm{BH}(G, h)$ *matrix X such that*

$$\chi(X) = \mu_\chi p^a \text{ for some root of unity } \mu_\chi \text{ for all characters } \chi \text{ of } G. \tag{23}$$

Let P be any abelian p-group of order p^a and let $f : G \to P \times H$ be the corresponding folding. Then $f(X)$ is a $\mathrm{BH}(P \times H, h)$ *matrix.*

Proof. As f is a bijection, the group ring elements of X and $f(X)$ have the same set of coefficients. Hence all coefficients of $f(X)$ are in $\mathcal{Q}(h)$. By Result 2.1, it remains to show

$$|\chi(f(X))|^2 = |P \times H| \tag{24}$$

for all characters χ of $P \times H$.

First assume that χ is trivial on P. Define the character τ of G by $\tau(g) = 1$ for $g \in \mathbb{Z}_{p^a}$ and $\tau(h) = \chi(h)$ for all $h \in H$. Then $\chi(f(X)) = \tau(X)$ and (24) holds, since $|\tau(X)|^2 = |G|$ by Result 2.1 and $|G| = |P \times H|$.

Now suppose that χ is nontrivial on P. Let U be the maximal left full subgroup of P contained in the kernel of χ. Note that $|U| < p^a$, since χ is nontrivial on P. Let W be the subgroup of $\mathbb{Z}_{p^a}$ of order $p|U|$. By Result 7.2 (b), there is a character τ of G such that

$$\tau(x) = \chi(f(x)) \text{ for all } x \in W \times H \tag{25}$$

and τ has order $p^a/|U|$ when restricted to $\mathbb{Z}_{p^a}$. Let Y be any element of $\mathbb{Z}[\zeta_h][W \times H]$ and write $Y = \sum_{x \in W \times H} a_x x$ with $a_x \in \mathbb{Z}[\zeta_h]$. Using (22) and (25), we get

$$\chi(f(Y)) = \sum_{x \in W \times H} a_x \chi(f(x)) = \sum_{x \in W \times H} a_x \tau(x) = \tau(Y). \tag{26}$$

Write $p^a/|U| = p^b$ and let α be a generator of $\mathbb{Z}_{p^a}$. As $p^a/|W| = p^{b-1}$, we can write $X = \sum_{i=0}^{p^{b-1}-1} X_i \alpha^i$ with $X_i \in \mathbb{Z}[\zeta_h][W \times H]$ for all i. Note that

$$\chi(f(X_i)) = \tau(X_i) \tag{27}$$

for all i by (26). Moreover, by (23) and Lemma 7.1, there is a j such that

$$\tau(X) = \tau(X_j \alpha^j) \text{ and } \tau(X_i) = 0 \text{ for all } j \neq i. \tag{28}$$

Fix i with $0 \leq i \leq p^{b-1}-1$ and write $X_i = \sum_{w\in W}\sum_{k\in H} a_{w,k}wk$ with $a_{w,k} \in \mathbb{Z}[\zeta_h]$. Recall that $f(gk) = f(g)k$ for all $g \in \mathbb{Z}_{p^a}$ and $k \in H$, as the restriction of f to H is the identity map. By Result 7.2 (a), we have $f(\alpha^i w) = f(\alpha^i)f(w)$ for all $w \in W$ and thus

$$\begin{aligned} f(X_i\alpha^i) &= \sum_{w\in W}\sum_{k\in H} a_{w,k} f(wk\alpha^i) = \sum_{w\in W}\sum_{k\in H} a_{w,k} f(w\alpha^i)k \\ &= \sum_{w\in W}\sum_{k\in H} a_{w,k} f(w)f(\alpha^i)k = \left(\sum_{w\in W}\sum_{k\in H} a_{w,k} f(wk)\right) f(\alpha^i) \\ &= f(X_i)f(\alpha^i). \end{aligned} \tag{29}$$

Using (27), (28), and (29), we compute

$$\begin{aligned} \chi(f(X)) &= \chi\left(\sum_{i=0}^{p^{b-1}-1} f(X_i\alpha^i)\right) = \chi\left(\sum_{i=0}^{p^{b-1}-1} f(X_i)f(\alpha^i)\right) = \sum_{i=0}^{p^{b-1}-1} \chi(f(X_i))\chi(f(\alpha^i)) \\ &= \sum_{i=0}^{p^{b-1}-1} \tau(X_i)\chi(f(\alpha^i)) = \tau(X_j)\chi(f(\alpha^j)) = \tau(X)\chi(f(\alpha^j))\tau(\alpha^{-j}). \end{aligned}$$

We have $|\tau(X)|^2 = |G| = |P \times H|$ by Result 2.1 and $\chi(f(\alpha^j))\tau(\alpha^{-j})$ is a root of unity. This completes the proof of (24). □

Corollary 7.4. *Let p be a prime and let a, h be positive integers with $p \in \mathcal{Q}(h)$. Then* $\mathrm{BH}\left(P \times \mathbb{Z}_p^a, h\right)$ *matrix exists for every abelian group P of order p^a.*

Proof. By Corollary 5.3 there is a $\mathrm{BH}(\mathbb{Z}_{p^a} \times (\mathbb{Z}_p)^a, h)$ matrix. The proof of Theorem 5.2 shows that this matrix satisfies condition (23). Hence there is a $\mathrm{BH}\left(P \times \mathbb{Z}_p^a, h\right)$ matrix by Theorem 7.3. □

A Appendix: Proof of Theorem 2.3

Part (a) of Theorem 2.3 is just Result 1.3. To prove part (b), we first show the sufficiency of each of the conditions (i)-(iii).

Assume that (i) holds, that is, h is even and $m+1 \in \mathcal{Q}(h)$. By part (a), there are $\eta_1, \ldots, \eta_{m+1} \in \mathcal{U}(h)$ with $\sum_{i=1}^{m+1} \eta_i = 0$. Thus $\sum_{i=1}^{m}(-\overline{\eta_{m+1}}\eta_i) = 1$ and this shows that (4) has solution.

Suppose that (ii) holds, that is, h is odd and $m-1 \in \mathcal{Q}(h)$. By part (a), there are $\eta_1, \ldots, \eta_{m-1} \in \mathcal{U}(h)$ with $\sum_{i=1}^{m-1} \eta_i = 0$. Setting $\eta_m = 1$ thus gives a solution of (4).

Now suppose that (iii) holds. Then

$$(\zeta_{q_1} + \cdots + \zeta_{q_1}^{q_1-1})(\zeta_{q_2} + \cdots + \zeta_{q_2}^{q_2-1}) = (-1)(-1) = 1 \tag{30}$$

gives a solution of (4), since the number of roots of unity obtained by expanding the left hand side of (30) is $(q_1-1)(q_2-1)=m$. In summary, we have shown the sufficiency of conditions (i)-(iii).

To prove necessity, assume that (4) holds. Note that (4) can be written in the form

$$\sum_{i=1}^{m+1} \eta_i = 0 \text{ with } \eta_{m+1} = -1. \tag{31}$$

First assume that h is even. Then $\eta_{m+1} = -1 \in \mathcal{U}(h)$ and thus $m+1 \in \mathcal{Q}(h)$ by (31) and part (a). Hence condition (i) of Theorem 2.3 is satisfied.

Hence we can assume that h is odd. Suppose that condition (ii) of Theorem 2.3 does not hold, that is,

$$m-1 \notin \mathcal{Q}(h). \tag{32}$$

To complete the proof, we have to show that condition (iii) of Theorem 2.3 holds.

We need to employ results from [17] and thus need some preparations. Let $G = \langle g \rangle$ be a cyclic group of order h and let $\rho : \mathbb{Z}[G] \to \mathbb{Z}[\zeta_h]$ be the homomorphism determined by $\rho(g) = \zeta_h$. Let $q_1, \ldots, q_t$ be the distinct prime divisors of h and let Q_i be the subgroup of order q_i of G, $i = 1, \ldots, t$. By [17, Thm. 2.2], we have

$$\ker(\rho) = \left\{ \sum_{i=1}^{t} X_i Q_i : X_i \in \mathbb{Z}[G] \right\}. \tag{33}$$

First suppose that h is a prime power, say $h = q^b$ where q is a prime. Note that, in this case, the kernel of ρ is $\{XQ : X \in \mathbb{Z}[G]\}$ where $Q = 1 + g^{q^{b-1}} + \cdots + g^{(q-1)q^{b-1}}$. As $\eta_i \in \mathcal{U}(h)$ for all i by assumption, we can write $\eta_i = \zeta_h^{a_i}$ with $a_i \in \mathbb{Z}$. We have

$$\rho\left(-1 + \sum_{i=1}^{m} g^{a_i}\right) = -1 + \sum_{i=1}^{m} \zeta_h^{a_i} = -1 + \sum_{i=1}^{m} \eta_i = 0$$

by (31) and thus

$$-1 + \sum_{i=1}^{m} g^{a_i} = QH \tag{34}$$

for some $X \in \mathbb{Z}[G]$. Applying the trivial character of G to (34), we get $m-1 \equiv 0 \pmod{q}$. But this contradicts (32).

Hence we can assume that h has at least two distinct prime divisors. Let q_1, q_2, $q_1 < q_2$, be the two smallest prime divisors of h. If $m-1 \geq (q_1-1)(q_2-1)$, then $m-1 \in \mathcal{Q}(h)$ by [17, Lem. 5.1], contradicting (32). Thus we have

$$m \leq (q_1-1)(q_2-1). \tag{35}$$

The proof is done if we can show that $m \geq (q_1-1)(q_2-1)$. Set

$$\mathbb{Z}_{\geq 0}[G] = \left\{ \sum_{g \in G} a_g g \in \mathbb{Z}[G] : a_g \geq 0 \text{ for all } g \in G \right\}.$$

Consider $Y = \sum_{i=1}^{q_1-1} g^{(h/q_1)i} + \sum_{i=1}^{m} g^{a_i}$. Observe that $Y \in \mathbb{Z}_{\geq 0}[G]$ and

$$\rho(Y) = \sum_{i=1}^{q_1-1} \zeta_{q_1}^i + \sum_{i=1}^{m} \zeta_h^{a_i} = -1 + \sum_{i=1}^{m} \eta_i = 0$$

by (31). Thus $Y \in \mathbb{Z}_{\geq 0}[G] \cap \ker(\rho)$. We claim that, in fact,

$$\sum_{i=1}^{q_1-1} g^{(h/q_1)i} + \sum_{i=1}^{m} g^{a_i} = Y = \sum_{j=1}^{t} Y_j Q_j \text{ for some } Y_j \in \mathbb{Z}_{\geq 0}[G]. \tag{36}$$

If h has only two distinct prime divisors, then (36) follows directly from [17, Thm. 3.3]. Thus assume that h has at least three distinct prime divisors, say $q_1 < q_2 < q_3$. Using (35) and the assumption that q_1 and q_2 are the smallest prime divisors of h, we conclude

$$m - 1 + q_1 \leq (q_1-1)(q_2-1) - 1 + q_1 = q_1q_2 - q_2 < q_1q_2 - q_1 - q_2 + q_3.$$

By [17, Cor. 4.9], this implies (36). Hence (36) holds in all cases.

If $g^{a_j} = 1$ for some j, then

$$\rho\left(\sum_{\substack{i=1 \\ i \neq j}}^{m} g^{a_i}\right) = \rho(Y) - \rho\left(\sum_{i=0}^{q_1-1} g^{(h/q_1)i}\right) = 0 - \sum_{i=0}^{q_1-1} \zeta_{q_1}^i = 0.$$

Using part (a), we conclude that $m-1 \in \mathcal{Q}(h)$, which contradicts (32). Hence we have

$$g^{a_i} \neq 1 \text{ for all } i. \tag{37}$$

By (36) and (37), the support of Y_1Q_1 does not contain 1. Thus, by (36), for each $i \in \{1, \ldots, q_1-1\}$, there is $j(i) \geq 2$ such that $g^{i(h/q_1)}Q_{j(i)} \subset \operatorname{supp}(Y)$. Note that the cosets $g^{i(h/q_1)}Q_{j(i)}$, $i = 1, \ldots, q_1-1$ are pairwise disjoint, since $j(i) \neq 1$ for all i and $g^{i(h/q_1)} \in Q_1$. Hence, by (37),

$$|\operatorname{supp}(Y)| \geq \sum_{i=1}^{q_1-1} \left|g^{i(h/q_1)}Q_{j(i)}\right| \geq (q_1-1)|Q_2| = (q_1-1)q_2.$$

On the other hand, by the definition of Y, we have $|\operatorname{supp}(Y)| \leq q_1 - 1 + m$. We conclude $m \geq (q_1-1)q_2 - (q_1-1) = (q_1-1)(q_2-1)$ and this completes the proof. □

References

[1] J. André: Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe. *Math. Z.* **60** (1954), 156–186.

[2] J. Backelin: Square Multiples n Give Infinite Many Cyclic n-roots. *Reports, Matematiska Institutionen, Stockholms Universitet*, **8** (1989), 1–2.

[3] T. Beth, D. Jungnickel, H. Lenz: *Design Theory* (2nd edition). Cambridge University Press 1999.

[4] Z. I. Borevich, I. R. Shafarevich: *Number Theory.* Academic Press 1966.

[5] B. W. Brock: Hermitian congruence and the existence and completion of generalized Hadamard matrices. *J. Combin. Theory A* **49** (1988), 233–261.

[6] J. H. Conway and A. J. Jones: Trigonometric Diophantine equations (On vanishing sums of roots of unity). *Acta Arith.* **30** (1976), 229–240.

[7] Y. Q. Chen, D. K. Ray-Chaudhuri, Q. Xiang: Constructions of partial difference sets and relative difference sets using Galois rings. II. *J. Combin. Theory A* **76** (1996), 179–196.

[8] J. A. Davis: Difference sets in abelian 2-groups. *J. Combin. Theory A* **57** (1991), 262–286.

[9] J. A. Davis: Construction of relative difference sets in p-groups. *Discrete Math.* **103** (1992), 7–15.

[10] J. A. Davis, J. Jewab: A unifying construction for difference sets. *J. Combin. Theory A* **80** (1997), 13–78.

[11] T. D. Duc: Necessary Conditions for the Existence of Group-Invariant Butson Hadamard Matrices and a New Family of Perfect Arrays. Submitted.

[12] T. D. Duc, B. Schmidt: Bilinear Forms on Finite Abelian Groups and Group-Invariant Butson Matrices. *J. Combin. Theory A* **166** (2019), 337–351.

[13] M. Hagita, B. Schmidt: Bijections between group rings preserving character sums. *Des. Codes Cryptogr.* **24** (2001), 243–254.

[14] G. Hiranandani, J. M. Schlenker: Small circulant complex Hadamard matrices of Butson type. *Eur. J. Com.* **51** (2016), 306–314.

[15] R. G. Kraemer: Proof of a conjecture on Hadamard 2-groups. *J. Combin. Theory A* **63** (1993), 1–10.

[16] P. H. J. Lampio, P. Östergård, F. Szöllősi: Orderly generation of Butson Hadamard matrices. Preprint. `arXiv:1707.02287`.

[17] T. Y. Lam, K. H. Leung: On vanishing sums of roots of unity. *J. Algebra* **224** (2000), 91–109.

[18] H. Lüneburg: *Translation Planes.* Springer 1980.

[19] B. R. McDonald: *Finite rings with identity.* Pure and Applied Mathematics **28**. Marcel Dekker 1974.

[20] S. L. Ma and A. Pott: Relative difference sets, planar functions, and generalized Hadamard matrices. *J. Algebra* **175** (1995), 505–525.

[21] B. Schmidt: A Survey of Group Invariant Butson Matrices and Their Relation to Generalized Bent Functions and Various Other Objects. *Radon Series on Computational and Applied Mathematics* **23** (2019), 241–251.

[22] F. Szöllősi: *Construction, classification and parametrization of complex Hadamard matrices.* Ph.D. Thesis. `arXiv:1110.5590`.

[23] R. J. Turyn: Character sums and difference sets. *Pacific J. Math.* **15** (1965), 319–346.