Applications of algebra and algebraic number theory in combinatorics

Do Duc, Tai

2019

Do Duc, T. (2019). Applications of algebra and algebraic number theory in combinatorics. Doctoral thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/136727>

<https://doi.org/10.32657/10356/136727>

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

Downloaded on 26 Apr 2023 22:53:50 SGT

**NANYANG
TECHNOLOGICAL
UNIVERSITY**

SINGAPORE

**Applications of Algebra and Algebraic Number
Theory in Combinatorics**

Do Duc Tai

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES

2019

Applications of Algebra and Algebraic Number Theory in Combinatorics

Do Duc Tai

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES

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

2019

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.

21/11/2019

.....
Date

.....
Do Duc Tai

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.

21/11/2019

.....
Date

Schmidt

.....
Bernhard Schmidt

Authorship Attribution Statement

This thesis contains material from five papers. Two papers were published and two papers were accepted in peer-reviewed journals in which I am listed as an author. The remaining paper is a preprint.

1. T. D. Duc, B. Schmidt: Bilinear Forms on Finite Abelian Groups and Group-Invariant Butson Hadamard Matrices. *J. Comb. Theory Ser. A.* **166** (2019), 337–351.

The contributions of the co-authors are as follows.

- (a) I figured out the preliminary construction for circulant Butson Hadamard matrices and obtained the necessary and sufficient conditions for the existence of those matrices with prime-power orders. The necessary and sufficient result later becomes one of the two main results of the paper, Theorem 3.6.
 - (b) Prof. Schmidt proposed the initial project direction. Moreover, using bilinear forms over finite abelian groups, he obtained a much more general construction which works for group-invariant Butson Hadamard matrices. This construction is one of the two main results of the paper, Theorem 2.1.
2. T. D. Duc, B. Schmidt: Unique Differences in Symmetric Subsets of $\mathbb{F}_p$. *Combinatorica* **37** (2017), 167–182.

The contributions of the co-authors are as follows.

- (a) I obtained the main result of the paper, Theorem 1.2, which is the asymptotically best lower bound on the size of a symmetric subset of the finite field $\mathbb{F}_p$ which contains no unique difference.
 - (b) Prof. Schmidt proposed the initial project direction. Moreover, he gave a simpler proof for the main result and applied this result to make improvement over a known result on Weil numbers, Theorem 7.2.
3. T. D. Duc, K. H. Leung, B. Schmidt: Upper Bounds for Cyclotomic Numbers. *Algebr. Comb.* Accepted. arXiv:1903.07314.

The contributions of the co-authors are as follows.

- (a) Prof. Leung and Prof. Schmidt provided the initial project direction.

- (b) Prof. Leung discovered a connection between cyclotomic numbers and systems of equations over finite fields, which yields various new bounds on cyclotomic numbers. Prof. Schmidt refined this approach and proved an equivalence between certain equations over finite fields and equations over the field of complex numbers. Moreover, he obtained a new bound on the norm of cyclotomic integers which serves as one of the main components in the main result of the paper.
 - (c) I proved the main result and gave a simpler proof for the result on the norm of cyclotomic integers. Moreover, I proposed an improvement over the main result in a special case, Theorem 1.3.
4. T. D. Duc: Necessary Conditions for the Existence of Group-Invariant Butson Hadamard Matrices and a New Family of Perfect Arrays. *Des. Codes Cryptogr.* Accepted. arXiv:1903.07334.
 5. T. D. Duc: New Constructions of Group-Invariant Butson Hadamard Matrices. Preprint. arXiv:1903.09824.

21/11/2019

.....
Date

.....
Do Duc Tai

Abstract

The aim of this monograph is to demonstrate the application of algebra and algebraic number theory to the study of combinatorics problems. Three problems which will be discussed in this monograph are *Group-Invariant Butson Hadamard Matrices*, *Unique Differences in Symmetric Subsets of $\mathbb{F}_p$* and *Upper Bounds for Cyclotomic Numbers*. The main contribution of this thesis is the construction of new classes of the mentioned objects and better necessary conditions (than the known ones) for their existence. In some cases, our necessary conditions are also sufficient conditions or asymptotically best conditions.

A Butson Hadamard matrix is a square matrix whose entries are complex roots of unity such that any two rows of the matrix are orthogonal. We focus on group-invariant Butson Hadamard matrices, that is, Butson Hadamard matrices whose rows and columns are indexed by elements of a group and are invariant under the action of that group. It turns out that the properties of these matrices can be wrapped in a single group-ring equation. By applying appropriate characters to this equation, we can unveil the original object. Using bilinear forms on finite abelian groups and ideas from the theory of relative difference sets, we constructed three new classes of group-invariant Butson Hadamard matrices in this thesis. Furthermore, the tools from algebraic number theory were employed to study necessary conditions for the existence of these matrices.

The second problem is unique differences in symmetric subsets of $\mathbb{F}_p$. We say that a subset B of the finite field $\mathbb{F}_p$, where p is a prime, has a unique difference if there is $x \in \mathbb{F}_p$ such that there is exactly one ordered pair (a, b) , $a, b \in B$, with $x = a - b$. Otherwise, the set B is said to have no unique difference. Moreover, the subset B is called symmetric if $B = -B$. Given a prime p , we aim to determine the minimum cardinality $g(p)$ of a symmetric subset of $\mathbb{F}_p$ which has no unique difference. Suppose that A is a symmetric subset of $\mathbb{F}_p$ which does not contain a unique difference. By studying the Smith Normal Form of the coefficient matrix M which corresponds to a linear system that represents the property A containing no unique difference, we find a lower bound for $|A|$. This is also a lower bound for $g(p)$. Moreover, a known construction by Straus [53] for a symmetric subset of $\mathbb{F}_p$ having no unique difference gives us an upper bound for $g(p)$. As these two bounds are asymptotically the same, our lower bound for $g(p)$ is asymptotically best possible. Furthermore, we use our lower bound on $g(p)$ to obtain an improvement over a known result on Weil numbers.

The last problem treated in this monograph is upper bounds for cyclotomic numbers. Let q be a power of a prime p , let k be a nontrivial divisor of $q - 1$ and put $e = (q - 1)/k$.

We study upper bounds for all cyclotomic numbers (a, b) of order e . The main idea we use is to transform equations over $\mathbb{F}_q$ into equations over the field of complex numbers on which we have more information. This can be done if the characteristic p is sufficiently large compared to k . A major tool for the improvements we obtain over known results is new upper bounds on the norm of cyclotomic integers.

Acknowledgments

First and foremost, I would like to express my deepest gratitude to my supervisor Prof. Bernhard Schmidt for his continuous support and encouragement throughout my four years of graduate studies. His immense knowledge, patience and motivation have urged me to become a better researcher. His originality and work ethic has been a guidance for me, both in life and in research.

Furthermore, I am grateful to Nanyang Technological University for generously sponsoring me many overseas conferences from those I gained a lot of knowledge and bettered myself as a researcher.

Contents

Abstract	i
Acknowledgments	iii
1 Introduction	1
1.1 Standard Notations Used in this Thesis	1
1.2 The Combinatorial Problems	3
1.2.1 Group-Invariant Butson Hadamard Matrices	3
1.2.2 Unique Differences in Symmetric Subsets of $\mathbb{F}_p$	5
1.2.3 Upper Bounds for Cyclotomic Numbers	8
1.3 Smith Normal Forms, Group Rings and Characters	9
1.3.1 Smith Normal Forms and Determinant Inequalities	9
1.3.2 Group Rings and Characters	11
1.4 Number Theoretic Tools	14
2 Group-Invariant Butson Hadamard Matrices	18
2.1 Notations, Bilinear Forms and Group-Ring Equations	18
2.2 Constructions	20
2.2.1 Construction from Bilinear Forms	20
2.2.2 Construction from Finite Local Rings	29
2.2.3 $\text{BH}(G, h)$ Matrices with G non-abelian	31
2.3 Necessary Conditions	36
2.3.1 Summary of Known Results	36
2.3.2 Bounds on Norms of Cyclotomic Integers	37
2.3.3 $\text{BH}(\mathbb{Z}_n, h)$ Matrices	41
2.3.4 $\text{BH}(G, 2p^b)$ Matrices	50
2.4 Application to Perfect Multiphase Arrays	52
2.5 Concluding Remarks	55

3	Unique Differences in Symmetric Subsets of $\mathbb{F}_p$	57
3.1	Symmetric Subsets of $\mathbb{F}_p$ with no Unique Difference	57
3.2	Set-up	60
3.3	Smith Normal Form of the Coefficient Matrix	62
3.4	Equations of Type 1	65
3.5	Proof of Theorem 1.2.6	68
3.6	Application to Weil Numbers	70
3.7	Concluding Remarks	73
4	Upper Bounds for Cyclotomic Numbers	75
4.1	Introduction and Definitions	75
4.2	Vanishing Sums of Roots of Unity	77
4.3	Bounds on Norms of Cyclotomic Integers	78
4.4	Equations over $\mathbb{F}_q$ and $\mathbb{C}$	82
4.5	Upper Bounds for Cyclotomic Numbers	84
4.6	The Case where k is Prime	92
4.7	Concluding Remarks	95
	Bibliography	96

Chapter 1

Introduction

As mentioned in the abstract, the three combinatorial problems which will be discussed in this monograph are *Group-Invariant Butson Hadamard Matrices*, *Unique Differences in Symmetric Subsets of $\mathbb{F}_p$* and *Upper Bounds for Cyclotomic Numbers*. We focus on studying necessary conditions for their existence and constructing new classes of these objects. In some cases, our constructions imply that our necessary conditions are actually sufficient, or are asymptotically best conditions. The structure of the monograph is as follows.

In the first chapter, we introduce the problems and provide basic algebraic and number theoretic tools which will be used later. Each problem will be discussed more in depth in a separate chapter. In this thesis, the results which are stated as **Lemma**, **Proposition**, **Corollary** and **Theorem**, are new. Previously known works are often mentioned explicitly or stated as **Result**. Almost all results presented in this thesis are based on published works [18, 20, 21] and preprints [19, 22].

1.1 Standard Notations Used in this Thesis

In this section, we fix notations which will be used throughout the thesis.

By $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ we denote the standard sets of integers, rational numbers, real numbers and complex numbers, respectively. By $\mathbb{F}_q$ we denote the finite field of q elements, where q is a prime power.

Let G be a finite group with identity 1. By $\exp(G)$ we denote the smallest positive integer e such that $g^e = 1$ for all $g \in G$.

Furthermore, we use the following number theoretic notations.

- For a positive integer h , the notation ζ_h denotes a primitive h th root of unity.
- For a positive integer m , Euler's phi function $\varphi(m)$ denotes the number of integers k in the range $[1, m]$ for which $\gcd(k, m) = 1$.
- For any two numbers (real or complex) t and s , the delta function δ_{ts} is defined by

$$\delta_{ts} = \begin{cases} 0 & \text{if } t \neq s, \\ 1 & \text{if } t = s. \end{cases}$$

- For an integer a and an odd prime p , the Legendre symbol $\left(\frac{a}{p}\right)$ is a function between a and p defined as follows.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p}, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

- For a prime p and an integer n , the function $\nu_p(n)$ denote the p -adic valuation of n , that is, $p^{\nu_p(n)}$ is the largest power of p dividing n .
- We call a positive integer **square-free** if it is not divisible by any square of a prime. We call an integer l the square-free part of n if l is the product of all prime divisors p of n in which $\nu_p(n)$ is odd.
- For coprime integers m and n , we denote the smallest positive integer j such that $m^j \equiv 1 \pmod{n}$ by $\text{ord}_n(m)$.
- We call a complex number X a **cyclotomic integer** if it is a sum of complex roots of unity. In other words, there exists a positive integer h such that

$$X = \sum_{i=0}^{h-1} a_i \zeta_h^i,$$

where a_i are integers.

1.2 The Combinatorial Problems

1.2.1 Group-Invariant Butson Hadamard Matrices

Butson Hadamard matrices were first studied by Butson [11] in 1962 under the name generalized Hadamard matrices. These are $n \times n$ matrices H whose entries are complex h th roots of unity such that $HH^* = nI_n$, where n and h are positive integers, H^* is the complex conjugate transpose of H and I_n is the identity matrix of order n . The set of Butson Hadamard matrices with parameters n and h is denoted by $\mathbf{BH}(n, h)$. We also call any matrix H in the set $\mathbf{BH}(n, h)$ a **$\mathbf{BH}(n, h)$ matrix**. The Ph.D. thesis [54] of Szöllősi provides a good overview of most of the known results on Butson Hadamard matrices; [28, 32] contain more recent work and survey open problems in this area.

In this thesis, we focus on Butson Hadamard matrices which are invariant under the action of a group. Let $(G, \cdot)$ be a group of order n . An $n \times n$ matrix $A = (a_{g,k})_{g,k \in G}$ is **G -invariant** if $a_{gl,kl} = a_{g,k}$ for all $g, k, l \in G$. Obviously, the entries of A are all determined by the entries in its first row, as $a_{g,k} = a_{1,kg^{-1}}$ for all $g, k \in G$. We call a G -invariant $\mathbf{BH}(n, h)$ matrix a **$\mathbf{BH}(G, h)$ matrix**. By $\mathbb{Z}_n$ we denote the cyclic group of order n . Note that in the case $G = \mathbb{Z}_n$, a $\mathbf{BH}(\mathbb{Z}_n, h)$ matrix is **circulant**, that is, a square matrix each of whose rows (except the first) is obtained from the previous row by shifting the entries one position to the right and moving the last entry to the front.

We remark that group-invariant Butson Hadamard matrices encompasses many other combinatorial structures like generalized Hadamard matrices, relative difference sets, generalized Bent functions, cyclic n -roots, perfect sequences and perfect arrays, see [51, 19] for more details.

For any multiple h' of h , a $\mathbf{BH}(G, h)$ matrix is also a $\mathbf{BH}(G, h')$ matrix, as an h th root of unity is a power of an h' th root of unity. Thus, it is important to find those positive integers h such that a $\mathbf{BH}(G, h)$ matrix exists, but $\mathbf{BH}(G, k)$ matrices do not exist for any divisor k of h . Most existing work on group-invariant Butson Hadamard matrices concerns (circulant) $\mathbf{BH}(\mathbb{Z}_n, h)$ matrices. Backelin [2] came up with the following result.

Result 1.2.1. *Let p be a prime and let n be a positive integer such that $n \equiv 0 \pmod{p^2}$ and $n \not\equiv 2 \pmod{4}$. Then there is a $\mathbf{BH}(\mathbb{Z}_n, n/p)$ matrix.*

We remark that Backelin actually formulated his result in terms of so called cyclic n -roots; Result 1.2.1 translates his theorem into the language of group-invariant Butson Hadamard matrices. We further remark that the condition $n \not\equiv 2 \pmod{4}$ is missing in the statement of the theorem in Backelin's paper, but is necessary for his construction

to work. In fact, for instance, it can be shown [35] that $\text{BH}(\mathbb{Z}_{2p^2}, 2p)$ matrices do not exist for any odd prime p . The special case $n = p^2$ of Result 1.2.1 was rediscovered in [16].

Using bilinear forms on finite abelian groups, we obtain the following generalization of Result 1.2.1.

Theorem 1.2.2. *Let G be a finite abelian group and let h be a positive integer such that*

$$\begin{aligned} \nu_p(h) &\geq \lceil \nu_p(\exp(G))/2 \rceil \text{ for every prime divisor } p \text{ of } |G|, \\ \nu_2(h) &\geq 2 \text{ if } \nu_2(|G|) \text{ is odd and } G \text{ has a direct factor } \mathbb{Z}_2. \end{aligned}$$

Then there exists a $\text{BH}(G, h)$ matrix.

The next construction uses ideas from the theory of relative difference sets in [37].

Theorem 1.2.3. *Let a, d, r be positive integers and let b be an integer with $0 \leq b \leq r-1$. Put $R = \mathbb{Z}_{p^{a+1}}^{db} \times \mathbb{Z}_{p^a}^{d(r-b)}$. If there exists a positive integer $t \leq d$ and complex h th roots of unity $\eta_0, \dots, \eta_{p^t-1}$ such that*

$$\sum_{i=0}^{p^t-1} \eta_i = 0,$$

then there exists a $\text{BH}(R \times R, h)$ matrix.

Our last construction is the only known class of $\text{BH}(G, h)$ matrices in which the group G does not need to be abelian. This construction utilizes the idea of *building sets* introduced in [14].

Theorem 1.2.4. *Let n be a positive integer and let h be the smallest positive integer such that*

$$h^2 \equiv 0 \pmod{n} \text{ and } (\nu_2(n), \nu_2(h)) \neq (1, 1). \quad (\star)$$

Define the divisor k of n as follows.

$$k = \begin{cases} n/h & \text{if } \nu_2(n) \neq 1, \\ 2n/h & \text{otherwise.} \end{cases} \quad (1.1)$$

Suppose that G is a group of order n which contains a normal subgroup isomorphic to $\mathbb{Z}_{n/k}$. Then there exists a $\text{BH}(G, h)$ matrix.

Lastly, we study necessary conditions for the existence of $\text{BH}(G, h)$ matrices. Prior to this thesis, there are 5071 open cases for the existence of $\text{BH}(\mathbb{Z}_n, h)$ matrices in which

$1 \leq n, h \leq 100$. Our results confirm the existence/nonexistence of 2384 matrices in these 5071 cases. There are 2687 open cases left and this full list of open cases is provided in [23].

We remark that the existence problem for $\text{BH}(\mathbb{Z}_n, h)$ matrices is in general a difficult problem. For example, the existence of $\text{BH}(\mathbb{Z}_n, 2)$ matrices is equivalent to the existence of circulant Hadamard matrices. Ryser [47, p. 134] conjectured in 1963 that circulant Hadamard matrices exist only for orders $n = 1$ or $n = 4$. This conjecture remains open till today. Though our necessary conditions do not rule out any open case of $\text{BH}(\mathbb{Z}_n, 2)$ matrices, we hope that the study of group-invariant Butson Hadamard matrices could suggest a more general point of view on the study of circulant Hadamard matrices.

1.2.2 Unique Differences in Symmetric Subsets of $\mathbb{F}_p$

Let p be a prime and let $\mathbb{F}_p$ denote the finite field with p elements. Let A be a nonempty subset of $\mathbb{F}_p$. We say that an element $x \in \mathbb{F}_p$ is a **difference** in A if there exist $a, b \in A$ such that $x = a - b$. The set A is said to have a **unique difference** if there is $x \in \mathbb{F}_p$ such that there is exactly one ordered pair (a, b) , $a, b \in A$, with $x = a - b$. Otherwise, we say that A has no unique difference. Unique sums are defined similarly. A subset B of $\mathbb{F}_p$ is called **symmetric** if $B = -B$.

Let A be a subset of $\mathbb{F}_p$. We observe that the smaller the size of A is, the more likely A has a unique difference. If $|A| = 0$, that is $A = \emptyset$, then A contains no difference at all. However, by abuse of language, we assume that A has a unique difference in this case. If $|A| = 1$, say $A = \{a\}$, then $0 = a - a$ is the only difference in A ; thus A contains a unique difference. If $|A| = 2$, say $A = \{a, b\}$, and $p \geq 3$, then it is clear that $a - b$ is a unique difference in A . On the other hand, if the size of A is large, then it is more likely that A does not have a unique difference. For example, if $A = \mathbb{F}_p$, then any difference $a - b$, $a, b \in A$, is not unique, as $a - b = (a + 1) - (b + 1)$.

According to Straus [53], the following problem was first proposed by W. Feit.

Problem 1.2.5. *Given a prime p , what is the largest number $f(p)$ such that every subset of $\mathbb{F}_p$ with at most $f(p)$ elements has a unique difference?*

Note that if we construct a subset A of $\mathbb{F}_p$ which contains no unique difference, then we obtain an upper bound for $f(p)$, that is, $f(p) < |A|$. For example, the subset $\{0, 1, 2, 4\} \in \mathbb{F}_7$ contains no unique difference, as $0 - 1 = 1 - 2$, $0 - 2 = 2 - 4$ and $0 - 4 = 4 - 1$. We obtain $f(7) < 4$. The following table gives examples of smallest

subsets of $\mathbb{F}_p$, up to $p = 59$, which have no unique difference. I would like to thank Bernhard Schmidt and Ong Wee Hern for providing these nice examples.

p	Smallest subsets with no unique difference	$f(p)$
5	$\{0, 1, 2, 3\}$	3
7	$\{0, 1, 2, 4\}$	3
11	$\{0, 1, 2, 4, 7\}$	4
13	$\{0, 1, 2, 3, 4, 8\}$	5
17	$\{0, 1, 2, 3, 6, 13\}$	5
19	$\{0, 1, 2, 3, 4, 7, 15\}$	6
23	$\{0, 1, 2, 3, 6, 7, 13\}$	6
29	$\{0, 1, 2, 3, 4, 7, 16, 24\}$	7
31	$\{0, 1, 2, 3, 4, 8, 17, 26\}$	7
37	$\{0, 1, 2, 3, 14, 18, 21, 25\}$	7
41	$\{0, 1, 2, 3, 6, 15, 29, 38\}$	7
43	$\{0, 1, 2, 3, 4, 7, 15, 31, 39\}$	8
47	$\{0, 1, 2, 3, 4, 7, 17, 34, 44\}$	8
53	$\{0, 1, 2, 3, 4, 8, 20, 37, 49\}$	8
59	$\{0, 1, 2, 3, 4, 5, 9, 22, 42, 55\}$	9

Let $\log_n(\cdot)$ denote the logarithm with base n . Straus [53] showed that $f(p) \geq 1 + \log_4(p - 1)$. This result was later improved by Browkin, Divis, and Schinzel [10] who obtained

$$f(p) \geq \log_2(p), \quad (1.2)$$

which is the best known lower bound for $f(p)$. It is not known whether this bound is asymptotically sharp.

Let $g(p)$ denote the minimum positive integer s such that there exists a symmetric subset B of $\mathbb{F}_p$ which has size s and contains no unique difference. Similar to the case of $f(p)$, a symmetric subset of $\mathbb{F}_p$ is more likely to contain a unique difference if its size is small. The following table gives examples of smallest symmetric subsets of $\mathbb{F}_p$, up to $p = 59$, which have no unique difference. Again, I would like to thank Bernhard Schmidt and Ong Wee Hern for these examples.

p	Smallest subsets with no unique difference	$g(p)$
5	$\{1, 2, 3, 4\}$	4
7	$\{0, 1, 2, 5, 6\}$	5
11	$\{1, 2, 3, 8, 9, 10\}$	6
13	$\{0, 1, 2, 4, 9, 11, 12\}$	7
17	$\{0, 1, 2, 5, 12, 15, 16\}$	7
19	$\{0, 1, 2, 6, 13, 17, 18\}$	7
23	$\{1, 2, 3, 6, 7, 16, 20, 21, 22\}$	8
29	$\{1, 2, 3, 9, 20, 26, 27, 28\}$	8
31	$\{0, 1, 2, 4, 9, 22, 27, 29, 30\}$	9
37	$\{0, 1, 2, 4, 12, 22, 25, 33, 36\}$	9
41	$\{0, 1, 2, 5, 12, 29, 36, 39, 40\}$	9
43	$\{0, 1, 2, 5, 15, 28, 38, 41, 42\}$	9
47	$\{0, 1, 2, 5, 15, 32, 42, 45, 46\}$	9
53	$\{0, 1, 2, 6, 18, 35, 47, 51, 42\}$	9
59	$\{0, 1, 2, 3, 8, 17, 42, 51, 56, 57, 58\}$	11

In [53, Thm. 2], subsets of $\mathbb{F}_p$ were constructed which do not have unique differences and are of cardinality $(2 + o(1)) \log_3(p)$. These sets are symmetric. Thus [53, Thm. 2] implies

$$g(p) \leq (2 + o(1)) \log_3(p). \quad (1.3)$$

Moreover, the above-mentioned result of Browkin, Divis, and Schinzel (1.2) implies that any subset of $\mathbb{F}_p$ with size at most $\log_2(p)$ has a unique difference. Thus

$$g(p) > \log_2(p). \quad (1.4)$$

Our contribution to the investigation of $g(p)$ is in finding a lower bound for $g(p)$ that is asymptotically tight. The following theorem implies $g(p) > 2 \log_3(p)$, which is a substantial improvement upon (1.4).

Theorem 1.2.6. *Let $p \geq 5$ be a prime and let A be a symmetric subset of $\mathbb{F}_p$ with $|A \setminus \{0\}| \leq 2 \log_3(p)$. Then A has a unique difference. As a result, we have*

$$g(p) > 2 \log_3(p).$$

In view of Straus' result (1.3), Theorem 1.2.6 is sharp in the following sense. Given any $\varepsilon > 0$, there exists a constant $C(\varepsilon)$ such that

$$2 \log_3(p) < g(p) \leq (2 + \varepsilon) \log_3(p) \quad (1.5)$$

for every prime $p > C(\varepsilon)$.

Note that a symmetric subset of $\mathbb{F}_p$ has a unique difference if and only if it has a unique sum. Thus, in the case of symmetric subsets, we could as well formulate our results in terms of unique sums.

1.2.3 Upper Bounds for Cyclotomic Numbers

Let q be a power of a prime p and let $e, k \geq 2$ be divisors of $q - 1$ such that $q = ek + 1$. Let g be a primitive element of the finite field $\mathbb{F}_q$. For each $i \in \{0, 1, \dots, e - 1\}$, write

$$C_i = \{g^i, g^{i+e}, \dots, g^{i+(k-1)e}\}. \quad (1.6)$$

For $a, b \in \{0, 1, \dots, e - 1\}$, define (a, b) as the number of solutions to the equation

$$1 + x = y, \quad x \in C_a, \quad y \in C_b.$$

Equivalently, this is the number of pairs $(r, s), 0 \leq r, s \leq k - 1$, such that

$$1 + g^{a+re} = g^{b+se}. \quad (1.7)$$

The number (a, b) is called a **cyclotomic number** of order e .

Under asymptotic conditions, cyclotomic numbers exhibit interesting uniform behaviour. Katre [30] proved that, for fixed e and $q \rightarrow \infty$, we asymptotically have $(a, b) \approx q/e^2$ for all $a, b \in \mathbb{Z}$. On the other hand, fixing k , it was proved by Betsumiya et al. [5] that $(0, 0) \leq 2$ if p is *sufficiently large* compared to k . In [5], the condition “sufficiently large” is not explicitly specified and, in fact, the lower bound on p required for their method is difficult to write down explicitly. Our goal in this problem is to find a simple and improved lower bound on p which guarantees that all cyclotomic numbers (a, b) are small. The following theorem is the main result of our study.

Theorem 1.2.7. *Let q be a power of a prime p . Let e and k be nontrivial divisors of $q - 1$ such that $q = ek + 1$. If*

$$p > \left(\sqrt{14}\right)^{k/\text{ord}_k(p)},$$

then $(a, b) \leq 3$ for all $a, b \in \mathbb{Z}$.

If k is a prime, we obtain a better bound as follows.

Theorem 1.2.8. *Let q be a power of a prime p . Let e and k be nontrivial divisors of $q - 1$ such that k is a prime and $q = ek + 1$. If*

$$p > (3^{k-1}k)^{1/\text{ord}_k(p)},$$

then

$$(a, b) \leq 2 \text{ for all } a, b \in \mathbb{Z}.$$

1.3 Smith Normal Forms, Group Rings and Characters

1.3.1 Smith Normal Forms and Determinant Inequalities

In this section, we review known results regarding the Smith Normal Form of a matrix and prove a generalization of Hadamard's inequality for determinant of a matrix.

For a ring R , let $M_{m,n}(R)$ denote the set of $m \times n$ matrices with entries from R . The Euclidean norm of a vector $x \in \mathbb{R}^n$ is denoted by $\|x\|$. The following well known result [43, p.41] describes the Smith Normal Form of a matrix.

Result 1.3.1. *Let $A \in M_{m,n}(R)$ with R being a principle ideal domain. Put $r = \text{rank}_R(A)$. Then there exist invertible matrices $S \in M_{m,m}(R)$ and $T \in M_{n,n}(R)$ such that SAT is a diagonal matrix with nonzero diagonal elements $d_1, \dots, d_r$ which satisfy*

$$d_i \mid d_{i+1} \text{ for } i = 1, \dots, r-1.$$

The elements d_i are determined uniquely (up to multiplication by units) by

$$d_i = \frac{\alpha_i}{\alpha_{i-1}},$$

where α_i is the greatest common divisor of all $i \times i$ minors of A and $\alpha_0 = 1$.

Result 1.3.2. *Let $m \leq n$, let $A \in M_{m,n}(\mathbb{R})$ and let $r_1, \dots, r_m$ denote the rows of A . Set $d(1) = \|r_1\|$. For $2 \leq j \leq m$, let $d(j)$ be the distance from r_j to the subspace of $\mathbb{R}^n$ spanned by $r_1, \dots, r_{j-1}$. We have*

$$\det(AA^T) = \prod_{j=1}^m d(j)^2. \tag{1.8}$$

Proof. If $\text{rank}_{\mathbb{R}}(A) < m$, then left hand and right side of (1.8) are both zero. Hence we may assume $\text{rank}_{\mathbb{R}}(A) = m$. By Gram-Schmidt orthogonalization, there is a nonsingular lower triangular matrix $L \in M_{m \times m}$ with diagonal entries $d(j)^{-1}$, $j = 1, \dots, m$, such that the rows of $Q = LA$ are an orthonormal basis of the subspace of $\mathbb{R}^n$ spanned by $r_1, \dots, r_m$. Thus $QQ^T = I_m$ where I_m denotes the $m \times m$ identity matrix. We conclude $AA^T = L^{-1}QQ^T(L^{-1})^T = L^{-1}(L^{-1})^T$. Hence

$$\det(AA^T) = (\det(L^{-1}))^2 = \prod_{j=1}^m d(j)^2.$$

□

Under the notations of Result 1.3.2, note that $d(j) \leq \|r_j\|$ for any $j = 1, \dots, m$. The next result, Hadamard's inequality, is a direct consequence of Result 1.3.2.

Result 1.3.3. (*Hadamard's inequality*) *Let A be an $m \times m$ matrix with real entries. Suppose that the row vectors of A are $r_1, \dots, r_m$. Then*

$$|\det(A)| \leq \prod_{i=1}^m \|r_i\|.$$

Result 1.3.4. *Let $A \in M_{u,n}(\mathbb{R})$, $B \in M_{w,n}(\mathbb{R})$, and $C = \begin{pmatrix} A \\ B \end{pmatrix}$. Then*

$$\det(CC^T) \leq \det(AA^T) \det(BB^T).$$

Proof. Let $r_1, \dots, r_u$ be the rows of A and let $r_{u+1}, \dots, r_{u+w}$ be the rows of B . For $1 \leq i < j \leq u+w$, let $d(i, j)$ denote the distance from r_j to the subspace of $\mathbb{R}^n$ generated by $r_i, \dots, r_{j-1}$. Furthermore, set $d(i, i) = \|r_i\|$ for all i . By Result 1.3.2, we have

$$\begin{aligned} \det(AA^T) &= \prod_{j=1}^u d(1, j)^2, \\ \det(BB^T) &= \prod_{j=u+1}^{u+w} d(u+1, j)^2, \\ \det(CC^T) &= \prod_{j=1}^{u+w} d(1, j)^2. \end{aligned}$$

Moreover, $d(1, j) \leq d(u+1, j)$ for $j \geq u+1$ by the definition of the $d(i, j)$'s. Hence

$$\begin{aligned} \det(CC^T) &= \prod_{j=1}^{u+w} d(1, j)^2 \\ &\leq \prod_{j=1}^u d(1, j)^2 \prod_{j=u+1}^{u+w} d(u+1, j)^2 \\ &= \det(AA^T) \det(BB^T). \end{aligned}$$

□

A repeated application of Result 1.3.4 gives the following.

Corollary 1.3.5. *Let $A_i \in M_{u_i, n}(\mathbb{R})$, $i = 1, \dots, k$, and*

$$C = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_k \end{pmatrix}.$$

Then

$$\det(CC^T) \leq \prod_{i=1}^k \det(A_i A_i^T). \quad (1.9)$$

Remark 1.3.6. If each matrix A_i in Corollary 1.3.5 is a row of the matrix C , then (1.9) is the Hadamard's inequality.

1.3.2 Group Rings and Characters

Let G be a finite abelian group of order n . Let R be a ring with identity 1 and let $R[G]$ denote the group ring of G over R . Any element $X \in R[G]$ is uniquely expressed as $X = \sum_{g \in G} a_g g$, $a_g \in R$. We call the set $\{g \in G : a_g \neq 0\}$ the **support** of X and denote it by $\text{supp}(X)$. Two elements $X = \sum_{g \in G} a_g g$ and $Y = \sum_{g \in G} b_g g$ are equal if and only if $a_g = b_g$ for all $g \in G$. We let 1_G denote the identity element of G . If there is no danger of confusion, for $c \in R$, we simply write c in the place of $c1_G$. A subgroup U of G is identified with $\sum_{u \in U} u$ in $R[G]$.

The group of complex characters of G is denoted by $\hat{G}$. It is well known that $\hat{G}$ is isomorphic to G . The trivial character of G , denoted by χ_0 , is defined by $\chi_0(g) = 1$ for all $g \in G$. For $D = \sum_{g \in G} a_g g \in R[G]$ and $\chi \in \hat{G}$, write $\chi(D) = \sum_{g \in G} a_g \chi(g)$. For a subgroup U of G , we write

$$U^\perp = \{\chi \in \hat{G} : \chi(g) = 1 \ \forall \ g \in U\}.$$

Note that $|U^\perp| = |G|/|U|$. The following is [26, Lem. 2.8].

Result 1.3.7. *Let G be a finite abelian group and let U be a subgroup of G . Suppose that $D = \sum_{g \in G} a_g g \in \mathbb{C}[G]$. Then for any character $\chi \in \hat{G}$, we have*

$$\sum_{\tau \in U^\perp} \chi \tau(D) = |U^\perp| \chi \left(\sum_{g \in U} a_g g \right)$$

The next result is the Fourier inversion formula for group-ring theory. A proof can be found in [6, Chapter VI, Lemma 3.5], for example.

Result 1.3.8. *Let G be a finite abelian group and let $D = \sum_{g \in G} a_g g \in \mathbb{C}[G]$. Then*

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

Consequently, if $D, E \in \mathbb{C}[G]$ and $\chi(D) = \chi(E)$ for all $\chi \in \hat{G}$, then $D = E$.

In our study, we often use group rings over $R = \mathbb{Z}[\zeta_h]$, where h is a positive integer. Let $D = \sum_{g \in G} a_g g, a_g \in \mathbb{Z}[\zeta_h]$ for all $g \in G$, be an element of $\mathbb{Z}[\zeta_h][G]$. Let t be an integer coprime to h and let $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_h)/\mathbb{Q})$ be defined by $\zeta_h^\sigma = \zeta_h^t$. We write

$$D^{(t)} = \sum_{g \in G} a_g^\sigma g^t.$$

The last result in this section is a generalization of Ma's lemma [38]. Its proof is similar to the proof of the original result. We provide it here for the convenience of the reader. We start with the following well known lemma.

Lemma 1.3.9. *Let p be a prime and let h be a positive integer with $(p, h) = 1$. Let s be a positive integer and let $S = \langle g \rangle$ be a cyclic group of order p^s . Denote the subgroup of S of order p by P . Let $\rho : \mathbb{Z}[\zeta_h][S] \rightarrow \mathbb{Z}[\zeta_{hp^s}]$ be the ring homomorphism defined by*

$$\sum_{i=0}^{p^s-1} a_i g^i \mapsto \sum_{i=0}^{p^s-1} a_i \zeta_{p^s}^i,$$

where $a_i \in \mathbb{Z}[\zeta_h]$ for all i . Then

$$\ker(\rho) = \{PY : Y \in \mathbb{Z}[\zeta_h][S]\}. \quad (1.10)$$

Proof. First note that $P = \sum_{j=0}^{p-1} g^{jp^{s-1}}$ and thus $\rho(P) = \sum_{j=0}^{p-1} \zeta_{p^s}^{jp^{s-1}} = \sum_{j=0}^{p-1} \zeta_p^j = 0$. This shows $\{PY : Y \in \mathbb{Z}[\zeta_h][S]\} \subset \ker(\rho)$. Let A be any element of $\ker(\rho)$, say $A = \sum_{i=0}^{p^s-1} a_i g^i$ with $a_i \in \mathbb{Z}[\zeta_h]$ for all i . Then $\rho(A) = \sum_{i=0}^{p^s-1} a_i \zeta_{p^s}^i = 0$. Since p does not divide h , the minimal polynomial of ζ_{p^s} over $\mathbb{Q}(\zeta_h)$ is $\phi(x) = 1 + x^{p^{s-1}} + \cdots + x^{p^{s-1}(p-1)}$. We thus have

$$\sum_{i=0}^{p^s-1} a_i x^i = \phi(x) f(x) = \sum_{j=0}^{p-1} x^{jp^{s-1}} f(x) \quad (1.11)$$

for some $f(x) \in \mathbb{Q}(\zeta_h)[x]$. Note that $\deg(f(x)) \leq p^s - 1 - \deg(\phi(x)) = p^{s-1} - 1$. Hence, comparing the coefficients of $1, x, \dots, x^{p^{s-1}-1}$ on both sides of (1.11), we conclude $f(x) = \sum_{i=0}^{p^{s-1}-1} a_i x^i$. In particular, we have $f(x) \in \mathbb{Z}[\zeta_h][x]$. Note that $A = \sum_{i=0}^{p^s-1} a_i g^i = \phi(g) f(g) = P f(g)$ and thus $A \in \{PY : Y \in \mathbb{Z}[\zeta_h][S]\}$. This completes the proof of (1.10). $\square$

The following is a variation of Ma's Lemma [38].

Result 1.3.10. *Let p be a prime and let G be a finite abelian group whose Sylow p -subgroup S is cyclic. Denote the subgroup of S of order p by P . Let t and h be positive integers with $\gcd(p, h) = 1$. If $D \in \mathbb{Z}[\zeta_h][G]$ satisfies*

$$\chi(D) \equiv 0 \pmod{p^t} \quad (1.12)$$

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

$$D = p^t X + PY. \quad (1.13)$$

Proof. Write $G = S \times H$ and note that $p \nmid |H|$. Let g be a generator of S and write $|S| = p^s$ for some $s \in \mathbb{Z}^+$.

First suppose that $D \in \mathbb{Z}[\zeta_h][S]$. Define $\rho : \mathbb{Z}[\zeta_h][S] \rightarrow \mathbb{Z}[\zeta_{hp^s}]$ as in Lemma 1.3.9. Note that the restriction of ρ to S is a character of S of order p^s . Thus we have $\rho(D) \equiv 0 \pmod{p^t}$ by assumption (1.12). As ρ is surjective, we conclude $\rho(D) = p^t \rho(X)$ for some $X \in \mathbb{Z}[\zeta_h][S]$. We obtain $D - p^t X \in \ker(\rho)$ and thus $D = p^t X + PY$ for some $Y \in \mathbb{Z}[\zeta_h][S]$ by Lemma 1.3.9. This shows that (1.13) holds for $D \in \mathbb{Z}[\zeta_h][S]$.

For the general case, assume that $D \in \mathbb{Z}[\zeta_h][G]$ satisfies (1.12). Let ψ be any character of S of order p^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 , let $\psi\gamma$ denote the character of G defined by

$$\psi\gamma(xy) = \psi(x)\gamma(y) \text{ for any } x \in S, y \in H.$$

As the order of $\psi\gamma$ is divisible by p^s for any character γ of H , we have, by assumption (1.12),

$$\psi\gamma(D) = \sum_{k \in H} \psi(D_k)\gamma(k) \equiv 0 \pmod{p^t}. \quad (1.14)$$

Let $M = (\gamma(k))_{\gamma \in \hat{H}, k \in H}$ be the character table of H . By the orthogonality relations for characters of finite abelian groups, we have $MM^* = |H|I$, where M^* is the complex conjugate transpose of M and I is an identity matrix. Let u be the column vector defined by $u = (\psi(D_k))_{k \in H}$. Note that the entry of Mu corresponding to the row of M indexed by γ is $\sum_{k \in H} \psi(D_k)\gamma(k)$. Hence, by (1.14), all entries of Mu are divisible by p^t . Since $M^{-1} = M^*/|H|$ and $\gcd(p, |H|) = 1$, all entries of $u = (1/|H|)M^*(Mu)$ are also divisible by p^t . We thus obtain

$$\psi(D_k) \equiv 0 \pmod{p^t} \quad (1.15)$$

for all characters ψ of S of order p^s . Recall that $D_k \in \mathbb{Z}[\zeta_h][S]$ and that we have shown the assertion of Result 1.3.10 for $D \in \mathbb{Z}[\zeta_h][S]$. Hence, by (1.15) and Result 1.3.10 for $D \in \mathbb{Z}[\zeta_h][S]$, we conclude that, for every $k \in H$, there are $X_k, Y_k \in \mathbb{Z}[\zeta_h][G]$ with $D_k = p^t X_k + P Y_k$. This shows that

$$D = \sum_{k \in H} D_k k = p^t \sum_{k \in H} X_k k + P \sum_{k \in H} Y_k k$$

satisfies (1.13) with $X = \sum_{k \in H} X_k k$ and $Y = \sum_{k \in H} Y_k k$. $\square$

1.4 Number Theoretic Tools

Definition 1.4.1. Let p be a prime, let n be a positive integer and write $n = p^a n'$ with $\gcd(p, n') = 1$. Then p is called **self-conjugate modulo n** if there exists an integer j such that $p^j \equiv -1 \pmod{n'}$. A composite integer m is self-conjugate modulo n if every prime divisor of m has this property.

A proof of the following result can be found in [50, Thm. 1.4.3].

Result 1.4.2. Let p be a prime and let m be a positive integer. Write $m = p^a m'$ with $(m', p) = 1$. Let $\mathcal{P}$ be a prime ideal above p in $\mathbb{Z}[\zeta_m]$. If $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ satisfies

$\zeta_{m'}^\sigma = \zeta_{m'}^{p^j}$ for some non-negative integer j , then $\mathcal{P}^\sigma = \mathcal{P}$. Consequently, if p is self-conjugate modulo m , then any prime ideal $\mathcal{P}$ above p is fixed by complex conjugation, that is $\mathcal{P} = \bar{\mathcal{P}}$.

The following result is a more general version of [36, Proposition 2.11]. We include a proof here for the convenience of the reader.

Result 1.4.3. *Suppose that $X = \sum_{i=0}^{m-1} a_i \zeta_m^i \in \mathbb{Z}[\zeta_m]$ satisfies $X\bar{X} = n$. Let u be the largest divisor of n which is self-conjugate modulo m . Write $u = w^2 k$, where $k = \prod_{i=1}^r p_i$ is the square-free part of u . Then*

$$m \equiv 0 \pmod{k}.$$

Furthermore, for $i = 1, \dots, r$, denote Θ_i as the following quadratic Gauss sum.

$$\Theta_i = \begin{cases} 1 - \zeta_4 & \text{if } p_i = 2, \\ \sum_{j=1}^{p_i-1} \left(\frac{j}{p_i}\right) \zeta_{p_i}^j & \text{otherwise,} \end{cases}$$

where $(-)$ is the Legendre symbol. Then

$$X \equiv 0 \pmod{w \prod_{i=1}^r \Theta_i}.$$

Proof. In this proof, we use basic algebraic number theory as covered in [29], for instance. For a nonzero prime ideal P of $\mathbb{Z}[\zeta_m]$, we use ν_P to denote the P -adic valuation of $\mathbb{Q}(\zeta_m)$, i.e., $\nu_P(X)$, where $X \in \mathbb{Q}(\zeta_m)$, is the exponent of P in the prime ideal factorization of $X\mathbb{Z}[\zeta_m]$.

Assume that there exists $p = p_i$, $1 \leq i \leq r$, such that $m \not\equiv 0 \pmod{p}$. The prime ideal factorization of $p\mathbb{Z}[\zeta_m]$ in $\mathbb{Z}[\zeta_m]$ is

$$p\mathbb{Z}[\zeta_m] = P_1 \dots P_s, \tag{1.16}$$

where P_i 's are distinct prime ideals above p . Consider a fixed ideal $P = P_1$. As $P = \bar{P}$ by Result 1.4.2, we have $\nu_P(X) = \nu_P(\bar{X})$, which implies that $\nu_P(n) = \nu_P(X\bar{X})$ is even. On the other hand, as p is contained in the square-free part of u and u is the largest divisor of n which is self-conjugate modulo m , the number $\nu_p(n)$ is odd. The equation (1.16) implies that $\nu_P(n) = \nu_p(n)$ is odd, a contradiction. We obtain $m \equiv 0 \pmod{p}$ for any prime divisor p of k . Thus $m \equiv 0 \pmod{k}$.

For the second claim, we first let q be any prime divisor of u which is not a divisor of k . Put $\nu_q(w) = a$, $a \in \mathbb{Z}^+$. Hence $\nu_q(n) = \nu_q(u) = 2a$. The self-conjugacy condition implies that

$$\nu_Q(X) = \nu_Q(\bar{X}) = \nu_Q(n)/2 = a$$

for any prime ideal Q of $\mathbb{Z}[\zeta_m]$ which lies above q . Hence $X \equiv 0 \pmod{Q^a}$ for any prime Q above q . Moreover, note that $\nu_Q(q) = \nu_R(q)$ for any two distinct primes Q and R lying above q . We obtain

$$X \equiv 0 \pmod{q^a}. \quad (1.17)$$

Next, let p_i be any divisor of k and put $2a + 1 = \nu_{p_i}(u) = \nu_{p_i}(n)$. Again, the self-conjugacy condition implies

$$\nu_P(X) = \nu_P(\bar{X}) = \nu_P(n)/2 = \nu_P(p_i^a) + \frac{\nu_P(p_i)}{2} \quad (1.18)$$

for any prime P of $\mathbb{Z}[\zeta_m]$ lying above p_i . Note that $\Theta_i \bar{\Theta}_i = p_i$, so $\nu_P(\Theta_i) = \nu_P(\bar{\Theta}_i) = \nu_P(p_i)/2$. We obtain, by (1.18),

$$\nu_P(X) = \nu_P(p_i^a) + \nu_P(\Theta_i) = \nu_P(p_i^a \Theta_i).$$

As this holds for any prime P of $\mathbb{Z}[\zeta_m]$ lying above p_i and $\nu_P(p) = \nu_R(p)$ for any primes $P \neq R$ both lying above p_i , we obtain

$$X \equiv 0 \pmod{p_i^a \Theta_i}. \quad (1.19)$$

The equations (1.17) and (1.19) imply $X \equiv 0 \pmod{w \prod_{i=1}^r \Theta_i}$. $\square$

Lemma 1.4.4. *Let p be a prime and let m be a positive integer not divisible by p . Write $\zeta = \zeta_p$ if p is odd and $\zeta = \zeta_4$ if $p = 2$. If $X \in \mathbb{Z}[\zeta_m]$ satisfies $X \equiv 0 \pmod{1 - \zeta}$, then $X \equiv 0 \pmod{p}$.*

Proof. Let $R = \mathbb{Z}[\zeta_{pm}]$ if p is odd and $R = \mathbb{Z}[\zeta_{4m}]$ if $p = 2$. The ideal $(1 - \zeta)R$ of R factorizes as

$$(1 - \zeta)R = \prod_{i=1}^k \mathfrak{p}_i,$$

where $k = \varphi(m)/\text{ord}_m(p)$ and the $\mathfrak{p}_i$'s are distinct prime ideals. Furthermore, $p\mathbb{Z}[\zeta_m] = \prod_{i=1}^k \mathfrak{q}_i$, where $\mathfrak{q}_i = \mathfrak{p}_i^{p-1}$ and the $\mathfrak{q}_i$'s are prime ideals of $\mathbb{Z}[\zeta_m]$. Note that $X \equiv 0 \pmod{\mathfrak{p}_i}$ for all i , as $X \equiv 0 \pmod{1 - \zeta}$ by assumption. Since $X \in \mathbb{Z}[\zeta_m]$, this implies $X \equiv 0 \pmod{\mathfrak{q}_i}$ for all i and hence $X \equiv 0 \pmod{p}$. $\square$

Result 1.4.5. *[49, Thm. 2.2.2] Let p be a prime, let a, b, h be positive integers with $(h, p) = 1$, and write $v = p^a h$. Suppose that X is an element of $\mathbb{Z}[\zeta_v]$ with $|X|^2 = p^b$. Then there exist $Y \in \mathbb{Z}[\zeta_h]$, a root of unity $\eta \in \mathbb{Z}[\zeta_h]$, $\eta \neq 1$, of order dividing $p - 1$, and an integer j such that either*

$$X = \zeta_v^j Y \text{ or } X = \zeta_v^j \Theta Y,$$

where Θ is a quadratic Gauss sum defined by

$$\Theta = \begin{cases} 1 - \zeta_4 & \text{if } p = 2, \\ \sum_{i=0}^{p-2} \eta^{-i} \zeta_p^{t^i}, & t \text{ being a primitive element modulo } p, \text{ if } p \text{ is odd.} \end{cases}$$

Chapter 2

Group-Invariant Butson Hadamard Matrices

2.1 Notations, Bilinear Forms and Group-Ring Equations

In this section, we adopt the following convention regarding the operation on a finite group G .

- (a) If G is abelian, we use addition “+” to denote the operation between elements of G and denote the identity element of G by 0.
- (b) If G is non-abelian (or not stated as abelian from the context), we use multiplication “ $\cdot$ ” to denote the operation between elements of G and denote the identity element of G by 1. In most cases where there is no danger of confusion, we simply write ab in place of $a \cdot b$.

Nondegenerate symmetric bilinear forms on finite abelian groups is one of the main components in our first construction of group-invariant Butson Hadamard matrices. Within our construction, given an abelian group G , there is ample freedom to choose “ingredients” (the bilinear form, a suitable subgroup of G , and a system of coset representatives).

There is a well developed theory of bilinear forms on finite abelian groups, see [40, 59, 60]. It is shown in these papers that, contrary to the case of bilinear forms over finite fields, in general there is quite a number of inequivalent nondegenerate symmetric bilinear forms on a finite abelian group. As *any* of these bilinear forms can be used in our construction, this theory turns out to be relevant for the existence of Butson Hadamard matrices and sheds light on the above mentioned flexibility of ingredients. We will not

discuss the theory of bilinear forms on finite abelian groups in this thesis though, and just focus on proving the correctness of our construction.

Definition 2.1.1. Let G be a finite abelian group and let e be a positive integer. We say that a map $f : G \times G \rightarrow \mathbb{Z}_e$ is a **bilinear form** over G if

$$\begin{aligned} f(g+h, k) &= f(g, k) + f(h, k) \text{ and} \\ f(g, h+k) &= f(g, h) + f(g, k) \end{aligned} \quad (2.1)$$

for all $g, h, k \in G$. If $f(g, h) = f(h, g)$ for all $g, h \in G$, then f is **symmetric**. If $f(g, h) = 0$, then g and h are said to be **orthogonal**. We say that f is **nondegenerate** if there is no $g \in G \setminus \{0\}$ such that $f(g, h) = 0$ for all $h \in G$.

It turns out that the properties of a group-invariant Butson Hadamard matrix can be wrapped in a single group-ring equation. The following lemma shows that the existence of a $\text{BH}(G, h)$ matrix is equivalent to the existence of a group-ring element in $\mathbb{Z}[\zeta_h][G]$ which has coefficients as complex h th roots of unity and satisfies a certain equation. Recall that $H = (H_{g,k})_{g,k \in G}$ is a $\text{BH}(G, h)$ matrix if all entries $H_{g,k}$ are complex h th roots of unity, $H_{gl,kl} = H_{g,k}$ for any $g, k, l \in G$, and any two rows of H are orthogonal.

Lemma 2.1.2. Let G be a finite group, let h be a positive integer, and let $a_g, g \in G$, be complex h th roots of unity. Consider the element $D = \sum_{g \in G} a_g g$ of $\mathbb{Z}[\zeta_h][G]$ and the 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

$$DD^{(-1)} = |G|. \quad (2.2)$$

Moreover if G is abelian, then the equation (2.2) holds if and only if

$$|\chi(D)|^2 = |G| \text{ for all } \chi \in \hat{G}. \quad (2.3)$$

Proof. First, it is clear that H is G -invariant, as

$$H_{gl,kl} = a_{gl(kl)^{-1}} = a_{gk^{-1}} = H_{g,k} \text{ for all } g, k, l \in G.$$

Let $g \in G$ be arbitrary. The coefficient of g in $DD^{(-1)}$ is

$$\sum_{\substack{k, l \in G \\ kl^{-1} = g}} a_k \bar{a}_l = \sum_{l \in G} a_{gl} \bar{a}_l.$$

On the other hand, let x and y be any two elements of G . Write $y = gx$ for some $g \in G$. The inner product between the row y and the row x of H is

$$\sum_{k \in G} H_{gx,k} \overline{H_{x,k}} = \sum_{k \in G} a_{g x k^{-1}} \overline{a_{x k^{-1}}} = \sum_{l \in G} a_{gl} \bar{a}_l.$$

Therefore, the equation (2.2) holds if and only if any two distinct rows of H have inner product 0, that is, if and only if H is a $\text{BH}(G, h)$ matrix. Finally, the equivalence of (2.2) and (2.3) follows from Result 1.3.8. $\square$

2.2 Constructions

2.2.1 Construction from Bilinear Forms

We will use the following conventions. For an abelian group G and $g \in G$, we say that $h \in G$ is a **square root** of g if $g = 2h$. Note that square roots are not unique in general. In fact, the construction in Theorem 2.2.2 works no matter which square roots are chosen.

Let L be an elementary abelian group of order 2^{2a+b} where $b \in \{0, 1\}$ and write $c = 2a + b$. We identify L with $\{(g_1, \dots, g_c) : g_1, \dots, g_c \in \{0, 1\}\}$, the group operation being componentwise addition modulo 2. For $g = (g_1, \dots, g_c) \in L$, set $G_1 = (g_1, \dots, g_a)$ and $G_2 = (g_{a+1}, \dots, g_{2a})$. Similarly, define X_1 and X_2 for $x = (x_1, \dots, x_c) \in L$. For $x, y \in \{0, 1\}^a$, write $xy^T = \sum_{i=1}^a x_i y_i$. Note that in this sum we use the addition of integers, not addition modulo 2. For instance, if $x = y = (1, 1)$, then xy^T is the integer 2. Define a function $s_L : L \rightarrow \mathbb{Z}$ by

$$s_L(g) = \begin{cases} 2G_1G_2^T & \text{if } b = 0, \\ 2G_1G_2^T + g_c & \text{if } b = 1. \end{cases}$$

For $u, w \in \mathbb{Z}$, set $u \oplus w = 0$ if $u + w$ is even and $u \oplus w = 1$ if $u + w$ is odd. For $x, y \in L$, define $x \oplus y$ by $(x \oplus y)_i = x_i \oplus y_i$ for all i .

Lemma 2.2.1. *Under the above notations, we have*

$$\sum_{x \in L} \zeta_4^{s_L(x) - s_L(x \oplus g)} = 0 \quad (2.4)$$

whenever $g \in L \setminus \{0\}$.

Proof. First assume $b = 1$. Let $g \neq 0$ be an element of L . We have

$$\begin{aligned} \sum_{x \in L} \zeta_4^{s_L(x) - s_L(x \oplus g)} &= \sum_{x \in L} \zeta_4^{2X_1X_2^T + x_c - 2(X_1X_2^T + X_1G_2^T + G_1X_2^T + G_1G_2^T) - (x \oplus g)_c} \\ &= (-1)^{G_1G_2^T} \sum_{x_c=0}^1 \zeta_4^{x_c - (x_c \oplus g_c)} \sum_{X_1 \in \{0,1\}^a} (-1)^{X_1G_2^T} \\ &\quad \sum_{X_2 \in \{0,1\}^a} (-1)^{G_1X_2^T} \end{aligned} \quad (2.5)$$

If $G_1 \neq (0, \dots, 0)$, then the last sum in (2.5) vanishes. Indeed, as $G_1 \neq (0, \dots, 0)$, there exists $Y_2 \in \{0, 1\}^a$ such that $(-1)^{G_1 Y_2^T} = -1$. We have

$$(-1) \left(\sum_{X_2 \in \{0, 1\}^a} (-1)^{G_1 X_2^T} \right) = \sum_{X_2 \in \{0, 1\}^a} (-1)^{G_1 (X_2 + Y_2)^T} = \sum_{X_2 \in \{0, 1\}^a} (-1)^{G_1 X_2^T},$$

so $\sum_{X_2 \in \{0, 1\}^a} (-1)^{G_1 X_2^T} = 0$. Similarly if $G_2 \neq (0, \dots, 0)$, then the second last sum in (2.5) vanishes. If $g_c \neq 0$, then $g_c = 1$ and

$$\sum_{x_c=0}^1 \zeta_4^{x_c - (x_c \oplus g_c)} = \zeta_4^{-1} + \zeta_4^1 = 0.$$

In summary, we obtain

$$\sum_{x \in L} \zeta_4^{s_L(x) - s_L(x \oplus g)} = 0$$

whenever $g \neq 0$, proving (2.4).

Lastly, if $b = 0$ and $g \in L \setminus \{0\}$, then

$$\begin{aligned} \sum_{x \in L} \zeta_4^{s_L(x) - s_L(x \oplus g)} &= \sum_{x \in L} \zeta_4^{2X_1 X_2^T - 2(X_1 X_2^T + X_1 G_2^T + G_1 X_2^T + G_1 G_2^T)} \\ &= (-1)^{G_1 G_2^T} \sum_{X_1 \in \{0, 1\}^a} (-1)^{X_1 G_2^T} \sum_{X_2 \in \{0, 1\}^a} (-1)^{G_1 X_2^T} \\ &= 0 \end{aligned}$$

by the same reasoning as before. $\square$

Theorem 2.2.2. *Let $K = G \times L$ be a finite abelian group, where either $L = \{0\}$ or L is an elementary abelian 2-group. Write $e = \exp(G)$. Let U be a subgroup of G such that every element of U has a square root in G . For each $u \in U$, fix a choice of square root of u and denote it by $u/2$. Suppose that $f : G \times G \rightarrow \mathbb{Z}_e$ is bilinear, symmetric, and nondegenerate, and that no element of $G \setminus U$ is orthogonal to all elements of U . Let $R \subset G$ be a complete system of coset representatives of U in G with $0 \in R$. For every $x \in K$, there are unique $x_1 \in U$, $x_2 \in R$, and $x_3 \in L$ with $x = x_1 + x_2 + x_3$. Let β be any integer coprime to $|G|$. Define a matrix $H = (H_{y,x})_{y,x \in K}$ by*

$$H_{y,x} = \zeta_e^{f((x-y)_1/2, (x-y)_1) + \beta f((x-y)_1, (x-y)_2)} \zeta_4^{s_L(x_3 \oplus y_3)}. \quad (2.6)$$

Then H is a $\text{BH}(K, e_1)$ matrix, where

$$e_1 = \begin{cases} \exp(U) & \text{if } L = \{0\}, \\ \text{lcm}(2, \exp(U)) & \text{if } L \text{ is of square order,} \\ \text{lcm}(4, \exp(U)) & \text{otherwise.} \end{cases} \quad (2.7)$$

Proof. We first remark that the assumption on every element of U having a square root in G is necessary for the right-hand side of (2.6) to be properly defined, as $(x - y)_1/2$ exists for all $x, y \in K$. The proof is divided into following claims.

Claim 1. *The matrix H is K -invariant.*

Note that the value of $H_{y,x}$ depends on $x - y$ and $x_3 \oplus y_3$. For any $k = k_1 + k_2 + k_3 \in K$, we have

$$(x + k)_3 \oplus (y + k)_3 = (x_3 + k_3) \oplus (y_3 + k_3) = x_3 \oplus y_3.$$

Thus

$$H_{y,x} = H_{y+k,x+k} \text{ for any } x, y, k \in K,$$

proving the claim.

From now on, we fix $y \in K$ and focus on the $(0, y)$ th entry of HH^* . We first look at the entry $H_{y,x}$ of H .

Claim 2. *For any $x \in K$, there exists $u(x_2) \in U$ such that*

$$H_{y,x} = \zeta_e^{f((x_1 - y_1 - u(x_2))/2, x_1 - y_1 - u(x_2)) + \beta f(x_1 - y_1 - u(x_2), x_2 - y_2 + u(x_2))} \zeta_4^{sL(x_3 \oplus y_3)} \quad (2.8)$$

Moreover

$$u(x_2) = 0 \text{ whenever } y_2 = 0. \quad (2.9)$$

Let $u(x_2)$ be the unique element in U with

$$(x - y)_2 = x_2 - y_2 + u(x_2). \quad (2.10)$$

Note that $u(x_2)$ depends on y , but we do not indicate this dependence, as we consider y as fixed. We have

$$(x - y)_1 = x_1 - y_1 - u(x_2) \quad (2.11)$$

by (2.10), as $x_1 + x_2 - y_1 - y_2 = (x - y)_1 + (x - y)_2$. Note that $u(x_2)$ only depends on x_2 (not on x_1), as $(x - y)_2 = (x' - y)_2$ whenever $x_2 = x'_2$. The equation (2.8) follows from (2.6), (2.10) and (2.11).

If $y_2 = 0$, then $u(x_2) = (x - y)_2 - x_2 = (x_1 + x_2 + x_3 - y_1 - y_3)_2 - x_2 = x_2 - x_2 = 0$, proving (2.9).

Claim 3. *Denote $\eta = \zeta_e^{-f(y_1/2, y_1) - \beta f(y_1, y_2)}$. Let $A(y)$ denote the $(0, y)$ th entry of HH^* and assume that $A(y) \neq 0$. Then $y_2 = y_3 = 0$ and*

$$A(y) = \eta |L| |U| \sum_{x_2 \in R} \zeta_e^{\beta f(y_1, x_2)}. \quad (2.12)$$

Using (2.8) and the bilinearity of f , we see that the $(0, y)$ th entry of HH^* is

$$\begin{aligned} A(y) &:= \sum_{x \in K} H_{0,x} \overline{H_{y,x}} \\ &= \sum_{x_3 \in L} \sum_{x_2 \in R} \sum_{x_1 \in U} H_{0,x_1+x_2+x_3} \overline{H_{y,x_1+x_2+x_3}} \\ &= \eta \sum_{x_3 \in L} \zeta_4^{s_L(x_3) - s_L(x_3 \oplus y_3)} \sum_{x_2 \in R} \zeta_e^{T(x_2)} \sum_{x_1 \in U} \zeta_e^{S(x_1, x_2)}, \end{aligned}$$

where

$$\begin{aligned} \eta &= \zeta_e^{-f(y_1/2, y_1) - \beta f(y_1, y_2)}, \\ T(x_2) &= \beta f(x_2, y_1 + u(x_2)) \\ &\quad + f(u(x_2), -u(x_2)/2 - y_1 + \beta(u(x_2) + y_1 - y_2)), \\ S(x_1, x_2) &= f(x_1, y_1 + \beta y_2 + (1 - \beta)u(x_2)). \end{aligned}$$

As $A(y) \neq 0$, we have $\sum_{x_3 \in L} \zeta_4^{s_L(x_3) - s_L(x_3 \oplus y_3)} \neq 0$ and thus $y_3 = 0$ by (2.4). Hence the first sum in the expression for $A(y)$ is equal to $|L|$ and

$$A(y) = \eta |L| \sum_{x_2 \in R} \zeta_e^{T(x_2)} \sum_{x_1 \in U} \zeta_e^{S(x_1, x_2)}. \quad (2.13)$$

Write $V(x_2) = \sum_{x_1 \in U} \zeta_e^{S(x_1, x_2)}$. Note that $S(x_1 + z_1, x_2) = S(x_1, x_2) + S(z_1, x_2)$ for all $x_1, z_1 \in U$, since f is bilinear. Suppose that there is $z_1 \in U$ such that $S(z_1, x_2) \neq 0$. Then

$$\zeta_e^{S(z_1, x_2)} V(x_2) = \sum_{x_1 \in U} \zeta_e^{S(x_1 + z_1, x_2)} = \sum_{x_1 \in U} \zeta_e^{S(x_1, x_2)} = V(x_2).$$

This implies $V(x_2) = 0$, as $\zeta_e^{S(z_1, x_2)} \neq 1$. So we see that $V(x_2)$ is only nonzero if

$$S(x_1, x_2) = f(x_1, y_1 + \beta y_2 + (1 - \beta)u(x_2)) = 0 \quad (2.14)$$

for all $x_1 \in U$. As no element of $G \setminus U$ is orthogonal to all elements of U by assumption, this implies $y_1 + \beta y_2 + (1 - \beta)u(x_2) \in U$ and thus $y_2 \in U$, as $y_1, u(x_2) \in U$ and β is coprime to $|G|$. This implies $y_2 = 0$, as $y_2 \in R \cap U$ and $R \cap U = \{0\}$. Hence we have $y_2 = 0$ whenever $V(x_2) \neq 0$. As $A(y) \neq 0$ by assumption, we have $V(x_2) \neq 0$ for at least one x_2 and thus

$$y_2 = 0. \quad (2.15)$$

Hence

$$u(x_2) = 0 \quad (2.16)$$

for all $x_2 \in R$ by (2.9). Combining (2.14), (2.15), and (2.16), we get

$$f(x_1, y_1) = 0 \text{ for all } x_1 \in U \quad (2.17)$$

and

$$A(y) = \eta|L||U| \sum_{x_2 \in R} \zeta_e^{T(x_2)} = \eta|L||U| \sum_{x_2 \in R} \zeta_e^{\beta f(y_1, x_2)},$$

proving (2.12).

Claim 4. Denote $W(y) := \sum_{x_2 \in R} \zeta_e^{\beta f(y_1, x_2)}$. Then

$$W(y) \neq 0 \text{ only if } y_1 = 0.$$

Suppose that there is $z_2 \in R$ such that $f(y_1, z_2) \neq 0$. Note that the map $R \rightarrow R$, $x_2 \mapsto (x_2 + z_2)_2$ is a bijection, as the elements of R represent each coset of U in G exactly once. Moreover, for any $r, s \in R$, we have

$$\begin{aligned} f(y_1, r + s) &= f(y_1, (r + s)_1 + (r + s)_2) \\ &= f(y_1, (r + s)_2), \end{aligned}$$

since $f(y_1, (r + s)_1) = 0$ by (2.17). Thus

$$\begin{aligned} \zeta_e^{\beta f(y_1, z_2)} W(y) &= \sum_{x_2 \in R} \zeta_e^{\beta f(y_1, x_2 + z_2)} \\ &= \sum_{x_2 \in R} \zeta_e^{\beta f(y_1, (x_2 + z_2)_2)} \\ &= \sum_{x_2 \in R} \zeta_e^{\beta f(y_1, x_2)} = W(y). \end{aligned}$$

As $\zeta_e^{\beta f(y_1, z_2)} \neq 1$, we conclude $W(y) = 0$, a contradiction. Hence we have

$$f(y_1, x_2) = 0 \text{ for all } x_2 \in R.$$

This, together with (2.17), implies

$$f(y_1, x) = f(y_1, x_1 + x_2) = f(y_1, x_1) + f(y_1, x_2) = 0 \text{ for all } x \in G.$$

Thus $y_1 = 0$, as f is nondegenerate.

In summary, we have shown that the $(0, y)$ th entry of HH^* is only nonzero if $y = 0$. As H is K -invariant by Claim 1, this shows that the (x, y) th entry of HH^* is only nonzero if $x = y$. Hence $HH^* = |K|I$, where I is the identity matrix of order $|K|$.

Claim 5. *The entries of H are e_1 th roots of unity, where e_1 is defined as in (2.7).*

Recall that

$$H_{y,x} = T_{y,x} \zeta_4^{s_L(x_3 \oplus y_3)}, \quad (2.18)$$

where $T_{y,x} = \zeta_e^{f((x-y)_1/2, (x-y)_1) + f((x-y)_1, (x-y)_2)}$. Write $k = \exp(U)$. As $kx = 0$ for all $x \in U$, we have $kf(x, y) = f(kx, y) = f(y, kx) = 0$ for all $x \in U$ and $y \in G$ by the bilinearity of f . As $(x - y)_1 \in U$ for all $x, y \in G$, this shows that

$$T_{y,x}^k = \zeta_e^{f((x-y)_1/2, k(x-y)_1) + f(k(x-y)_1, (x-y)_2)} = \zeta_e^0 = 1 \quad (2.19)$$

for all $x, y \in K$. If $L = \{0\}$, then $e_1 = k$ and $H_{y,x} = T_{y,x}$ and thus $H_{y,x}^{e_1} = 1$ for all $x, y \in K$ by (2.19). If L is of square order, then $e_1 = \text{lcm}(2, k)$, $s_L(x_3 \oplus y_3) \equiv 0 \pmod{2}$ and thus $H_{y,x}^{e_1} = 1$ for all $x, y \in K$ by (2.18) and (2.19). Note that, in any case, $H_{y,x}^{\text{lcm}(4,k)} = 1$ for all $x, y \in K$ by (2.18) and (2.19). Hence H indeed is a $\text{BH}(G, e_1)$ matrix. $\square$

Remark 2.2.3. *In Theorem 2.2.2, there are alternative choices for the function s_L for which the construction still works. Write $|L| = 2^{2a+d}$, where a and d are any nonnegative integers. We call $F : (\mathbb{Z}_2)^{2a} \rightarrow \mathbb{Z}_2$ a **bent function** if*

$$\left| \sum_{x \in (\mathbb{Z}_2)^{2a}} (-1)^{F(x) + \alpha x^T} \right| = 2^a \quad (2.20)$$

for all nonzero $\alpha \in (\mathbb{Z}_2)^{2a}$. Bent functions exist in abundance, see [45, 46], for instance. Let $F : (\mathbb{Z}_2)^{2a} \rightarrow \mathbb{Z}_2$ be any bent function and set

$$s_L(g_1, \dots, g_{2a+d}) = 2F(g_1, \dots, g_{2a}) + \sum_{i=2a+1}^{2a+d} g_i. \quad (2.21)$$

Then (2.6), with s_L defined by (2.21), is still a $\text{BH}(K, e_1)$ matrix with $e_1 = \text{lcm}(4, \exp(U))$. Moreover, if we require $d \in \{0, 1\}$ such that $|L| = 2^{2a+d}$, then e_1 is defined exactly as in (2.7). The proof of this claim follows the same as the proof of Theorem 2.2.2. All we need to verify is that the function s_L , defined in (2.21), still satisfies the equation (2.4).

Lemma 2.2.4. *Under the above notations, we have*

$$\sum_{x \in L} \zeta_4^{s_L(x) - s_L(x \oplus g)} = 0 \quad (2.22)$$

for any $g \in L \setminus \{0\}$.

Proof. First, we claim that for any $h \in (\mathbb{Z}_2)^{2a} \setminus \{0\}$,

$$\sum_{x \in (\mathbb{Z}_2)^{2a}} (-1)^{F(x) - F(x+h)} = 0. \quad (2.23)$$

Write $G = (\mathbb{Z}_2)^{2a}$. The set of characters of G is $\chi_\alpha, \alpha \in G$, each of which is defined by $\chi_\alpha(x) = (-1)^{\alpha x^T}$ for any $x \in G$. Define

$$D = \sum_{x \in G} (-1)^{F(x)} x \in \mathbb{Z}[G].$$

Note that $\chi_\alpha(D) = (-1)^{F(x) + \alpha x^T}$. The equation (2.20) implies $\chi_\alpha(DD^{-1}) = 2^{2a}$ for any $\alpha \in G$. By Result 1.3.8, we obtain

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

The coefficient of $(-h)$ in $DD^{(-1)}$ is equal to $\sum_{x \in (\mathbb{Z}_2)^{2a}} (-1)^{F(x) - F(x+h)}$. As $h \neq 0$, this coefficient is also equal to 0, proving the claim (2.23).

Now for $x \in L$, define $X_1 = (x_1, \dots, x_{2a}) \in G$ and $X_2 = (x_{2a+1}, \dots, x_{2a+d})$. Define G_1 and G_2 similarly for $g \in L$. Write

$$A(g) = \sum_{x \in L} \zeta_4^{s_L(x) - s_L(x \oplus g)} = \sum_{X_1 \in G, X_2 \in (\mathbb{Z}_2)^d} \zeta_4^{2F(X_1) - 2F(X_1 + G_1) + \sum_{i=2a+1}^{2a+d} (x_i - x_i \oplus g_i)}$$

Suppose that $A(g) \neq 0$. By (2.23), we have $G_1 = 0$. Hence

$$A(g) = 2^{2a} \sum_{X_2 \in (\mathbb{Z}_2)^d} \zeta_4^{\sum_{i=2a+1}^{2a+d} (x_i - x_i \oplus g_i)} = 2^{2a} \prod_{i=2a+1}^{2a+d} \left(\sum_{x_i=0,1} \zeta_4^{x_i - x_i \oplus g_i} \right).$$

For any $2a+1 \leq i \leq 2a+d$, we have

$$\sum_{x_i=0,1} \zeta_4^{x_i - x_i \oplus g_i} = \begin{cases} 0 & \text{if } g_i = 1, \\ 2 & \text{if } g_i = 0. \end{cases}$$

Therefore, we have $A(g) \neq 0$ only if $g_i = 0$ for all $2a+1 \leq i \leq 2a+d$. To sum up, we obtain $A(g) \neq 0$ only when $g = 0$. $\square$

Remark 2.2.5. The functions $s_L : L \rightarrow \mathbb{Z}$ defined in Lemma 2.2.1 and Remark 2.2.3 can be viewed as special cases of $\mathbb{Z}_4$ -valued quadratic forms in [64] as follows. A function $s_L : L \rightarrow \mathbb{Z}_4$ is called a $\mathbb{Z}_4$ -valued quadratic form if the map $B : L \times L \rightarrow 2\mathbb{Z}_4$ defined by

$B(g, h) = s_L(g \oplus h) - s_L(g) - s_L(h)$ is a bilinear form. If B is nondegenerate and $g \neq 0$, then

$$\sum_{x \in L} \zeta_4^{s_L(x) - s_L(x \oplus g)} = \sum_{x \in L} \zeta_4^{-B(x, g) - s_L(g)} = \zeta_4^{-s_L(g)} \sum_{x \in L} \zeta_4^{-B(x, g)} = 0,$$

since $\chi : L \rightarrow \mathbb{C}^*$, $\chi(x) = \zeta_4^{-B(x, g)} = (-1)^{B(x, g)/2}$, is a nontrivial character of L (note that $B(x, g) \in \{0, 2\}$ and B is nondegenerate). Thus, the proofs of Lemmas 2.2.1 and 2.2.4 reduce to checking the nondegeneracy of $B(g, h)$, which is true in both of these cases.

For groups K and W , we say that K has a **direct factor** W if $K \cong W \times V$ for some group V .

Corollary 2.2.6. *Let K be a finite abelian group and let h be a positive integer such that*

$$\nu_p(h) \geq \lceil \nu_p(\exp(K))/2 \rceil \text{ for every prime divisor } p \text{ of } |K|, \quad (2.24)$$

$$\nu_2(h) \geq 2 \text{ if } \nu_2(|K|) \text{ is odd and } K \text{ has a direct factor } \mathbb{Z}_2. \quad (2.25)$$

Then there exists a $\text{BH}(K, h)$ matrix.

Proof. Write $K = G \times L$, where either $L = \{0\}$ or L is an elementary abelian 2-group, such that G does not have a direct factor $\mathbb{Z}_2$. Without loss of generality, we can assume $G = \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_s^{a_s}}$, where $p_1, \dots, p_s$ are (not necessarily distinct) primes and $a_1, \dots, a_s$ are positive integers. Note that $p_i^{a_i} \neq 2$ for all i , as G has no direct factor $\mathbb{Z}_2$. Furthermore, $|L| > 1$ if and only if K has a direct factor $\mathbb{Z}_2$. We identify G with

$$\{(g_1, \dots, g_s) : 0 \leq g_i \leq p_i^{a_i} - 1, i = 1, \dots, s\},$$

where the group operation is componentwise addition, the i th component being taken modulo $p_i^{a_i}$. Let U be the subgroup of G given by

$$U = \left\{ \left(p_1^{\lfloor a_1/2 \rfloor} k_1, \dots, p_s^{\lfloor a_s/2 \rfloor} k_s \right) : 0 \leq k_i \leq p_i^{\lfloor a_i/2 \rfloor} - 1, i = 1, \dots, s \right\}.$$

Write $e = \exp(G)$ and define a map $f : G \times G \rightarrow \mathbb{Z}_e$ by

$$f((g_1, \dots, g_s), (h_1, \dots, h_s)) = \sum_{i=1}^s \frac{e}{p_i^{a_i}} g_i h_i.$$

It is straightforward to verify that f is bilinear and symmetric. Let $g = (g_1, \dots, g_s)$ be any nonzero element of G . Then $g_i \neq 0$ for some i . Let t be the element of G with $t_i = 1$

and $t_j = 0$ for all $j \neq i$. Then $f(g, t) = \frac{e}{p_i^{a_i}} g_i \neq 0$, since $g_i \not\equiv 0 \pmod{p_i^{a_i}}$. This shows that f is nondegenerate.

Suppose that $g = (g_1, \dots, g_s)$ is an element which is orthogonal to all elements of U . Let i be arbitrary and let s be the element of U with $s_i = p_i^{\lfloor a_i/2 \rfloor}$ and $s_j = 0$ for all $j \neq i$. Then

$$f(g, s) = \frac{e}{p_i^{a_i}} g_i p_i^{\lfloor a_i/2 \rfloor} = \frac{e}{p_i^{\lfloor a_i/2 \rfloor}} g_i = 0$$

and thus $g_i \equiv 0 \pmod{p_i^{\lfloor a_i/2 \rfloor}}$. This implies $g \in U$. Hence there is no element of $G \setminus U$ which is orthogonal to all elements of U .

Next, we show that every element $u = (u_1, \dots, u_s)$ of U has a square root in G . If $p_i = 2$, then $a_i \geq 2$, as we are assuming $p_i^{a_i} \neq 2$ for all i . Thus $u_i \equiv 0 \pmod{2}$ by the definition of U , that is, $u_i = 2y_i$ with $y_i \in \{0, \dots, 2^{a_i-1} - 1\}$. On the other hand, if p_i is odd, then the map $x \mapsto 2x \pmod{p_i^{a_i}}$ is a bijection and thus there is $y_i \in \{0, \dots, p_i^{a_i} - 1\}$ with $2y_i \equiv u_i \pmod{p_i^{a_i}}$. In summary, we have $u = 2y$, i.e., y is a square root of u .

We have shown that all assumptions of Theorem 2.2.2 are satisfied. Hence there exists a $\text{BH}(K, e_1)$ matrix, where e_1 is defined in Theorem 2.2.2, that is

$$e_1 = \begin{cases} \exp(U) & \text{if } L = \{0\}, \\ \text{lcm}(2, \exp(U)) & \text{if } L \text{ is of square order,} \\ \text{lcm}(4, \exp(U)) & \text{otherwise.} \end{cases} \quad (2.26)$$

As a $\text{BH}(K, e_1)$ matrix is automatically a $\text{BH}(K, e_2)$ matrix whenever $e_1 \mid e_2$, it suffices to show

$$h \equiv 0 \pmod{e_1}. \quad (2.27)$$

Note that

$$\exp(U) = \text{lcm} \left(p_i^{\lfloor a_i/2 \rfloor} : i = 1, \dots, s \right) \quad (2.28)$$

and $h \equiv 0 \pmod{p_i^{\lfloor a_i/2 \rfloor}}$ by (2.24). Hence

$$h \equiv 0 \pmod{\exp(U)}. \quad (2.29)$$

If $L = \{0\}$, then $e_1 = \exp(U)$ and (2.27) follows from (2.29). Now assume $|L| > 1$. If $\nu_2(\exp(K)) \geq 3$, then $h \equiv 0 \pmod{4}$ by (2.24) and thus (2.27) holds by (2.29) and (2.26). Hence we can assume $\nu_2(\exp(K)) \in \{1, 2\}$, i.e., $a_i = 2$ whenever $p_i = 2$. Note that this implies that $\nu_2(|G|)$ is even. Suppose that $\nu_2(|K|)$ is even. Then $\nu_2(|L|)$ is also even, that is, L is of square order. Thus $e_1 = \text{lcm}(2, \exp(U))$ and (2.27) follows from (2.24) and (2.29). Finally, suppose that $\nu_2(|K|)$ is odd. Then K has a direct factor

$\mathbb{Z}_2$, as we are assuming $\nu_2(\exp(K)) \leq 2$. Thus $h \equiv 0 \pmod{4}$ by (2.25), which implies (2.27). Thus (2.27) holds in every case and this completes the proof. $\square$

Corollary 2.2.7. *If v and h are positive integers with*

- (i) $\nu_p(h) \geq \lceil \nu_p(v)/2 \rceil$ for every prime divisor p of v and
- (ii) $\nu_2(h) \geq 2$ if $v \equiv 2 \pmod{4}$,

then a (circulant) $\text{BH}(\mathbb{Z}_v, h)$ matrix exists.

We remark that Corollary 2.2.7 is a generalization of Result 1.2.1.

2.2.2 Construction from Finite Local Rings

The construction in this section comes from the study of relative difference sets in finite local rings by Ma and Leung [37]. Eventually, the idea of using local rings goes back to the paper “Difference Sets in 2-groups” by Dillon [17]. We start with the definition and basic properties of finite local rings which will be needed for our construction.

A ring R is called a **local ring** if it has a unique maximal ideal. We recall the following result [37, Proposition 2.4] on the existence of a finite local ring.

Result 2.2.8. *Let d, r and s be positive integers. Then for any prime p , there exists a finite local ring R of order p^{ds} such that*

- (i) *its maximal ideal I is generated by a prime element π ,*
- (ii) *$\pi^{s-1} \neq 0, \pi^s = 0$ and $p = \pi^r u$ for some unit u in R , and*
- (iii) *R/I is a finite field of order p^d .*

Furthermore, if we write $s = ar + b$, where $0 \leq b \leq r - 1$, then the additive group $(R, +)$ is isomorphic to $\mathbb{Z}_{p^{a+1}}^{db} \times \mathbb{Z}_{p^a}^{d(r-b)}$.

Note that each element $x \in R \setminus \{0\}$ can be written uniquely as $x = \pi^k u$ for some non-negative integer $k \leq s - 1$ and a unit u in R . The next result [37, Thm. 3.1 and Thm. 4.1] partitions the group $R \times R$ in a nice way which later becomes the main ingredient for our construction.

Result 2.2.9. *Let $\phi : R \rightarrow R$ be defined by $x = \pi^k u \rightarrow \phi(x) = \pi^k u^{-1}$. Assume that $\{R_0, \dots, R_{p^t-1}\}$, $1 \leq t \leq d$, is a partition of R such that for any coset $a + I^{s-1}$ of R (there are $p^{d(s-1)}$ cosets) and $0 \leq i \leq p^t - 1$, we have $|R_i \cap (a + I^{s-1})| = p^{d-t}$. Denote the characteristic function of R_i by f_i . We have the following.*

(a) $\sum_{w \in I^{s-1}} f_i(a+w) = p^{d-t}$ for any $a \in R$ and $i = 0, \dots, p^t - 1$, and

(b) $\sum_{i=0}^{p^t-1} f_i(a) = 1$ for any $a \in R$.

For each $i = 0, \dots, p^t - 1$, define

$$D_i = \{(x, y) \in R \times R : f_i(\phi(x)y) = 1\}. \quad (2.30)$$

Then $\{D_0, \dots, D_{p^t-1}\}$ is a partition of $R \times R$. Moreover for any character χ of $R \times R$, we have

$$\chi(D_i) = \begin{cases} p^{sd} f_i(0) + p^{sd-t}(p^{sd} - 1) & \text{if } \chi = \chi_0, \\ p^{sd} f_i(c_\chi) - p^{sd-t} & \text{if } \chi \neq \chi_0 \end{cases},$$

where $c_\chi \in R$ depends only on χ .

Theorem 2.2.10. Let d and r be positive integers, let a be a non-negative integer and let b be an integer with $0 \leq b \leq r-1$. Put $R = \mathbb{Z}_{p^{a+1}}^{db} \times \mathbb{Z}_{p^a}^{d(r-b)}$. If there exists a positive integer $t \leq d$ and h th roots of unity $\eta_0, \dots, \eta_{p^t-1}$ such that

$$\sum_{i=0}^{p^t-1} \eta_i = 0, \quad (2.31)$$

then a $\text{BH}(R \times R, h)$ matrix exists.

Proof. Putting $s = ar + b$, we can assume that R is a finite local ring as defined in Result 2.2.8. Let D_i be defined as in (2.30) and let η_i be h th roots of unity which satisfy (2.31). Define

$$D = \sum_{i=0}^{p^t-1} \eta_i D_i \in \mathbb{Z}[\zeta_h][R \times R].$$

We prove that the group ring element D implies a $\text{BH}(R \times R, h)$ matrix. As $\{D_0, \dots, D_{p^t-1}\}$ is a partition of $R \times R$, all coefficients of D are h th roots of unity. It remains, by Lemma 2.1.2, to prove that $DD^{(-1)} = |R \times R| = p^{2ds}$.

Let χ_0 denote the trivial character of $R \times R$. We have

$$\chi_0(D) = p^{sd} \left(\sum_{i=0}^{p^t-1} \eta_i f_i(0) \right) + p^{sd-t}(p^{sd} - 1) \left(\sum_{i=0}^{p^t-1} \eta_i \right) = p^{sd} \eta_j,$$

where j is in unique index in $\{0, \dots, p^t - 1\}$ such that $0 \in R_j$. Hence $\chi_0(DD^{(-1)}) = p^{2sd}$. Moreover, let χ be any nontrivial character of $R \times R$. We have

$$\chi(D) = p^{sd} \left(\sum_{i=0}^{p^t-1} \eta_i f_i(c_\chi) \right) - p^{sd-t} \left(\sum_{i=0}^{p^t-1} \eta_i \right) = p^{sd} \eta_j,$$

where j is in unique index in $\{0, \dots, p^t - 1\}$ such that $c_\chi \in R_j$. Hence $\chi(DD^{(-1)}) = p^{2sd}$.

We have proved $\chi(DD^{(-1)}) = p^{2sd} = |R \times R|$ for any character χ of $R \times R$. By Result 1.3.8, we obtain

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

□

2.2.3 BH(G, h) Matrices with G non-abelian

In this section, we construct a family of group-invariant Butson Hadamard matrices in which the group G does not need to be abelian. The main idea in our construction comes from modifying the building set idea used in the study of relative difference sets, see [14] for more details about building sets. The following lemma is the main ingredient for our construction.

Lemma 2.2.11. *Let n be a positive integer and let h be the smallest positive integer with the property*

$$h^2 \equiv 0 \pmod{n} \text{ and } (\nu_2(n), \nu_2(h)) \neq (1, 1). \quad (2.32)$$

Define

$$k = \begin{cases} n/h & \text{if } \nu_2(n) \neq 1, \\ 2n/h & \text{otherwise.} \end{cases} \quad (2.33)$$

Then there exists a set of k group-ring elements $D_i \in \mathbb{Z}[\zeta_h][\mathbb{Z}_{n/k}]$, $0 \leq i \leq k-1$, which has the following properties.

1. $D_i = \sum_{g \in \mathbb{Z}_{n/k}} a_{ig} g$, where each a_{ig} is a complex h th root of unity.
2. For each character χ of $\mathbb{Z}_{n/k}$, the character value $\chi(D_i)$ is nonzero for exactly one $i \in \{0, \dots, k-1\}$ and $\chi(D_i D_i^{-1}) = n$ for this value of i .

Consequently, we have

$$D_i D_j^{(-1)} = 0 \text{ whenever } i \neq j \text{ and } \sum_{i=0}^{k-1} D_i D_i^{(-1)} = n. \quad (2.34)$$

To prove Lemma 2.2.11, we need the following result. The first part of the result is a familiar property of quadratic Gauss sums. The sum in the second part looks similar to a quadratic Gauss sum in the first glance, yet they are different. For completeness, we include proofs for both parts.

Lemma 2.2.12. *Let n be an odd positive integer and let b be an integer.*

(a) *If $X \in \mathbb{Z}[\zeta_n]$ has form $X = \sum_{i=0}^{n-1} \zeta_n^{i^2+bi}$, then*

$$X\bar{X} = n.$$

(b) *If $X \in \mathbb{Z}[\zeta_{4n}]$ has form $X = \sum_{i=0}^{2n-1} \zeta_{4n}^{i^2+2bi}$, then*

$$X\bar{X} = 2n.$$

Proof. (a) We have

$$X\bar{X} = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \zeta_n^{(i+j)^2+b(i+j)-i^2-bi} = \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} \zeta_n^{j^2+bj+2ji}$$

As n is odd, we have $\sum_{i=0}^{n-1} \zeta_n^{2ji} = 0$ for any $j \neq 0$. Thus $X\bar{X} = n$.

(b) For $0 \leq i \leq 2n-1$, write $i = 2j + k$ with $0 \leq k \leq 1$ and $0 \leq j \leq n-1$. We obtain

$$\begin{aligned} X &= \sum_{k=0}^1 \sum_{j=0}^{n-1} \zeta_{4n}^{4j^2+4jk+k^2+4bj+2bk} \\ &= \sum_{j=0}^{n-1} \zeta_n^{j^2+bj} + \zeta_{4n}^{2b+1} \sum_{j=0}^{n-1} \zeta_n^{j^2+(b+1)j}. \end{aligned}$$

Put $Y = \sum_{j=0}^{n-1} \zeta_n^{j^2+bj}$ and $Z = \sum_{j=0}^{n-1} \zeta_n^{j^2+(b+1)j}$. Hence

$$X = Y + \zeta_{4n}^{2b+1} Z. \quad (2.35)$$

By part (a), we have

$$Y\bar{Y} = Z\bar{Z} = n. \quad (2.36)$$

Moreover, we have

$$\begin{aligned} Z\bar{Y} &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \zeta_n^{(i+j)^2+(b+1)(i+j)-i^2-bi} \\ &= \sum_{j=0}^{n-1} \zeta_n^{j^2+(b+1)j} \sum_{i=0}^{n-1} \zeta_n^{(2j+1)i} \\ &= n \zeta_{4n}^{(n^2-1)+2b(n-1)}. \end{aligned}$$

Hence $Y\bar{Z} = n\zeta_{4n}^{(1-n^2)+2b(1-n)}$. Combining with (2.35) and (2.36), we obtain

$$\begin{aligned} X\bar{X} &= Y\bar{Y} + Z\bar{Z} + \zeta_{4n}^{-2b-1}Y\bar{Z} + \zeta_{4n}^{2b+1}Z\bar{Y} \\ &= 2n + n(\zeta_{4n}^{-n^2-2bn} + \zeta_{4n}^{n^2+2bn}) \\ &= 2n. \end{aligned}$$

□

Proof of Lemma 2.2.11

Proof. Let g denote a generator of $\mathbb{Z}_{n/k}$. Let m be a fixed positive integer which is coprime to n . There are three cases concerning the parity of $\nu_2(n)$ and whether $\nu_2(n) = 1$.

Case 1. $\nu_2(n)$ is even.

In this case, we have $h = n/k$ and $\mathbb{Z}_{n/k} = \mathbb{Z}_h$. For each $0 \leq i \leq k-1$, define

$$D_i = \sum_{j=0}^{h-1} \zeta_h^{j^2k+mij} g^j \in \mathbb{Z}[\zeta_h][\mathbb{Z}_h].$$

As h is the smallest positive integer with the property (2.32), we have $\nu_2(h) = \nu_2(n)/2$. Hence, the number $l = h/k = h^2/n$ is odd. Let χ be any character of $\mathbb{Z}_h$. Assume $\chi(g) = \zeta_h^t$ for some $t \in \mathbb{Z}$. We have

$$\chi(D_i) = \sum_{j=0}^{h-1} \zeta_h^{j^2k+j(mi+t)}.$$

Note that $h = lk$. Write $j = lx + y$ with $0 \leq x \leq k-1$ and $0 \leq y \leq l-1$. We obtain

$$\chi(D_i) = \sum_{y=0}^{l-1} \sum_{x=0}^{k-1} \zeta_h^{y^2k+y(mi+t)+lx(mi+t)} = \sum_{y=0}^{l-1} \zeta_h^{y^2k+y(mi+t)} \sum_{x=0}^{k-1} \zeta_k^{x(mi+t)}.$$

Hence

$$\chi(D_i) = \begin{cases} 0 & \text{if } mi+t \not\equiv 0 \pmod{k}, \\ k \sum_{y=0}^{l-1} \zeta_l^{y^2+y(mi+t)/k} & \text{if } mi+t \equiv 0 \pmod{k}. \end{cases}$$

As $(m, k) = 1$, there is only one $i \in \{0, \dots, k-1\}$ with $mi+t \equiv 0 \pmod{k}$. Thus, there is only one $D_i \in \{D_0, \dots, D_{k-1}\}$ such that $\chi(D_i) \neq 0$. Moreover by Lemma 2.2.12 part (a), the sum $\sum_{y=0}^{l-1} \zeta_l^{y^2+y(mi+t)/k}$ has square norm l . We obtain

$$\chi(D_i D_i^{(-1)}) = |\chi(D_i)|^2 = k^2 l = n.$$

Case 2. $\nu_2(n)$ is odd and $\nu_2(n) \geq 3$.

In this case, we have $h = n/k$ and $\mathbb{Z}_{n/k} = \mathbb{Z}_h$. For each $0 \leq i \leq k-1$, define

$$D_i = \sum_{j=0}^{h-1} \zeta_h^{j^2 k/2 + mij} g^j \in \mathbb{Z}[\zeta_h][\mathbb{Z}_h].$$

As h is the smallest positive integer with the property (2.32), we have $\nu_2(h) = (\nu_2(n) + 1)/2$. Note that the group-ring elements D_i are well defined, as $k = n/h \equiv 0 \pmod{2}$. Moreover, the number $l = h/(2k) = h^2/(2n)$ is odd. Let χ be any character of $\mathbb{Z}_h$. Assume $\chi(g) = \zeta_h^t$ for some $t \in \mathbb{Z}$. We have

$$\chi(D_i) = \sum_{j=0}^{h-1} \zeta_h^{j^2 k/2 + j(mi+t)}.$$

Note that $h = 2lk$. Write $j = 2lx + y$ with $0 \leq x \leq k-1$ and $0 \leq y \leq 2l-1$. We obtain

$$\chi(D_i) = \sum_{y=0}^{2l-1} \sum_{x=0}^{k-1} \zeta_h^{y^2 k/2 + y(mi+t) + 2lx(mi+t)} = \sum_{y=0}^{2l-1} \zeta_h^{y^2 k/2 + y(mi+t)} \sum_{x=0}^{k-1} \zeta_k^{x(mi+t)}.$$

Hence

$$\chi(D_i) = \begin{cases} 0 & \text{if } mi+t \not\equiv 0 \pmod{k}, \\ k \sum_{y=0}^{2l-1} \zeta_{4l}^{y^2 + 2y(mi+t)/k} & \text{if } mi+t \equiv 0 \pmod{k}. \end{cases}$$

There is only one $i \in \{0, \dots, k-1\}$ with $mi+t \equiv 0 \pmod{k}$, so there is only one $D_i \in \{D_0, \dots, D_{k-1}\}$ such that $\chi(D_i) \neq 0$. Moreover by Lemma 2.2.12.(b), the sum $\sum_{y=0}^{2l-1} \zeta_{4l}^{y^2 + 2y(mi+t)/k}$ has square norm $2l$. We obtain

$$\chi(D_i D_i^{(-1)}) = |\chi(D_i)|^2 = k^2(2l) = n.$$

Case 3. $\nu_2(n) = 1$.

In this case, we have $h = 2n/k$ and $\mathbb{Z}_{n/k} = \mathbb{Z}_{h/2}$. For each $0 \leq i \leq k-1$, define

$$D_i = \sum_{j=0}^{h/2-1} \zeta_h^{j^2 k + 2mij} g^j \in \mathbb{Z}[\zeta_h][\mathbb{Z}_{h/2}].$$

By (2.32), we have $\nu_2(h) = 2$. Hence, the number $l = h/(4k) = h^2/(8n)$ is odd. Let χ be any character of $\mathbb{Z}_{h/2}$. Assume $\chi(g) = \zeta_{h/2}^t = \zeta_h^{2t}$ for some $t \in \mathbb{Z}$. We have

$$\chi(D_i) = \sum_{j=0}^{h/2-1} \zeta_h^{j^2 k + 2j(mi+t)}.$$

Note that $h = 4lk$. Write $j = 2lx + y$ with $0 \leq x \leq k-1$ and $0 \leq y \leq 2l-1$. We obtain

$$\chi(D_i) = \sum_{y=0}^{2l-1} \sum_{x=0}^{k-1} \zeta_h^{y^2 k + 2y(mi+t) + 4lx(mi+t)} = \sum_{y=0}^{2l-1} \zeta_h^{y^2 k + 2y(mi+t)} \sum_{x=0}^{k-1} \zeta_k^{x(mi+t)}.$$

Hence

$$\chi(D_i) = \begin{cases} 0 & \text{if } mi + t \not\equiv 0 \pmod{k}, \\ k \sum_{y=0}^{2l-1} \zeta_{4l}^{y^2 + 2y(mi+t)/k} & \text{if } mi + t \equiv 0 \pmod{k}. \end{cases}$$

There is only one $i \in \{0, \dots, k-1\}$ which satisfies $mi + t \equiv 0 \pmod{k}$, so there is only one $D_i \in \{D_0, \dots, D_{k-1}\}$ such that $\chi(D_i) \neq 0$. Moreover by Lemma 2.2.12.(b), the sum $\sum_{y=0}^{2l-1} \zeta_{4l}^{y^2 + 2y(mi+t)/k}$ has square norm $2l$. We obtain

$$\chi(D_i D_i^{(-1)}) = |\chi(D_i)|^2 = k^2(2l) = n.$$

Lastly, the claim (2.34) follows from Result 1.3.8. $\square$

Theorem 2.2.13. *Let n and h be positive integers such that*

$$h^2 \equiv 0 \pmod{n} \text{ and } (\nu_2(n), \nu_2(h)) \neq (1, 1). \quad (\star)$$

Let k be a positive integer of n which is defined by

$$k = \begin{cases} n/h & \text{if } \nu_2(n) \neq 1, \\ 2n/h & \text{otherwise.} \end{cases} \quad (2.37)$$

Suppose that G is a group of order n which contains a normal subgroup isomorphic to $\mathbb{Z}_{n/k}$. Then there exists a $\text{BH}(G, h)$ matrix.

Proof. Note that a $\text{BH}(G, h)$ matrix is automatically a $\text{BH}(G, h')$ matrix whenever $h \mid h'$, as an h th root of unity is a power of an h' root of unity. Hence, we can assume that h is the smallest positive integer with the property $(\star)$. Let $D_0, \dots, D_{k-1}$ be defined as in Lemma 2.2.11. Let $x_0, \dots, x_{k-1}$ be a full set of coset representatives of $\mathbb{Z}_{n/k}$ in G . Define

$$D = \sum_{i=0}^{k-1} x_i D_i.$$

Using (2.34), we obtain

$$DD^{(-1)} = \sum_{i,j=0}^{k-1} x_i D_i D_j^{(-1)} x_j^{-1} = \sum_{i=0}^{k-1} D_i D_i^{(-1)} = n.$$

The existence of a $\text{BH}(G, h)$ matrix follows by Lemma 2.1.2. $\square$

2.3 Necessary Conditions

In this section, we study necessary conditions for the existence of $\text{BH}(G, h)$ matrices in which the group G is abelian. Our focus is on two types of matrices: $\text{BH}(\mathbb{Z}_n, h)$ matrices and $\text{BH}(G, 2p^b)$ matrices, where p is an odd prime and n, h, b are positive integers.

We first give an overview of our approach. Assume that $H = (H_{g,k})_{g,k \in G}$ is a $\text{BH}(G, h)$ matrix. For any $g \in G$, define $a_g = H_{1,g^{-1}}$. Define $D = \sum_{g \in G} a_g g$. By Lemma 2.1.2, we have $DD^{(-1)} = |G|$. Put $n = |G|$ and put $m = \text{lcm}(\exp(G), h)$. Let χ be a character of G and write $X = \chi(D) \in \mathbb{Z}[\zeta_m]$. We have

$$|X|^2 = n, \quad X \in \mathbb{Z}[\zeta_m]. \quad (2.38)$$

By the field-descent method, there exists an integer j such that $X\zeta_m^j$ belongs to a proper subfield $\mathbb{Q}(\zeta_k)$ of $\mathbb{Q}(\zeta_m)$. Note that $X\zeta_m^j$ is a sum of roots of unity in $\mathbb{Q}(\zeta_m)$. As $X\zeta_m^j$ belongs to the subfield $\mathbb{Q}(\zeta_k)$, usually a lot of the roots of unity in the sum cancel out. The norm of the remaining terms can be bounded using our result on the norm of cyclotomic integers. On the other hand, by (2.38), this norm is equal to $\sqrt{n}$. We thus obtain a restriction on n and h .

2.3.1 Summary of Known Results

In this section, we summarize known results on the existence of group-invariant Butson Hadamard matrices. We will illustrate later that our results can further improve the known ones.

First, we note that the only known sufficient condition for the existence of circulant Butson Hadamard matrices is Result 1.2.1 by Backelin, which states that there exists a $\text{BH}(\mathbb{Z}_n, n/p)$ matrix if n is a positive integer and p is a prime such that

$$n \equiv 0 \pmod{p^2} \text{ and } n \not\equiv 2 \pmod{4}.$$

Result 2.3.1. *The following Butson Hadamard matrices do not exist*

1. [35, Leung-Schmidt] $\text{BH}(\mathbb{Z}_{2p^2}, 2p)$ matrices with p being an odd prime.
2. [39, Ma-Ng] $\text{BH}(\mathbb{Z}_{3pq}, 3)$ matrices with $p, q > 3$ being distinct primes.
3. [28, Hiranandani-Schlenker] $\text{BH}(\mathbb{Z}_{p+q}, pq)$ matrices with $p, q > 3$ being distinct primes.

Result 2.3.2. [28, Sylvester conditions]

- (i) If a $\text{BH}(n, 2)$ matrix exists, then $n = 2$ or $n \equiv 0 \pmod{4}$. Furthermore, if a $\text{BH}(\mathbb{Z}_n, 2)$ matrix exists, then $n \equiv 0 \pmod{4}$ and $n/4$ is a square.
- (ii) Let $p \geq 3$ be a prime. If a $\text{BH}(p+2, h)$ matrix exists, then h does not have the form $2^a p^b$ for some positive integer b .
- (iii) Let $q \geq 3$ be a prime. If a $\text{BH}(2q, h)$ matrix exists, then h does not have the form $2^a p^b$ for $a, b \in \mathbb{Z}^+$ and any prime $p > q$.

Result 2.3.3. [31, Lam-Leung] If a $\text{BH}(G, h)$ matrix exists and $p_1, \dots, p_r$ are the distinct prime divisors of h , then there exist nonnegative integers a_i such that $|G| = \sum_{i=1}^r a_i p_i$.

Result 2.3.4. [9, Brock] Let n and h be positive integers. Let m be the square-free part of n and assume that m is odd. If a $\text{BH}(n, h)$ matrix exists, then m has no prime factor p which satisfies

- (a) p does not divide h , and
- (b) $p^j \equiv -1 \pmod{h}$ for some integer j .

Remark 2.3.5. Using Results 1.2.1, 2.3.1, 2.3.2, 2.3.3 and 2.3.4, we have 5071 open cases for the existence of a $\text{BH}(\mathbb{Z}_n, h)$ matrix in which $1 \leq n, h \leq 100$. We will illustrate in Remark 2.3.23 that our results can be used to reduce this number of open cases.

2.3.2 Bounds on Norms of Cyclotomic Integers

Recall that a cyclotomic integer is a complex number which can be expressed as a sum of roots of unity. We start this section with the following bound on the norm of a cyclotomic integer. This bound will also be used in Chapter 4 in our study on cyclotomic numbers.

Lemma 2.3.6. Let $\alpha = \sum_{i=0}^{m-1} c_i \zeta_m^i$, $c_i \in \mathbb{Z}$, be an element of $\mathbb{Z}[\zeta_m]$. Then

$$|N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha)| \leq \left(\frac{m}{\varphi(m)} \sum_{i=0}^{m-1} c_i^2 \right)^{\varphi(m)/2}. \quad (2.39)$$

Proof. Put $f(x) = \sum_{i=0}^{m-1} c_i x^i \in \mathbb{Z}[x]$. Note that $\alpha = f(\zeta_m)$ and the conjugates of α in $\mathbb{Q}(\zeta_m)$ are $f(\zeta_m^t)$, where t is coprime to m . We have

$$\sum_{k=0}^{m-1} |f(\zeta_m^k)|^2 = \sum_{i,j,k=0}^{m-1} c_i c_j \zeta_m^{(i-j)k} = m \sum_{i=0}^{m-1} c_i^2.$$

By the inequality of arithmetic and geometric means, we obtain

$$\begin{aligned}
|N(f(\zeta_m))| &= \left| \prod_{(t,m)=1} f(\zeta_m^t) \right| \\
&\leq \left(\frac{\sum_{(t,m)=1} |f(\zeta_m^t)|^2}{\varphi(m)} \right)^{\varphi(m)/2} \\
&\leq \left(\frac{\sum_{k=0}^{m-1} |f(\zeta_m^k)|^2}{\varphi(m)} \right)^{\varphi(m)/2} \\
&= \left(\frac{m}{\varphi(m)} \sum_{i=0}^{m-1} c_i^2 \right)^{\varphi(m)/2}.
\end{aligned}$$

□

The following result by Schmidt [49] will be needed later. We include a proof for the convenience of the reader.

Result 2.3.7. *Let $m = \prod_{i=1}^t p_i^{a_i}$ be the prime factorization of a positive integer m , and let k be a divisor of m . Write $k = \prod_{i=1}^s p_i^{b_i}$, where $s \leq t$ and $1 \leq b_i \leq a_i$ for $i = 1, \dots, s$. Then*

$$\begin{aligned}
\mathcal{B}_{m,k} &= \left\{ \prod_{i=1}^s \zeta_{p_i^{a_i}}^{r_i} \prod_{i=s+1}^t \zeta_{p_i^{a_i}}^{k_i} \zeta_{p_i^{a_i}}^{l_i} : 0 \leq r_i \leq p_i^{a_i-b_i} - 1, \right. \\
&\quad \left. 0 \leq k_i \leq p_i - 2, 0 \leq l_i \leq p_i^{a_i-1} - 1 \right\}
\end{aligned}$$

is an integral basis of $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}(\zeta_k)$. Furthermore, assume that

$$X = \sum_{i=0}^{m-1} c_i \zeta_m^i, \quad c_i \in \mathbb{Z},$$

is an element in $\mathbb{Z}[\zeta_m]$ with $0 \leq c_i \leq C$ for all i , then we can express X as

$$X = \sum_{x \in \mathcal{B}_{m,k}} x \left(\sum_{j=0}^{k-1} c_{xj} \zeta_k^j \right), \quad \text{where } |c_{xj}| \leq 2^{t-s-1+\delta_{ts}} C \text{ for all } x, j. \quad (2.40)$$

Proof. For each $0 \leq j \leq m-1$, we can write ζ_m^j as

$$\begin{aligned}
\zeta_m^j &= \prod_{i=1}^t \zeta_{p_i^{a_i}}^{c_{ij}} = \prod_{i=1}^s \zeta_{p_i^{a_i}}^{u_{ij} p_i^{a_i-b_i} + r_{ij}} \prod_{i=s+1}^t \zeta_{p_i^{a_i}}^{k_{ij} p_i^{a_i-1} + l_{ij}} \\
&= \zeta_k^{u_j} \prod_{i=1}^s \zeta_{p_i^{a_i}}^{r_{ij}} \prod_{i=s+1}^t \zeta_{p_i^{a_i}}^{k_{ij}} \zeta_{p_i^{a_i}}^{l_{ij}},
\end{aligned}$$

where $\zeta_k^{u_j} = \prod_{i=1}^s \zeta_{p_i}^{u_{ij}} \in \mathbb{Z}[\zeta_k]$ and $0 \leq c_{ij} \leq p_i^{a_i} - 1$, $0 \leq u_{ij} \leq p_i^{b_i} - 1$, $0 \leq r_{ij} \leq p_i^{a_i - b_i} - 1$, $0 \leq k_{ij} \leq p_i - 1$, $0 \leq l_{ij} \leq p_i^{a_i - 1} - 1$. Moreover note that $\zeta_{p_i}^{p_i - 1} = -1 - \zeta_{p_i} - \dots - \zeta_{p_i}^{p_i - 2}$ for any $i = s + 1, \dots, t$. So the linear combination of elements of $\mathcal{B}_{m,k}$ with coefficients from $\mathbb{Z}[\zeta_k]$ covers $\mathbb{Z}[\zeta_m]$. This shows that $\mathcal{B}_{m,k}$ is an integral basis of $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}(\zeta_k)$, as $|\mathcal{B}_{m,k}| = \varphi(m)/\varphi(k) = \dim_{\mathbb{Q}(\zeta_k)}(\mathbb{Q}(\zeta_m))$.

Next, write $X = \sum_{j=0}^{m-1} c_j \zeta_m^j$ as

$$X = \sum_{u, r_i, k_i, l_i} c_{ur_1 \dots r_s k_{s+1} \dots k_t l_{s+1} \dots l_t} \zeta_k^u \prod_{i=1}^s \zeta_{p_i}^{r_i} \prod_{i=s+1}^t \zeta_{p_i}^{k_i} \zeta_{p_i}^{l_i}, \quad (2.41)$$

where the sum is taken over $0 \leq u \leq k - 1$, $0 \leq r_i \leq p_i^{a_i - b_i} - 1$, $0 \leq k_i \leq p_i - 1$, $0 \leq l_i \leq p_i^{a_i - 1} - 1$, and the set $\{c_{ur_1 \dots r_s k_{s+1} \dots k_t l_{s+1} \dots l_t}\}$ is a permutation of the set $\{c_i\}_{i=0}^{m-1}$. To transform X from (2.41) into the form (2.40), we need to get rid of all the terms in (2.41) with $k_i = p_i - 1$. We do this subsequently for $i = s + 1, \dots, t$ using the relation $\zeta_{p_i}^{p_i - 1} = -1 - \zeta_{p_i} - \dots - \zeta_{p_i}^{p_i - 2}$. This takes $t - s$ steps, and in each step, the range of coefficients at most doubles. $\square$

The next result essentially appeared in [50, Theorem 2.3.2]. We state the result below and give it another proof which makes use of our norm bound (2.39).

Result 2.3.8. *Let m be a positive integer. Suppose that $X = \sum_{i=1}^{m-1} c_i \zeta_m^i \in \mathbb{Z}[\zeta_m]$ satisfies $X\bar{X} = n$. Assume that there exists an integer j and a divisor k of m which is divisible by every prime factor of m such that*

$$X \zeta_m^j \in \mathbb{Z}[\zeta_k]. \quad (2.42)$$

Put $d_i = c_{im/k-j}$ for $i = 0, \dots, k - 1$. Then

$$n \leq \min \left\{ \left(\sum_{i=0}^{k-1} |d_i| \right)^2, \left(\frac{k}{\varphi(k)} \sum_{i=0}^{k-1} d_i^2 \right) \right\}, \quad (2.43)$$

Proof. Replacing X by $X \zeta_m^j$, if necessary, we can assume $X \in \mathbb{Z}[\zeta_k]$. Let

$$m = \prod_{i=1}^r p_i^{s_i} \text{ and } k = \prod_{i=1}^r p_i^{t_i}$$

be the prime factorizations of m and k , respectively, where $s_i, t_i \in \mathbb{Z}$ and $1 \leq t_i \leq s_i$ for all i . By Result 2.3.7, the set

$$\mathcal{B} = \left\{ \prod_{i=1}^r \zeta_{p_i}^{l_i} : 0 \leq l_i \leq p_i^{s_i - t_i} - 1 \right\}$$

is an integral basis for $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}(\zeta_k)$. Expressing X as a linear combination of elements in $\mathcal{B}$ over $\mathbb{Q}(\zeta_k)$, we have

$$\begin{aligned} X &= \sum_{\substack{0 \leq x_i \leq p_i^{s_i-t_i}-1 \\ 0 \leq y_i \leq p_i^{t_i}-1}} b_{x_1 \dots x_r y_1 \dots y_r} \prod_{i=1}^r \zeta_{p_i^{s_i}}^{x_i + y_i p_i^{s_i-t_i}} \\ &= \sum_{0 \leq x_i \leq p_i^{s_i-t_i}-1} \left(\sum_{0 \leq y_i \leq p_i^{t_i}-1} b_{x_1 \dots x_r y_1 \dots y_r} \prod_{i=1}^r \zeta_{p_i^{t_i}}^{y_i} \right) \prod_{i=1}^r \zeta_{p_i^{s_i}}^{x_i} \\ &= \sum_{x \in \mathcal{B}} A_x x, \end{aligned}$$

where $x = \prod_{i=1}^r \zeta_{p_i^{s_i}}^{x_i} \in \mathcal{B}$, $A_x = \sum_{0 \leq y_i \leq p_i^{t_i}-1} b_{x_1 \dots x_r y_1 \dots y_r} \prod_{i=1}^r \zeta_{p_i^{t_i}}^{y_i} \in \mathbb{Q}(\zeta_k)$ and the set $\{b_{x_1 \dots x_r y_1 \dots y_r}\}$ is a permutation of the set $\{c_i\}_{i=0}^{m-1}$. As $X \in \mathbb{Q}(\zeta_k)$ and $\mathcal{B}$ is a basis for $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}(\zeta_k)$, we have $A_x = 0$ for any $x \neq 1$. Hence

$$X = A_1 = \sum_{i=0}^{k-1} d_i \zeta_k^i, \quad (2.44)$$

where $d_i = c_{im/k}$. We obtain

$$n = |X|^2 \leq \left(\sum_{i=1}^k |d_i| \right)^2.$$

Lastly, note that $n^{\varphi(k)/2} = N_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(X)$. So the inequality $n \leq k \left(\sum_{i=0}^{k-1} d_i^2 \right) / \varphi(k)$ follows from (2.44) and Lemma 2.3.6. The inequality (2.43) is proved. $\square$

To apply Result 2.3.8, we need to find a divisor k of m which contains all prime factors of m and satisfies $X\zeta_m^j \in \mathbb{Z}[\zeta_k]$ for some $j \in \mathbb{Z}$. Fortunately, the field-descent theory by Schmidt [49, 50] provides exactly what we need.

Result 2.3.9. *If $X \in \mathbb{Z}[\zeta_m]$ satisfies $X\bar{X} = n$, then there exists an integer j and a divisor $F(m, n)$ of m which is divisible by every prime divisor of m such that $X\zeta_m^j \in \mathbb{Z}[\zeta_{F(m, n)}]$.*

The number $F(m, n)$ is defined as follows:

Definition 2.3.10. *Let m, n be positive integers and let $m = \prod_{i=1}^t p_i^{c_i}$ be the prime factorization of m . For each prime divisor q of n , let*

$$\tilde{m}_q = \begin{cases} \prod_{p_i \neq q} p_i & \text{if } m \text{ is odd or } q = 2, \\ 4 \prod_{p_i \neq 2, q} p_i & \text{otherwise.} \end{cases}$$

Let $D(n)$ denote the set of all prime divisors of n . Define

$$F(m, n) = \prod_{i=1}^t p_i^{b_i}$$

to be the minimum multiple of $\prod_{i=1}^t p_i$ such that for every pair (i, q) , $1 \leq i \leq t$, $q \in D(n)$, at least one of the following conditions is satisfied.

- (a) $q = p_i$ and $(p_i, b_i) \neq (2, 1)$,
- (b) $b_i = c_i$,
- (c) $q \neq p_i$ and $q^{\text{ord}_{\bar{m}_q}(q)} \not\equiv 1 \pmod{p_i^{b_i+1}}$.

We obtain an immediate corollary using Result 2.3.8 and Result 2.3.9.

Corollary 2.3.11. *Let m be a positive integer and let $X = \sum_{i=0}^{m-1} c_i \zeta_m^i$, $a_i \in \mathbb{Z}$, be an element of $\mathbb{Z}[\zeta_m]$ such that $X\bar{X} = n$. Then there exists an integer j such that $X\zeta_m^j \in \mathbb{Z}[\zeta_{F(m,n)}]$. Moreover, putting $d_i = c_{im/F(m,n)-j}$ for $0 \leq i \leq F(m, n) - 1$, we have*

$$n \leq \min \left\{ \left(\sum_{i=0}^{F(m,n)-1} |d_i| \right)^2, \left(\frac{F(m, n)}{\varphi(F(m, n))} \sum_{i=0}^{F(m,n)-1} d_i^2 \right) \right\}. \quad (2.45)$$

2.3.3 $\text{BH}(\mathbb{Z}_n, h)$ Matrices

Note that by Corollary 2.2.7, there exist $\text{BH}(\mathbb{Z}_n, h)$ matrices whenever $(h, n)^2 \equiv 0 \pmod{n}$ and $(\nu_2(n), \nu_2(h)) \neq (1, 1)$. We conjecture that these conditions are also necessary for the existence of $\text{BH}(\mathbb{Z}_n, h)$ matrices.

Conjecture 2.3.12. *Let n and h be positive integers. Then there exists a $\text{BH}(\mathbb{Z}_n, h)$ matrix if and only if*

- (i) $\nu_p(h) \geq \lceil \nu_p(n)/2 \rceil$ for every prime divisor p of n , and
- (ii) $\nu_2(h) \geq 2$ if $n \equiv 2 \pmod{4}$.

A special case of Conjecture 2.3.12 is the circulant Hadamard matrix conjecture which was mentioned in the introduction. Unfortunately, we are far from proving Conjecture 2.3.12. In support of it, we prove that $n \leq (h, n)^2$ under certain restrictions on n and h .

Theorem 2.3.13. *Let n and h be positive integers and put $m = \text{lcm}(n, h)$. Suppose that a $\text{BH}(\mathbb{Z}_n, h)$ matrix exists. Furthermore, assume that for any prime divisor p of n , we have*

(i) $h \equiv 0 \pmod{p}$, and

(ii) $q^{\text{ord}_{\tilde{m}_q}(q)} \not\equiv 1 \pmod{p^{\nu_p(h)+1}}$ for any prime divisor $q \neq p$ of n ,

where $\tilde{m}_q$ is defined in Definition 2.3.10. Then

$$n \leq (h, n)^2. \quad (2.46)$$

Proof. Let g be a generator of the group $\mathbb{Z}_n$. By Lemma 2.1.2, there exists an element D in the group ring $\mathbb{Z}[\zeta_h][\mathbb{Z}_n]$ of the form $D = \sum_{i=0}^{n-1} \zeta_h^{a_i} g^i$, $a_i \in \mathbb{Z}$, which satisfies

$$DD^{(-1)} = n. \quad (2.47)$$

Let χ be a character of $\mathbb{Z}_n$ such that $\chi(g) = \zeta_n$. We have $\chi(D) = \sum_{i=0}^{n-1} \zeta_h^{a_i} \zeta_n^i \in \mathbb{Z}[\zeta_m]$. By Result 2.3.9, there exists an integer j such that $\chi(D)\zeta_m^j \in \mathbb{Z}[\zeta_{F(m,n)}]$. Since $\gcd(m/h, m/n) = 1$, there exist integers α and β such that $\alpha m/h + \beta m/n = j$. Replacing D by $D\zeta_h^\alpha g^\beta$, if necessary, we may assume that

$$X = \chi(D\zeta_h^\alpha g^\beta) = \chi(D)\zeta_n^{\alpha n/h + \beta} = \chi(D)\zeta_m^j \in \mathbb{Z}[\zeta_{F(m,n)}].$$

Thus $X \in \mathbb{Z}[\zeta_h]$, as $h \equiv 0 \pmod{F(m,n)}$ by the definition of $F(m,n)$ and by the conditions (i) and (ii). Note that with h in the place of k , the condition (2.42) in Result 2.3.8 is satisfied. To apply the inequality (2.43), we need to find the exponents in

$$X = \sum_{i=0}^{n-1} \zeta_m^{a_i(m/h) + i(m/n)}$$

which are divisible by m/h . These are the ones containing i such that im/n is divisible by m/h , i.e., $i \equiv 0 \pmod{n/(n,h)}$. There are (h, n) such exponents, as $0 \leq i \leq n-1$. Recall that $X \in \mathbb{Z}[\zeta_h]$. When expressing X in the form $\sum_{i=0}^{h-1} d_i \zeta_h^i$, $d_i \in \mathbb{Z}$, we have $d_i \geq 0$ for all i and $\sum_{i=0}^{h-1} d_i = (h, n)$. We obtain, by (2.43),

$$n \leq \left(\sum_{i=0}^{h-1} d_i \right)^2 = (h, n)^2.$$

□

The next result gives us necessary and sufficient conditions for the existence of $\text{BH}(\mathbb{Z}_{p^a}, h)$ matrices.

Theorem 2.3.14. *Let n be a power of a prime p and let h be a positive integer. Then a (circulant) $\text{BH}(\mathbb{Z}_n, h)$ matrix exists if and only if*

$$\nu_p(h) \geq \lceil \nu_p(n)/2 \rceil \text{ and } (n, \nu_p(h)) \neq (2, 1). \quad (2.48)$$

Proof. If (2.48) is satisfied, then a $\text{BH}(\mathbb{Z}_n, h)$ matrix exists by Corollary 2.2.7. Now denote $n = p^a$ and suppose that a $\text{BH}(\mathbb{Z}_{p^a}, h)$ matrix exists. If $p^a = 2$, then it can be verified directly that $\nu_2(h) \geq 2$ as follows. Let H be a $\text{BH}(\mathbb{Z}_2, h)$ matrix with the first row $[\zeta_h^c, \zeta_h^d]$ for some $c, d \in \{0, 1, \dots, h-1\}$. The second row of H is $[\zeta_h^d, \zeta_h^c]$. The equation $HH^* = 2I_2$ is equivalent to $\zeta_h^{c-d} + \zeta_h^{d-c} = 0$, which is possible only when $4 \mid h$.

From now on, suppose that $p^a \neq 2$. Note that the condition (ii) of Theorem 2.3.13 automatically holds in this case, as $n = p^a$ is a prime power. Moreover, the inequality $\nu_p(h) \geq \lceil \nu_p(n)/2 \rceil$ is equivalent to $n \leq (n, h)^2$, which can be obtained by Theorem 2.3.13. Thus, it suffices to prove that the condition (i) of Theorem 2.3.13 is met, that is, $h \equiv 0 \pmod{p}$. Suppose that a $\text{BH}(\mathbb{Z}_{p^a}, h)$ exists and that $h \not\equiv 0 \pmod{p}$. Write $G = \mathbb{Z}_{p^a}$ and let g be a generator of G . By Lemma 2.1.2, there is an element D in the group ring $\mathbb{Z}[\zeta_h][G]$ of the form $D = \sum_{i=0}^{p^a-1} \zeta_h^{a_i} g^i$, $a_i \in \mathbb{Z}$, which satisfies

$$|\chi(D)|^2 = p^a \quad (2.49)$$

for all $\chi \in \hat{G}$. Let χ be the character of G with $\chi(g) = \zeta_{p^a}$. By Result 1.4.5, we have $\chi(D) = \zeta_{p^a h}^k Y$ or $\chi(D) = \zeta_{p^a h}^k \Theta Y$ for some integer k , where $Y \in \mathbb{Z}[\zeta_h]$ and Θ is defined in Result 1.4.5 with the property

$$|\Theta|^2 = p \text{ and } |Y|^2 = p^{a-1}.$$

Replacing D by $\zeta_h^c g^d D$ with suitable integers c, d , if necessary, we can assume $k = 0$. Hence

$$\chi(D) \in \mathbb{Z}[\zeta_h] \text{ or } \chi(D) = \Theta Y. \quad (2.50)$$

We first assume $p = 2$. In this case $a \geq 2$ as $p^a \neq 2$. Moreover, h is odd and we have $\chi(D) \in \mathbb{Z}[\zeta_{4h}]$ by (2.50) (note that $\Theta = 1 - \zeta_4$ in this case). Write

$$D = \sum_{i=0}^{2^{a-2}-1} g^i \sum_{j=0}^3 \zeta_h^{a_{i,j}} g^{2^{a-2}j}, \quad a_{i,j} \in \mathbb{Z}.$$

We have

$$\chi(D) = \sum_{i=0}^{2^{a-2}-1} \zeta_{2^a}^i \sum_{j=0}^3 \zeta_h^{a_{i,j}} \zeta_4^j.$$

As $\chi(D) \in \mathbb{Z}[\zeta_{4h}]$ and $\{1, \zeta_{2^a}, \dots, \zeta_{2^a}^{2^a-2-1}\}$ is linearly independent over $\mathbb{Q}(\zeta_{4h})$, we conclude

$$\chi(D) = \sum_{j=0}^3 \zeta_h^{a_{0,j}} \zeta_4^j = A + B\zeta_4,$$

where $A = \zeta_h^{a_{0,0}} - \zeta_h^{a_{0,2}}$ and $B = \zeta_h^{a_{0,1}} - \zeta_h^{a_{0,3}}$. We conclude

$$2^a = |\chi(D)|^2 = (A + B\zeta_4)(\bar{A} - \bar{B}\zeta_4) = A\bar{A} + B\bar{B} + (-A\bar{B} + B\bar{A})\zeta_4.$$

As $\{1, \zeta_4\}$ is linearly independent over $\mathbb{Q}(\zeta_h)$, this implies $-A\bar{B} + B\bar{A} = 0$ and $A\bar{A} + B\bar{B} = 2^a$. As h is odd, we have $|A|, |B| < 2$ and thus $A\bar{A} + B\bar{B} < 8$. Hence $a = 2$ and $A\bar{A} + B\bar{B} = |\chi(D)|^2 = 4$. A quick computation shows that this implies $\eta + \bar{\eta} + \gamma + \bar{\gamma} = 0$, where $\eta = \zeta_h^{a_{0,0}-a_{0,2}}$ and $\gamma = \zeta_h^{a_{0,1}-a_{0,3}}$. Hence $\text{Re}(\eta) = -\text{Re}(\gamma)$, where $\text{Re}(z)$ denotes the real part of $z \in \mathbb{C}$. Write $\eta = \zeta_h^c$ and $\gamma = \zeta_h^d$ with $c, d \in \mathbb{Z}$. We have $\text{Re}(\eta) = \cos(2\pi ic/h)$ and $\text{Re}(\gamma) = \cos(2\pi id/h)$ and thus $\text{Re}(\eta) = -\text{Re}(\gamma)$ implies $2\pi d/h = \pm 2\pi c/h + k\pi$ where k is an odd integer. This is only possible if h is even. The proof is complete for $p = 2$.

Now assume that p is odd. We rewrite D in the form

$$D = \sum_{i=0}^{p^a-1-1} \sum_{j=0}^{p-1} \zeta_h^{a_{i,j}} g^{i+jp^{a-1}},$$

where the $a_{i,j}$'s are integers with $0 \leq a_{i,j} \leq p-1$. Note that

$$\chi(D) = \sum_{i=0}^{p^a-1-1} \zeta_{p^a}^i \sum_{j=0}^{p-1} \zeta_h^{a_{i,j}} \zeta_p^j. \quad (2.51)$$

As $\{1, \zeta_{p^a}, \dots, \zeta_{p^a}^{p^a-1-1}\}$ is linearly independent over $\mathbb{Q}(\zeta_{ph})$ and $\chi(D) \in \mathbb{Z}[\zeta_{ph}]$ by (2.50) (note that $\Theta \in \mathbb{Z}[\zeta_{ph}]$ in this case), we conclude that $\sum_{j=0}^{p-1} \zeta_h^{a_{i,j}} \zeta_p^j = 0$ for all $i > 0$ and thus

$$\chi(D) = \sum_{j=0}^{p-1} \zeta_h^{b_j} \zeta_p^j, \quad (2.52)$$

where $b_j = a_{0,j}$. This implies $|\chi(D)| < p$ and thus $a = 1$ by (2.49). In particular, g has order p and we have

$$D = \sum_{j=0}^{p-1} \zeta_h^{b_j} g^j. \quad (2.53)$$

According to (2.50), it suffices to consider the following two cases.

Case 1. $\chi(D) = \Theta Y$. Recall that $\Theta = \sum_{i=0}^{p-2} \eta^{-i} \zeta_p^{ti}$ and note that

$$\Theta \equiv \sum_{i=0}^{p-2} \eta^{-i} \equiv 0 \pmod{1 - \zeta_p},$$

since $\eta \neq 1$ and the order of η divides $p - 1$. We conclude

$$\sum_{i=0}^{p-1} \zeta_h^{b_i} \equiv \sum_{i=0}^{p-1} \zeta_h^{b_i} \zeta_p^i \equiv \chi(D) \equiv \Theta Y \equiv 0 \pmod{1 - \zeta_p}.$$

By Lemma 1.4.4, this implies

$$\sum_{j=0}^{p-1} \zeta_h^{b_j} \equiv 0 \pmod{p}. \quad (2.54)$$

However, for the trivial character χ_0 of G , we have $\chi_0(D) = \sum_{j=0}^{p-1} \zeta_h^{b_j}$ by (2.53) and $|\chi_0(D)|^2 = p$ by (2.49). But (2.54) implies $|\chi_0(D)|^2 \equiv 0 \pmod{p^2}$, a contradiction.

Case 2. $\chi(D) \in \mathbb{Z}[\zeta_h]$. By (2.52), we have $\chi(D) = \sum_{j=0}^{p-2} (\zeta_h^{b_j} - \zeta_h^{b_{p-1}}) \zeta_p^j$ and since $\chi(D) \in \mathbb{Z}[\zeta_h]$ and $\{1, \zeta_p, \dots, \zeta_p^{p-2}\}$ is linearly independent over $\mathbb{Q}(\zeta_h)$, we conclude $b_1 = \dots = b_{p-1}$ and $\chi(D) = \zeta_h^{b_0} - \zeta_h^{b_{p-1}}$. As $|\chi(D)|^2 = p$ and p is odd, this implies $p = 3$. Replacing D by $\zeta_h^{-b_0} D$, if necessary, we can assume $\chi(D) = 1 - \zeta_h^u$ for some integer u . Note that $\zeta_h^u \neq 1$. We have $3 = |\chi(D)|^2 = 2 - \zeta_h^u - \zeta_h^{-u}$ and thus $\zeta_h^u + \zeta_h^{2u} + 1 = 0$, which implies $\zeta_h^{3u} = 1$. As $\zeta_h^u \neq 1$, we conclude $h \equiv 0 \pmod{3}$, contradicting the assumption that $h \not\equiv 0 \pmod{p}$. □

We note that a combination of Corollary 2.2.7 and Theorem 2.3.14 rule out 1761 cases in 5071 open cases for the existence of $\text{BH}(\mathbb{Z}_n, h)$ matrices in which $1 \leq n, h \leq 100$.

For the next result, we recall the self-conjugacy concept in Definition 1.4.1. The following result works for any $\text{BH}(G, h)$ matrix, where G is a finite abelian group. The result on $\text{BH}(\mathbb{Z}_n, h)$ matrices will be stated as a corollary.

Theorem 2.3.15. *Let G be a finite abelian group and let h be a positive integer such that a $\text{BH}(G, h)$ matrix exists. Put $n = |G|$ and $m = \text{lcm}(n, h)$. Assume that p is a prime divisor of n which is self-conjugate modulo m . Moreover, assume that the Sylow p -subgroup of G is cyclic. Then*

$$h \equiv 0 \pmod{p}.$$

Proof. Assume that $h \not\equiv 0 \pmod{p}$. By Lemma 2.1.2, there exists an element D in the group ring $\mathbb{Z}[\zeta_h][G]$ of the form $D = \sum_{g \in G} a_g g$, each a_g an h th root of unity, which satisfies $DD^{(-1)} = n$. For any character χ of G , we have

$$|\chi(D)|^2 = n, \quad \chi(D) \in \mathbb{Z}[\zeta_m]. \quad (2.55)$$

Applying χ_0 to (2.55) and putting $Y = \chi_0(D) \in \mathbb{Z}[\zeta_h]$, we obtain $|Y|^2 = n$. Note that p is self-conjugate modulo m and $m \equiv 0 \pmod{h}$, so p is also self-conjugate modulo h . By Result 1.4.3 for $|Y|^2 = n$ and by the condition $h \not\equiv 0 \pmod{p}$, we obtain $\nu_p(n) = 2t$ for some $t \in \mathbb{Z}^+$. This implies $\nu_p(m) = 2t$, as $m = \text{lcm}(n, h)$ and $h \not\equiv 0 \pmod{p}$. Moreover, since $|\chi(D)|^2 = n$ and $\chi(D) \in \mathbb{Z}[\zeta_m]$, Result 1.4.3 implies $\chi(D) \equiv 0 \pmod{p^t}$ for any character χ of G . By Result 1.3.10, we obtain

$$D = p^t X + PY, \quad (2.56)$$

where P is the cyclic subgroup of G of order p and $X, Y \in \mathbb{Z}[\zeta_h][G]$. As $kP = P$ for any $k \in P$, we can assume that no two elements in the support of Y are contained in the same coset of P in G . Moreover, the equation (2.56) implies that for any two elements $g, k \in G$ which belong to the same coset of P , we have

$$a_g \equiv a_k \pmod{p^t}. \quad (2.57)$$

Suppose that $a_g = a_k$ for any two elements g, k in the same coset of P . We have $D = PZ$ for some $Z \in \mathbb{Z}[\zeta_h][G]$. Let τ be the character of G which is nontrivial on P . We have $\tau(D) = 0$, as $\tau(P) = 0$, contradicting (2.55).

Therefore, there exists two elements $g, k \in G$ which belong to the same coset of P such that $a_g \neq a_k$. Note that both a_g and a_k are h th roots of unity. The congruence (2.57) happens only when $t = 1$, $p = 2$ and $a_k = -a_g$. Since both a_k and a_g are h th roots of unity, the condition $a_k = -a_g$ implies $h \equiv 0 \pmod{2}$, so $h \equiv 0 \pmod{p}$, a contradiction. □

Let n be a positive integer and let p be a prime divisor of n . In the group $\mathbb{Z}_n$, any Sylow p -subgroup is cyclic. The following corollary is an immediate consequence of Theorem 2.3.15.

Corollary 2.3.16. *Let n and h be positive integers and put $m = \text{lcm}(n, h)$. If a $\text{BH}(\mathbb{Z}_n, h)$ matrix exists, then any prime divisor of n which is self-conjugate modulo m is also a divisor of h . In particular if $\gcd(n, h) = 1$, then no prime divisor of n is self-conjugate modulo nh .*

In the next result, we assume the existence of a $\text{BH}(\mathbb{Z}_n, h)$ matrix and look more closely at the part of n which is self-conjugate modulo $m = \text{lcm}(n, h)$.

Theorem 2.3.17. *Let n and h be positive integers and put $m = \text{lcm}(n, h)$. Let u be the largest divisor of n which is self-conjugate modulo m . Write $u = w^2 k$, where k is the square-free part of u . Let t and r be the numbers of prime divisors of h and k , respectively. Suppose that a $\text{BH}(\mathbb{Z}_n, h)$ matrix exists. We obtain the following.*

(a) *If $k \not\equiv 0 \pmod{2}$, then*

$$w \leq 2^{t-r-1+\delta_{rt}}(h, u) \sqrt{\frac{k}{\varphi(k)}}. \quad (2.58)$$

(b) *If $k \equiv 0 \pmod{2}$, then*

$$w \leq 2^{t-r-1}(h, u) \sqrt{\frac{2k}{\varphi(k)}}. \quad (2.59)$$

Proof. Let g be a generator of $\mathbb{Z}_n$. By Lemma 2.1.2, there exists an element D in the group ring $\mathbb{Z}[\zeta_h][\mathbb{Z}_n]$ of the form $D = \sum_{i=0}^{n-1} \zeta_h^{a_i} g^i$, $a_i \in \mathbb{Z}$, which satisfies $DD^{(-1)} = n$. Hence for any character χ of $\mathbb{Z}_n$, we have

$$|\chi(D)|^2 = n, \quad \chi(D) \in \mathbb{Z}[\zeta_m]. \quad (2.60)$$

Put $v = n/u$. Note that $(u, v) = 1$, as u is the largest divisor of n which is self-conjugate modulo m . Let τ be a character of $\mathbb{Z}_n$ such that $\tau(g^v) = \zeta_u$. The proof of the theorem is divided into following claims.

Claim 1. *Replacing D by Dy with suitable $y \in G$, we can assume that*

$$\tau(D \cap \mathbb{Z}_u) \neq 0. \quad (2.61)$$

Let $R = \{1, g, \dots, g^{v-1}\}$ be a complete set of coset representatives of $\mathbb{Z}_u$ in $\mathbb{Z}_n$. If $\tau(D \cap x\mathbb{Z}_u) = 0$ for all $x \in R$, then $\tau(D) = \sum_{x \in R} \tau(D \cap x\mathbb{Z}_u) = 0$, contradicting (2.60). Thus, there exists $x \in R$ such that $\tau(D \cap x\mathbb{Z}_u) \neq 0$. Hence $\tau(Dx^{-1} \cap \mathbb{Z}_u) = \tau(x^{-1})\tau(D \cap x\mathbb{Z}_u) \neq 0$. Replacing D by Dx^{-1} , we can assume that $\tau(D \cap \mathbb{Z}_u) \neq 0$, proving (2.61).

Claim 2. *Write $D \cap \mathbb{Z}_u = \sum_{i=0}^{u-1} \zeta_h^{a_{vi}} g^{vi} = \sum_{i=0}^{u-1} \zeta_h^{b_i} g^{vi}$ and write $k = \prod_{i=1}^r p_i$. Define Θ_i as in Result 1.4.3. Then*

$$X = \sum_{i=0}^{u-1} \zeta_h^{b_i} \zeta_u^i \equiv 0 \pmod{w \prod_{i=1}^r \Theta_i}. \quad (2.62)$$

By Result 1.4.3, we have $\chi(D) \equiv 0 \pmod{w \prod_{i=1}^r \Theta_i}$ for any character χ of $\mathbb{Z}_n$. On the other hand, by Result 1.3.7, we have

$$\sum_{\chi \in \mathbb{Z}_u^\perp} \chi \tau(D) = |\mathbb{Z}_u^\perp| \tau(D \cap \mathbb{Z}_u) = v \left(\sum_{i=0}^{u-1} \zeta_h^{b_i} \zeta_u^i \right), \quad (2.63)$$

Since $(u, v) = 1$ and each term on the left-hand side of (2.63) is divisible by $w \prod_{i=1}^r \Theta_i$, we obtain the congruence (2.62).

Claim 3. Put $l = \text{lcm}(h, u)$, $d = \text{gcd}(h, u)$ and write $X = \sum_{i=0}^{u-1} \zeta_h^{b_i} \zeta_u^i$ in the form $X = \sum_{i=0}^{l-1} c_i \zeta_l^i$, $c_i \in \mathbb{Z}^+$. Then

$$0 \leq c_i \leq d \text{ for any } i = 0, \dots, l-1. \quad (2.64)$$

For a fixed $0 \leq i \leq l-1$, let a and b be fixed integers such that $(u/d)a + (h/d)b = i$. Note that a and b exist as $(u/d, h/d) = 1$. All the solutions $j \pmod{h}$ and $f \pmod{u}$ to $\zeta_l^i = \zeta_h^j \zeta_u^f$ are

$$j = a + \lambda \frac{h}{d}, \quad f = b - \lambda \frac{u}{d}, \quad \lambda \in \{0, \dots, d-1\}.$$

Thus, there are at most d solutions to $\zeta_l^i = \zeta_h^{b_z} \zeta_u^z$, $0 \leq z \leq u-1$. The claim is proved.

Claim 4. If $k \not\equiv 0 \pmod{2}$, then

$$w \leq 2^{t-r-1+\delta_{tr}}(h, u) \sqrt{\frac{k}{\varphi(k)}}.$$

First, note that $X = \tau(D \cap \mathbb{Z}_u) \neq 0$ by Claim 1. By Corollary 2.3.16, any prime divisor of u divides h , so the numbers of prime divisors of $l = \text{lcm}(h, u)$ and h are the same, both equal to t . By Result 2.3.7 and (2.64), we can express X as a linear combination of the basis elements in $\mathcal{B}_{l,k} \subset \mathbb{Q}(\zeta_l)$ over $\mathbb{Q}(\zeta_k)$ as follows.

$$X = \sum_{x \in \mathcal{B}_{l,k}} x \left(\sum_{j=0}^{k-1} c_{xj} \zeta_k^j \right),$$

where

$$|c_{xj}| \leq 2^{t-r-1+\delta_{tr}} d \text{ for all } x \in \mathcal{B}_{l,k} \text{ and } 0 \leq j \leq k-1. \quad (2.65)$$

Note that $X \equiv 0 \pmod{w \prod_{i=1}^r \Theta_i}$ by (2.62). Moreover note that $w \prod_{i=1}^r \Theta_i \in \mathbb{Q}(\zeta_k)$, as $\Theta_i \in \mathbb{Q}(\zeta_{p_i}) \subset \mathbb{Q}(\zeta_k)$ for all i (by the definition of Θ_i for odd p_i). Hence $\sum_{j=0}^{k-1} c_{xj} \zeta_k^j \equiv 0 \pmod{w \prod_{i=1}^r \Theta_i}$ for all $x \in \mathcal{B}_{l,k}$. As $X \neq 0$, there exists $x \in \mathcal{B}_{l,k}$ so that

$$Y = \sum_{j=0}^{k-1} c_{xj} \zeta_k^j \neq 0 \text{ and } Y \equiv 0 \pmod{w \prod_{i=1}^r \Theta_i}. \quad (2.66)$$

Note that each Θ_i has absolute value $\sqrt{p_i}$. Using (2.65), (2.66) and the inequality (2.39), we obtain

$$\begin{aligned} (w^2 k)^{\varphi(k)/2} = \left| N_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(w \prod_{i=1}^r \Theta_i) \right| &\leq \left| N_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(Y) \right| \leq \left(\frac{k}{\varphi(k)} \sum_{j=0}^{k-1} c_{xj}^2 \right)^{\varphi(k)/2} \\ &\leq \left(4^{t-r-1+\delta_{tr}} d^2 \frac{k^2}{\varphi(k)} \right)^{\varphi(k)/2}, \end{aligned}$$

proving Claim 4.

Claim 5. *If $k \equiv 0 \pmod{2}$, then*

$$w \leq 2^{t-r-1}(h, u) \sqrt{\frac{2k}{\varphi(k)}}.$$

We assume that $p_r = 2$. Similar to the proof of Claim 4, we express X as a linear combination of the basis elements in $\mathcal{B}_{l,k/2} \subset \mathbb{Q}(\zeta_l)$ over $\mathbb{Q}(\zeta_{k/2})$ as follows.

$$X = \sum_{x \in \mathcal{B}_{l,k/2}} x \left(\sum_{j=0}^{k/2-1} d_{xj} \zeta_{k/2}^j \right), \quad |d_{xj}| \leq 2^{t-r} d \text{ for all } x, j. \quad (2.67)$$

Note that $w \prod_{i=1}^{r-1} \Theta_i \in \mathbb{Q}(\zeta_{k/2})$ and divides X , so it divides $\sum_{j=0}^{k/2-1} d_{xj} \zeta_{k/2}^j$ for any $x \in \mathcal{B}_{l,k/2}$. As $X \neq 0$, there exists $x \in \mathcal{B}_{l,k/2}$ such that

$$Z = \sum_{j=0}^{k/2-1} d_{xj} \zeta_{k/2}^j \neq 0 \text{ and } Z \equiv 0 \pmod{w \prod_{i=1}^{r-1} \Theta_i}. \quad (2.68)$$

Using (2.67), (2.68) and the inequality (2.39), we obtain

$$\begin{aligned} (w^2 k/2)^{\varphi(k/2)/2} &= \left| N_{\mathbb{Q}(\zeta_{k/2})/\mathbb{Q}}(Z) \right| \leq \left(\frac{k/2}{\varphi(k/2)} \sum_{j=0}^{k/2-1} d_{xj}^2 \right)^{\varphi(k/2)/2} \\ &\leq \left(4^{t-r} d^2 \frac{k^2}{4\varphi(k)} \right)^{\varphi(k/2)/2}, \end{aligned}$$

proving Claim 5. □

Corollary 2.3.18. *Let n and b be positive integers and let p be a prime. Suppose that a $\text{BH}(\mathbb{Z}_n, p^b)$ matrix exists. Then $n = p^c m$ for some positive integers c and m with $\gcd(p, m) = 1$. Moreover, assume that p is self-conjugate modulo m . Then*

$$b \geq \lfloor c/2 \rfloor. \quad (2.69)$$

Proof. The claim that $n = p^c m$ follows directly from Result 2.3.3. Moreover note that p is the only prime divisor of n which is self conjugate modulo $\text{lcm}(n, p^b)$ by Corollary 2.3.16. In the notation of Theorem 2.3.17, we have $u = p^c$, $w = p^{\lfloor c/2 \rfloor}$, $t = 1$, $k \in \{1, p\}$ and $r \in \{0, 1\}$.

If $k \equiv 0 \pmod{2}$, then $k = p = 2$, $r = 1$ and the inequality (2.59) implies

$$p^{\lfloor c/2 \rfloor} \leq (p^b, p^c) \leq p^b.$$

If $k \not\equiv 0 \pmod{2}$, then $p \geq 3$ and the inequality (2.58) implies

$$p^{\lfloor c/2 \rfloor} \leq 2^{-r+\delta_{r1}}(p^b, p^c) \sqrt{\frac{k}{\varphi(k)}} \leq (p^b, p^c) \sqrt{\frac{p}{p-1}} < p^{b+1}.$$

The first and the third inequalities are clear. The second inequality follows from $\delta_{r1} = r$, as $r \in \{0, 1\}$. $\square$

Remark 2.3.19. We consider the impact of Theorem 2.3.13, Corollary 2.3.16 and Theorem 2.3.17 on the existence of $\text{BH}(\mathbb{Z}_n, h)$ matrices with $1 \leq n, h \leq 100$. Theorem 2.3.13 confirms the non-existence of 178 cases. Corollary 2.3.16 confirms the nonexistence of 2946 cases. Lastly, Theorem 2.3.17 confirms the nonexistence of 723 cases.

2.3.4 $\text{BH}(G, 2p^b)$ Matrices

Let G be a finite abelian group, let p be an odd prime and let b be a positive integer. The main result in this section relies on the following result by Leung and Schmidt, see [35, Theorem 22 and Theorem 23] .

Result 2.3.20. *Let p be an odd prime and let a be a positive integer. Let m be a nonsquare integer and let $q_1, \dots, q_s$ be all distinct prime divisors of m . Put $f = \gcd(\text{ord}_p(q_1), \dots, \text{ord}_p(q_s))$. Suppose that $X \in \mathbb{Z}[\zeta_{p^a}]$ satisfies $|X|^2 = m$. Then the following hold.*

- (i) f is an odd integer.
- (ii) Either $f \leq m$ or $p \leq (f^2 - m)/(f - m)$.
- (iii) $p \leq m^2 + m + 1$.

Theorem 2.3.21. *Let b be a positive integer, let p be an odd prime and let G be an abelian group. Write $|G| = p^c m$, where $c \geq 0$ and $\gcd(p, m) = 1$. Suppose that m is not a square. Let $q_1, \dots, q_s$ be all distinct prime divisors of m . Put $f = \gcd(\text{ord}_p(q_1), \dots, \text{ord}_p(q_s))$. If either a $\text{BH}(G, p^b)$ matrix or a $\text{BH}(G, 2p^b)$ matrix exists, then the following hold.*

(i) f is odd.

(ii) Either $f \leq m$ or $p \leq (f^2 - m)/(f - m)$.

(iii) $p \leq m^2 + m + 1$.

Proof. As $\text{BH}(G, p^b) \subset \text{BH}(G, 2p^b)$, it suffices to assume that a $\text{BH}(G, 2p^b)$ matrix exists. By Lemma 2.1.2, there exists an element D in the group ring $\mathbb{Z}[\zeta_{2p^b}][G]$ of the form $D = \sum_{g \in G} \zeta_{2p^b}^{a_g} g$, each a_g an integer, which satisfies

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

Put $X = \chi_0(D) = \sum_{g \in G} \zeta_{2p^b}^{a_g}$. We obtain

$$X\bar{X} = p^c m, \quad X \in \mathbb{Z}[\zeta_{2p^b}] = \mathbb{Z}[\zeta_{p^b}].$$

In the ring $\mathbb{Z}[\zeta_{p^b}]$, we have $p\mathbb{Z}[\zeta_{p^b}] = (1 - \zeta_{p^b})^{\varphi(p^b)}$ and $(1 - \zeta_{p^b})$ is the only prime ideal above p . Thus $(1 - \zeta_{p^b})^{\varphi(p^b)c/2}$ divides (X) as ideals of $\mathbb{Z}[\zeta_{p^b}]$. Putting $Y = X(1 - \zeta_{p^b})^{-\varphi(p^b)c/2} \in \mathbb{Z}[\zeta_{p^b}]$, we obtain

$$Y\bar{Y} = m, \quad Y \in \mathbb{Z}[\zeta_{p^b}].$$

The conclusion follows directly from Result 2.3.20. $\square$

Corollary 2.3.22. *If G is an abelian group with $|G| = 2p^c$ for some non-negative integer c and odd prime p , then there is no $\text{BH}(G, 2p^b)$ matrix.*

Proof. Assume the contrary. Using Theorem 2.3.21 part (iii) for $m = 2$, we obtain $p \leq 7$. The case $p = 3$ or $p = 5$ cannot satisfy the condition $f = \text{ord}_p(2)$ is odd. Therefore, the only possible value for p is $p = 7$. The case $p = 7$ was also ruled out by Leung and Schmidt [35, Corollary 43a]. $\square$

We note that Theorem 2.3.21 confirms the nonexistence of 2361 $\text{BH}(\mathbb{Z}_n, h)$ matrices in which $1 \leq n, h \leq 100$.

Remark 2.3.23. As discussed in Remark 2.3.5, there are 5071 open cases for the existence of a $\text{BH}(\mathbb{Z}_n, h)$ matrix in which $1 \leq n, h \leq 100$. Corollary 2.2.7 and Theorem 2.3.14 settle the existence problem for 1761 of these cases, so there are 3310 cases left. Theorem 2.3.13, Corollary 2.3.16, Theorem 2.3.17 and Theorem 2.3.21 confirm the nonexistence of 623 cases in these 3310 cases. There are 2687 open cases left. This full list of open cases is provided in [23].

2.4 Application to Perfect Multiphase Arrays

A sequence $\{a_0, \dots, a_{n-1}\}$ is called a **perfect h -phase sequence** of length n if each a_i is a complex h th root of unity and

$$\sum_{i=0}^{n-1} a_i \bar{a}_{i+j} = 0 \text{ whenever } j \neq 0,$$

where the indices are taken modulo n . Such a sequence is equivalent to a $\text{BH}(\mathbb{Z}_n, h)$ matrix whose first row is $(a_0, \dots, a_{n-1})$. More generally, a multi-dimensional array $A = (a_{i_1, \dots, i_k})$ of size $n_1 \times \dots \times n_k$ is called a **perfect h -phase array** if its entries are complex h th roots of unity and

$$\sum_{0 \leq i_j \leq n_j - 1 \forall j} a_{i_1, \dots, i_k} \bar{a}_{i_1 + s_1, \dots, i_k + s_k} = 0$$

whenever $(s_1, \dots, s_k) \neq (0, \dots, 0)$, where each index i_j is taken modulo n_j , $1 \leq j \leq k$. The values

$$R_{s_1, \dots, s_k} = \sum_{i_1, \dots, i_k} a_{i_1, \dots, i_k} \bar{a}_{i_1 + s_1, \dots, i_k + s_k}$$

are called **autocorrelations** of the array A . In Lemma 2.4.2 below, we show that such an array is equivalent to a $\text{BH}(\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}, h)$ matrix.

Perfect sequences and perfect arrays have a wide range of applications in communication systems and radar systems, see [8, 25, 27] for example. In this section, we discover a connection between perfect arrays and group-invariant Butson Hadamard matrices. Using this connection and our constructions on group-invariant Butson Hadamard matrices, we find new families of perfect arrays. The following table gives parameters of known perfect arrays [7].

Author	Array size	Alphabet size (value of h)
Jedwab, Mitchell	$2^n \times 2^n$	2
Kopilovich	$(3 \times 2^{n+1}) \times (3 \times 2^{n+1})$ $(3 \times 2^n) \times (3 \times 2^{n+2})$	2
Wild	$2^n \times 2^{n+2}$	2
Blake, Hall, Tirkel	$n \times n$	n if n is odd, $2n$ if n is even
Blake, Hall, Tirkel	$n \times n^{2k+1}$	n^{k+1} if n is odd, $\text{lcm}(2n, n^{k+1})$ if n is even
Blake, Hall, Tirkel	$n \times n^2$	n if n is odd, $2n$ if n is even
Blake, Hall, Tirkel	$n^{2k+1} \times n^{2k+1}$	n^{k+1}
Blake, Hall, Tirkel	$n^2 \times n^2$	n

To prepare for the main results of this section, we need the following lemmas.

Lemma 2.4.1. *Let h_1 and h_2 be positive integers and put $h = \text{lcm}(h_1, h_2)$. Let G_1 and G_2 be finite abelian groups. Assume that H_1 is a $\text{BH}(G_1, h_1)$ matrix and H_2 is a $\text{BH}(G_2, h_2)$ matrix. Then the Kronecker product $H = H_1 \otimes H_2$ is a $\text{BH}(G_1 \times G_2, h)$ matrix.*

Proof. Assume that $H_1 = (h_{x_1, y_1})_{x_1, y_1 \in G_1}$ and $H_2 = (k_{x_2, y_2})_{x_2, y_2 \in G_2}$. The elements of the matrix $H = H_1 \otimes H_2$ are indexed by $G_1 \times G_2$ in which the $((x_1, x_2), (y_1, y_2))$ th element is $H_{(x_1, x_2), (y_1, y_2)} = h_{x_1, y_1} k_{x_2, y_2}$. Let (a_1, a_2) be any element in $G_1 \times G_2$. We have

$$\begin{aligned}
H_{(a_1+x_1, a_2+x_2), (a_1+y_1, a_2+y_2)} &= h_{a_1+x_1, a_1+y_1} k_{a_2+x_2, a_2+y_2} \\
&= h_{x_1, y_1} k_{x_2, y_2} \\
&= H_{(x_1, x_2), (y_1, y_2)},
\end{aligned}$$

proving that H is $G_1 \times G_2$ -invariant.

On the other hand, each entry of H is a product of a (h_1) th root of unity and a (h_2) th root of unity, so it is a h th root of unity. It remains to verify that $HH^* = |H|I_{|H|}$, or equivalently, any two distinct rows (a_1, a_2) and (b_1, b_2) of H are orthogonal. The inner product of these two rows is

$$\begin{aligned}
\sum_{x_1 \in G_1, x_2 \in G_2} H_{(a_1, a_2), (x_1, x_2)} \overline{H}_{(b_1, b_2), (x_1, x_2)} &= \sum_{x_1 \in G_1, x_2 \in G_2} h_{a_1, x_1} \overline{h}_{b_1, x_1} k_{a_2, x_2} \overline{k}_{b_2, x_2} \\
&= \left(\sum_{x_1 \in G_1} h_{a_1, x_1} \overline{h}_{b_1, x_1} \right) \left(\sum_{x_2 \in G_2} k_{a_2, x_2} \overline{k}_{b_2, x_2} \right) \\
&= 0,
\end{aligned}$$

where the last equality holds as $(a_1, b_1) \neq (a_2, b_2)$ and H_1 is a $\text{BH}(G_1, h_1)$ matrix and H_2 is a $\text{BH}(G_2, h_2)$ matrix. $\square$

Lemma 2.4.2. *Let $k, h, n_1, \dots, n_k$ be positive integers. Then a $\text{BH}(\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}, h)$ matrix exists if and only if a perfect h -phase array of size $n_1 \times \dots \times n_k$ exists.*

Proof. Put $G = \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ and suppose that a $\text{BH}(G, h)$ matrix exists. For each $1 \leq i \leq k$, let g_i be a generator of $\mathbb{Z}_{n_i}$. By Lemma 2.1.2, there exists an element D in the group ring $\mathbb{Z}[\zeta_h][G]$ such that all its coefficients are complex h th roots of unity and $DD^{(-1)} = n_1 \dots n_k$. Define

$$I = \{(i_1, \dots, i_k) : 0 \leq i_j \leq n_j - 1 \text{ for } j = 1, \dots, k\}.$$

Write

$$D = \sum_{(i_1, \dots, i_k) \in I} a_{i_1, \dots, i_k} g_1^{i_1} \dots g_k^{i_k},$$

where each $a_{i_1, \dots, i_k}$ is a complex h th root of unity. We have

$$DD^{(-1)} = \sum_{(s_1, \dots, s_k) \in I} \left(\sum_{(i_1, \dots, i_k) \in I} a_{i_1+s_1, \dots, i_k+s_k} \bar{a}_{i_1, \dots, i_k} \right) g_1^{s_1} \dots g_k^{s_k},$$

As $DD^{(-1)} = n_1 \dots n_k$, we obtain

$$\sum_{(i_1, \dots, i_k) \in I} a_{i_1+s_1, \dots, i_k+s_k} \bar{a}_{i_1, \dots, i_k} = \begin{cases} n_1 \dots n_k & \text{if } s_1 = \dots = s_k = 0, \\ 0 & \text{otherwise.} \end{cases} \quad (2.70)$$

Define the array A of size $n_1 \times \dots \times n_k$ by

$$A = (a_{i_1, \dots, i_k}), \quad 0 \leq i_j \leq n_j - 1 \text{ for all } j.$$

The equation (2.70) implies that A is perfect. Conversely, it is straightforward to verify that the existence of a perfect array A implies the existence of a group ring element $D \in \mathbb{Z}[\zeta_h][G]$ whose coefficients are complex h th roots of unity such that $DD^{(-1)} = |G|$, which implies a $\text{BH}(G, h)$ matrix by Lemma 2.1.2. $\square$

Theorem 2.4.3. *Suppose that $k, h, n_1, \dots, n_k$ are positive integers such that*

$$(h, n_i)^2 \equiv 0 \pmod{n_i} \text{ and } (\nu_2(n_i), \nu_2(h)) \neq (1, 1) \text{ for } i = 1, \dots, k. \quad (*)$$

Then a perfect h -phase array of size $n_1 \times \dots \times n_k$ exists.

Proof. By Corollary 2.2.7, the condition $(*)$ imply that $\text{BH}(\mathbb{Z}_{n_i}, h)$ matrices exist for $i = 1, \dots, k$. By Lemma 2.4.1, a $\text{BH}(\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}, h)$ matrix exists. The desired array is constructed as in Lemma 2.4.2. $\square$

Theorem 2.4.4. *Let a, d, r be positive integers and let b be an integer with $0 \leq b \leq r-1$. Let h be a positive integer and assume that $p_1, \dots, p_e$ are all prime divisors of h . If p^d can be written as*

$$p^d = \sum_{i=1}^e p_i a_i, \quad (2.71)$$

where $a_i \in \mathbb{N}$ for all i , then a perfect h -phase array of size $p^{a+1} \times \dots \times p^{a+1} \times p^a \times \dots \times p^a$ exists, where there are $2db$ terms p^{a+1} and $2d(r-b)$ terms p^a in the size of the array.

Proof. By [31, Main Theorem], the condition (2.71) implies that there are h th roots of unity $\eta_0, \dots, \eta_{p^d-1}$ such that $\sum_{i=0}^{p^d-1} \eta_i = 0$. By Theorem 2.2.10, there exists a $\text{BH}(R \times R, h)$ matrix, where $R = \mathbb{Z}_{p^{a+1}}^{db} \times \mathbb{Z}_{p^a}^{d(r-b)}$. The result follows from Lemma 2.4.2. $\square$

2.5 Concluding Remarks

Group-invariant Butson Hadamard matrices encompass many combinatorial structures like generalized Hadamard matrices, relative difference sets, generalized Bent functions, cyclic n -roots, perfect sequences and perfect arrays. Using bilinear forms over finite abelian groups and the tools from the theory of relative difference sets, we constructed three classes of group-invariant Butson matrices in this thesis.

1. $\text{BH}(G, h)$ matrices in which G is abelian and $\nu_p(h)$ is large enough compared to $\nu_p(\exp(G))$ for any prime divisor p of $|G|$.
2. $\text{BH}(G, h)$ matrices in which G is nonabelian and $\nu_p(h)$ is large enough compared to $\nu_p(\exp(G))$ for any prime divisor p of $|G|$.
3. $\text{BH}(R \times R, h)$ matrix in which $R = \mathbb{Z}_{p^{a+1}}^{db} \times \mathbb{Z}_{p^a}^{d(r-b)}$, where $a, d, r \in \mathbb{Z}^+$ and $0 \leq b \leq r-1$, and there exist p^d th roots of unity $\eta_0, \dots, \eta_{p^d-1}$ such that $\sum_{i=0}^{p^d-1} \eta_i = 0$.

Moreover, we study various necessary conditions for the existence of group-invariant Butson Hadamard matrices. Based on our study, there are 2687 open cases for the existence of $\text{BH}(\mathbb{Z}_n, h)$ matrices in which $1 \leq n, h \leq 100$. Lastly, we use our constructions

of group-invariant Butson Hadamard matrices to construct two new families of perfect arrays.

To end this section, we propose several open questions on the study of group-invariant Butson Hadamard matrices.

1. Construct more classes of $\text{BH}(G, h)$ matrices.
2. Classify the constructed classes of $\text{BH}(G, h)$ matrices. For example, let be G one of the three groups from which we constructed three classes of $\text{BH}(G, h)$ matrices in this thesis. Find a condition on h so that our construction is *unique* in the following sense.

Let H be the $\text{BH}(G, h)$ matrix obtained by one of our constructions. Then any other $\text{BH}(G, h)$ matrix K has the first row obtained from the first row of H by either

- (i) multiplying the first row of H by a h th root of unity, or
- (ii) permuting the positions of the elements in the first row of H by an action of an element $l \in G$.

Equivalently, this means $K_{g,k} = \eta H_{g,kl}$ for some h th root of unity η and some fixed $l \in G$.

3. Most known necessary conditions on $\text{BH}(G, h)$ matrices involve a condition on $\gcd(|G|, h)$. However, this is not always the case, as suggested by Theorem 2.2.10. A question in this direction is finding other types of necessary conditions which do not involve $\gcd(|G|, h)$, for example, conditions on vanishing sums of roots of unity.
4. Our conjecture on the necessary and sufficient conditions for the existence of $\text{BH}(\mathbb{Z}_n, h)$ matrices, Conjecture 2.3.12, is

$$h^2 \equiv 0 \pmod{n} \text{ and } (\nu_2(n), \nu_2(h)) \neq (1, 1).$$

The conjecture is confirmed if n is a prime power, see Theorem 2.3.14. However, it remains wide open in the general case.

Chapter 3

Unique Differences in Symmetric Subsets of $\mathbb{F}_p$

3.1 Symmetric Subsets of $\mathbb{F}_p$ with no Unique Difference

In this chapter, we always identify $\mathbb{F}_p$ with the set $\{0, 1, \dots, p-1\}$ of residues modulo p . We recall that a subset B of $\mathbb{F}_p$ is said to have a unique difference if there exists $(a, b) \in B \times B$, such that there is no $(c, d) \in B \times B \setminus \{(a, b)\}$ with $c - d = a - b$. Moreover, we assume that the empty set contains a unique difference. Our goal for this problem is to investigate the number $g(p)$, the smallest size of a symmetric subset of $\mathbb{F}_p$ which has no unique difference.

We remark that if a subset B of $\mathbb{F}_p$ has large size, then it is more likely that B does not have a unique difference. For example when $B = \mathbb{F}_p$, then for any $a, b \in B$, we have $a - b = (a + 1) - (b + 1)$. A stronger claim is that if $|B| \geq (p + 3)/2$, then B contains no unique difference. Denote $B = \{b_1, \dots, b_n\}$, $n \geq (p + 3)/2$, and consider a fixed difference $b_k - b_l$, where $k \neq l \in \{1, \dots, n\}$, in B . The set $B' = \{b_i + b_k - b_l : 1 \leq i \leq n, i \neq l\}$ contains $n - 1$ elements. Hence $B \cap B' \neq \emptyset$ because $|B| \geq (p + 3)/2$ and $|B \cup B'| \leq p$. Let $b_j \in B \cap B'$. There exists $i \neq l$ such that $b_j - b_i = b_k - b_l$. Thus, the difference $b_k - b_l$ is not unique.

In this subsection, we study upper bounds for $g(p)$ by giving two constructions for symmetric subsets of $\mathbb{F}_p$ both of which contain no unique difference. The first construction is due to Nedev and Quas [42]. The second construction is by Straus [53]. We include proofs for both of these constructions for the convenience of the reader.

Note that for a symmetric subset A of $\mathbb{F}_p$, we have $a - b = (-b) - (-a)$ whenever

$b \neq \pm a$. Thus, the possible unique differences in A have the form $a - (-a) = 2a$, where $a \in A$. The following result is by Nedev and Quas [42].

Result 3.1.1. *Let $p \geq 7$ be a prime. Then there exists a symmetric subset A of $\mathbb{F}_p$ such that $|A| \leq 2\lfloor \log_2(p) \rfloor + 1$ and A contains no unique difference. As a result, we have*

$$g(p) \leq 2\lfloor \log_2(p) \rfloor + 1$$

for any $p \geq 7$.

Proof. Put $k = \lfloor \log_2(p) \rfloor$ and $a = p - 2^k$. Note that $1 \leq a \leq 2^k - 1$. Let A be the following symmetric subset of $\mathbb{F}_p$:

$$A = \{0, \pm 2^{k-1}, \pm(2^{k-1} - a)\}.$$

This set contains no unique difference if $p = 7$ and $|A| = 5 = 2\lfloor \log_2(7) \rfloor + 1$. From now on, we assume $p > 7$. Note that $2 \cdot 2^{k-1} = (-2^{k-1}) - (-(2^{k-1} - a))$, so possible unique differences in A come from $2 \cdot x$, where $x \in \{\pm(2^{k-1} - a)\}$. We will proceed to iteratively add elements to A until there is no unique difference. As $1 \leq a \leq 2^k - 1$, exactly one of the two elements $\pm(2^{k-1} - a)$, say T , is in $[0, 2^{k-1}]$. Let $[L_0, R_0]$ denote the initial interval $[0, 2^{k-1}]$. We repeat the following steps.

- (i) Set $M_i = (L_i + R_i)/2$ and add $\pm M_i$ to A .
- (ii) Of the two subintervals $[L_i, M_i]$ and $[M_i, R_i]$, choose the one which contains T and let it be the new interval $[L_{i+1}, R_{i+1}]$.
- (iii) Repeat (i) and (ii) until $\pm T$ is added to A .

Note that $2M_i$ is not a unique difference in A , as $2M_i = L_i + R_i$. The above algorithm makes sure that the new elements added to A do not form a unique difference. Therefore, the resulting set A does not have a unique difference. As we stop the algorithm after at most $k - 1$ steps, we obtain

$$|A| \leq 2(k - 1) + 3 = 2\lfloor \log_2(p) \rfloor + 1.$$

□

The following construction by Straus [53] provides a symmetric subset of $\mathbb{F}_p$ of size $(2 + o(1)) \log_3(p)$ which contains no unique difference. In view of our result Theorem 1.2.6, this subset has asymptotically smallest size.

Result 3.1.2. *Let $\epsilon > 0$ be a fixed real number. Then there exists a prime $p(\epsilon)$ such that for any prime $p \geq p(\epsilon)$, there exists a symmetric subset A of $\mathbb{F}_p$ such that $|A| \leq (2 + \epsilon) \log_3(p)$ and A contains no unique difference. As a result, we have*

$$g(p) \leq (2 + \epsilon) \log_3(p)$$

for any $p \geq p(\epsilon)$.

Proof. Choose a prime p and a positive integer k such that $p > 2 \cdot 3^k$. The exact values of p and k are to be chosen later. Consider the following set of integers

$$R = \{0, \pm 1, \dots, \pm(3^k - 1)\}.$$

Construct a decreasing sequence of positive integers $a_1, \dots, a_l$ as follows.

$$a_1 = (p - r)/2, \quad r \in R, \quad p \equiv r \pmod{2 \cdot 3^k}, \quad (3.1)$$

$$a_{i+1} = \begin{cases} a_i/3 & \text{if } a_i \equiv 0 \pmod{3}, \\ (a_i - r_i)/2 & \text{if } a_i \not\equiv 0 \pmod{3}, \end{cases} \quad (3.2)$$

where $r_i \in R$ such that $a_i - r_i \equiv 0 \pmod{2 \cdot 3^k}$. The last element a_l in this sequence satisfies $a_l \geq 3^k$ and $a_{l+1} \in R$. Let A denote the following symmetric subset of $\mathbb{F}_p$.

$$A = \{0, \pm 1, \dots, \pm(3^k - 1), \pm a_l, \dots, \pm a_1\}. \quad (3.3)$$

By symmetry, A contains no unique difference if any number $2a$, $a \in \{1, \dots, 3^k - 1, a_1, \dots, a_l\}$, has another representation $2a = b - c$ with $b, c \in A$ and $(b, c) \neq (a, -a)$.

For $1 \leq a \leq 3^k - 2$, we have $2a = (a + 1) - (-a + 1)$.

Since $3^k \leq a_l \leq 3(3^k - 1)$, we have $2(3^k - 1) = a_l - r_0$ for some $r_0 \in \mathbb{Z}$ with $0 \leq |r_0| \leq 3^k - 1$.

For $1 < j \leq l$, we have

$$2a_j = \begin{cases} a_{j-1} - a_j & \text{if } a_{j-1} \equiv 0 \pmod{3}, \\ a_{j-1} - r_{j-1} & \text{if } a_{j-1} \not\equiv 0 \pmod{3}. \end{cases}$$

Finally, we have $2a_1 = 0 - r$ with $r \in R$. Thus, the set A , defined in (3.3), contains no unique difference.

Now we count the number of elements in A . Note that $a_{i+1} < a_i$ for all i and $a_{i+1} = a_i/3$ for all except for one out of every $k + 1$ consecutive terms $a_j, \dots, a_{j+k}$ (by definitions (3.1) and (3.2)). Thus

$$a_{j+k+1} < a_j 3^{-k}. \quad (3.4)$$

We claim that

$$3^k \leq a_l < 3p3^{-lk/(k+1)}. \quad (3.5)$$

The inequality $a_l \geq 3^k$ is clear from the definition of a_l . For the inequality $a_l < 3p3^{-lk/(k+1)}$, we first assume that $l \equiv 0 \pmod{k+1}$. By (3.4), we have

$$a_l < a_{k+1}3^{-lk/(k+1)+k}.$$

Note that $a_1 = (p-r)/2 \equiv 0 \pmod{3^k}$, so $a_2 = a_1/3 \equiv 0 \pmod{3^{k-1}}$, $a_3 = a_1/3^2 \equiv 0 \pmod{3^{k-2}}$, and so on. We obtain $a_{k+1} = a_1/3^k$ and hence

$$a_l < a_{k+1}3^{-lk/(k+1)+k} = a_13^{-lk/(k+1)} < 3p3^{-lk/(k+1)}.$$

Now assume that $l \not\equiv 0 \pmod{k+1}$. By (3.4), we have

$$a_l < a_{l-(k+1)\lfloor l/(k+1) \rfloor}3^{-k\lfloor \frac{l}{k+1} \rfloor} = a_13^{-l+(k+1)\lfloor \frac{l}{k+1} \rfloor+1}3^{-k\lfloor \frac{l}{k+1} \rfloor}$$

Hence

$$a_l < a_13^{1+\lfloor \frac{l}{k+1} \rfloor-l} < 3p3^{-lk/(k+1)},$$

proving (3.5). Taking $\log_3$ in (3.5), we have $k < \log_3(p) + 1 - lk/(k+1)$, which implies

$$l < \frac{(k+1)\log_3(p) + 1 - k^2}{k} \leq \left(1 + \frac{1}{k}\right)\log_3(p).$$

We obtain

$$|A| = 2l + 2(3^k - 1) + 1 < \left(2 + \frac{2}{k}\right)\log_3(p) + 2 \cdot 3^k < (2 + \epsilon)\log_3(p)$$

if we choose

$$\frac{4}{\epsilon} < k < \log_3\left(\frac{\epsilon}{4}\log_3(p)\right),$$

which is possible for any $\epsilon > 0$ provided that p is sufficiently large. $\square$

3.2 Set-up

First, we recall our main result.

Theorem 1.2.6. Let $p \geq 5$ be a prime and let A be a symmetric subset of $\mathbb{F}_p$ with $|A \setminus \{0\}| \leq 2\log_3(p)$. Then A has a unique difference. As a result, we have

$$g(p) > 2\log_3(p).$$

We will prove this theorem in Section 3.5. In preparation for the proof, we introduce some notations and assumptions which will be implicitly assumed in the rest of this chapter. Let p be an odd prime and suppose that A is a symmetric subset of $\mathbb{F}_p$ which has no unique difference. Write $A = \{\pm a_1, \dots, \pm a_n\}$ such that $a_j \neq \pm a_i$ for $i \neq j$. We set $a_n = 0$ if $0 \in A$. Let $m = \lfloor |A|/2 \rfloor$. Note that $m = n$ if $0 \notin A$ and $m = n - 1$ if $0 \in A$.

Next, we show that we may assume $|A| \geq 4$. If $|A| = 0$, then A has a unique difference by our assumption for the empty set. If $|A| = 1$, then $A = \{0\}$ certainly has a unique difference. If $2 \leq |A| \leq 3$, then $A = \{\pm a_1\}$ or $A = \{0, \pm a_1\}$ for some $a_1 \neq 0$. Then $a_1 - (-a_1) = 2a_1$ is a unique difference in A . Hence we can indeed assume $|A| \geq 4$.

We now set up a linear system arising from A and derive some useful properties of its coefficient matrix. Let i be arbitrary with $1 \leq i \leq m$. As $2a_i = a_i - (-a_i)$ is not a unique difference in A and $2a_i \neq \pm a_i - a_i$, there exists an ordered pair $(\sigma(i), \tau(i)) \neq (i, i)$ such that

$$2a_i \pm a_{\sigma(i)} \pm a_{\tau(i)} = 0. \quad (3.6)$$

Here “ $\pm a_{\sigma(i)} \pm a_{\tau(i)}$ ” means that *any* combination of signs is possible including $a_{\sigma(i)} + a_{\tau(i)}$, $-a_{\sigma(i)} - a_{\tau(i)}$, $a_{\sigma(i)} - a_{\tau(i)}$ and $-a_{\sigma(i)} + a_{\tau(i)}$. We use this convention throughout the rest of the paper.

We consider the homogeneous linear system corresponding to these equations:

$$2x_i \pm x_{\sigma(i)} \pm x_{\tau(i)} = 0, \quad i = 1, \dots, m. \quad (3.7)$$

Here we use the convention $x_n = 0$ if $0 \in A$ (and thus $a_n = 0$).

Note that the coefficient vectors corresponding to the system (3.7) all have at most 3 nonzero entries. The nonzero coefficients, however, are not necessarily $2, \pm 1$, since $i, \sigma(i), \tau(i)$ are not necessarily distinct. We now determine exactly which coefficient vectors can occur.

Case 1 $\sigma(i) = i$ or $\tau(i) = i$. By symmetry, we can assume $\tau(i) = i$. Thus $2a_i \pm a_{\sigma(i)} \pm a_i = 0$. As $(\sigma(i), \tau(i)) \neq (i, i)$, we have $\sigma(i) \neq i$. If $2a_i \pm a_{\sigma(i)} - a_i = 0$, then $a_i \pm a_{\sigma(i)} = 0$, contradicting the assumption $a_i \neq \pm a_j$ for $i \neq j$. Hence $2a_i \pm a_{\sigma(i)} + a_i = 3a_i \pm a_{\sigma(i)} = 0$. Recall that we assume $p \geq 5$. If $a_{\sigma(i)} = 0$, then $3a_i = 0$ and thus $a_i = 0$, contradicting the assumptions. Thus $a_{\sigma(i)} \neq 0$, i.e., $\sigma(i) \leq m$.

Hence (3.6) can be written as

$$3x_i \pm x_{\sigma(i)} = 0 \quad (3.8)$$

with $\sigma(i) \neq i$ and $\sigma(i) \leq m$. We call (3.8) an equation of **type 1**.

Case 2 $\sigma(i) \neq i$ and $\tau(i) \neq i$. If $\tau(i) = \sigma(i)$, then (3.6) implies $a_i = 0$ or $a_i = \pm a_{\sigma(i)}$, contradicting the assumptions. Thus $\tau(i) \neq \sigma(i)$. Hence $i, \sigma(i), \tau(i)$ are pairwise distinct.

Recall that $x_n = 0$ if $0 \in A$. Hence, if $0 \in A$ and $n \in \{\sigma(i), \tau(i)\}$, then one of the variables $x_{\sigma(i)}, x_{\tau(i)}$ occurs with coefficient zero in (3.6). By symmetry, we can assume that $x_{\tau(i)}$ occurs with coefficient zero in this case.

Hence, in Case 2, we can write (3.6) as

$$\begin{aligned} 2x_i \pm x_{\sigma(i)} &= 0 \quad \text{if } 0 \in A \text{ and } \tau(i) = n, \\ 2x_i \pm x_{\sigma(i)} \pm x_{\tau(i)} &= 0 \quad \text{otherwise,} \end{aligned} \tag{3.9}$$

where $i, \sigma(i), \tau(i)$ are pairwise distinct. In both cases, we call (3.9) an equation of **type 2**.

In summary, as Case 1 and Case 2 cover all possible cases, for every $i \in \{1, \dots, m\}$, one of the following equations is contained in the linear system (3.7).

$$\begin{aligned} 3x_i \pm x_{\sigma(i)} &= 0 \quad (\text{type 1}), \\ 2x_i \pm x_{\sigma(i)} &= 0 \quad (\text{type 2}), \\ 2x_i \pm x_{\sigma(i)} \pm x_{\tau(i)} &= 0 \quad (\text{type 2}). \end{aligned} \tag{3.10}$$

Furthermore, the following hold.

- $\sigma(i) \leq m$ and $\tau(i) \leq m$,
- $i, \sigma(i), \tau(i)$ are pairwise distinct.

Of course, the statements involving $\tau(i)$ only apply if the equation $2x_i \pm x_{\sigma(i)} \pm x_{\tau(i)} = 0$ is contained (3.7).

We use a similar terminology for the coefficient vectors of the system (3.7). We say a coefficient vector is of **type 1** if it has exactly one entry 3, exactly one entry ± 1 , and all its remaining entries are zero. A coefficient vector is of **type 2** if it has exactly one entry 2, at most two entries ± 1 , and all its remaining entries are zero.

3.3 Smith Normal Form of the Coefficient Matrix

Let $A = \{\pm a_1, \dots, \pm a_n\}$ be a symmetric subset of $\mathbb{F}_p$ which has size smallest as possible and contains no unique difference, that is,

$$|A| = g(p).$$

Let M be the coefficient matrix of the linear system (3.7). Recall that all entries of M are from $\{0, \pm 1, 2, 3\}$. In this section, we study the Smith Normal Form of M . Note that M can be considered as a matrix with rational entries as well as a matrix with entries from $\mathbb{F}_p$. In the following, we make use of both interpretations.

Theorem 3.3.1. *Suppose that $A = \{\pm a_1, \dots, \pm a_n\} \subset \mathbb{F}_p$ does not have a unique difference and let M be the coefficient matrix of the corresponding linear system (3.7). Write $r = \text{rank}_{\mathbb{Q}}(M)$. Every $r \times r$ -minor of M is divisible by p .*

Proof. Recall that M is an $m \times m$ -matrix and that M has entries from $\{0, \pm 1, 2, 3\}$ only. In this proof, we consider the entries of M as *integers* (not as elements of $\mathbb{F}_p$), and we will work with the Smith Normal Form of M over the integers.

Let $D = \text{diag}(d_1, \dots, d_r, 0, \dots, 0)$ be the Smith Normal Form of M , see Result 1.3.1 for more details about Smith Normal Form. Note that $d_1, \dots, d_r$ are positive integers such that d_i divides d_{i+1} for $i = 1, \dots, r-1$. Furthermore, there are $B, C \in M_{m,m}(\mathbb{Z})$ with $\det(B) = \pm 1$, $\det(C) = \pm 1$, and $M = BDC$. It is important for this proof to note that B, C, D are matrices with *integer* entries and the equation $M = BDC$ holds over $\mathbb{Z}$ (not only over $\mathbb{F}_p$). Furthermore, note that all entries of C^{-1} are integers, as $\det(C) = \pm 1$.

Write $x = (a_1, \dots, a_m)^T$. Note $x \in \mathbb{F}_p^m$. We have $x \neq 0$, as $|A| > 1$. Recall that $Mx = 0$ over $\mathbb{F}_p$ by (3.7).

Suppose that p does not divide d_r . Then p does not divide any of the integers $d_1, \dots, d_r$. Write $Cx = (b_1, \dots, b_m)^T$ where $b_1, \dots, b_m \in \mathbb{F}_p$. Note that $DCx = 0$ over $\mathbb{F}_p$ if and only if $b_1 = \dots = b_r = 0$, since we assume that $d_1, \dots, d_r$ are not divisible by p . Hence $DCx = 0$ if and only if $x = C^{-1}(0, \dots, 0, b_{r+1}, \dots, b_m)^T$ for some $b_i \in \mathbb{F}_p$. As $BDCx = Mx = 0$ over $\mathbb{F}_p$, we indeed have $DCx = 0$ over $\mathbb{F}_p$. Thus

$$x = C^{-1}b \text{ with } b = (0, \dots, 0, b_{r+1}, \dots, b_m)^T \in \mathbb{F}_p^m. \quad (3.11)$$

For convenience, we set $b_i = 0$ for $i = 1, \dots, r$.

We now switch from equations over $\mathbb{F}_p$ to equations over $\mathbb{Z}$. We first define a vector c with *integer entries* which represent the residue classes $b_1, \dots, b_m \bmod p$. Formally, let $c_1, \dots, c_m$ be the unique integers with $0 \leq c_i \leq p-1$ and

$$b_i = c_i + p\mathbb{Z}/\mathbb{Z} \quad (3.12)$$

(here we use the standard notation $\mathbb{F}_p = \{k + p\mathbb{Z}/\mathbb{Z} : k = 0, \dots, p-1\}$). Note that $c_1 = \dots = c_r = 0$, as $b_1 = \dots = b_r = 0$ (again, note that $c_1 = \dots = c_r = 0$ are equations over $\mathbb{Z}$, not only over $\mathbb{F}_p$).

Define $y = (y_1, \dots, y_m) \in \mathbb{Z}^m$ by

$$y = C^{-1}(0, \dots, 0, c_{r+1}, \dots, c_m)^T \quad (3.13)$$

(recall that the c_i 's are considered as integers, not as elements of $\mathbb{F}_p$). Then we have

$$My = BDCy = B \operatorname{diag}(d_1, \dots, d_r, 0, \dots, 0)(0, \dots, 0, c_{r+1}, \dots, c_m)^T = 0 \quad (3.14)$$

over $\mathbb{Z}$ (note that all entries of matrices and vectors occurring in (3.14) are considered as integers and to derive (3.14), we need the fact that the equation $M = BDC$ holds over $\mathbb{Z}$, not only over $\mathbb{F}_p$).

Let Γ_j be the j th row of C^{-1} , $j = 1, \dots, m$. By (3.11) and (3.13), we have

$$a_j = \Gamma_j b \text{ and } y_j = \Gamma_j c \quad (3.15)$$

where $b = (0, \dots, 0, b_{r+1}, \dots, b_m)^T$ and $c = (0, \dots, 0, c_{r+1}, \dots, c_m)^T$. Note that (3.12) and (3.15) imply

$$a_j = y_j + p\mathbb{Z}/\mathbb{Z}, \quad i = 1, \dots, m. \quad (3.16)$$

Recall that M is the coefficient matrix of the linear system (3.7) and that $My = 0$ over $\mathbb{Z}$ by (3.14). This implies that $\{\pm y_1, \dots, \pm y_m\}$ does not have a unique difference (where the differences are taken in $\mathbb{Z}$). Recall that $a_i \neq \pm a_j$ for $i \neq j$ by assumption. Thus (3.16) implies $y_i \neq \pm y_j$ for $i \neq j$. Hence there is $k \in \{1, \dots, m\}$ such that $|y_k| > |y_i|$ for all $i \neq k$. This implies that $2y_k = y_k - (-y_k)$ is a unique difference of $\{\pm y_1, \dots, \pm y_m\}$, a contradiction. We conclude that p divides d_r .

By Result 1.3.1, d_r divides the greatest common divisor of all $r \times r$ -minors of M . $\square$

The following corollary gives a clearer description of the invariant factors $d_1, \dots, d_r$ of M in the case A has cardinality $g(p)$.

Corollary 3.3.2. *Let A be a symmetric subset of $\mathbb{F}_p$ which has cardinality $g(p)$ and contains no unique difference. Under the notations of Theorem 3.3.1, there exist matrices $S, T \in M_{m,m}(\mathbb{Z})$ such that $\det(S) = \pm 1$, $\det(T) = \pm 1$ and*

$$SMT = \begin{pmatrix} d_1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \cdots & 0 \\ 0 & 0 & \cdots & d_r & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}, \quad (3.17)$$

where $d_1, \dots, d_r$ are positive integers with the following properties.

- (i) $d_r = \delta p$ for some $\delta \in \mathbb{Z}^+$;
- (ii) $d_1 \mid d_2 \mid \cdots \mid d_{r-1} \mid \delta$;
- (iii) $d_1 \cdots d_{r-1} \delta \leq p^{\log_2(\sqrt{10})-1}$.

Proof. Part (i) is proved in Theorem 3.3.1. We note that (ii) is a consequence of (iii). Assume that (iii) holds. We have $d_{r-1} \leq d_1 \cdots d_{r-1} \delta \leq p^{\log_2(\sqrt{10})-1} < p$. As d_{r-1} divides $d_r = \delta p$, we obtain $d_{r-1} \mid \delta$. Thus, it suffices to prove (iii) for both (ii) and (iii). Note that by (3.10), each row of M has norm at most $\sqrt{10}$, so each row of an $r \times r$ submatrix of M has norm at most $\sqrt{10}$. By Result 1.3.3 (Hadamard's inequality), all $r \times r$ minors of M are bounded by $(\sqrt{10})^r$. We obtain

$$d_1 \cdots d_{r-1} \delta p \leq (\sqrt{10})^r,$$

which results in

$$\lfloor |A|/2 \rfloor = m \geq r \geq \log_{\sqrt{10}}(d_1 \cdots d_{r-1} \delta p). \quad (3.18)$$

Note that $|A| = g(p) \leq 2\lfloor \log_2(p) \rfloor + 1$ by Result 3.1.1. Hence $\lfloor |A|/2 \rfloor \leq \log_2(p)$. By (3.18), we obtain

$$\log_{\sqrt{10}}(d_1 \cdots d_{r-1} \delta p) \leq \log_2(p),$$

proving (iii). □

3.4 Equations of Type 1

Equations of type 1 play a critical role in the proof of Theorem 1.2.6, as the Euclidean norm of their coefficient vectors is the largest among the equations occurring in the linear system (3.7). In this section, we study the structure of the set of equations of type 1 contained in (3.7). Recall that equations of type 1 have the form

$$3x_i \pm x_{\sigma(i)} = 0,$$

where $1 \leq i \leq m$, $\sigma(i) \neq i$, and $\sigma(i) \leq m$.

Lemma 3.4.1. *Suppose $3^{\lfloor |A|/2 \rfloor} \leq p$. Let I be a subset of $\{1, \dots, m\}$ such that $3x_i \pm x_{\sigma(i)} = 0$, $i \in I$, are equations of type 1 contained in (3.7). Let G be the directed graph with vertex set $I \cup \{\sigma(i) : i \in I\}$ and edge set $E = \{(i, \sigma(i)) : i \in I\}$. Then E can be decomposed into directed paths which are pairwise vertex disjoint.*

Proof. We show

- (i) every vertex of G has outdegree at most 1,
- (ii) every vertex of G has indegree at most 1,
- (iii) G does not contain a directed cycle.

Note that (i-iii) imply that G indeed can be decomposed into directed paths which are pairwise vertex disjoint.

First of all, there is at most one edge $(i, \sigma(i))$ for every vertex i . This means that the outdegree of every vertex in G is at most one.

Suppose that the indegree of a vertex i is at least 2. Then there are distinct vertices j, k with $\sigma(j) = \sigma(k) = i$. By definition, this implies $3a_j \pm a_i = 0$ and $3a_k \pm a_i = 0$ and thus $3(a_j - a_k) = 0$ or $3(a_j + a_k) = 0$. As $p > 3$, we conclude $a_j = \pm a_k$ which contradicts the assumption $a_j \neq \pm a_k$ for $j \neq k$. This shows that all vertices of G have indegree at most 1.

Now suppose that G contains a directed cycle. Then there are vertices $v_1, v_2, \dots, v_k$ with $v_k = v_1$ such that $(v_i, v_{i+1}) \in E$ for $i = 1, \dots, k-1$, i.e., $v_{i+1} = \sigma(v_i)$ for $i = 1, \dots, k-1$. By definition, this implies $3a_{v_i} = \pm a_{v_{i+1}}$ for $i = 1, \dots, k-1$. Hence

$$a_{v_1} = a_{v_k} = \pm 3a_{v_{k-1}} = \pm 9a_{v_{k-2}} = \dots = \pm 3^{k-1}a_{v_1}.$$

Thus $(\pm 3^{k-1} - 1)a_{v_1} = 0$. Note that $k \leq m+1$, as the cycle contains every vertex $\neq v_1$ at most once. Moreover, $p \geq 3^m = 3^{\lfloor |A|/2 \rfloor}$ by assumption and thus $p \geq 3^m + 2$, as $p > 3$ is a prime. We conclude $3^{k-1} + 1 \leq 3^m + 1 < p$. Hence $(\pm 3^{k-1} - 1)a_{v_1} = 0$ implies $a_{v_1} = 0$, contradicting the assumption $a_i \neq 0$ for $i = 1, \dots, m$. This shows that G does not contain a directed cycle.

In summary, we have shown that (i)-(iii) hold, and this completes the proof. $\square$

Remark 3.4.2. Note that Lemma 3.4.1 implies that G does not contain *any* cycle, directed or undirected.

Next, we compute determinants arising from matrices whose rows are coefficient vectors of equations of type 1.

Lemma 3.4.3. *Let G be the graph defined in Lemma 3.4.1. Suppose J is a subset of $\{1, \dots, m\}$ such that $\{(i, \sigma(i)) : i \in J\}$ is a directed path in G and let B be the coefficient matrix of the corresponding equations $3x_i \pm x_{\sigma(i)} = 0$, $i \in J$. Then*

$$\det(BB^T) = \frac{1}{8} \left(-1 + 9^{|J|+1} \right). \quad (3.19)$$

Proof. Write $v = |J|$. By relabeling vertices of G , if necessary, we may assume that the directed path consists of the edges $(i, i+1)$, $i = 1, \dots, v$. The corresponding equations are $3x_i \pm x_{i+1} = 0$, $i = 1, \dots, v$. Hence B is a $v \times m$ -matrix of the form

$$\begin{pmatrix} 3 & \pm 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 3 & \pm 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 3 & \pm 1 & 0 & \cdots & 0 \end{pmatrix}.$$

Thus

$$BB^T = \begin{pmatrix} 10 & 3\delta_1 & 0 & \cdots & 0 & 0 & 0 \\ 3\delta_1 & 10 & 3\delta_2 & \cdots & 0 & 0 & 0 \\ 0 & 3\delta_2 & 10 & 3\delta_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \\ 0 & \cdots & 0 & 3\delta_{v-3} & 10 & 3\delta_{v-2} & 0 \\ 0 & \cdots & 0 & 0 & 3\delta_{v-2} & 10 & 3\delta_{v-1} \\ 0 & \cdots & 0 & 0 & 0 & 3\delta_{v-1} & 10 \end{pmatrix}$$

with $\delta_i = \pm 1$, $i = 1, \dots, v-1$. We now prove (3.19) by induction on v . It is straightforward to check that (3.19) holds for $v = 1$. Suppose $v \geq 2$. Using Laplace expansion with respect to the last column of BB^T and the inductive hypothesis, we find

$$\det(BB^T) = 10 \left(\frac{1}{8} (-1 + 9^v) \right) - (3\delta_{v-1})^2 \left(\frac{1}{8} (-1 + 9^{v-1}) \right).$$

Note $(3\delta_{v-1})^2 = 9$. Hence

$$\det(BB^T) = \frac{1}{8} (-10 + 9 + (10 - 1)9^v) = \frac{1}{8} (-1 + 9^{v+1}).$$

□

Corollary 3.4.4. *Suppose $3^{\lfloor |A|/2 \rfloor} \leq p$. Let I be a subset of $\{1, \dots, m\}$ such that $3x_i \pm x_{\sigma(i)} = 0$, $i \in I$, are equations of type 1. Let G be the directed graph defined in Lemma 3.4.1 and let $P_1, \dots, P_t$ be vertex disjoint directed paths in G with $E = \bigcup_{j=1}^t P_j$. Let B be the matrix whose rows are the coefficient vectors of the equations $3x_i \pm x_{\sigma(i)} = 0$, $i \in I$. Then*

$$\det(BB^T) < 11^t 9^{|I|-t}.$$

Proof. For $j = 1, \dots, t$, let B_j be the matrix whose rows are the coefficient vectors of the equations $3x_i \pm x_{\sigma(i)} = 0$, $(i, \sigma(i)) \in P_j$. By Lemma 3.4.3, we have

$$\det(B_j B_j^T) = \frac{1}{8} (-1 + 9^{|P_j|+1}).$$

Note that

$$\frac{1}{8}(-1 + 9^{x+1}) < 11 \cdot 9^{x-1}$$

for all $x \geq 1$. Using Corollary 1.3.5 and $\sum_{j=1}^t |P_j| = |I|$, we conclude

$$\begin{aligned} \det(BB^T) &\leq \prod_{j=1}^t \det(B_j B_j^T) \\ &= \prod_{j=1}^t \left(\frac{1}{8} (-1 + 9^{|P_j|+1}) \right) \\ &< \prod_{j=1}^t (11 \cdot 9^{|P_j|-1}) \\ &= 11^t 9^{|I|-t}. \end{aligned}$$

□

3.5 Proof of Theorem 1.2.6

Let p be prime and let A be a symmetric subset of $\mathbb{F}_p$ with

$$|A \setminus \{0\}| \leq 2 \log_3(p). \quad (3.20)$$

We have to prove that A has a unique difference.

Suppose A does not have a unique difference. Write $A = \{\pm a_1, \dots, \pm a_n\}$ as in Section 3.2, where $a_n = 0$ if $0 \in A$. Recall $m = \lfloor |A|/2 \rfloor$. Note $|A \setminus \{0\}| = 2\lfloor |A|/2 \rfloor$. Hence $3^{\lfloor |A|/2 \rfloor} \leq p$ by (3.20) and thus

$$3^{\lfloor |A|/2 \rfloor} < p, \quad (3.21)$$

as $p \neq 3$.

Let M be the coefficient matrix of the linear system (3.7) and write $r = \text{rank}_{\mathbb{Q}}(M)$. Note $r \leq m$. Let N be a nonsingular $r \times r$ submatrix of M .

We claim that

$$|\det(N)| \leq 3^r. \quad (3.22)$$

We say that a row vector is of **type 3** if it has exactly one entry 3 and all its remaining entries are zero. Note that N may contain rows of type 3, as some rows of M of type

1 may turn into type 3 when columns of M are deleted. If N contains a row of type 3, then, by Laplace expansion, $|\det(N)| = 3|\det(N_1)|$ where N_1 is a $(r-1) \times (r-1)$ submatrix of M . Repeating this process, if necessary, we either get $|\det(N)| = 3^r$ or obtain a $d \times d$ submatrix N_2 of M with

$$|\det(N)| = 3^{r-d} |\det(N_2)| \quad (3.23)$$

such that N_2 does not contain any row of type 3. If $|\det(N)| = 3^r$, then (3.22) holds. Thus we may assume that (3.23) holds.

As N_2 is a submatrix of M , all rows of N_2 which are not of type 1 have at most three nonzero entries $\pm 1, 2$, at most one of which is 2. Hence every row of N_2 which is not of type 1 has Euclidean norm at most $\sqrt{6}$.

Swapping rows, if necessary, we can write

$$N_2 = \begin{pmatrix} B \\ C \end{pmatrix}$$

where B consists of the rows of N_2 of type 1 and C of the remaining rows of N_2 . Let I be the subset of $\{1, \dots, m\}$ such that $3x_i \pm x_{\sigma(i)} = 0$, $i \in I$, are the equations corresponding to the rows of B . Note that $|I|$ is the number of rows of B and $d - |I|$ is the number of rows of C .

Let G be the directed graph with vertex set $V = I \cup \{\sigma(i) : i \in I\}$ and edge set $E = \{(i, \sigma(i)) : i \in I\}$. Note that $|V| \leq d$, as every element of V is an index of a column of N_2 .

By Lemma 3.4.1, there is a decomposition of E into pairwise vertex disjoint directed paths. Note that these directed paths are connected components of G . Let t be the number of paths in the decomposition and let $E_1, \dots, E_t$ denote these paths. In each E_i , the number of vertices is $|V_i| = |E_i| + 1$. The number of vertices of G is $|V| \geq \sum_{i=1}^t |V_i| = \sum_{i=1}^t |E_i| + t = |E| + t$. Hence

$$t \leq |V| - |E| \leq d - |I|. \quad (3.24)$$

By Corollary 3.4.4, we have

$$\det(BB^T) < 11^t 9^{|I|-t}. \quad (3.25)$$

From (3.24) and (3.25), we get

$$\det(BB^T) < 11^{d-|I|} 9^{|I|-(d-|I|)} = 11^{d-|I|} 9^{2|I|-d}. \quad (3.26)$$

As the rows of C all have Euclidean norm at most $\sqrt{6}$, we have

$$\det(CC^T) \leq 6^{d-|I|} \quad (3.27)$$

by Result 1.3.2. From Result 1.3.4, we get

$$\det(N_2 N_2^T) \leq \det(BB^T) \det(CC^T). \quad (3.28)$$

Putting (3.26)-(3.28) together, we find

$$\begin{aligned} \det(N_2 N_2^T) &< 11^{d-|I|} 9^{2|I|-d} 6^{d-|I|} \\ &= 66^{d-|I|} 9^{2|I|-d} \\ &\leq 81^{d-|I|} 9^{2|I|-d} \\ &= 9^d. \end{aligned}$$

Hence $|\det(N_2)| \leq 3^d$ and thus $|\det(N)| \leq 3^r$ by (3.23). This proves (3.22).

Finally, recall that $\det(N)$ is a nonzero $r \times r$ -minor of M . Hence $|\det(N)| \geq p$ by Theorem 3.3.1. But $r \leq \lfloor |A|/2 \rfloor$ and thus $|\det(N)| \leq 3^r < p$ by (3.21), a contradiction. This completes the proof of Theorem 1.2.6. $\square$

3.6 Application to Weil Numbers

Let m, n be positive integers. Write $\zeta_m = \exp(2\pi i/m)$. An **n -Weil number** in $\mathbb{Z}[\zeta_m]$ is an element Y of $\mathbb{Z}[\zeta_m]$ with $|Y|^2 = n$. In this section, we show that Theorem 1.2.6 implies that under certain conditions Weil numbers in $\mathbb{Z}[\zeta_m]$ necessarily are contained in proper subfields of $\mathbb{Q}(\zeta_m)$. This result is a partial improvement of the “field descent” introduced in [49] and is relevant for the study of difference sets and related objects. We will assume basic algebraic number theory in this sections, as treated in [29], for instance.

For a finite group G and a ring R , let $R[G]$ denote the group ring of G over R . Every element B of $R[G]$ can be written as $B = \sum_{g \in G} r_g g$ with $r_g \in R$. The r_g ’s are called the **coefficients** of B . We write $B^{(-1)} = \sum_{g \in G} \bar{r}_g g^{-1}$ where $\bar{r}_g$ is the complex conjugate of r_g .

For $Y \in \mathbb{Z}[\zeta_m]$, let

$$\mathcal{M}(Y) = \frac{1}{\varphi(m)} \sum_{\sigma \in \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})} (Y \bar{Y})^\sigma,$$

where φ denote the Euler totient function. Note

$$\mathcal{M}(Y) \geq 1 \quad (3.29)$$

for $Y \neq 0$ by the inequality of geometric and arithmetic means, since $\prod (Y\bar{Y})^\sigma$ is the norm of an algebraic integer and thus $\prod (Y\bar{Y})^\sigma \geq 1$. The following is due to Cassels [12].

Result 3.6.1. *Let $X \in \mathbb{Z}[\zeta_m]$ where $m = pm'$ and p is a prime with $(p, m') = 1$. Write $X = \sum_{i=0}^{p-1} X_i \zeta_p^i$ with $X_i \in \mathbb{Z}[\zeta_{m'}]$. We have*

$$(p-1)\mathcal{M}(X) = \sum_{i < j}^{p-1} \mathcal{M}(X_i - X_j).$$

We denote the cyclic group of order k by C_k .

Theorem 3.6.2. *Let p, q be distinct primes and r be a positive integer with $\gcd(r, pq) = 1$. Let $n = q^b$ where b is a positive integer. Suppose that $Y\bar{Y} = n$ for some $Y \in \mathbb{Z}[\zeta_{pr}]$. If $\text{ord}_p(q)$ is even and $p > \max\{3^{n/2}, n^2 + n + 1\}$, then $Y\eta \in \mathbb{Z}[\zeta_r]$ for some root of unity η .*

Proof. Write $\text{ord}_p(q) = 2f$, and define $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_{pr})/\mathbb{Q})$ by $\zeta_{pr}^\sigma = \zeta_{pr}^{q^f}$. Note that σ fixes all prime ideals above n in $\mathbb{Z}(\zeta_{pr})$ (see [49, Thm. 2.1], for instance). Hence $Y^\sigma = Y\alpha$ for some unit α . Note $|\alpha|^2 = Y^\sigma \bar{Y}^\sigma / (Y\bar{Y}) = n^\sigma / n = 1$. Thus α is a root of unity, i.e., $\alpha = \pm \zeta_p^c \zeta_r^d$ for some integers c, d . Let e be an integer with $2e \equiv c \pmod{p}$. Note that $\zeta_p^\sigma = \zeta_p^{-1}$ and thus

$$(Y\zeta_p^e)^\sigma = Y(\pm \zeta_p^c \zeta_r^d) \zeta_p^{-e} = Y(\pm \zeta_p^{c-e} \zeta_r^d) = Y(\pm \zeta_p^e \zeta_r^d).$$

Let $Y_1 = Y\zeta_p^e$. Then

$$Y_1^\sigma = Y_1(\pm \zeta_r^d). \quad (3.30)$$

Write $Y_1 = \sum_{i=0}^{p-1} a_i \zeta_p^i$ with $a_i \in \mathbb{Z}[\zeta_r]$. Note $\mathcal{M}(Y_1) = \mathcal{M}(Y) = n$. By Result 3.6.1, we have

$$(p-1)n = (p-1)\mathcal{M}(Y_1) = \sum_{i < j}^{p-1} \mathcal{M}(a_i - a_j). \quad (3.31)$$

Let t be the maximum number such that there are distinct indices $i_1, \dots, i_t$ with $a_{i_1} = \dots = a_{i_t}$. If $t \leq p/2$, then, by (3.29), the right hand side of (3.31) is at least $p^2/4$ and thus $4n > p$, contradicting the assumption $p > n^2 + n + 1$. Hence $t \geq p/2$. Note that, by (3.29), the right hand side of (3.31) is at least $(p-t)t$. Hence $(p-t)t \leq n(p-1)$.

Note that $(p-t)t$ is decreasing for $t \in [p/2, p]$ and that $(p - (p - n - 1))(p - n - 1) = n(p - 1) + p - n - 1 - n^2 > n(p - 1)$, as $p > n^2 + n + 1$. Hence $t \geq p - n$. Recall that $a_{i_1} = \dots = a_{i_t}$. Note $Y_1 = \sum_{i=0}^{p-1} (a_i - a_{i_1})\zeta_p^i$. Thus, writing $b_i = a_i - a_{i_1}$, we have $Y_1 = \sum_{i=0}^{p-1} b_i \zeta_p^i$ and $|\{i : b_i \neq 0\}| \leq n$. If $|\{i : b_i \neq 0\}| = 1$, then the assertion of Theorem 3.6.2 holds. Hence, to complete the proof, it suffices to show that

$$2 \leq |\{i : b_i \neq 0\}| \leq n \quad (3.32)$$

leads to a contradiction. Define $X = \sum b_i g^i$ where g is a generator of C_p , the cyclic group of order p . Let K be the kernel of the ring homomorphism $\rho : \mathbb{Z}[\zeta_r][C_p] \rightarrow \mathbb{Z}[\zeta_{pr}]$ determined by $g \mapsto \zeta_p$. It is well known and straightforward to verify that $K = \{AC_p : A \in \mathbb{Z}[\zeta_r][C_p]\}$. Note that $\rho(X) = Y_1$, $\rho(X^{(-1)}) = \overline{Y_1}$ and thus $\rho(XX^{(-1)}) = Y_1 \overline{Y_1} = n$. Hence

$$XX^{(-1)} = n + AC_p \quad (3.33)$$

for some $A \in \mathbb{Z}[\zeta_r][C_p]$. Suppose $A \neq 0$. Then there are at least $p-1$ nonzero coefficients on the right hand side of (3.33). On the other hand, by (3.32), there are at most $n(n-1)$ nonzero coefficients on the left hand side of (3.33). Hence $p \leq n(n-1) + 1$ which contradicts the assumptions. Thus $A = 0$ and hence

$$XX^{(-1)} = n. \quad (3.34)$$

Recall that $X = \sum b_i g^i$. By (3.32), we can write $X = \sum_{j=1}^z b_{i_j} g^{i_j}$ with $2 \leq z \leq n$ and $b_{i_j} \neq 0$ for all j . Note

$$XX^{(-1)} = \sum_{k=0}^{p-1} \left(\sum_{i_r - i_s \equiv k \pmod{p}} b_{i_r} \overline{b_{i_s}} \right) g^k. \quad (3.35)$$

Write $S = \{i_1, \dots, i_z\}$ and view S as a subset of $\mathbb{F}_p$. Note $2 \leq |S| \leq n$. Suppose S has a unique difference, say, $k = i_r - i_s \in \mathbb{F}_p$ is a unique difference in S . Note that $k \neq 0$, as $|S| \geq 2$ and thus 0 is not a unique difference in S . In view of (3.35), the coefficient of g^k in $XX^{(-1)}$ is nonzero. But this contradicts $XX^{(-1)} = n$. Thus S has no unique difference.

Using (3.30), we get

$$Y_1^\sigma = \sum_{i=0}^{p-1} b_i^\sigma \zeta_p^{-i} = \pm \zeta_r^d Y_1 = \pm \zeta_r^d \sum_{i=0}^{p-1} b_i \zeta_p^i$$

Hence, for $i \neq 0$, we have $b_i \neq 0$ if and only if $b_{p-i} \neq 0$. This implies that S is symmetric. As S has no unique difference, we have $p \leq 3^{|S|/2}$ by Theorem 1.2.6. As $|S| \leq n$, we conclude $p \leq 3^{n/2}$, contradicting the assumptions. $\square$

Remark 3.6.3. Under the same notations as in Theorem 3.6.2, the previously known conditions for $Y\eta \in \mathbb{Z}[\zeta_r]$ are $\text{ord}_p(q)$ being even and $p > \max\{2^n, n^2 + n + 1\}$. Theorem 3.6.2 is an improvement of this result.

Example Let $p = 107$, $q = 2$, and $n = 8$ in Theorem 3.6.2. Note that $\text{ord}_p(2)$ is even and that $p > \max\{3^{n/2}, n^2 + n + 1\}$. Thus, for any odd prime $r \neq 107$ and $Y \in \mathbb{Z}[\zeta_{107r}]$ with $|Y|^2 = 8$, we have $Y\eta \in \mathbb{Z}[\zeta_r]$ for some root of unity η .

3.7 Concluding Remarks

In this chapter, we study $g(p)$ - the smallest cardinality of a symmetric subset of $\mathbb{F}_p$ which has no unique difference. Combining Theorem 1.2.6 and Result 3.1.2, we obtain (asymptotically)

$$2 \log_3(p) < g(p) \leq (2 + o(1)) \log_3(p).$$

Furthermore, our main result, Theorem 1.2.6, on the lower bound for $g(p)$ is applied to improve an existing result on Weil numbers, Theorem 3.6.2.

To the end of this chapter, we propose several open questions and future research in this direction. The first question is proposed by Feit [53].

Problem 3.7.1. *Given a prime p , what is the largest number $f(p)$ such that every subset of $\mathbb{F}_p$ with at most $f(p)$ elements has a unique difference?*

We remark that the results by Straus [53] and Browkin et al. [10] give an asymptotic bound for $f(p)$ as follows.

$$\log_2(p) \leq f(p) \leq (2 + o(1)) \log_3(p).$$

It remains an open question to find a lower bound better than $\log_2(p)$ for $f(p)$.

Another problem similar to the unique difference problem is the **balanced set** problem.

Problem 3.7.2. *A subset A of $\mathbb{F}_p$ is called a balanced set if for any element $a \in A$, there exist $b, c \in A \setminus \{a\}$ such that $2a = b + c$. Find the smallest positive integer $h(p)$ such that there exists a balanced subset A of $\mathbb{F}_p$ of size $h(p)$.*

For the balanced set problem, a combination of results by Nedev [42] and Straus [53] asymptotically give

$$\log_2(p) \leq h(p) \leq (2 + o(1)) \log_3(p).$$

Numerical evidence suggests that $h(p) \approx \log_2(p) + c$ for some constant c . However, this question remains open.

Problem 3.7.3. *Study the unique difference problem and the balanced set problem in other settings, for instance, in a finite field or in a group.*

Chapter 4

Upper Bounds for Cyclotomic Numbers

4.1 Introduction and Definitions

First, we fix some notation and definitions which will be used throughout this chapter. By q we denote a power of a prime p . Let e and k be nontrivial divisors of $q - 1$ such that $q = ek + 1$. Let g be a primitive element of the finite field $\mathbb{F}_q$. For each $a \in \mathbb{Z}$, write

$$C_a = \{g^a, g^{a+e}, \dots, g^{a+(k-1)e}\}. \quad (4.1)$$

As $C_a = C_{a+e}$, we only need to consider the sets C_a with $a \in \{0, 1, \dots, e-1\}$.

Definition 4.1.1. For $a, b \in \{0, 1, \dots, e-1\}$, define (a, b) as the number of solutions to the equation

$$1 + x = y, \quad x \in C_a, \quad y \in C_b.$$

Equivalently, this is the number of pairs (r, s) with $0 \leq r, s \leq k-1$ such that

$$1 + g^{a+re} = g^{b+se}. \quad (4.2)$$

The number (a, b) is called a **cyclotomic number** of order e .

Cyclotomic numbers have been studied for decades by many authors, as they have applications in various areas. These numbers can be used to compute Jacobi sums, and vice versa, see [1]. Vandiver [33], [55], [56], [57], [58] related cyclotomic numbers to Fermat's Last Theorem and proved the theorem for exponents ≤ 2000 . Cyclotomic classes C_a were used by Paley [44] in 1933 to construct difference sets. This approach

was later employed by many other authors. Storer's book [52] summarizes the results in this direction up to 1967. In the 1960s to 1980s, Baumert [3], Evans [24], Lehmer [34], Whiteman [61, 62, 63], et al. explicitly determined all cyclotomic numbers (a, b) of orders $e \leq 12$ and $e = 14, 15, 16, 18, 20, 24$. See [4, p.152] for more details.

Under asymptotic conditions, cyclotomic numbers exhibit interesting uniform behaviour. Katre [30] proved that, for fixed e and $q \rightarrow \infty$, we have $(a, b) \approx q/e^2$ for all $a, b \in \mathbb{Z}$. On the other hand, fixing k , it was proved by Betsumiya et al. [5] that $(0, 0) \leq 2$ if p is sufficiently large compared to k . In [5], the condition "sufficiently large" is not explicitly specified and, in fact, the lower bound on p required for their method is difficult to write down explicitly. Our goal in this problem is to find a simple and improved lower bound on p which guarantees that all cyclotomic numbers (a, b) are small. The following is our main result.

Theorem 4.1.2. *Let q be a power of a prime p . Let e and k be nontrivial divisors of $q - 1$ such that $q = ek + 1$. If*

$$p > \left(\sqrt{14}\right)^{k/\text{ord}_k(p)},$$

then $(a, b) \leq 3$ for all $a, b \in \mathbb{Z}$.

If k is a prime, we obtain a better bound as follows.

Theorem 4.1.3. *Let q be a power of a prime p . Let e and k be nontrivial divisors of $q - 1$ such that k is a prime and $q = ek + 1$. If*

$$p > (3^{k-1}k)^{1/\text{ord}_k(p)},$$

then

$$(a, b) \leq 2 \text{ for all } a, b \in \mathbb{Z}.$$

We continue with introducing some notation and results we need later. A square matrix is called **circulant** if each of its rows (except the first) is obtained from the previous row by shifting the entries one position to the right and moving the last entry to the front. Moreover, given a matrix H , we denote the conjugate transpose of H by H^* . The following result about eigenvalues and eigenvectors of a circulant matrix is well known, see [15], for example.

Result 4.1.4. *Let k be a positive integer and let M be a circulant matrix with the first row $(a_0, \dots, a_{k-1})$ where $a_0, \dots, a_{k-1} \in \mathbb{C}$. Then the eigenvalues and eigenvectors of M are*

$$\lambda_i = \sum_{j=0}^{k-1} a_j \zeta_k^{ij} \text{ and } X_i = (1, \zeta_k^i, \dots, \zeta_k^{i(k-1)})^T, \quad 0 \leq i \leq k-1.$$

In the next section, we review some results on vanishing sums of roots of unity which will be needed for our study. The following terminology was used in [13]. Let T be a finite set of complex roots of unity and let c_α , $\alpha \in T$, be nonzero rational numbers. The sum

$$S = \sum_{\alpha \in T} c_\alpha \alpha, \quad c_\alpha \in \mathbb{Q} \setminus \{0\},$$

is called a **vanishing sum** of roots of unity if $S = 0$. We say that S is **nonempty** if $T \neq \emptyset$. The **length** $l(S)$ is the cardinality of T . The **exponent** $e(S)$ denotes the least common multiple of all orders of the roots of unity $\alpha \in T$. We say that S is **similar** to any sum of the form $k \cdot \beta S'$, where $k \in \mathbb{Q} \setminus \{0\}$ and β is a root of unity and S' has the form

$$S' = \sum_{\alpha \in T} (\varepsilon_\alpha c_\alpha) (\varepsilon_\alpha \alpha), \quad \text{where } \varepsilon_\alpha \in \{1, -1\}.$$

We call the vanishing sum S **minimal** if S contains no vanishing subsum. The sum S is a **reduced sum** if $\alpha = 1$ for some $\alpha \in T$.

4.2 Vanishing Sums of Roots of Unity

The following result states that a minimal vanishing sum of roots of unity is equivalent to a vanishing sum whose order is squarefree, see [31, Corollary 3.2] or [13, Theorem 1] for a proof.

Result 4.2.1. *If $S = \alpha_1 + \cdots + \alpha_n$ is a minimal vanishing sum of m th roots of unity, then after multiplying S by a suitable m th root of unity, we may assume that all α_i 's are m_0 th roots of unity, where m_0 is the largest square-free divisor of m .*

The next result is part of [13, Theorem 6] and will be useful for our study. We include a proof for the convenience of the reader.

Result 4.2.2. *Let S be a nonempty vanishing sum of length at most 6 that does not contain a subsum similar to $1 + (-1)$. Then either S contains subsums each of which is similar to $1 + \zeta_3 + \zeta_3^2$, or S is similar to one of the sums*

$$\begin{aligned} &1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4, \quad \text{or} \\ &-\zeta_3 - \zeta_3^2 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4. \end{aligned}$$

Proof. First, suppose that S is minimal. Since S contains no vanishing subsum and S is nonempty, we can assume, by Result 4.2.1 and by dividing S by a root of unity if necessary, that S is a reduced sum and $e(S)$ is square-free. For an odd integer m , we write ζ_{2m} as $(-1) \cdot \zeta_m^{(m+1)/2}$. Hence we can assume that $e(S)$ is odd using this convention. Note that $e(S) \neq 1$ because S is not similar to $1 + (-1)$. Next, let p be the largest prime divisor of $e(S)$ and write $S = \sum_{i=0}^{p-1} S_i \zeta_p^i$, where each S_i has exponent coprime to p . Note that $1 \in S_0$ because S is a reduced sum. Since $S = 0$ and S is minimal, we have $S_0 = S_1 = \dots = S_{p-1} \neq 0$. Hence $p \in \{3, 5\}$, as $l(S) = \sum_{i=0}^{p-1} l(S_i) \leq 6$. If $p = 3$, then $e(S) = 3$ and S involves only $1, \zeta_3, \zeta_3^2$, so it is similar to $1 + \zeta_3 + \zeta_3^2$.

Suppose that $p = 5$. Since $l(S) = \sum_{i=0}^4 l(S_i) \leq 6$ and $S_i \neq 0$ for all i , we have either

- (i) $l(S_i) = 1$ for all i , or
- (ii) $l(S_j) = 2$ for exactly one $j \in \{0, \dots, 4\}$ and $l(S_i) = 1$ for any $i \neq j$.

Note that $e(S_i)$ is square-free, odd and has the biggest prime divisor smaller than 5, so $e(S_i) \in \{1, 3\}$. In the case $l(S_i) = 1$ for all i , we obtain $S_i = 1$ for all i , as S_0 contains 1 and $S_0 = \dots = S_4$. Hence $S = \sum_{i=0}^4 \zeta_5^i$. Now suppose that $l(S_j) = 2$ for exactly one $j \in \{0, \dots, 4\}$ and $l(S_i) = 1$ for all the remaining $i \neq j$. As $e(S_i) \in \{1, 3\}$, we obtain $S_i \in \{\pm 1, \pm \zeta_3^a\}$, where $a \in \{1, 2\}$, for all $i \neq j$. Moreover since $S_j - S_i = 0$ and $l(S_j) = 2$, we obtain $S_j \in \{\mp(\zeta_3 + \zeta_3^2), \mp(1 + \zeta_3^b)\}$, where $\{b\} = \{1, 2\} \setminus \{a\}$. In this case, S is similar to $-\zeta_3 - \zeta_3^2 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4$.

Lastly, consider the case S is not minimal. Any minimal vanishing subsum of S has been shown to satisfy the theorem. Since $l(S) \leq 6$, each minimal vanishing subsum of S is similar to $1 + \zeta_3 + \zeta_3^2$. $\square$

4.3 Bounds on Norms of Cyclotomic Integers

A **cyclotomic integer** (not to be confused with a cyclotomic number) is an algebraic integer in a cyclotomic field. Every cyclotomic integer can be written as a sum of complex roots of unity. The improvements over the previously known results we obtain arise from new bounds on absolute norms of cyclotomic integers. First, we discuss a general norm bound.

Note that every cyclotomic integer in $\mathbb{Q}(\zeta_k)$ can be written as $f(\zeta_k)$, where $f(x) = \sum_{i=0}^{k-1} a_i x^i$ is a polynomial with integer coefficients. Since $|f(\zeta_k^j)| \leq \sum_{i=0}^{k-1} |a_i|$, an obvious

bound for the absolute norm of $f(\zeta_k)$ is

$$|N(f(\zeta_k))| = \left| \prod_{j: \gcd(j,k)=1} f(\zeta_k^j) \right| \leq \left(\sum_{i=0}^{k-1} |a_i| \right)^{\varphi(k)}. \quad (4.3)$$

In this section, we provide some stronger bounds that are suitable for the applications to cyclotomic numbers we are interested in. We note that the following bound essentially appeared in Lemma 2.3.6. We state and prove an improved version of this bound below.

Theorem 4.3.1. *Let k be a positive integer, let $f(x) = \sum_{i=0}^{k-1} a_i x^i \in \mathbb{Z}[x]$ and let N denote the absolute norm of $\mathbb{Q}(\zeta_k)$. Then*

$$|N(f(\zeta_k))| \leq \left(\frac{k \left(\sum_{i=0}^{k-1} a_i^2 \right) - \left(\sum_{i=0}^{k-1} a_i \right)^2}{\varphi(k)} \right)^{\varphi(k)/2}. \quad (4.4)$$

In particular, if $\sum_{i=0}^{k-1} a_i^2 \geq 3$, then

$$|N(f(\zeta_k))| \leq \left(\sum_{i=0}^{k-1} a_i^2 \right)^{k/2}. \quad (4.5)$$

Proof. We have

$$\sum_{h=0}^{k-1} |f(\zeta_k^h)|^2 = \sum_{i,j,h=0}^{k-1} a_i a_j \zeta_k^{(i-j)h} = k \sum_{i=0}^{k-1} a_i^2.$$

By the inequality between arithmetic and geometric means, we have

$$\begin{aligned} |N(f(\zeta_k))| &= \left| \prod_{(h,k)=1} f(\zeta_k^h) \right| \leq \left(\frac{\sum_{(h,k)=1} |f(\zeta_k^h)|^2}{\varphi(k)} \right)^{\varphi(k)/2} \\ &\leq \left(\frac{\sum_{h=0}^{k-1} |f(\zeta_k^h)|^2 - |f(\zeta_k^0)|^2}{\varphi(k)} \right)^{\varphi(k)/2} \\ &= \left(\frac{k \left(\sum_{i=0}^{k-1} a_i^2 \right) - \left(\sum_{i=0}^{k-1} a_i \right)^2}{\varphi(k)} \right)^{\varphi(k)/2}, \end{aligned}$$

proving (4.4).

Now assume that $S = \sum_{i=0}^{k-1} a_i^2 \geq 3$. Consider function $g(x) = (kS/x)^{x/2}$ on interval $[1, k]$. We have $g'(x) = (kS/x)^{x/2} (\ln(kS/x)/2 - 1/2) > 0$ for $x \in [1, k]$, so $g(x)$ is increasing on $[1, k]$. We obtain

$$|N(f(\zeta_k))| \leq g(\varphi(k)) \leq g(k) = S^{k/2}.$$

□

In the case k is a prime, we obtain a different bound on the norm of $f(\zeta_k)$ in the next theorem. This bound is better than (4.4) in certain situations.

For the rest of this section, we assume that k is a prime. For $f(x) = \sum_{i=0}^{k-1} a_i x^i$, let M denote the circulant matrix with first row $(a_0, \dots, a_{k-1})$ and let N denote the $(k-1) \times (k-1)$ matrix obtained from M by deleting its first row and its first column. To find an upper bound for $|N(f(\zeta_k))|$, we first find a relation between $N(f(\zeta_k))$ and $\det(M)$ or $\det(N)$. Then an upper bound for $|\det(M)|$ or $|\det(N)|$ will give us an upper bound for $|N(f(\zeta_k))|$.

Bounds for the determinant of a matrix are abundant in the literature. We only need the following result by Schinzel [48].

Result 4.3.2. *Let $N = (a_{ij})_{i,j=0}^{n-1}$ be an $n \times n$ matrix with real entries. For $i = 0, 1, \dots, n-1$, write $N_i^+ = \sum_{j=0}^{n-1} \max\{0, a_{ij}\}$ and $N_i^- = \sum_{j=0}^{n-1} \max\{0, -a_{ij}\}$. We have*

$$|\det(N)| \leq \prod_{i=0}^{n-1} \max\{N_i^+, N_i^-\}. \quad (4.6)$$

Proposition 4.3.3. *Using the notation introduced above, we have the following*

(a) *If $\sum_{i=0}^{k-1} a_i \neq 0$, then*

$$N(f(\zeta_k)) = \frac{\det(M)}{\sum_{i=0}^{k-1} a_i}. \quad (4.7)$$

(b) *If $\sum_{i=0}^{k-1} a_i = 0$, then*

$$N(f(\zeta_k)) = k \det(N). \quad (4.8)$$

Proof. For each $0 \leq i \leq k-1$, define a column vector

$$X_i = \frac{1}{\sqrt{k}}(1, \zeta_k^i, \zeta_k^{2i}, \dots, \zeta_k^{(k-1)i})^T.$$

By Result 4.1.4, the eigenvalues of M are $\lambda_i = f(\zeta_k^i)$ and the corresponding eigenvectors are X_i , $0 \leq i \leq k-1$. Since k is a prime, we have

$$N(f(\zeta_k)) = \prod_{i=1}^{k-1} f(\zeta_k^i) = \prod_{i=1}^{k-1} \lambda_i. \quad (4.9)$$

Note that $\det(M) = \prod_{i=0}^{k-1} \lambda_i$. If $\lambda_0 = \sum_{i=0}^{k-1} a_i \neq 0$, then (4.7) is clear.

Suppose that $\lambda_0 = 0$. Note that $X_i^* X_j = 1$ if $i = j$ and $X_i^* X_j = 0$ if $i \neq j$. Let Q be the $k \times k$ matrix with columns $X_0, \dots, X_{k-1}$, then Q^{-1} is the $k \times k$ matrix with rows $X_0^*, \dots, X_{k-1}^*$. We have

$$M = Q \begin{pmatrix} \lambda_0 & & & \\ & \lambda_1 & & \\ & & \ddots & \\ & & & \lambda_{k-1} \end{pmatrix} Q^{-1}.$$

By the definition of N , we have

$$N = Q_1 \begin{pmatrix} \lambda_0 & & & \\ & \lambda_1 & & \\ & & \ddots & \\ & & & \lambda_{k-1} \end{pmatrix} Q_1',$$

where Q_1 is the $(k-1) \times k$ matrix formed by the last $k-1$ rows of Q and Q_1' is the $k \times (k-1)$ matrix formed by the last $k-1$ columns of Q^{-1} . Since $\lambda_0 = 0$, we have

$$N = Q_2 \begin{pmatrix} \lambda_1 & & & \\ & \ddots & & \\ & & & \lambda_{k-1} \end{pmatrix} Q_2',$$

where Q_2 is the $(k-1) \times (k-1)$ matrix formed by the last $k-1$ columns of Q_1 and Q_2' is the matrix formed by the last $k-1$ rows of Q_1' . We obtain

$$\det(N) = \det(Q_2 Q_2') \prod_{i=1}^{k-1} \lambda_i.$$

By (4.9), the equation (4.8) is equivalent to $\det(Q_2 Q_2') = 1/k$. Note that $(Q_2')_{ij} = \overline{(Q_2)_{ij}}$ for any i, j , as Q_2 and Q_2' are submatrices of Q and Q^{-1} , respectively. More precisely, we have

$$Q_2 = \frac{1}{\sqrt{k}} \begin{pmatrix} \zeta_k & \zeta_k^2 & \cdots & \zeta_k^{k-1} \\ \zeta_k^2 & \zeta_k^4 & \cdots & \zeta_k^{2(k-1)} \\ & & \ddots & \\ \zeta_k^{k-1} & \zeta_k^{2(k-1)} & \cdots & \zeta_k^{(k-1)(k-1)} \end{pmatrix}.$$

The (i, j) th entry of $Q_2 Q_2'$ is

$$\frac{1}{k} \sum_{t=1}^{k-1} \zeta_k^{(i-j)t} = \begin{cases} (k-1)/k & \text{if } i = j \\ -1/k & \text{if } i \neq j \end{cases}.$$

Hence $Q_2 Q_2'$ is a circulant matrix of size $(k-1) \times (k-1)$ with the first row $((k-1)/k, -1/k, \dots, -1/k)$. By Result 4.1.4, the eigenvalues of $Q_2 Q_2'$ are

$$\beta_j = \frac{1}{k} \left(k-1 - \sum_{i=1}^{k-2} \zeta_{k-1}^{ij} \right) = \begin{cases} 1/k & \text{if } j = 0, \\ 1 & \text{if } 1 \leq j \leq k-2. \end{cases}$$

We thus obtain

$$\det(Q_2 Q_2') = \prod_{j=0}^{k-2} \beta_j = 1/k.$$

□

Combining Result 4.3.2 and Proposition 4.3.3, we get the following norm bound, which in numerous cases is stronger than Theorem 4.3.1.

Corollary 4.3.4. *Let k be a prime and let $f(x) = \sum_{i=0}^{k-1} a_i x^i \in \mathbb{Z}[x]$. Write $A^+ = \sum_{j=0}^{n-1} \max\{0, a_j\}$, $A^- = \sum_{j=0}^{n-1} \max\{0, -a_j\}$, and $A = \max\{A^+, A^-\}$.*

(a) *If $\sum_{i=0}^{k-1} a_i \neq 0$, then*

$$|N(f(\zeta_k))| \leq \frac{A^k}{|\sum_{i=0}^{k-1} a_i|}.$$

(b) *If $\sum_{i=0}^{k-1} a_i = 0$, then*

$$|N(f(\zeta_k))| \leq k A^{k-1}.$$

4.4 Equations over $\mathbb{F}_q$ and $\mathbb{C}$

The following theorem shows that under some condition on the characteristic of the finite field $\mathbb{F}_q$, we can transform certain equations over $\mathbb{F}_q$ to equations over the field of complex numbers $\mathbb{C}$, and vice versa.

Theorem 4.4.1. *Let q be a power of a prime p and let e, k be nontrivial divisors of $q-1$ such that $q = ek+1$. Let g be a primitive element of $\mathbb{F}_q$ and let $f(x) = \sum_{i=0}^{k-1} a_i x^i \in \mathbb{Z}[x]$. Suppose that*

$$p > \left(\frac{k \left(\sum_{i=0}^{k-1} a_i^2 \right) - \left(\sum_{i=0}^{k-1} a_i \right)^2}{\varphi(k)} \right)^{\frac{\varphi(k)}{2 \operatorname{ord}_k(p)}}, \quad (4.10)$$

then $f(g^e) = 0$ over $\mathbb{F}_q$ if and only if $f(\zeta_k) = 0$ over $\mathbb{C}$.

In particular, the same conclusion holds if $\sum_{i=0}^{k-1} a_i^2 \geq 3$ and

$$p > \left(\sum_{i=0}^{k-1} a_i^2 \right)^{\frac{k}{2 \operatorname{ord}_k(p)}}. \quad (4.11)$$

Proof. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\zeta_k]$ that contains p . Write $q = p^n$ and $b = \operatorname{ord}_k(p)$. Note that b divides n because $q = p^n \equiv 1 \pmod{k}$. Since $\mathbb{Z}[\zeta_k]/\mathfrak{p}$ is a finite field extension of $\mathbb{Z}/p\mathbb{Z}$ of order b , we have $\mathbb{Z}[\zeta_k]/\mathfrak{p} \cong \mathbb{F}_{p^b}$. Let $\phi : \mathbb{F}_{p^b} \rightarrow \mathbb{Z}[\zeta_k]/\mathfrak{p}$ be an isomorphism. Note that g^e is a primitive k th root of unity in $\mathbb{F}_{p^b}$, so $\phi(g^e)$ is also a primitive k th root of unity in $\mathbb{Z}[\zeta_k]/\mathfrak{p}$, which implies $\phi(g^e) = \zeta_k^j + \mathfrak{p}$ for some integer j coprime to k . We have

$$f(g^e) = 0 \text{ over } \mathbb{F}_q \Leftrightarrow \phi(f(g^e)) = f(\zeta_k^j) + \mathfrak{p} = 0 \text{ in } \mathbb{Z}[\zeta_k]/\mathfrak{p} \Leftrightarrow f(\zeta_k^j) \in \mathfrak{p}. \quad (4.12)$$

Suppose that $f(\zeta_k) = 0$ over $\mathbb{C}$. We have $f(\zeta_k^j) = 0$, as j is coprime to k . By (4.12), $f(g^e) = 0$ over $\mathbb{F}_q$. Now assume that $f(g^e) = 0$ over $\mathbb{F}_q$. Note that $N(\mathfrak{p}) = p^b$, where by $N(\mathfrak{p})$ we mean the norm of the ideal $\mathfrak{p}$ in $\mathbb{Z}[\zeta_k]$. By (4.12), we have $N(f(\zeta_k^j)) \equiv 0 \pmod{p^b}$. As j is coprime to k , we have $N(f(\zeta_k^j)) = N(f(\zeta_k))$. Thus

$$N(f(\zeta_k)) \equiv 0 \pmod{p^b}. \quad (4.13)$$

On the other hand, by Theorem 4.3.1 we have

$$|N(f(\zeta_k))| \leq \left(\frac{k \left(\sum_{i=0}^{k-1} a_i^2 \right) - \left(\sum_{i=0}^{k-1} a_i \right)^2}{\varphi(k)} \right)^{\varphi(k)/2}. \quad (4.14)$$

If $f(\zeta_k) \neq 0$, then $N(f(\zeta_k)) \neq 0$ and (4.13), (4.14) imply

$$p^b \leq \left(\frac{k \left(\sum_{i=0}^{k-1} a_i^2 \right) - \left(\sum_{i=0}^{k-1} a_i \right)^2}{\varphi(k)} \right)^{\varphi(k)/2},$$

contradicting (4.10). Therefore, $f(\zeta_k) = 0$.

Lastly, the conclusion for the case $\sum_{i=0}^{k-1} a_i^2 \geq 3$ follows from (4.5). $\square$

The next theorem follows from Corollary 4.3.4 in the same way as Theorem 4.4.1 follows from Theorem 4.3.1, so we skip the proof.

Theorem 4.4.2. *Let q be a power of a prime p and let e, k be nontrivial divisors of $q - 1$ such that $q = ek + 1$ and k is a prime. Let g be a primitive element of $\mathbb{F}_q$ and let $f(x) = \sum_{i=0}^{k-1} a_i x^i \in \mathbb{Z}[x]$. Write $A^+ = \sum_{j=0}^{n-1} \max\{0, a_j\}$, $A^- = \sum_{j=0}^{n-1} \max\{0, a_j\}$, and $A = \max\{A^+, A^-\}$. Suppose that one of the following conditions holds.*

(a) $\sum_{i=0}^{k-1} a_i \neq 0$ and

$$p^{\text{ord}_k(p)} > \frac{A^k}{|\sum_{i=0}^{k-1} a_i|}. \quad (4.15)$$

(b) $\sum_{i=0}^{k-1} a_i = 0$ and

$$p^{\text{ord}_k(p)} > kA^{k-1}. \quad (4.16)$$

Then we have $f(g^e) = 0$ over $\mathbb{F}_q$ if and only if $f(\zeta_k) = 0$ over $\mathbb{C}$.

4.5 Upper Bounds for Cyclotomic Numbers

In this section, we apply Theorem 4.4.1 to derive upper bounds for cyclotomic numbers (a, b) . In Theorem 4.3.1, the upper bound $(k/\varphi(k) \sum a_i^2)^{\varphi(k)/2}$ is largest when $\varphi(k)$ is approximately k . Thus, in this case, and in particular when k is a prime, an improved bound is desirable. Theorem 4.4.2 will come into play in this situation and we will discuss this case separately in the last section.

Note that $(a, b) = (a', b')$ whenever $a \equiv a' \pmod{e}$ and $b \equiv b' \pmod{e}$. From now on, we always assume that $a, b \in \{0, 1, \dots, e-1\}$. First, we recall the main result of this section.

Theorem 4.5.1. *Let q be a power of a prime p . Let e and k be nontrivial divisors of $q - 1$ such that $q = ek + 1$. If*

$$p > \left(\sqrt{14}\right)^{k/\text{ord}_k(p)}, \quad (4.17)$$

then

$$(a, b) \leq 3 \text{ for all } a, b \in \mathbb{Z}. \quad (4.18)$$

Our proof for this theorem is divided into five cases: We separately investigate cyclotomic numbers $(0, 0)$, $(0, a)$, $(a, 0)$, (a, a) and (a, b) where $a \neq b$ and $a, b \in \{1, \dots, e-1\}$. In fact, in each case, we obtain a stronger result than Theorem 4.5.1, which is just a simplified consequence of the analysis of the different cases.

Theorem 4.5.2. *If*

$$p > \left(\frac{3k-1}{\varphi(k)} \right)^{\frac{\varphi(k)}{2 \operatorname{ord}_k(p)}}, \quad (4.19)$$

then

$$(0, 0) = \begin{cases} 0 & \text{if } k \not\equiv 0 \pmod{6} \text{ and } 2 \notin C_0, \\ 1 & \text{if } k \not\equiv 0 \pmod{6} \text{ and } 2 \in C_0, \\ 2 & \text{if } k \equiv 0 \pmod{6} \text{ and } 2 \notin C_0, \\ 3 & \text{if } k \equiv 0 \pmod{6} \text{ and } 2 \in C_0. \end{cases} \quad (4.20)$$

Proof. Suppose that there are $0 \leq a, b \leq k-1$ with $1 + g^{ae} = g^{be}$. Then $2 \in C_0$ if $a = 0$. Thus in the case $2 \in C_0$, there is one solution to $1 + g^{ae} = g^{be}$ in which $a = 0$.

From now on, suppose that $a \neq 0$ and $1 + g^{ae} = g^{be}$. We have $b \notin \{0, a\}$ and $f(x) = 1 + x^a - x^b$ is a polynomial of degree at most $k-1$ with two coefficients 1, one coefficient -1 and all other coefficients 0. Write $f(x) = \sum_{i=0}^{k-1} a_i x^i$, then $\sum_{i=0}^{k-1} a_i^2 = 3$, $\sum_{i=0}^{k-1} a_i = 1$ and $f(g^e) = 0$. By (4.19) and Theorem 4.4.1, we have

$$f(\zeta_k) = 1 + \zeta_k^a - \zeta_k^b = 0.$$

By Result 4.2.2, we obtain $1 + \zeta_k^a - \zeta_k^b = 1 + \zeta_3 + \zeta_3^2$, which happens only when $6 \mid k$ and $(a, b) \in \{(k/3, k/6), (2k/3, 5k/6)\}$, proving (4.20). $\square$

Note that by (4.11), Theorem 4.5.2 still holds when (4.19) is replaced by $p > 3^{k/(2 \operatorname{ord}_k(p))}$. This shows that Theorem 4.5.1 holds in the case $(a, b) = (0, 0)$.

We mentioned in the introduction that Vandiver has used cyclotomic numbers to obtain results on Fermat's Last Theorem. The next Corollary gives an example for this kind of argument. Considering the Diophantine equation $x^e + y^e = z^e$ modulo p , Theorem 4.5.2 implies the following.

Corollary 4.5.3. *If p is a prime with $p = ek + 1 > 3^{k/2}$ and $k \not\equiv 0 \pmod{6}$, then $x^e + y^e = z^e$ with $x, y, z \in \mathbb{Z}$, implies that either 2 is an e th power modulo p or $xyz \equiv 0 \pmod{p}$.*

For example, let $p = 1301 = 100 \cdot 13 + 1$ and let $e = 100, k = 13$. Note that 2 is not a 100th power modulo 1301. Therefore, if $x^{100} + y^{100} \equiv z^{100} \pmod{1301}$, then $xyz \equiv 0 \pmod{1301}$.

Theorem 4.5.4. *Let $a \in \{1, \dots, e-1\}$. If*

$$p > \left(\frac{4k}{\varphi(k)} \right)^{\frac{\varphi(k)}{2 \operatorname{ord}_k(p)}}, \quad (4.21)$$

then

$$(0, a) \leq \begin{cases} 3 & \text{if } 2 \in C_a, \\ 2 & \text{if } 2 \notin C_a. \end{cases} \quad (4.22)$$

Proof. Note that $1 + g^{ie} = g^{je+a}$ implies $1 + g^{-ie} = g^{(j-i)e+a}$, so each solution (i, j) to $1 + g^{ie} = g^{je+a}$ induces a solution $(-i, j-i)$ (calculation is modulo k) to the same equation, two of which are different if and only if $i \neq 0$. Moreover if $i = 0$, then $2 = g^{je+a} \in C_a$ and there is one solution to $1 + g^{ie} = g^{je+a}$ in which $i = 0$.

Suppose that $2 \in C_a$ and $(0, a) \geq 4$. There are two different pairs $(i_1, j_1), (i_2, j_2)$ with

$$i_1 \neq 0, i_2 \neq 0, (i_2, j_2) \neq (-i_1, j_1 - i_1) \text{ and } (i_1, j_1) \neq (-i_2, j_2 - i_2) \quad (4.23)$$

such that $1 + g^{i_1 e} = g^{j_1 e+a}$ and $1 + g^{i_2 e} = g^{j_2 e+a}$. We obtain

$$1 + g^{i_1 e} - g^{(j_1-j_2)e} - g^{(j_1-j_2+i_2)e} = 0. \quad (4.24)$$

In (4.24), the numbers $0, i_1, j_1 - j_2$ and $j_1 - j_2 + i_2$ are pairwise different. Indeed, by (4.23), we need only to show that $i_1 \neq j_1 - j_2 + i_2$. If $i_1 - i_2 = j_1 - j_2$, then by subtracting two equations $1 + g^{i_1 e} = g^{j_1 e+a}$ and $1 + g^{i_2 e} = g^{j_2 e+a}$, we obtain $g^{i_2 e}(g^{(i_1-i_2)e} - 1) = g^{j_2 e+a}(g^{(j_1-j_2)e} - 1)$, which implies $g^{i_2 e} = g^{j_2 e+a}$, a contradiction as $C_0 \cap C_a = \emptyset$.

By (4.21) and Theorem 4.4.1, the equation (4.24) implies

$$1 + \zeta_k^{i_1} - \zeta_k^{j_1-j_2} - \zeta_k^{j_1-j_2+i_2} = 0.$$

By Result 4.2.2, this is possible only when the sum on left-hand side cancels in pairs. This happens only when “ $2 \mid k$ and $i_1 = i_2 = k/2$ ” or “ $j_1 = j_2$ and $i_1 = i_2$ ”, both of which are not possible. Therefore, we obtain $(0, a) \leq 3$ if $2 \in C_a$.

Next, suppose that $2 \notin C_a$ and $(0, a) \geq 3$. Note that for any $0 \leq i, j \leq k-1$ with $1 + g^{ie} = g^{je+a}$, we have $i \neq 0$. There exist two pairs (i_1, j_1) and (i_2, j_2) with

$$i_1 \neq 0, i_2 \neq 0, (i_2, j_2) \neq (-i_1, j_1 - i_1) \text{ and } (i_1, j_1) \neq (-i_2, j_2 - i_2)$$

such that $1 + g^{i_1 e} = g^{j_1 e+a}$ and $1 + g^{i_2 e} = g^{j_2 e+a}$. We obtain a contradiction by the same argument as in the previous case. $\square$

Theorem 4.5.5. *Let $a \in \{1, \dots, e-1\}$. If*

$$p > \left(\frac{4k}{\varphi(k)} \right)^{\frac{\varphi(k)}{2 \operatorname{ord}_k(p)}}, \quad (4.25)$$

then

$$(a, 0) \leq \begin{cases} 3 & \text{if } 2 \in C_a \text{ and } 2 \mid k, \\ 2 & \text{if } 2 \notin C_a \text{ and } 2 \mid k, \\ 2 & \text{if } 2 \nmid k. \end{cases} \quad (4.26)$$

Proof. First, assume that k is even. If $1 + g^{ie+a} = g^{je}$, then $1 + g^{(k/2+j)e} = g^{(k/2+i)e+a}$, as $g^{ek/2} = -1$. This implies $(a, 0) = (0, a)$ and the conclusion follows from Theorem 4.5.4.

From now on, we assume that k is odd and $(a, 0) \geq 3$. For $t = 1, 2, 3$, let (i_t, j_t) be three different pairs with $0 \leq i_t, j_t \leq k-1$ and $1 + g^{i_te+a} = g^{j_te}$ for $t = 1, 2, 3$. First, note that $j_t \neq 0$ for all t because $0 \notin C_a$. Moreover, we obtain the following two equations which result from $1 + g^{i_te+a} = g^{j_te}$ for $t = 1, 2, 3$.

$$1 - g^{j_1e} - g^{(i_1-i_2)e} + g^{(i_1-i_2+j_2)e} = 0, \text{ and} \quad (4.27)$$

$$1 - g^{j_1e} - g^{(i_1-i_3)e} + g^{(i_1-i_3+j_3)e} = 0. \quad (4.28)$$

Suppose that there are four distinct terms in one of the equations above, assume that is (4.27). By (4.25) and Theorem 4.4.1, we have

$$1 - \zeta_k^{j_1} - \zeta_k^{i_1-i_2} + \zeta_k^{i_1-i_2+j_2} = 0.$$

By Result 4.2.2, the left-hand-side sum cancels in pairs, which is impossible because k is odd and all terms in the sum are distinct. Thus, we cannot have all four terms different in both (4.27) and (4.28). In (4.27), we have either $i_1 - i_2 = j_1$ or $i_1 - i_2 + j_2 = 0$. In (4.28), we have either $i_1 - i_3 = j_1$ or $i_1 - i_3 + j_3 = 0$. Due to the difference between three pairs (i_t, j_t) , $t = 1, 2, 3$, we can only have two cases: $i_1 - i_2 = j_1$ and $i_1 - i_3 + j_3 = 0$, or $i_1 - i_2 + j_2 = 0$ and $i_1 - i_3 = 0$. The following argument works the same for both cases. Assuming that the first case happens, we have, by (4.27) and (4.28),

$$1 - 2g^{j_1e} + g^{(j_1+j_2)e} = 0 \text{ and } 2 - g^{j_1e} - g^{-j_3e} = 0,$$

or equivalently

$$2 - g^{-j_1e} - g^{j_2e} = 0 \text{ and } 2 - g^{j_1e} - g^{-j_3e} = 0. \quad (4.29)$$

Hence $g^{-j_1e} + g^{j_2e} - g^{j_1e} - g^{-j_3e} = 0$, which implies

$$1 + g^{(j_1+j_2)e} - g^{2j_1e} - g^{(j_1-j_3)e} = 0. \quad (4.30)$$

We claim that the numbers $0, j_1 + j_2, 2j_1, j_1 - j_3$ are pairwise different. As j_1, j_2, j_3 are pairwise different, the claim is equivalent to $2j_1 \neq 0$, $j_1 + j_2 \neq 0$, $j_2 + j_3 \neq 0$ and $j_1 + j_3 \neq 0$. Firstly, k odd and $j_1 \neq 0$ implies $2j_1 \neq 0$. Secondly, if $j_1 + j_2 = 0$, then the first equation in (4.29) implies $2 - 2g^{-j_1e} = 0$, so $j_1 = 0$ (note that $p > 2$ by (4.25)), impossible. Thirdly, if $j_2 + j_3 = 0$, then (4.30) implies $1 - g^{2j_1e} = 0$, so $j_1 = 0$. Lastly, if $j_1 + j_3 = 0$, then the second equation in (4.29) implies $2 - 2g^{j_1e} = 0$, so $j_1 = 0$, a contradiction. Now by (4.25) and Theorem 4.4.1, the equation (4.30) implies

$$1 + \zeta_k^{(j_1-j_2)e} - \zeta_k^{2j_1} - \zeta_k^{(j_1-j_3)e} = 0.$$

By Result 4.2.2, the left-hand-side sum cancels in pairs, impossible as k is odd and the terms $0, j_1 - j_2, 2j_1, j_1 - j_3$ are pairwise different. $\square$

Theorem 4.5.6. *Let $a \in \{1, \dots, e-1\}$. If*

$$p > \left(\frac{4k}{\varphi(k)} \right)^{\frac{\varphi(k)}{2 \operatorname{ord}_k(p)}}, \quad (4.31)$$

then

$$(a, a) \leq \begin{cases} 3 & \text{if } 2 \in C_a \text{ and } 2 \mid k, \\ 2 & \text{if } 2 \notin C_a \text{ and } 2 \mid k, \\ 2 & \text{if } 2 \nmid k. \end{cases} \quad (4.32)$$

Proof. For each $0 \leq i, j \leq k-1$ with $1 + g^{ie+a} = g^{je+a}$, we have $1 + g^{-ie-a} = g^{(j-i)e}$. Thus $(a, a) = (-a, 0)$ and the conclusion follows directly from Theorem 4.5.5. $\square$

Theorem 4.5.7. *Let $a \neq b \in \{1, \dots, e-1\}$. If*

$$p > \left(\frac{14k}{\varphi(k)} \right)^{\frac{\varphi(k)}{2 \operatorname{ord}_k(p)}}, \quad (4.33)$$

then

$$(a, b) \leq 2.$$

This theorem is proved by contradiction. Let $(i_1, j_1), (i_2, j_2), (i_3, j_3)$ be three different pairs with $0 \leq i_t, j_t \leq k-1$ and $1 + g^{i_te+a} = g^{j_te+b}$ for $t = 1, 2, 3$. The following lemma states a simple relation between i_t 's and j_t 's which will be used repeatedly later.

Lemma 4.5.8. *Let $i_t, j_t, t = 1, 2, 3$, be defined as above, then the numbers $i_1 - j_1, i_2 - j_2, i_3 - j_3$ are pairwise different.*

Proof. Suppose that $i_1 - j_1 = i_2 - j_2$. We have $i_1 - i_2 = j_1 - j_2$. Subtracting two equations $1 + g^{i_1 e + a} = g^{j_1 e + b}$ and $1 + g^{i_2 e + a} = g^{j_2 e + b}$, we obtain $g^{i_2 e + a}(g^{(i_1 - i_2)e} - 1) = g^{j_2 e + b}(g^{(j_1 - j_2)e} - 1)$, which implies

$$g^{i_2 e + a} = g^{j_2 e + b},$$

a contradiction as $C_a \cap C_b = \emptyset$. □

A major part in the proof of Theorem 4.5.7 is proving that the sum $\zeta_k^{i_1 + j_2} + \zeta_k^{i_2 + j_3} + \zeta_k^{i_3 + j_1} - \zeta_k^{i_1 + j_3} - \zeta_k^{i_2 + j_1} - \zeta_k^{i_3 + j_2}$, is nonzero, where $i_t, j_t, t = 1, 2, 3$, are given as above. We prove this result in the following proposition.

Proposition 4.5.9. *Let $i_t, j_t, t = 1, 2, 3$, be integers such that the i_t 's are pairwise different modulo k , the j_t 's are pairwise different modulo k and the $i_t - j_t$'s are pairwise different modulo k . Then the following sum is nonzero*

$$T = \zeta_k^{i_1 + j_2} + \zeta_k^{i_2 + j_3} + \zeta_k^{i_3 + j_1} - \zeta_k^{i_1 + j_3} - \zeta_k^{i_2 + j_1} - \zeta_k^{i_3 + j_2}.$$

Proof. Suppose that $T = 0$. Since T is a vanishing sum of roots of unity of length at most 6, Result 4.2.2 implies that T contains a subsum similar to $1 + (-1)$, or T contains two subsums each of which is similar to $1 + \zeta_3 + \zeta_3^2$, or T itself is similar to either $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4$ or $-\zeta_3 - \zeta_3^2 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4$.

Case 1. T contains a subsum similar to $1 + (-1)$.

Discarding this subsum, the new T is a vanishing sum of 4 roots of unity. By Result 4.2.2 again, T cancels in pairs. Thus, the original sum T cancels in pairs. Note that none of the first three terms in T is canceled by any of the last three terms. Otherwise, let's say $\zeta_k^{i_1 + j_2}$ is canceled by one of the last three terms. By the difference between the i_t 's and j_t 's, we can only have $i_1 + j_2 = i_2 + j_1$, which implies $i_1 - j_1 = i_2 - j_2$, a contradiction. Thus, the first three terms of T cancel in pairs, impossible.

Case 2. T is similar to $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4$.

Note that by Case 1, the sets $\{i_1 + j_2, i_2 + j_3, i_3 + j_1\}$ and $\{i_1 + j_3, i_2 + j_1, i_3 + j_2\}$ are disjoint. As T has length 5, we can assume that the first two terms in T are the same, say $T = 2\zeta_k^{i_1 + j_2} + \zeta_k^{i_3 + j_1} - \zeta_k^{i_1 + j_3} - \zeta_k^{i_2 + j_1} - \zeta_k^{i_3 + j_2}$. Hence, T is similar to the sum $2 + \zeta_k^{i_3 + j_1 - i_1 - j_2} - \zeta_k^{j_3 - j_2} - \zeta_k^{i_2 + j_1 - i_1 - j_2} - \zeta_k^{i_3 - i_1}$. It is impossible that this sum has the form $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4$.

Case 3. T contains two subsums each of which is similar to $1 + \zeta_3 + \zeta_3^2$.

Due to symmetry, we can consider two possibilities for these two subsums.

Subcase 1. The subsums are $\zeta_k^{i_1+j_2} + \zeta_k^{i_2+j_3} + \zeta_k^{i_3+j_1}$ and $\zeta_k^{i_1+j_3} + \zeta_k^{i_2+j_1} + \zeta_k^{i_3+j_2}$.

We obtain $1 + \zeta_k^{i_2+j_3-i_1-j_2} + \zeta_k^{i_3+j_1-i_1-j_2} = 1 + \zeta_k^{i_2+j_1-i_1-j_3} + \zeta_k^{i_3+j_2-i_1-j_3}$ and both sums have the form $1 + \zeta_3 + \zeta_3^2$. Thus $3 \mid k$,

$$\{i_2 + j_3 - i_1 - j_2, i_3 + j_1 - i_1 - j_2\} = \{k/3, 2k/3\}, \text{ and} \quad (4.34)$$

$$\{i_2 + j_1 - i_1 - j_3, i_3 + j_2 - i_1 - j_3\} = \{k/3, 2k/3\}. \quad (4.35)$$

Since $k/3 + 2k/3 = 0$, we have $(i_2 + j_3 - i_1 - j_2) + (i_3 + j_1 - i_1 - j_2) = 0$ and $(i_2 + j_1 - i_1 - j_3) + (i_3 + j_2 - i_1 - j_3) = 0$, which implies

$$2(i_1 + j_2) = (i_2 + j_3) + (i_3 + j_1) \quad (4.36)$$

and

$$2(i_1 + j_3) = (i_2 + j_1) + (i_3 + j_2). \quad (4.37)$$

Subtracting (4.36) and (4.37), we obtain $j_2 - j_3 = k/3$. Now, the equation (4.34) gives $i_2 - i_1 = 2k/3$ and the equation (4.35) gives $i_3 - i_1 = k/3$. We obtain $i_2 - i_3 = j_2 - j_3 = k/3$, so $i_2 - j_2 = i_3 - j_3$, a contradiction.

Subcase 2. The subsums are $\zeta_k^{i_1+j_2} + \zeta_k^{i_2+j_3} - \zeta_k^{i_2+j_1}$ and $\zeta_k^{i_3+j_1} - \zeta_k^{i_1+j_3} - \zeta_k^{i_3+j_2}$.

We obtain $1 + \zeta_k^{i_2+j_3-i_1-j_2} - \zeta_k^{i_2+j_1-i_1-j_2} = 1 + \zeta_k^{i_3+j_2-i_1-j_3} - \zeta_k^{i_3+j_1-i_1-j_3}$ and both sums are equal to $1 + \zeta_3 + \zeta_3^2$. Thus $6 \mid k$ and the two sums $1 + \zeta_k^{i_2+j_3-i_1-j_2} - \zeta_k^{i_2+j_1-i_1-j_2}$ and $1 + \zeta_k^{i_3+j_2-i_1-j_3} - \zeta_k^{i_3+j_1-i_1-j_3}$ have form $1 + \zeta_k^{k/3} - \zeta_k^{k/6}$ or $1 + \zeta_k^{2k/3} - \zeta_k^{5k/6}$. If these two sums have the same form, then $i_2 + j_1 - i_1 - j_2 = i_3 + j_1 - i_1 - j_3$, so $i_2 - j_2 = i_3 - j_3$, a contradiction. Thus, the two sums have different forms. Noting that $k/6 + 2k/3 = 5k/6$ and $5k/6 + k/3 = k/6$, we have

$$(i_2 + j_1 - i_1 - j_2) + (i_3 + j_2 - i_1 - j_3) = (i_3 + j_1 - i_1 - j_3),$$

so $i_2 = i_1$, a contradiction.

Case 4. T is similar to $-\zeta_3 - \zeta_3^2 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4$.

A reduced sum of this sum is

$$S' = 1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 - \zeta_3\zeta_5^{-1} - \zeta_3^2\zeta_5^{-1}.$$

Let S be the reduced sum obtained from T as follows.

$$S = 1 + \zeta_k^{i_2+j_3-i_1-j_2} + \zeta_k^{i_3+j_1-i_1-j_2} - \zeta_k^{j_3-j_2} - \zeta_k^{i_2+j_1-i_1-j_2} - \zeta_k^{i_3-i_1}.$$

Dividing by a common divisor if necessary, we can assume that the greatest common divisor between k and all the exponents of ζ_k occurring in S is 1. This implies $e(S) = k$. In view of Result 4.2.1, we can assume that k is square-free. Since S and S' are similar reduced sums, we have $S = S'\zeta_{30}^t$ with $t \in \{0, 1, 11, 12, 18, 24\}$ (the possible values of t are obtained from the fact that 1 appears in S). The 6 possibilities are

- (i) $S' = 1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 - \zeta_{15}^2 - \zeta_{15}^7$.
- (ii) $S'\zeta_{30} = 1 + \zeta_3^2 - \zeta_{15}^8 - \zeta_{15}^{11} - \zeta_{15}^{14} - \zeta_{15}^2$.
- (iii) $S'\zeta_{30}^{11} = 1 + \zeta_3 - \zeta_{15}^{13} - \zeta_{15} - \zeta_{15}^4 - \zeta_{15}^7$.
- (iv) $S'\zeta_{30}^{12} = 1 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 - \zeta_{15}^8 - \zeta_{15}^{13}$.
- (v) $S'\zeta_{30}^{18} = 1 + \zeta_5 + \zeta_5^3 + \zeta_5^4 - \zeta_{15}^{11} - \zeta_{15}$.
- (vi) $S'\zeta_{30}^{24} = 1 + \zeta_5 + \zeta_5^2 + \zeta_5^4 - \zeta_{15}^{14} - \zeta_{15}^4$.

Suppose that k is odd. We obtain $k = 15$ and the sum S has form exactly as one of the 6 possibilities above, impossible as the sum of the coefficients in any of these possibilities is nonzero and the sum of the coefficients in S is zero. Therefore, k is even. Note that $e(S'\zeta_{30}^t) = 15$ in any case and we can write $\zeta_{30} = -\zeta_{15}^8$. So $k = 30$. Multiplying all the terms in both sides of the equation $S = S'\zeta_{30}^t$, we obtain

$$\zeta_{30}^{2(i_2+i_3+j_1+j_3)-4(i_1+j_2)+15} = \zeta_{30}^{24+6t},$$

which implies $2(i_2 + j_3 + j_1 + j_3) - 4(i_1 + j_2) - 6t \equiv 9 \pmod{30}$, impossible. □

Proof of Theorem 4.5.7. Let $(i_1, j_1), (i_2, j_2), (i_3, j_3)$ be three different pairs so that $0 \leq i_t, j_t \leq k-1$ and $1 + g^{i_te+a} = g^{j_te+b}$ for $t = 1, 2, 3$. We have

$$g^a(g^{i_1e} - g^{i_2e}) = g^b(g^{j_1e} - g^{j_2e}),$$

$$g^b(g^{j_1e} - g^{j_3e}) = g^a(g^{i_1e} - g^{i_3e}).$$

Multiplying these two equations, we obtain

$$g^{(i_1+j_2)e} + g^{(i_2+j_3)e} + g^{(i_3+j_1)e} - g^{(i_1+j_3)e} - g^{(i_2+j_1)e} - g^{(i_3+j_2)e} = 0. \quad (4.38)$$

Write $f(x) = \sum_{i=0}^{k-1} a_i x^i$, where $f(g^e)$ is equal to the left-hand-side of (4.38). Each a_i is an integer in $[-3, 3]$ and $\sum_{i=0}^{k-1} a_i = 0$ and $\sum_{i=0}^{k-1} |a_i| \leq 6$. We claim that $\sum_{i=0}^{k-1} a_i^2 \leq 14$. Note that $\sum_{i=0}^{k-1} a_i^2$ is largest when one term a_i^2 is largest possible and other terms a_j^2

are smallest possible. First, there are no $i \neq j$ with $|a_i| = |a_j| = 3$. Otherwise, we have $g^{(i_1+j_2)e} = g^{(i_2+j_3)e} = g^{(i_3+j_1)e}$ and $g^{(i_1+j_3)e} = g^{(i_2+j_1)e} = g^{(i_3+j_2)e}$, and (4.38) implies $3(g^{(i_1+j_2)e} - g^{(i_1+j_3)e}) = 0$. Since $j_2 \neq j_3$, we have $p = 3$, contradicting (4.33) because $p > \sqrt{14} > 3$. Therefore, the sum $\sum_{i=0}^{k-1} a_i^2$ is largest when there are three nonzero terms, one equal to $(\pm 3)^2$, one equal to $(\pm 2)^2$ and one equal to $(\pm 1)^2$, that is

$$\sum_{i=0}^{k-1} a_i^2 \leq 9 + 4 + 1 = 14.$$

Now combining (4.38), (4.33) and Theorem 4.4.1, we obtain

$$f(\zeta_k) = \zeta_k^{i_1+j_2} + \zeta_k^{i_2+j_3} + \zeta_k^{i_3+j_1} - \zeta_k^{i_1+j_3} - \zeta_k^{i_2+j_1} - \zeta_k^{i_3+j_2} = 0, \quad (4.39)$$

which is impossible by Lemma 4.5.8 and Proposition 4.5.9. □

Proof of Theorem 4.5.1

Summarizing the results of Theorem 4.5.2, Theorem 4.5.4, Theorem 4.5.5, Theorem 4.5.6 and Theorem 4.5.7, we obtain $(a, b) \leq 3$ if $p > (14k/\varphi(k))^{\varphi(k)/(2 \operatorname{ord}_k(p))}$. Furthermore, by the proof for (4.5) in Theorem 4.3.1, we have

$$\left(\frac{14k}{\varphi(k)} \right)^{\frac{\varphi(k)}{2 \operatorname{ord}_k(p)}} \leq \left(\sqrt{14} \right)^{k/\operatorname{ord}_k(p)}.$$

We obtain $(a, b) \leq 3$ if $p > (\sqrt{14})^{k/\operatorname{ord}_k(p)}$, proving Theorem 4.5.1. □

4.6 The Case where k is Prime

In this section, we always assume that k is a prime. First, we recall our main result in this case.

Theorem 4.6.1. *Let q be a power of a prime p . Let e and k be nontrivial divisors of $q - 1$ such that $q = ek + 1$ and k is a prime. If*

$$p > (3^{k-1}k)^{1/\operatorname{ord}_k(p)}, \quad (4.40)$$

then

$$(a, b) \leq 2 \text{ for all } a, b \in \mathbb{Z}. \quad (4.41)$$

Similar to the proof of Theorem 4.5.1, the proof of Theorem 4.6.1 is divided into the cases $(0, 0)$, $(0, a)$, $(a, 0)$, (a, a) and (a, b) , where a and b are distinct elements in $\{1, \dots, e-1\}$, and Theorem 4.6.1 is just a simplified consequence of the results for the different cases. We remark that only in the cases $(0, a)$ and (a, b) , we obtain better upper bounds for these numbers than the bounds obtained in the last section. We restate the results for $(0, 0)$, $(a, 0)$ and (a, a) here for the completeness of the proof.

Corollary 4.6.2. *If*

$$p > \left(\frac{3k}{k-1} \right)^{\frac{k-1}{2 \operatorname{ord}_k(p)}},$$

then

$$(0, 0) = \begin{cases} 0 & \text{if } 2 \notin C_0, \\ 1 & \text{if } 2 \in C_0. \end{cases}$$

Proof. This theorem is a direct consequence of Theorem 4.5.2. Note that the case $6 \mid k$ cannot occur because k is a prime. $\square$

Corollary 4.6.3. *If*

$$p > \left(\frac{4k}{k-1} \right)^{\frac{k-1}{2 \operatorname{ord}_k(p)}},$$

then

$$(a, 0) \leq 2 \quad \text{and} \quad (a, a) \leq 2.$$

Proof. If k is even, then $k = 2$ and it is trivial that $(a, 0) \leq 2$. If k is odd, then $(a, 0) \leq 2$ by Theorem 4.5.5 (the case k is odd). Lastly, note that $(a, a) = (-a, 0) \leq 2$. $\square$

Theorem 4.6.4. *If*

$$p > \left(2^{k-1} k \right)^{1/\operatorname{ord}_k(p)}, \tag{4.42}$$

then

$$(0, a) \leq 2. \tag{4.43}$$

Proof. Note that $1 + g^{ie} = g^{je+a}$ implies $1 + g^{-ie} = g^{(j-i)e+a}$, so each solution (i, j) to $1 + g^{ie} = g^{je+a}$ induces a solution $(-i, j-i)$ (calculation is modulo k) to the same equation, two of which are different if and only if $i \neq 0$. Moreover if $i = 0$, then $2 = g^{je+a} \in C_a$ and there is one solution to $1 + g^{ie} = g^{je+a}$ in which $i = 0$.

First, suppose that $2 \in C_a$ and $(0, a) \geq 3$. We have $g^{le+a} = 2$ for some $0 \leq l \leq k-1$. There exist $0 \leq i, j \leq k-1$ with $i \neq 0$ and $j \neq l$ such that $1 + g^{ie} = g^{je+a}$. Writing $t = j - l$, we obtain

$$1 + g^{ie} - 2g^{te} = 0.$$

Note that the numbers $0, i, t$ are pairwise different. Write $1 + x^i - 2x^t$ in the polynomial form $f(x) = \sum_{i=0}^{k-1} a_i x^i$. Note that, using the notation of Theorem 4.4.2, we have $A = 2$. Thus, by Theorem 4.4.2 (b) and (4.42), we have $f(\zeta_k) = 0$, as $f(g^e) = 0$. Hence

$$f(\zeta_k) = 1 + \zeta_k^i - 2\zeta_k^t = 0.$$

By Result 4.2.2, this happens only when the terms in $f(\zeta_k)$ cancel in pairs or $f(\zeta_k)$ is similar to $1 + \zeta_3 + \zeta_3^2$, both of which are not possible.

Next, suppose that $2 \notin C_a$ and $(0, a) \geq 3$. Similar to the proof of Theorem 4.5.4, we obtain the equation

$$1 + g^{i_1 e} - g^{(j_1 - j_2)e} - g^{(j_1 - j_2 + i_2)e} = 0,$$

where the two pairs (i_1, j_1) and (i_2, j_2) are different and satisfy

$$i_1 \neq 0, i_2 \neq 0, (i_2, j_2) \neq (-i_1, j_1 - i_1) \text{ and } (i_1, j_1) \neq (-i_2, j_2 - i_2).$$

Write $f(x) = 1 + x^{i_1} - x^{j_1 - j_2} - x^{j_1 - j_2 + i_2}$. Note that $f(x)$ is a polynomial with exactly 4 nonzero coefficients, as the numbers $0, i_1, j_1 - j_2$ and $j_1 - j_2 + i_2$ are pairwise different (by the proof of Theorem 4.5.4). Thus, by Theorem 4.4.2 (b) and (4.42), we have

$$f(\zeta_k) = 1 + \zeta_k^{i_1} - \zeta_k^{j_1 - j_2} - \zeta_k^{j_1 - j_2 + i_2} = 0.$$

By Result 4.2.2, the terms in $f(\zeta_k)$ cancel in pairs. This implies in $2 \mid k$ and $i_1 = i_2 = k/2$, or $j_1 = j_2$ and $i_1 = i_2$, both of which are not possible. $\square$

Remark 4.6.5. The bound (4.42) is not better than the previous bound in (4.21) (in fact, they are very close). However, the conclusion (4.43) is better than the conclusion (4.22).

Theorem 4.6.6. *If*

$$p > (3^{k-1}k)^{1/\text{ord}_k(p)}, \tag{4.44}$$

then

$$(a, b) \leq 2.$$

Proof. Similar to the proof of Theorem 4.5.7, we obtain the equation

$$g^{(i_1+j_2)e} + g^{(i_2+j_3)e} + g^{(i_3+j_1)e} - g^{(i_1+j_3)e} - g^{(i_2+j_1)e} - g^{(i_3+j_2)e} = 0, \quad (4.45)$$

where (i_t, j_t) , $t = 1, 2, 3$, are pairwise different pairs each of which satisfy $1 + g^{i_t e + a} = g^{j_t e + b}$. Write the left-hand-side of (4.45) as $\sum_{i=0}^{k-1} a_i g^{ie}$ and set $f(x) = \sum_{i=0}^{k-1} a_i x^i$. We have $\sum_{i=0}^{k-1} a_i = 0$ and, using the notation of Theorem 4.4.2, we have $A \leq 3$. Hence Theorem 4.4.2 (b) and (4.44) imply

$$f(\zeta_k) = \zeta_k^{i_1+j_2} + \zeta_k^{i_2+j_3} + \zeta_k^{i_3+j_1} - \zeta_k^{i_1+j_3} - \zeta_k^{i_2+j_1} - \zeta_k^{i_3+j_2} = 0.$$

This is impossible by Proposition 4.5.9. $\square$

Proof of Theorem 4.6.1.

Summarizing the results of Corollary 4.6.2, Corollary 4.6.3, Theorem 4.6.4 and Theorem 4.6.6, we obtain $(a, b) \leq 2$ if

$$p > \max \left\{ \left(\frac{3k}{k-1} \right)^{\frac{k-1}{2\text{ord}_k(p)}}, \left(\frac{4k}{k-1} \right)^{\frac{k-1}{2\text{ord}_k(p)}}, \left(2^{k-1}k \right)^{\frac{1}{\text{ord}_k(p)}}, \left(3^{k-1}k \right)^{\frac{1}{\text{ord}_k(p)}} \right\},$$

that is, $p > (3^{k-1}k)^{1/\text{ord}_k(p)}$, proving Theorem 4.6.1. $\square$

4.7 Concluding Remarks

Let q be a power of a prime p , let k be a nontrivial divisor of $q-1$ and put $e = (q-1)/k$. We proved that all cyclotomic numbers (a, b) of order e have values at most 3 if p is sufficiently large compared to k . We also gave explicit bounds between p and k under which we have $(a, b) \leq 3$ for all $a, b \in \mathbb{Z}$. This bound can be improved if k is a prime.

The key to our results is our new bounds on the norm of cyclotomic integers. Moreover, we prove an equivalence between equations over $\mathbb{F}_q$ and equations over the field of complex numbers $\mathbb{C}$, where on the latter equations we have more information.

In closing of this section, we propose the following general question.

Problem 4.7.1. *Let e be a divisor of $q-1$ and let $e_1, \dots, e_k$ be positive integers which are divisible by e . Find an upper bound for the number of solutions to the following equation over $\mathbb{F}_q$:*

$$x_1^{e_1} + \dots + x_k^{e_k} = 0.$$

Bibliography

- [1] M. K. Agrawal, J. C. Parnami, A. R. Rajwade Jacobi sums and cyclotomic numbers for a finite field. *Acta Arith.* **41**(1) (1982), 1–13.
- [2] J. Backelin: Square multiples n gives infinite many cyclic n -roots. *Reports, Matematiska Institutionen, Stockholms Universitet*, **8** (1989), 1–2.
- [3] L. D. Baumert, H. Fredricksen: The cyclotomic numbers of order eighteen with applications to difference sets. *Math. Comp.* **21** (1967), 204–219.
- [4] B. C. Berndt, R. J. Evans, K. S. Williams: *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons Inc., New York, 1998.
- [5] K. Betsumiya, M. Hirasaka, T. Komatsu, A. Munemasa: Upper bounds on cyclotomic numbers. *Linear Algebra and its Applications* (2013).
- [6] T. Beth, D. Jungnickel, H. Lenz: *Design Theory* (2nd edition), Cambridge University Press 1999.
- [7] S. T. Blake, T. E. Hall, A. Z. Tirkel: Arrays over roots of unity with perfect autocorrelation and good ZCZ cross-correlation, *Adv. Math. Commun.* **7** (2013), 231 – 242.
- [8] L. Bomer, M. Antweiler: Perfect N -phase sequences and arrays [spread spectrum communication], *IEEE J. Sel. Areas Commun.*, **10** (1992), 782 – 789.
- [9] B. W. Brock: Hermitian congruence and the existence and completion of generalized Hadamard matrices, *J. Combin. Theory Ser. A* **49** (1988), 233 – 261.
- [10] J. Browkin, B. Divis, and A. Schinzel: Addition of sequences in general fields, *Monatsh. Math.* **82** (1976), 261–268.

- [11] A. T. Butson: Generalized Hadamard Matrices. *Proc. Amer. Math. Soc.* **13** (1962), 894–898.
- [12] J. W. S. Cassels: On a conjecture of R. M. Robinson about sums of roots of unity. *J. Reine Angew. Math.* **238** (1969), 112–131.
- [13] J. H. Conway and A. J. Jones: Trigonometric diophantine equations (On vanishing sums of roots of unity) *Acta Arithmetica* **30** (1976).
- [14] J. A. Davis, J. Jedwab: A unifying construction for difference sets. *J. Combin. Theory Ser. A* **80** (1997), 13 – 78.
- [15] P. J. Davis: Circulant matrices. *Chelsea Publishing, New York*, (1979) xv+250 pp.
- [16] W. de Launey: Circulant $GH(p^2, \mathbb{Z}_p)$ Exist for All Primes p . *Graphs Comb.* **8** (1992), 317–321.
- [17] J. F. Dillon: Difference sets in 2-groups. *Proc. NSA Math. Sci. Meeting* (1987) 165–172.
- [18] T. D. Duc, B. Schmidt: Bilinear Forms on Finite Abelian Groups and Group-Invariant Butson Hadamard Matrices. *J. Comb. Theory Ser. A* **166** (2019), 337–351.
- [19] T. D. Duc: Necessary Conditions for the Existence of Group-Invariant Butson Matrices and a New Family of Perfect Arrays. Submitted. arXiv:1903.07334.
- [20] T. D. Duc, B. Schmidt: Unique Differences in Symmetric Subsets of $\mathbb{F}_p$. *Combinatorica* **37** (2017), 167–182.
- [21] T. D. Duc, K. H. Leung, B. Schmidt: Upper Bounds for Cyclotomic Numbers. *Algebr. Comb.* Accepted.
- [22] T. D. Duc: New Constructions of Group-Invariant Butson Hadamard Matrices. Preprint. arXiv:1903.09824.
- [23] T. D. Duc: List of Open Cases for $BH(\mathbb{Z}_n, h)$ Matrices with $n, h \leq 100$. http://www3.ntu.edu.sg/home/Bernhard/BH/BH_open_cases.txt
- [24] R. J. Evans, J. R. Hill: The cyclotomic numbers of order sixteen. *Math. Comp.* **33** (1979), 827–835.
- [25] P. Z. Fan, M. Darnell: *Sequence Design for Communications Applications*. Hoboken, NJ, USA: Wiley, 1996.

- [26] T. Feng, K. H. Leung, B. Schmidt, K. W. Smith: Hadamard difference sets related to Lander's conjecture, *J. Alg.* **403** (2014) 29 – 47.
- [27] S. W. Golomb, G. Gong: *Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar*. New York, NY, USA: Cambridge Univ. Press, 2005.
- [28] G. Hiranandani, J. M. Schlenker: Small circulant complex Hadamard matrices of Butson type. *Eur. J. Com.* **51** (2016), 306–314.
- [29] K. Ireland, M. Rosen: *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics **84**, Springer 1990.
- [30] S. A. Katre: Cyclotomic Numbers and A Conjecture of Snapper. *Indian J. pure appl. Math.* **20**(2) (1989), 99–103.
- [31] T. Y. Lam, K. H. Leung: On vanishing sums of roots of unity *J. Algebra* **224**(1) (2000), 91–109.
- [32] P. H. J. Lampio, P. Östergård, F. Szöllösi: Orderly generation of Butson Hadamard matrices. Preprint. [arXiv:1707.02287](https://arxiv.org/abs/1707.02287).
- [33] E. Lehmer, H. S. Vandiver: On the computation of the number of solutions of certain trinomial congruences. *J. Assoc. Comput. Mach.* **4** (1957), 505–510.
- [34] E. Lehmer: On the cyclotomic numbers of order sixteen. *Canadian J. Math.* **6** (1954), 449–454.
- [35] K. H. Leung, B. Schmidt: Nonexistence Results on Generalized Bent Functions $\mathbb{Z}_q^m \rightarrow \mathbb{Z}_q$ with Odd m and $q \equiv 2 \pmod{4}$. *J. Comb. Theory Ser. A* **163** (2019) 1–33.
- [36] K. H. Leung, B. Schmidt: The anti-field-descent method. *J. Combin. Theory Ser. A* **139** (2016), 87 – 131.
- [37] 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.
- [38] S. L. Ma: *Polynomial addition sets*. Ph.D. thesis, University of Hong Kong, 1985.
- [39] S. L. Ma, W. S. Ng: On non-existence of perfect and nearly perfect sequences, *Int. J. Inform. Coding Theory*, **1** (2009), 15 – 38.

- [40] R. Miranda: Nondegenerate symmetric bilinear forms on finite abelian 2-groups. *Trans. Amer. Math. Soc.* **284** (1984), 535–542.
- [41] W. H. Mow: A new unified construction of perfect root-of-unity sequences, *Proc. IEEE 4th Int. Symp. Spread Spectr. Techn. Appl.*, **3** (1996), 955 – 959.
- [42] Z. Nedeв, A. Quas: Balanced Sets and the Vector Game, *International Journal of Number Theory*, **4** (2008), 339 – 347.
- [43] C. Norman: *Finitely Generated Abelian Groups and Similarity of Matrices over a Field*. Springer 2012.
- [44] R.E.A.C. Paley: On orthogonal matrices. *J. Math. Phys.* **12** (1933), 311–320.
- [45] O. S. Rothaus: On Bent Functions. Institute of Defense Analysis, USA, W. P. 169 (1966).
- [46] O. S. Rothaus: On 'bent' functions. *J. Combin. Theory Ser. A* **20** (1976), 300–305.
- [47] H. J. Ryser: *Combinatorial Mathematics*. Wiley, New York 1963.
- [48] A. Schinzel: An inequality for determinants with real entries. *Colloq. Math.* **38** (1977/78), 319–321.
- [49] B. Schmidt: Cyclotomic integers and finite geometry. *J. Am. Math. Soc.* **12**(4) (1999), 929–952.
- [50] B. Schmidt: *Characters and Cyclotomic Fields in Finite Geometry*, Lecture Notes in Mathematics, vol. 1797. Springer, Berlin (2002).
- [51] B. Schmidt: A Survey of Group Invariant Butson Matrices and Their Relation to Generalized Bent Functions and Various Other Objects.
- [52] T. Storer: Cyclotomy and difference sets. Lectures in Advanced Mathematics, **2** Markham Publishing Co., Chicago, Ill. (1967) vii+134 pp.
- [53] E. G. Straus: Differences of residues (mod p). *J. Number Theory* **8** (1976), 40–42.
- [54] F. Szőllősi: *Construction, classification and parametrization of complex Hadamard matrices* Ph.D. Thesis. [arXiv:1110.5590](https://arxiv.org/abs/1110.5590).
- [55] H. S. Vandiver: New types of trinomial congruence criteria applying to Fermat's last theorem. *Proc. Nat. Acad. Sci. U. S. A.* **40** (1954), 248–252.

- [56] H. S. Vandiver: On trinomial equations in a finite field. *Proc. Nat. Acad. Sci. U. S. A.* **40** (1954), 1008–1010.
- [57] H. S. Vandiver: Relation of the theory of certain trinomial equations in a finite field to Fermat's last theorem. *Proc. Nat. Acad. Sci. U. S. A.* **41** (1955), 770–775.
- [58] H. S. Vandiver: On distribution problems involving the numbers of solutions of certain trinomial congruences. *Proc. Nat. Acad. Sci. U. S. A.* **45** (1959), 1635–1641.
- [59] C. T. C. Wall: Quadratic forms on finite groups, and related topics. *Topology* **2** (1963), 281–298.
- [60] C. T. C. Wall: Quadratic forms on finite groups. II. *Bull. London Math. Soc.* **4** (1972), 156–160.
- [61] A. L. Whiteman: The cyclotomic numbers of order sixteen. *Trans. Amer. Math. Soc.* **86** (1957), 401–413.
- [62] A. L. Whiteman: The cyclotomic numbers of order ten. *Proc. Sympos. Appl. Math.* **10** (1960), 95–111.
- [63] A. L. Whiteman: The cyclotomic numbers of order twelve. *Acta Arith.* **6** (1960), 53–76.
- [64] J. A. Wood: Witt's extension theorem for mod four valued quadratic forms. *Trans. Amer. Math. Soc.* **336** (1993), 445–461.