

**γ -BUTSON-HADAMARD MATRICES AND
THEIR CRYPTOGRAPHIC APPLICATIONS**

**γ -BUTSON HADAMARD MATRİSLERİ VE
ONLARIN KRİPTOGRAFİK UYGULAMALARI**

SİBEL KURT

ASSIST. PROF. DR. OĞUZ YAYLA

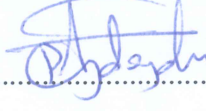
Supervisor

Submitted to Graduate School of Science and Engineering of Hacettepe University
as a Partial Fulfillment to the Requirements
for the Award of the Degree of Master of Science
in Mathematics

2017

This work named " γ -Butson-Hadamard Matrices and Their Cryptographic Applications" by SİBEL KURT has been approved as a thesis for the Degree of MASTER OF SCIENCE IN MATHEMATICS by the below mentioned Examining Committee Members.

Assoc. Prof. Dr. Pınar AYDOĞDU
Head



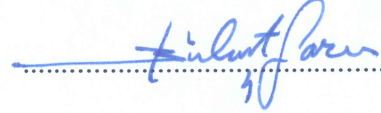
.....

Assist. Prof. Dr. Oğuz YAYLA
Supervisor



.....

Assoc. Prof. Dr. Bülent SARAÇ
Member



.....

Assoc. Prof. Dr. Mesut ŞAHİN
Member



.....

Assoc. Prof. Dr. Zülfükar SAYGI
Member



.....

This thesis has been approved as a thesis for the Degree of MASTER OF SCIENCE IN MATHEMATICS by Board of Directors of the Institute for Graduate School of Science and Engineering.

Prof. Dr. Menemşe GÜMÜŞDERELİOĞLU
Director of the Institute of
Graduate School of Science and Engineering

YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin/raporumun tamamını veya herhangi bir kısmını, basılı (kağıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinlerin yazılı izin alınarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Tezimin/Raporumun tamamı dünya çapında erişime açılabilir ve bir kısmı veya tamamının fotokopisi alınabilir.

(Bu seçenekle teziniz arama motorlarında indekslenebilecek, daha sonra tezinizin erişim statüsünün değiştirilmesini talep etmeniz ve kütüphane bu talebinizi yerine getirse bile, teziniz arama motorlarının önbelleklerinde kalmaya devam edebilecektir)

Tezimin/Raporumun 02/ 08/ 2020 tarihine kadar erişime açılmasını ve fotokopi alınmasını (İç Kapak, Özet, İçindekiler ve Kaynakça hariç) istemiyorum.

(Bu sürenin sonunda uzatma için başvuruda bulunmadığım takdirde, tezimin/raporumun tamamı her yerden erişime açılabilir, kaynak gösterilmek şartıyla bir kısmı veya tamamının fotokopisi alınabilir).

Tezimin/Raporumun 02/ 08/ 2020 tarihine kadar erişime açılmasını istemiyorum ancak kaynak gösterilmek şartıyla bir kısmı veya tamamının fotokopisinin alınmasını onaylıyorum.

Serbest Seçenek/Yazarın Seçimi:

02.08.2017

SİBEL KURT



Sevgili anneanneme ve dedeme

ETHICS

In this thesis study, prepared in accordance with the spelling rules of Institute of Graduate Studies in Science of Hacettepe University.

I declare that

- all the information and documents have been obtained in the base of the academic rules
- all audio-visual and written information and results have been presented according to the rules of scientific ethics
- in case of using other Works, related studies have been cited in accordance with the scientific standards
- all cited studies have been fully referenced
- I did not do any distortion in the data set
- and any part of this thesis has not been presented as another thesis study at this or any other university.

21/06/2017

SİBEL KURT



This thesis was supported by TÜBİTAK (The Scientific and Technological Research Council of Turkey) -1002 - Short Term R&D Funding Program, Project No: 116R001).

ABSTRACT

γ -BUTSON-HADAMARD MATRICES AND THEIR CRYPTOGRAPHIC APPLICATIONS

Sibel KURT

Master of Science, Department of Mathematics

Supervisor: Assist. Prof. Dr. Oğuz YAYLA

June 2017, 37 pages

A Hadamard matrix is a square matrix with entries ± 1 whose rows are orthogonal to each other. Hadamard matrices appear in various fields including cryptography, coding theory, combinatorics etc. This thesis takes an interest in γ -Butson-Hadamard matrix that is a generalization of Hadamard matrices for $\gamma \in \mathbb{R} \cap \mathbb{Z}[\zeta_m]$. These matrices are examined for non-existence cases in this thesis. In particular, the unsolvability of certain equations is studied in the case of cyclotomic number fields whose ring of integers is not a principal ideal domain. Winterhof et al. considered the equations for $\gamma \in \mathbb{Z}$. We first extend this result to $\gamma \in \mathbb{R} \cap \mathbb{Z}[\zeta_m]$ by using some new methods from algebraic number theory. Secondly, we obtain another method for checking the non-existence cases of these equations, which uses the tool of norm from algebraic number theory. Then, the direct applications of these results to γ -Butson-Hadamard matrices, γ -Conference matrices, nearly perfect sequences are obtained. Finally, the connection between nonlinear Boolean cryptographic functions and γ -Butson-Hadamard matrices having small $|\gamma|$ is established. In addition, a computer search is done for checking the cases which are excluded by our results and for obtaining new examples of existence parameters.

Keywords: Butson-Hadamard matrices, algebraic number fields, nearly perfect sequences, conference matrices, cryptographic functions

ÖZET

γ -BUTSON-HADAMARD MATRİSLERİ VE ONLARIN KRİPTOGRAFİK UYGULAMALARI

Sibel Kurt

Yüksek Lisans, Matematik Bölümü

Tez Danışmanı: Yrd. Doç. Dr. Oğuz Yayla

Haziran 2017, 37 sayfa

Hadamard matrisleri uygulamalı matematikte, kuantum bilgisayar bilimlerinde, telekomünikasyon, uydu teknolojileri, akıllı telefonlar ve kablosuz iletişim gibi alanlarda kullanılır. Modern KBÇE (Kod bölmeli çoklu erişim) tabanlı cep telefonları, baz istasyonlarına ulaşan sinyallerin karışması gibi durumları minimize etmede ve sinyalleri modülize etmek için Hadamard matrisleri kullanılır. Kablosuz ağlarda saklanan bilgi, optik telekomünikasyon, sinir bilimi ve örüntü tanıma, Hadamard matrislerinin kullanıldığı diğer alanlardandır. Ek olarak, Hadamard matrisleri bilgisayar bilimlerinde örneğin, Hadamard kodlar (en iyi doğrulama kodu olarak bilinir.) ve Hadamard kapıları (kuantum kapılarında kullanılır.) gibi bir çok alana doğrudan uygulanabilir (bkz. [8]).

Bu tezde, Butson-Hadamard matrislerinin bir sınıfı çalışılmış ve onların uygulamaları araştırılmıştır. Yakın tarihte $\gamma \in \mathbb{Z}$ için m -li γ -Butson Hadamard matrisleri WYZ [16] makalesinde çalışılmıştır. Bu tezde, m -li γ -Butson Hadamard matrisleri $\gamma \in (\mathbb{Z}[\zeta_m] \cap \mathbb{R}) \setminus \mathbb{Z}$ için çalışılmış ve yeni γ -Butson Hadamard örnekleri, onların var olmasını sağlayan gereklilikler $m \in \mathbb{Z}^+$ ve ζ_m birimin m -inci dereceden kökü olmak üzere araştırılmıştır. WYZ [16] çalışmasındaki ve cebirsel sayı teorisindeki yöntemlerden ve sonuçlardan yararlanılıp m -li γ -Butson-Hadamard matrisleri üzerinde yeni sonuçlar bulunmuştur. Buna ek olarak, Hadamard matrisleri üzerindeki bu yeni sonuçlar, kodlama teorisi ve kriptografideki yeni uygulamaların araştırılmasında kullanılmıştır.

Bu tezde γ -Butson-Hadamard matrislerini yeni metotlarla analiz edip, onları kodlama teorisi ve kriptografiye uygulanması amaçlanmıştır. γ -Butson-Hadamard matrisleri üzerindeki yakın

zamanlı çalışmalarda kullanılan analizlerin daha genel hali geliştirilmiş ve yeni γ -Butson-Hadamard matrisleri keşfedilmiştir.

Girdileri ± 1 olan ve tüm satırları birbirine dik olan karesel matrise, *Hadamard matrisi* denir. Hadamard matrislerinin ilk genelleştirilmesi, 1962 yılında Butson tarafından yapılmıştır. Butson, Hadamard matrislerinin girdileri için birimin 2-inci dereceden kökünü almak yerine, birimin m -inci dereceden karmaşık kökünü almıştır [3]. γ -Butson-Hadamard matrisleri, bir satırın diğer satırın karmaşık eşleniğiyle iç çarpımından elde edilen γ değeri dışında, Butson Hadamard matrislerine benzerdir. Butson-Hadamard matrisleri için en yaygın sonuç Brock'un [2] ve Winterhof vd. [16]'nin çalışmalarıdır.

Winterhof vd. γ -Butson-Hadamard matrisinin var olabilmesi için olan koşulları siklotomik cismin sayı halkası üzerindeki bir denkleme indirgediler. Yani, onlar aşağıda verilen denklemin,

$$\alpha\bar{\alpha} = ((\gamma + 1)v - \gamma)(v - \gamma)^{v-1}, \quad (0.1)$$

$v \in \mathbb{Z}^+$ boyutlu γ -Butson Hadamard matrisini $\gamma \in \mathbb{Z}$ olmak üzere $\alpha \in \mathbb{Z}$ çözümlerini düşündüler. Onlar, $D = ((\gamma + 1)v - \gamma)(v - \gamma)^{v-1}$ 'nin temel ideal çarpanlarına ayrılmasını ve (1.1) denkleminin çözümünün var olmama koşullarını ele almışlardır. Ayrıca, D 'nin ideal çarpanlarına ayrılabilmesi için yalnızca γ tamsayısını düşünmüşlerdir. Bu tezde, Bölüm 3'de $\gamma \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$ için olan yöntem geliştirildi. $\gamma \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$ olmak üzere (1.1) denkleminin çözümü olmaması için koşulları ele alındı. $\gamma \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$ olduğunda (1.1)'in çözümü olmaması için ekstradan D 'nin temel olmayan ideal çarpanının normu ile temel ideal çarpanının normunun aralarında asal olması koşuluna ihtiyacımız vardır (bkz. Theorem 3.3).

İkinci olarak, Bölüm 4'te, belirli $\gamma \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$ için γ -Butson Hadamard matrisi var olmadığını kontrol etmek için bir yeni yöntem üretildi. (1.1) denklemindeki α 'yı bölen asal ideallerin normunun $\bar{\alpha}$ 'yı da böldüğü gerçeği de kullanıldı. Bu yüzden, D 'yi bölen her asal ideal \mathfrak{p} için, eğer \mathfrak{p} 'nin normu tarafından bölünen D 'nin normu, \mathfrak{p} 'nin normuyla aralarında asalsa, (1.1)'in çözümü yoktur (bkz. Theorem 4.1). Ayrıca, D 'nin normunun çarpanlarına ayrıldığında üsler en fazla bir ise (1.1)'nin hiç bir çözümü olmadığı açıktır (bkz Corollary 4.2). Sabit bir m ve ζ_m için $v \in \{2, 3, \dots, 100\}$ üzerinde Teoremler 3.3 ve 4.1'in gücünü görmek için (1.1) denkleminin var olmaması bilgisayar tarama programı olan MAGMA [1] ile detaylı bir araştırma yapıldı. Theorem 3.3 ve Theorem 4.1 kullanılarak bazı değerler için γ -Butson-Hadamard matrislerinin var olmadığı görüldü. Diğer yandan, bu iki teoremin birbirlerini kapsamadığı gözlemlendi (bkz. Remark 4.4). Uygulamamızın MAGMA kodları tezin

ek kısmında verilmiştir.

Bölüm 5'te Teorem 3.3 ve Teorem 4.1'den çıkan iki yeni sonucu γ -Butson-Hadamard matrislerine uyguladık. Yani, γ -Butson-Hadamard matrislerinin varolmama koşulları için uygun $v \in \mathbb{Z}$ ve $\gamma \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$ bulmaya çalıştık. Bu ise $\alpha \in \mathbb{Z}[\zeta_m]$ için $\alpha\bar{\alpha} = ((\gamma + 1)v - \gamma)(v - \gamma)^{v-1}$ denkleminin çözümü için gerekli koşullar bulmaya denktir. Bu yüzden, ana teoremlerimizi kullanarak, γ -Butson-Hadamard matrislerinin var olmadığı koşulları elde ettik (bkz. Corollary 5.9-(i) ve Corollary 5.11-(i)). Diğer yandan, dolanır (circulant) γ -Butson-Hadamard matrisinin ilk satırı *neredeyse mükemmel diziyeye* denktir (bkz. [5] ve Remark 5.8). Mükemmel diziler literatürde detaylı bir şekilde çalışılmış ve onların bir çok uygulaması üretilmiştir (bkz. [7]). Bu yüzden, bizim teoremlerimizi neredeyse mükemmel dizilere uygulayıp, onların var olmama durumlarında gerekli koşulları belirttik (bkz. Corollary 5.9-(ii) ve 5.11-(ii)).

Buna ek olarak, γ -Butson Hadamard matrisinin köşegeninin sıfır olma durumunda bu matris, γ -Konferans matrisi adını alır. Benzer olarak, γ -Butson Hadamard matrisinin ve m -li neredeyse mükemmel dizilerinin birbirlerine denklikleri gibi, bir γ -Konferans matrislerinin de neredeyse mükemmel dizilere denklikleri vardır (bkz. Remark 5.8). Bölüm 5'te, γ -Konferans matrisleri ve m -li neredeyse mükemmel diziler için benzer varolmama sonuçları elde ettik (bkz. Corollary 5.10 ve 5.12).

Dolanır γ -Butson-Hadamard matrislerinin ve küçük $|\gamma|$ için γ tipinde neredeyse mükemmel dizilerinin var olan durumları da tez kapsamında düşünülebilir. Çünkü, küçük $|\gamma|$ değerlerine sahip mükemmel diziler bir çok uygulamada kullanılır. Bu yüzden, $v \in \{1, 2, \dots, 11\}$ ve $m \in \{1, 2, \dots, 11\}$ için MAGMA'yı kullanarak detaylı bir bilgisayar taraması yaptık ve γ tipinde neredeyse mükemmel dizilerin varlığı (ya da dolanır γ -Butson Hadamard matrisi) için γ aradık. γ tipinde yeni bir çok neredeyse mükemmel diziler elde ettik gerçekten de çok küçük γ 'ya sahip bazı diziler bulduk (bkz. Tablo 5.1). Uygulamamızın MAGMA kodları tezin ekler bölümünde verilmiştir.

Sonuç olarak, tezde, bir Butson-Hadamard matrisi ile kriptografik fonksiyon arasındaki ilişki araştırıldı. Kriptografide, gizlilik (ya da güvenlik) doğrusal olmayan Boolean fonksiyonlar aracılığıyla şifreli metnin içindeki mesajı karıştıran blok şifreleme kullanılarak sağlanır. Lineer olmama durumu maksimum olan bir Boolean fonksiyonu, *Bent fonksiyon* olarak adlandırılır. Butson Hadamard matrisleri, kriptografik bent fonksiyonlarının bir eşiti (dengi) olarak bilinir (bkz. [10] ya da Teorem 6.7). Bölüm 6'da bu denklik kullanarak, γ -Butson-

Hadamard matrisini bir Boolean fonksiyonuna dönüştürüldü. Bir hayli küçük bir $|\gamma|$ değerine sahip dolanır γ -Butson-Hadamard matrisleri kullanılarak elde edilen büyük bir lineer olmama ölçüsüne sahip Boolean fonksiyonları bulunabileceği gözlemlenmiştir (bkz. Tablo 6.1).

Anahtar Kelimeler: Butson-Hadamard matrisleri, cebirsel sayı cisimleri, neredeyse mükemmel diziler, konferans matrisleri, kriptografik fonksiyonlar

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to Assist. Prof. Dr. Oğuz YAYLA for supervising this thesis and valuable suggestions. And I express sincere appreciation to him for his guidance, insight and cooperation throughout the research without whom this work would never be finished.

A huge thanks to grandma Şükran Saraç and grandpa Sadık Saraç for all their support over the years, encouragement and all the beautiful things that they have done for me.

I would like to thank to my friends who have always been up not also for support but also for a good laugh. I am thankful to them for their patience and support.

I acknowledge financial support from TUBİTAK-1002 program during my graduate academic life.

Lastly, I owe my thanks to my family for their continuous support throughout my life.

TABLE OF CONTENTS

	<u>Page</u>
ABSTRACT	i
ÖZET	ii
ACKNOWLEDGEMENT	vi
TABLE OF CONTENTS	vii
NOTATIONS	x
1 INTRODUCTION	1
2 Algebraic Number Theory	4
2.1 Factorization of an element	5
2.2 Factorization of an ideal	6
2.3 Cyclotomic Fields	8
3 Ideal Factorization Method	9
4 Norm Method	13
5 Application to Butson-Hadamard Matrix, Conference Matrix, Sequences	15
6 Cryptographic Applications	23
7 CONCLUSION	28
REFERENCES	29
APPENDICES	31
CURRICULUM VITAE	36

LIST OF FIGURES

Figure 3.1. Ideal Decomposition of D for value $v = 5, \gamma = 1 - \zeta_{23} - \zeta_{23}^{22}$	11
Figure 3.2. Ideal Decomposition of D for value $v = 46, \gamma = 1 - \zeta_{23} - \zeta_{23}^{22}$	11
Figure 3.3. Ideal Decomposition of D for value $v = 39, \gamma = 1 - \zeta_{23} - \zeta_{23}^{22}$	12
Figure 4.1. Ideal Decomposition of D for value $v = 30, \gamma = 1 - \zeta_{23} - \zeta_{23}^{22}$	14

LIST OF TABLES

Table 3.1. The class number h_m of $\mathbb{Q}(\zeta_m)$ for $m \leq 70$ [15].	10
Table 5.1. Samples of perfect sequences with non-integer correlations	22
Table 6.1. Samples of γ -Butson Hadamard Matrices, corresponding Boolean functions f and their Walsh spectrum \hat{F}	26

NOTATIONS

\mathbb{Z}	Integers
\mathbb{Q}	Rationals
\mathbb{R}	Reals
\mathbb{C}	Complex numbers
$b a$	b divides
$L : K$	Field extension
$\langle x \rangle$	Ideal generated by x
A	Algebraic numbers
B	Algebraic Integers
\mathcal{O}	Ring of Integers of number field
\mathcal{O}_K	Ring of Integers of number field K
$\mathbb{Z}[\zeta_m]$	Ring of integers of Cyclotomic Field
$a \sim b$	Equivalence class
a_{ij}	Entry of matrix

1. INTRODUCTION

Hadamard matrices are used in computational mathematics and quantum computer science. They have also been used in many practical areas e.g. telecommunication of satellites, modern cell phones and wireless networks. Modern CDMA based cell phones use Hadamard matrices to modulate the signals and to minimize the interference between signals arriving at the base station. Information hiding in wireless networks, optical telecommunication, neuroscience and pattern recognition are other practical areas where Hadamard matrices are used. In addition, Hadamard matrices are directly applied in computer science, for example, Hadamard codes (known as best error correcting codes) and Hadamard gates (used in quantum gates), see [8] for details and other applications.

In this thesis, a class of Butson-Hadamard matrices is studied and their applications are investigated. Very recently, new properties of m -ary γ -Butson-Hadamard matrices for $\gamma \in \mathbb{Z}$ are studied in [16]. In this thesis, we study m -ary γ -Butson-Hadamard matrices for $\gamma \in (\mathbb{Z}[\zeta_m] \cap \mathbb{R}) \setminus \mathbb{Z}$, and look for new γ -Butson-Hadamard examples and their existence requirements, where $m \in \mathbb{Z}^+$ and ζ_m is a primitive m -th root of unity. We use the methods in algebraic number theory and results in [16] to find new results on m -ary γ -Butson-Hadamard matrices. Moreover, these new results on Hadamard matrices are used in the investigation of new applications in cryptography and coding theory.

The aim of this study is to analyze the γ -Butson-Hadamard matrices with new methods and then apply them to the cryptography and coding theory. An extension of analysis in recent work [16] on Butson-Hadamard matrices is developed and then new γ -Butson Hadamard matrices are explored.

A *Hadamard matrix* is a square matrix with entries ± 1 whose rows are orthogonal to each other. First generalization of Hadamard matrices was made by Butson in 1962. Butson [3] handled complex m -th root of unity for entries of Hadamard matrices, instead of 2-th root of unity. γ -Butson-Hadamard matrices are similar to Butson-Hadamard matrices, except inner product of a row with a complex conjugate of another row is γ . The most common result for Butson-Hadamard matrices is presented by [2] and [16].

Winterhof et al. [16] reduces the existence condition of a γ -Butson Hadamard matrix to an equation over ring of integers of a cyclotomic field. Namely, they consider the solutions $\alpha \in \mathbb{Z}[\zeta_m]$ of the following equation

$$\alpha \bar{\alpha} = ((\gamma + 1)v - \gamma)(v - \gamma)^{v-1}, \quad (1.1)$$

where $v \in \mathbb{Z}^+$ is the dimension of the γ -Butson Hadamard matrix and $\gamma \in \mathbb{Z}$. Then they consider the principal ideal factorization of $D = ((\gamma + 1)v - \gamma)(v - \gamma)^{v-1}$ and deal with the unsolvability conditions of (1.1). They only consider integer γ for ideal factorization of D . In this thesis, we extend this method to $\gamma \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$ in Chapter 3. For the unsolvability of (1.1) in case $\gamma \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$, we require an extra condition that the norm of nonprincipal part of D is relatively prime to the norm of principal part of D (see Theorem 3.3).

Secondly, in Chapter 4, another novel method is built up for checking the cases in which a γ -Butson Hadamard matrix does not exist for certain $\gamma \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$. We use the fact that the norm of a prime ideal dividing α in (1.1), also divides $\bar{\alpha}$. Therefore, for any prime ideal \mathfrak{p} dividing D , if the norm of D divided by the norm of \mathfrak{p} is relatively prime to the norm of \mathfrak{p} , then (1.1) has no solution (see Theorem 4.1). In particular, if the norm of D is square-free then it is clear that (1.1) has no solution (see Corollary 4.2). In addition, we perform an exhaustive computer search by using MAGMA [1] on the set $v \in \{2, 3, \dots, 100\}$ for fixed m and ζ and for the non-existence of the equation (1.1) to see the strength of Theorems 3.3 and 4.1. It is seen that Theorems 3.3 and 4.1 exclude the existence of many values, on the other hand, we see that they do not cover each other (see Remark 4.4). MAGMA codes of our implementation are given in Appendix of this thesis.

We applied our two novel results (Theorem 3.3 and Theorem 4.1) to γ -Butson-Hadamard matrices in Chapter 5. Namely, we look for dimension $v \in \mathbb{Z}$ and $\gamma \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$ for which a γ -Butson-Hadamard matrix does not exist. This is equivalent to finding necessary conditions for solvability of $\alpha\bar{\alpha} = ((\gamma + 1)v - \gamma)(v - \gamma)^{v-1}$ for some $\alpha \in \mathbb{Z}[\zeta_m]$. Hence, by using our main theorems we obtain non-existence results for γ -Butson-Hadamard matrices (see Corollaries 5.9-(i) and 5.11-(i)). On the other hand, the first row of a circulant¹ γ -Butson-Hadamard matrix is equivalent to a *nearly perfect sequence* (see [5] and Remark 5.8 in this thesis). Perfect sequences are extensively studied in literature and they have many applications (see [7]). Therefore, we apply our main theorems to nearly perfect sequences and state the necessary conditions for their non-existence (see Corollaries 5.9-(ii) and 5.11-(ii)).

Furthermore, if the diagonal of a γ -Butson-Hadamard matrix is allowed to be 0 then such a matrix is called a γ -Conference matrix. Similar to the equivalence of a γ -Butson-Hadamard matrix and an m -ary nearly perfect sequence, a γ -Conference matrix is equivalent to an

¹the other rows are cyclic shift of the first row

almost m -ary nearly perfect sequence (see Remark 5.8). In Chapter 5, we obtain analogous non-existence results for γ -Conference matrices and almost m -ary nearly perfect sequences (see Corollaries 5.10 and 5.12).

The existence cases of circulant γ -Butson-Hadamard matrices and nearly perfect sequence of type γ for small $|\gamma|$ is also considered in this thesis. Because, perfect sequences with small integer γ values are used in many applications. Hence, we perform an exhaustive computer search by using MAGMA [1] on period $v \in \{1, 2, \dots, 11\}$ and alphabet $m \in \{1, 2, \dots, 11\}$, and look for γ , for which a nearly perfect sequence of type γ (or a circulant γ -Butson-Hadamard matrix) exists. We obtain many new nearly perfect sequences of type γ , in deed we have some sequences with very small $|\gamma|$ (see Table 5.1). MAGMA codes of our implementation are given in Appendix of this thesis.

Finally, in this thesis, the relationship between a Butson-Hadamard matrix and a cryptographic function is investigated. In cryptography, secrecy (or confidentiality) is satisfied by using block ciphers which confuses a message into a ciphertext via a nonlinear *Boolean function*. A nonlinear Boolean function attaining the maximum nonlinearity is called a *bent function*. It is known that a Butson-Hadamard matrix is equivalent to cryptographic bent function (see [10] or Theorem 6.7 in this thesis). By using this equivalence, we convert a γ -Butson-Hadamard matrix into a Boolean function in Chapter 6. It is seen that one can find a highly nonlinear Boolean function via circulant γ -Butson-Hadamard matrices having very small $|\gamma|$ values (see Table 6.1).

The outline of this thesis is as follows. In Chapter 2, the definitions and the theorems from algebraic number theory are presented without proofs. In Chapter 3, a novel method based on principal ideal factorization is presented. In Chapter 4, a new result for deciding the non-existence of a solution to (1.1) is given. Then, in Chapter 5, the consequences of the results given in Chapters 3 and 4 are applied to Hadamard matrices, Conference matrices and sequences. Next, the a cryptographic application of the results given Chapter 5 is presented in Chapter 6. Finally, the conclusion of this thesis is given in Chapter 7.

2. Algebraic Number Theory

In this chapter, primary concepts in algebraic number theory are studied since the factorization of ideals over a ring of integers of a number field is used as a tool in the preceding chapters. A ring of integers of a number field may not possess a unique factorization of elements. If a ring of integers is not a principal ideal domain, then unique factorization of elements into irreducibles fails. However, they do still retain many important algebraic properties of \mathbb{Z} . In particular, they possess unique factorization of non-zero ideals. Hence, we should consider ideals, rather than elements when we consider a factorization. It is known that factorization of an ideal into prime ideals is unique over a Dedekind domain, and a ring of integers is a particular example of Dedekind domains [9, p.175]. This is an outline of this chapter, and the details are below. For proofs of theorems and other details please see [14] and [9].

Definition 2.1. [4, p.106] *A number field is a commutative field of characteristic 0 which is a finite extension of the field \mathbb{Q} of rational numbers.*

Definition 2.2. [9, p.66] *Let be $a_0, a_1, a_2, \dots, a_n \in \mathbb{Q}$ and $a_0 \neq 0$. A complex number α satisfying $a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n = 0$ is called an algebraic number. Let be $b_1, b_2, \dots, b_n \in \mathbb{Z}$. A complex number α satisfying $x^n + b_1x^{n-1} + \dots + b_n = 0$ is called an algebraic integer.*

Proposition 2.3. [4, p.126] *Let α and β be algebraic integers. Then $\alpha\beta$ and $\alpha + \beta$ are algebraic integers.*

Proposition 2.4. [4, p.126] *Let be $\alpha \in \mathbb{C}$ and $P(X)$ be a monic polynomial with algebraic integer coefficients. Then α is an algebraic integer if $P(\alpha) = 0$.*

A unit is called non-zero algebraic integer whose inverse is also an algebraic integer. The algebraic integers form a subring of the field of algebraic numbers. For any number field K and the set of algebraic integers B , $\mathcal{O} = B \cap K$ is called the ring of integers of K . We will use term \mathcal{O}_K to grasp which field has the ring of integers. The \mathcal{O}_K is the subring of \mathbb{C} , on account of the fact that both K and B are subrings of \mathbb{C} . Moreover, $\mathbb{Z} \subseteq \mathbb{Q} \subseteq K$ and $\mathbb{Z} \subseteq B$ namely, $\mathbb{Z} \subseteq \mathcal{O}$. Let $\alpha \in K$, then $c\alpha \in \mathcal{O}$ for some non-zero \mathbb{Z} . We note that for an algebraic number $\theta \in B$; a number field has the form $\mathbb{Q}(\theta)$ [14, Theorem 2.2].

2.1. Factorization of an element

In this section, factorization of an element is studied in the ring of integers of an algebraic number field. The existence and uniqueness of factorizations are dealt with in this section.

A non-unit element p is called *irreducible* if $p = mn$ then one of m or n must be a unit. A non-unit element p is called *prime* if $p|mn$ then $p|m$ or $p|n$. If factorization into primes is possible, then it is unique. In contrast, factorization into irreducibles may not be unique even when it is possible. For instance, if we work in $\mathbb{Z}[\sqrt{-10}]$, then there are two factorizations $10 = 2 \cdot 5$ and $10 = \sqrt{-10} \sqrt{-10}$. Here the elements $2, 5, \sqrt{-10}$ are all irreducible, however, they are not prime. We will see in a moment that even though factorization into irreducibles is always possible in \mathcal{O}_K , there is an extensive list of \mathcal{O}_K examples where such a factorization is not unique.

Any element $x \in R$ may be trivially factorized as $x = uy$ where $y = u^{-1}x$, if u is a unit in a ring R . For a unit u if $x = uy$, then the element y is called an *associate* of x . Factorization of $x \in R$, $x = yz$ is said to be *proper* if y or z are not units. If not a factorization is proper, then one of the factors is a unit and the other is an associate of x . If a non-unit is reducible in a domain D , then $x = mn$. If either of m or n is reducible, we can express it as a product of proper factors; then carry on this process, seeking to write

$$x = p_1 p_2 \dots p_m$$

where each p_i is irreducible. If every $x \in D$, neither a unit nor zero, is a product of a finite number of irreducibles, then factorization into irreducibles is possible in D .

Let α be a non-zero nonunit algebraic integer. Since $\alpha = \sqrt{\alpha} \sqrt{\alpha}$ and α is an algebraic integer, then α is not irreducible. Hence, any element in the ring B of all algebraic integers are reducible, so factorization into irreducibles is not possible in B . Thus, it is significant to study domains in which factorization of an element into irreducibles is possible.

Definition 2.5. [14, p.80] *If there exists some M for which $I_m = I_M$ for all $m \geq M$ for a given ascending chain of ideals of D*

$$I_0 \subseteq I_1 \subseteq \dots \subseteq I_m \subseteq \dots$$

then an integral domain D is called Noetherian. This condition is called the ascending chain condition of ideals.

Let an integral domain D be Noetherian, then every non-empty set of ideals of D is of a maximal element and vice versa.

We note that an integral domain D is Noetherian if and only if every non-empty set of ideals of D has a maximal element. This means that an element is not properly contained in every other element. This condition is called *the maximal condition*. Now, we state the importance of a Noetherian domain in factorization of elements.

Theorem 2.6. [14, p.81] *A factorization into irreducibles is possible in D , if a domain D is Noetherian.*

Theorem 2.7. [14, p.81] *In a number field K , the ring of integers \mathcal{O}_K is Noetherian.*

Therefore, it is now clear that factorization into irreducibles is possible in \mathcal{O}_K . Now the criteria for being a unique factorization domain is discussed. We have already noted that a prime p in \mathbb{Z} satisfies the property that $p|mn$ implies $p|m$ or $p|n$. Similarly, in a domain D , an element x is called to be *prime* if it is not zero or a unit and $x|ab$ implies $x|a$ or $x|b$. So, a prime in a domain D is always irreducible clearly. Then the main theorem follows.

Theorem 2.8. [14, p.87] *Suppose that factorization into irreducibles in a domain D is possible. Then factorization in D is unique if and only if every irreducible is prime in D .*

A domain D is called a *unique factorization domain*, if factorization into irreducibles is possible and unique. In a unique factorization domain all irreducibles are primes, so we may speak of a factorization into irreducibles as a *prime factorization*. A prime factorization is unique in the usual sense.

2.2. Factorization of an ideal

Unique factorization of irreducible elements on the ring of integers \mathcal{O}_K of some number fields K does not hold. Therefore, *ideal factorization* is used for solving this issue. If d is a proper ideal of \mathcal{O}_K and there are no ideals of \mathcal{O}_K certainly between d and \mathcal{O}_K , then d is called a *maximal ideal* of \mathcal{O}_K . The ideal $d \neq \mathcal{O}_K$ of \mathcal{O}_K is *prime* if, whenever b and c are ideals of \mathcal{O}_K with $bc \subseteq d$, then either $b \subseteq d$ or $c \subseteq d$. And, it is denoted that $d|b$ or $d|c$. It is clear that every maximal ideal is prime.

First, some properties of a ring of integers of a number field are presented below, which play important role in classification of domains having unique factorization.

Proposition 2.9. [14, p.106] *The ring of integers \mathcal{O}_K of a number field K has the following properties.*

(i) *It is a domain, with field of fractions K ,*

(ii) *it is Noetherian.*

(iii) *If $\alpha \in K$ satisfies a monic polynomial equation with coefficients in \mathcal{O}_K then $\alpha \in \mathcal{O}_K$,*

(iv) *Every non-zero prime ideal of \mathcal{O}_K is maximal.*

In general, we will call a domain *Dedekind* if it satisfies the properties (i)-(iv) above.

Theorem 2.10. [6, p.40] *Let \mathcal{D} be a Dedekind domain. Any non-zero integral ideal d in \mathcal{D} may be written as a product*

$$d = p_1 \dots p_n$$

where the p_i are prime ideals (not necessarily distinct), and this expression is unique up to the order of the factors.

Therefore, in Dedekind domains, every non-zero ideal can be factored uniquely as a product of prime ideals. We know that the ring \mathcal{O}_K of integers of an algebraic number field K is Dedekind, hence unique factorization of ideals holds in \mathcal{O}_K . Moreover, it is noted that factorization of elements into irreducibles is unique in a ring of integers if and only if every ideal is principal [14, Theorem 5.21]. Generally, a ring R is a principal ideal domain, if it is a Dedekind domain and a unique factorization domain.

For a principal ideal d in a ring of integers \mathcal{O}_K we have a unique factorization into ideals,

$$\langle d \rangle = I_1 I_2 \dots I_n,$$

but the ideals I_1, I_2, \dots, I_n may not be principal. However, the ideals in \mathcal{O}_K are not far from being principal, having at most two generators.

We would like to know how far is any ideal in a domain from unique factorization. We should give a definition first.

Definition 2.11. [12, p.11] *Two ideals E, M in a domain D are said to be equivalent if there exist non-zero $\epsilon, \mu \in D$ such that $(\epsilon)E = (\mu)M$. This is an equivalence relation. The equivalence classes are called ideal classes. The number of ideal classes, h_K , is called the class number of K .*

We note that $h_K = 1$ if and only if \mathcal{O}_K is a unique factorization domain (UFD) and if and only if \mathcal{O}_K is a principal ideal domain (PID) [9, p.178]. Therefore, the class number measures how far \mathcal{O}_K is from being a UFD and PID. We finalize this section with two results on the class number of a number field.

Theorem 2.12. [9, p.178] *The class number of K is finite.*

Proposition 2.13. [9, p.179] *For any ideal $A \subset \mathcal{O}$, there is an integer $k, 1 \leq k \leq h_F$, such that A^k is principal.*

2.3. Cyclotomic Fields

In this section, a special kind of number fields is investigated. The cyclotomic field is one of the form $\mathbb{Q}(\zeta_m)$ where $\zeta_m = e^{2\pi i/m}$ is a primitive complex m -th roots of unity.

The minimum polynomial of $\zeta_m = e^{2\pi i/m}$ over \mathbb{Q} is

$$f(t) = \prod_{i, (i,m)=1} t - \zeta_m^i$$

Thus, the extension degree of $\mathbb{Q}(\zeta_m)$ is $\phi(m)$, where ϕ is the Euler Phi function. The conjugates of ζ_m are ζ_m^i for $1 \leq i \leq m - 1$ and $\gcd(i, m) = 1$. Namely, the monomorphisms of cyclotomic fields are given as $\sigma_i : \mathbb{Q}(\zeta_m) \rightarrow \mathbb{C}$ for $1 \leq i \leq m - 1$ and $\gcd(i, m) = 1$:

$$\sigma_i(\zeta_m) = \zeta_m^i$$

Theorem 2.14. [15, p.11] $\mathbb{Z}[\zeta_m]$ is the ring \mathcal{O} of integers of $\mathbb{Q}(\zeta_m)$.

Proof. Assume that $\beta = \beta_0 + \beta_1\zeta_m + \dots + \beta_{p-2}\zeta_m^{p-2}$ is an integer in $\mathbb{Q}(\zeta_m)$. It should be shown that the coefficients β_i are integers. For $0 \leq k \leq p - 2$, the element

$$\beta\zeta_m^{-k} - \beta\zeta_m$$

is an integer.

3. Ideal Factorization Method

In this chapter, we study the equation $D = \alpha\bar{\alpha}$ over $\mathbb{Z}[\zeta_m]$ for some $m \in \mathbb{Z}^+$ and $D \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$. We present a condition for the non-existence of a solution $\alpha \in \mathbb{Z}[\zeta_m]$ to this equation. Our method extends the method in [16]. The authors in [16] consider the case $D \in \mathbb{Z}$, whereas we study $D \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$. In particular, we consider $D = ((\gamma + 1)v - \gamma)(v - \gamma)^{v-1}$ for some $m, v \in \mathbb{Z}^+$ and $\gamma \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$, which we get in case of proving non-existence of some Butson-Hadamard matrices in Chapter 5.

We first give definitions of the *norm of an element* in a number field and *norm of an ideal* of the ring of integers of a number field.

Definition 3.1. [14, p.49] Let $\sigma_1, \dots, \sigma_m$ be monomorphisms $K \rightarrow \mathbb{C}$ and let $K = \mathbb{Q}(\theta)$ be a number field of degree m . $\alpha \in K$ is an algebraic integer. For any $\alpha \in K$, we define the norm.

$$N_K(\alpha) = \prod_{i=1}^m \sigma_i(\alpha)$$

Definition 3.2. [14, p.115] Let \mathcal{O}_K be the ring of unit of a number field K and I be non-zero ideal of \mathcal{O}_K , the norm of I is defined by

$$N(I) = |\mathcal{O}_K/I|.$$

We note that if $\mathfrak{a} = \langle a \rangle$ is a principal ideal then $N(\mathfrak{a}) = \langle N(a) \rangle$ [14, Corollary 5.10]. If $\mathfrak{a}|\mathfrak{b}$ then $N(\mathfrak{a})|N(\mathfrak{b})$ [14, Theorem 5.12]. For an ideal \mathfrak{a} , its conjugate ideal is $\bar{\mathfrak{a}} := \{\bar{\alpha} : \alpha \in \mathfrak{a}\}$. It can be seen that $N(\mathfrak{a}) = N(\bar{\mathfrak{a}})$ and if \mathfrak{a} is a prime ideal, then $\bar{\mathfrak{a}}$ is also prime ideal.

The main theorem that there is no solution on $D = \alpha\bar{\alpha} \in \mathbb{Z}[\zeta_m]$ for some $\gamma \in \mathbb{Z}[\zeta_m]$ is given below. h_m denotes class numbers of cyclotomic number field $\mathbb{Q}(\zeta_m)$. The class numbers Table 3.1 is listed for $m \leq 70$.

Theorem 3.3. Let $D \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$ such that $D = tq^{2e+1}$ where $q, t \in \mathbb{Z}[\zeta_m]$ and q is squarefree, provided that every prime ideal $\mathfrak{t} \triangleleft \mathbb{Z}[\zeta_m]$ with $\mathfrak{t} | (t)$ is principal, $(q) = \mathfrak{q}_1 \mathfrak{q}_2$ where \mathfrak{q}_1 and \mathfrak{q}_2 are non-principal prime ideals of $\mathbb{Z}[\zeta_m]$, $e > 0$ be rational integer, $\gcd(2e + 1 - 2k, h_m) = 1$ for $0 \leq k \leq e - 1$ and $\gcd(N(q), N(t)) = 1$. Then, there exists no $\alpha \in \mathbb{Z}[\zeta_m]$ satisfying $D = \alpha\bar{\alpha}$.

Proof. We first suppose that there exists $\alpha \in \mathbb{Z}[\zeta_m]$ for $\alpha\bar{\alpha} = tq^{2e+1}$ such that

Table 3.1: The class number h_m of $\mathbb{Q}(\zeta_m)$ for $m \leq 70$ [15].

m	h_m	m	h_m	m	h_m	m	h_m	m	h_m	m	h_m
1	1	11	1	21	1	31	9	41	121	51	5
2	1	12	1	22	1	32	1	42	1	52	3
3	1	13	1	23	3	33	1	43	211	53	48891
4	1	14	1	24	1	34	1	44	1	54	1
5	1	15	1	25	1	35	1	45	1	55	10
6	1	16	1	26	1	36	1	46	3	56	2
7	1	17	1	27	1	37	37	47	695	57	9
8	1	18	1	28	1	38	1	48	1	58	8
9	1	19	1	29	8	39	2	49	43	59	41421
10	1	20	1	30	1	40	1	50	1	60	1

$$(\alpha) = \mathfrak{t}_1 \mathfrak{q}_1^{2e+1-k} \mathfrak{q}_2^k$$

$$(\bar{\alpha}) = \mathfrak{t}_2 \mathfrak{q}_1^k \mathfrak{q}_2^{2e+1-k}$$

for some $\mathfrak{t} \triangleleft \mathbb{Z}[\zeta_m]$. We have

$$(\alpha) = \mathfrak{t}_1 \mathfrak{q}_1^{2e+1-k} \mathfrak{q}_2^k = \mathfrak{t}_1 \mathfrak{q}_1^{2e+1-2k} q^k$$

We know that \mathfrak{t}_1 and q are principal ideals of $\mathbb{Z}[\zeta_m]$ but $\mathfrak{q}_1^{2e+1-2k}$ is nonprincipal since $\gcd(2e+1-2k, h_m) = 1$. Hence we get a contradiction.

Next, we assume that $\alpha = \mathfrak{t}_1 q^s$, $\bar{\alpha} = \mathfrak{t}_2 q^{2e+1-s}$ for some principal ideals $\mathfrak{t}_1, \mathfrak{t}_2 \triangleleft \mathbb{Z}[\zeta_m]$ and $s \in \mathbb{Z}^+ \cup \{0\}$, $s \leq e$. Then, $q^{2e+1-2s} | \mathfrak{t}_1$. However, this contradicts to $\gcd(N(q), N(\mathfrak{t})) = 1$.

We now give an example of Theorem 3.3.

Example 3.4. Let $D = ((-\zeta_{23} - \zeta_{23}^{22})5 + 1 + \zeta_{23} + \zeta_{23}^{22})(6 + \zeta_{23} + \zeta_{23}^{22})^4 \in \mathbb{Z}[\zeta_{23}]$ be obtained by setting $v = 5$, $m = 23$, $\gamma = -1 - \zeta_{23} - \zeta_{23}^{22}$. D has two non-principal prime ideals such that $D = \mathfrak{p}_1^4 \mathfrak{p}_2^4 \mathfrak{p}_3^4 \mathfrak{q}_4 \mathfrak{q}_5$ where $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3 \triangleleft \mathbb{Z}[\zeta_{23}]$ are principal prime ideals and $\mathfrak{q}_4, \mathfrak{q}_5 \in \mathbb{Z}[\zeta_{23}]$ are the non-principal prime ideals, see Figure 3.1. By Theorem 3.3 we say that there is no $\alpha \in \mathbb{Z}[\zeta_m]$ satisfying $D = \alpha \bar{\alpha}$.

$$D = ((-\zeta_{23} - \zeta_{23}^{22})5 + 1 + \zeta_{23} + \zeta_{23}^{22})(6 + \zeta_{23} + \zeta_{23}^{22})^4$$

Figure 3.1: Ideal Decomposition of D for value $v = 5, \gamma = 1 - \zeta_{23} - \zeta_{23}^{22}$

We note that the method given in Theorem 3.3 to the case that q has more than two non-principal ideals factors does not work. We give two examples below. In the first one, powers of the non-principal ideals are 1, but in the later, some of the non-principal ideals have power more than 1.

Example 3.5. Let $D = ((-\zeta_{23} - \zeta_{23}^{22})46 + 1 + \zeta_{23} + \zeta_{23}^{22})(47 + \zeta_{23} + \zeta_{23}^{22})^{45} \in \mathbb{Z}[\zeta_{23}]$ be obtained by setting $v = 46, m = 23, \gamma = -1 - \zeta_{23} - \zeta_{23}^{22}$. D has four non-principal prime ideals such that $D = \mathfrak{p}_1 \mathfrak{p}_2^{45} \mathfrak{p}_3^{45} \mathfrak{q}_4 \mathfrak{q}_5 \mathfrak{q}_6 \mathfrak{q}_7$ where $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3 \triangleleft \mathbb{Z}[\zeta_{23}]$ are principal prime ideals and $\mathfrak{q}_4, \mathfrak{q}_5, \mathfrak{q}_6, \mathfrak{q}_7 \triangleleft \mathbb{Z}[\zeta_{23}]$ are the non-principal ideals. The methodology in Example 3.4 does not work for this example. Note that $(\alpha) = \mathfrak{t}_1 \mathfrak{q}_5 \mathfrak{q}_7$ is a principal ideal and satisfies $D = \alpha \bar{\alpha}$ for a convenient principal ideal $\mathfrak{t}_1 \triangleleft \mathbb{Z}[\zeta_{23}]$ such that $\mathfrak{t}_1 \mid D$. The ideal factorization of this example is shown in Figure 3.2.

$$D = ((-\zeta_{23} - \zeta_{23}^{22})46 + 1 + \zeta_{23} + \zeta_{23}^{22})(47 + \zeta_{23} + \zeta_{23}^{22})^{45}$$

Figure 3.2: Ideal Decomposition of D for value $v = 46, \gamma = 1 - \zeta_{23} - \zeta_{23}^{22}$

Example 3.6. Let $D = ((-\zeta_{23} - \zeta_{23}^{22})39 + 1 + \zeta_{23} + \zeta_{23}^{22})(40 + \zeta_{23} + \zeta_{23}^{22})^{38} \in \mathbb{Z}[\zeta_{23}]$ be obtained by setting $v = 39, m = 23, \gamma = -1 - \zeta_{23} - \zeta_{23}^{22}$. D has four prime non-principal ideals such that $D = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \mathfrak{p}_4 \mathfrak{p}_5^2 \mathfrak{p}_6^{38} \mathfrak{p}_7^{38} \mathfrak{p}_8^{38} \mathfrak{q}_9 \mathfrak{q}_{10} \mathfrak{q}_{11}^{38} \mathfrak{q}_{12}^{38}$ where $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7, \mathfrak{p}_8 \triangleleft \mathbb{Z}[\zeta_{23}]$ are principal ideals and $\mathfrak{q}_9, \mathfrak{q}_{10}, \mathfrak{q}_{11}, \mathfrak{q}_{12} \triangleleft \mathbb{Z}[\zeta_{23}]$ are non-principal ideals. Note that $(\alpha) = \mathfrak{t}_1 \mathfrak{q}_{10} \mathfrak{q}_{12}^{38}$ is a principal ideal and satisfies $D = \alpha \bar{\alpha}$ for a convenient principal ideal $\mathfrak{t}_1 \triangleleft \mathbb{Z}[\zeta_{23}]$ such that $\mathfrak{t}_1 \mid D$. The ideal factorization of this example is shown in Figure 3.3.

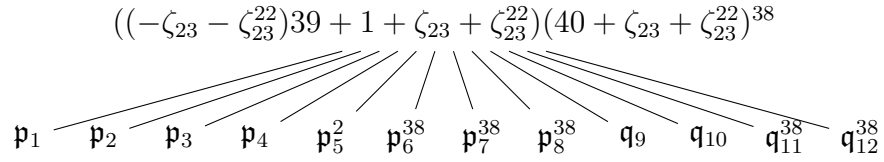


Figure 3.3: Ideal Decomposition of D for value $v = 39, \gamma = 1 - \zeta_{23} - \zeta_{23}^{22}$

In order to speak of the non-existence of a solution to the equation $D = \alpha\bar{\alpha}$ for $\alpha \in \mathbb{Z}[\zeta_m]$ with D is divisible by more than two non-principal ideals, one can consider principal parts produced by the non-principal ones. We remark this method below.

Remark 3.7. If D is divisible by four non-principal prime ideals which are distinct and relatively prime to each other, then there exists no solution $\alpha \in \mathbb{Z}[\zeta_m]$ satisfying $D = \alpha\bar{\alpha}$. In other words, let $q_1, q_2, q_3, q_4 \triangleleft \mathbb{Z}[\zeta_m]$ be non-principal prime ideals of $\mathbb{Z}[\zeta_m]$ dividing D . Assume that $q_1q_2, q_3q_4, q_1q_3, q_2q_4$ are all principal in $\mathbb{Z}[\zeta_m]$. If $\gcd(N(q_1q_2), N(q_3q_4)) = 1$, $\gcd(N(q_1q_3), N(q_2q_4)) = 1$, then we can conclude that there exists no solution.

4. Norm Method

In this section, we present another method for deciding an existence of a solution $\alpha \in \mathbb{Z}[\zeta_m]$ to the equation $D = \alpha\bar{\alpha}$ where $m \in \mathbb{Z}^+$ and $D \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$.

Theorem 4.1. *Let $\mathfrak{p} \triangleleft \mathbb{Z}[\zeta_m]$ be a prime ideal with $\mathfrak{p} \mid D$ and $\gcd(N(D)/N(\mathfrak{p}), N(\mathfrak{p})) = 1$. Then there is no solution $\alpha \in \mathbb{Z}[\zeta_m]$ satisfying $D = \alpha\bar{\alpha}$.*

Proof. Assume $\alpha \in \mathbb{Z}[\zeta_m]$ is a solution of $D = \alpha\bar{\alpha}$ and $\mathfrak{p} \triangleleft \mathbb{Z}[\zeta_m]$ is a prime ideal factor of α . We know that if $\mathfrak{p} \mid D$, then $N(\mathfrak{p}) \mid N(D)$. We have $N(\mathfrak{p}) \nmid \frac{N(D)}{N(\mathfrak{p})}$ since $\gcd(N(D)/N(\mathfrak{p}), N(\mathfrak{p})) = 1$. By $N(\mathfrak{p}) = N(\bar{\mathfrak{p}})$, we have $N(\bar{\mathfrak{p}}) \nmid \frac{N(D)}{N(\mathfrak{p})}$. Hence, $N(\mathfrak{p})N(\bar{\mathfrak{p}}) \nmid N(D)$. This is a contradiction to $D = \alpha\bar{\alpha}$.

There is an immediate consequence of Theorem 4.1.

Corollary 4.2. *If the norm of non-principal part of D is square-free, then there exists no $\alpha \in \mathbb{Z}[\zeta_m]$ satisfying $D = \alpha\bar{\alpha}$.*

Next, we give an example of Theorem 4.1. Below, we consider $D = ((\gamma+1)v - \gamma)(v - \gamma)^{v-1}$ for some $m, v \in \mathbb{Z}^+$ and $\gamma \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$.

Example 4.3. *Let be $v = 30$, $m = 23$, $\gamma = -1 - \zeta_{23} - \zeta_{23}^{22}$. Then $D = ((-\zeta_{23} - \zeta_{23}^{22})39 + 1 + \zeta_{23} + \zeta_{23}^{22})(40 + \zeta_{23} + \zeta_{23}^{22})^{38} \in \mathbb{Z}[\zeta_{23}]$ has four non-principal prime ideal factors, such that $D = \mathfrak{p}_1\mathfrak{p}_2^{29}\mathfrak{q}_3\mathfrak{q}_4\mathfrak{q}_5^{29}\mathfrak{q}_6^{29}$ where $\mathfrak{p}_1, \mathfrak{p}_2 \triangleleft \mathbb{Z}[\zeta_{23}]$ are principal prime ideals and $\mathfrak{q}_3, \mathfrak{q}_4, \mathfrak{q}_5, \mathfrak{q}_6 \triangleleft \mathbb{Z}[\zeta_{23}]$ are non-principal prime ideals. Then,*

$$N(D) = 47^{58} \cdot 229^2 \cdot 63276304836881^2 \cdot 517725371091023^2, N(\mathfrak{p}_1) = 229^2$$

and

$$\gcd\left(\frac{47^{58} \cdot 229^2 \cdot 63276304836881^2 \cdot 517725371091023^2}{229^2}, 229^2\right) = 1.$$

Hence, we say that there is no $\alpha \in \mathbb{Z}[\zeta_{23}]$ satisfying $D = \alpha\bar{\alpha}$ by Theorem 4.1. The ideal factorization of this example is shown in Figure 4.1.

$$\begin{array}{c}
 ((-\zeta_{23} - \zeta_{23}^{22})30 + 1 + \zeta_{23} + \zeta_{23}^{22})(31 + \zeta_{23} + \zeta_{23}^{22})^{29} \\
 \swarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \searrow \\
 \mathfrak{p}_1 \quad \mathfrak{p}_2^{29} \quad \mathfrak{q}_3 \quad \mathfrak{q}_4 \quad \mathfrak{q}_5^{29} \quad \mathfrak{q}_6^{29}
 \end{array}$$

Figure 4.1: Ideal Decomposition of D for value $v = 30, \gamma = 1 - \zeta_{23} - \zeta_{23}^{22}$

Remark 4.4. We performed an exhaustive computer search by using MAGMA [1] to check the cases for which Theorem 4.1 excludes the existence of a solution to $D = \alpha\bar{\alpha}$. We fixed $m = 23, \gamma = -1 - \zeta_{23} - \zeta_{23}^{22}$ and searched on the set $v \in \{2, 3, \dots, 100\}$. We obtained that Theorem 4.1 excludes the existence of a solution for all $v = \{2, 3, \dots, 100\}$ except $\{6, 8, 15, 16, 26, 44, 49, 62, 67, 75, 84, 85, 88, 94\}$.

We note that Theorem 4.1 does not completely cover Theorem 3.3 and vice versa. For $\gamma = -1 - \zeta_{23} - \zeta_{23}^{22}$ and $m = 23$, the existence of a solution to the equation $D = \alpha\bar{\alpha}$ over $\mathbb{Z}[\zeta_{23}]$ for $v \in \{8, 26\}$ can be excluded by Theorem 3.3, but Theorem 4.1. On the other hand, the existence of a solution to the equation $D = \alpha\bar{\alpha}$ over $\mathbb{Z}[\zeta_{23}]$ for $v \in \{9, 10, 11, 12, 13, 14\}$ can be excluded by Theorem 4.1, but Theorem 3.3. Therefore, the two theorems do not cover each other, but they intersect.

5. Application to Butson-Hadamard Matrix, Conference Matrix, Sequences

In this section, we define Butson-Hadamard matrix, conference matrix, perfect and nearly perfect sequences and apply the results of the previous sections.

A *Hadamard matrix* is an $(v \times v)$ square matrix with entries 1 or -1 satisfying $HH^T = vI$. Two examples of Hadamard matrices are given below.

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

A square matrix $H = (h_{ij})$ of order v is called *circulant* if $h_{i+1 \bmod v, j+1 \bmod v} = h_{i,j}$ for all $0 \leq i, j < v$. An example of a circulant matrix H is given below.

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

For an integer $m \geq 2$, let ζ_m denote a primitive complex m -th root of unity and let $\mathcal{E}_m = \{1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{m-1}\}$. The identity matrix is denoted by I and all one matrix is denoted by J .

Definition 5.1. A *Butson-Hadamard matrix* is a square matrix H of order v with entries in \mathcal{E}_m such that $H\overline{H}^T = vI$. It is denoted by $\text{BH}(v, m)$. $\text{BH}(v, 2)$ is so called Hadamard matrix of order v . In general, a γ -*Butson-Hadamard matrix* is a square matrix H of order v with entries in \mathcal{E}_m such that $H\overline{H}^T = (v - \gamma)I + \gamma J$ for a $\gamma \in \mathbb{R} \cap \mathbb{Z}[\zeta_m]$. Similarly, it is denoted by $\text{BH}_\gamma(v, m)$.

We demonstrate the equation $H\overline{H}^T = (v - \gamma)I + \gamma J$ below.

$$\begin{aligned}
H\bar{H}^T &= (v - \gamma)I + \gamma J \\
H\bar{H}^T &= \begin{bmatrix} v - \gamma & 0 & 0 & 0 & 0 \\ 0 & v - \gamma & 0 & 0 & 0 \\ 0 & 0 & v - \gamma & 0 & 0 \\ 0 & 0 & 0 & v - \gamma & 0 \\ 0 & 0 & 0 & 0 & v - \gamma \end{bmatrix} + \begin{bmatrix} \gamma & \gamma & \gamma & \gamma & \gamma \\ \gamma & \gamma & \gamma & \gamma & \gamma \\ \gamma & \gamma & \gamma & \gamma & \gamma \\ \gamma & \gamma & \gamma & \gamma & \gamma \\ \gamma & \gamma & \gamma & \gamma & \gamma \end{bmatrix} \\
&= \begin{bmatrix} \mathbf{v} & \gamma & \gamma & \gamma & \gamma \\ \gamma & \mathbf{v} & \gamma & \gamma & \gamma \\ \gamma & \gamma & \mathbf{v} & \gamma & \gamma \\ \gamma & \gamma & \gamma & \mathbf{v} & \gamma \\ \gamma & \gamma & \gamma & \gamma & \mathbf{v} \end{bmatrix}
\end{aligned}$$

Two examples on the existence of γ -Butson-Hadamard matrices are presented below.

Example 5.2. $BH_\gamma(5,5)$ exists for $\gamma \in \{-\xi_5^3 - \xi_5^2 + 2, 0, 5, \xi_5^3 + \xi_5^2 + 3\}$ with $|\gamma| \in \{1.38, 0, 5, 3.61\}$, respectively. For instance, the matrix H has $\gamma = -\xi_5^3 - \xi_5^2 + 2$ with $|\gamma| = 1.38$

$$H = \begin{bmatrix} 1 & 1 & -\xi_5^2 & 1 & 1 \\ 1 & 1 & 1 & -\xi_5^2 & 1 \\ 1 & 1 & 1 & 1 & -\xi_5^2 \\ -\xi_5^2 & 1 & 1 & 1 & 1 \\ 1 & -\xi_5^2 & 1 & 1 & 1 \end{bmatrix}.$$

Example 5.3. Similarly, we obtained by an exhaustive search that $BH_\gamma(8,5)$ exists for $\gamma \in \{-\xi_5^3 - \xi_5^2 + 5, -\xi_5^3 - \xi_5^2, 8, \xi_5^3 + \xi_5^2 + 1, \xi_5^3 + \xi_5^2 + 6\}$ with $|\gamma| \in \{6.61, 1.61, 8, 0.61, 4.38\}$, respectively. In particular, the matrix H has $\gamma = -\xi_5^3 - \xi_5^2 + 2$ with $|\gamma| = 0.61$

$$H = \begin{bmatrix} 1 & 1 & \zeta_5^2 & \zeta_5^3 & 1 & \zeta_5^3 & \zeta_5 & 1 \\ 1 & 1 & 1 & \zeta_5^2 & \zeta_5^3 & 1 & \zeta_5^3 & \zeta_5 \\ \zeta_5 & 1 & 1 & 1 & \zeta_5^2 & \zeta_5^3 & 1 & \zeta_5^3 \\ \zeta_5^3 & \zeta_5 & 1 & 1 & 1 & \zeta_5^2 & \zeta_5^3 & 1 \\ 1 & \zeta_5^3 & \zeta_5 & 1 & 1 & 1 & \zeta_5^2 & \zeta_5^3 \\ \zeta_5^3 & 1 & \zeta_5^3 & \zeta_5 & 1 & 1 & 1 & \zeta_5^2 \\ \zeta_5^2 & \zeta_5^3 & 1 & \zeta_5^3 & \zeta_5 & 1 & 1 & 1 \\ 1 & \zeta_5^2 & \zeta_5^3 & 1 & \zeta_5^3 & \zeta_5 & 1 & 1 \end{bmatrix}.$$

We now investigate a property that a γ -Butson-Hadamard matrix H satisfy. It is clear that $\det(H) \in \mathbb{Z}[\zeta_m]$ and we have the following equalities:

$$\begin{aligned} H\overline{H}^T &= (v - \gamma)I + \gamma J, \\ \det(H\overline{H}^T) &= \det((v - \gamma)I + \gamma J) \\ \det(H) \det(\overline{H}) &= ((\gamma + 1)v - \gamma)(v - \gamma)^{v-1}. \end{aligned}$$

Therefore, a $\text{BH}_\gamma(v, m)$ exists then the following equation has a solution $\alpha \in \mathbb{Z}[\zeta_m]$

$$\alpha\overline{\alpha} = ((\gamma + 1)v - \gamma)(v - \gamma)^{v-1}. \quad (5.1)$$

Example 5.4. Let $v = 4$. Then the determinant of a Hadamard matrix is obtained as follows. We first reduce rows and columns of $(4 - \gamma)I + \gamma J$, then obtain its determinant from the reduced matrix on the far-right easily.

$$\begin{bmatrix} 4 & \gamma & \gamma & \gamma \\ \gamma & 4 & \gamma & \gamma \\ \gamma & \gamma & 4 & \gamma \\ \gamma & \gamma & \gamma & 4 \end{bmatrix} \rightarrow \begin{bmatrix} 4 & \gamma - 4 & \gamma - 4 & \gamma - 4 \\ \gamma & 4 - \gamma & 0 & 0 \\ \gamma & 0 & 4 - \gamma & 0 \\ \gamma & 0 & 0 & 4 - \gamma \end{bmatrix} \rightarrow \begin{bmatrix} 4 - 3\gamma & 0 & 0 & 0 \\ \gamma & 4 - \gamma & 0 & 0 \\ \gamma & 0 & 4 - \gamma & 0 \\ \gamma & 0 & 0 & 4 - \gamma \end{bmatrix}$$

$$\begin{aligned} H_4\overline{H}_4^T &= (4 - \gamma)I + \gamma J, \\ \det(H_4\overline{H}_4^T) &= \det((4 - \gamma)I + \gamma J) \\ \det(H_4) \det(\overline{H}_4) &= ((\gamma + 1)4 - \gamma)(4 - \gamma)^{4-1}. \\ \det(H_4) \det(\overline{H}_4) &= ((\gamma + 1)4 - \gamma)(4 - \gamma)^3. \end{aligned}$$

Next, the concept of a conference matrix is introduced.

Definition 5.5. A square matrix C of order v with 0 on the diagonal and all off-diagonal entries in \mathcal{E}_m is called a γ -conference matrix $C_\gamma(v, m)$ if $C\overline{C}^T = (v - 1 - \gamma)I + \gamma J$ for a $\gamma \in \mathbb{R} \cap \mathbb{Z}[\zeta_m]$.

A matrix C with entries in \mathcal{E}_3 and having the first row $(0, \zeta_3^2, \zeta_3^2, \zeta_3^2, 1, \zeta_3^2, \zeta_3, \zeta_3, \zeta_3^2, 1, \zeta_3^2, \zeta_3^2, \zeta_3^2)$ is an example of a circulant conference matrix. Note that $C\overline{C}^T = 10I + 2J$.

Similar to the case γ -Butson-Hadamard matrices, we obtain that a γ -conference matrix $C = C_\gamma(v, m)$ satisfies

$$\det(C)\overline{\det(C)} = (\gamma + 1)(v - 1)(v - 1 - \gamma)^{v-1}$$

and hence we have an other main equation

$$\alpha\overline{\alpha} = (\gamma + 1)(v - 1)(v - 1 - \gamma)^{v-1}. \quad (5.2)$$

Therefore, a $C_\gamma(v, m)$ exists then equation (5.2) has a solution $\alpha \in \mathbb{Z}[\zeta_m]$.

We continue with the concept of sequences. A v -periodic sequence $\underline{a} = (a_0, a_1, \dots, a_{v-1}, \dots)$ an m -ary sequence if $a_0, a_1, \dots, a_{v-1} \in \mathcal{E}_m = \{1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{m-1}\}$ and an almost m -ary sequence if $a_0 = 0$ and $a_1, \dots, a_{v-1} \in \mathcal{E}_m$.

For $0 \leq t \leq v - 1$, the autocorrelation function $C_{\underline{a}}(t)$ is defined by

$$C_{\underline{a}}(t) = \sum_{i=0}^{v-1} a_i \overline{a_{i+t}},$$

where \overline{a} is the complex conjugate of $a \in \mathbb{C}$.

Definition 5.6. An m -ary or almost m -ary sequence \underline{a} of period v is called a perfect sequence (PS) if $C_{\underline{a}}(t) = 0$ for all $1 \leq t \leq v - 1$. Similarly, an almost m -ary sequence \underline{a} of period v is called a nearly perfect sequence (NPS) of type γ if $C_{\underline{a}}(t) = \gamma$ for all $1 \leq t \leq v - 1$.

Proposition 5.7. If a NPS of type γ exists, then γ is a real number.

Proof. Let a be a NPS of type γ with period v . We know that autocorrelation value of a is γ and $C_a(t) = C_a(v - t) = \gamma$. So,

$$\begin{aligned}
\gamma &= C_a(t), \\
&= \sum_{i=0}^{v-1} a_i \overline{a_{i+t}}, \\
&= \overline{\sum_{i=0}^{v-1} a_i \overline{a_{i+t}}}, \\
&= \overline{\sum_{i=0}^{v-1} a_{i+t} \overline{a_i}}, \\
&= \sum_{j=t}^{v-1+t} a_j \overline{a_{j-t}} \quad (i+t=j), \\
&= \overline{C_a(-t)}.
\end{aligned}$$

and so

$$\gamma = C_a(t) = \overline{C_a(-t)} = \overline{\gamma}$$

This means that $\gamma \in \mathbb{R}$.

For instance, $(0, \zeta_3^2, \zeta_3^2, \zeta_3^2, 1, \zeta_3^2, \zeta_3, \zeta_3, \zeta_3^2, 1, \zeta_3^2, \zeta_3^2, \zeta_3^2)$ is a 3-ary NPS of period 13 and type $\gamma = 2$.

Remark 5.8. NPSs are equivalent to circulant γ -Butson-Hadamard matrices and conference matrices. Let $\underline{a} = (a_0, a_1, \dots, a_{v-1}, \dots)$ be an m -ary NPS of period v . Let $H = (h_{i,j})$ be a circulant matrix defined by $h_{0,j} = a_j$ for $j = 0, 1, \dots, v-1$ then H is a circulant γ -Butson-Hadamard matrix of order v . Similarly, an almost m -ary NPS is equivalent to a circulant conference matrix.

In this thesis, we consider the case $\gamma \in (\mathbb{Z}[\zeta_m] \cap \mathbb{R}) \setminus \mathbb{Z}$. Such sequences indeed exists and have a counter part in cryptographic and coding theoretic applications (see Chapter 6). For instance, the sequence $\underline{a} = (1, 1, -\xi_5^2, 1, 1)$ has $\gamma = -\xi_5^3 - \xi_5^2 + 2$ with $|\gamma| = 1.38$. The sequence $\underline{a} = (1, 1, \xi_5^2, \xi_5^3, 1, \xi_5^3, \xi_5, 1)$ has $\gamma = -\xi_5^3 - \xi_5^2 + 2$ with $|\gamma| = 0.61$.

Now, we give three direct consequences of Theorem 3.3. Namely, applying Theorem 3.3 to (5.1), we get a criterion for the non-existence of $\text{BH}_\gamma(v, m)$ and m -ary NPS:

Corollary 5.9. *Let $v, m \in \mathbb{Z}^+$ and $\gamma \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$ such that $D = ((\gamma + 1)v - \gamma)(v - \gamma)^{v-1}$ and $D = tq^{2e+1}$ where $e > 0$ be rational integer, $q, t \in \mathbb{Z}[\zeta_m]$ and q is squarefree. Suppose that (i) to (iv) below are satisfied.*

- (i) Every prime ideal $\mathfrak{t} \triangleleft \mathbb{Z}[\zeta_m]$ with $\mathfrak{t} \mid (t)$ is principal.
- (ii) $(q) = \mathfrak{q}_1 \mathfrak{q}_2$ where \mathfrak{q}_1 and \mathfrak{q}_2 are non-principal prime ideals of $\mathbb{Z}[\zeta_m]$.
- (iii) $\gcd(2e + 1 - 2k, h_m) = 1$ for $0 \leq k \leq e - 1$.
- (iv) $\gcd(N(q), N(t)) = 1$.

Then the following hold:

- (i) there exists no $BH_\gamma(v, m)$.
- (ii) there exists no v -periodic m -ary NPS of type γ .

Applying Theorem 3.3 to (5.2), we get a criterion for the non-existence of $C_\gamma(v, m)$ and almost m -ary NPS:

Corollary 5.10. *Let $v, m \in \mathbb{Z}^+$, $\gamma \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$ such that $D = (\gamma + 1)(v - 1)(v - 1 - \gamma)^{v-1}$ and $D = tq^{2e+1}$ where $e > 0$ be rational integer, $q, t \in \mathbb{Z}[\zeta_m]$ and q is squarefree. If the conditions (i) - (iv) given in Corollary 5.9 are satisfied, then*

- There exists no $C_\gamma(v, m)$,
- There exists no v -periodic an almost m -ary NPS of type γ .

Next, we apply Theorem 4.1 to (5.1), we get a criterion for the non-existence of $BH_\gamma(v, m)$ and almost m -ary NPS:

Corollary 5.11. *Let $v, m \in \mathbb{Z}^+$ and $\gamma \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$ such that $D = ((\gamma + 1)v - \gamma)(v - \gamma)^{v-1}$ and $p \triangleleft \mathbb{Z}[\zeta_m]$ be a prime ideal with $p \mid D$ and $\gcd(N(D)/N(p), N(p)) = 1$. Then,*

- There exists no $BH_\gamma(v, m)$,
- There exists no v -periodic an m -ary NPS of type γ .

Applying Theorem 3.3 to (5.2), we get a necessary criterion for the existence of $C_\gamma(v, m)$ and almost m -ary NPS.

Corollary 5.12. *Let $v \in \mathbb{Z}^+$, $D = (\gamma + 1)(v - 1)(v - 1 - \gamma)^{v-1}$ where $v \in \mathbb{Z}^+$, $\gamma \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$, $p \triangleleft \mathbb{Z}[\zeta_m]$ be a prime ideal with $p \mid D$ and $\gcd(N(D)/N(p), N(p)) = 1$. Then;*

- There exists no $C_\gamma(v, m)$,

- *There exists no v -periodic an almost m -ary NPS of type γ .*

We give some examples illustrating the results above.

Example 5.13. *Consider $\text{BH}_\gamma(5, 23)$, $\gamma = -1 - \zeta_{23}$, $v = 5$ and $m = 23$.*

$$\alpha\bar{\alpha} = (1 - 4\zeta_{23})(6 + \zeta_{23})^4$$

Every prime ideal dividing $(6 + \zeta_{23})^4$ is principal. $(1 - 4\zeta_{23})$ has the non-principal ideal decomposition over $\mathbb{Z}[\zeta_{23}]$. Hence, $\text{BH}_\gamma(25, 23)$ does not exist by Corollary 5.9. Furthermore, we conclude that a 23-ary NPS of period 5 and $\gamma = -1 - \zeta_{23}$ does not exist.

Example 5.14. *Consider $\text{BH}_\gamma(67, 23)$, $\gamma = -1 - \zeta_{23}$, $v = 67$ and $m = 23$.*

$$\alpha\bar{\alpha} = (1 - 66\zeta_{23})(68 + \zeta_{23})^{66}$$

Every prime ideal dividing $(68 + \zeta_{23})^{66}$ is principal. $(1 - 66\zeta_{23})$ has the non-principal ideal decomposition over $\mathbb{Z}[\zeta_{23}]$. Hence, $\text{BH}_\gamma(67, 23)$ does not exist by Corollary 5.9. Furthermore, we conclude that a 23-ary NPS of period 67 and $\gamma = -1 - \zeta_{23}$ does not exist.

We tabulate existence results of NPS of length $n \leq 20$ in Table 5.1. We obtained the examples in Table 5.1 by an exhaustive search on all sequences of length n . These examples are obtained by using programming language MAGMA [1].

Table 5.1: Samples of perfect sequences with non-integer correlations

v	m	γ	$ \gamma $	a
3	5	$\zeta_5^3 + \zeta_5^2 + 1$	0.61	$1, 1, \zeta_5^2$
3	7	$\zeta_7^5 + \zeta_7^2 + 1$	0.55	$\zeta_7^2, \zeta_7^2, 1$
4	5	$\zeta_5^3 + \zeta_5^2 + 2$	0, 38	$1, 1, 1, \zeta_5^2$
4	7	$\zeta_7^4 + \zeta_7^3 + 2$	0, 19	$\zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^5$
5	5	$\zeta_5^3 + \zeta_5^2 + 3$	1, 38	$1, 1, 1, 1, \zeta_5^2$
5	7	$-\zeta_7^5 - \zeta_7^2$	0, 44	$\zeta_7^2, \zeta_7^2, \zeta_7^3, \zeta_7^6, \zeta_7^3$
25	5	$\zeta_5^3 + \zeta_5^2 + 23$	21, 38	$1, \dots, 1, \zeta_5^2$
125	5	$\zeta_5^3 + \zeta_5^2 + 123$	121, 38	$1, \dots, 1, \zeta_5^2$
6	5	$\zeta_5^3 + \zeta_5^2 + 4$	2, 38	$1, 1, 1, 1, 1, \zeta_5^2$
6	6	-1	1	$\zeta_6^4, 1, \zeta_6^4, \zeta_6^2, \zeta_6, \zeta_6^2$
6	7	$\zeta_7^4 + \zeta_7^3 + 4$	2, 19	$\zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^5$
7	5	$2\zeta_5^3 + 2\zeta_5^2 + 3$	0, 23	$1, 1, 1, \zeta_5^2, 1, \zeta_5^2, \zeta_5^2$
7	7	$2\zeta_7^4 + 2\zeta_7^3 + 3$	0, 60	$\zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^3, \zeta_7^2, \zeta_7^3, \zeta_7^3$
8	5	$\zeta_5^3 + \zeta_5^2 + 1$	0, 61	$1, 1, 1, \zeta_5^2, \zeta_5^3, 1, \zeta_5^3, \zeta_5$
8	7	$\zeta_7^4 + \zeta_7^3 + 6$	4, 19	$\zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^5$
8	8	0	0	$\zeta_8^5, \zeta_8^5, 1, \zeta_8^5, \zeta_8^7, \zeta_8^7, 1, \zeta_8^7$
9	7	$\zeta_7^4 + \zeta_7^3 + 7$	5, 19	$\zeta_7^6, \zeta_7^5 \dots$
9	9	$\zeta_9^5 + \zeta_9^4 + 7$	5, 12	$\zeta_9^6, \zeta_9^6, \zeta_9^6, \zeta_9^6, \zeta_9^6, \zeta_9^6, \zeta_9^6, \zeta_9^6, \zeta_9^2$
10	5	$\zeta_5^3 + \zeta_5^2 + 8$	6, 38	$\zeta_5^2, \zeta_5^2, \zeta_5^2, \zeta_5^2, \zeta_5^2, \zeta_5^2, \zeta_5^2, \zeta_5^2, \zeta_5^2, 1$
10	7	$\zeta_7^4 + \zeta_7^3 + 8$	6, 19	$\zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^5$
10	10	$\zeta_{10}^3 - \zeta_{10}^2 + 7$	6, 38	$\zeta_{10}^8, \zeta_{10}^8, \zeta_{10}^8, \zeta_{10}^8, \zeta_{10}^8, \zeta_{10}^8, \zeta_{10}^8, \zeta_{10}^8, \zeta_{10}^8, \zeta_{10}^2$
11	11	$3\zeta_{11}^6 + 3\zeta_{11}^5 + 5$	0.75	$1, 1, 1, \zeta_{11}^6, 1, 1, \zeta_{11}^6, 1, \zeta_{11}^6, \zeta_{11}^6, \zeta_{11}^6$
11	11	0	0	$1, 1, \zeta_{11}^6, \zeta_{11}^7, \zeta_{11}^3, \zeta_{11}^5, \zeta_{11}^2, \zeta_{11}^5, \zeta_{11}^3, \zeta_{11}^7, \zeta_{11}^6$
11	11	$\zeta_{11}^6 + \zeta_{11}^5 + 9$	7, 08	$1, 1, 1, 1, 1, 1, 1, 1, 1, 1, \zeta_{11}^6$

6. Cryptographic Applications

There is a close relationship between the family of Hadamard matrices and cryptography. For instance there is a class of functions called bent function used in block cipher cryptosystems, and they can be constructed via Butson-Hadamard matrices. Functions used in block cipher design have to satisfy some properties in order to resist attacks. Two of them are balancedness and nonlinearity. A function is said to be balanced if each value in its image set is attained by the same probability. And, a function's nonlinearity is measured by its minimum distance to all linear functions.

The family of bent functions is a branch of the Boolean functions. Their Walsh spectrum coefficients allow us to examine their non-linearity. Hence, we start with the definition of a Boolean function.

Definition 6.1. A function $f : (\mathbb{Z}_2)^n \rightarrow \mathbb{Z}_2$ is called a Boolean function of n variables. Let B_n be the set of all Boolean functions of n variables. A function $f \in B_n$ is represented with a vector of length 2^n having values $f(x)$ for all $x \in (\mathbb{Z}_2)^n$ where x values are in lexicographic order.

Definition 6.2. For any $f \in B_n$, define $(-1)^f$ to be the function $F : (\mathbb{Z}_2)^n \rightarrow \{-1, 1\}$ such that $F(x) = (-1)^{f(x)}$ for all $x \in (\mathbb{Z}_2)^n$.

For cryptographic systems, the method of confusion and diffusion is used as a fundamental technique to achieve security [13]. Confusion is satisfied by including a highly nonlinear function into the cryptosystem. These functions simultaneously have maximum distance to affine functions and maximum distance to linear structures, as well. So they are called as strong functions, i.e. not weak. A function is considered weak whenever it can be turned into a cryptographically weak function by means of simple (linear or affine) transformations as a minimum correlation to affine functions [11, p.549].

The nonlinearity of a function can be calculated by using the Walsh transform, one of the important tools in cryptography. The definition of Walsh transform and its properties are given below. After that, a method for computing the nonlinearity will be demonstrated.

The inner product of two vectors $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n) \in (\mathbb{Z}_2)^n$ is $x.y = \sum_{i=1}^n x_i y_i \pmod{2}$.

If F be any real-valued function defined on $(\mathbb{Z}_2)^n$, then *the Walsh transform* of F is the function $\hat{F} : (\mathbb{Z}_2)^n \rightarrow \mathbb{R}$ defined by the following formula. $\forall x \in (\mathbb{Z}_2)^n$, $\hat{F}(x) = \sum_{y \in (\mathbb{Z}_2)^n} (-1)^{x \cdot y} F(y)$.

Let A_n be the set of all affine functions in B_n . Nonlinearity of a Boolean function is the minimum distance of a Boolean function f to the set of all linear functions

$$nl(f) = \min\{d(f, A_n)\},$$

Below we consider $F(x) = (-1)^{f(x)}$.

$$\begin{aligned} \hat{F}(x) &= \sum_{y \in (\mathbb{Z}_2)^n} (-1)^{x \cdot y} (-1)^{f(x)} \\ &= \sum_{f(x)=x \cdot y} 1 - \sum_{f(x) \neq x \cdot y} 1, \\ &= 2^n - 2d(f, x \cdot y). \end{aligned}$$

Then, $d(f, x \cdot y) = 2^{n-1} - \frac{1}{2}\hat{F}(x)$ is the distance between $f(x)$ and $l_y(x) = x \cdot y$.

Theorem 6.3. *The nonlinearity of a Boolean function f on \mathbb{Z}_2^n can be expressed by $nl(f) = 2^{n-1} - \frac{1}{2}\max\{|\hat{F}(x)| : x \in \mathbb{Z}_2^n\}$.*

Theorem 6.4. *For any function f on \mathbb{Z}_2^n , the nonlinearity of f satisfies $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.*

A function f on \mathbb{Z}_2^n attains the upper bound of nonlinearity $2^{n-1} - 2^{\frac{n}{2}-1}$ is called a *bent function*. It is clear that if $\hat{F}(x) = \pm 2^{n/2}$ for all $x \in \mathbb{Z}_2^n$, a function $f \in B_n$ is a bent function. Maximal nonlinearity is hence attained by bent functions, with only even n . For instance, let $P(x)$ be a function from \mathbb{Z}_2 to \mathbb{Z}_2 . $P(x)$ is bent if all Walsh coefficients of $(-1)^{P(x)}$ are ± 1 . This definition of a bent function over \mathbb{Z}_2 can be directly extended to functions on \mathbb{Z}_q . First the Walsh transform is extended to the functions on \mathbb{Z}_q .

Definition 6.5. [10, p.339] *Suppose $F : (\mathbb{Z}_q)^n \rightarrow \mathbb{C}$ and let $\zeta = e^{2i\pi/q}$. The Walsh transform of F is the function $\hat{F} : (\mathbb{Z}_q)^n \rightarrow \mathbb{C}$ defined for all $\mathbf{x} \in (\mathbb{Z}_q)^n$ by the formula:*

$$\hat{F}(x) = \sum_{y \in (\mathbb{Z}_q)^n} \zeta^{x \cdot y} F(y).$$

Then a generalized bent function is defined similarly.

Definition 6.6. *Suppose $f : (\mathbb{Z}_q)^n \rightarrow \mathbb{Z}_q$ and define $F : (\mathbb{Z}_q)^n \rightarrow \mathbb{C}$ by the rule $F(\mathbf{x}) = \zeta^{f(\mathbf{x})}$ for all $\mathbf{x} \in (\mathbb{Z}_q)^n$, where $\zeta = e^{2i\pi/q}$. If $|\hat{F}(\mathbf{x})| = q^{n/2} \forall \mathbf{x} \in (\mathbb{Z}_q)^n$, then f is a generalized bent function.*

The connection between Hadamard matrices and generalized bent functions is given in Theorem 6.7.

Theorem 6.7. [10] *Let the matrix $H_f = (h_{x,y})$, where $h_{x,y} = F(\mathbf{x} - \mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in (\mathbb{Z}_q)^n$. Then f is a generalized bent function if and only if H_f is a Butson-Hadamard matrix.*

We give a well known result on the existence of a generalized bent function.

Theorem 6.8. [10, p.96] *Assume that n is even or $q \equiv 2 \pmod{4}$. Then there exists a generalized bent function $f : (\mathbb{Z}_q)^n \rightarrow \mathbb{Z}_q$.*

Therefore, we see that there is a one to one correspondence between generalized bent functions and Butson-Hadamard matrices. We give an example below.

Example 6.9. $f: \mathbb{Z}_3^2 \rightarrow \mathbb{Z}_3$ and $f(x_1, x_2) = x_1x_2$. The matrix H corresponding to the bent function f is given below. The entries of the Hadamard matrix forms a power of 3-th of unity ζ .

$$\begin{aligned}
 H &= \begin{bmatrix}
 \zeta^{f(0,0)} & \zeta^{f(0,2)} & \zeta^{f(0,1)} & \zeta^{f(2,0)} & \zeta^{f(2,2)} & \zeta^{f(2,1)} & \zeta^{f(1,0)} & \zeta^{f(1,2)} & \zeta^{f(1,1)} \\
 \zeta^{f(0,1)} & \zeta^{f(0,0)} & \zeta^{f(0,2)} & \zeta^{f(2,1)} & \zeta^{f(2,0)} & \zeta^{f(2,2)} & \zeta^{f(1,1)} & \zeta^{f(1,0)} & \zeta^{f(1,2)} \\
 \zeta^{f(0,2)} & \zeta^{f(0,1)} & \zeta^{f(0,0)} & \zeta^{f(2,2)} & \zeta^{f(2,1)} & \zeta^{f(2,0)} & \zeta^{f(1,2)} & \zeta^{f(1,1)} & \zeta^{f(1,0)} \\
 \zeta^{f(1,0)} & \zeta^{f(1,2)} & \zeta^{f(1,1)} & \zeta^{f(0,0)} & \zeta^{f(0,2)} & \zeta^{f(0,1)} & \zeta^{f(2,0)} & \zeta^{f(2,2)} & \zeta^{f(2,1)} \\
 \zeta^{f(1,1)} & \zeta^{f(1,0)} & \zeta^{f(1,2)} & \zeta^{f(0,1)} & \zeta^{f(0,0)} & \zeta^{f(0,2)} & \zeta^{f(2,1)} & \zeta^{f(2,0)} & \zeta^{f(2,2)} \\
 \zeta^{f(1,2)} & \zeta^{f(1,1)} & \zeta^{f(1,0)} & \zeta^{f(0,2)} & \zeta^{f(0,1)} & \zeta^{f(0,0)} & \zeta^{f(2,2)} & \zeta^{f(2,1)} & \zeta^{f(2,0)} \\
 \zeta^{f(2,0)} & \zeta^{f(2,2)} & \zeta^{f(2,1)} & \zeta^{f(1,0)} & \zeta^{f(1,2)} & \zeta^{f(1,1)} & \zeta^{f(0,0)} & \zeta^{f(0,2)} & \zeta^{f(0,1)} \\
 \zeta^{f(2,1)} & \zeta^{f(2,0)} & \zeta^{f(2,2)} & \zeta^{f(1,0)} & \zeta^{f(1,1)} & \zeta^{f(1,2)} & \zeta^{f(0,1)} & \zeta^{f(0,0)} & \zeta^{f(0,2)} \\
 \zeta^{f(2,2)} & \zeta^{f(2,1)} & \zeta^{f(2,0)} & \zeta^{f(1,2)} & \zeta^{f(1,1)} & \zeta^{f(1,0)} & \zeta^{f(0,2)} & \zeta^{f(0,1)} & \zeta^{f(0,0)}
 \end{bmatrix} \\
 &= \begin{bmatrix}
 \zeta^0 & \zeta^2 & \zeta^1 & \zeta^6 & \zeta^8 & \zeta^7 & \zeta^3 & \zeta^5 & \zeta^4 \\
 \zeta^1 & \zeta^0 & \zeta^2 & \zeta^7 & \zeta^6 & \zeta^8 & \zeta^4 & \zeta^3 & \zeta^5 \\
 \zeta^2 & \zeta^1 & \zeta^0 & \zeta^8 & \zeta^7 & \zeta^6 & \zeta^5 & \zeta^4 & \zeta^3 \\
 \zeta^3 & \zeta^5 & \zeta^4 & \zeta^0 & \zeta^2 & \zeta^1 & \zeta^6 & \zeta^8 & \zeta^7 \\
 \zeta^4 & \zeta^3 & \zeta^5 & \zeta^1 & \zeta^0 & \zeta^2 & \zeta^7 & \zeta^6 & \zeta^8 \\
 \zeta^5 & \zeta^4 & \zeta^3 & \zeta^2 & \zeta^1 & \zeta^0 & \zeta^8 & \zeta^7 & \zeta^6 \\
 \zeta^6 & \zeta^8 & \zeta^7 & \zeta^3 & \zeta^5 & \zeta^4 & \zeta^0 & \zeta^2 & \zeta^1 \\
 \zeta^7 & \zeta^6 & \zeta^8 & \zeta^4 & \zeta^3 & \zeta^5 & \zeta^1 & \zeta^0 & \zeta^2 \\
 \zeta^8 & \zeta^7 & \zeta^6 & \zeta^5 & \zeta^4 & \zeta^3 & \zeta^2 & \zeta^1 & \zeta^0
 \end{bmatrix}
 \end{aligned}$$

On the other hand, we can show an example for the other direction of Theorem 6.7. The matrix H is a Butson-Hadamard matrix.

$$H = \begin{bmatrix} \zeta^0 & \zeta^2 & \zeta^0 & \zeta^0 \\ \zeta^0 & \zeta^0 & \zeta^2 & \zeta^0 \\ \zeta^0 & \zeta^0 & \zeta^0 & \zeta^2 \\ \zeta^2 & \zeta^0 & \zeta^0 & \zeta^0 \end{bmatrix}$$

Then, $f : \mathbb{Z}_4 \rightarrow \mathbb{Z}_4$, as follows $f(0) = 0, f(1) = 0, f(2) = 0, f(3) = 2$.

We now investigate the functions corresponding to γ -Butson Hadamard matrices. We start with a circulant γ -Butson Hadamard matrix H and convert the first row of H into a truth table of a function f as in Theorem 6.7 and Example 6.9. Then the Walsh transform of f is calculated by Definition 6.5. We apply this conversion for the examples obtained in Table 5.1 and some of their trivial extensions. We tabulate our results in Table 6.1.

Table 6.1: Samples of γ -Butson Hadamard Matrices, corresponding Boolean functions f and their Walsh spectrum \hat{F}

m	v	γ	$ \gamma $	f	$ \hat{F} $
5	5	$\zeta_5^3 + \zeta_5^2 + 3$	1.38	(0, 2, 0, 0, 0)	(3.24, 1.90, 1.90, 1.90, 1.90)
5	25	$\zeta_5^3 + \zeta_5^2 + 23$	21.38	(0, 0, 0, 0, 0, 2, 0, ..., 0)	(23.19, 1.90, ..., 1.90)
5	125	$\zeta_5^3 + \zeta_5^2 + 123$	121.38	(0, ..., 0, 2, 0, ..., 0)	(123.19, 1.90, ..., 1.90)
6	6	-1	1	(6, 2, 0, 2, 6, 1)	(3.60, 1, 1, 4.35, 1, 1)
7	7	$2\zeta_7^4 + 2\zeta_7^3 + 3$	0.60	(2, 3, 3, 2, 3, 2, 2)	(6.32, 1.22, ..., 1.22)
8	8	0	0	(5, 7, 1, 5, 1, 7, 5, 5)	(2.82, ..., 2.82)
9	9	$\zeta_9^5 + \zeta_9^4 + 7$	5.12	(6, 2, 6, 6, 6, 6, 6, 6, 6)	(7.06, 1.97, ..., 1.97)
10	10	$\zeta_{10}^3 - \zeta_{10}^2 + 7$	6.38	(0, 6, 7, 3, 5, 2, 5, 3, 7, 6, 0)	(3.55, 3.23, 1.32, 2.55, 4.30 3.59, 4.29, 2.55, 1.32, 3.23)
11	11	$3\zeta_{11}^6 + 3\zeta_{11}^5 + 5$	0.75	(0, 6, 6, 6, 0, 6, 0, 0, 6, 0, 0)	(1.85, 3.42, ..., 3.42)
11	11	$\zeta_{11}^6 + \zeta_{11}^5 + 9$	7.08	(0, 6, 0, 0, 0, 0, 0, 0, 0, 0, 0)	(9.044, 1.979, ..., 1.979)
11	11	0	0	(0, 6, 7, 3, 5, 2, 5, 3, 7, 6, 0)	(3.31, ..., 3.31)

We note that nonlinearity is an important concept in cryptography. Looking at Table 6.1, it is seen that the smaller $|\gamma|$ values, the more flat Walsh spectrum and so the higher nonlin-

arity. Therefore one can obtain new families of nonlinear functions by searching matrices $BH_\gamma(v, m)$ for non integer $\gamma \in \mathbb{Z}[\zeta_m]$ having small absolute value.

7. CONCLUSION

In this thesis, we studied the γ -Butson-Hadamard matrices and their cryptographic applications. We studied the existence cases of γ -Butson-Hadamard matrices for $\gamma \in (\mathbb{Z}[\zeta_m] \cap \mathbb{R}) \setminus \mathbb{Z}$ by using the tools from algebraic number theory.

Firstly, we converted the existence condition of a γ -Butson-Hadamard matrix to an equation over a ring of integers of a cyclotomic number field. Then we obtained two novel results stating necessary conditions for the non-existence of this equation. Then the direct applications of these results to γ -Butson-Hadamard matrices were shown. We presented examples of non-existence cases in details and obtained existence examples by computer search.

It is known that a sequence obtained from the first row of a circulant γ -Butson-Hadamard matrix is used in many applications. They are known as nearly perfect sequences. Therefore the analogous consequences of our results applied to the concept of sequences were presented. Examples of non-existence cases for nearly perfect sequences were given in details. On the other hand, the exhaustive search on nearly perfect sequences was performed, and the existence results were tabulated. In deed, some examples of nearly perfect sequences with $|\gamma| < 1$ were obtained, which points to new research directions.

There is another family of matrices known as Conference matrices. The results obtained for γ -Butson-Hadamard matrices were similarly extended to Conference matrices. Two novel necessary conditions for the non-existence of a Conference matrix were presented.

Finally, the connection of γ -Butson-Hadamard matrices to cryptographic functions was drawn. Cryptographers look for nonlinear Boolean (multivariate) functions on residue rings. These functions are used in block ciphers to provide confidentiality of the message between two parties. In this thesis, it was shown that a γ -Butson-Hadamard matrix can be converted to a Boolean function whose nonlinearity is proportional with the value $|\gamma|$. And, the examples of nonlinear functions obtained from γ -Butson-Hadamard matrices were presented.

REFERENCES

- [1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [2] Bradley W Brock. Hermitian congruence and the existence and completion of generalized hadamard matrices. *Journal of Combinatorial Theory, Series A*, 49(2):233–261, 1988.
- [3] AT Butson. Generalized hadamard matrices. *Proceedings of the American Mathematical Society*, 13(6):894–898, 1962.
- [4] Henri Cohen. *Number theory: Volume I: Tools and diophantine equations*, volume 239. Springer Science & Business Media, 2008.
- [5] Charles J Colbourn and Jeffrey H Dinitz. *Handbook of combinatorial designs*. CRC press, 2006.
- [6] Albrecht Fröhlich, Martin J Taylor, and Martin J Taylor. *Algebraic number theory*, volume 27. Cambridge University Press, 1993.
- [7] Solomon W Golomb and Guang Gong. *Signal design for good correlation: for wireless communication, cryptography, and radar*. Cambridge University Press, 2005.
- [8] Kathy J Horadam. *Hadamard matrices and their applications*. Princeton university press, 2007.
- [9] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84. Springer Science & Business Media, 2013.
- [10] P Vijay Kumar, Robert A Scholtz, and Lloyd R Welch. Generalized bent functions and their properties. *Journal of Combinatorial Theory, Series A*, 40(1):90–107, 1985.
- [11] Willi Meier and Othmar Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology—EUROCRYPT’89*, pages 549–562. Springer, 1990.
- [12] James S Milne. *Algebraic number theory*. JS Milne, 2008.

- [13] Claude E Shannon. A mathematical theory of cryptography. *Memorandum MM*, 45:110–02, 1945.
- [14] Ian Stewart and David Tall. *Algebraic number theory and Fermat's last theorem*. CRC Press, 2015.
- [15] Lawrence C Washington. *Introduction to cyclotomic fields*, volume 83. Springer Science & Business Media, 1997.
- [16] Arne Winterhof, Oğuz Yayla, and Volker Ziegler. Non-existence of some nearly perfect sequences, near butson-hadamard matrices, and near conference matrices. *arXiv preprint arXiv:1407.6548*, 2014.

Appendix: MAGMA CODES

We present the MAGMA source code for the main Theorem 3.3 in Chapter 3.

```
IsSelfConj := function (p, w)
    w_prime := w;
    while IsDivisibleBy(w_prime, p) do
        w_prime := ExactQuotient(w_prime, p);
    end while;
    for j in [1..w_prime] do
        if (p^j mod w_prime) eq w_prime-1 then
            return true;
        end if;
    end for;
    return false;
end function;
```

```
exponent := function (n, q)
    s := 0;
    while IsDivisibleBy(n, q) and (not (n eq 0)) do
        s += 1;
        n := ExactQuotient(n, q);
    end while;
    return s;
end function;
```

```
IsValidExponent := function (e, h)
    for k in [0..Floor(e/2)] do
        if GCD(e-2*k, h) ne 1 then
            return false;
        end if;
    end for;
    return true;
end function;
```

```

set_mh := [[23,3],[29,8],[31,9],[37,37],[39,2],[41,121],[43,211],
[46,3],[47,695],[49,43],[51,5],[52,3],[56,2],[62,9]];
set_mh := {[23,3]};
q_set := {2,3,13,29,31,41,71,73,
127,131,151,163,179,193,197};
for mh in set_mh do
    m:=mh[1];
    h:=mh[2];

    K:=CyclotomicField(m);
    O:=RingOfIntegers(K);

    unity:=K.1;
    for gamma in [-1-unity-unity^22] do
        Im(gamma);
        set_v := {};
        set_conj := {};
        for v in [46..46] do
            v;

            if not (IsDivisibleBy(v+2,m)) then
                end if;

            D:=((gamma+1)*v-gamma)*
            (v-gamma)^(v-1); // hadamard
            //D:=(gamma+1)*(v-1)*
            (v-1-gamma)^(v-1); // Determinant
                                of Conference Matrix
            if D eq 0 then
                continue v;
            end if;
        end if;
    end if;
end if;

```

```

D_factors := Factorization(D*O);

set_non := [];  \ \ set of non-principal
set_prin := {}; \ \ set of principal
set_ram := {};  \ \ set of ramified

for Q in D_factors do
    if IsPrincipal(Q[1]) then
        Include(~set_prin, Q);
    else
        Include(~set_non, Q);
    end if;
end for;

if (#set_non eq 2) then
    Include(~set_v, v);
    set_v;

    for Q in set_non do
        printf "v: %o Q: %o";
    end for;

    set_non[1][1]*set_non[2][1];

    end if;
end for;
printf "m: %o gamma: %o set_v: ";
end for;
end for;

```

We present source code of the Walsh spectrum for value of TT , q , n in MAGMA.

```

Abs := function(x)
    return Sqrt(Re(x*ComplexConjugate(x)));
end function;

```

```

end function;

WalshSpectrum:=function(TT,q,n)
    K:=GF(q);          \ General Field
    carK:=CartesianPower(K,n);
    w:=RootOfUnity(q);

    S := [];

    for i in carK do
        s:=Tuplist(i);
        Append(~S,s);
    end for;

    F:=[];
    t:=K!0;

    for x in [1..q^n] do
        F[x]:=w-w;
        for y in [1..q^n] do
            for l in [1..n] do
                s:=S[x][l];
                m:=S[y][l];
                t+=K!(s*m);
            end for;
            F[x]+=w^(Integers()!(t + TT[y]));
            t:=0;
        end for;
    end for;
    return F;
end function;

```

```
q:=5;  \ The values of q, n, TT is selected.  
n:=4;  
TT:=[0,2,0,0];  
  
for x in WalshSpectrum(TT,q,n) do  
    x,Abs(x);  
end for;
```

CURRICULUM VITAE

Credentials

Name, Surname : Sibel Kurt
Place of Birth : DENİZLİ, 1991
Marital Status : single
E-mail : sibelkurt3211@gmail.com
Address : Hacettepe Üniversitesi, Beytepe Kampüsü, Beytepe,
Çankaya, Ankara, TURKEY

Education

High School : 2005-2009 Lütü Ege Anatolian Teacher High School
BSc. : 2009-2015 Hacettepe University, Faculty of Education, Department of
Mathematics Teaching
MSc. : 2015-2017 Hacettepe University, Institute of Graduate Studies in Science,
Department of Mathematics

Foreign Languages

English

Work Experience

Areas of Experience

Publications

Projects and Budgets

2016-2017 TUBITAK-1002 - Quick Support Program (Project No: 116R001)

Oral and Poster Presentations

- 7.1. Koç University Presentation "Near Butson-Hadamard Matrices with Small Off-diagonal Entries" presentation speaker
- 7.2. Aksaray University 19. Academic Computing Conference "Presentation of New Perfect Series for CDMA Systems" presentation speaker
- 7.3. Hacettepe University, Ankara Mathematics Days 2017, "Small Autocorrelation of Almost Perfect Sequences" presentation speaker



HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SCIENCE AND ENGINEERING
THESIS/DISSERTATION ORIGINALITY REPORT

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SCIENCE AND ENGINEERING
TO THE DEPARTMENT OF MATHEMATICS

Date: 02/08/2017

Thesis Title : γ -BUTSON-HADAMARD MATRICES AND THEIR CRYPTOGRAPHIC APPLICATIONS

According to the originality report obtained by my thesis advisor by using the *Turnitin* plagiarism detection software and by applying the filtering options stated below on 31/07/2017 for the total of 39 pages including the a) Title Page, b) Introduction, c) Main Chapters, d) Conclusion sections of my thesis entitled as above, the similarity index of my thesis is 10 %.

Filtering options applied:

1. Bibliography/Works Cited excluded
2. Quotes ~~excluded~~ / included
3. Match size up to 5 words excluded

I declare that I have carefully read **Hacettepe University Graduate School of Science and Engineering Guidelines for Obtaining and Using Thesis Originality Reports**; that according to the maximum similarity index values specified in the Guidelines, my thesis does not include any form of plagiarism; that in any future detection of possible infringement of the regulations I accept all legal responsibility; and that all the information I have provided is correct to the best of my knowledge.

I respectfully submit this for approval.

Date and Signature

Name Surname: Sibel Kurt

Student No: N14327289

Department: Mathematics

Program: Mathematics

Status: Masters Ph.D. Integrated Ph.D.

02.08-2017

ADVISOR APPROVAL

APPROVED.

Assist. Prof. Dr. Oğuz YAYLA

(Title, Name Surname, Signature)