Construction and classification of group invariant Butson Hadamard matrices

Wong, Dai Quan

2020

Wong, D. Q. (2020). Construction and classification of group invariant Butson Hadamard matrices. Doctoral thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/145710>

<https://doi.org/10.32657/10356/145710>

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0
International License (CC BY-NC 4.0).

Downloaded on 26 Apr 2023 19:19:22 SGT

**NANYANG
TECHNOLOGICAL
UNIVERSITY**

SINGAPORE

**CONSTRUCTION AND CLASSIFICATION OF GROUP
INVARIANT BUTSON HADAMARD MATRICES**

WONG DAI QUAN

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES

2020

**CONSTRUCTION AND CLASSIFICATION OF GROUP
INVARIANT BUTSON HADAMARD MATRICES**

WONG DAI QUAN

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES

A thesis submitted to the Nanyang Technological
University in partial fulfilment of the requirement for the
degree of Doctor of Philosophy

2020

Statement of Originality

I hereby certify that the work embodied in this thesis is the result of original research done by me except where otherwise stated in this thesis. The thesis work has not been submitted for a degree or professional qualification to any other university or institution. I declare that this thesis is written by myself and is free of plagiarism and of sufficient grammatical clarity to be examined. I confirm that the investigations were conducted in accord with the ethics policies and integrity standards of Nanyang Technological University and that the research data are presented honestly and without prejudice.

30/6/2020

.....
Date

.....
Wong Dai Quan

Schmidt

Supervisor Declaration Statement

I have reviewed the content and presentation style of this thesis and declare it of sufficient grammatical clarity to be examined. To the best of my knowledge, the thesis is free of plagiarism and the research and writing are those of the candidate's except as acknowledged in the Author Attribution Statement. I confirm that the investigations were conducted in accord with the ethics policies and integrity standards of Nanyang Technological University and that the research data are presented honestly and without prejudice.

30/6/2020

.....
Date

Schmidt

.....
Bernhard Schmidt

Authorship Attribution Statement

This thesis contains material from 2 papers, one of which is currently submitted to a peer-reviewed journal in which I am listed as an author. The other paper is a preprint

Chapter 2 is submitted as B. Schmidt, D. Q. Wong, Q. Xiang: Constructions of Butson Hadamard Matrices Invariant Under Abelian p -Groups. *Journal of Combinatorial Theory Series A*. Submitted

The contributions of the co-authors are as follows:

- Prof. Schmidt provided the initial project direction with the construction of group invariant Butson Hadamard matrices by using translation planes, Theorem 3.1.
- We expanded upon his ideas which resulted in the nested cyclic subgroups construction, recursive hyperplane construction, Theorems 4.2 and 5.2. I proved the correctness of the constructions.
- Prof. Xiang gave the construction of group invariant Butson Hadamard matrices using Galois Rings, Theorem 6.2.
- I discovered that the folding theorem can be applied to our construction to obtain more group invariant Butson Hadamard matrices. Prof. Bernhard refined the idea which resulted in the folding construction, Theorem 7.3.
- The necessary conditions on the sum of roots of unity, Theorem 2.3, were first formulated by Prof. Schmidt. Together we proved the result.
- I prepared the manuscript drafts. The manuscript was revised and edited by Prof Schmidt and reviewed by Prof Xiang.

Chapters 3 and 4 are submitted as B. Schmidt, D. Q. Wong: An Exponent Bound and the Classification of Butson Hadamard Matrices Invariant Under $\mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$. *Preprint*.

The contributions of the co-authors are as follows:

- Prof. Schmidt provided the initial project direction with the classification of Butson Hadamard Matrices Invariant Under $\mathbb{Z}_p \times \mathbb{Z}_p$. I completed the missing part of his proofs.
- Prof. Schmidt proposed the exponent bound which I refined and proved the result.
- We expanded upon the classification of Butson Hadamard Matrices under $\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p$. The intermediate results were obtained by Prof. Schmidt from which I finished the analysis and completed the classification.

30/6/2020

.....
Date

.....
Wong Dai Quan

Abstract

The purpose of this dissertation is to introduce the reader to the study of group-invariant Butson Hadamard matrices and to present our contribution in this area. Our focus is on abelian p -groups since one can obtain group-invariant Butson Hadamard matrices for larger abelian groups by using Kronecker products. The main areas of study we have identified are:

- The existence and the construction of group-invariant Butson Hadamard matrices
- The non-existence and the necessary conditions for their existence
- The classification of group-invariant Butson Hadamard matrices

Our contribution to this study is the outline of five types of constructions of group-invariant Butson Hadamard matrices, a new necessary condition for existence under the self-conjugacy assumption and the classification of Butson Hadamard matrices which are invariant under the groups $\mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p$.

Acknowledgements

I am greatly indebted to my supervisor, Professor Bernhard Schmidt, for taking me under his wing and for his continued support throughout my Ph.D programme. His invaluable insight into our research was always thought provoking and often encouraged more creative thinking on my part. I am fortunate to have had the opportunity to learn from him and doing research with him.

I would like to extend my thanks to Samuel Teo, a senior I met during my freshmen year. Knowing my interest in mathematics, he often engaged me in discussion to broaden my perspective on the subject. His enthusiasm for mathematics is contagious and has ignited my own passion in the field, for which I am very thankful for.

Lastly, I am grateful to Nanyang Technological University for supporting my Ph.D financially through the Graduate Research Officer Scheme.

Contents

Abstract	i
Acknowledgements	iii
Introduction	1
1 Preliminaries	7
1.1 Group-Invariant Butson Hadamard matrices	7
1.2 Group Rings and Characters	10
1.2.1 Group Rings	11
1.2.2 Characters of Finite Abelian Groups	12
1.3 Number Theoretic Tools	13
1.3.1 Vanishing Sums of Roots of Unity	14
2 Constructions	21
2.1 Constructions Using Subgroups	23
2.1.1 Spread Construction	24
2.1.2 Nested Cyclic Subgroups Construction	30
2.1.3 Recursive Subspace Construction	37
2.2 Constructions using Folding and Permutation Theorems	45
2.2.1 Folding Theorem	45
2.2.2 Permutation Theorem	50
2.3 Galois Ring Construction	53
2.3.1 Galois Rings over $\mathbb{Z}_{p^2}$	54

2.3.2	Construction using Galois Rings $\text{GR}(p^2, a)$	55
2.4	Summary of Results	58
3	Necessary Conditions	61
3.1	Ma's Lemma	61
3.2	Exponent Bound	65
4	Classification	67
4.1	Classification of $\text{BH}(\mathbb{Z}_p \times \mathbb{Z}_p, h)$ Matrices	67
4.2	Classification of $\text{BH}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p, h)$ Matrices	73
4.2.1	Setup	73
4.2.2	Structure of Putative $\text{BH}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p, h)$ Matrices	76
5	Conclusion and Future Work	97

Introduction

This thesis is based on our contribution to the study of group-invariant Butson Hadamard matrices. We will be focused on the existence and non-existence problem of these objects. Along the way, we will also explore the necessary conditions for their existence and classify some of these matrices. All new results are joint work with Bernhard Schmidt, Qing Xiang, and Du Doc Tai. All previously known results are labeled as “**Result**”.

A Butson Hadamard matrix (or simply a Butson matrix) H of order n is a $n \times n$ matrix whose entries are complex roots of unity such that $HH^* = nI_n$, where H^* denotes the conjugate transpose of H and I_n denotes the identity matrix of order n . Specifically, a Hadamard matrix is a $n \times n$ matrix with entries ± 1 which satisfies $HH^T = nI$, where H^T is the transpose of H . We denote the set of all Butson Hadamard matrices of order n with h^{th} roots of unity by $BH(n, h)$ and we often refer to matrices in this set as a $BH(n, h)$ matrix. Note that Hadamard matrices are just $BH(n, 2)$ matrices. Observe that for any multiple k of h , a $BH(n, h)$ matrix is also a $BH(n, k)$ matrix since an h^{th} root of unity is also a k^{th} roots of unity.

The simplest examples of Butson Hadamard matrices which are not Hadamard matrices are the Fourier matrices, given by $F_n = (f_{i,j})_{0 \leq i,j \leq n-1}$ where $f_{i,j} = \zeta_n^{ij}$ and ζ_n is a primitive n th root of unity.

There are many combinatorial objects which are closely related to Butson Hadamard matrices [53] and the similarity between them is that they can be described in terms of group rings. For example, a subset R of k elements of a group G of order mn is difference set relative to a normal subgroup N if the collection of differences, $r - s$, $r, s \in R$, $r \neq s$, contains only the elements of $G \setminus N$ exactly λ times. The set R is also called a (m, n, k, λ) -relative difference set (or RDS for short). In particular, the connection between RDS and

Butson Hadamard matrices has been studied in [5]. Furthermore, given a $(m, n, m, m/n)$ -relative difference set, we can construct $BH(m, e)$ matrices, where $e = \exp(N)$ is the exponent of N [53, Proposition 2.7]. As these objects have been thoroughly researched throughout the years, the numerous available methods and results in the literature can be adapted to our needs for our study of Butson Hadamard matrices. Additionally, as sums of roots of unity are often a focus when considering Butson Hadamard matrices, results in number theory, such as those from [41], are also integral in our investigation of these matrices. In Chapter 1, we give a brief overview of Butson Hadamard matrices and outline the algebraic and number-theoretic tools which are needed.

One of the major open problems in combinatorics is the ‘‘Hadamard Matrix Conjecture’’ which posits that Hadamard matrices of order $4t$ for all positive integers t . Viewing Hadamard matrices from a general perspective, Butson [4] introduced the concept of Butson Hadamard matrices to understand the problem in a broader setting. In the new realm of Butson Hadamard matrices, it is then natural to ask for which pairs of n, h do $BH(n, h)$ matrices exist. One of the many ways one might construct a matrix is to start with a single row vector and use permutations of it for the other rows. In our study, we consider permutations which are generated by the action of group elements of G on itself where the matrix is indexed by group elements in G , that is matrices which are group-invariant, or G -invariant. More specifically, a square matrix A with its rows and columns indexed by group elements of G , that is $A = (a_{g,k})_{g,k \in G}$, is G -invariant if $a_{gl,kl} = a_{g,k}$ for all $g, k, l \in G$. Note that circulant matrices are simply matrices which are invariant under a cyclic group. For a Butson Hadamard matrix, we use $BH(G, h)$ to denote G -invariant $BH(|G|, h)$ matrices. Much of the research on the topic is devoted to the question of existence and non-existence of $BH(np, p^a)$ matrices [8, 18, 28, 39, 40] or $BH(n, h)$ matrices, where h is a product of a small number of primes [9, 16, 20, 25].

Many group-invariant Butson Hadamard matrices have been shown to exist. Let $\mathbb{Z}_n$ denote the cyclic group of order n . Rothaus [51, 52] showed that $BH(\mathbb{Z}_2^m, 2)$ matrices exist if and only if m is even, and K.U. Schmidt [54] constructed $BH(\mathbb{Z}_2^m, 4)$ matrices for all positive m . Jungnickel [29] proved the existence of $BH(\mathbb{Z}_p^m, p)$ matrices for odd primes p and all positive m . Kumar, Scholtz, and Welch [36] extended the result by showing that $BH(\mathbb{Z}_q^m, q)$ matrices exist whenever m is even or $q \not\equiv 2 \pmod{4}$. For circulant matrices,

Backelin [2] proved the existence of $\text{BH}(\mathbb{Z}_n, n/r)$ matrices where $n \not\equiv 2 \pmod{4}$ and r^2 divides n . More recently, Duc and Schmidt [18] constructed $\text{BH}(G, h)$ matrices where $v_p(h) \geq \lceil v_p(\exp(G))/2 \rceil$ for all prime divisors p of $|G|$ and $v_2(h) \geq 2$ if $v_2(G)$ is odd and G has a direct factor $\mathbb{Z}_2$ using bilinear forms on finite abelian groups, where $v_p(x)$ is the p -adic valuation of x and $\exp(G)$ is the exponent of G . Also, Duc [17] constructed $\text{BH}(G, h)$ matrices for (possibly non-abelian) groups G containing $\mathbb{Z}_h$ or $\mathbb{Z}_{h/2}$ where h^2 divides n and $v_2(h), v_2(n)$ are not both 1. In that same paper, he also constructed $\text{BH}(\mathbb{Z}_{p^{a+1}}^{2e} \times \mathbb{Z}_{p^a}^{2f}, h)$ matrices, where a, e, f are nonnegative integers with $f \geq 1$, using finite local rings. We note that in all the constructions but the last, the integers h and $|G|$ always share a common divisor. In contrast, the constructions we present in Chapter 2 of this dissertation all produce $\text{BH}(G, h)$ matrices where $|G|$ is coprime to h .

We outline our strategy for construction at this point. In [15], Davis and Jedwab formalized the concept of a *building set* which they discovered was the central idea, in particular, behind the construction of many relative difference sets. When described in terms of group rings, RDSs are subsets of a group G which takes on specific character values depending on the character and parameters. Davis and Jedwab showed that the computation of the character values can be simplified by carefully taking a collection of “building blocks” with some properties. More specifically, a building block of modulus m is a subset of G such that its character values are 0 or m for all nontrivial characters of G . Then a building set relative to a subgroup U of G is a collection of building blocks such that for all nontrivial characters χ of G , exactly one of them has a nonzero character value if χ is nontrivial on U , and all the blocks have character values of 0 otherwise. The RDSs are then constructed as unions of translates of these building blocks. We take inspiration from their approach and construct Butson Hadamard matrices in a similar way. Our building blocks in most cases are simply certain subgroups of G , which automatically have the building blocks property due to the orthogonality relations for characters. Next, a group ring element is constructed from these subgroups by assigning roots of unity as coefficients to the chosen subgroups and taking the sum of all of them. However, there are several key differences to the approach of Davis and Jedwab here. The first is that the subgroups chosen must cover the whole group and the second is that the coefficients are selected such that the conditions placed upon them by the definition of

Butson Hadamard matrices are satisfied.

We now discuss necessary conditions for the existence of Butson Hadamard matrices. It is a well-known fact [50] that a Hadamard matrix must necessarily be of order 1, 2 or $4t$ for some positive integer t . There is an analogous result for Butson Hadamard matrices. Winterhoff [59] showed that if p is prime, then a $BH(n, p^a)$ matrix can only exist if n is divisible by p . For group-invariant Hadamard matrices, Davis [13], Kraemer [35] and Turyn [58] proved that for an abelian 2-group G of order 2^{2a} , a $BH(G, 2)$ matrix exists if and only if the exponent of G is at most 2^{a+1} . On the other hand, Brock [7] and Winterhoff [59] showed that if p does not divide h , $p^j \equiv -1 \pmod{h}$ for some integer j , and G is an abelian p -group of order p^a with a odd, then $BH(G, h)$ matrices does not exist. As an extension of the non-existence result of Brock and Winterhoff, we prove in Chapter 3, under the first two assumptions (which we call the self-conjugacy assumption), that the exponent of an abelian group of order p^{2a} must be at most p^a if a $BH(G, h)$ matrix exists.

If H is a $BH(n, h)$ matrix, then any matrix which is obtained from H by row or column permutations is also a $BH(n, h)$ matrix. Furthermore if ζ is a root of unity, then ζH is also a $BH(n, h)$ matrix. Hence, we will call two Butson Hadamard matrices equivalent if they can be obtained from each other by row or column permutations or by a scalar multiple of a root of unity. Sylvester [55] asserted (without proof) in 1867 that if p is prime and a $BH(p, h)$ matrix exists, then the matrix must be equivalent to the Fourier matrix (and consequently p divides h). In the case that n is composite, he (falsely) believed that the number of equivalence classes of $BH(n, h)$ matrices is equal to the number of ways which n can be factored. However, Hadamard [22] showed that this assertion is false for composite integers n . The problem of characterizing $BH(n, h)$ matrices up to equivalence has since been a question worthy of investigation for several authors. Hadamard matrices have been classified for orders up to 32 by Hall [24], Kimura [33, 34], Kharaghani and Tayfeh-Rezaie [30, 31] while Topalova [57] classified Hadamard matrices of order 44 with automorphisms of order 7. Craigen [11] classified Butson Hadamard matrices of orders $n \leq 4$ with Haagerup [21] classifying them for $n = 5$. Meanwhile, Hirasaka, Kim and Mizoguchi [26] showed the uniqueness of $BH(p, p)$ for primes p up to 17. Lampio, Östergård, Szöllősi enumerated Butson Hadamard matrices

for small n , h and classified $\text{BH}(21, 3)$, $\text{BH}(14, 6)$ matrices and also $\text{BH}(n, 4)$ matrices for $n \leq 16$ [37, 38]. For a different type of Butson Hadamard matrices, Egan, Flannery and O Cathain [19] classified cocyclic $\text{BH}(n, p)$ matrices for odd primes p and $np < 100$. Denote the cyclic group of order n by $\mathbb{Z}_n$. Hiranandani and Schlenker [25] proved that for every prime p , all matrices in $\text{BH}(\mathbb{Z}_p, p)$ are equivalent to the Fourier matrix of order p . In Chapter 4, we classify $\text{BH}(\mathbb{Z}_p \times \mathbb{Z}_p, h)$ and $\text{BH}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p, h)$ matrices under the assumption that p , h are co-prime and p is self-conjugate modulo h .

Chapter 1

Preliminaries

1.1 Group-Invariant Butson Hadamard matrices

A **Butson Hadamard matrix** of order n is a matrix is a $n \times n$ matrix H whose entries are complex roots of unity and

$$HH^* = nI,$$

where H^* is the complex conjugate of H and I denotes the identity matrix. The set of all Butson Hadamard matrix of order n whose entries are h^{th} roots of unity is denoted by **BH**(n, h) and the matrices in this set as often referred to as **BH**(n, h) **matrices**.

Example 1.1. It is straightforward to check that

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}$$

is are BH(2,2) and BH(4,2) matrices. In fact, any Hadamard matrix of order n is a BH($n, 2$) matrix. For a non-trivial example, consider the Fourier matrices, given by

$F_n = (f_{i,j})_{0 \leq i,j \leq n-1}$ where $f_{i,j} = \zeta_n^{ij}$ and ζ_n is a primitive n th root of unity:

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta & \zeta^2 & \cdots & \zeta^{n-1} \\ 1 & \zeta^2 & \zeta^4 & \cdots & \zeta^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{n-1} & \zeta^{2(n-1)} & \cdots & \zeta^{(n-1)^2} \end{bmatrix}.$$

We compute

$$[F_n F_n^*]_{i,j} = \sum_{k=0}^{n-1} f_{i,k} \overline{f_{k,j}} = \sum_{k=0}^{n-1} \zeta_n^{ik} \zeta_n^{-jk} = \sum_{k=0}^{n-1} \zeta_n^{(i-j)k}.$$

If $i = j$, then the roots of unity in the sum are just 1's and so it evaluates to n . Otherwise, it is the sum of n distinct n^{th} roots, which evaluates to 0. Therefore $F_n F_n^* = nI$ and so F_n is a $\text{BH}(n, n)$ matrix for each integer n .

We remark that if k is a multiple of h , then a $\text{BH}(n, h)$ matrix is also a $\text{BH}(n, k)$ matrix since an h^{th} root of unity is also a k^{th} root of unity. Thus, for a given n , we aim to construct $\text{BH}(n, h)$ matrices such that h has few prime divisors as possible. In particular, the case where n and h are coprime is of special interest, and this is exactly the case for which the constructions in this thesis provide the main contribution.

Let G be an abelian group of order n which is written multiplicatively. An $n \times n$ matrix $A = (a_{g,k})_{g,k \in G}$, indexed by the 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 $\text{BH}(n, h)$ matrix is also denoted by **$\text{BH}(G, h)$ matrix**. Denote the cyclic group of order n by $\mathbb{Z}_n$. Note that a $\text{BH}(\mathbb{Z}_n, h)$ matrix is the same as a circulant $\text{BH}(n, h)$ matrix.

Example 1.2. In this example, we let the group G be written additively instead. The matrix

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

is not $\mathbb{Z}_2$ -invariant since $-1 = a_{1,1} = a_{0+1,0+1} \neq a_{0,0} = 1$. On the other hand, one can

easily check that the matrix

$$\begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}$$

is $\mathbb{Z}_4$ -invariant and thus is a $\text{BH}(\mathbb{Z}_4, 2)$ matrix.

An easy way to construct new Butson Hadamard matrices from smaller ones is to use their Kronecker product.

Definition 1.3. If $M = (m_{i,j})$ is a $m \times p$ matrix and $N = (n_{i,j})$ is an $n \times q$ matrix, then the Kronecker product of M and N , denoted by $M \otimes N$, is the $mn \times pq$ block matrix given by

$$M \otimes N = \begin{pmatrix} m_{1,1}N & m_{1,2}N & \cdots & m_{1,p}N \\ m_{2,1}N & m_{2,2}N & \cdots & m_{2,p}N \\ \vdots & \vdots & \ddots & \vdots \\ m_{m,1}N & m_{m,2}N & \cdots & m_{m,p}N \end{pmatrix}$$

More compactly, we have $(M \otimes N)_{p(r-1)+v, q(s-1)+w} = m_{rs}n_{vw}$ for $1 \leq r \leq m$, $1 \leq s \leq p$, $1 \leq v \leq n$, $1 \leq w \leq q$.

Result 1.4. If H_1 is a $\text{BH}(n, h_1)$ matrix and H_2 is a $\text{BH}(m, h_2)$ matrix, then $H_1 \otimes H_2$ is a $\text{BH}(mn, h)$ matrix, where $h = \text{lcm}(h_1, h_2)$.

Proof. We have

$$(H_1 \otimes H_2)(H_1 \otimes H_2)^* = (H_1 \otimes H_2)(H_1^* \otimes H_2^*) = H_1 H_1^* \otimes H_2 H_2^* = nI_n \otimes mI_m = nmI_{nm},$$

where I_n is the identity matrix of order n . Furthermore the entries of $H_1 \otimes H_2$ are products of a h_1^{th} and a h_2^{th} root of unity, and thus is a h^{th} root of unity. $\square$

Example 1.5. Let

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

be a $\text{BH}(2, 2)$ matrix. We can take the Kronecker product of H_2 with itself and check that

$$H_4 := H_2 \otimes H_2 = \begin{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} & \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\ \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} & -\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

is a $\text{BH}(4, 2)$ matrix. Furthermore, we observe that the matrix

$$H_{2^k} := \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix} = H_2 \otimes H_{2^{k-1}}$$

is a $\text{BH}(2^{2^k}, 2)$ matrix for every positive integer k by Result 1.4. In fact, these matrices were first constructed by Sylvester in [55].

If a matrix M is indexed by a finite abelian group G , we can order the group elements, say $g_1, \dots, g_{|G|}$ and write down the matrix M with $m_{i,j} = m_{g_i, g_j}$. So if M, N are matrices indexed by groups G, K respectively, we can compute their Kronecker product $M \otimes N$. The matrix $M \otimes N$ can then be indexed by $G \times K$ where $g_i k_j$ is the $[(i-1)|K| + j]^{th}$ element of $G \times K$. This is also the most natural order since the row (or column) of $M \otimes N$ indexed by $g_i k_j$ would be the row (or column) obtained by multiplying values in the row (or column) in M indexed by g_i and values in the row (or column) in N indexed by k_j . Furthermore in this way, we have $(M \otimes N)_{g_r k_s, g_v k_w} = m_{g_r, g_v} n_{k_s, k_w}$. Therefore we have the following definition:

Definition 1.6. *If $M = (m_{u,v})_{u,v \in G}$ is a matrix indexed by G and $N = (n_{x,y})_{x,y \in K}$, then the Kronecker product of M and N , denoted by $M \otimes N$, is the matrix indexed by $G \times K$ given by $(M \otimes N)_{ux, vy} = m_{u,v} n_{x,y}$.*

1.2 Group Rings and Characters

The group ring notation introduced in this section is used throughout this dissertation to describe Butson Hadamard matrices. Although this is simply a change of language, this

proves to be invaluable due to the wealth of existing literature on related combinatorial objects also described by group rings, from which we can extend existing tools to suit our needs. Characters of finite abelian groups are introduced afterwards, which are extended linearly to group rings. Group invariant Butson Hadamard matrices are then characterized in terms of group rings and characters.

1.2.1 Group Rings

Let G be a finite group of order n written multiplicatively and R be a ring with identity. The group ring $R[G]$ of G over R is the set of formal expressions of the form

$$X = \sum_{g \in G} a_g g, \quad a_g \in R.$$

The ring elements a_g are referred to as the **coefficients** and the set $\text{supp}(X) = \{g \in G : a_g \neq 0\}$ is the **support** of X . Addition of group ring elements is defined by summing the corresponding coefficients for each element g :

$$X + Y = \sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g.$$

Multiplication of group ring elements is defined distributively:

$$XY = \left(\sum_{g \in G} a_g g \right) \left(\sum_{g \in G} b_g g \right) = \sum_{k \in G} \left(\sum_{gh=k} a_g b_h \right) k.$$

Two elements $X = \sum_{g \in G} a_g g$ and $Y = \sum_{g \in G} b_g g$ of $R[G]$ are equal if and only if $a_g = b_g$ for all $g \in G$. A subset S of G is often identified with the group ring element $\sum_{g \in S} g$ when the context is clear. For the identity element 1_G of G and $\lambda \in R$, we write λ for the group ring element $\lambda 1_G$. For $R = \mathbb{Z}[\zeta]$, where ζ is a root of unity, and $X = \sum_{g \in G} a_g g \in \mathbb{Z}[\zeta][G]$, we write

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

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

1.2.2 Characters of Finite Abelian Groups

Let G be a finite abelian group of order n . A **character**¹ χ of G is a group homomorphism from G to the group of complex numbers under multiplication.

Example 1.7. Let $G = \mathbb{Z}_n$ be a cyclic group generated by g and let χ be a character. Since $g^n = 1$ and characters are group homomorphisms, we have

$$\chi(g)^n = \chi(g^n) = \chi(1) = 1,$$

and thus $\chi(g)$ is a n^{th} root of unity. (This can be easily extended to show that the character value on any group element of a finite abelian group must be a root of unity.) Hence, $\chi(g) = \zeta_n^i$ for some i , where ζ_n is a primitive n^{th} root of unity. Note that since g is a generator of G , one can compute the character values for any element via $\chi(g^j) = \chi(g)^j = \zeta_n^{ij}$. In fact, since there are n choices for i , there are exactly n characters of G .

The trivial character refers to the character χ_0 which sends every group element to 1. If we define the product of characters χ and τ of G to be their point-wise multiplication, $(\chi\tau)(g) = \chi(g)\tau(g)$ for all $g \in G$, then set of characters of G is an abelian group. We denote the character group of G by $\widehat{G}$. For a subgroup U of G , write

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

The following is the orthogonality relation of characters (see [3, Chapter VI, Lemma 3.4], for instance),

Result 1.8 (Orthogonality Relation). *Let G be a finite abelian group and U be a subgroup*

¹A representation of a group G on a finite-dimensional vector space V over a field F is a group homomorphism from G to $\text{GL}(V)$, the general linear group of V or the set of automorphisms of V . A character is usually defined on a representation to be its trace. In this thesis, as we are restricting our use of characters to finite abelian groups G with a representation on the vector space $\mathbb{C}$ over $\mathbb{C}$, the given definition is an equivalent characterization and any results stated will apply only to our definition of character.

of G . Then for any character χ of G ,

$$\sum_{g \in U} \chi(g) = \begin{cases} |U|, & \text{if } \chi \in U^\perp, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. If $\chi \in U^\perp$, then $\sum_{g \in U} \chi(g) = \sum_{g \in U} 1 = |U|$. If $\chi \notin U^\perp$, then there exist a $u \in U$ such that $\chi(u) \neq 1$. Then,

$$\chi(u) \sum_{g \in U} \chi(g) = \sum_{g \in U} \chi(u) \chi(g) = \sum_{g \in U} \chi(ug) = \sum_{g \in U} \chi(g),$$

implying that $(\chi(u) - 1) \sum_{g \in U} \chi(g) = 0$. Therefore $\sum_{g \in U} \chi(g) = 0$. $\square$

A character χ of G is extended to group ring elements $X = \sum_{g \in G} a_g g \in R[G]$ by $\chi(X) := \sum_{g \in G} a_g \chi(g)$. The orthogonality relation can thus be restated: For any subgroup U of G , we have $\chi(U) = |U|$ if χ is trivial on U and $\chi(U) = 0$ otherwise.

For finite abelian groups, the character values of a group ring element completely determine its coefficients and thus the group ring element itself. For a proof of the following result, see [3, Chapter VI, Lemma 3.5], for instance.

Result 1.9 (Fourier Inversion). *Let G be a finite abelian group and $D = \sum_{g \in G} a_g g$ with $a_g \in \mathbb{C}$. Then*

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

If $D, E \in \mathbb{Z}[\zeta][G]$, where ζ is a root of unity, satisfy $\chi(D) = \chi(E)$ for all characters χ of G , then $D = E$.

1.3 Number Theoretic Tools

In this section, we develop some number theoretic tools which we subsequently will use to study the structure of group invariant Butson Hadamard matrices.

Definition 1.10. *A complex number α is called an algebraic integer if it is a root of a monic polynomial with coefficients in $\mathbb{Z}$.*

It is straightforward to see that a root of unity is an algebraic integer and it is well-known that sums and products of algebraic integers are algebraic integers.

In our study of $\text{BH}(G, h)$, we often come across sums of roots of unity whose absolute value is small compared to their length. For this, there is a well-known result of Kronecker. See [6, Section 2.3, Thm. 2] for a proof of the following result.

Result 1.11 (Kronecker). *An algebraic integer all of whose conjugates have absolute value at most 1 is a root of unity or 0.*

One situation which we frequently encounter is that our construction of Butson Hadamard matrices requires that a sum of roots of unity must be equal to 0 or 1. Explicitly, we often require roots of unity $\zeta_h^{a_i}$ which satisfy

$$\sum_{i=1}^t \zeta_h^{a_i} = 0 \quad \text{or} \quad \sum_{i=1}^t \zeta_h^{a_i} = 1.$$

We prove a number-theoretic result that determines when these conditions can be satisfied. Another situation which comes up is the equations

$$\sum_{i=1}^t \zeta_h^{a_i} = s \quad \text{or} \quad \sum_{i=1}^t \zeta_h^{a_i} = t - s + (s - 1)\eta + \mu,$$

where η, μ are roots of unity. We demonstrate that there is a lower bound on the number of $\zeta_h^{a_i}$ s that are equal to 1 or η in the following subsection for each of these cases.

1.3.1 Vanishing Sums of Roots of Unity

Let h be a fixed positive integer whose distinct prime divisors are $q_1, \dots, q_t$, where $q_1 < \dots < q_t$. We set

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

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

Vanishing sums of roots of unity were studied by Conway and Jones [10], in which they characterized all vanishing sums with at most 9 terms. Lam and Leung [41] determined fully the conditions on the positive integers m for which there exists h^{th} roots of unity such that $\eta_1 + \cdots + \eta_m = 0$,

Result 1.12. (Lam-Leung [41, Main Theorem]) *Let h, m be positive integers. There are $\eta_1, \dots, \eta_m \in \mathcal{U}(h)$ with $\sum_{i=1}^m \eta_i = 0$ if and only if $m \in \mathcal{Q}(h)$.*

Thus the condition $m \in \mathcal{Q}(h)$ is important for our study of the existence of Butson Hadamard matrices. There is a well-known elementary number theoretic fact that gives a sufficient condition for this.

Result 1.13. (LeVeque [44, p. 22, Ex. 4]) *Let p, q be two coprime positive integers. If n is an integer such that $n \geq (p-1)(q-1)$, then $n \in \mathcal{Q}(pq)$.*

We note that Result 1.12 was formulated in the setting of group rings, or more specifically in $\mathbb{Z}[G]$, where G is a cyclic group. The set $\mathbb{N}G \cap \ker(\varphi)$, where $\mathbb{N}G = \{\sum_{g \in G} a_g g \in \mathbb{Z}[G] : a_g \geq 0\}$ with the map $\varphi : \mathbb{Z}[G] \rightarrow \mathbb{Z}[\zeta_h]$ defined by $\varphi(g) = \zeta_h$, was the main focus of the study. For a set $S \subseteq \mathbb{Z}[G]$ and subgroup P of G , we define $S \cdot P = \{XP \in \mathbb{Z}[G] : X \subseteq S\}$. The following are some relevant results which we need for the analysis:

Result 1.14. (Lam-Leung [41, Thm. 2.2]) *Let h be a positive integer with the prime decomposition $h = q_1^{a_1} \cdots q_t^{a_t}$, with $q_1 < \cdots < q_t$, and ζ_h be a primitive h^{th} root of unity. Let $G = \langle g \rangle$ be a cyclic group of order h and Q_i be the unique subgroup of order q_i for each $i = 1, \dots, t$. Suppose that $\varphi : \mathbb{Z}[G] \rightarrow \mathbb{Z}[\zeta_h]$ is the map defined by $\varphi(g) = \zeta_h$. Then,*

$$\ker(\varphi) = \sum_{i=1}^t \mathbb{Z}G \cdot Q_i \quad \text{and} \quad \ker(\varphi) = \mathbb{Z} \cdot Q_1, \quad \text{if } t = 1.$$

Result 1.15. (Lam-Leung [41, Thm. 4.1]) *Let h be a positive integer with the prime decomposition $h = q_1^{a_1} \cdots q_t^{a_t}$, with $q_1 < \cdots < q_t$, with $t \geq 2$, and ζ_h be a primitive h^{th} root of unity. Let $G = \langle g \rangle$ be a cyclic group of order h and $\varphi : \mathbb{Z}[G] \rightarrow \mathbb{Z}[\zeta_h]$ be the map defined by $\varphi(g) = \zeta_h$. Suppose that $X = \sum_{g \in G} a_g g$ and $Y = \sum_{g \in G} b_g g \in \mathbb{Z}[G]$ are group*

ring elements such that $a_g, b_g \geq 0$ for all $g \in G$ and $\rho(X) = \rho(Y)$. If $\text{supp}(X) \leq q_1 - 1$, then either $b_g \geq a_g$ for all $g \in G$ or $\text{supp}(Y) \geq (q_1 - \text{supp}(X))(q_2 - 1)$.

We use a similar method and the above results to deal with the issue of $\sum_{i=1}^t \zeta_h^{a_i} = 1$.

Theorem 1.16. *Let h, m be positive integers. There are $\eta_1, \dots, \eta_m \in \mathcal{U}(h)$ with*

$$\sum_{i=1}^m \eta_i = 1 \quad (1.1)$$

if and only if

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

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

(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 .*

Proof. Assume that (i) holds, that is, h is even and $m + 1 \in \mathcal{Q}(h)$. By Result 1.12, there are $\eta_1, \dots, \eta_{m+1} \in \mathcal{U}(h)$ 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 (1.1) has solution.

Suppose that (ii) holds, that is, h is odd and $m - 1 \in \mathcal{Q}(h)$. By Result 1.12, there are $\eta_1, \dots, \eta_{m-1} \in \mathcal{U}(h)$ with $\sum_{i=1}^{m-1} \eta_i = 0$. Setting $\eta_m = 1$ thus gives a solution of (1.1).

Now suppose that (iii) holds. Then

$$(\zeta_{q_1} + \dots + \zeta_{q_1}^{q_1-1})(\zeta_{q_2} + \dots + \zeta_{q_2}^{q_2-1}) = (-1)(-1) = 1 \quad (1.2)$$

gives a solution of (1.1), since the number of roots of unity obtained by expanding the left hand side of (1.2) is $(q_1 - 1)(q_2 - 1) = m$. In summary, we have shown the sufficiency of conditions (i) – (iii).

To prove necessity, assume that (1.1) holds. Note that (1.1) can be written in the form

$$\sum_{i=1}^{m+1} \eta_i = 0 \text{ with } \eta_{m+1} = -1. \quad (1.3)$$

First assume that h is even. Then $\eta_{m+1} = -1 \in \mathcal{U}(h)$ and thus $m+1 \in \mathcal{Q}(h)$ by (1.4) and Result 1.12. Hence condition (i) of Theorem 1.16 is satisfied.

Hence we can assume that h is odd. Suppose that condition (ii) of Theorem 1.16 does not hold, that is,

$$m-1 \notin \mathcal{Q}(h). \quad (1.4)$$

To complete the proof, we have to show that condition (iii) of Theorem 1.16 holds.

Let $G = \langle g \rangle$ be a cyclic group of order h and let $\rho : \mathbb{Z}[G] \rightarrow \mathbb{Z}[\zeta_h]$ be the homomorphism determined by $\rho(g) = \zeta_h$. As $\eta_i \in \mathcal{U}(h)$ for all i by assumption, we can write $\eta_i = \zeta_h^{a_i}$ with $a_i \in \mathbb{Z}$. Define $Y := \sum_{i=1}^m g^{a_i}$ and observe that $\rho(Y) = \sum_{i=1}^m \eta_i = 1$.

First suppose that h is a prime power, say $h = q^b$ where q is a prime. By Result 1.14, the kernel of ρ is $\{nQ : n \in \mathbb{Z}\}$ where $Q = 1 + g^{q^{b-1}} + \dots + g^{(q-1)q^{b-1}}$. We have $\rho(Y-1) = 0$ and thus $Y-1 = nQ$ for some $n \in \mathbb{Z}$. Applying the trivial character of G , we get $m-1 \equiv 0 \pmod{q}$. But this contradicts (1.4).

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 . Since $\rho(Y) = 1 = \rho(1)$ and $\text{supp}(1) = 1 < q_1 - 1$, we can use Result 1.15 to conclude either $g^{a_j} = 1$ for some j or $m \geq (q_1 - 1)(q_2 - 1)$. In the first case, we have $\sum_{i=1, i \neq j}^m \eta_i = 0$ and thus $m-1 \in \mathcal{Q}(h)$ by Result 1.12, a contradiction to (1.4). In the second case, we have $m-1 \in \mathcal{Q}(h)$ by Result 1.13 if $m > (q_1 - 1)(q_2 - 1)$. Therefore $m = (q_1 - 1)(q_2 - 1)$ and this completes the proof. $\square$

Intuitively, if a sum of s roots of unity is equal to a positive integer t which is close to s , we expect that many of the roots of unity occurring in the sum must be equal to 1. We now make this idea precise and also prove some related results that are relevant for investigating the structure of group invariant Butson Hadamard matrices.

Lemma 1.17. *Let h be a positive integer which has at least one odd prime divisor and let s, t be positive integers. Suppose that*

$$\sum_{i=1}^s \eta_i = t\eta, \quad (1.5)$$

where $\eta, \eta_1, \dots, \eta_s$ are complex h th roots of unity. Then

$$|\{i : \eta_i = \eta, 1 \leq i \leq s\}| \geq t - \frac{s-t}{q-2},$$

where q is the smallest odd prime divisor of h .

Proof. Without loss of generality, we can assume that $\eta = 1$. Suppose Lemma 1.17 has been proved for $a = |\{i : \eta_i = 1\}| = 0$. Then we have $0 \geq t - (s-t)/(q-2)$. Now assume that $a = |\{i : \eta_i = 1\}| > 0$. Then subtracting a on both sides of (1.5), we get $\sum_{i=1}^{s-a} \eta_i = t - a$ and thus

$$0 \geq t - a' - \frac{(s-a) - (t-a)}{q-2}.$$

Therefore, $a' \geq t - (s-t)/(q-2)$ as desired. So it remains to prove Lemma 1.17 for $a = 0$. We proceed by induction on h .

Write $h = q^b h'$ where $q \nmid h'$. Write $\sum_{i=1}^s \eta_i = \sum_{j=0}^{q-1} X_j \zeta_{q^b}^j$, where $X_j = \sum_{i=1}^{s_j} \mu_{ji}$ with $\mu_{ji} \in \mathcal{U}(2h/q)$. Clearly we can assume $\sum_{j=0}^{q-1} s_j = s$.

If $b = 1$, then we have $X_0 - X_j = t$ for any $j = 1, \dots, q-1$ as the minimal polynomial of ζ_q over $\mathbb{Q}(\zeta_{h/q})$ is $x^{q-1} + \dots + x + 1$. Let t_j be the number of 1's in each summand of $-X_j$. If h is prime, then every term in the summand X_0 or $-X_j$ is ± 1 . As $a = 0$, none of the terms in X_0 is 1 and so $t_j > t$ for $j = 1, \dots, q-1$. Hence Lemma 1.17 holds. If $h \neq q$, then we may apply induction to get $t_j \geq t - (s_0 + s_j - t)/(q-2)$ for $j = 1, \dots, q-1$. Therefore,

$$\sum_{j=1}^{q-1} s_j \geq \sum_{j=1}^{q-1} t_j \geq \frac{(q-1)^2 t}{q-2} - \frac{s}{q-2} - s_0.$$

Note that $\sum_{j=0}^{q-1} s_j = s$. Therefore $s \geq (q-1)^2 t/(q-2) - s/(q-2)$ and hence $s \geq (q-1)t$. We then have $0 \geq t - (s-t)/(q-2)$ as desired.

If $b \geq 2$, then as $1, \zeta_{q^b}, \dots, \zeta_{q^b}^{q-1}$ are linearly independent over $\mathbb{Q}(\zeta_{h/q})$, we observe that $X_0 = t$ and $X_j = 0$ for all $j \neq 0$. Note that X_0 is a subsum of $\sum_{i=1}^s \eta_i$ and recall that $\eta_i \neq 1$ for any i . As assumed, we have $\eta_i \in \mathcal{U}(2h/q)$ and so we may apply induction to conclude that $0 \geq t - (s_0 - t)/(q-2) \geq t - (s-t)/(q-2)$. $\square$

Sometimes, we come across the situation of two sums of roots of unity which are equal but one of which consists of only a few distinct roots. In this case, the number of solutions for the unknown roots on the other sums is also quite restricted as we see in the following lemma:

Lemma 1.18. *Let $h > 1$ be an integer that does not have a prime divisor ≤ 5 . Suppose that*

$$\sum_{i=1}^s \eta_i = s - a + (a - 1)\zeta_h^j + \mu, \quad (1.6)$$

where a, s, j are integers with $a, s \geq 1$, $j \not\equiv 0 \pmod{h}$, μ is a $(2h)$ th root of unity, and $\eta_1, \dots, \eta_s$ are h th roots of unity. Then $\mu^h = 1$ and

$$|\{i : \eta_i = 1\}| \geq s - a \text{ and } |\{i : \eta_i = \zeta_h^j\}| \geq a - 1. \quad (1.7)$$

Proof. We proceed by induction on s . If $s = 1$ then both sides has only one term. Then μ is a h^{th} root of unity and condition (1.7) holds.

Assume $s > 1$. After dividing by ζ_h^j if necessary, we may assume that $a \leq (s - 1)/2$. On the other hand, we have $-\mu - (a - 1)\zeta_h^j + \sum_{i=1}^s \eta_i = s - a$. By Lemma 1.17 and the fact that the smallest prime divisor of h is at least 5, the number of η_i 's equal to 1 is at least

$$(s - a) - \frac{s + a - (s - a)}{3} \geq \frac{3s - 5a}{3} > 0$$

as $a \leq (s - 1)/2$. Thus we may assume $\eta_s = 1$ and so $\sum_{i=1}^{s-1} \eta_i = (s - 1 - a) + (a - 1)\zeta_h^j + \mu$. By induction, we conclude that $\eta^h = 1$,

$$|\{1 \leq i \leq s - 1 : \eta_i = 1\}| \geq s - 1 - a \text{ and } |\{i : \eta_i = \zeta_h^j\}| \geq a - 1.$$

Hence $|\{1 \leq i \leq s : \eta_i = 1\}| \geq s - a$. □

Lemma 1.19. *Let $h > 1$ be an odd integer that does not have a prime divisor ≤ 5 . Suppose that*

$$\sum_{i=1}^s \eta_i = s - 1 + \mu, \quad (1.8)$$

where s is a positive integer and μ is a $(2h)$ th root of unity, and $\eta_1, \dots, \eta_s$ are h th roots of unity. Then $\mu^h = 1$ and

$$|\{i : \eta_i = 1\}| \geq s - 1. \quad (1.9)$$

Proof. Let q be the smallest prime divisor of h . By Corollary 1.17, at least $(s-1)-2/(q-2)$ terms of roots of unity in $\sum_{i=1}^s \eta_i - \mu$ must be equal to 1. Thus we may assume $\eta_1 = \dots = \eta_{s-2} = 1$. By (1.8) we hence have $\eta_{s-1} + \eta_s = 1 + \mu$. If $\mu = -1$, then $\eta_{s-1} + \eta_s = 0$, which is impossible as η_{s-1} and η_s are of odd order. Thus $\mu \neq -1$. As $\eta_{s-1} + \eta_s - \mu = 1$ and $-\mu \neq 1$, at least one of η_{s-1} and η_s must be equal to 1 by Corollary 1.17. This proves (1.9). Moreover, we conclude $\mu = \eta_{s-1}$ or $\mu = \eta_s$ and thus $\mu^h = 1$. $\square$

Chapter 2

Constructions

In this chapter, we study the problem of the existence of group invariant Butson Hadamard matrices. We will show that G -invariant Butson Hadamard matrices exist for a group G by constructing them explicitly. To do so, we use the blueprint in the following result which allows us to create group invariant Butson Hadamard matrices from group rings. For a proof of the following result, see [53, Lem. 2.1].

Result 2.1. *Let G be a finite abelian group, let h be a positive integer, and for each $g \in G$, let a_g be a complex h th root of unity. Consider the element $D = \sum_{g \in G} a_g g$ of $\mathbb{Z}[\zeta_h][G]$ and the G -invariant matrix $H = (H_{g,k})$, $g, k \in G$ given by $H_{g,k} = a_{gk^{-1}}$. Then H is a $\text{BH}(G, h)$ matrix if and only if*

$$DD^{(-1)} = |G|. \quad (2.1)$$

Moreover, (2.1) holds if and only if

$$|\chi(D)|^2 = |G| \text{ for all } \chi \in \hat{G}. \quad (2.2)$$

Hence, we now need to construct group rings in $\mathbb{Z}[\zeta_h]$ satisfying equation (2.2) to obtain Butson Hadamard matrices. In light of Result 2.1, we will often say that D is in $\text{BH}(G, h)$ in place of the matrix H as in Result 2.1 to mean that H is a G -invariant Butson Hadamard matrix for the rest of this paper.

One way to obtain Butson Hadamard matrices is to construct them from smaller Butson Hadamard matrices. If H_1 and H_2 are Butson Hadamard matrices, then $H_1 \otimes H_2$ is also a Butson Hadamard matrix where $\otimes$ is the Kronecker product. In the same way, we can multiply two group ring elements D, E which are G_1 and G_2 -invariant Butson Hadamard matrix to obtain a $(G_1 \times G_2)$ -invariant Butson Hadamard matrix. Furthermore, the matrix $H(DE)$ obtained from DE correspond to the matrix $H(D) \otimes H(E)$.

Lemma 2.2. *Let G_1, G_2 be finite abelian groups and let h, v be positive integers. Suppose that $D \in \mathbb{Z}[\zeta_h][G_1]$ and $E \in \mathbb{Z}[\zeta_v][G_2]$ are $\text{BH}(G_1, h)$ and $\text{BH}(G_2, v)$ matrices respectively. Then DE is a $\text{BH}(G_1 \times G_2, d)$ matrix, where $d = \gcd(h, v)$. Furthermore we have*

$$H(DE) = H(D) \otimes H(E). \quad (2.3)$$

Proof. Write $D = \sum_{g \in G_1} a_g g$ and $E = \sum_{g \in G_2} b_g g$. We define $DE = \sum_{g_1 \in G_1} \sum_{g_2 \in G_2} (a_{g_1} b_{g_2}) g_1 g_2$. Note that DE has the form $\sum_{g \in G} c_g g$ where c_g is a root of unity since g has a unique representation $g = g_1 g_2$ with $g_1 \in G_1$ and $g_2 \in G_2$. Thus $H(DE)$ is $(G_1 \times G_2)$ -invariant.

Now, we show that (2.3) holds. Let $g, k \in G_1 \times G_2$ and write $g = g_1 g_2, k = k_1 k_2$ where $g_i, k_i \in G_i$ for $i = 1, 2$. Observe that in the Kronecker product $H(D) \otimes H(E)$, the row indexed by g corresponds to the row obtained by multiplying values in the rows indexed by g_1 and g_2 in $H(D)$ and $H(E)$ respectively. In the same vein, we can also say the same for the columns of $H(D) \otimes H(E)$. So,

$$\begin{aligned} H(DE)_{g,k} &= c_{gk^{-1}} = c_{g_1 k_1^{-1} g_2 k_2^{-1}} = a_{g_1 k_1^{-1}} b_{g_2 k_2^{-1}} \\ &= H(D)_{g_1, k_1} H(E)_{g_2, k_2} = [H(D) \otimes H(E)]_{g,k}, \end{aligned}$$

and we are done. □

Lemma 2.2 allows us to focus our attention on the situation when G is a primary group when dealing with the existence problem. Let G be a finite abelian group of order $n = p_1^{a_1} \cdots p_n^{a_n}$, where $p_1, \dots, p_n$ are the prime divisors of n and $a_1, \dots, a_n$ are positive integers. By the fundamental theorem of finite abelian groups, any finite abelian group

G can be decomposed into $G = G_1 \times \cdots \times G_t$, where G_i is a primary group of order $p_i^{a_i}$. Then we can use Lemma 2.2 to obtain $\text{BH}(G, h)$ matrices by constructing them from $\text{BH}(G_i, h)$ matrices for $i = 1, \dots, t$.

Multiplying D with a root of unity $\zeta_h^{a_i}$ corresponds to multiplying its associated Butson Hadamard matrix by $\zeta_h^{a_i}$ and translating D by a group element g , which is Dg , corresponds to a series of row and column swapping. On the other hand, it is straightforward to see that if D satisfies (2.2), then any translate and any root of unity multiple, say $\zeta_h^{a_i} Dg$, would still satisfy (2.2). In this sense, there are no meaningful differences between these matrices and so we identify these group ring elements as the same.

Definition 2.3. *Let G be a finite abelian group, h be a positive integer, and ζ_h be a h^{th} root of unity. Two group ring elements $D, E \in \mathbb{Z}[\zeta_h][G]$ are said to be **equivalent** if one of them is a translate or a root of unity multiple of the other, i.e. $E = \zeta_h^{a_i} Dg$ for some integer a_i and $g \in G$.*

2.1 Constructions Using Subgroups

In this section, we use the subgroups of G as building blocks for the group ring elements we desire. Our strategy starts with considering the group ring elements which are the sum of some subgroups, say $X = \sum_{i=1}^n U_i$ with $|U_i|^2 = |G|$. Recall that for a subgroup S and a character χ of G , the orthogonality relation (see Result 1.8) tells us that $\chi(U)$ is simply $|U|$ if χ acts trivially on U and 0 otherwise. Hence, we have $|\chi(X)|^2 = |G|$ for characters χ which act trivially on just one subgroup U_i . The next step consists of replacing each subgroup U_i by $\zeta_h^{a_i} U_i g_i$ and determining the conditions on $\zeta_h^{a_i}$ to obtain a new group ring element D , so that $|\chi(D)|^2 = |G|$ for the other characters χ which does not act trivially on just one subgroup and also that D is in the form $\sum_{g \in G} a_g g$ with $|a_g| = 1$ for all $g \in G$.

Furthermore, the orthogonality relation simplifies the computation of character values on any group ring elements which consist of just a sum of the subgroups and enables us to check if a group ring D satisfies (2.2) easily. This will be used throughout this section to prove that our constructions are indeed correct.

2.1.1 Spread Construction

Let $\text{EA}(p^b)$ denote the elementary abelian group of order p^b , i.e., $\text{EA}(p^b) \cong (\mathbb{Z}/p\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p\mathbb{Z})$ (b copies). In [14], Davis gave a construction of relative difference sets in $\text{EA}(p^{2a})$ using its hyperplanes. If $E = \text{EA}(p^{2a})$ is viewed as a vector space of dimension 2 over the field $\mathbb{F}_{p^a}$, then the hyperplanes of dimension 1 are all the subgroups of E of order p^a . There are exactly $p^a + 1$ of these subgroups and they cover the whole group E , with the identity being contained in all of them. In other words, we have

$$D = \sum_{i=0}^{p^a} U_i = E + p^a,$$

where the U_i 's are the subgroups of order p^a . Note that each non-trivial character χ of E is trivial on exactly one of U_i and so

$$\left| \chi \left(\sum_{i=0}^{p^a} U_i \right) \right|^2 = \left| \sum_{i=0}^{p^a} \chi(U_i) \right|^2 = |U_i|^2 = |E|. \quad (2.4)$$

However by Result 2.1, this group ring element D would not give us a Butson Hadamard matrix since

$$\left| \chi_0 \left(\sum_{i=0}^{p^a} U_i \right) \right|^2 = |\chi_0(E + p^a)|^2 = |p^{2a} + p^a|^2 \neq |E|,$$

where χ_0 is the trivial character of E . Instead, if each U_i were to be replaced with $\eta_i U_i$, then (2.4) still holds and

$$\left| \chi_0 \left(\sum_{i=0}^{p^a} \eta_i U_i \right) \right|^2 = \left| \sum_{i=0}^{p^a} \eta_i |U_i| \right|^2 = p^{2a} \left| \sum_{i=0}^{p^a} \eta_i \right|^2,$$

implying that the sum $\sum_{i=0}^{p^a} \eta_i$ should be a root of unity if D were to give us a Butson Hadamard matrix. Next we observe that this condition is also crucial in another context since the coefficient a_1 takes on the value $\sum_{i=0}^{p^a} \eta_i$ in this construction. Furthermore since we are only concerned about group ring elements up to an equivalence, we can assume that $\sum_{i=0}^{p^a} \eta_i = 1$. Thus the requirement that all coefficients are roots of unity is also

satisfied.

Interestingly, the key properties of our subgroups $U_0, \dots, U_{p^a}$ are that they partition the non-identity elements of E and $U_i U_j = G$ for all $i \neq j$. In fact, these mathematical objects have been studied before. For a group G of order m^2 , the collection $U_0, \dots, U_m$ of subgroups of G with $U_i U_j = G$ for all $i \neq j$ and $\bigcup_{i=0}^m U_i = G$ is called a **spread**. 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 2.4. *Let $U_0, \dots, U_m$ be a spread of a group G of order m^2 and let $\eta_0, \dots, \eta_m$ be any complex roots of unity with $\sum_{i=0}^m \eta_i = 1$. Then*

$$X = \sum_{i=0}^m U_i \eta_i \quad (2.5)$$

is a $\text{BH}(G, h)$ 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 $|\chi(X)|^2 = m^2$.

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 $|\chi(X)|^2 = m^2$ for all characters χ of G . Hence $X \in \text{BH}(G, h)$ by Result 2.1. $\square$

Translation planes and thus spreads of elementary abelian groups exist in abundance; see the monograph [45], for instance. In particular, we have the following.

Corollary 2.5. *Let G be an elementary abelian group of order p^{2a} and let h be any positive integer such that $p^a \in \mathcal{Q}(h)$ or $p^a + 1 = (q_1 - 1)(q_2 - 1)$ where q_1 and q_2 are distinct prime divisors of h . Then there is a $\text{BH}(G, h)$ matrix.*

Proof. It is well known [45] that there is a spread in G . Hence, by Theorem 2.4, it suffices to show that there are $\eta_1, \dots, \eta_{p^a+1} \in \mathcal{Q}(h)$ with

$$\sum_{i=1}^{p^a+1} \eta_i = 1. \quad (2.6)$$

If $p^a \in \mathcal{Q}(h)$, then this follows from Theorem 1.16. 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 $(\zeta_{q_1} + \dots + \zeta_{q_1}^{q_1-1})(\zeta_{q_2} + \dots + \zeta_{q_2}^{q_2-1}) = 1$ gives a solution of (2.6). $\square$

Corollary 2.6. *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 $\text{BH}(G, h)$ matrix.*

Proof. If $p^a = (q_1 - 1)(q_2 - 1) - 1$, then a $\text{BH}(G, h)$ matrix exists by Corollary 2.5. Hence we can assume $p^a \geq (q_1 - 1)(q_2 - 1)$. Then $p^a \in \mathcal{Q}(h)$ by Result 1.13. and thus a $\text{BH}(G, h)$ matrix exists by Corollary 2.5. $\square$

Corollary 2.7. *A $\text{BH}(G, 6)$ matrix exists for every elementary abelian group G of square order.*

Proof. This follows from Corollary 2.6, as $(q_1 - 1)(q_2 - 1) = 2$ for $h = 6$. $\square$

Example 2.8. We now look at an example of a $\text{BH}(\mathbb{Z}_p \times \mathbb{Z}_p, 6)$ matrix given by Szöllősi and Craigen. Let P denote the Paley matrix of order p given by $P_{i,j} = \left(\frac{i-j}{p}\right)$, where $\left(\frac{a}{p}\right)$ is the Legendre symbol, and let J be the all ones matrix. Then, the matrix

$$H = P \otimes P + J \otimes I + \zeta_3 I \otimes J$$

is a $\text{BH}(p^2, 6)$ matrix [56, Thm. 1.4.41]. This construction is actually $(\mathbb{Z}_p \times \mathbb{Z}_p)$ -invariant and also appears as a special case of our construction, even though both are described in different ways. Index the entries of P, I, J by elements of $\mathbb{Z}_p$ so that the matrix $A \otimes B$, where $A, B \in \{P, I, J\}$, indexed by $\mathbb{Z}_p \times \mathbb{Z}_p$ can be written as $[A \otimes B]_{(i,s),(j,t)} = [A \otimes B]_{ip+s, jp+t}$, that is the indexing by group elements corresponds to the lexicographical order of the group elements. This is done so that $[A \otimes B]_{(i,s),(j,t)} = [A \otimes B]_{ip+s, jp+t} = A_{i,j} B_{s,t}$. Since P, I, J are all circulant (and thus $\mathbb{Z}_p$ -invariant), it follows that the Kronecker product of any pair of them is $(\mathbb{Z}_p \times \mathbb{Z}_p)$ -invariant and consequently H is too.

Next, consider the group ring element $D = \sum_{(i,j) \in \mathbb{Z}_p \times \mathbb{Z}_p} H_{(i,j),(0,0)}(i,j)$. We need to show that D is in the form (2.5), up to equivalence. Note that the subgroups of order p of $\mathbb{Z}_p \times \mathbb{Z}_p$ are $U_k = \langle (1, k) \rangle$ for $k = 0, \dots, p-1$ and $U_p = \langle (0, 1) \rangle$. Then, we have

$$H_{(i,j),(0,0)} = P_{i,0}P_{j,0} + J_{i,0}I_{j,0} + \zeta_3 I_{i,0}J_{j,0} = \begin{cases} -\zeta_3^2, & \text{if } i = j = 0, \\ \zeta_3, & \text{if } i = 0, j \neq 0, \\ 1, & \text{if } i \neq 0, j = 0, \\ \left(\frac{ij}{p}\right), & \text{otherwise.} \end{cases}$$

Furthermore if t, k are nonzero positive integers, then

$$H_{(t,tk),(0,0)} = \left(\frac{t^2k}{p}\right) = \left(\frac{k}{p}\right) = H_{(1,k),(0,0)}.$$

and thus

$$D = -\zeta_3^2(0,0) + U_0^* + \zeta_3 U_p^* + \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) U_k^* = U_0 + \zeta_3 U_p + \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) U_k,$$

which is indeed in the form of equation (2.5). Lastly, we also observe the condition that the sum $\sum_{k=0}^p \eta_k$ must be a root of unity is also satisfied.

Example 2.9. Consider the group $G = \mathbb{Z}_3 \times \mathbb{Z}_3$ with $h = 10$. Corollary 2.5 tells us that such a $\text{BH}(G, h)$ matrix exists since $3^1 + 1 = 4 = (2-1)(5-1)$. We observe that we can use all the cyclic subgroups of order 3 as a spread of G . So we have

$$\begin{aligned} U_1 = \langle(1,0)\rangle &= \{(0,0), (1,0), (2,0)\}, & U_2 = \langle(1,1)\rangle &= \{(0,0), (1,1), (2,2)\}, \\ U_3 = \langle(1,2)\rangle &= \{(0,0), (1,2), (2,1)\}, & U_4 = \langle(0,1)\rangle &= \{(0,0), (0,1), (0,2)\}. \end{aligned}$$

and assign $\eta_i = -\zeta_5^i$ for $i = 1, 2, 3, 4$. Then we obtain a $\text{BH}(\mathbb{Z}_3 \times \mathbb{Z}_3, 10)$ matrix from the group ring element $\sum_{i=1}^4 \eta_i U_i$

$$\begin{bmatrix} 1 & -\zeta_5^4 & -\zeta_5^4 & -\zeta_5 & -\zeta_5^2 & -\zeta_5^3 & -\zeta_5 & -\zeta_5^3 & -\zeta_5^2 \\ -\zeta_5^4 & 1 & -\zeta_5^4 & -\zeta_5^3 & -\zeta_5 & -\zeta_5^2 & -\zeta_5^2 & -\zeta_5 & -\zeta_5^3 \\ -\zeta_5^4 & -\zeta_5^4 & 1 & -\zeta_5^2 & -\zeta_5^3 & -\zeta_5 & -\zeta_5^3 & -\zeta_5^2 & -\zeta_5 \\ -\zeta_5 & -\zeta_5^3 & -\zeta_5^2 & 1 & -\zeta_5^4 & -\zeta_5^4 & -\zeta_5 & -\zeta_5^2 & -\zeta_5^3 \\ -\zeta_5^2 & -\zeta_5 & -\zeta_5^3 & -\zeta_5^4 & 1 & -\zeta_5^4 & -\zeta_5^3 & -\zeta_5 & -\zeta_5^2 \\ -\zeta_5^3 & -\zeta_5^2 & -\zeta_5 & -\zeta_5^4 & -\zeta_5^4 & 1 & -\zeta_5^2 & -\zeta_5^3 & -\zeta_5 \\ -\zeta_5 & -\zeta_5^2 & -\zeta_5^3 & -\zeta_5 & -\zeta_5^3 & -\zeta_5^2 & 1 & -\zeta_5^4 & -\zeta_5^4 \\ -\zeta_5^3 & -\zeta_5 & -\zeta_5^2 & -\zeta_5^2 & -\zeta_5 & -\zeta_5^3 & -\zeta_5^4 & 1 & -\zeta_5^4 \\ -\zeta_5^2 & -\zeta_5^3 & -\zeta_5 & -\zeta_5^3 & -\zeta_5^2 & -\zeta_5 & -\zeta_5^4 & -\zeta_5^4 & 1 \end{bmatrix},$$

where the matrix is indexed by elements of G ordered lexicographically.

Example 2.10. Now consider the group $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ with $h = 6$. Note that we can view G as a 2-dimensional vector space over the Galois field of order 4 but restricted to just vector addition as its operation. This perspective is convenient since we can take all the 1-dimensional subspaces as a spread over G . In particular, let $\mathbb{F}_4 = \mathbb{Z}_2(\alpha)$ be a field extension of $\mathbb{Z}_2$ with α satisfying $\alpha^2 = 1 + \alpha$. Then we have the following addition and multiplication table:

+	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

*	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Next, we have the following 1-dimensional subspaces of $\mathbb{F}_4 \times \mathbb{F}_4$:

$$\begin{aligned}
U_0 &= \text{span}\{(1, 0)\} = \{(0, 0), (1, 0), (\alpha, 0), (1 + \alpha, 0)\}, \\
U_1 &= \text{span}\{(1, 1)\} = \{(0, 0), (1, 1), (\alpha, \alpha), (1 + \alpha, 1 + \alpha)\}, \\
U_2 &= \text{span}\{(1, \alpha)\} = \{(0, 0), (1, \alpha), (\alpha, 1 + \alpha), (1 + \alpha, 1)\}, \\
U_3 &= \text{span}\{(1, 1 + \alpha)\} = \{(0, 0), (1, 1 + \alpha), (\alpha, 1), (1 + \alpha, \alpha)\}, \\
U_4 &= \text{span}\{(0, 1)\} = \{(0, 0), (0, 1), (0, \alpha), (0, 1 + \alpha)\},
\end{aligned}$$

which we can map onto G via the group homomorphism $\varphi : (a + b\alpha, c + d\alpha) \mapsto (a, b, c, d)$.

This then gives

$$\begin{aligned}
U_0 &= \{(0, 0, 0, 0), (1, 0, 0, 0), (0, 1, 0, 0), (1, 1, 0, 0)\}, \\
U_1 &= \{(0, 0, 0, 0), (1, 0, 1, 0), (0, 1, 0, 1), (1, 1, 1, 1)\}, \\
U_2 &= \{(0, 0, 0, 0), (1, 0, 0, 1), (0, 1, 1, 1), (1, 1, 1, 0)\}, \\
U_3 &= \{(0, 0, 0, 0), (1, 0, 1, 1), (0, 1, 1, 0), (1, 1, 0, 1)\}, \\
U_4 &= \{(0, 0, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1), (0, 0, 1, 1)\},
\end{aligned}$$

Furthermore, let $(\eta_0, \eta_1, \eta_2, \eta_3, \eta_4) = (1, \zeta_3, \zeta_3^2, -\zeta_3, -\zeta_3^2)$ and we obtain a $\text{BH}(\mathbb{Z}_2 \times \mathbb{Z}_2 \times$

$\mathbb{Z}_2 \times \mathbb{Z}_6$) matrix from the group ring element $\sum_{i=0}^4 \eta_i U_i$:

$$\begin{bmatrix} 1 & -\zeta_3^2 & -\zeta_3^2 & -\zeta_3^2 & 1 & \zeta_3 & \zeta_3^2 & -\zeta_3 & 1 & -\zeta_3 & \zeta_3 & \zeta_3^2 & 1 & \zeta_3^2 & -\zeta_3 & \zeta_3 \\ -\zeta_3^2 & 1 & -\zeta_3^2 & -\zeta_3^2 & \zeta_3 & 1 & -\zeta_3 & \zeta_3^2 & -\zeta_3 & 1 & \zeta_3^2 & \zeta_3 & \zeta_3^2 & 1 & \zeta_3 & -\zeta_3 \\ -\zeta_3^2 & -\zeta_3^2 & 1 & -\zeta_3^2 & \zeta_3^2 & -\zeta_3 & 1 & \zeta_3 & \zeta_3 & \zeta_3^2 & 1 & -\zeta_3 & -\zeta_3 & \zeta_3 & 1 & \zeta_3^2 \\ -\zeta_3^2 & -\zeta_3^2 & -\zeta_3^2 & 1 & -\zeta_3 & \zeta_3^2 & \zeta_3 & 1 & \zeta_3^2 & \zeta_3 & -\zeta_3 & 1 & \zeta_3 & -\zeta_3 & \zeta_3^2 & 1 \\ 1 & \zeta_3 & \zeta_3^2 & -\zeta_3 & 1 & -\zeta_3^2 & -\zeta_3^2 & -\zeta_3^2 & 1 & \zeta_3^2 & -\zeta_3 & \zeta_3 & 1 & -\zeta_3 & \zeta_3 & \zeta_3^2 \\ \zeta_3 & 1 & -\zeta_3 & \zeta_3^2 & -\zeta_3^2 & 1 & -\zeta_3^2 & -\zeta_3^2 & \zeta_3^2 & 1 & \zeta_3 & -\zeta_3 & -\zeta_3 & 1 & \zeta_3^2 & \zeta_3 \\ \zeta_3^2 & -\zeta_3 & 1 & \zeta_3 & -\zeta_3^2 & -\zeta_3^2 & 1 & -\zeta_3^2 & -\zeta_3 & \zeta_3 & 1 & \zeta_3^2 & \zeta_3 & \zeta_3^2 & 1 & -\zeta_3 \\ -\zeta_3 & \zeta_3^2 & \zeta_3 & 1 & -\zeta_3^2 & -\zeta_3^2 & -\zeta_3^2 & 1 & \zeta_3 & -\zeta_3 & \zeta_3^2 & 1 & \zeta_3^2 & \zeta_3 & -\zeta_3 & 1 \\ 1 & -\zeta_3 & \zeta_3 & \zeta_3^2 & 1 & \zeta_3^2 & -\zeta_3 & \zeta_3 & 1 & -\zeta_3^2 & -\zeta_3^2 & -\zeta_3^2 & 1 & \zeta_3 & \zeta_3^2 & -\zeta_3 \\ -\zeta_3 & 1 & \zeta_3^2 & \zeta_3 & \zeta_3^2 & 1 & \zeta_3 & -\zeta_3 & -\zeta_3^2 & 1 & -\zeta_3^2 & -\zeta_3^2 & \zeta_3 & 1 & -\zeta_3 & \zeta_3^2 \\ \zeta_3 & \zeta_3^2 & 1 & -\zeta_3 & -\zeta_3 & \zeta_3 & 1 & \zeta_3^2 & -\zeta_3^2 & -\zeta_3^2 & 1 & -\zeta_3^2 & \zeta_3^2 & -\zeta_3 & 1 & \zeta_3 \\ \zeta_3^2 & \zeta_3 & -\zeta_3 & 1 & \zeta_3 & -\zeta_3 & \zeta_3^2 & 1 & -\zeta_3^2 & -\zeta_3^2 & -\zeta_3^2 & 1 & -\zeta_3 & \zeta_3^2 & \zeta_3 & 1 \\ 1 & \zeta_3^2 & -\zeta_3 & \zeta_3 & 1 & -\zeta_3 & \zeta_3 & \zeta_3^2 & 1 & \zeta_3 & \zeta_3^2 & -\zeta_3 & 1 & -\zeta_3^2 & -\zeta_3^2 & -\zeta_3^2 \\ \zeta_3^2 & 1 & \zeta_3 & -\zeta_3 & -\zeta_3 & 1 & \zeta_3^2 & \zeta_3 & \zeta_3 & 1 & -\zeta_3 & \zeta_3^2 & -\zeta_3^2 & 1 & -\zeta_3^2 & -\zeta_3^2 \\ -\zeta_3 & \zeta_3 & 1 & \zeta_3^2 & \zeta_3 & \zeta_3^2 & 1 & -\zeta_3 & \zeta_3^2 & -\zeta_3 & 1 & \zeta_3 & -\zeta_3^2 & -\zeta_3^2 & 1 & -\zeta_3^2 \\ \zeta_3 & -\zeta_3 & \zeta_3^2 & 1 & \zeta_3^2 & \zeta_3 & -\zeta_3 & 1 & -\zeta_3 & \zeta_3^2 & \zeta_3 & 1 & -\zeta_3^2 & -\zeta_3^2 & -\zeta_3^2 & 1 \end{bmatrix},$$

indexed by elements of G ordered lexicographically.

2.1.2 Nested Cyclic Subgroups Construction

Throughout this subsection, 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 $\text{BH}(G, h)$ matrices. We first introduce some notation and prove 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 2.11. *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 $\text{Aut}(G)$ 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). $\square$

We first consider the case of $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ to get a general sense of the group ring structure involved. There are $p+1$ cyclic subgroups of order p for which each of them is contained in p cyclic subgroups of order p^2 by Lemma 2.11(ii). Denote the cyclic subgroups of order p by U_i for $i = 0, \dots, p$. Also, we denote the cyclic subgroups of order p^2 by $U_{i,j}$, for $j = 0, \dots, p-1$, such that each U_i is contained in $U_{i,j}$ for every i, j . Following the

blueprint of the previous construction, we use

$$D = \sum_{i=0}^p \sum_{j=0}^{p-1} \eta_{i,j} U_{i,j} \quad (2.7)$$

(c.f. equation (2.5)) as a starting point, where $\eta_{i,j}$ are roots of unity to be determined. First we observe that G is contained in $\bigcup_{i=0}^p \bigcup_{j=0}^{p-1} U_{i,j}$. So if we view the coefficients a_g , where $g \in G$, as a function of the roots $\eta_{i,j}$, then none of the coefficients a_g is identically equal to 0. Note that this condition is required since if otherwise, the resulting matrix we obtained by $H_{g,k} = a_{gk^{-1}}$ via Result 2.1 will contain entries equal to 0. Hence, the group ring element D is a candidate for a construction of $\text{BH}(G, h)$ and it remains to determine what the roots of unity $\eta_{i,j}$ should be.

Next, we observe that for each i , the subgroup U_i is contained in $U_{i,j}$ for every j and the identity is contained in all $U_{i,j}$'s. So in order for D to be a $\text{BH}(G, h)$ matrix, we require the conditions

$$\sum_{j=0}^{p-1} \eta_{i,j} = \eta_i, \text{ for all } i, \quad \text{and} \quad \sum_{i=0}^p \eta_i = 1, \quad (2.8)$$

where η_i 's are roots of unity. Lastly, we determine the conditions such that $|\chi(D)|^2 = p^4$. Now consider a character χ of G . If χ has order p^2 , then it acts trivially on a unique $U_{i,j}$ and thus $|\chi(D)|^2 = p^4$ by the orthogonality relation (Result 1.8). If χ has order p , then there is a unique i , for all j such that it is trivial on $U_{i,j}$ and so $|\chi(D)|^2 = p^4$ by the first condition of (2.8). Otherwise χ is the trivial character and hence $|\chi(D)|^2 = p^4$ by the second condition of (2.8). Therefore, the group ring D given by (2.7) with conditions (2.8) is a $\text{BH}(\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}, h)$ matrix, where h is the lowest common multiple of the orders of all the $\eta_{i,j}$.

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 2.11, 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

$$\mathcal{C}(G) = \bigcup_U \mathcal{S}(U), \quad (2.9)$$

where U runs over all cyclic subgroups U of G with $1 \leq |U| \leq p^{a-1}$ and the right hand side of (2.9) is a partition of $\mathcal{C}(G)$ into pairwise disjoint subsets.

Theorem 2.12. *Let η_W , $W \in \mathcal{C}(G)$, be complex roots of unity such that*

$$\sum_{W \in \mathcal{S}(U)} \eta_W = \eta_U \quad (2.10)$$

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 $\text{BH}(G, h)$ 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 (2.10) implies

$$\sum_{\substack{W \in \mathcal{M}(a) \\ U \subseteq W}} \eta_W = \eta_U \quad (2.11)$$

for every cyclic subgroup U of G . We prove (2.11) by backward induction on $|U|$. For $|U| = p^a$, the only subgroup in $\mathcal{M}(a)$ containing U is U itself, so (2.11) holds. Now assume that (2.11) holds for all U with $|U| = p^b$ where $1 \leq b \leq a$. Let K be a cyclic subgroup of G of order p^{b-1} . Note that, for any $W \in \mathcal{M}(a)$, we have $K \subseteq W$ if and only if $K' \subseteq W$ for some $K' \in \mathcal{S}(K)$. Since $|K'| = p^b$ for $K' \in \mathcal{S}(K)$, we have

$$\sum_{\substack{W \in \mathcal{M}(a) \\ K' \subseteq W}} \eta_W = \eta_{K'} \quad (2.12)$$

by the inductive assumption. Using (2.10) and (2.12), 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 (2.11).

From the definition of X , it is clear that $X = \sum_{g \in G} a_g g$ with $a_g \in \mathbb{Z}[\zeta_h]$. 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 (2.11), 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 2.11, there is a cyclic subgroup T of G such that the following holds for every $W \in \mathcal{M}(a)$.

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

Moreover, note that $\chi(W) = p^a$ if $W \leq \ker(\chi)$ 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 (2.11). Hence $|\chi(X)|^2 = p^{2a}$ for all characters χ of G . Thus X is a $\text{BH}(G, h)$ matrix by Result 2.1. $\square$

Example 2.13. Let $G = \mathbb{Z}_4 \times \mathbb{Z}_4$ and $h = 6$. We construct a $\text{BH}(\mathbb{Z}_4 \times \mathbb{Z}_4, 6)$ matrix using Theorem 2.12.

Let U be the trivial subgroup, the cyclic subgroup of order 1. For the cyclic subgroups of order 2, we have

$$U_1 = \{(0, 0), (0, 2)\}, \quad U_2 = \{(0, 0), (2, 2)\}, \quad U_3 = \{(0, 0), (2, 0)\},$$

and for the cyclic subgroups of order 4, we have

$$\begin{aligned} U_{1,1} &= \{(0, 0), (0, 1), (0, 2), (0, 3)\}, & U_{1,2} &= \{(0, 0), (2, 1), (0, 2), (2, 3)\}, \\ U_{2,1} &= \{(0, 0), (1, 1), (2, 2), (3, 3)\}, & U_{2,2} &= \{(0, 0), (1, 3), (2, 2), (3, 1)\}, \\ U_{3,1} &= \{(0, 0), (1, 0), (2, 0), (3, 0)\}, & U_{3,2} &= \{(0, 0), (1, 2), (2, 0), (3, 2)\}. \end{aligned}$$

So, we have the subset relations $U \subset U_i \subset U_{i,j}$ for $i = 1, 2, 3$ and $j = 1, 2$. Next, let $\eta_{U_{i,j}} = \eta_{i,j} = (-1)^i \zeta_3^j$. Consequently, we get $\eta_{U_i} = \eta_i = \eta_{i,1} + \eta_{i,2} = (-1)^{i+1}$ and $\eta_U = \sum_{i=1}^3 \eta_i = 1$. Hence, equation (2.10) is satisfied. Using (2.11), we construct the $\text{BH}(G, h)$ matrix

$$\begin{bmatrix} 1 & -\zeta_3 & 1 & -\zeta_3 & \zeta_3 & -\zeta_3 & \zeta_3^2 & -\zeta_3^2 & 1 & -\zeta_3^2 & -1 & -\zeta_3^2 & \zeta_3 & -\zeta_3^2 & \zeta_3^2 & -\zeta_3 \\ -\zeta_3 & 1 & -\zeta_3 & 1 & -\zeta_3^2 & \zeta_3 & -\zeta_3 & \zeta_3^2 & -\zeta_3^2 & 1 & -\zeta_3^2 & -1 & -\zeta_3 & \zeta_3 & -\zeta_3^2 & \zeta_3^2 \\ 1 & -\zeta_3 & 1 & -\zeta_3 & \zeta_3^2 & -\zeta_3^2 & \zeta_3 & -\zeta_3 & -1 & -\zeta_3^2 & 1 & -\zeta_3^2 & \zeta_3^2 & -\zeta_3 & \zeta_3 & -\zeta_3^2 \\ -\zeta_3 & 1 & -\zeta_3 & 1 & -\zeta_3 & \zeta_3^2 & -\zeta_3^2 & \zeta_3 & -\zeta_3^2 & -1 & -\zeta_3^2 & 1 & -\zeta_3^2 & \zeta_3^2 & -\zeta_3 & \zeta_3 \\ \zeta_3 & -\zeta_3^2 & \zeta_3^2 & -\zeta_3 & 1 & -\zeta_3 & 1 & -\zeta_3 & \zeta_3 & -\zeta_3 & \zeta_3^2 & -\zeta_3^2 & 1 & -\zeta_3^2 & -1 & -\zeta_3^2 \\ -\zeta_3 & \zeta_3 & -\zeta_3^2 & \zeta_3^2 & -\zeta_3 & 1 & -\zeta_3 & 1 & -\zeta_3^2 & \zeta_3 & -\zeta_3 & \zeta_3^2 & -\zeta_3^2 & 1 & -\zeta_3^2 & -1 \\ \zeta_3^2 & -\zeta_3 & \zeta_3 & -\zeta_3^2 & 1 & -\zeta_3 & 1 & -\zeta_3 & \zeta_3^2 & -\zeta_3^2 & \zeta_3 & -\zeta_3 & -1 & -\zeta_3^2 & 1 & -\zeta_3^2 \\ -\zeta_3^2 & \zeta_3^2 & -\zeta_3 & \zeta_3 & -\zeta_3 & 1 & -\zeta_3 & 1 & -\zeta_3 & \zeta_3^2 & -\zeta_3^2 & \zeta_3 & -\zeta_3^2 & -1 & -\zeta_3^2 & 1 \\ 1 & -\zeta_3^2 & -1 & -\zeta_3^2 & \zeta_3 & -\zeta_3^2 & \zeta_3^2 & -\zeta_3 & 1 & -\zeta_3 & 1 & -\zeta_3 & \zeta_3 & -\zeta_3 & \zeta_3^2 & -\zeta_3^2 \\ -\zeta_3^2 & 1 & -\zeta_3^2 & -1 & -\zeta_3 & \zeta_3 & -\zeta_3^2 & \zeta_3^2 & -\zeta_3 & 1 & -\zeta_3 & 1 & -\zeta_3^2 & \zeta_3 & -\zeta_3 & \zeta_3^2 \\ -1 & -\zeta_3^2 & 1 & -\zeta_3^2 & \zeta_3^2 & -\zeta_3 & \zeta_3 & -\zeta_3^2 & 1 & -\zeta_3 & 1 & -\zeta_3 & \zeta_3^2 & -\zeta_3^2 & \zeta_3 & -\zeta_3 \\ -\zeta_3^2 & -1 & -\zeta_3^2 & 1 & -\zeta_3^2 & \zeta_3^2 & -\zeta_3 & \zeta_3 & -\zeta_3 & 1 & -\zeta_3 & 1 & -\zeta_3 & \zeta_3^2 & -\zeta_3^2 & \zeta_3 \\ \zeta_3 & -\zeta_3 & \zeta_3^2 & -\zeta_3^2 & 1 & -\zeta_3^2 & -1 & -\zeta_3^2 & \zeta_3 & -\zeta_3^2 & \zeta_3^2 & -\zeta_3 & 1 & -\zeta_3 & 1 & -\zeta_3 \\ -\zeta_3^2 & \zeta_3 & -\zeta_3 & \zeta_3^2 & -\zeta_3^2 & 1 & -\zeta_3^2 & -1 & -\zeta_3 & \zeta_3 & -\zeta_3^2 & \zeta_3^2 & -\zeta_3 & 1 & -\zeta_3 & 1 \\ \zeta_3^2 & -\zeta_3^2 & \zeta_3 & -\zeta_3 & -1 & -\zeta_3^2 & 1 & -\zeta_3^2 & \zeta_3^2 & -\zeta_3 & \zeta_3 & -\zeta_3^2 & 1 & -\zeta_3 & 1 & -\zeta_3 \\ -\zeta_3 & \zeta_3^2 & -\zeta_3^2 & \zeta_3 & -\zeta_3^2 & -1 & -\zeta_3^2 & 1 & -\zeta_3^2 & \zeta_3^2 & -\zeta_3 & \zeta_3 & -\zeta_3 & 1 & -\zeta_3 & 1 \end{bmatrix},$$

indexed by elements of G ordered lexicographically.

For certain values of p and h , equation (2.10) can be satisfied easily via Theorem 1.16,

thus guaranteeing the existence of a $\text{BH}(\mathbb{Z}_{p^a} \times \mathbb{Z}_{p^a}, h)$ matrix by Theorem 2.12.

Corollary 2.14. *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 $\text{BH}(\mathbb{Z}_{p^a} \times \mathbb{Z}_{p^a}, h)$ matrix.*

Proof. Write $G = \mathbb{Z}_{p^a} \times \mathbb{Z}_{p^a}$. By Theorem 2.12, it suffices to show that there are roots of unity $\eta_W \in \mathcal{Q}(h)$, $W \in \mathcal{C}(G)$, such that

$$\sum_{W \in \mathcal{S}(U)} \eta_W = \eta_U \quad (2.13)$$

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 $W_1, \dots, W_{p+1}$ denote these subgroups. We first show that there are $\eta_1, \dots, \eta_{p+1} \in \mathcal{Q}(h)$ with

$$\sum_{i=1}^{p+1} \eta_i = 1. \quad (2.14)$$

If h is odd, then (2.14) has a solution by Theorem 1.16 (ii), since $p \in \mathcal{Q}(h)$ by assumption. If h is even, then $p+2 \in \mathcal{Q}(h)$, as $p \in \mathcal{Q}(h)$ and 2 is a prime divisor of h . Hence (2.14) has a solution by Theorem 1.16 (i). This completes the proof of (2.14). Now set $\eta_{\{1\}} = 1$ and $\eta_{W_i} = \eta_i$ for $i = 1, \dots, p+1$. This solves (2.13) for $U = \{1\}$.

Suppose that η_W 's have been chosen such that (2.13) 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 $\mu_1, \dots, \mu_p \in \mathcal{Q}(h)$ with $\sum_{i=1}^p \mu_i = 1$. Now let U be any cyclic subgroup of G with $|U| = p^{b+1}$ and let $K_1, \dots, K_p$ the subgroups in $\mathcal{S}(U)$. Setting $\eta_{K_i} = \mu_i \eta_U$ for $i = 1, \dots, p$ solves (2.13) for U . Since the sets $\mathcal{S}(U)$ are pairwise disjoint, we can thus solve (2.13) for all cyclic subgroups U of G with $|U| = p^{b+1}$. This shows that (2.13) has a solution. $\square$

2.1.3 Recursive Subspace Construction

In this subsection, we give a recursive construction for $\text{BH}(\mathbb{Z}_{p^a} \times (\mathbb{Z}_p)^a, h)$ matrices. Let G_a be the group $\mathbb{Z}_{p^a} \times (\mathbb{Z}_p)^a$ and write $G_a = \langle \alpha \rangle \times \langle \beta \rangle \times \langle \gamma_1 \rangle \times \cdots \times \langle \gamma_{a-1} \rangle$ such that the order of α is p^a and the orders of β, γ_i , for $i = 1, \dots, a-1$, are p . Let $W = \langle \alpha^{p^{a-1}}, \beta, \gamma_1, \dots, \gamma_{a-1} \rangle$ be a subgroup of G_a of order p^{a+1} and let $U = \langle \alpha^{p^{a-1}} \rangle$ be a subgroup of G of order p .

We view W as a vector space of dimension $(a+1)$ over $\mathbb{F}_p$ and U as a 1-dimensional subspace of W . Recall that if V is a vector space of dimension a , then the **hyperplanes** of V are the $(a-1)$ dimensional subspaces of V . Furthermore, let S be the hyperplane of W with basis $\{\alpha^{p^{a-1}}, \gamma_1, \dots, \gamma_{a-1}\}$. Note that S contains U .

The following results on hyperplanes are well-known. See [27, Chapter 3, Theorem 3.1.1] for instance. We provide proofs of the following results here for the convenience of the reader.

Result 2.15. *Let $q = p^a$ be a prime power and V be a vector space of dimension n over $\mathbb{F}_q$. The number of k -dimensional subspaces of V is $\binom{n}{k}_q$, where $\binom{n}{k}_q$ is the Gaussian binomial coefficient given by*

$$\binom{n}{k}_q = \begin{cases} \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}, & \text{if } k \leq n, \\ 0, & \text{if } k > n. \end{cases}$$

Proof. This follows by counting the number of ways we can choose the basis of the subspace divided by the number of sets of basis vectors which we can choose to generate that subspace. The number of unordered sets with k vectors contained in V is

$$\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{k!}.$$

On the other hand, the number of unordered sets with k vectors contained in a k -dimensional subspace of V is

$$\frac{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}{k!}.$$

Therefore the number of k -dimensional subspace of V is

$$\frac{\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{k!}}{\frac{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}{k!}} = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

□

Lemma 2.16. *Suppose that V is a vector space of dimension n over $\mathbb{F}_q$ and U is a k -dimensional subspace of V . Then the number of m -dimensional subspaces of V containing U is $\binom{n-k}{m-k}_q$.*

Proof. Let $\mathcal{G}$ be the set of subspaces of V containing U and $\mathcal{S}$ be the set of subspaces of V/U . Note that there is a one-to-one correspondence between $\mathcal{G}$ and $\mathcal{S}$ and is given explicitly by the map $\phi(W) = W/U$, where $W \in \mathcal{G}$. Furthermore, W is an m -dimensional subspace of V if and only if W/U is an $(m-k)$ -dimensional subspace of V/U . Lastly, observe that V/U is a vector space of dimension $n-k$ and the lemma then follows. □

Corollary 2.17. *Suppose that W is a vector space of dimension n over $\mathbb{F}_p$ and U is a 1-dimensional subspace of W .*

1. *There are p^{n-1} subspaces of W of dimension $n-1$ not containing U .*
2. *If L is a $(n-2)$ -dimensional subspace of W not containing U , then there are p subspaces of W of dimension $n-1$ which contain L but not U .*

Proof. 1. We note that $\binom{n}{k}_p = \binom{n}{n-k}_p$ and $\binom{n}{1}_p = p^{n-1} + p^{n-2} + \cdots + 1$. So the number of subspaces of W of dimension $n-1$ not containing U is $\binom{n}{n-1}_p - \binom{n-1}{n-2}_p = p^{n-1}$.

2. First, the number of $(n-1)$ -dimensional subspaces containing L is $\binom{2}{1}_p = p+1$. If V is a subspace of dimension $n-1$ which contains L and U , then it must contain $L \oplus U$. Since $L \cap U = \{1\}$, the direct sum $L \oplus U$ has dimension $n-1$. So there is only one possible choice of V .

□

By the first part of Corollary 2.17, there are p^{a-1} hyperplanes of S not containing U which we will label as $L_0, \dots, L_{p^{a-1}-1}$. And each these L_i is contained in exactly p

hyperplanes of W , which do not contain U by the second part of Corollary 2.17. We label them as $V_{i,0}, \dots, V_{i,p-1}$. Note that all the $V_{i,j}$'s are distinct since if a hyperplane contains L_{i_1} and L_{i_2} , then it must contain S and thus U . Furthermore, these are all the hyperplanes of W not containing U . Lastly, let $R = \langle \gamma_1, \dots, \gamma_{a-1} \rangle$ and note that $S = RU$.

Theorem 2.18. *Suppose that $\zeta_{i,j}$ are roots of unity satisfying*

$$\sum_{j=0}^{p-1} \zeta_{i,j} = 0, \quad \text{for } i = 0, \dots, p^{a-1} - 1. \quad (2.15)$$

For $i = 0, \dots, p^{a-1} - 1$ and $g \in R$, suppose that $\eta_{i,g}$ are 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 $\text{BH}(G_{a-1}, h)$ matrix. Then

$$X := \sum_{i=0}^{p^{a-1}-1} \left(\sum_{j=0}^{p-1} \zeta_{i,j} V_{i,j} g_i + \sum_{g \in R} \eta_{i,g} U g \right) \alpha^i \beta^{ki}, \quad (2.16)$$

is a $\text{BH}(G_a, h)$ matrix, where $g_i \in R$, k is an integer and h is the lowest common multiple the orders of $\zeta_{i,j}$'s and $\eta_{i,g}$'s.

Proof. We first show that X has the form $\sum_{x \in G} a_x x$, where each a_x is a root of unity. We claim that for each $i = 0, \dots, p^{a-1} - 1$, we have $\bigcup_{j=0}^{p-1} (V_{i,j} \setminus L_i) = W \setminus S$. Indeed this is the case as $\bigcup_{j=0}^{p-1} (V_{i,j} \setminus L_i) \subseteq W \setminus S$ and since the $V_{i,j}$'s are distinct, we have

$$\left| \bigcup_{j=0}^{p-1} (V_{i,j} \setminus L_i) \right| = p(p^a - p^{a-1}) = p^{a+1} - p^a = |W \setminus S|.$$

In other words, each $x \in (W \setminus S) \alpha^i \beta^{ki}$ is contained in just one of $V_{i,j} g_i \alpha^i \beta^{ki}$ for some j . Thus we have $a_x = \zeta_{i,j}$. In the case that $x \in (S \setminus L_i) g_i \alpha^i \beta^{ki}$, then it is contained in just one of $U g \alpha^i \beta^{ki}$ for some $g \in R$ and hence $a_x = \eta_{i,g}$. Lastly if $x \in L_i g_i \alpha^i \beta^{ki}$, then it is contained in $V_{i,j} g_i \alpha^i \beta^{ki}$ for $j = 0, \dots, p-1$ and also in $U g \alpha^i \beta^{ki}$ for some $g \in R$. So we

have $a_x = \sum_{j=0}^{p-1} \zeta^{i,j} + \eta_{i,g} = \eta_{i,g}$.

Next, we show that $|\chi(X)|^2 = p^{2a}$ for all characters χ of G . Suppose that χ is a character of G such that $\chi \in W^\perp$. Then it 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 p^{a-1} . So we have

$$\chi(X) = \sum_{i=0}^{p^{a-1}-1} \left(\sum_{j=0}^{p-1} \zeta_{i,j} |V_{i,j}| + \sum_{g \in R} \eta_{i,g} |U| \right) \chi(\alpha)^i = p \sum_{i=0}^{p^{a-1}-1} \sum_{g \in R} \eta_{i,g} \tau(h)^i = p\tau(Y),$$

where τ is a character of $\mathbb{Z}_{p^{a-1}} \times \mathbb{Z}_p^{a-1}$ such that $\tau(h) = \chi(\alpha)$ and $\tau(\gamma_i) = 1$ for $i = 1, \dots, a-1$. Hence $|\chi(X)|^2 = p^2 |\tau(Y)| = p^{2a}$.

Now, suppose that $\chi \in \widehat{G} \setminus W^\perp$. Then χ is trivial on exactly one of the hyperplanes of W , say V . If $V = V_{i,j}$ for some i, j , then it is nontrivial on U since if otherwise, then χ would be trivial on W as $W = V_{i,j}U$. 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 $|\chi(X)|^2 = p^{2a}$.

On the other hand if $V \neq V_{i,j}$ for all i, j , then U is contained in V and thus χ is trivial on U . Note that in this case, $\chi(\alpha)$ is again root of unity of order p^{a-1} . Consider the character τ of $\mathbb{Z}_{p^{a-1}} \times \mathbb{Z}_p^{a-1}$ defined by $\tau(h) = \chi(\alpha \beta^k)$ and $\tau(\gamma_i) = 1$ for $i = 1, \dots, a-1$. Then,

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

Hence $|\chi(X)|^2 = p^2 |\tau(Y)| = p^{2a}$ and this concludes the proof. $\square$

From Result 2.18 and Theorem 1.12 we get the following:

Corollary 2.19. *Suppose that $p \in \mathcal{Q}(h)$. Then there exists a $\text{BH}(G_a, h)$ matrix for all positive integers a .*

We remark that even though the hyperplane construction for $\text{BH}(\mathbb{Z}_p \times \mathbb{Z}_p, h)$ matrices appears different from the previous two constructions, it gives an equivalent group ring

element. Recall that the two former constructions for $\text{BH}(\mathbb{Z}_p \times \mathbb{Z}_p)$ matrices are given as

$$\sum_{i=0}^p \eta_i U_i, \text{ under the condition that } \sum_{i=0}^{p-1} \eta_i = 1, \quad (2.17)$$

where U_i are the subgroups of order p and η_i are roots of unity. If we fix $a = 1$ in Theorem 2.18, we have $W = G_1 = \mathbb{Z}_p \times \mathbb{Z}_p$, which we will write as $\langle \alpha \rangle \times \langle \beta \rangle$, and $S = U = \langle \alpha \rangle$. Then there is just 1 hyperplane of S not containing U , namely the trivial subspace, which we denote as L_0 . Next, the p subspaces of G_1 , given by $V_{0,0}, \dots, V_{0,p-1}$, containing L_0 but not U , are the other p subgroups of order p . We rewrite these as $U_0, \dots, U_{p-1}$. Lastly, note that R is also the trivial subgroup in this case. Then the equation (2.16) gives

$$X = \sum_{j=0}^{p-1} \zeta_{0,j} V_{0,j} + \eta_{0,1_G} U = \sum_{i=0}^p \eta_i U_i,$$

where $U_i = V_{0,i}$, $\zeta_{0,j} = \eta_i$ for $i = 0, \dots, p-1$ and $U_p = U$, $\eta_p = \eta_{0,1_G}$. Furthermore, we also have $\sum_{i=0}^{p-1} \eta_i = \eta_p$ from (2.15) and thus X is equivalent to the group ring element given by (2.17).

For the case of $\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p$, which we will write as $\langle \alpha \rangle \times \langle \beta \rangle \times \langle \gamma \rangle$, a similar construction with a different condition exist. Using the same notations as before, we have the following:

Theorem 2.20. *Suppose that $\xi, \zeta_{i,j}$ are roots of unity satisfying*

$$\sum_{j=0}^{p-1} \zeta_{0,j} = 1 - \xi \quad \text{and} \quad \sum_{j=0}^{p-1} \zeta_{i,j} = 0, \quad \text{for } i = 1, \dots, p-1, \quad (2.18)$$

For each $i, k = 1, \dots, p-1$, suppose that $\eta_{i,k}$ are roots of unity such that $\eta_{0,k} = \eta$ with the condition that $\eta = \xi$ if $\xi \neq 1$ and

$$Y := \langle \gamma \rangle + \sum_{i=1}^{p-1} \sum_{k=0}^{p-1} \eta_{i,k} \alpha^{pi} \gamma^k \quad (2.19)$$

is a $\text{BH}(\mathbb{Z}_p \times \mathbb{Z}_p, h)$ matrix in the form given by Theorem 2.4. Let

$$e_i = \begin{cases} \lambda i + \mu, & \text{if } i \neq 0, \\ 0, & \text{otherwise,} \end{cases} \quad (2.20)$$

where λ, μ are integers, and f_i be an integer, for $i = 0, \dots, p-1$. Then

$$X := \sum_{i=0}^{p-1} \left(\sum_{j=0}^{p-1} \zeta_{i,j} V_{i,j} \gamma^{f_i} + \sum_{k=0}^{p-1} \eta_{i,k} U \gamma^k \right) \alpha^i \beta^{e_i}, \quad (2.21)$$

is a $\text{BH}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p, h)$ matrix, and h is the lowest common multiple the orders of $\zeta_{i,j}$'s and $\eta_{i,j}$'s.

Proof. As before, we show that X has the form $\sum_{x \in G} a_x x$, where each a_x is a root of unity. Most of the proof is the same if we replace β^{ki} with β^{e_i} as before, except that the computation of a_x , where $x \in L_i g_i \alpha^i \beta^{e_i}$, is different. Instead, we compute that

$$a_x = \sum_{j=0}^{p-1} \zeta_{i,j} + \eta_{i,k} = \begin{cases} \eta_{i,k}, & \text{if } i \neq 0 \text{ or } \xi = 1, \\ 1, & \text{otherwise.} \end{cases}$$

Before we show that $|\chi(X)|^2 = p^4$ for all characters χ of G , we make the following observation. For any roots of unity ζ_1 and ζ_2 , define

$$Y_{\zeta_1, \zeta_2} := \zeta_1 \langle \gamma \rangle + \sum_{i=1}^{p-1} \sum_{k=0}^{p-1} \zeta_2 \eta_{i,k} \alpha^{pi} \gamma^k.$$

By (2.18) and Theorem 2.4, we have

$$\sum_{k=1}^{p-1} \eta_{i,k} = 0 \text{ for } i > 0 \quad \text{and} \quad \eta_{i_1, j_1} = \eta_{i_2, j_2} \text{ if } i_1 j_2 \equiv i_2 j_1 \pmod{p}.$$

Thus $\zeta_1 + \sum_{k=1}^{p-1} \zeta_2 \eta_{1,k} = \zeta_1$ and hence Y_{ζ_1, ζ_2} is in the form (2.5). In other words for any character τ of $\mathbb{Z}_p \times \mathbb{Z}_p = \langle \alpha^{pi} \rangle \times \langle \gamma \rangle$, we have $|\tau(Y_{\zeta_1, \zeta_2})|^2 = p^2$.

Suppose that χ is a character of G such that $\chi \in W^\perp$. Then it is trivial on all $V_{i,j}$'s and on U . Furthermore, we have $\chi(\beta) = \chi(\gamma) = 1$ and $\chi(\alpha)$ is a root of unity of order p . Let τ be a character of $\mathbb{Z}_p \times \mathbb{Z}_p$ such that $\tau(\gamma) = \chi(\alpha)$ and $\tau(\alpha^{p^i}) = 1$. So we have

$$\chi(X) = \sum_{i=0}^{p-1} \left(\sum_{j=0}^{p-1} \zeta_{i,j} |V_{i,j}| + \sum_{k=0}^{p-1} \eta_{i,k} |U| \right) \chi(\alpha)^i = p \left(p\xi_0 + \sum_{i=1}^{p-1} \sum_{k=0}^{p-1} \eta_{i,k} \tau(\gamma)^i \right) = p\tau(Y_{\xi_0,1}),$$

where $\xi_0 = 1$ or η . Hence $|\chi(X)|^2 = p^4$.

Now, suppose that $\chi \in \widehat{G} \setminus W^\perp$. Then χ is trivial on exactly one of the hyperplanes of W , say V . If $V = V_{i,j}$ for some i, j , then it is nontrivial on U since if otherwise, then χ would be trivial on W as $W = V_{i,j}U$. Hence $\chi(X) = |V_{i,j}| \zeta_{i,j} \chi(\gamma^{f_i} \alpha^i \beta^{e_i})$ and thus $|\chi(X)|^2 = p^4$.

On the other hand if $V \neq V_{i,j}$ for all i, j , then U is contained in V and thus χ is trivial on U . Note that in this case, $\chi(\alpha)$ is again a root of unity of order p . Consider the character τ of $\mathbb{Z}_p \times \mathbb{Z}_p$ defined by $\tau(h) = \chi(\alpha \beta^k)$ and $\tau(\gamma) = \chi(\gamma)$ and write $\xi_0 = \chi(\beta^k)$. Then,

$$\begin{aligned} \chi(X) &= \sum_{i=0}^{p-1} \sum_{k=0}^{p-1} \eta_{i,k} |U| \chi(\gamma^k) \chi(\alpha^i \beta^{e_i}) \\ &= p \left(p\xi + \sum_{i=1}^{p-1} \sum_{k=0}^{p-1} \eta_{i,k} \tau(\gamma)^k \tau(h)^i \xi_0 \right) = p\tau(Y_{\xi, \xi_0}). \end{aligned}$$

Hence $|\chi(X)|^2 = p^2 |\tau(Y_{\xi, \xi_0})| = p^4$. This concludes the proof. $\square$

Example 2.21. Let $G = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, and h be any positive integer at least 2, and $\xi = \zeta_h$. We construct a $\text{BH}(G, \text{lcm}(2, h))$ matrix using Theorem 2.20.

First of all, we have $\alpha = (1, 0, 0)$, $\beta = (0, 1, 0)$, $\gamma = (0, 0, 1)$. Recall that $W = \langle (2, 0, 0), (0, 1, 0), (0, 0, 1) \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is viewed as a 3-dimensional vector space over $\mathbb{Z}_2$ with the planes $S = \{(0, 0, 0), (0, 0, 1), (2, 0, 0), (2, 0, 1)\}$ and $U = \{(0, 0, 0), (2, 0, 0)\}$. The planes of S not containing U are $L_0 = \{(0, 0, 0), (0, 0, 1)\}$ and $L_1 = \{(0, 0, 0), (2, 0, 1)\}$.

Then for $i, j = 0, 1$, the planes $V_{i,j}$ of W containing L_i but not U are

$$\begin{aligned} V_{0,0} &= \{(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1)\}, & V_{0,1} &= \{(0, 0, 0), (0, 0, 1), (2, 1, 0), (2, 1, 1)\}, \\ V_{1,0} &= \{(0, 0, 0), (2, 0, 1), (0, 1, 0), (2, 1, 1)\}, & V_{1,1} &= \{(0, 0, 0), (2, 0, 1), (2, 1, 0), (0, 1, 1)\}. \end{aligned}$$

For the roots of unity, let $(\zeta_{0,0}, \zeta_{0,1}, \zeta_{1,0}, \zeta_{1,1}) = (1, -\xi, \xi, -\xi)$ and $(\eta_{0,0}, \eta_{0,1}, \eta_{1,0}, \eta_{1,1}) = (\xi, \xi, \xi, -\xi)$. It is straightforward to verify that conditions (2.18) and (2.19) are satisfied. For the sake of simplicity, we let $f_i = e_i = 0$ for all i . We then use (2.21) to construct the $\text{BH}(\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, h)$ matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \xi & -\xi & -\xi & \xi & \xi & \xi & -\xi & -\xi & \xi & -\xi & \xi & -\xi \\ 1 & 1 & 1 & 1 & -\xi & \xi & \xi & -\xi & \xi & \xi & -\xi & -\xi & -\xi & \xi & -\xi & \xi \\ 1 & 1 & 1 & 1 & -\xi & \xi & \xi & -\xi & -\xi & -\xi & \xi & \xi & \xi & -\xi & \xi & -\xi \\ 1 & 1 & 1 & 1 & \xi & -\xi & -\xi & \xi & -\xi & -\xi & \xi & \xi & -\xi & \xi & -\xi & \xi \\ \xi & -\xi & \xi & -\xi & 1 & 1 & 1 & 1 & \xi & -\xi & -\xi & \xi & \xi & \xi & -\xi & -\xi \\ -\xi & \xi & -\xi & \xi & 1 & 1 & 1 & 1 & -\xi & \xi & \xi & -\xi & \xi & \xi & -\xi & -\xi \\ \xi & -\xi & \xi & -\xi & 1 & 1 & 1 & 1 & -\xi & \xi & \xi & -\xi & -\xi & -\xi & \xi & \xi \\ -\xi & \xi & -\xi & \xi & 1 & 1 & 1 & 1 & \xi & -\xi & -\xi & \xi & -\xi & -\xi & \xi & \xi \\ \xi & \xi & -\xi & -\xi & \xi & -\xi & \xi & -\xi & 1 & 1 & 1 & 1 & \xi & -\xi & -\xi & \xi \\ \xi & \xi & -\xi & -\xi & -\xi & \xi & -\xi & \xi & 1 & 1 & 1 & 1 & -\xi & \xi & \xi & -\xi \\ -\xi & -\xi & \xi & \xi & \xi & -\xi & \xi & -\xi & 1 & 1 & 1 & 1 & -\xi & \xi & \xi & -\xi \\ -\xi & -\xi & \xi & \xi & -\xi & \xi & -\xi & \xi & 1 & 1 & 1 & 1 & \xi & -\xi & -\xi & \xi \\ \xi & -\xi & -\xi & \xi & \xi & \xi & -\xi & -\xi & \xi & -\xi & \xi & -\xi & 1 & 1 & 1 & 1 \\ -\xi & \xi & \xi & -\xi & \xi & \xi & -\xi & -\xi & -\xi & \xi & -\xi & \xi & 1 & 1 & 1 & 1 \\ -\xi & \xi & \xi & -\xi & -\xi & -\xi & \xi & \xi & \xi & -\xi & \xi & -\xi & 1 & 1 & 1 & 1 \\ \xi & -\xi & -\xi & \xi & -\xi & -\xi & \xi & \xi & -\xi & \xi & -\xi & \xi & 1 & 1 & 1 & 1 \end{bmatrix},$$

indexed by elements of G ordered lexicographically.

2.2 Constructions using Folding and Permutation Theorems

In [23], Hagita and Schmidt showed that there were bijections between groups that we can extend to group rings such that the character values are preserved. These are the so-called folding and permutation theorems [23, Thm 4.6 and 5.2]. Since difference sets were the focus of the study, the theorems were formulated for the group rings $\mathbb{Z}[G]$. In this subsection, we extend the folding and permutation theorems to the group rings $\mathbb{Z}[\zeta_h][G]$. We can then apply them to our constructions to obtain more Butson Hadamard matrices.

2.2.1 Folding Theorem

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

Lemma 2.22. *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

$$\chi(D) = \chi(D_j \alpha^j) \text{ and } \chi(D_i) = 0 \text{ for all } i \neq j. \quad (2.22)$$

Proof. Note that $\chi(\alpha)$ is a primitive p^b th 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

$$\sum_{i=0}^{p^{b-1}-1} \chi(D_i) \zeta_{p^b}^i = \sum_{i=0}^{p^{b-1}-1} \chi(D_i) \chi(\alpha)^i = \chi(D) = \mu m = (\pm \zeta_k^w m) \zeta_{p^b}^u. \quad (2.23)$$

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 (2.23) that $\chi(D_i) = 0$ whenever $i \not\equiv u \pmod{p^{b-1}}$. Hence $\chi(D) = \chi(D_j \alpha^i)$ by (2.23) where j is the unique index with $j \equiv u \pmod{p^{b-1}}$. This completes the proof of (2.22). $\square$

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 $\mathbb{Z}_{p^{t_i}} = \langle \alpha_i \rangle$, $i = 1, \dots, s$. 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 $\mathbb{Z}_{p^a} = \{1, \alpha, \dots, \alpha^{p^a-1}\}$. For $n = 0, \dots, p^a - 1$, let $f(\alpha^n)$ be the n^{th} element of P in the lexicographical order. We call the bijection $f : \mathbb{Z}_{p^a} \rightarrow P, \alpha^n \mapsto f(\alpha^n)$ 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 $\mathbb{Z}_{p^a} \times H \rightarrow P \times H$ 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

$$f(X) = \sum_{g \in G} a_g f(g). \quad (2.24)$$

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

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

for some l and some $r \in \{1, \dots, s\}$. The following is proved in [23, Lem. 4.1, 4.3].

Result 2.23. *Let p be a prime, let a be a positive integer, and let α be a generator of $\mathbb{Z}_{p^a}$. Suppose that $f : \mathbb{Z}_{p^a} \times H \rightarrow P \times H$ 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 [23, Thm. 4.6], but we include it for the convenience of the reader, as the setting is slightly different.

Theorem 2.24. *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 $\text{BH}(G, h)$ matrix X such that*

$$\chi(X) = \mu_\chi p^a \text{ for some root of unity } \mu_\chi \text{ for all characters } \chi \text{ of } G. \quad (2.25)$$

Let P be any abelian p -group of order p^a and let $f : G \rightarrow P \times H$ be the corresponding folding. Then $f(X)$ is a $\text{BH}(P \times H, h)$ 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 $\mathcal{U}(h)$. By Result 2.1, it remains to show

$$|\chi(f(X))|^2 = |P \times H| \quad (2.26)$$

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 (2.26) 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 2.23 (b), there is a character τ of G such that

$$\tau(x) = \chi(f(x)) \text{ for all } x \in W \times H \quad (2.27)$$

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 (2.24) and (2.27), we get

$$\chi(f(Y)) = \sum_{x \in W \times H} a_x \chi(f(x)) = \sum_{x \in W \times H} a_x \tau(x) = \tau(Y). \quad (2.28)$$

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

$$\chi(f(X_i)) = \tau(X_i) \quad (2.29)$$

for all i by (2.28). Moreover, by (2.25) and Lemma 2.22, there is a j such that

$$\tau(X) = \tau(X_j \alpha^j) \text{ and } \tau(X_i) = 0 \text{ for all } i \neq j. \quad (2.30)$$

Fix i with $0 \leq i \leq p^{b-1} - 1$ and write $X_i = \sum_{w \in W} \sum_{k \in H} a_{w,k} w k$ 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 2.23 (a), we have $f(\alpha^i w) = f(\alpha^i) f(w)$ for all $w \in W$ and thus

$$\begin{aligned} f(X_i \alpha^i) &= \sum_{w \in W} \sum_{k \in H} a_{w,k} f(wk \alpha^i) = \sum_{w \in W} \sum_{k \in H} a_{w,k} f(w \alpha^i) k \\ &= \sum_{w \in W} \sum_{k \in H} a_{w,k} f(w) f(\alpha^i) k = \left(\sum_{w \in W} \sum_{k \in H} a_{w,k} f(wk) \right) f(\alpha^i) \\ &= f(X_i) f(\alpha^i). \end{aligned} \quad (2.31)$$

Using (2.29), (2.30), and (2.31), 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 (2.26). $\square$

Corollary 2.25. *Let p be a prime and let a, h be positive integers with $p \in \mathcal{Q}(h)$. Then $\text{BH}(P \times \mathbb{Z}_p^a, h)$ matrix exists for every abelian group P of order p^a .*

Proof. By Corollary 2.19 there is a $\text{BH}(\mathbb{Z}_{p^a} \times \mathbb{Z}_p^a, h)$ matrix. The proof of Theorem 2.18 shows that this matrix satisfies condition (2.25). Hence there is a $\text{BH}(P \times \mathbb{Z}_p^a, h)$ matrix by Theorem 2.24. $\square$

Example 2.26. We use Theorem 2.24 on the $\text{BH}(G, \text{lcm}(2, h))$ matrix from Example 2.21 to obtain a $\text{BH}(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \text{lcm}(2, h))$ matrix and we assume that 4 does not divide h . The p -folding from $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is given by

$$\begin{aligned} (0, 0, 0) &\mapsto (0, 0, 0, 0) & (0, 0, 1) &\mapsto (0, 0, 0, 1) & (0, 1, 0) &\mapsto (0, 0, 1, 0) & (0, 1, 1) &\mapsto (0, 0, 1, 1) \\ (1, 0, 0) &\mapsto (0, 1, 0, 0) & (1, 0, 1) &\mapsto (0, 1, 0, 1) & (1, 1, 0) &\mapsto (0, 1, 1, 0) & (1, 1, 1) &\mapsto (0, 1, 1, 1) \\ (2, 0, 0) &\mapsto (1, 0, 0, 0) & (2, 0, 1) &\mapsto (1, 0, 0, 1) & (2, 1, 0) &\mapsto (1, 1, 1, 0) & (2, 1, 1) &\mapsto (1, 0, 1, 1) \\ (3, 0, 0) &\mapsto (1, 1, 0, 0) & (3, 0, 1) &\mapsto (1, 1, 0, 1) & (3, 1, 0) &\mapsto (1, 1, 1, 0) & (3, 1, 1) &\mapsto (1, 1, 1, 1). \end{aligned}$$

Then, we obtain the $\text{BH}(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \text{lcm}(2, h))$ matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \xi & -\xi & \xi & -\xi & \xi & \xi & -\xi & -\xi & \xi & -\xi & -\xi & \xi \\ 1 & 1 & 1 & 1 & -\xi & \xi & -\xi & \xi & \xi & \xi & -\xi & -\xi & -\xi & \xi & \xi & -\xi \\ 1 & 1 & 1 & 1 & \xi & -\xi & \xi & -\xi & -\xi & -\xi & \xi & \xi & -\xi & \xi & \xi & -\xi \\ 1 & 1 & 1 & 1 & -\xi & \xi & -\xi & \xi & -\xi & -\xi & \xi & \xi & \xi & -\xi & -\xi & \xi \\ \xi & -\xi & \xi & -\xi & 1 & 1 & 1 & 1 & \xi & -\xi & -\xi & \xi & \xi & \xi & -\xi & -\xi \\ -\xi & \xi & -\xi & \xi & 1 & 1 & 1 & 1 & -\xi & \xi & \xi & -\xi & \xi & \xi & -\xi & -\xi \\ \xi & -\xi & \xi & -\xi & 1 & 1 & 1 & 1 & -\xi & \xi & \xi & -\xi & -\xi & -\xi & \xi & \xi \\ -\xi & \xi & -\xi & \xi & 1 & 1 & 1 & 1 & \xi & -\xi & -\xi & \xi & -\xi & -\xi & \xi & \xi \\ \xi & \xi & -\xi & -\xi & \xi & -\xi & -\xi & \xi & 1 & 1 & 1 & 1 & \xi & -\xi & \xi & -\xi \\ \xi & \xi & -\xi & -\xi & -\xi & \xi & \xi & -\xi & 1 & 1 & 1 & 1 & -\xi & \xi & -\xi & \xi \\ -\xi & -\xi & \xi & \xi & -\xi & \xi & \xi & -\xi & 1 & 1 & 1 & 1 & \xi & -\xi & \xi & -\xi \\ -\xi & -\xi & \xi & \xi & \xi & -\xi & -\xi & \xi & 1 & 1 & 1 & 1 & -\xi & \xi & -\xi & \xi \\ \xi & -\xi & -\xi & \xi & \xi & \xi & -\xi & -\xi & \xi & -\xi & \xi & -\xi & 1 & 1 & 1 & 1 \\ -\xi & \xi & \xi & -\xi & \xi & \xi & -\xi & -\xi & -\xi & \xi & -\xi & \xi & 1 & 1 & 1 & 1 \\ -\xi & \xi & \xi & -\xi & -\xi & -\xi & \xi & \xi & \xi & -\xi & \xi & -\xi & 1 & 1 & 1 & 1 \\ \xi & -\xi & -\xi & \xi & -\xi & -\xi & \xi & \xi & -\xi & \xi & -\xi & \xi & 1 & 1 & 1 & 1 \end{bmatrix}.$$

2.2.2 Permutation Theorem

When the group P is $\mathbb{Z}_{p^a}$, the p -folding is the identity map. In this context, we consider U -permutations instead.

Definition 2.27. Let $G = \mathbb{Z}_{p^a} \times T$ be an abelian group where $a \geq 2$ and with $T = \mathbb{Z}_p^a$. Let U be a subgroup of $\mathbb{Z}_{p^a}$ of order at least p^2 . Let $X \in \mathbb{Z}[\zeta_h][G]$ and write

$$X = \sum_{i=0}^{p^a/|U|-1} g_i U_i, \quad (2.32)$$

where $U_i \in \mathbb{Z}[\zeta_h][U \times T]$ and $\{g_i\}$ is a complete set of coset representatives of $U \times T$ in G . For each i , let σ_i be an automorphism of $U \times T$ such that $\sigma_i|_T$ is the identity and $\sigma_i|_U$

has order p . Then

$$P_\sigma(X) := \sum_{i=0}^{p^a/|U|-1} g_i \sigma_i(U_i),$$

is called a **U -permutation** of X , where each σ_i is extended linearly to the group ring element U_i .

Given $X = \sum_{g \in G} c_g g \in \mathbb{Z}[\zeta_h][G]$, note that we can write $c_g = \sum_{i=0}^{h-1} d_{i,g} \zeta_h^i$, where $d_{i,g} \in \mathbb{Z}$. Define the group ring element $D_X \in \mathbb{Z}[G \times \mathbb{Z}_h]$ obtained from X by $D_X = \sum_{g \in G} \sum_{i=0}^{h-1} d_{i,g} \alpha^i g$, where α is the generator of $\mathbb{Z}_h$. This has the effect of replacing each occurrence of ζ_h with α . The usefulness of this replacement comes from the fact that every character value $\chi(X)$, where $\chi \in \widehat{G}$, can be represented as $\varphi(D_X)$, where $\varphi \in \widehat{G \times \mathbb{Z}_h}$ such that $\varphi|_G = \chi$ and $\varphi(\alpha) = \zeta_h$. We call φ the **ζ_h -extension of χ** . Conversely if φ is any character with $\varphi(\alpha) = \zeta_h$, then $\varphi(D_X) = \varphi|_G(X)$.

Let $X \in \mathbb{Z}[\zeta_h][G]$ be given as in (2.32) and thus $D_X = \sum_{i=0}^{p^a/|U|-1} g_i D_{U_i}$. Suppose that $P_\sigma(X)$ is a U -permutation of X with the associated automorphisms σ_i 's of $U \times T$. For each i , let π_i be the extension of σ_i to the group $U \times T \times \mathbb{Z}_h$ by $\pi_i(g\alpha^j) = \sigma_i(g)\alpha^j$, where $g \in U \times T$ and α is a generator of $\mathbb{Z}_h$. Then π_i is an automorphism such that $\pi_i|_{T \times \mathbb{Z}_h}$ is the identity and $\pi_i|_U = \sigma_i|_U$ has order p . So $P_\pi(D_X)$ is a U -permutation of D_X . Write $U_i = \sum_{g \in U \times T} \sum_{j=0}^{h-1} d_{i,j,g} \zeta_h^j g$, where $d_{i,j,g} \in \mathbb{Z}$ and $U_i^{\sigma_i} = \sigma_i(U_i)$. If χ is a character of G and φ is a ζ_h -extension of χ , then

$$\begin{aligned} \chi(U_i^{\sigma_i}) &= \sum_{g \in U \times T} \sum_{j=0}^{h-1} d_{i,j,g} \zeta_h^j \chi(\sigma_i(g)) = \sum_{g \in U \times T} \sum_{j=0}^{h-1} d_{i,j,g} \varphi(\alpha^j) \varphi(\sigma_i(g)) \\ &= \sum_{g \in U \times T} \sum_{j=0}^{h-1} d_{i,j,g} \varphi(\alpha^j \sigma_i(g)) = \sum_{g \in U \times T} \sum_{j=0}^{h-1} d_{i,j,g} \varphi(\pi_i(\alpha^j g)) = \varphi(D_{U_i}^{\pi_i}). \end{aligned}$$

Hence, we have $\chi(P_\sigma(X)) = \varphi(P_\pi(D_X))$. Furthermore if X is a $\text{BH}(G, h)$ matrix given by Theorem 2.18 or 2.20, then for all characters τ of G , we have $\tau(X) = \mu p^a$ for some root of unity μ . Supposing that the other assumptions of [23, Theorem 5.2] also hold, we can conclude that

$$\chi(P_\sigma(X)) = \varphi(P_\pi(D_X)) = \eta \tau(D_X),$$

for some character $\tau \in \widehat{G \times \mathbb{Z}_h}$. Note that in the proof of [23, Theorem 5.2], the character τ satisfies $\tau(\alpha) = \zeta_h$ and thus $\tau(D_X) = \tau|_G(X) = \mu p^a$. Hence $P_\sigma(X)$ is a $\text{BH}(G, h)$ matrix.

Theorem 2.28. *Let p be a prime, let a, h be positive integers such that $a \geq 2$. Let $G = \mathbb{Z}_{p^a} \times T$ where T is an abelian p -group. Assume that p^a does not divide $\exp(T \times \mathbb{Z}_h)$ and let p^b be any prime power that divides $\exp(T \times \mathbb{Z}_h)$ with $b < a$. Suppose $X \in \mathbb{Z}[\zeta_h][G]$ is a group ring element such that it is a $\text{BH}(G, h)$ matrix and for all characters χ of G ,*

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

If U be a subgroup of $\mathbb{Z}_{p^a}$ of order $\max\{p^2, p^{b+1}\}$ and $P_\sigma(X)$ is a U -permutation of X , then $P_\sigma(X)$ is a $\text{BH}(G, h)$ matrix.

Since U -permutations are just bijections from G to itself, they do not give new groups for which Butson Hadamard matrices exist. As an example, we use a U -permutation on our construction from Theorem 2.20 with $U = \mathbb{Z}_{p^2}$ and $T = \mathbb{Z}_p \times \mathbb{Z}_p$. Using the notations from Section 2.1.3, recall that we have the group ring element

$$X = \sum_{i=0}^{p-1} \left(\sum_{j=0}^{p-1} \zeta_{i,j} V_{i,j} \gamma^{f_i} + \sum_{k=0}^{p-1} \eta_{i,k} V \gamma^k \right) \alpha^i \beta^{e_i} \in \mathbb{Z}[\zeta_h][\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p],$$

and we consider a $\mathbb{Z}_{p^2}$ -permutation to $X = U_0$. Note that the required automorphism σ (which is also the $\mathbb{Z}_{p^2}$ -permutation P) acts trivially when restricted to $\mathbb{Z}_p \times \mathbb{Z}_p$ and has order p when restricted to $\mathbb{Z}_{p^2}$. So we have $\sigma|_V$ is trivial and subsequently $\sigma(V) = V$ and $\sigma(V_{i,j}) = V_{i,j}$ for all i, j . Write $\sigma(\alpha) = \alpha^t$, where $t^p \equiv 1 \pmod{p^2}$. Then,

$$\sigma(X) = \sum_{i=0}^{p-1} \left(\sum_{j=0}^{p-1} \zeta_{i,j} V_{i,j} \gamma^{f_i} + \sum_{k=0}^{p-1} \eta_{i,k} V \gamma^k \right) \alpha^{ti} \beta^{e_i},$$

with no change to conditions (2.18), (2.19) and (2.20). Hence, the group ring element $\sigma(X)$ is also of the same form since α^{ti} is also a generator of $\mathbb{Z}_{p^2}$.

2.3 Galois Ring Construction

In [16], Tai constructed Butson Hadamard matrices from the ideas in the construction of relative difference sets in finite local rings of Leung, Ling, and Ma [42, 43]. Similarly, we can use the ideas from the construction of partial and relative difference sets from Galois rings by Chen, Ray and Xiang [12] to construct more Butson Hadamard matrices. We give a simple introduction of Galois rings, taken from [32, Chapter III].

Definition 2.29. *A finite commutative ring R with identity is called a Galois ring if its set of zeros divisors including 0 is a principal ideal $\langle r \rangle$, where r is a prime element of R .*

For example, the ring $\mathbb{Z}_{p^a}$ is a Galois ring for every positive integer a , where p is prime. The set of zero divisors, including 0, of $\mathbb{Z}_{p^a}$, is the prime ideal $\langle p \rangle$. Additionally, the Galois ring $\mathbb{Z}_{p^a}$ contains p^a elements and has characteristic p^a .

For any integer $a \geq 1$, let $\mathbb{F}_{p^a}$ denote the finite field of order p^a , where p is prime. Let $\mu : \mathbb{Z}_{p^a} \rightarrow \mathbb{Z}_p = \mathbb{F}_p$ be the modulo p reduction map, that is $c \mapsto c \pmod{p}$ for $c \in \mathbb{Z}_{p^a}$. We can extend μ to $\mathbb{Z}_{p^a}[x]$ by defining $\sum_{i=0}^n c_i x^i \mapsto \sum_{i=0}^n \mu_1(c_i) x^i$.

Definition 2.30. *Let $P_m(x)$ be a monic polynomial of degree m in $\mathbb{Z}_{p^a}[x]$, where m is a positive integer. If its image $\mu(P_m(x))$ in $\mathbb{Z}_p[x]$ is primitive over $\mathbb{Z}_p$ then $P_m(x)$ is called a monic basic primitive polynomial over $\mathbb{Z}_{p^a}$.*

The residue class ring $\mathbb{Z}_p[x]/(P_m(x))$ can be used to construct more Galois rings and classify them.

Result 2.31. *Let $P_m(x)$ be a monic basic primitive polynomial of degree m over $\mathbb{Z}_{p^a}$. Then the residue class ring $\mathbb{Z}_{p^a}[x]/(P_m(x))$ is a Galois ring with p^{am} elements with characteristic p^a . Furthermore, any Galois ring with p^{am} elements with characteristic p^a is isomorphic to an extension of $\mathbb{Z}_{p^a}[x]/(P_m(x))$ of $\mathbb{Z}_{p^a}[x]$, where $P_m(x)$ is a monic basic primitive polynomial degree of degree m .*

Example 2.32. Let $\mathbb{F}_4 = \mathbb{Z}_2(\alpha)$ be the Galois field of order 4 as described in Example 2.10, with the minimal primitive polynomial $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. We lift this to the monic primitive polynomial $\mu(x) = x^2 + x + 1 \in \mathbb{Z}_4[x]$ and let g be its root in

$\mathbb{Z}_4[x]/(x^2 + x + 1)$. By Result 2.31, the algebraic extension $\mathbb{Z}_4[g]$ is a Galois ring with 16 elements with characteristic 4. Note that the elements of the Galois ring $\mathbb{Z}_4[g]$ can be written as $a + bg$, where $a, b \in \mathbb{Z}_4$. In particular, the elements are

$$\begin{array}{llll} 0, & 1 \equiv 3g + 2g^2, & 2 \equiv 2g + 2g^2, & 3 \equiv g + g^2, \\ g, & 1 + g \equiv 3g^2, & 2 + g \equiv 3g + 2g^2, & 3 + g \equiv 2g + g^2, \\ 3g, & 1 + 2g \equiv g + 3g^2, & 2 + 2g \equiv 2g^2, & 3 + 2g \equiv 3g + g^2, \\ 2g, & 1 + 3g \equiv 2g + 3g^2, & 2 + 3g \equiv g + 2g^2, & 3 + 3g \equiv g^2, \end{array}$$

modulo 4 and modulo $g^2 + g + 1$. Furthermore, we check that the set $\{0, 2, 2g, 2 + 2g\}$ is the set of all zero divisors which is also the principal ideal $\langle 2 \rangle$ of $\mathbb{Z}_4[g]$. Therefore, $\mathbb{Z}_4[g]$ is a Galois ring by definition.

2.3.1 Galois Rings over $\mathbb{Z}_{p^2}$

Write $\text{GR}(p^2, a)$ as the algebraic extension $\mathbb{Z}_{p^2}[g]$, where g is the root of a unique monic basic primitive polynomial degree of degree 2 such that g satisfies $g^{p^a-1} = 1$. The Galois ring $\text{GR}(p^2, a)$ is a finite local ring with the unique maximal ideal $B = \{0, p, pg, \dots, pg^{q-2}\}$, where $q = p^a$. The residue class field $\text{GR}(p^2, a)/B = K = \{\bar{0}, \bar{1}, \bar{g}, \dots, \bar{g}^{q-2}\}$ is isomorphic to $\mathbb{F}_q$. We can take the *Teichmüller system* $\mathcal{T} = \{0, 1, g, \dots, g^{q-2}\}$ as a set of representative of $\text{GR}(p^2, a)/B$. Thus, an arbitrary element α of $\text{GR}(p^2, a)$ can be expressed uniquely as $\alpha = \alpha_0 + p\alpha_1$, where $\alpha_0, \alpha_1 \in \mathcal{T}$. Observe that $\alpha \in \text{GR}(p^2, a)$ is a unit if and only if $\alpha_0 \neq 0$. So every element of the set $\text{GR}(p^2, a)^* = \text{GR}(p^2, a) \setminus B$, the set of all units of $\text{GR}(p^2, a)$, has a unique representation $g^i(1 + p\alpha)$, with $0 \leq i \leq q - 2$ and $\alpha \in \mathcal{T}$. $\text{GR}(p^2, a)^*$ is a multiplicative group of order $(p^a - 1)p^a$ and is a direct product $H \times \mathcal{U}$, where H is a cyclic group of order $p^a - 1$ generated by g and $\mathcal{U}$ is the group of principal units of $\text{GR}(p^2, a)^*$, that is, elements of the form $(1 + p\alpha)$, $\alpha \in \mathcal{T}$. The group $\mathcal{U}$ has the structure of the elementary abelian p -group of order p^a and is isomorphic to the additive group of K via the map $1 + p\alpha \mapsto \bar{\alpha}$, $\alpha \in \mathcal{T}$.

We refer the reader to McDonalds [49] for the proofs of the assertions on the structure of $\text{GR}(p^2, t)^*$ and more detailed background of Galois rings.

For $\alpha \in K$, define the trace function $tr_{a,1}$ from K to $\mathbb{F}_p$ by

$$tr_{a,1}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{a-1}}.$$

Let $b > 0$ be a divisor of a . Then there is a unique subfield $\mathbb{F}_{p^b}$ of K with p^b elements. Denote the trace maps from K to $\mathbb{F}_{p^b}$ and $\mathbb{F}_{p^b}$ to $\mathbb{F}_p$ by $tr_{a,b}$ and $tr_{b,1}$ respectively. By the transitivity of trace, we have $tr_{a,1} = tr_{b,1} \circ tr_{a,b}$.

2.3.2 Construction using Galois Rings $\text{GR}(p^2, a)$

In this section, we describe a construction of $\text{BH}((\mathbb{Z}_{p^2})^a, h)$ using the Galois ring $\text{GR}(p^2, a)$. Observe that the additive group of $\text{GR}(p^2, t)$ is isomorphic to $\mathbb{Z}_{p^2} \times \cdots \times \mathbb{Z}_{p^2}$ (a copies) and the additive group of B is isomorphic to $EA(p^a)$. Consider the subgroup H of $\text{GR}(p^2, a)^*$ and write the cosets of H in $\text{GR}(p^2, a)^*$ as $E_{\bar{0}} = H$, $E_{\bar{1}} = (1+p)H$, $E_{\bar{g}^i} = (1+pg^i)H$, for $1 \leq i \leq q-2$, where $q = p^a$. Note that $|H| = |E_{\bar{0}}| = |E_{\bar{1}}| = \cdots = |E_{\bar{g}^{q-2}}| = q-1$.

Let $b > 0$ be a proper divisor of a . There exists an element $\bar{0} \neq \bar{g}^t \in K$ such that $tr_{a,b}(\bar{g}^t) = \bar{0}$. Let $V = \{\bar{x} \in K : tr_{a,b}(\bar{g}^t \bar{x}) = \bar{0}\}$. Since $tr_{a,b}$ is linear over $\mathbb{F}_{p^b}$, the set V is a $(a/b - 1)$ dimensional $\mathbb{F}_{p^b}$ -subspace of K . Consequently, the set $D = \bigcup_{\bar{x} \in V} E_{\bar{x}}$ is a subgroup of $\text{GR}(p^2, a)^*$. Write the cosets of D as $D_0 = D$ and $D_i = g_i D$, for $1 \leq i \leq p^b - 1$, where $g_i \in \mathcal{U}$. The character values for these cosets are given in [12, p. 183–185] as follows:

Result 2.33. *Suppose that χ is an additive character of $\text{GR}(p^2, a)$.*

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

Theorem 2.34. *Let G be the additive group of $\text{GR}(p^2, a)$ (which is isomorphic to $\mathbb{Z}_{p^2}^a$) and let $b > 0$ be a proper divisor of a . Let $B, D_0, \dots, D_{p^b-1}$ be the subsets of $\text{GR}(p^2, a)$*

as described above. Suppose that $\eta, \eta_0, \dots, \eta_{p^b-1}$ are complex roots of unity such that $\sum_{i=0}^{p^b-1} \eta_i = 0$. Then

$$X = \sum_{i=0}^{p^b-1} \eta_i D_i + \eta B \quad (2.33)$$

is a G -invariant $BH(p^{2a}, h)$, where h is the least common multiple of the orders of all the η and η_i 's

Proof. It is straightforward from definition that the sets B and D_i , where $0 \leq i \leq p^b - 1$, partition G and therefore X has the form $\sum_{x \in G} a_x x$, where each a_x is a root of unity.

Let χ be a character of G . If χ is the trivial character or has order p , then

$$\chi(X) = \sum_{i=0}^{p^b-1} \eta_i \chi(D_i) + \eta \chi(B) = \chi(D_0) \sum_{i=0}^{p^b-1} \eta_i + p^a \eta = p^a \eta,$$

by Result 2.33. Thus, we have $|\chi(X)| = p^a$.

Now suppose that χ has order p^2 . Then by Result 2.33, there is a unique j , $0 \leq j \leq p^b - 1$, such that $\chi(D_j) = p^{a-b}(p^a - 1)$ and for all $i \neq j$, $\chi(D_i) = -p^{a-b}$. Hence,

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

and we obtain $|\chi(X)| = p^a$. Therefore, $X \in BH(G, h)$ by Result 2.1. $\square$

As the only required condition is having roots of unity η_i , for $i = 0, \dots, p^b - 1$ such that $\sum_{i=0}^{p^b-1} \eta_i = 0$, we can use Theorem 1.16 to get the following:

Corollary 2.35. *Let p be a prime and let a, h be positive integers such that $p^b \in \mathcal{Q}(h)$ for some proper divisor b of a . Then there is a $BH(\mathbb{Z}_{p^2}^a, h)$ matrix.*

Example 2.36. For an integer h , we now construct a $BH(\mathbb{Z}_4 \times \mathbb{Z}_4, \text{lcm}(2, h))$ matrix using $GR(4, 2)$ from Example 2.32. As an additive group, $\mathbb{Z}_4[g]$ is isomorphic as a group to $\mathbb{Z}_4 \times \mathbb{Z}_4$ via the group homomorphism $\varphi : xg + y \mapsto (x, y)$. Its maximal ideal is

$$B = \{0, 2, 2g, 2g + 2\}. \quad (2.34)$$

The Teichmuller system for this ring is $\mathcal{T} = \{0, 1, g, 3g + 3g\}$. Every unit can be written uniquely as $g^i(1+2\beta)$, for some $i = 0, 1, 2$ and $\beta \in \mathcal{T}$. We have the following multiplication table:

*	1	3	$1 + 2g$	$1 + 2g^2$
1	1	3	$2g + 1$	$2g + 3$
g	g	$3g$	$3g + 2$	$g + 2$
g^2	$3g + 3$	$g + 1$	$3g + 1$	$g + 3$

Thus the unit group can be written as the direct product $\mathcal{H} \times \mathcal{U}$, where $\mathcal{H} = \langle g \rangle = \{1, g, 3g + 3\}$ and the $\mathcal{U} = \{1, 3, 2g + 1, 2g + 3\}$ is the group of principle units of the form $1 + 2\beta$, with $\beta \in \mathcal{T}$. Next, we have the cosets of $\mathcal{H}$ in $\text{GR}(4, 2)^*$:

$$\begin{aligned} E_{\bar{0}} &= \mathcal{H} = \{1, g, 3g + 3\}, & E_{\bar{g}} &= (1 + 2g)\mathcal{H} = \{2g + 1, 3g + 2, 3g + 1\}, \\ E_{\bar{1}} &= 3\mathcal{H} = \{3, 3g, g + 1\}, & E_{\bar{g}^2} &= (1 + 2g^2)\mathcal{H} = \{2g + 3, g + 2, g + 3\}. \end{aligned}$$

The residue class field $\text{GR}(4, 2)/B = K = \{\bar{0}, \bar{1}, \bar{g}, \bar{g}^2\}$ is isomorphic to $\mathbb{Z}_2(\alpha)$. Next, take $b = 1$ since it is the only proper divisor of 2 and the trace function from K to $\mathbb{F}_2$ is given by is $tr_{2,1}(x) = x + x^2$. We can easily compute that

$$tr_{2,1}(\bar{0}) = \bar{0}, \quad tr_{2,1}(\bar{1}) = \bar{0}, \quad tr_{2,1}(\bar{g}) = \bar{1}, \quad tr_{2,1}(\bar{g}^2) = \bar{1},$$

and so $\bar{g}^t = \bar{1}$ and $V = \{\bar{x} \in K : tr_{2,1}(\bar{g}^t \bar{x}) = \bar{0}\} = \{\bar{0}, \bar{1}\}$. Lastly, we arrive at our required cosets of D in $\text{GR}(4, 2)^*$:

$$D_0 = D = \sum_{v \in V} E_{\bar{v}} = \{1, 3, g, g + 1, 3g, 3g + 3\}, \quad (2.35)$$

$$D_1 = Dg = \{g + 2, g + 3, 2g + 1, 2g + 3, 3g + 1, 3g + 2\} \quad (2.36)$$

Let $(\eta_0, \eta_1, \eta) = (1, -1, \zeta_h)$, and construct the group ring element X using (2.33) from (2.34), (2.35) and (2.36). Then by Theorem 2.34, the group ring element X is a $\text{BH}(\mathbb{Z}_4 \times$

$\mathbb{Z}_4, \text{lcm}(2, h))$ matrix:

$$\begin{bmatrix} \zeta_h & 1 & \zeta_h & 1 & 1 & 1 & -1 & -1 & \zeta_h & -1 & \zeta_h & -1 & 1 & -1 & -1 & 1 \\ 1 & \zeta_h & 1 & \zeta_h & -1 & 1 & 1 & -1 & -1 & \zeta_h & -1 & \zeta_h & 1 & 1 & -1 & -1 \\ \zeta_h & 1 & \zeta_h & 1 & -1 & -1 & 1 & 1 & \zeta_h & -1 & \zeta_h & -1 & -1 & 1 & 1 & -1 \\ 1 & \zeta_h & 1 & \zeta_h & 1 & -1 & -1 & 1 & -1 & \zeta_h & -1 & \zeta_h & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & \zeta_h & 1 & \zeta_h & 1 & 1 & 1 & -1 & -1 & \zeta_h & -1 & \zeta_h & -1 \\ 1 & 1 & -1 & -1 & 1 & \zeta_h & 1 & \zeta_h & -1 & 1 & 1 & -1 & -1 & \zeta_h & -1 & \zeta_h \\ -1 & 1 & 1 & -1 & \zeta_h & 1 & \zeta_h & 1 & -1 & -1 & 1 & 1 & \zeta_h & -1 & \zeta_h & -1 \\ -1 & -1 & 1 & 1 & 1 & \zeta_h & 1 & \zeta_h & 1 & -1 & -1 & 1 & -1 & \zeta_h & -1 & \zeta_h \\ \zeta_h & -1 & \zeta_h & -1 & 1 & -1 & -1 & 1 & \zeta_h & 1 & \zeta_h & 1 & 1 & 1 & -1 & -1 \\ -1 & \zeta_h & -1 & \zeta_h & 1 & 1 & -1 & -1 & 1 & \zeta_h & 1 & \zeta_h & -1 & 1 & 1 & -1 \\ \zeta_h & -1 & \zeta_h & -1 & -1 & 1 & 1 & -1 & \zeta_h & 1 & \zeta_h & 1 & -1 & -1 & 1 & 1 \\ -1 & \zeta_h & -1 & \zeta_h & -1 & -1 & 1 & 1 & 1 & \zeta_h & 1 & \zeta_h & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & \zeta_h & -1 & \zeta_h & -1 & 1 & -1 & -1 & 1 & \zeta_h & 1 & \zeta_h & 1 \\ -1 & 1 & 1 & -1 & -1 & \zeta_h & -1 & \zeta_h & 1 & 1 & -1 & -1 & 1 & \zeta_h & 1 & \zeta_h \\ -1 & -1 & 1 & 1 & \zeta_h & -1 & \zeta_h & -1 & -1 & 1 & 1 & -1 & \zeta_h & 1 & \zeta_h & 1 \\ 1 & -1 & -1 & 1 & -1 & \zeta_h & -1 & \zeta_h & -1 & -1 & 1 & 1 & 1 & \zeta_h & 1 & \zeta_h \end{bmatrix}.$$

2.4 Summary of Results

In this chapter, we have provided several constructions of group invariant Butson Hadamard matrices $\text{BH}(p^{2a}, h)$ with the use of subgroups, Galois Rings, hyperplanes and also with the folding and permutation theorems. Let q_1 and q_2 be the two smallest prime divisors of h . To recap, G -invariant Butson Hadamard matrices exist for the following groups with the conditions as follows:

1. (Theorem 2.4) Group $G = \mathbb{Z}_p^{2a}$ with
 - h even and $p^a + 2 \in \mathcal{Q}(h)$, or
 - h odd and $p^a \in \mathcal{Q}(h)$, or
 - h odd and $p^a + 1 = (q_1 - 1)(q_2 - 1)$.

2. (Theorem 2.12) Group $G = \mathbb{Z}_{p^a} \times \mathbb{Z}_{p^a}$ with
 - h even and $p, p+1 \in \mathcal{Q}(h)$, or
 - h odd, $p-1 \in \mathcal{Q}(h)$ and either $p \in \mathcal{Q}(h)$ or $p-1 = (q_1-1)(q_2-1)$.
3. (Theorem 2.18) Group $G = \mathbb{Z}_{p^a} \times \mathbb{Z}_p^a$ with
 - h even and $p+1 \in \mathcal{Q}(h)$, or
 - h odd and $p-1 \in \mathcal{Q}(h)$.
4. (Theorem 2.18 and 2.24) Group $G = P \times \mathbb{Z}_p^a$, where $|P| = p^a$, with
 - h even and $p+1 \in \mathcal{Q}(h)$, or
 - h odd and $p-1 \in \mathcal{Q}(h)$.
5. (Theorem 2.34) Group $G = \mathbb{Z}_{p^2}^a$ with
 - h even and $p^b+2 \in \mathcal{Q}(h)$, or
 - h odd and $p^b \in \mathcal{Q}(h)$, or
 - h odd and $p^b+1 = (q_1-1)(q_2-1)$, for some proper divisor b of a .
6. (Lemma 2.2) Group $G \times H$, where G, H are any of the groups above with the associated conditions on h

Chapter 3

Necessary Conditions

In this chapter, we present a necessary condition for the existence of G -invariant Butson Hadamard matrices. First, several generalised versions of Ma's Lemma are introduced as they are instrumental in the study of group rings and will be used extensively in proving the other results in this section. Next, a new necessary condition for the existence of G -invariant Butson Hadamard matrix exists is given. In particular, we show that under the self conjugacy assumption, the exponent of the group G must be at most square-root of its order. For a list of other currently known non-existence results, we refer the reader to [53].

3.1 Ma's Lemma

Let p be a prime, let m be a positive integer, and write $m = p^a m'$ with $(p, m') = 1$, $a \geq 0$. If there is an integer j with $p^j \equiv -1 \pmod{m'}$, then p is called *self-conjugate modulo m* . A composite integer n is called self-conjugate modulo m if every prime divisor of n has this property. The following is a result of Turyn [58].

Result 3.1. *Suppose that $X \in \mathbb{Z}[\zeta_h]$ satisfies*

$$|X|^2 \equiv 0 \pmod{n^2}$$

for some positive integer n which is self-conjugate modulo h . Then $X \equiv 0 \pmod{n}$.

The famous Ma's Lemma [47] is one of the most useful results in the study of the non-existence theory of difference sets. It has also seen widespread use in the study of other related mathematical objects which use group rings in their description. So it is no surprise that the lemma is very helpful here. However, the focus has always been on the group ring $\mathbb{Z}[G]$. We extend Ma's Lemma to group rings $\mathbb{Z}[\zeta_h][G]$ under the self conjugacy assumption.

Result 3.2. *Let p be a prime and let G be a finite abelian group with the cyclic Sylow p -subgroup S . Let P be the subgroup of S of order p . Let $t, h \in \mathbb{Z}^+$ so that h is not divisible by p . If $D \in \mathbb{Z}[\zeta_h][G]$ satisfies*

$$\chi(D) \equiv 0 \pmod{p^t} \quad (3.1)$$

for all characters $\chi \in \hat{G}$ of order divisible by $|S|$, then there exists $X, Y \in \mathbb{Z}[\zeta_h][G]$ such that

$$D = p^t X + PY.$$

Proof. Write $G = S \times H$. Note that $p \nmid |H|$. Let $s \in \mathbb{Z}^+$ such that $|S| = p^s$ and assume $S = \langle g \rangle$. Let ψ be a character of S of order p^s . First, we claim that we can assume $D \in \mathbb{Z}[\zeta_h][S]$. Write

$$D = \sum_{k \in H} D_k k, \quad D_k \in \mathbb{Z}[\zeta_h][S]$$

For any character γ of H , $\psi\gamma$ is a character of G defined by $\psi\gamma(xy) = \psi(x)\gamma(y)$ for any $x \in S, y \in H$. We have

$$\psi\gamma(D) = \sum_{k \in H} \psi(D_k)\gamma(k) \equiv 0 \pmod{p^t}.$$

Put $M = (\gamma(k))_{\gamma \in \hat{H}, k \in H}$ and $u = (\psi(D_k))_{k \in H}$ as a column vector in $\mathbb{C}^{|H|}$. By (3.1), all entries of Mu are divisible by p^t . Since $M^{-1} = M^*/|H|$ and $\gcd(p, |H|) = 1$, we obtain

$$\psi(D_k) \equiv 0 \pmod{p^t}. \quad (3.2)$$

Note that (3.2) holds for any character ψ of S of order p^s and $D_k \in \mathbb{Z}[\zeta_h][S]$. Therefore,

we can assume $D \in \mathbb{Z}[\zeta_h][S]$. Define

$$\begin{aligned} \rho : \mathbb{Z}[\zeta_h][S] &\rightarrow \mathbb{Z}[\zeta_{hp^s}], \\ g &\rightarrow \zeta_{p^s}. \end{aligned}$$

We claim that

$$\ker(\rho) = \{PY : Y \in \mathbb{Z}[\zeta_h][S]\}. \quad (3.3)$$

Let $\sum_{i=0}^{p^s-1} a_i g^i \in \ker(\rho)$, then $\sum_{i=0}^{p^s-1} a_i \zeta_{p^s}^i = 0$. Since p does not divide h , the minimal polynomial of ζ_{p^s} over $\mathbb{Z}[\zeta_h]$ is $\phi(x) = 1 + x^{p^{s-1}} + \dots + x^{p^{s-1}(p-1)}$. We obtain

$$\sum_{i=0}^{p^s-1} a_i x^i = \phi(x) f(x), \quad f(x) \in \mathbb{Z}[\zeta_h][x],$$

so $\sum_{i=0}^{p^s-1} a_i g^i = \phi(g) f(g) = P f(g)$, which proves (3.3). Now since $\rho(D) \equiv 0 \pmod{p^t}$, there exists $X \in \mathbb{Z}[\zeta_h][S]$ so that $\rho(D) = p^t \rho(X)$. We obtain $(D - p^t X) \in \ker(\rho)$ and thus,

$$D = p^t X + PY, \quad Y \in \mathbb{Z}[\zeta_h][S].$$

□

For our purpose, we need to know more about D so we impose a stronger condition that $|\chi(D)|^2 = p^{2a}$. The following is a variation of [48, Lemma 4.2], adapted to the situation we are interested in.

Lemma 3.3. *Let p be a prime, let a, s, h be positive integers with $\gcd(h, p) = 1$, and assume that p is self-conjugate modulo h . Let G be a cyclic group of order p^s . For $i = 0, \dots, s$, let P_i denote the subgroup of G of order p^i . Suppose that $D \in \mathbb{Z}[\zeta_h][G]$ satisfies*

$$\chi(D)\chi(D^{(-1)}) = p^{2a}, \quad (3.4)$$

for every character χ on G . Then there are $\varepsilon_i = \pm 1$, $g_i \in G$, and $a_i \in \mathbb{Z}$, such that

$$D = \sum_{i=0}^{s-1} \varepsilon_i \zeta_h^{a_i} g_i (p^{a-i} P_i - p^{a-i-1} P_{i+1}) + \varepsilon_s \zeta_h^{a_s} p^{a-s} G. \quad (3.5)$$

Proof. Let $0 \leq i \leq s$ and let χ be a character of G of order p^{s-i} . Note that $\chi(D) \in \mathbb{Z}[\zeta_{p^{s-i}h}]$. By (3.4) and Result 3.1, we have $\chi(D) \equiv 0 \pmod{p^a}$, that is, $\chi(D) = p^a X$ for some $X \in \mathbb{Z}[\zeta_{p^{s-i}h}]$. As $|X| = 1$ by (3.4), Result 1.11 shows that X is a root of unity. Since $X \in \mathbb{Z}[\zeta_{p^{s-i}h}]$, we have $X = \varepsilon_i \zeta_{p^{s-i}}^{b_i} \zeta_h^{a_i}$ where $\varepsilon_i = \pm 1$ and $a_i, b_i \in \mathbb{Z}$ and thus

$$\chi(D) = p^a \varepsilon_i \zeta_{p^{s-i}}^{b_i} \zeta_h^{a_i}. \quad (3.6)$$

Let g_i be any element of G with $\chi(g_i) = \zeta_{p^{s-i}}^{b_i}$.

Now let Y denote the right hand side of (3.5). First suppose $i = s$. Then χ is the trivial character of G and thus $\chi(p^{a-i}P_i - p^{a-i-1}P_{i+1}) = 0$ for $i = 0, \dots, s-1$. Hence we get

$$\chi(Y) = \chi(\varepsilon_s \zeta_h^{a_s} p^{a-s} G) = p^a \varepsilon_s \zeta_h^{a_s} = \chi(D) \quad (3.7)$$

by (3.6).

Now suppose $0 \leq i \leq s-1$. Note that χ is trivial on $P_0, \dots, P_i$ and nontrivial on $P_{i+1}, \dots, P_s$. Hence $\chi(p^{a-j}P_j - p^{a-i-1}P_{j+1}) = 0$ for all $j \neq i$ and $\chi(G) = \chi(P_s) = 0$. We conclude

$$\chi(Y) = \chi(\varepsilon_i \zeta_h^{a_i} g_i (p^{a-i}P_i - p^{a-i-1}P_{i+1})) = p^a \varepsilon_i \zeta_{p^{s-i}}^{b_i} \zeta_h^{a_i} = \chi(D) \quad (3.8)$$

by (3.6).

Now let τ be any character of G that has the same order as χ . Then there is $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_{p^{s-i}})/\mathbb{Q})$ such that $\tau(g) = \chi(g)^\sigma$ for all $g \in G$. Let $\psi \in \text{Gal}(\mathbb{Q}(\zeta_{hp^{s-i}})/\mathbb{Q})$ be defined by $\zeta_{p^{s-i}}^\psi = \zeta_{p^{s-i}}^\sigma$ and $\zeta_h^\psi = \zeta_h$. Then $\tau(A) = \chi(A)^\phi$ for all $A \in \mathbb{Z}[\zeta_h][G]$ and thus $\tau(Y) = \chi(Y)^\phi = \chi(D)^\phi = \tau(D)$ by (3.7) and (3.8). This shows that $\tau(Y) = \tau(D)$ for all characters τ of G . Now (3.5) follows from Result 1.9. $\square$

Remark 3.4. Note that Lemma 3.3 holds even in the case where $s > a$. In this case, all terms on the right-hand side of (3.5) whose coefficients are not algebraic integers will cancel out.

Since the groups that we consider in our study are abelian p -groups, we cannot directly apply Result 3.2 and 3.3 in most cases. However the results are still useful if we consider

the canonical map, say ρ , onto G/H , where G/H is a cyclic group. Then we obtain information about the coefficients $\rho(D)$ from using Result 3.2 or 3.3. Since the map ρ groups the elements of G into cosets Hg , the coefficients of Hg are then the sum of the coefficients of all elements x which are contained in Hg . We then repeat the same process for other subgroups H to obtain sums of different coefficients. Afterwards, we put together all the information we have gathered to deduce the structure of the group ring element D and the conditions that its coefficients satisfy. This will be our main line of attack when we derive a necessary condition for existence, and several results in the classification of $\text{BH}(G, h)$ matrices.

3.2 Exponent Bound

At first glance, it is curious that all our constructions in Chapter 2 are for p -groups of order p^{2a} . This is due to the necessary condition on the existence of $\text{BH}(G, h)$ matrices by Brock [7] and Winterhoff [59]:

Result 3.5. *Suppose that G is an abelian group of order p^a , where p is prime and a is an odd integer. Let h be a positive integer such that $(p, h) = 1$ and $p^j \equiv -1 \pmod{h}$ for some positive integer j . Then $\text{BH}(G, h)$ matrix does not exist.*

Our next necessary condition comes from Turyn, Davis and Kraemer's work on Hadamard difference sets [35], which is a result on $\text{BH}(G, 2)$ matrices where G is an abelian 2-group.

Result 3.6. *Let G be an abelian 2-group of order 2^{2a} . A $\text{BH}(G, 2)$ matrix exists if and only if $\exp(G) \leq 2^{a+1}$.*

Recall that two important aspects in the study of group-invariant Butson Hadamard matrices are those concerning their existence and non-existence for a given group G and integer h . Thus, having results in the same vein of that of Result 3.6 would be a huge step in that direction. With this in mind, it would be a nice generalisation to Result 3.6 if we could show that a $\text{BH}(G, h)$ matrix exists for an abelian p -group G if and only if the exponent of G is at most $\sqrt{|G|}$. Although we were only partially successful in showing

the existence of $\text{BH}(G, h)$ matrices for groups G satisfying this bound in the previous chapter, we can use Result 3.2 to show the non-existence of $\text{BH}(G, h)$ matrices for all groups G with exponent exceeding the bound.

Theorem 3.7. *Let G be an abelian group of order p^{2a} , where p is prime. Suppose that $D \in \mathbb{Z}[\zeta_h][G]$ is a $\text{BH}(G, h)$ matrix. Assume that $\gcd(p, h) = 1$ and that p is self-conjugate modulo h . Then $\exp(G) \leq p^a$.*

Proof. Write $\exp(G) = p^m$. Choose a subgroup H of G of order p^{2a-m} such that $G/H \cong \mathbb{Z}_{p^m}$ and let $\rho : G \rightarrow G/H$ be the natural epimorphism. Let P denote the subgroup of G/H of order p . By Lemma 3.2, we have

$$\rho(D) = \pm p^a \zeta g + YP,$$

where ζ is an h th root of unity, $g \in G/H$, and $Y \in \mathbb{Z}[\zeta_h][G]$. Write $\rho(D) = \sum_{g \in G/H} a_g g$, $Y = \sum_{g \in G/H} b_g g$ and $Y_x = \sum_{g \in P} b_{xg}$. Thus, $YP = \sum_{x \in R} Y_x Px$, where R is the set of all coset representatives of P in G/H . Let k be an element in gP distinct from g . Clearly we have $a_k = Y_k = Y_g$ and $a_g = \pm p^a \zeta_h + a_k$. However,

$$p^a = |\pm p^a \zeta| = |a_g - a_k| \leq |a_g| + |a_k| \leq 2p^{2a-m}, \quad (3.9)$$

implying that $p^{m-a} \leq 2$ and thus $m \leq a$ for odd primes p .

For $p = 2$, we obtain $m \leq a + 1$. However if $m = a + 1$, then inequality (3.9) is in fact an equality. Write $D = \sum_{x \in G} \alpha_x x$. Since $\pm p^a \zeta = a_g - a_k = \sum_{x \in g} \alpha_x + \sum_{x \in k} (-\alpha_x)$ is a sum of h^{th} roots of unity, it must be the case that $a_x = \pm \zeta$ for $x \in g$ and $a_x = \mp \zeta$ for $x \in k$. So $\alpha_x = -\zeta$ for some $x \in g \cup k$ and thus implies that 2 divides h , which is a contradiction. Therefore, $m \leq a$ also in the case $p = 2$. $\square$

Chapter 4

Classification

In this chapter, we classify G -invariant Butson Hadamard matrices where the group G is $\mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p$. We will show that under the self-conjugacy assumption, all $\text{BH}(\mathbb{Z}_p \times \mathbb{Z}_p, h)$ and $\text{BH}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p, h)$ matrices are given by our constructions.

4.1 Classification of $\text{BH}(\mathbb{Z}_p \times \mathbb{Z}_p, h)$ Matrices

We have seen three constructions of $\text{BH}(\mathbb{Z}_p \times \mathbb{Z}_p, h)$ matrices in Theorems 2.4, 2.12 and 2.18 by fixing $a = 1$. The fact that they give group ring elements of the form $D = \sum_{i=0}^p \eta_i U_i$ with the conditions $\sum_{i=0}^p \eta_i = 1$ is of coincidence.

Theorem 4.1. *Let p be an odd prime and let h be a positive integer which is not divisible by p . Furthermore, assume that p is self-conjugate modulo h . Let $U_0, \dots, U_p$ be all the cyclic subgroups of $\mathbb{Z}_p \times \mathbb{Z}_p$ of order p . Then all $\text{BH}(\mathbb{Z}_p \times \mathbb{Z}_p, h)$ matrices is of the form*

$$D = \sum_{i=0}^p \eta_i U_i, \tag{4.1}$$

and $\eta_0, \dots, \eta_p$ are h th roots of unity satisfying

$$\sum_{i=0}^p \eta_i = 1, \tag{4.2}$$

up to equivalence.

Proof. Write $G = \mathbb{Z}_p \times \mathbb{Z}_p$. Let $D = \sum_{g \in G} a_g g \in \mathbb{Z}[\zeta_h][G]$ be the group ring element which corresponds to the $\text{BH}(\mathbb{Z}_p \times \mathbb{Z}_p, h)$ matrix. We have

$$DD^{(-1)} = p^2.$$

Replacing h by $2h$ if necessary, we may assume that h is even. Note that this replacement preserves the property that p is self-conjugate modulo h . Replacing D by $\zeta_h^k D$ for some integer k , if necessary, we can assume $\chi_0(D) = p$, where χ_0 is the trivial character of G .

Write $G_i = G/U_i$ and let $\rho_i : G \rightarrow G/U_i$ denote the natural epimorphism. We have $\chi(D) \equiv 0 \pmod{p}$ for any $\chi \in \hat{G}$. Hence $\tau(\rho_i(D)) \equiv 0 \pmod{p}$ for every $\tau \in \hat{G}_i$. By Lemma 3.3, we thus have

$$\rho_i(D) = \varepsilon_0 \zeta_h^{k_i} x_i (p - G_i) + \varepsilon_1 \zeta_h^{b_i} G_i,$$

where $\varepsilon_0, \varepsilon_1 = \pm 1$, $k_i, b_i \in \mathbb{Z}$, and $x_i \in G_i$. Since h is even, we can assume $\varepsilon_0 = \varepsilon_1 = 1$. Thus

$$\rho_i(D) = p \zeta_h^{k_i} x_i + (-\zeta_h^{k_i} + \zeta_h^{b_i}) G_i. \quad (4.3)$$

Applying the trivial character to (4.3), we find $p = \chi_0(D) = p \zeta_h^{k_i} + p(-\zeta_h^{k_i} + \zeta_h^{b_i})$ and thus $\zeta_h^{b_i} = 1$. In summary, we have

$$\rho_i(D) = p \zeta_h^{k_i} x_i + (1 - \zeta_h^{k_i}) G_i \text{ for all } i. \quad (4.4)$$

Note that (4.4) implies the following

$$\begin{aligned} \sum_{g \in U_i g_i} a_g &= 1 + (p - 1) \zeta_h^{k_i}, \\ \sum_{g \in U_i y} a_g &= 1 - \zeta_h^{k_i} \text{ for all } y \in G \setminus U_i g_i. \end{aligned} \quad (4.5)$$

Fix $y \in G$. Using (4.5), we get

$$\begin{aligned} \sum_{i=0}^p \sum_{g \in U_i y} a_g &= \sum_{y \in U_i g_i} (1 + (p-1)\zeta_h^{k_i}) + \sum_{y \notin U_i g_i} (1 - \zeta_h^{k_i}) \\ &= \sum_{i=0}^p (1 - \zeta_h^{k_i}) + p \sum_{y \in U_i g_i} \zeta_h^{k_i} \\ &= p + 1 - \sum_{i=0}^p \zeta_h^{k_i} + p \sum_{y \in U_i g_i} \zeta_h^{k_i}. \end{aligned}$$

On the other hand,

$$\sum_{i=0}^p \sum_{g \in U_i y} a_g = p a_y + \sum_{g \in G} a_g = p a_y + \chi_0(D) = p(1 + a_y).$$

Therefore, we obtain

$$a_y = \sum_{y \in U_i g_i} \zeta_h^{k_i} + \alpha, \quad \alpha = \frac{1 - \sum_{i=0}^p \zeta_h^{k_i}}{p} \in \mathbb{Z}[\zeta_h]. \quad (4.6)$$

We claim that the theorem is proved if we can show that $\cup_{i=0}^p U_i g_i = G$. Assume $\cup_{i=0}^p U_i g_i \neq G$. In this case, all the lines $U_i g_i$ intersect at an element $g \in G$. Indeed, let S_n be the number of points of $\cup_{i=0}^n U_i g_i$, then $S_n \leq S_{n-1} + (p-1)$, which implies $S_p = |\cup_{i=0}^p U_i g_i| \leq p^2$. The equality must happen and it implies that all the lines $U_i g_i$ intersect at one point, say g . Replacing D by Dg^{-1} , we may assume $\cap_{i=0}^p U_i g_i = \{1\}$. Hence $U_i g_i = U_i$ for all i . In other words, each non-identity element $y \in G$ is contained in a unique subgroup U_i for some i .

We claim that for each $y \in U_i \setminus \{1\}$, where $i = 0, \dots, p$, we have $a_y = \zeta_h^{k_i}$. Suppose on the contrary that there exists $z \in U_j \setminus \{1\}$ such that $a_z \neq \zeta_h^{k_j}$. Since α is a constant not depending on any group element y , equation (4.6) gives

$$a_z - \zeta_h^{k_j} = a_y - \zeta_h^{k_i},$$

for any $y \in G \setminus \{1\}$ such that $y \in U_i$ for some i . Since all terms involved are roots of unity, they must cancel out in pairs. In particular, this implies $\zeta_h^{k_i} = \zeta_h^{k_j}$ or $\zeta_h^{k_i} = -a_z$; the remaining case $\zeta_h^{k_j} = a_z$ contradicts $a_y \neq \zeta_h^{k_i}$. Substituting back into equation (4.6) gives

$$pa_z - p\zeta_h^{k_i} = 1 + na_z - (p - n + 1)\zeta_h^{k_j}, \quad (4.7)$$

where n is the number of terms for which $\zeta_h^{k_i} = -a_z$, for $0 \leq i \leq p$. Rearranging (4.7) gives $(p-n)a_z = 1 + (n-1)\zeta_h^{k_j}$, implying that $p-n = |(p-n)a_z| = |1 + (n-1)\zeta_h^{k_j}| \leq n-1+1 = n$, or simply $n \geq \frac{p}{2}$. On the other hand, $p-n = |1 + (n-1)\zeta_h^{k_j}| \geq (n-1) - 1 = n-2$ and thus $n \leq \frac{p+2}{2}$. Combining the two inequality gives $n = \frac{p+1}{2}$ since n is an integer. Substituting back into equation (4.7) gives

$$1 = a_z \left(p - \frac{p+1}{2} \right) - \left(\frac{p+1}{2} - 1 \right) \zeta_h^{k_i} = \left(\frac{p-1}{2} \right) (a_z - \zeta_h^{k_i}).$$

Then the cyclotomic integer $a_z - \zeta_h^{k_i} = \frac{2}{p-1}$ is real and (all its conjugates) has absolute value at most 1 since $p \geq 3$. By a theorem of Kronecker (Result 1.11), it is a root of unity. However this is not possible unless $p = 3$, in which case we get $a_z - \zeta_h^{k_i} - 1 = 0$. But this implies that p (which is 3) divides h by [10, Thm. 6], a contradiction. The coefficients a_y are the same for $y \in U_i \setminus \{1\}$, and are equal to $\zeta_h^{k_i}$. Together with equation (4.6), this implies $\alpha = 0$ and thus $a_1 = \sum_{i=0}^p \zeta_h^{k_i} = 1$. Therefore, we obtain

$$D = \sum_{i=0}^p \zeta_h^{k_i} U_i - (p+1) \left(a_1 - \sum_{i=0}^p \zeta_h^{k_i} \right) = \sum_{i=0}^p \zeta_h^{k_i} U_i,$$

which is of the form given in (4.1) and also satisfies equation (4.7), with $\eta_i = \zeta_h^{k_i}$.

From now on, suppose that $\cup_{i=0}^p U_i g_i \subsetneq G$. For each $y \in G$, define

$$S(y) = \{0 \leq i \leq p : y \in U_i g_i\}.$$

Suppose that $|S(y)| \neq 1$ for all $y \in G$. Hence we have

$$|S(y)| \geq 2 \text{ whenever } S(y) \neq \emptyset.$$

Now consider any of the cosets $U_i g_i$. As $S(y) \neq \emptyset$ for $y \in U_i g_i$, we have $|S(y)| \geq 2$ for all $y \in U_i g_i$. This implies that the intersections of $U_i g_i$ with $U_j g_j$, $j \neq i$, are pairwise distinct. This implies $|S(y)| = 2$ for all $y \in U_i g_i$. Since this is true for any coset $U_i g_i$, we conclude

$$|S(y)| = 2 \text{ whenever } S(y) \neq \emptyset. \quad (4.8)$$

Now let $z \in G \setminus U_0 g_0$. Then $U_0 g_0 \cap U_0 z = \emptyset$ and $|U_j g_j \cap U_0 z| = 1$ for all $j \in \{1, \dots, p\}$. This implies $\sum_{y \in U_0 z} |S(y)| = p$. As p is odd by assumption, this contradicts (4.8).

Now, suppose there exists $y \in G$ such that $|S(y)| = 1$. As $\cup_{i=0}^p U_i g_i$ is strictly contained in G , there exists $g \in G$ such that $S(g) = \emptyset$. The equation (4.6) implies $\alpha = a_g$ is a root of unity. We have

$$1 - \left(\sum_{i=0}^p \zeta_h^{k_i} \right) = p\alpha. \quad (4.9)$$

Assume that $\zeta_h^{k_j} = 1$ for some j , where $0 \leq j \leq p$. Then

$$\sum_{\substack{i=0 \\ i \neq j}}^p \zeta_h^{k_i} = p\alpha,$$

and thus $\zeta_h^{k_i} = -\alpha$ for all $i \neq j$. Fix $i \neq j$ and consider any element $x \in U_i g_i$. Write $|S(x)| = n \geq 1$. Suppose that x is not contained in $U_j g_j$, then equation (4.6) gives $a_x = (1 - n)\alpha$, implying that $n = 2$. Since i was arbitrary, this is true for all $x \in U_i g_i \setminus U_j g_j$, for all $i \in \{0, 1, \dots, p\} \setminus \{j\}$. Now let $z \in G \setminus U_j g_j$ and consider the line $U_j z$. Then $U_j g_j \cap U_j z = \emptyset$ and $|U_i g_i \cap U_j z| = 1$ for all $i \in \{0, 1, \dots, p\} \setminus \{j\}$. This implies $\sum_{x \in U_j z} |S(x)| = p$. Moreover, the element contained in $U_i g_i \cap U_j z$ is not in $U_j g_j$ and so the values $|S(x)|$ are all either 2 or 0. As p is odd by assumption, this is a contradiction. Hence $\zeta_h^{k_j} \neq 1$ for all $j \in \{0, \dots, p\}$.

By (4.6) and (4.9), we have $a_y = \zeta_h^{k_i} + \alpha$, which implies that 6 divides h by [10, Thm. 6]. Write $N = \#\{i \in \{0, \dots, p\} : \zeta_h^{k_i} = \alpha\}$. Using Corollary 1.17 with equation (4.9), we have $N \geq p - 2$.

Case 1: $N = p$.

Then by the same reasoning as the previous paragraph, we can show that the lines

$U_i g_i$ are all equal, which is impossible.

Case 2: $N = p - 1$.

Assume that $\zeta_h^{k_0}, \zeta_h^{k_1} \neq -\alpha$. Simplifying (4.9), we get

$$1 - \zeta_h^{k_0} - \zeta_h^{k_1} = \alpha,$$

and so the terms must cancel out in pairs. We know that $\zeta_h^{k_0}$ and $\zeta_h^{k_1}$ cannot cancel out with α and thus we have $\alpha = 1$. But this is a contradiction since that implies $\zeta_h^{k_2} = \alpha = 1$.

Case 3: $N = p - 2$.

Assume that $\zeta_h^{k_0}, \zeta_h^{k_1}, \zeta_h^{k_2} \neq -\alpha$. First, note that for each i , where $3 \leq i \leq p$, we have $|S(x)| \neq 1$. Otherwise, equation (4.6) gives $a_x = \zeta_h^{k_i} + \alpha = 0$. In other words, $|S(x)| \geq 2$ for all $x \in U_i g_i$, where $i \geq 3$. Recall that this would imply

$$|S(x)| = 2 \text{ for all } x \in U_i g_i, \text{ where } 3 \leq i \leq p. \quad (4.10)$$

Next, substituting the values of $\zeta_h^{k_i}$ into (4.9) gives

$$1 - \zeta_h^{k_0} - \zeta_h^{k_1} - \zeta_h^{k_2} - 2\alpha = 0.$$

By Result 1.14, the terms must cancel in pairs or in groups of three. Using the same argument in the previous case, we conclude that the terms must cancel out in threes. Moreover, the α terms cannot be cancelled out in the same group. Without loss of generality, we can assume that

$$1 - \zeta_h^{k_0} - \alpha = 0 \quad \text{and} \quad \zeta_h^{k_1} + \zeta_h^{k_2} + \alpha = 0. \quad (4.11)$$

The intersections $U_1 g_1 \cap U_i g_i$, for $2 \leq i \leq p$, must be pairwise distinct by (4.10). Meanwhile, the element $w \in U_1 g_1 \cap U_2 g_2$ must also be in $U_0 g_0$. Otherwise equations (4.6) and (4.11) would imply that $a_w = 0$, which is impossible. The last remaining element in $g_1 U_1$, say y_1 , has the property that $|S(y_1)| = 1$. Consequently, the same can be said for $g_0 U_0$

and g_2U_2 . As such, for $i = 0, 1, 2$, we can write

$$g_iU_i = \{w, y_i, x_{i,3}, \dots, x_{i,p}\},$$

where $w \in U_0g_0 \cap U_1g_1 \cap U_2g_2$, $x_{i,j} \in U_ig_i \cap U_jg_j$, for $3 \leq j \leq p$ and $|S(y_i)| = 1$.

As 6 divides h and $(p, h) = 1$ by assumption, we conclude that $p \neq 3$. Since $p \geq 5$, then we can find a line U_0z such that w, y_1, y_2, y_3 are not contained in U_0z . Using the same line of reasoning as before, we have $U_0g_0 \cap U_0z = \emptyset$ and $|U_ig_i \cap U_jz| = 1$ for all $i \in \{1, \dots, p\}$, which implies $\sum_{x \in U_0z} |S(x)| = p$. Additionally, the elements contained in $U_ig_i \cap U_jz$ are different from $\{w, y_1, y_2, y_3\}$ and so the values $|S(x)|$ are all either 2 or 0. As p is odd by assumption, this is a contradiction. $\square$

4.2 Classification of $BH(\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p, h)$ Matrices

Recall that we have two constructions of $BH(\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p, h)$ matrices with $\gcd(p, h) = 1$ with almost the same structure but with different conditions from Theorems 2.18 and 2.20. We investigate this now and determine that these are all the possible constructions. Our method is based on considering the subgroup of G isomorphic to $\mathbb{Z}_p^3$ and the subgroups of G of order p^2 and applying Ma's Lemma on the quotient groups G projected on these subgroups. Then, we deduce the coefficients of the group ring element D by using the number theoretic tools we developed on the information obtained by Ma's Lemma.

4.2.1 Setup

Let $D = \sum_{g \in G} a_g g$ be a $BH(G, h)$ where $G = \mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p$, $\gcd(p, h) = 1$, p is self-conjugate mod h . Write $G = \langle \alpha \rangle \times \langle \beta \rangle \times \langle \gamma \rangle$, where α has order p^2 and β, γ have order p .

Write $\zeta = \zeta_h$. Let $W = \langle \alpha^p \rangle \times \langle \beta \rangle \times \langle \gamma \rangle$ and $U = \langle \alpha^p \rangle$. Let $V_1, \dots, V_{p^2}$ be the subgroups of W of order p^2 which do not contain U and let $\rho_i : G \rightarrow G/V_i$ and $\rho : G \rightarrow G/W$ be the natural epimorphisms. Note that $G/V_i = \{\rho_i(1), \rho_i(\alpha), \dots, \rho_i(\alpha^{p^2-1})\}$. To simplify notation, when considering equations over G/V_i , we identify G/V_i with $\{1, \alpha, \dots, \alpha^{p^2-1}\}$.

By Result 3.3, we have

$$\rho_i(D) = \varepsilon_i \zeta^{m_i} \alpha^{n_i} p^2 + (\varepsilon_0 \zeta^n - \varepsilon_i \zeta^{m_i} \alpha^{n_i}) p \langle \alpha^p \rangle + (-\varepsilon_0 \zeta^n + \varepsilon) \langle \alpha \rangle, \quad (4.12)$$

$$\rho(D) = p^2 \varepsilon_0 \zeta^n + p(\varepsilon - \varepsilon_0 \zeta^n) G/W, \quad (4.13)$$

where n, m_i, n_i are integers, $\varepsilon, \varepsilon_0, \varepsilon_i = \pm 1$, and P_i is the subgroup of G/V_i of order p . Expressing (4.12) and (4.13) in terms of coefficient sums over cosets, we get the following. If $n_i \equiv 0 \pmod{p}$, then

$$\sum_{x \in V_i \alpha^j} a_x = \begin{cases} (p^2 - p) \varepsilon_i \zeta^{m_i} + (p - 1) \varepsilon_0 \zeta^n + \varepsilon & \text{if } j \equiv n_i \pmod{p^2}, \\ -p \varepsilon_i \zeta^{m_i} + (p - 1) \varepsilon_0 \zeta^n + \varepsilon & \text{if } j \equiv 0 \pmod{p}, j \not\equiv n_i \pmod{p^2}, \\ -\varepsilon_0 \zeta^n + \varepsilon & \text{otherwise.} \end{cases} \quad (4.14)$$

If $n_i \not\equiv 0 \pmod{p}$, then

$$\sum_{x \in V_i \alpha^j} a_x = \begin{cases} (p^2 - p) \varepsilon_i \zeta^{m_i} - \varepsilon_0 \zeta^n + \varepsilon & \text{if } j \equiv n_i \pmod{p^2}, \\ -p \varepsilon_i \zeta^{m_i} - \varepsilon_0 \zeta^n + \varepsilon & \text{if } j \equiv n_i \pmod{p}, j \not\equiv n_i \pmod{p^2}, \\ (p - 1) \varepsilon_0 \zeta^n + \varepsilon & \text{if } j \equiv 0 \pmod{p}, \\ -\varepsilon_0 \zeta^n + \varepsilon & \text{otherwise.} \end{cases} \quad (4.15)$$

Finally, we have

$$\sum_{x \in Wg} a_x = \begin{cases} (p^2 - p) \varepsilon_0 \zeta^n + p\varepsilon & \text{if } g \in W, \\ -p \varepsilon_0 \zeta^n + p\varepsilon & \text{if } g \in G \setminus W. \end{cases} \quad (4.16)$$

Note that $|V_i \alpha^{n_i} \cap V_j \alpha^{n_j}| = p$ if $i \neq j$ and $n_i \equiv n_j \pmod{p}$ and $|V_i \alpha^{n_i} \cap V_j \alpha^{n_j}| = 0$ if $n_i \not\equiv n_j \pmod{p}$

If we view W as a three-dimensional affine space, the cosets of subgroups of order p and p^2 of W represent lines and planes, respectively. Similarly, we view each coset of Wg in G as a three-dimensional affine space and consider the cosets of cardinality p and p^2 contained in Wg as lines and planes, respectively. If $C \subset G$ is a coset of a subgroup A of G , we write $\mathcal{L}(C) = A$. We say that two cosets C_1 and C_2 are **parallel** if $\mathcal{L}(C_1) \subset \mathcal{L}(C_2)$

or vice versa. We call the cosets $F_i := V_i \alpha^{n_i}$, $i = 1, \dots, p^2$, **full planes**.

Let Wg be any coset of W and let E be any plane in Wg that is not parallel to U . Set $\delta_E = 1$ if $E \subset W$ and $\delta_E = 0$ otherwise. Note that there is a unique full plane $F_i = V_i \alpha^{n_i}$ parallel to E , that $E = V_i \alpha^b$ for some integer b , and that $F_i \subset Wg$ if and only if $b \equiv n_i \pmod{p}$. Hence, by (4.12), we have

$$\sum_{x \in E} a_x = \begin{cases} (p^2 - p)\varepsilon_i \zeta^{m_i} + (\delta_E p - 1)\varepsilon_0 \zeta^n + \varepsilon & \text{if } E = F_i, \\ -p\varepsilon_i \zeta^{m_i} + (\delta_E p - 1)\varepsilon_0 \zeta^n + \varepsilon & \text{if } F_i \subset Wg, E \neq F_i, \\ (\delta_E p - 1)\varepsilon_0 \zeta^n + \varepsilon & \text{if } F_i \not\subset Wg. \end{cases} \quad (4.17)$$

Lemma 4.2. *Let q be the smallest odd prime divisor of h . We have*

$$|\{x \in V_i \alpha^{n_i} : a_x = \varepsilon_i \zeta^{m_i}\}| \geq \begin{cases} p^2 - p - \frac{p+2}{q-2} - 2 & \text{if } V_i \alpha^{n_i} \not\subset W, \\ p^2 - 2p - \frac{2p}{q-2} & \text{if } V_i \alpha^{n_i} \subset W. \end{cases} \quad (4.18)$$

Furthermore, if h is odd and $(p, q) \neq (3, 3)$, then $\varepsilon_i = 1$ for all i .

Proof. Write $T = \{x \in V_i \alpha^{n_i} : a_x = \varepsilon_i \zeta^{m_i}\}$. First assume that $V_i \alpha^{n_i} \not\subset W$. By (4.15), we have

$$\varepsilon_0 \zeta^n - \varepsilon + \sum_{x \in V_i \alpha^{n_i}} a_x = (p^2 - p)\varepsilon_i \zeta^{m_i}. \quad (4.19)$$

Applying Corollary 1.17 to (4.19) with $s = p^2 + 2$ and $t = p^2 - p$, we see that at least $p^2 - p - (p + 2)/(q - 2)$ roots of unity on the left hand side of (4.19) are equal to $\varepsilon_i \zeta^{m_i}$. Thus $|T| \geq p^2 - p - (p + 2)/(q - 2) - 2$. This proves (4.18) for $V_i \alpha^{n_i} \not\subset W$.

Now suppose that $V_i \alpha^{n_i} \subset W$. By (4.14), we have

$$-(p - 1)\varepsilon_0 \zeta^n - \varepsilon + \sum_{x \in V_i \alpha^{n_i}} a_x = (p^2 - p)\varepsilon_i \zeta^{m_i}. \quad (4.20)$$

Applying Corollary 1.17 to (4.20) with $s = p^2 + p$ and $t = p^2 - p$, we infer that at least $p^2 - p - 2p/(q - 2)$ roots of unity on the left hand side of (4.20) are equal to $\varepsilon_i \zeta^{m_i}$. Thus $|T| \geq p^2 - 2p - (p + 2)/(q - 2)$. This completes the proof of (4.18)

Finally, suppose that h is odd and that $(p, q) \neq (3, 3)$. Then $p^2 - p - \frac{p+2}{q-2} - 2 > 0$ and $p^2 - 2p - \frac{p+2}{q-2} > 0$. Thus, (4.18), there is $x \in V_i \alpha^{n_i}$ with $a_x = \varepsilon_i \zeta^{m_i}$. This implies that ε_i is a h th root of unity. As $\varepsilon_i = \pm 1$, we conclude $\varepsilon_i = 1$, as h is odd. $\square$

From now on, we assume that h is odd and that

$$p > \frac{7q-8}{q-5} \text{ and } q \geq 7, \quad (4.21)$$

where q is the smallest prime divisor of h . Note that (4.21) implies $p \geq 11$.

4.2.2 Structure of Putative $\text{BH}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p, h)$ Matrices

Let $L \subset Wg$ be any line that is not parallel to U . Note that there are exactly $p+1$ planes in Wg that contain L . Let $E_0, \dots, E_p$ denote these planes. Note that LU is the unique plane that contains L and is parallel to U . So we can assume $E_0 = LU$. We can make the following assumptions without loss of generality. Let $E_1, \dots, E_s$ be the full planes that contain L (if there is no full plane containing L , we set $s = 0$), and assume $E_i = F_i$ for $i = 1, \dots, s$. Moreover, let $E_{s+1}, \dots, E_t$, $t \geq s$, be the planes that contain L , are parallel to full planes in Wg , but are not full planes (if there is no such plane, we set $t = s$). Assume that E_i is parallel to F_i for $s+1 \leq i \leq t$. By (4.17), we have

$$\sum_{x \in E_i} a_x = \begin{cases} (p^2 - p)\zeta^{m_i} + (\delta_{E_i} p - 1)\varepsilon_0 \zeta^n + \varepsilon & \text{if } i \leq s, \\ -p\zeta^{m_i} + (\delta_{E_i} p - 1)\varepsilon_0 \zeta^n + \varepsilon & \text{if } s+1 \leq i \leq t, \\ (\delta_{E_i} p - 1)\varepsilon_0 \zeta^n + \varepsilon & \text{if } i > t. \end{cases} \quad (4.22)$$

Using (4.22), we get

$$\begin{aligned} \sum_{i=1}^p \sum_{x \in E_i} a_x &= \sum_{i=1}^s ((p^2 - p)\zeta^{m_i} + (\delta_{E_i} p - 1)\varepsilon_0 \zeta^n + \varepsilon) + \sum_{i=s+1}^t (-p\zeta^{m_i} + (\delta_{E_i} p - 1)\varepsilon_0 \zeta^n + \varepsilon) \\ &\quad + (p - t)((\delta_{E_i} p - 1)\varepsilon_0 \zeta^n + \varepsilon) \\ &= (\delta_{E_i} p^2 - p)\varepsilon_0 \zeta^n + p\varepsilon - p \sum_{i=1}^t \zeta^{m_i} + p^2 \sum_{i=1}^s \zeta^{m_i}. \end{aligned} \quad (4.23)$$

Note that the multiset $\bigcup_{i=0}^p E_i$ covers each element of $Wg \setminus L$ exactly once and each element of L exactly $p+1$ times. Using (4.16), we find

$$(\delta_{E_i} p^2 - p)\varepsilon_0 \zeta^n + p\varepsilon = \sum_{x \in Wg} a_x = \sum_{i=0}^p \sum_{x \in E_i} a_x - p \sum_{x \in L} a_x. \quad (4.24)$$

Set $R = \sum_{x \in E_0} a_x$. Using (4.23), we get

$$\begin{aligned} \sum_{i=0}^p \sum_{x \in E_i} a_x &= R + \sum_{i=1}^p \sum_{x \in E_i} a_x \\ &= R + (\delta_{E_i} p^2 - p)\varepsilon_0 \zeta^n + p\varepsilon - p \sum_{i=1}^t \zeta^{m_i} + p^2 \sum_{i=1}^s \zeta^{m_i}. \end{aligned}$$

Combining this with (4.24) yields

$$\sum_{x \in L} a_x = \frac{1}{p}R + p \sum_{i=1}^s \zeta^{m_i} - \sum_{i=1}^t \zeta^{m_i}.$$

We summarize this result as follows.

Lemma 4.3. *Let Wg be any coset of W in G , and let L be a line in Wg that is not parallel to U . Let $F_1, \dots, F_s$ be all the full planes that contain L , let $F_{s+1}, \dots, F_t$ be all the full planes in Wg that are parallel to L , but do not contain L . Then*

$$\sum_{x \in L} a_x = \frac{1}{p}R + p \sum_{i=1}^s \zeta^{m_i} - \sum_{i=1}^t \zeta^{m_i},$$

where $R = \sum_{x \in LU} a_x$.

Looking at our constructions, there are p full planes contained in each coset of W and they intersect in a common line. We now work towards proving that this is indeed necessary.

Lemma 4.4. *Let Wg be any coset of W in G different from W . If F_i , F_j , and F_k are three distinct full planes in Wg that do not contain a common line, then $\zeta^{m_i} = \zeta^{m_j} = \zeta^{m_k}$.*

Proof. It suffices to show that $\zeta^{m_i} \neq \zeta^{m_j}, \zeta^{m_k}$ is impossible. Thus suppose $\zeta^{m_i} \neq \zeta^{m_j}, \zeta^{m_k}$. By Lemma 4.2, we have $\varepsilon_r = 1$ for $r = i, j, k$.

Write $\delta = (p+2)/(q-2) + 2$ where q is the smallest odd prime divisor of h . and $T_r = \{x \in F_r : a_x = \zeta^{m_r}\}$ for $r = i, j, k$. By Lemma 4.2, we have

$$|T_r| \geq p^2 - p - \delta \quad \text{for } r = i, j, k. \quad (4.25)$$

Note that $|F_i \cap (F_j \cup F_k)| \geq 2p - 1$, as F_i, F_j , and F_k do not contain a common line. Moreover, at most $p + \delta$ elements of F_i are not in T_i by (4.25). Thus at least $2p - 1 - (p + \delta) = p - \delta - 1$ elements of T_i are contained in $F_j \cup F_k$. Hence, without loss of generality, we can assume that F_j contains at least $(p - \delta - 1)/2$ elements of T_i , that is, we have

$$|F_j \cap T_i| \geq (p - \delta - 1)/2. \quad (4.26)$$

By (4.25), we can write $|T_j| = p^2 - p - \delta_1$ with $\delta_1 \leq \delta$. We have

$$\varepsilon_0 \zeta^n - \varepsilon + \sum_{x \in F_j} a_x = (p^2 - p) \zeta^{m_j}$$

by (4.15) and thus

$$\varepsilon_0 \zeta^n - \varepsilon + \sum_{x \in F_j \setminus T_j} a_x = \delta_1 \zeta^{m_j}. \quad (4.27)$$

Note that T_i and T_j are disjoint, as $\zeta^{m_i} \neq \zeta^{m_j}$ by assumption. Hence $R_j := F_j \cap T_i$ is a subset of $F_j \setminus T_j$ and $F_j \setminus T_j$ is the disjoint union of R_j and $S_j := F_j \setminus (T_j \cup R_j)$. Hence (4.27) can be written as

$$-\varepsilon_0 \zeta^n + \varepsilon + \delta_1 \zeta^{m_j} - \sum_{x \in S_j} a_x = \sum_{x \in R_j} a_x.$$

Since $R_j \subset T_i$, we have $a_x = \zeta^{m_i}$ for all $x \in R_j$ and thus

$$-\varepsilon_0 \zeta^n + \varepsilon + \delta_1 \zeta^{m_j} - \sum_{x \in S_j} a_x = |R_j| \zeta^{m_i}. \quad (4.28)$$

Note that F_j is the disjoint union of T_j , R_j , and S_j , that $|T_j| \geq p^2 - p - \delta$ by (4.25) and $|R_j| \geq (p - \delta - 1)/2$ by (4.26). Hence

$$|S_j| \leq p^2 - \left((p^2 - p - \delta) + \frac{p - \delta - 1}{2} \right) = \frac{p + 3\delta + 1}{2}$$

and thus

$$|S_j| - |R_j| \leq \frac{p + 3\delta + 1}{2} - \frac{p - \delta - 1}{2} = 2\delta + 1. \quad (4.29)$$

Applying Corollary 1.17 to (4.28), using $|R_j| \geq (p - \delta - 1)/2$, $\delta_1 \leq \delta$, and (4.29), we conclude that at least

$$|R_j| - \frac{(2 + \delta_1 + |S_j|) - |R_j|}{q - 2} \geq \frac{p - \delta - 1}{2} - \frac{3(\delta + 1)}{q - 2}$$

roots of unity on the left hand side of (4.28) are equal to ζ^{m_i} . But the only roots of unity on the left hand side of (4.28) that may be equal to ζ^{m_i} are $-\varepsilon_0 \zeta^n$ and ε . We conclude

$$\frac{p - \delta - 1}{2} - \frac{3(\delta + 1)}{q - 2} \leq 2.$$

Using $\delta = (p+2)/(q-2)+2$, it is straightforward to check that this contradicts (4.21). $\square$

Lemma 4.5. *Every coset of W contains at most $p + 1$ full planes.*

Proof. Write $D = \sum_{j=0}^{p-1} D_j \alpha^j$ with $D_j \in \mathbb{Z}[\zeta_h][W]$. By (4.12), we have

$$\rho_i(D) = \sum_{j=0}^{p-1} \rho_i(D_j) \alpha^j = p^2 \zeta^{m_i} \alpha^{n_i} + p(\varepsilon_0 \zeta^n - \varepsilon_i \zeta^{m_i} \alpha^{n_i}) \langle \alpha^p \rangle + (\varepsilon - \varepsilon_0 \zeta^n) \langle \alpha \rangle. \quad (4.30)$$

Let t be the unique number in $\{0, \dots, p-1\}$ such that $t \equiv n_i \pmod{p}$ and write $n_i = t + sp$ with $0 \leq s \leq p-1$. First assume $n_i \not\equiv 0 \pmod{p}$. Comparing the terms that involve α^u with $u \equiv n_i \pmod{p}$ on both sides of (4.5), we conclude

$$\rho_i(D_t) \alpha^t = p^2 \zeta^{m_i} \alpha^{t+sp} - p \zeta^{m_i} \alpha^{t+sp} \langle \alpha^p \rangle + (\varepsilon - \varepsilon_0 \zeta^n) \alpha^t \langle \alpha^p \rangle$$

and thus

$$\rho_i(D_t) = p^2 \zeta^{m_i} \alpha^{sp} + (-p \zeta^{m_i} + \varepsilon - \varepsilon_0 \zeta^n) \langle \alpha^p \rangle. \quad (4.31)$$

Note that every nontrivial character of W that is trivial on V_i can be written in the form $\tau \circ \rho_i$ where τ is a nontrivial character of G/V_i . Hence (4.31) implies

$$\chi(D_t) = p^2 \zeta^{m_i} \chi(\alpha)^{sp} \quad (4.32)$$

for all nontrivial characters χ of W that are trivial on V_i . If $n_i \equiv 0 \pmod{p}$, then $t = 0$ and

$$\rho_i(D_0) = p^2 \zeta^{m_i} \alpha^{sp} + (\varepsilon_0 \zeta^n - p \zeta^{m_i} + \varepsilon - \varepsilon_0 \zeta^n) \langle \alpha^p \rangle$$

by (4.30). Hence, by a similar argument as above, we see that (4.32) also holds for $n_i \equiv 0 \pmod{p}$.

Note that the right hand side of (4.32) has absolute value p^2 . Hence, in summary, we have shown the following. If $n_i \equiv t \pmod{p}$, then

$$|\chi(D_t)| = p^2 \quad (4.33)$$

for all nontrivial characters χ of W that are trivial on V_i . Note that the number of such characters is $p - 1$.

Now assume that there are N full planes in a coset $W\alpha^t$. Then $n_i \equiv t \pmod{p}$ for N values $i \in \{1, \dots, p^2\}$. Thus, by (4.33), there are at least $N(p - 1)$ characters χ of W with $|\chi(D_t)| = p^2$. Since the coefficients of D_t are roots of unity, the coefficient of 1 in $D_t D_t^{(-1)}$ is p^3 . Hence, by the inversion formula,

$$p^3 = \frac{1}{p^3} \sum_{\chi \in \hat{W}} \chi(D_t D_t^{(-1)}) = \frac{1}{p^3} \sum_{\chi \in \hat{W}} |\chi(D_t)|^2.$$

As there are at least $N(p - 1)$ characters χ of W with $|\chi(D_t)| = p^2$, this implies $N(p - 1)p^4 \leq p^6$ and thus $N \leq p^2/(p - 1)$. As $p > 5$ by assumption (4.21), we conclude $N \leq p + 1$. $\square$

Lemma 4.6. *Let Wg be any coset of W in G , let L be a line in Wg not parallel to U , and let $F_1, \dots, F_s$ be all the full planes that contain L . If $s \geq 2$, then $\zeta^{m_1}, \dots, \zeta^{m_s}$ are not all equal.*

Proof. Assume that $\zeta^{m_1}, \dots, \zeta^{m_s}$ are all equal, say

$$\zeta^{m_1} = \dots = \zeta^{m_s} = \eta. \quad (4.34)$$

Write $R = \sum_{x \in LU} a_x$. By (4.34) and Lemma 4.3, we have

$$X_1 := \sum_{x \in L} a_x = \frac{1}{p}R + (p-1)s\eta - \sum_{i \in T} \zeta^{m_i}, \quad (4.35)$$

where $\{F_i : i \in T\}$ is the set of full planes in Wg that are parallel to L , but do not contain L . Write $U = \{u_1, \dots, u_p\}$. Note that a plane only can contain a line Lu_j if it is parallel to L . Moreover, in total there are exactly p full planes that are parallel to L . Thus there are at most p full planes in Wg that are parallel to L . As L is contained in at least two full planes by assumption, there is a line Lu_j , $1 \leq j \leq p$, which is not contained in any full plane. Note that a full plane is parallel to Lu_j if and only if it is parallel to L . Hence, using Lemma 4.3, we get

$$X_2 := \sum_{x \in Lu_j} a_x = \frac{1}{p}R - s\eta - \sum_{i \in T} \zeta^{m_i}. \quad (4.36)$$

By (4.35) and (4.36), we have $X_1 - X_2 = ps\eta$. But both X_1 and X_2 are sums of p roots of unity. This implies $s = 2$. Moreover all roots of unity occurring in X_1 are equal to η and all roots of unity occurring in X_2 are equal to $-\eta$. This is impossible since the roots of unity occurring in X_2 have odd order and η also has odd order. This contradiction shows that $\zeta^{m_1}, \dots, \zeta^{m_s}$ cannot all be equal. $\square$

Corollary 4.7. *Let Wg be any coset of W in G different from W . Then there is a line in Wg that is contained in all full planes Wg .*

Proof. Without loss of generality, let $V_1\alpha^{n_1}, \dots, V_t\alpha^{n_t}$, $0 \leq t \leq p^2$, be the full planes contained in Wg . Note that $|V_i\alpha^{n_i} \cap V_j\alpha^{n_j}| = p$ for all $i \neq j$. Thus the assertion of

the lemma holds for $t \leq 2$. Hence we may assume $t \geq 3$. By Lemma 4.6, not all of $\zeta^{m_1}, \dots, \zeta^{m_t}$ are equal. Thus we can assume $\zeta^{m_1} \neq \zeta^{m_2}$. Write $Q = V_1\alpha^{n_1} \cap V_2\alpha^{n_2}$. If any full plane $V_j\alpha^{n_j}$, $3 \leq j \leq t$, did not contain Q , then $V_1\alpha^{n_1}, V_2\alpha^{n_2}, V_j\alpha^{n_j}$ would form a prism. But then $\zeta^{m_1} = \zeta^{m_2}$ by Lemma 4.4, a contradiction. Hence all full lines in Wg must contain Q . $\square$

Corollary 4.8. *Let Wg be any coset of W in G different from W . Then Wg contains at most p full planes.*

Proof. Let $F_1, \dots, F_t$ be the full planes in Wg . By Lemma 4.7, there is a line L in Wg that is contained in each of those full planes. Note that LU is a plane in Wg that contains L and LU is not a full plane. As there are exactly $p+1$ planes in Wg that contain L , we conclude $t+1 \leq p+1$, that is, $t \leq p$. $\square$

Corollary 4.9. *There are at least p full planes contained in W .*

Proof. This follows from Corollary 4.8, since the total number of full planes is p^2 and the number of cosets of W in G that are different from W is $p-1$. $\square$

At this point, we have shown that all the full planes in a coset Wg distinct from W must intersect in a line and so there are at most p of them. Additionally, there are either p or $p+1$ full planes contained in W . We now show that the latter case is not possible by looking at the distribution of the coefficients in the full planes of W .

Lemma 4.10. *We have $\varepsilon = \varepsilon_0 = 1$. Furthermore, if F_i is a full plane in W , then*

$$|\{x \in F_i : a_x = \zeta^{m_i}\}| \geq \begin{cases} p^2 - 1, & \text{if } \zeta^{m_i} = \zeta^n, \\ p^2 - p, & \text{otherwise} \end{cases} \quad (4.37)$$

and

$$|\{x \in F_i : a_x = \zeta^n\}| \geq p - 1 \text{ if } \zeta^{m_i} \neq \zeta^n. \quad (4.38)$$

Proof. Without loss of generality, let $F_1, \dots, F_t$ be the full planes in W . By Corollary 4.9, we have $t \geq p$. Thus, by Lemma 4.6, not all of $\zeta^{m_1}, \dots, \zeta^{m_t}$ can be equal. In particular, we can assume $\zeta^{m_1} \neq \zeta^n$.

By (4.14), we have

$$\sum_{x \in F_1} a_x = (p^2 - p)\zeta^{m_1} + (p - 1)\varepsilon_0\zeta^n + \varepsilon$$

and thus

$$-(p - 1)\varepsilon_0\zeta^n - \varepsilon + \sum_{x \in F_1} a_x = (p^2 - p)\zeta^{m_1}. \quad (4.39)$$

Using Corollary 1.17, we conclude that at least $p^2 - p - 2p/(q - 2)$ roots of unity on the left hand side of (4.39) are equal to ζ^{m_1} . Thus, as $\zeta^{m_1} \neq \zeta^n$, we have $a_x = \zeta^{m_1}$ for at least $p^2 - p - 2p/(q - 2) - 1$ values of x . Hence there is a subset T of F_1 such $|T| \leq p + 2p/(q - 2) + 1$ and $a_x = \zeta^{m_1}$ for all $x \in F_1 \setminus T$. Using (4.39), we get

$$-(p - 1)\varepsilon_0\zeta^n - \varepsilon + \sum_{x \in T} a_x = d\zeta^{m_1},$$

where d is an integer with $0 \leq d \leq 2p/(q - 2) + 1$. We conclude

$$d\zeta^{m_1} - \varepsilon + \sum_{x \in T} a_x = (p - 1)\varepsilon_0\zeta^n. \quad (4.40)$$

Applying Corollary 1.17 again, we see that at least

$$p - 1 - \frac{(d + 1 + |T|) - (p - 1)}{q - 2} \geq p - 1 - \frac{\frac{4p}{q-2} + 4}{q - 2} = p - 1 - \frac{4(p + q - 2)}{(q - 2)^2}$$

roots of unity on the left hand side of (4.40) are equal to $\varepsilon_0\zeta^n$. Hence at least

$$p - 1 - \frac{4(p + q - 2)}{(q - 2)^2} - (d + 1) \geq p - 1 - \frac{4(p + q - 2)}{(q - 2)^2} - (2p/(q - 2) + 2) \quad (4.41)$$

of the numbers a_x , $x \in T$, are equal to $\varepsilon_0\zeta^n$. Using the assumptions $q \geq 7$ and (4.21), it is straightforward to show that the right hand side of (4.41) is positive. In particular, there is an x with $a_x = \varepsilon_0\zeta^n$. As a_x and ζ^n are both roots of unity of odd order, this implies $\varepsilon_0 = 1$.

Now consider any full plane F_i . By (4.14), we have

$$\sum_{x \in F_i} a_x = (p^2 - p)\zeta^{m_1} + (p - 1)\zeta^n + \varepsilon. \quad (4.42)$$

Now (4.37) and (4.38) follow from applying Lemmas 1.18 and 1.19 to (4.42). Finally, Lemmas 1.18 and 1.19 imply $\varepsilon^h = 1$. As $\varepsilon = \pm 1$ and h is odd, we conclude $\varepsilon = 1$. $\square$

In the following, we use a short form for specifying multisets, where (a, v) represents v occurrences of the element a . For instance, $\{(\zeta, 3), (\zeta^2, 2)\}$ and $\{(\zeta, 2), (\zeta, 1), (\zeta^2, 2)\}$ both denote the multiset $\{\zeta, \zeta, \zeta, \zeta^2, \zeta^2\}$.

Corollary 4.11. *Let F_i be any full plane in W . Then, as multisets,*

$$\{a_x : x \in F_i\} = \begin{cases} \{(\zeta^{m_i}, p^2 - p), (\zeta^n, p - 1), (1, 1)\} & \text{if } \zeta^{m_i} \neq \zeta^n, \\ \{(\zeta^n, p^2 - 1), (1, 1)\} & \text{if } \zeta^{m_i} = \zeta^n. \end{cases} \quad (4.43)$$

Proof. This follows from Lemma 4.10 and (4.42). $\square$

Lemma 4.12. *There is a line that is contained in all full planes in W .*

Proof. Without loss of generality, let $F_1, \dots, F_t$ be the full planes in W . By Lemma 4.5 and Corollary 4.9, we have $p \leq t \leq p + 1$. By Lemma 4.6, not all of $\zeta^{m_1}, \dots, \zeta^{m_t}$ are equal. Hence we can assume $\zeta^{m_1} \neq \zeta^{m_2}$ and $\zeta^{m_1} \neq \zeta^n$.

Assume that no line is contained in all full planes in W . First suppose that at least two of the numbers $\zeta^{m_2}, \dots, \zeta^{m_t}$ are equal to ζ^n . Consider any j, k with $\zeta^{m_j} = \zeta^{m_k} = \zeta^n$, $2 \leq j, k \leq t$, $j \neq k$, and any i with $1 \leq i \leq t$ and $\zeta^{m_i} \neq \zeta^n$. If F_i intersects F_j and F_k in different lines, then, by (4.43), the multiset $\{a_x : x \in F_i\}$ contains at least $2(p - 1)$ copies of the element ζ^n . But, again by (4.43), the element ζ^n occurs at most p times in $\{a_x : x \in F_i\}$, a contradiction. Hence we have shown the following.

$$\text{If } \zeta^{m_i} \neq \zeta^n \text{ and } \zeta^{m_j} = \zeta^{m_k} = \zeta^n, \text{ then } F_i \text{ contains } F_j \cap F_k. \quad (4.44)$$

Consider any r with $\zeta^{m_r} = \zeta^n$ and $r \neq j, k$. Then F_1 contains $F_j \cap F_r$ by (4.44). But F_1 also contains $F_j \cap F_k$ by (4.44) and thus $F_j \cap F_r = F_j \cap F_k$. Together with (4.44), this

shows that all full planes in W contain the line $F_j \cap F_k$. Hence we have shown that at most one of the numbers $\zeta^{m_2}, \dots, \zeta^{m_t}$ is equal to ζ^n .

Now suppose that one of the numbers $\zeta^{m_2}, \dots, \zeta^{m_t}$ is different from both ζ^{m_1} and ζ^n , say $\zeta^{m_2} \neq \zeta^{m_1}, \zeta^n$. Write $L = F_1 \cap F_2$. Note that $a_x \notin \{\zeta^{m_1}, \zeta^{m_2}\}$ for all $x \in L$ by (4.43), as $\zeta^{m_1} \neq \zeta^{m_2}$. Hence $a_x = \zeta^{m_1}$ for all $x \in F_1 \setminus L$ and $a_x = \zeta^{m_2}$ for all $x \in F_2 \setminus L$. Let $3 \leq i \leq t$. If F_i intersected F_1 and F_2 in two different lines L_1, L_2 , then $L_1, L_2 \neq L$ and thus there is $x \in L_1$ with $a_x = \zeta^{m_1}$ and $y \in L_2$ with $a_y = \zeta^{m_2}$. But this is impossible, since $\{a_x : x \in F_i\}$ cannot contain both ζ^{m_1} and ζ^{m_2} by (4.43). Hence every full plane in W contains the line $F_1 \cap F_2$. This contradicts our assumption that no line is contained in all full planes in W . Thus we have proved that none of $\zeta^{m_2}, \dots, \zeta^{m_t}$ is different from both ζ^{m_1} and ζ^n .

On the other hand, at most one of the numbers $\zeta^{m_2}, \dots, \zeta^{m_t}$ is equal to ζ^n . Thus exactly one of the numbers $\zeta^{m_2}, \dots, \zeta^{m_t}$ is equal to ζ^n and the others are equal to ζ^{m_1} . Without loss of generality, assume $\zeta^{m_1} = \dots = \zeta^{m_{t-1}}$ and $\zeta^{m_t} = \zeta^n$.

First assume that $F_i \cap F_j \subset F_t$ for all $i, j = 1, \dots, t-1, i \neq j$. Then $F_i \cap F_j = F_i \cap F_t$ for all such i, j and thus $F_i \cap F_j = F_1 \cap F_t$. Hence the line $F_1 \cap F_t$ is contained in all full planes in W , which contradicts our assumption.

Thus there are i, j with $i, j = 1, \dots, t-1, i \neq j$, and $F_i \cap F_j \not\subset F_t$. Write $L = F_i \cap F_j$. If F_k is any full line that contains L , then $k \neq t$ and thus $\zeta^{m_k} = \zeta^{m_1}$. But this contradicts Lemma 4.6. $\square$

Corollary 4.13. *Each coset of W in G contains exactly p full planes and these p planes contain a common line.*

Proof. By Lemma 4.12, there are at most p full planes in W , since any line is contained in at most p full planes. Each of the other cosets of W also contains at most p full planes by Corollary 4.8. Since the total number of full planes in G is p^2 , we conclude that every coset of W in G contains exactly p full planes. The remaining assertion of Corollary 4.13 is contained in Corollary 4.8 and Lemma 4.12. $\square$

Now we have shown that every coset of W contains p full planes such that they

intersect in a common line. However, we do not know where each of these lines lies with respect to each other. The next lemma reveals their structure.

Lemma 4.14. *Let $Wh_1, \dots, Wh_p$ be the cosets of W in G . Let L_i be the line in Wh_i that is contained in all full planes in Wh_i . Write $L_i = K_i c_i$, where K_i is a subgroup of W of order p . Then $UK_i = UK_j$ for all i, j and UK_1 is the union of U and $K_1, \dots, K_p$.*

Proof. Suppose that UK_i is different from UK_j . Then $K_i K_j$ is a subgroup of W of order p^2 that does not contain U . Note that $K_i K_j c_i$ is a plane that contains L_i and is not parallel to U . Thus $K_i K_j c_i$ is a full plane in Wh_i . Similarly, $K_i K_j c_j$ is a full plane in Wh_j . But this is impossible since no two full planes are parallel. Hence $UK_i = UK_j$ for all i, j . Note that K_i is different from K_j for all $i \neq j$, since otherwise there would exist distinct parallel full planes. This shows that UK_1 is the union of U and $K_1, \dots, K_p$. $\square$

The above lemma tells us that all the lines are parallel to a common plane containing U . Consequently, any lines contained in this plane are either K_i or U . Our next task is to show that the group ring element $\zeta^{m_i} F_i$ should appear in any group ring construction for $\text{BH}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p, h)$ and determine the conditions on the coefficients ζ^{m_i} .

Lemma 4.15. *Let L be the unique line in W which is contained in all full planes of W . Then as a multiset,*

$$\{a_x : x \in L\} = \{(\zeta^n, p-1), (1, 1)\}. \quad (4.45)$$

Furthermore for any full planes F_i contained in W ,

$$\{a_x : x \in F_i \setminus L\} = \{(\zeta^{m_i}, p^2 - p)\}. \quad (4.46)$$

Proof. Note that (4.46) follows immediately from (4.45) by (4.43). Thus, we will show that (4.45) is satisfied. Let F_1 and F_2 be full planes in W . By Lemma 4.6 and Corollary 4.13, we can assume that $\zeta^{m_1} \neq \zeta^{m_2}$ and $\zeta^{m_1} \neq \zeta^n$ without loss of generality. If there is no $x \in L$ such that $a_x = \zeta^{m_1}$, then $\{a_x : x \in L\} \subseteq \{(\zeta^n, p-1), (1, 1)\}$ as a multiset by (4.43). Since there are exactly p elements in both sets, the subset relation is actually an equality and thus (4.45) holds.

Now assume that there is a $x \in L$ such that $a_x = \zeta^{m_1}$. Recall that $a_x \in \{1, \zeta^n, \zeta^{m_2}\}$ as L is contained in F_2 . Hence $\zeta^{m_1} = 1$ in this case. By our assumption, we now have $\zeta^n \neq 1$ and $\zeta^{m_2} \neq 1$.

In the same way if there are no $y \in L \setminus \{x\}$ such that $a_y = \zeta^{m_2}$, then we have (4.45) since the remaining a_y 's must be equal to ζ^n and there are $p - 1$ of them. Now suppose on the contrary that there is some $y \in L \setminus \{x\}$ such that $a_y = \zeta^{m_2}$. Since L is also in F_1 and thus $a_y \in \{1, \zeta_n\}$, we get $\zeta^{m_2} = \zeta^n$. Consequently, this implies that $a_y = \zeta^n$ for all $y \in L \setminus \{x\}$ by (4.43) and hence (4.45) holds in particular. Therefore the lemma is proved in both cases. $\square$

Lemma 4.16. *Let Wg be a coset of W different from W . Suppose that F is a full plane in Wg and let $\alpha = \zeta^{m_i}$ be its associated coefficient. Let L be the common line in Wg contained in all full planes of Wg . Then for all $g \in F \setminus L$, we have $a_g = \alpha$.*

Proof. Let E be another full plane in Wg and its associated coefficient β . By Lemma 4.6 and Corollary 4.15, we can assume that $\alpha \neq \beta$. Write $F^- = F \setminus L$ and $E^- = E \setminus L$. By (4.17), we have

$$\sum_{x \in F^-} a_x - \sum_{x \in E^-} a_x = (p^2 - p)(\alpha - \beta). \quad (4.47)$$

Define $S = \{g \in F^- : a_g = \alpha\}$ and $T = \{g \in E^- : a_g = \beta\}$. Write $|F^- \setminus S| = N$ and $|E^- \setminus T| = M$. So

$$\sum_{x \in F^- \setminus S} a_x - \sum_{x \in E^- \setminus T} a_x + M\beta = N\alpha. \quad (4.48)$$

Since h is odd, all the roots of unity on the left side of (4.48) are different from α . Applying Lemma 1.17, we have $N \leq 2M/(q - 2)$. Using the same line of argument, we also get $M \leq 2N/(q - 2)$. With these two inequalities, we arrive at $N \leq 4N/(q - 2)^2$. Since $q \geq 7$, this implies that $N = 0$. In other words, the set S is equal to F^- and thus the lemma is proved. $\square$

Corollary 4.17. *Let Wg be a coset of W different from W and L be the common line in Wg contained in all full planes of Wg . Then $\sum_{x \in L} a_x = 1 - \zeta^n$.*

Proof. This follows immediately from (4.17) and Lemma 4.16. $\square$

Lemma 4.18. *Let Wg be any coset of W . Let $F_1, \dots, F_p$ be the full planes in Wg and $\zeta^{m_1}, \dots, \zeta^{m_p}$ denote their corresponding coefficients. Let L be the line in Wg that is contained in all the full planes F_i . Then for all $y \in L$ and $x \in Uy \setminus \{y\}$.*

$$a_x = \begin{cases} 1 - \sum_{i=1}^p \zeta^{m_i}, & \text{if } Wg = W \text{ and } y = 1, \\ \zeta^n - \sum_{i=1}^p \zeta^{m_i}, & \text{if } Wg = W \text{ and } y \neq 1, \\ a_y, & \text{otherwise.} \end{cases}$$

Furthermore if Wg is different from W , then $\sum_{i=1}^p \zeta^{m_i} = 0$.

Proof. Write $L = K_1c$, where K_1 is a subgroup of W of order p and let $K_0, K_1, \dots, K_p$ be the subgroups of UK_1 of order p , with $K_0 = U$. For each $y \in LU$, write $y = lu$ where $l \in L, u \in U$. Recall that line $K_1y = L$ is contained in all the full planes in Wg if $y \in L$, line K_1y is parallel to, but not contained in, all full planes in Wg , if $y \notin L$, and line K_iy is not parallel to any full planes in Wg . So by Lemma 4.3,

$$\sum_{x \in K_iy} a_x = \begin{cases} (p-1) \sum_{j=1}^p \zeta^{m_j} + \frac{1}{p}R, & \text{if } i = 1, u = 1 \\ - \sum_{j=1}^p \zeta^{m_j} + \frac{1}{p}R, & \text{if } i = 1, u \neq 1 \\ \frac{1}{p}R, & \text{if } 2 \leq i \leq p, \end{cases}$$

where $R = \sum_{x \in LU} a_x$.

Fix $y = lu \in LU$. Since every element not equal to y of LU is contained in exactly only one of the line K_iy with y contained in all the lines K_iy 's, this gives

$$\begin{aligned} R &= \sum_{x \in LU} a_x = \sum_{i=0}^p \sum_{x \in K_iy} a_x - pa_y \\ &= R - pa_y + (\gamma_y p - 1) \sum_{i=1}^p \zeta^{m_i} + \sum_{x \in Uy} a_x, \end{aligned}$$

where $\gamma_y = 1$ if $y \in L$ and $\gamma_y = 0$ otherwise. That is,

$$\sum_{x \in Uy} a_x = pa_y - (\gamma_y p - 1) \sum_{i=1}^p \zeta^{m_i}. \quad (4.49)$$

Consider $y \in L$ and $x \in Uy$ distinct from y . Note that if we write $y = l_1 u_1$ and $x = l_2 u_2$, then $u_1 = 1$, $u_2 \neq 1$. So $\gamma_y = 1$ and $\gamma_x = 0$ and by (4.49), we have

$$pa_y - (p-1) \sum_{i=1}^p \zeta^{m_i} = pa_x + \sum_{i=1}^p \zeta^{m_i}. \quad (4.50)$$

This proves the lemma for $Wg = W$.

It remains to show that $\sum_{i=1}^p \zeta^{m_i} = 0$ for cosets Wg different from W . From (4.50) we have

$$a_{y_1} - a_{x_1} = a_{y_2} - a_{x_2},$$

where $y_1, y_2 \in L$ and $x_i \in Uy_i \setminus \{y_i\}$. Since the terms are all roots of unity, they must cancel out in pairs. As h is odd, we have $a_{y_1} \neq -a_{x_2}$. This leaves us with $a_{y_1} \in \{a_{x_1}, a_{y_2}\}$.

Suppose that $\sum_{i=1}^p \zeta^{m_i} \neq 0$. Then $a_{y_1} = a_{y_2}$. Furthermore, this is true for any pair of $y_1, y_2 \in L$ and so $\sum_{y \in L} a_y = p\eta$, for some h^{th} root of unity η . We can assume that $\eta \neq \zeta^{m_i}$ for some i . In the full plane F_i , we have

$$\sum_{x \in F_i} a_x = (p^2 - p)\zeta^{m_i} + p\eta = (p^2 - p)\zeta^{m_i} + 1 - \zeta^n,$$

by Lemma 4.16. But this implies that $p \leq 2$, a contradiction. Therefore $\sum_{i=1}^p \zeta^{m_i} = 0$ as desired. $\square$

Corollary 4.19. *Let $\zeta^{m_1}, \dots, \zeta^{m_p}$ be the coefficients corresponding to the full planes contained in W . Then either $1 = \zeta^n$ or $\sum_{i=1}^p \zeta^{m_i} = 0$.*

We summarize the results on $BH(G, h)$ so far. We use the notation from subsection 4.2.1. Recall that we write $G = \langle \alpha \rangle \times \langle \beta \rangle \times \langle \gamma \rangle$, $W = \langle \alpha^p \rangle \times \langle \beta \rangle \times \langle \gamma \rangle$ and $U = \langle \alpha^p \rangle$, where the order of α is p^2 and the orders of β and γ are p .

By Corollary 4.13, there are exactly p full planes in each coset of W and the p full planes contain a common line. So for each $i = 0, \dots, p-1$, let $F_{i,0}, \dots, F_{i,p-1}$ be full planes in $W\alpha^i$. Furthermore, let L_i be the unique line contained in the full planes $F_{i,j}$, $j = 1, \dots, p-1$, that is $L_i = F_{i,0} \cap \dots \cap F_{i,p-1}$. Without loss of generality, we can assume that $L_0 = \langle \gamma \rangle$. Let $K_0, \dots, K_{p-1}$ be the subgroups of L_0U which are distinct from U . By Lemma 4.14, we can write $L_i = K_i g_i$, where $g_i = \alpha^i \beta^{e_i} \gamma^{f_i}$ for some integers e_i, f_i , with $e_0 = 0$ and $\{e_1, \dots, e_{p-1}\} = \{1, \dots, p-1\}$, and $f_i \in \mathbb{Z}$.

Write $F_{i,j} = V_{i,j} g_i$, where $V_{i,j}$ is a subgroup of W of order p^2 not containing U . Using Lemma 4.15 and 4.16, we have $\{a_x : x \in F_{i,j} \setminus L_i\} = \{(\zeta^{m_{i,j}}, p)\}$. Let $h_{i,k} = \alpha^i \beta^{e_i} \gamma^k$ and $U_{i,k} = U h_{i,k}$. Note that $U_{i,k}$ are simply the cosets of U in $L_i U$ with $h_{i,k} \in L_i$. For $i > 0$, we have $\{a_x : x \in U_{i,k}\} = \{(\eta_{i,k}, p)\}$, with $\sum_{k=0}^{p-1} \eta_{i,k} = 1 - \zeta^n$ by Corollary 4.17 and $\sum_{j=1}^p \zeta^{m_{i,j}} = 0$. If $i = 0$, then $\{a_x : x \in U_{0,k} \setminus L_0\} = \{(\eta_{0,k}, p-1)\}$ such that $\eta_{0,1} = \dots = \eta_{0,p-1} = \eta$, and $\{a_x : x \in L_0\} = \{(1, 1), (\zeta^n, p-1)\}$. Using Lemma 4.18, we have

$$\sum_{j=1}^p \zeta^{m_{0,j}} = 1 - \eta_{0,0} = \zeta^n - \eta_{0,k},$$

where $k > 0$. Furthermore, either $\sum_{j=1}^p \zeta^{m_{0,j}} = 0$ or $\zeta^n = 1$ by Corollary 4.19. Therefore, X has the form

$$X = \sum_{i=0}^{p-1} \left(\sum_{j=0}^{p-1} \zeta^{m_{i,j}} F_{i,j} + \sum_{k=0}^{p-1} \eta_{i,k} U_{i,k} \right) = \sum_{i=0}^{p-1} \left(\sum_{j=0}^{p-1} \zeta^{m_{i,j}} V_{i,j} \gamma^{f_i} + \eta_{i,j} U \gamma^j \right) \alpha^i \beta^{e_i},$$

where e_i and $\eta_{i,j}$ are to be determined.

Our next step is to determine the coefficients of the cosets $U\alpha^i \beta^{e_i}$. Let Ug be a coset of U contained in $W\alpha^i$ but not contained in $L_i U$. In other words, $Ug \neq U_{i,k}$ for any k . Since U is not contained in $V_{i,j}$, we have $|F_{i,j} \cap Ug| = 1$. Let u be the unique element in

$F_{i,j} \cap Ug$. Then $u \notin L_i$ and thus $a_u = \zeta^{m_{i,j}}$. Hence,

$$\sum_{x \in Ug} a_x = \begin{cases} p - (p-1)S, & \text{if } Ug = U, \\ p\zeta^n - (p-1)S, & \text{if } Ug \subset L_0U \text{ and } Ug \neq U, \\ S, & \text{if } Ug \subset W \text{ and } Ug \not\subset L_0U, \\ p\eta_{i,k}, & \text{if } Ug = U_{i,k} \text{ and } i > 0 \\ 0, & \text{otherwise,} \end{cases} \quad (4.51)$$

where $S = \sum_{j=1}^p \zeta^{m_{0,j}} = 1 - \xi$. Let $\pi : G \rightarrow G/U$ be the natural epimorphism and write $\pi(g) = \bar{g}$. Hence, we have

$$\begin{aligned} \pi(D) &= p - (p-1)S + \sum_{k=1}^{p-1} (p\zeta^n - (p-1)S) \bar{\gamma}^k + \sum_{j=1}^{p-1} \sum_{k=0}^{p-1} S \bar{\beta}^j \bar{\gamma}^k \\ &\quad + \sum_{i=1}^{p-1} \left(\sum_{k=0}^{p-1} p\eta_{i,k} \bar{\gamma}^k \right) \bar{\alpha}^i \bar{\beta}^{e_i}. \end{aligned} \quad (4.52)$$

Suppose that $S = 0$. Then (4.52) gives

$$\pi(D) = p + \sum_{k=1}^{p-1} p\zeta^n \bar{\gamma}^k + \sum_{i=1}^{p-1} \left(\sum_{k=0}^{p-1} p\eta_{i,k} \bar{\gamma}^k \right) \bar{\alpha}^i \bar{\beta}^{e_i}.$$

On the other hand if $S \neq 0$, then $\zeta^n = 1$. Note that this implies that $\eta_{0,k} = \xi$ for all k . In this case, (4.52) gives

$$\pi(D) = \sum_{k=0}^{p-1} \left[(1 + (p-1)\xi) + \sum_{j=1}^{p-1} (1 - \xi) \bar{\beta}^j \right] \bar{\gamma}^k + \sum_{i=1}^{p-1} \left(\sum_{k=0}^{p-1} p\eta_{i,k} \bar{\gamma}^k \right) \bar{\alpha}^i \bar{\beta}^{e_i}.$$

Let χ be a character of G/U satisfying $\chi(\bar{\beta}) = 1$. Then in both cases, we obtain

$$p^4 = |\chi(\pi(D))|^2 = p^2 \left| 1 + \sum_{k=1}^{p-1} \zeta^n \chi(\bar{\gamma}^k) + \sum_{i=1}^{p-1} \left(\sum_{k=0}^{p-1} \eta_{i,k} \chi(\bar{\gamma}^k) \right) \chi(\bar{\alpha}^i) \right|^2.$$

Note that there is a one-to-one correspondence between χ and the characters τ of $\mathbb{Z}_p \times \mathbb{Z}_p$ generated by $\bar{\alpha}$ and $\bar{\gamma}$. Therefore, we have the following lemma.

Lemma 4.20. *The group ring element Y given by*

$$Y := 1 + \sum_{k=1}^{p-1} \zeta^n \bar{\gamma}^k + \sum_{i=1}^{p-1} \sum_{k=0}^{p-1} \eta_{i,k} \bar{\gamma}^k \bar{\alpha}^i \quad (4.53)$$

is a $BH(\mathbb{Z}_p \times \mathbb{Z}_p, h)$ matrix.

Since the coefficients $\eta_{i,j}$ necessarily appears as entries in a $BH(\mathbb{Z}_p \times \mathbb{Z}_p, h)$ matrix, we use Theorem 4.1 to see that most of them should be equal to one another.

Lemma 4.21. *Suppose that $0 \leq i_1, i_2, j_1, j_2 \leq p-1$ with $i_1, i_2 \neq 0$. If $i_1 j_2 \equiv i_2 j_1 \pmod{p}$ then $\eta_{i_1, j_1} = \eta_{i_2, j_2}$.*

Proof. Consider the group ring element Y defined in (4.53). Note that $\tau_0(Y) = p$ and so by Theorem 4.1 and Lemma 4.20, we have

$$Y g^{-1} = \sum_{k=0}^{p-1} \xi_k \langle \bar{\alpha} \bar{\gamma}^k \rangle + \xi_p \langle \bar{\gamma} \rangle,$$

for some h th roots of unity ξ_k and $g = \bar{\alpha}^e \bar{\gamma}^f$ for some integers e, f . We claim that $e = 0$. Suppose that $e > 0$ and let k be an integer such that $0 \leq k \leq p-1$ and let $j \equiv f - ek \pmod{p}$. Then,

$$\bar{\gamma}^j = \bar{\gamma}^{f-ek} = \bar{\alpha}^e \bar{\gamma}^f \cdot (\bar{\alpha} \bar{\gamma}^k)^{-e} \in \langle \bar{\alpha} \bar{\gamma}^k \rangle g.$$

Also note that if $\bar{\gamma}^j$ is contained in another coset $\langle \bar{\alpha} \bar{\gamma}^{k_0} \rangle g$ or $\langle \bar{\gamma} \rangle g$, then $\bar{\gamma}^j = g$ which is not possible. So $\bar{\gamma}^j$ is contained in only in $\langle \bar{\alpha} \bar{\gamma}^k \rangle g$. Hence $\xi_k = z_{0,j} = 1$, if $k \equiv e^{-1}f \pmod{p}$ and $\xi_k = z_{0,j} = \zeta^n$ otherwise. Using (4.2), we get $\sum_{k=0}^p \xi_k = 1$ and this gives $(p-1)\zeta^n + \xi_p = 0$ which implies that $p = 2$, a contradiction.

Furthermore if $\zeta^n \neq 1$, then we have $f = 0$. Indeed if $f > 0$, then g is contained in $\langle \bar{\gamma} \rangle g$ and $\langle \bar{\alpha} \bar{\gamma}^k \rangle g$, $k = 0, \dots, p-1$. So $\zeta^n = \sum_{k=0}^p \xi_k = 1$, which is not possible. On the other hand, if $\zeta^n = 1$, then we can replace X with $X \bar{\gamma}^f$ without any loss of generality

and therefore $f = 0$ again. Hence for $i > 0$, we get $\eta_{i,j} = \xi_k$, where $k \equiv i^{-1}j \pmod{p}$. This proves the lemma. $\square$

It remains to find out what the values of e_i should be. To that end, we can use Result 3.3 on the quotient group of G over the subgroups of order p^3 which are different from W .

Lemma 4.22. *Suppose that $\zeta^n \neq 1$. Then $e_i \equiv \lambda i \pmod{p}$, for some $\lambda \in \mathbb{Z}$.*

Proof. First, observe that ζ^n is not real since h is odd and $\zeta^n \neq 1$. Let $H = LU\langle\alpha\rangle$ and consider the projection $\pi : G \rightarrow G/H$. By Lemma 3.3, we have

$$\pi(D) = p^2\eta \cdot H\beta^b + p(1 - \eta) \cdot G/H,$$

for some integer b and h^{th} root of unity η . In other words, that is

$$\sum_{x \in H\beta^j} a_x = \begin{cases} (p^2 - p)\eta + p, & \text{if } j = b, \\ -p\eta + p, & \text{otherwise.} \end{cases}$$

On the other hand by Lemma 4.15, 4.16, 4.18 and Corollary 4.19, we have

$$\sum_{x \in LUg} a_x = \begin{cases} p + (p^2 - p)\zeta^n, & \text{if } LUg = LU, \\ p(1 - \zeta^n), & \text{if } LUg = L_iU = LU\alpha^i\beta^{e_i} \text{ and } i > 0 \\ 0, & \text{otherwise.} \end{cases}$$

Consequently, this gives

$$\sum_{x \in H\beta^j} a_x = \begin{cases} p + (p^2 - p)\zeta^n + N_j p(1 - \zeta^n), & \text{if } j = 0, \\ N_j p(1 - \zeta^n), & \text{otherwise,} \end{cases}$$

where $N_j = \#\{i \in \{1, \dots, p-1\} : e_i = j\}$, that is, the number of cosets L_iU contained in $H\beta^j$.

We claim that $b = 0$, that is, $H = H\beta^b$. Suppose not and assume that $b = 1$ without

loss of generality. Observe that

$$N_i(1 - \zeta^n) = 1 - \eta = N_j(1 - \zeta^n), \quad \text{for } 2 \leq i, j \leq p-1,$$

and thus $N_2 = \cdots = N_{p-1}$. Consequently, we have $N_0 + N_1 + (p-2)N_2 = p-1$ and so $N_2 \leq (p-1)/(p-2)$. This implies that $N_2 = 0$ or 1 . Suppose that $N_2 = 0$, then $\eta = 1$. This gives $N_0\zeta^n = N_0 - p$ but this implies that ζ^n is real if $N_0 > 0$. On the other hand if $N_0 = 0$, then $p = 0$, which is a contradiction. Now suppose that $N_2 = 1$, then $\eta = \zeta^n$. This gives $(p - N_1)\zeta^n = -N_1$, which implies that ζ^n is real or $p = 0$, both of which are impossible.

We can repeat the same line of reasoning in the previous paragraph to get $N_0 = p-1$, $N_1 = \cdots = N_{p-1} = 0$ or $N_0 = 0$, $N_1 = \cdots = N_{p-1} = 1$. In the first case, we obtain $e_i = 0 = 0 \cdot i$, for $i = 1, \dots, p-1$. In the second case, write $k = e_1 \neq 0$ and consider $H_1 = LU\langle\alpha\beta^k\rangle$. Note that everything from above still holds if we replace H with H_1 and N_j with $M_j = \#\{i \in \{1, \dots, p-1\} : e_i \equiv ki + j \pmod{p}\}$ instead. In particular $M_0 \geq 1$ and so $M_0 = p-1$. In other words, we have $e_i \equiv ki \pmod{p}$ for $i = 1, \dots, p-1$. $\square$

Note in the case that $\zeta^n \neq 1$, we have completely determined the form of X . From here on, we assume that $\zeta^n = 1$. Let $H = \langle\alpha\rangle \times \langle\beta\gamma\rangle$ and consider the natural epimorphism π of G onto G/H . By Lemma 3.3, we have

$$\pi(D) = p^2\eta H\gamma^b + p(1 - \eta)G/H,$$

for some integer b and h^{th} root of unity η . In other words, that is

$$\sum_{x \in H\gamma^k} a_x = \begin{cases} (p^2 - p)\eta + p, & \text{if } k = b, \\ -p\eta + p, & \text{otherwise.} \end{cases}$$

On the other hand, we rewrite (4.51) to get

$$\sum_{x \in U\alpha^i\beta^j\gamma^k} a_x = \begin{cases} 1 + (p-1)\xi, & \text{if } i \equiv j \equiv 0 \pmod{p}, \\ 1 - \xi, & \text{if } i \equiv 0 \text{ and } j \not\equiv 0 \pmod{p}, \\ p\eta_{i,k}, & \text{if } i \not\equiv 0 \text{ and } j \equiv e_i \pmod{p}, \\ 0, & \text{otherwise.} \end{cases}$$

From here on, all computations in the indices are to be taken modulo p . Thus we obtain $\sum_{x \in H\gamma^k} a_x = p + p \sum_{i=1}^{p-1} \eta_{i,e_i+k}$ and therefore

$$\sum_{i=1}^{p-1} \eta_{i,e_i+k} = \begin{cases} (p-1)\eta & \text{if } k = b, \\ -\eta, & \text{otherwise.} \end{cases}$$

Hence we have $\eta_{i,e_i+b} = \eta_{j,e_j+b}$, for all $1 \leq i, j \leq p-1$.

Lemma 4.23. *Suppose that $\zeta^n = 1$. Then there are integers λ, μ such that $e_i \equiv \lambda i + \mu \pmod{p}$, for all $i = 1, \dots, p-1$.*

Proof. Let $m_i \equiv (e_i + b)i^{-1} - (e_1 + b) \pmod{p}$. Using Lemma 4.21, we write $\eta_{i,ci} = \xi_c$, where c is an integer. Then for any i ,

$$\xi_{e_1+b} = \eta_{1,e_1+b} = \eta_{i,e_i+b} = \eta_{i,(e_1+b+m_i)i} = \xi_{e_1+b+m_i}. \quad (4.54)$$

Let A be the subgroup of $(\mathbb{Z}_p, +)$ generated by $\{m_1, \dots, m_{p-1}\}$. For any x, y in the coset $(e_1 + b) + A$, we have $\xi_x = \xi_y$ by (4.54). If there is some m_i such that $m_i \not\equiv 0 \pmod{p}$, then the subgroup A is the whole of $\mathbb{Z}_p$. Consequently, this implies that all the ξ_c 's are equal. By (4.2), this gives $1 = \sum_{c=0}^{p-1} \xi_c = (p-1)\xi_0$. But this is impossible since that implies $p = 2$. Hence $m_i \equiv 0 \pmod{p}$ for all i . In other words, we get $e_i \equiv (e_1 + b)i - b \pmod{p}$ and we are done. $\square$

With Lemmas 4.21, 4.22 and 4.23, we have determined the conditions on the values of e_i and the coefficients $\eta_{i,j}$.

Theorem 4.24. *Let p be an odd prime and let h be a positive odd integer which is not divisible by p . Further assume that p is self-conjugate modulo h and*

$$p > \frac{7q-8}{q-5} \text{ and } q \geq 7,$$

where q is the smallest prime divisor of h .

Write $\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p = \langle \alpha \rangle \times \langle \beta \rangle \times \langle \gamma \rangle$ and $U = \langle \alpha^p \rangle$, where the order of α is p^2 and the orders of β and γ are p . Let $W = \langle \alpha^p \rangle \times \langle \beta \rangle \times \langle \gamma \rangle$, $S = \langle \alpha^p \rangle \times \langle \gamma \rangle$ and $U = \langle \alpha^p \rangle$. For $i, j = 0, \dots, p-1$, let L_i be the subgroups of order p different from U contained in S and $V_{i,j}$ be the subgroups of order p^2 contained in W such that $\cap_{j=0}^{p-1} V_{i,j} = L_i$.

Let f_i be any integer and write $e_0 = 0$ and $e_i = \lambda i + \mu$, where λ, μ are integers, for $i = 1, \dots, p-1$. Then all $\text{BH}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p, h)$ matrices must be obtained from the group ring elements

$$D = \sum_{i=0}^{p-1} \left(\sum_{j=0}^{p-1} \zeta_{i,j} V_{i,j} \gamma^{f_i} + \eta_{i,j} U \gamma^j \right) \alpha^i \beta^{e_i},$$

using Result 2.1, in which the $\zeta_{i,j}, \eta_{i,j}$'s are h th roots of unity satisfying

$$\sum_{j=0}^{p-1} \zeta_{0,j} = 1 - \xi \quad \text{and} \quad \sum_{j=0}^{p-1} \zeta_{i,j} = 0, \quad \text{for } i = 1, \dots, p-1,$$

where ξ is a root of unity, and $\eta_{0,0} = \eta_{0,1} = \dots = \eta_{0,p-1}$,

$$1 + \sum_{k=1}^{p-1} \xi' \gamma^k + \sum_{i=1}^{p-1} \sum_{k=0}^{p-1} \eta_{i,k} \gamma^k \alpha^{pi} \in \text{BH}(\mathbb{Z}_p \times \mathbb{Z}_p, h)$$

and one of the following holds:

1. $\xi' = \xi = 1$, or
2. $\xi' = 1$, $\xi = \eta_{0,0} \neq 1$, or
3. $\xi' = \eta_{0,0} \neq 1$, $\xi = 1$, $\mu = 0$.

Chapter 5

Conclusion and Future Work

Our study of Butson Hadamard matrices deals with the existence, non-existence, and classification of these objects. In the first part of this dissertation, we adapted ideas from similar combinatorial objects, such as difference sets, to construct group-invariant Butson Hadamard matrices for $\mathbb{Z}_p^{2a}$ by using big subgroups, for $\mathbb{Z}_{p^a}^2$ by using nested cyclic groups, for $\mathbb{Z}_{p^2}^a$ by using the structure of Galois Rings, for $\mathbb{Z}_{p^a} \times \mathbb{Z}_p^a$ by using hyperplanes, and for $G \times \mathbb{Z}_p^a$ with $|G| = p^a$ by using the Folding theorem and the direct product of any groups listed by using the Kronecker product. Thus we demonstrated the existence of many different types of $\text{BH}(p^{2a}, h)$ matrices. Next, we extended a version of Ma's Lemma for $\mathbb{Z}[G]$ so that we can apply it to group ring elements $\mathbb{Z}[\zeta_h][G]$ instead and used it to derive an exponent bound for groups G for which a $\text{BH}(G, h)$ matrix exists. And to conclude our study, we completely classified $\text{BH}(\mathbb{Z}_p \times \mathbb{Z}_p, h)$ and $\text{BH}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p, h)$ matrices, under the self conjugacy assumption.

In the existence problem of $\text{BH}(G, h)$ matrices, where G is an abelian p -group and h is not divisible by p , the smallest abelian p -group satisfying the exponent bound for which the construction of a group-invariant Butson Hadamard matrix has not been discovered is $\mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_p$. However, we conjecture that for all abelian p -groups G of order p^{2a} with $\exp(G) \leq p^a$, there exists a $\text{BH}(G, h)$ matrix, where h satisfies some conditions. In the classification problem, the next unsolved case is that for $\text{BH}(\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}, h)$ case. Otherwise, one might be interested to see if the conditions $p > (7q - 8)/(q - 5)$ and $q \geq 7$ can be relaxed for the $\text{BH}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p, h)$ case. We believe these are some possible

directions to look at for future work in this area.

Bibliography

- [1] J. André: Über nicht-desarguessche Ebenen mit transitiver Translationsgruppe. *Mathematische Zeitschrift*, **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] A. T. Butson: Generalized Hadamard Matrices *Proc. Amer. Math. Soc.*, **13** (1962), 894–898
- [5] A. T. Butson: Relations among generalized Hadamard matrices, relative difference sets, and maximal length linear recurring sequences. *Canad. J. Math.*, **15** (1963), 42–48
- [6] Z. I. Borevich, I. R. Shafarevich: *Number Theory*. Academic Press 1966.
- [7] B. W. Brock: Hermitian congruence and the existence and completion of generalized Hadamard matrices. *J. Combin. Theory A* **49** (1988), 233–261.
- [8] C. H. Cooke, I. Heng: On the non-existence of some generalized Hadamard matrices. *Australas. J. Combin.* **19** (1999), 137–148.
- [9] B. Compton, R. Craigen, W. de Launey: Unreal $BH(n, 6)$ ’s and Hadamard matrices. *Des. Codes Cryptogr.* **79** (2016), 219–229.

- [10] J. H. Conway and A. J. Jones: Trigonometric Diophantine equations (On vanishing sums of roots of unity). *Acta Arith.* **30** (1976), 229–240.
- [11] R. Craigen: Equivalence classes of inverse orthogonal and unit Hadamard matrices. *Bull. Austral. Math. Soc.* **44** (1991), 109–115.
- [12] 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.
- [13] J. A. Davis: Difference sets in abelian 2-groups. *J. Combin. Theory A* **57** (1991), 262–286.
- [14] J. A. Davis: Construction of relative difference sets in p -groups. *Discrete Math.* **103** (1992), 7–15.
- [15] J. A. Davis, J. Jewab: A unifying construction for difference sets. *J. Combin. Theory A* **80** (1997), 13–78.
- [16] T. D. Duc: Necessary Conditions for the Existence of Group-Invariant Butson Hadamard matrices and a New Family of Perfect Arrays. *Des. Codes Cryptogr.* **88** (2020), 73–90.
- [17] T. D. Duc: New Constructions of Group-Invariant Butson Hadamard matrices. Preprint. [arXiv:1903.09824](https://arxiv.org/abs/1903.09824)
- [18] T. D. Duc, B. Schmidt: Bilinear Forms on Finite Abelian Groups and Group-Invariant Butson Hadamard matrices. *J. Combin. Theory A* **166** (2019), 337–351.
- [19] R. Egan, D. Flannery, P. Cathin: Classifying cocyclic Butson Hadamard matrices. *Springer Proc. Math. Stat.* **133** (2015), 93106
- [20] K. Fender, H. Kharaghani, S. Suda: On a class of quaternary complex Hadamard matrices. *Discrete Math.* **341** (2018), 421–426.

- [21] U. Haagerup: Orthogonal maximal abelian $*$ -subalgebras of the $n \times n$ matrices and cyclic n -roots. *Operator Algebras and Quantum Field Theory (Rome)*, Int. Press, Cambridge, MA (1996), 296–322
- [22] J. Hadamard: Resolution d’une question relative aux determinants. *Bull. Des Sciences Math.* **17** (1983), 240–246
- [23] M. Hagita, B. Schmidt: Bijections between group rings preserving character sums. *Des. Codes Cryptogr.* **24** (2001), 243–254.
- [24] M. Hall Jr.: Hadamard matrices of order 16. *Jet Propulsion Laboratory Research Summary* **1** (1961), 21–26
- [25] G. Hiranandani, J. M. Schlenker: Small circulant complex Hadamard matrices of Butson type. *Eur. J. Com.* **51** (2016), 306–314.
- [26] M. Hirasaka, K. Kim, Y. Mizoguchi: Uniqueness of Butson Hadamard matrices of small degrees. *J. Discrete Algorithms* **34** (2015), 70–77.
- [27] J. W. P. Hirschfeld: *Projective Geometries over Finite Fields* (Second Edition), Oxford University Press 1998.
- [28] T. Ikuta, A. Munemasa: Butson-type complex Hadamard matrices and association schemes on Galois rings of characteristic 4. *Spec. Matrices* **6** (2018), 1–10.
- [29] D. Jungnickel: On automorphism groups of divisible designs. *Canadian J. Math.* **34** (1982), 257–297.
- [30] H. Kharaghani, B. Tayfeh-Rezaie: Hadamard matrices of order 32. *J. Combin. Des.* **21** (2013), 212–221.
- [31] H. Kharaghani, B. Tayfeh-Rezaie: On the classification of Hadamard matrices of order 32. *J. Combin. Des.* **18** (2010), 328–336.
- [32] M. Kibler: *Galois Fields and Galois Rings Made Easy*. Elsevier, 2017.

- [33] H. Kimura: Classification of Hadamard matrices of order 28. *Discrete Math.* **133** (1994), 171–180.
- [34] H. Kimura: Classification of Hadamard matrices of order 28 with Hall sets. *Discrete Math.* **128** (1994), 257–268.
- [35] R. G. Kraemer: Proof of a conjecture on Hadamard 2-groups. *J. Combin. Theory A* **63** (1993), 1–10.
- [36] P. V. Kumar, R. A. Scholtz, L. R. Welch: Generalized bent functions and their properties. *J. Combin. Theory Ser. A* **40** (1985), 90–107.
- [37] P. H. J. Lampio, P. Östergård, F. Szöllösi: Orderly generation of Butson Hadamard matrices. *Math. Comp.* **89** **321** (2020), 313–331.
- [38] P. H. J. Lampio, P. Östergård, F. Szöllösi: The quaternary complex Hadamard matrices of orders 10, 12, and 14. *Discrete Math.* **313** (2013), 189–206.
- [39] W. de Launey: Circulant $\text{GH}(p^2, \mathbb{Z}_p)$ exist for all primes p . *Graphs Combin.* **8** (1992), 317–321.
- [40] W. de Launey: Generalised Hadamard matrices which are developed modulo a group. *Discrete Math.* **104** (1992), 49–65.
- [41] T. Y. Lam, K. H. Leung: On vanishing sums of roots of unity. *J. Algebra* **224** (2000), 91–109.
- [42] K. H. Leung, S. L. Ma: Constructions of partial difference sets and relative difference sets on p -groups. *Bull. London Math. Soc.* **22** (1990), 533–539.
- [43] K. H. Leung, S. Ling, S. L. Ma: Constructions of semi-regular relative difference sets. *Finite Fields Appl.* **7** (2001), 397–414.
- [44] W. LeVeque: Topics in Number Theory, Vol. 1 *Addison-Wesley, Reading, Mass.* (1956)
- [45] H. Lüneburg: *Translation Planes*. Springer 1980.

- [46] S. L. Ma: Polynomial addition sets and polynomial digraphs. *Linear Algebra Appl.* **69** (1985), 213–230.
- [47] S. L. Ma: *Polynomial addition sets*. Ph.D. thesis, University of Hong Kong, 1985.
- [48] S. L. Ma and A. Pott: Relative difference sets, planar functions, and generalized Hadamard matrices. *J. Algebra* **175** (1995), 505–525.
- [49] B. R. McDonald: *Finite rings with identity*. Pure and Applied Mathematics, Vol. 28. Marcel Dekker, Inc., New York, 1974.
- [50] R. E. A. C. Paley: On Orthogonal Matrices *J. Math. Phys.* **12** (1933), 311–320.
- [51] O. S. Rothaus: On Bent Functions. Institute of Defense Analysis, USA, W. P. 169 (1966).
- [52] O. S. Rothaus: On “bent” functions. *J. Combinatorial Theory Ser. A* **20** (1976), 300–305.
- [53] B. Schmidt: A Survey of Group Invariant Butson Hadamard matrices and Their Relation to Generalized Bent Functions and Various Other Objects. *Radon Series on Computational and Applied Mathematics* **23** (2019), 241–251.
- [54] K.-U. Schmidt: Quaternary constant-amplitude codes for multicode CDMA. *IEEE Trans. Inform. Theory* **55** (2009), 1824–1832.
- [55] J. J. Sylvester: Thoughts on inverse orthogonal matrices, simultaneous sign-successions, and tessellated pavements in two or more colours, with applications to Newton’s rule, ornamental tile-work, and the theory of numbers. *Phil. Mag.* **34** (1867) 461–475
- [56] F. Szöllősi: *Construction, classification and parametrization of complex Hadamard matrices*. Ph.D. Thesis. arXiv:1110.5590.
- [57] S. Topalova: Classification of Hadamard matrices of order 44 with automorphisms of order 7. *Discrete Math.* **260** (2003), 275–283.

- [58] R. J. Turyn: Character sums and difference sets. *Pacific J. Math.* **15** (1965), 319–346.
- [59] A. Winterhof: On the non-existence of generalized Hadamard matrices. *J. Statist. Plann. Inference* **84** (2000), 337–342.