2007
KARABÜK
ÜNİVERSİTESİ

CORRELATION PROPERTIES OF SEQUENCES OVER FINITE FIELDS

2024
MASTER THESIS
MATHEMATICS DEPARTMENT

Rashid Hussein QASM

Thesis Advisor
Assist .Prof. Dr. Eda TEKİN

CORRELATION PROPERTIES OF SEQUENCE OVER FINITE FIELDS

Rashid Hussein QASM

Thesis Advisor
Assist. Prof. Dr. Eda TEKİN

T.C.
Karabuk University
Institute of Graduate Programs
Department of Mathematics
Prepared as
Master Thesis

KARABUK
January 2024

I certify that in my opinion the thesis submitted by Rashid Hussein QASM titled "CORRELATION PROPERTIES OF SEQUENCE OVER FINITE FIELDS" is fully adequate in scope and in quality as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Eda TEKİN ....
Thesis Advisor, Department of Mathematics

This thesis is accepted by the examining committee with a unanimous vote in the Department of Mathematics as a Master of Science thesis. January 12, 2024

Examining Committee Members (Institutions)		Signature
Chairman	: Assist. Prof. Dr. Eda TEKİN (KBU)	....
Member	: Assist. Prof. Dr. Tülay YILDIRIM TURAN (KBU)	....
Member	: Assist. Prof. Dr. Rabia Nagehan ÜREGEN (EBYU)	....

The degree of Master of Science by the thesis submitted is approved by the Administrative Board of the Institute of Graduate Programs, Karabuk University.

Assoc. Prof. Dr. Zeynep ÖZCAN ....
Director of the Institute of Graduate Programs

“I declare that all the information within this thesis has been gathered and presented in accordance with academic regulations and ethical principles and I have according to the requirements of these regulations and principles cited all those which do not originate in this work as well.”

Rashid Hussein QASM

ABSTRACT

M. Sc. Thesis

CORRELATION PROPERTIES OF SEQUENCES OVER FINITE FIELDS

Rashid Hussein QASM

Karabuk University
Institute of Graduate Programs
The Department of Mathematics

Thesis Advisor:
Assist. Prof. Dr. Eda TEKİN

January 2024, 62 Pages

This thesis investigates the correlation properties of sequences over finite fields and explores their applications in communication systems, cryptography, and signal processing. The study focuses on algorithms for generating sequences with favorable correlation properties, giving special attention to the distinctive features of Zadoff-Chu sequences.

The initial sections provide a thorough overview of finite fields and their relevance to sequence generation. The report introduces key algorithms for constructing sequences, emphasizing their impact on correlation properties. The Zadoff-Chu sequence, a well-established class known for its unique characteristics, is examined in detail for its suitability in communication and radar applications. An analysis of correlation functions is presented, exploring correlation properties of sequences over finite fields.

This research contributes to a broader understanding of sequence design over finite fields, offering insights into correlation aspects for applications.

**Key Words : ** Finite Fields, Sequences , Zaddof-Chu Sequence , 5G Prach

**Science Code : ** 20401

ÖZET

Yüksek Lisans Tezi

SONLU CİSİMLER ÜZERİNDE DİZİLER VE KORELASYON ÖZELLİKLERİ

Rashid Hussein QASM

Karabük Üniversitesi
Lisansüstü Eğitim Enstitüsü
Matematik Anabilim Dalı

Tez Danışmanı:
Dr. Öğr. Üyesi Eda TEKİN

Ocak 2024, 62 Sayfa

Bu tezde sonlu cisimler üzerinde tanımlı dizilerin korelasyon özelliklerini ve bunların iletişim sistemleri, kriptografi ve sinyal işlemedeki uygulamalarını inceledik. Ayrıca, Zadoff-Chu dizilerinin ayırt edici özelliklerine ve uygun korelasyon özelliklerine sahip dizi ailelerine odaklandık.

İlk bölümler sonlu cisimlere ve dizilere kapsamlı bir genel bakış sağlamaktadır. Bu tezde dizilerin oluşturulmasına yönelik temel algoritmaları tanıtıp ve bunların korelasyon özellikleri üzerindeki etkisini vurgulamaktayız. Kendine has özellikleriyle bilinen köklü bir sınıf olan Zadoff-Chu dizisinin iletişim ve radar uygulamalarına uygunluğunu inceledik. Dizi tasarımı ve uygulamasının pratik yönleri, belirli uygulama gereksinimlerine göre korelasyon özelliklerinin optimize edilmesine odaklanılarak tartışılmaktadır.

Bu tezde amaç, sonlu cisimler üzerinde dizi tasarımının daha geniş bir şekilde anlaşılmasına katkıda bulunmaktır.

Anahtar Kelimeler **:** Sonlu Cisimler, Diziler, Zaddof-Chu Dizisi , 5G Prach

Bilim Kodu **:** 20401

ACKNOWLEDGMENT

First of all, I would like to give thanks to my advisor, Assist. Prof. Dr. Eda TEKIN, for his great interest and assistance in preparation of this thesis.

CONTENTS

Page

Page

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

LIST OF ABBREVIATIONS

$\mathbb{F}_k$	: Finite field with k elements
p	: Prime number
k	: Prime power
Tr	: Trace function
Gcd	: Greatest common divisor
R	: Rank
$\delta_{i,j}(\tau)$	: Cross-correlation function
δ_{max}	: Maximum correlation magnitude
$B(y,z)$	: Symplectic form
$\mathrm{s}_{\mathrm{q}}[n]$	: Sequence

PART 1

INTRODUCTION

In the dynamic landscape of signal processing and communication systems, the intricate properties of sequences over finite fields stand as the cornerstone shaping the reliability, efficiency, and security of a myriad of applications. This comprehensive report delves into the correlation properties of sequences, illuminating their theoretical underpinnings and real-world applications. With a specific focus on the ever-evolving domain of 5G technology and the distinctive Zadoff-Chu sequences, we embark on a journey to unravel the intricate interplay of mathematics and practical utility.

1.1. BACKGROUND

Sequences, as ordered sets of elements from finite fields, have long been the subject of profound mathematical exploration. The inherent characteristics of these sequences, often expressed through algebraic structures, contribute to their multifaceted utility in communication systems, cryptography, and error detection. The nuanced understanding of correlation properties within sequences becomes imperative as we navigate the complexities of modern communication systems.

As we lay the groundwork for this exploration, it is essential to recognize that sequences are not mere mathematical abstractions but rather indispensable tools in the arsenal of engineers and researchers. Their influence extends across various domains, from wireless communication to secure data transmission, making the study of their correlation properties a fundamental pursuit.

1.2.IMPORTANCE OF CORRELATION PROPERTIES

The paramount importance of correlation properties in sequences lies in their ability to discern signals amidst noise and interference. The low cross-correlation and high auto-correlation exhibited by sequences form the bedrock for reliable signal detection, distinguishing one signal from another in scenarios where multiple signals coexist [3]. This characteristic resilience becomes particularly critical in the realm of wireless communication, where the airwaves are crowded with signals and prone to interference.

The significance of sequences with robust correlation properties is further underscored by their role in enabling efficient and error-resistant communication. [3] In essence, these sequences act as the silent architects behind the scenes, ensuring the seamless flow of data and the integrity of transmitted information.

1.3. APPLICATION OF SEQUENCES WITH GOOD CORRELATION PROPERTIES COMMUNICATION SYSTEMS

Sequences serve as the linchpin in communication systems, where the ability to accommodate multiple users, devices, and signals concurrently is of paramount importance. The low cross-correlation between sequences allows for the simultaneous transmission of signals without mutual interference, a characteristic crucial in the design of modern multi-user communication protocols.

1.4. ERROR DETECTION AND CORRECTION:

In the realm of error detection and correction, sequences with good correlation properties emerge as unsung heroes. By leveraging these sequences, communication systems can not only identify errors but also correct them, ensuring the accuracy and reliability of the transmitted data. The resilience to noise and distortion offered by such sequences makes them invaluable in scenarios where data integrity is non-negotiable.

1.5. SECURITY AND CRYPTOGRAPHY:

The role of sequences extends into the realms of security and cryptography, where their correlation properties contribute to the generation of secure keys and robust encryption processes [14]. The ability of sequences to resist correlation-based attacks is pivotal in fortifying communication channels and safeguarding sensitive information.

1.6. SEQUENCES IN 5G TECHNOLOGY

As we stand at the precipice of the fifth generation of wireless communication technology, the landscape is defined by unprecedented challenges and opportunities [12]. The requirements for high data rates, low latency, and massive device connectivity necessitate sequences that not only meet but exceed the stringent demands of 5G networks.

Sequences, and in particular, Zadoff-Chu sequences, emerge as protagonists in the 5G narrative. Their unique properties make them prime candidates for addressing the challenges posed by the dynamic and complex nature of modern communication channels. The intricacies of 5G technology, with its emphasis on enhanced performance and connectivity, amplify the significance of sequences with superior correlation properties.

1.7. ZADOFF-CHU SEQUENCES

Within the expansive realm of sequences, the Zadoff-Chu family stands out as a distinguished class, bearing the names of Emil Zadoff and Robert Chu, whose contributions have left an indelible mark on the field. [14] Zadoff-Chu sequences are characterized by their constant amplitude and periodic properties, making them particularly well-suited for applications in communication systems.

The inherent qualities of Zadoff-Chu sequences, including low cross-correlation and favorable periodicity, position them as ideal candidates for the intricate requirements of 5G communication [13]. Their application in the design of the Physical Random-

Access Channel (PRACH) exemplifies their relevance in optimizing the access procedure, contributing to the overall efficiency of 5G communication systems.

1.8. OBJECTIVES OF THE REPORT

As we navigate through the chapters that follow, our primary objective is to provide a comprehensive understanding of the correlation properties of sequences over finite fields. By scrutinizing the theoretical foundations and practical implications, we aim to bridge the gap between abstract mathematical concepts and their tangible impact on modern communication technologies. The subsequent sections will delve into finite fields, the broader context of sequences, and the unique characteristics of the Zadoff-Chu family, culminating in a detailed analysis of their application in the 5G PRACH.

PART 2

FINITE FIELD

2.1. FINITE FIELD

A set having two binary operations (+) and (.) that satisfy the following conditions for any a, b, and c $\in$ F is called a field (F, +, .).

i. $a + b \in F$ and $a \cdot b \in F$, that is, F is closed under (+) and (·).

ii. $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. that is (+) and (·) are associative.

iii. $a + e = e + a = a$ and $a \cdot e' = e' \cdot a = a$, that is, For two binary operations (+) and (·), F has unique identity elements e and e' respectively.

iv. $a + a' = a' + a = e$ and $a \cdot a'' = a'' \cdot a = e'$. Note that for the operation (·) $a \neq e$, that is, Each element of F has a unique inverse in F for (+) and (·).

v. $a + b = b + a$ and $a \cdot b = b \cdot a$, that is, (+) and (·) are commutative.

vi. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$, that is, Distributive laws hold.

vii. $a \cdot b = e$ implies $a = e$ or $b = e$, that is F has no zero divisors.

A field containing finite number of elements is called **finite field**.

2.2. IRREDUCIBLE POLYNOMIALS

let F be a field. If we can factor f (x) as the product of m(x) and n(x) ϵ F[x], where the degree of m(x) and the degree of n(x) are both smaller than the degree of f (x), and f (x) = m(x)n(x), and d(m(x)) < d(f (x)), d(n(x) < d(f(x)), we may state that a non-constant polynomial f (x) is **reducible**. If a non-constant polynomial f (x) cannot be reduced, then it is said to be **irreducible**.

Examples:

1. **Polynomials of degree 2 over $\mathbb{F}_2$**

All polynomials of degree 2 over $\mathbb{F}_2$ are: t^2 , $t^2 + 1$, $t^2 + t$, $t^2 + t +1$.

Let g (t) = $t^2 + 1$ in $\mathbb{F}_2$ then g(0) = 1, g(1) = 1 + 1 = 0. t = 1 is satisfies the polynomial and t -1 is its factor. g(t) = $t^2 + 1 = (t + 1)^2$.

Now, let g(t) = $t^2 + t +1$, g(0) = 1, g(1) = 1. 0 and 1 are not roots of g (t). Thus $t^2 + t +1$ is an irreducible polynomial of degree 2 over $\mathbb{F}_2$.

2. **Polynomials of degree 3 over $\mathbb{F}_2$**

All polynomials of degree 3 over $\mathbb{F}_2$ are: t^3 , $t^3 + 1$, $t^3+ t$, $t^3 + t +1$, $t^3 + t^2$, $t^3 + t^2 + 1$, $t^3 + t^2 + t$, $t^3 + t^2 + t + 1$.

Let g(t) = $t^3 + t +1$. Then, g(0) = 1, g(1) = 1

Let g(t) = $t^3 + t^2 +1$. Then, g(0) = 1, g(1) = 1.

Irreducible polynomials of degree 3 over $\mathbb{F}_2$ are $t^3 + t +1$, $t^3 + t^2 + 1$.

3. **Polynomials of degree 4 over $\mathbb{F}_2$**

All polynomials of degree 4 over $\mathbb{F}_2$ are : t^4, $t^4 + 1$, $t^4 + t$, $t^4 + t + 1$, $t^4 + t^2$, $t^4 + t^2 +1$, $t^4 + t^2 + t$, $t^4 + t^2 + t +1$, $t^4 + t^3$, $t^4 + t^3 +1$, $t^4 + t^3 + t$, $t^4 + t^3 + t + 1$, $t^4 + t^3 + t^2$, $t^4 + t^3 + t^2 +1$, $t^4 + t^3 + t^2 +t$, $t^4 + t^3 + t^2 +t +1$.

g(t) = $t^4 + t + 1$, g(0) = 1, g(1) =1

g(t) = $t^4 + t^3 +1$, g(0) = 1, g(1) =1

g(t) = $t^4 + t^3 + t^2 + t +1$, g(0) = 1, g(1) = 1

All irreducible polynomials of degree 4 over $\mathbb{F}_2$ are $t^4 + t + 1$, $t^4 + t^3 +1$, $t^4 + t^3 + t^2 +t +1$

4. **Polynomials of degree 2 over $\mathbb{F}_3$**

All polynomials of degree 2 over $\mathbb{F}_3$ are : t^2 , $t^2 + 1$, $t^2 +2$, $t^2 + t$, $t^2 + t + 1$, $t^2 + t + 2$, $t^2 +2t$, $t^2 +2t +1$, $t^2 + 2t+2$, $2t^2$, $2t^2+1$, $2t^2+2$, $2t^2 +t$, $2t^2+t+1$, $2t^2 +t +2$, $2t^2+2t$, $2t^2 +2t +1$, $2t^2 +2t + 2$.

g(t) = $t^2 + 1$, g(0) = 1, g(1) = 2 , g(2) = 2

g(t) = $t^2 + t + 2$, g(1) = 1, g(2) = 2

g(t) = $t^2 + 2t+2$, g(1) = 2, g(2) = 1

Irreducible polynomials of degree 2 are $\mathbb{F}_3$ are

$t^2 + 1$, $t^2 +t + 2$, $t^2 +2t + 2$.

Construction of $\mathbb{F}_4$

$t^2 + t + 1 \epsilon \mathbb{F}_2[\ t\ ]$ is irreducible. $\mathbb{F}_2[\ t\ ]/(\ t^2 + t + 1)$ is a field , $\mathbb{F}_2[\ t\ ] = \{\ a + bt \mid a\ ,\ b\ \epsilon\ \mathbb{F}_2\ ,\ t^2 = t + 1\ \} = \mathbb{F}_{2^2} = \mathbb{F}_4$.

+	0	1	t	t + 1
0	0	1	t	t+ 1
1	1	0	t+1	t
T	t	t+1	0	1
t + 1	t+1	t	1	0

and

.	0	1	t	t + 1
0	0	0	0	0
1	0	1	t	t+1
t	0	t	t+1	1
t + 1	0	t+1	1	t

All elements of $\mathbb{F}_4$ are $\{\ 0\ ,\ 1\ ,\ t\ ,t^2\ \} = \{\ 0\ ,\ 1\ ,\ t\ ,\ t + 1\ \}$

Construction of $\mathbb{F}_8$

$g(t) = t^3 + t + 1$ is an irreducible polynomial over $\mathbb{F}_2\ [\ t\ ]$. t is a primitive root of this field.

t^2

$t^3 = t + 1$

$t^4 = t\ (t + 1) = t^2 + t$

$t^5 = t\ (t^2 + t\ ) = t^3 + t^2 = t^2 + t + 1$

$t^6 = t\ (\ t^2 + t + 1) = t^3 + t^2 + t = t + 1 + t^2 + t = t^2 + 1$

$t^7 = t(t^2 + 1) = t^3 + t = 1$

Elements of $\mathbb{F}_8 = \{0,1\ ,\ t\ ,\ t^2,\ t^3,\ t^4,\ t^5,\ t^6\ \} = \{\ 0\ ,\ 1\ ,\ t\ ,\ t^2,\ t+1\ ,\ t^2 + t\ ,\ t^2 + t + 1, t^2 + 1\}$

+	0	1	t	t^2	t + 1	t^2 + t	t^2 + t+1	t^2 + 1
0	0	1	t	t^2	t + 1	t^2 + t	t^2 +t +1	t^2 + 1
1	1	0	t + 1	t^2 + 1	t	t^2 +t +1	t^2 + t	t^2
t	t	t + 1	0	t^2 + t	1	t^2	t^2 + 1	t^2 + t +1
t^2	t^2	t^2 + 1	t^2 + t	0	t^2 +t +1	t	t + 1	1
t + 1	t + 1	t	1	t^2 +t +1	0	t^2 + 1	t^2	t^2 + t

$t^2 + t$	$t^2 + t$	$t^2 +t+1$	t^2	t	$t^2 + 1$	0	1	$t + 1$
$t^2 + t +1$	$t^2 +t+1$	$t^2 + t$	$t^2 + 1$	$t + 1$	t^2	1	0	t
$t^2 + 1$	$t^2 + 1$	t^2	$t^2 +t+1$	1	$t^2 + t$	$t + 1$	t	0

.	0	1	t	t^2	$t + 1$	$t^2 + t$	$t^2 + t+1$	$t^2 + 1$
0	0	0	0	0	0	0	0	0
1	0	1	t	t^2	$t + 1$	$t^2 + t$	$t^2 + t+1$	$t^2 + 1$
t	0	t	t^2	$t + 1$	$t^2 + t$	$t^2 +t +1$	$t^2 + 1$	1
t^2	0	t^2	$t + 1$	$t^2 +t$	$t^2 +t +1$	$t^2 + 1$	1	t
$t + 1$	0	$t + 1$	$t^2 +t$	$t^2 +t +1$	$t^2 + 1$	1	t	t^2
$t^2 + t$	0	$t^2 +t$	$t^2+ t+1$	$t^2 + 1$	1	t	t^2	$t + 1$
$t^2 + t +1$	0	$t^2+ t+1$	$t^2 + 1$	1	t	t^2	$t + 1$	$t^2 + t$
$t^2 + 1$	0	$t^2 +1$	1	t	t^2	$t + 1$	$t^2 + t$	$t^2 + t+1$

Construction of $\mathbb{F}_9$

$\mathbb{F}_9 = \{ \alpha t + \beta , \alpha , \beta \,\epsilon\, \{0,1,2 \}\}$

$g(t) = t^2 + 1$ is an irreducible polynomial in $\mathbb{F}_9 [t]$. The elements of $\mathbb{F}_9$ are : { 0, 1, 2, t, t +1, t +2, 2t, 2t +1 , 2t +2}

The Additional table

+	0	1	2	t	t+1	t+2	2t	2t + 1	2t + 2
0	0	1	2	t	t+1	t+2	2t	2t + 1	2t + 2
1	1	2	0	t+1	t+2	t	2t + 1	2t + 2	2t
2	2	0	1	t+2	t	t+1	2t + 2	2t	2t + 1
t	t	t+1	t+2	2t	2t + 1	2t + 2	0	1	2
t + 1	t + 1	t+2	t	2t + 1	2t + 2	2t	1	2	0
t + 2	t + 2	t	t+1	2t + 2	2t	2t + 1	2	0	1
2t	2t	2t + 1	2t + 2	0	1	2	t	t+1	t+2
2t + 1	2t + 1	2t + 2	2t	1	2	0	t+1	t+2	t
2t + 2	2t + 2	2t	2t + 1	2	0	1	t+2	t	t+1

×	0	1	2	t	t + 1	t + 2	2t	2t + 1	2t + 2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	t	t + 1	t + 2	2t	2t + 1	2t + 2
2	0	2	1	2t	2t + 2	2t + 1	t	t + 2	t + 1
t	0	t	2t	2	t + 2	2t + 2	1	t + 1	2t + 1
t + 1	0	t + 1	2t + 2	t + 2	2t	1	2t + 1	2	t
t + 2	0	t + 2	2t + 1	2t + 2	1	t	t + 1	2t	2
2t	0	2t	t	1	2t + 1	t + 1	2	2t + 2	t + 2
2t+ 1	0	2t + 1	t + 2	t + 1	2	2t	2t + 2	t	1
2t+ 2	0	2t + 2	t + 1	2t + 1	t	2	t + 2	1	2t

2.3. DEFINITION

If g has a positive degree and g = nm with n, m ∈ F_k [x] means that either n or m is a constant polynomial, the polynomial g ∈ F_k[x] is an irreducible polynomial over F_k.

Lemma. 2.1

Let S be a subfield of the finite field 𝔽 that has k elements. then k^n elements are in 𝔽, where n = [𝔽 : S]

Lemma. 2.2

If 𝔽 has k elements and is a finite field. Then, $\alpha^k = \alpha$ is satisfied by every α ϵ .

2.4. DEFINITION

A prime field is a field that has no proper subfields. For example, $\mathbb{F}_{\boldsymbol{p}}$ is a prime field because every subfield must include the elements 0 and 1, and because it is closed under addition, it also must include all other elements, i.e., it must be the entire field.

2.5. DEFINITION

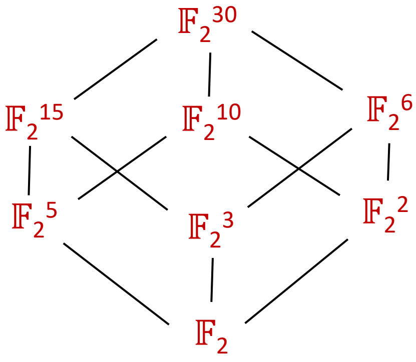
Let $\mathbb{F}$ be a field, the prime subfield is a field contains the intersection of all subfield of a field $\mathbb{F}$.

Theorem 2.1: There is a finite field with k elements for every prime p and every positive integer m. The splitting field of $\alpha^m = \alpha$ over $\mathbb{F}_{\boldsymbol{p}}$ is isomorphic to any finite field with $k = p^m$ elements.

Theorem 2.2: Let $\mathbb{F}_{\boldsymbol{k}}$ be the finite field with elements with $k = p^\alpha$. When β is a positive divisor of α, every subfield of $\mathbb{F}_{\boldsymbol{k}}$ has order p^β. On the other hand, there is only one subfield of $\mathbb{F}_{\boldsymbol{k}}$ with p^β elements if β is a positive divisor of α.

Example 2.1:

List all positive divisors of 30 to identify the subfields of the finite field $F_{2^{30}}$. The following figure shows the confinement relations between these different subfields.



Theorem. 2.3 : The multiplicative group $\mathbb{F}_k^*$ of nonzero elements of any finite field $\mathbb{F}_k$ is cyclic.

Theorem.2.4: A primitive element of $\mathbb{F}_k$ is a generator of the cyclic group $\mathbb{F}_k^*$.

Theorem 2.5: Except for the field $\mathbb{F}_2$, the sum of all elements in a finite field is 0.

Lemma 2.3: let $\mathbb{F}_k$ be a finite field with k elements and β ≠ 0 ϵ $\mathbb{F}_k$ and thus, $\beta^q = \beta$, for all β ϵ $\mathbb{F}_k$.

Theorem 2.6: Let $\mathbb{F}_{k^n}$ be the k^n element finite field. For some positive integer m dividing n, each $\mathbb{F}_{k^n}$ subfield has k^m elements. On the other hand, there is a single subfield of $\mathbb{F}_{k^n}$ of order k^m for any positive integer m dividing n.

Definition 2.6: Let E be a field that falls under the operations of F and a subset of F. E is thus referred to as a subfield of F, while F is referred to as an extension field of K.

Definition. 2.7: A primitive element, and occasionally a primitive root, is one that multiplicatively forms the group $\mathbb{F}_k^*$ of all nonzero elements of the field $\mathbb{F}_k$.

Remark 2.1: Let $\mathbb{F}_k$ be a finite field with a primitive element θ. Every nonzero element of $\mathbb{F}_k$ can then be expressed as a power of θ. It is fairly simple to compute the multiplication of field elements using this representation.

Theorem 2.7: Existence and Uniqueness of Finite Fields: A finite field with p^m elements exist for every prime number p and every positive integer m. Every finite field with p^m elements is also isomorphic to $\mathbb{F}_{p^m}$, as well. $\mathbb{F}_{p^m}$ is an extension field of $\mathbb{F}_p$ with the extension degree m and is the splitting field of $x^{p^m} - x$ over $\mathbb{F}_p$.

Definition 2.8: The trace $Tr_{F/S}$ (a) of a over S for a ϵ F = F_{k^n} and S = F_k is defined by

$$Tr_{F/S}(a) = a + a^k + \ldots + a^{k^{n-1}} .$$

Theorem 2.8: The trace function $Tr_{F/S}$ satisfies the following properties if S =F_k and F = F_{k^n} are given.

(a) $Tr_{F/S}$ (a + b) = $Tr_{F/S}$ (a) + $Tr_{F/S}$ (b) for all a , b ϵ F

(b) $Tr_{F/S}$ (c a) =c $Tr_{F/S}$ (a) for all c ϵ S , a ϵ F

(c) Considering F and S as vector spaces over S, $Tr_{F/S}$ is a linear transformation from F onto S;

(d) $Tr_{F/S}$ (α) = n α for all α ϵ S.

(e) $Tr_{F/S}$ (a^k) = $Tr_{F/S}$ (a) for all a ϵ F.

Theorem. 2.9: Assume that S is a finite field. Let S and D be the finite extensions of F and S, respectively. Then $Tr_{D/S}$ (a)= $Tr_{F/S}$ ($Tr_{D/S}$ (a)) for all a ϵ D.

Definition. 2.9: The norm $N_{F/S}(a)$ of a over S for a ϵ F = F_{k^n} and S =F_k is defined by

$$N_{F/S}(a) = a . a^k . . . a^{k^n} = a^{(k^n-1)/(k-1)} .$$

Theorem.2.10: The norm function $N_{F/S}$.satisfies the following properties if S =F_k and F = F_{k^n}

(a) $N_{F/S}(ab)$ = $N_{F/S}(a)N_{F/S}(b)$ for all a,b ϵ F.

(b) $N_{F/S}$ maps F onto S and F^* onto S^*.

(c) $N_{F/S}(a)$ = a^n for all a ϵ S.

(d) $N_{F/S}(a^k)$ = $N_{F/S}(a)$ for all a ϵ F

Theorem. 2.11: Assume that S is a finite field. Let S and D be the finite extensions of F and S, respectively. Then $N_{D/S}(a)$ = $N_{F/S}(N_{D/F}(a)$) for all a ϵ D.

PART 3

SOME SEQUENCES AND CORRELATIONS

3.1. SEQUENCES

3.1.1. Definition

Let b_0 , b_1 ,..., b_{m-1} be fixed elements of the finite field F_k and let m be a positive integer. a sequence of F_k elements s_0, s_1 ,..., s_n that meet the linear recurrence relation $s_{n+m} = \sum_{i=0}^{m-1} b_i s_{n+i}$ for n = 0, 1, . . .
is an LFSR sequence (or a linear feedback shift register sequence, also a linear recurring sequence) in F_k. The linear recurrence relation's or the LFSR sequence's order is represented by the integer m.

3.1.2. Theorem

Any LFSR sequence (s_n) in F_k of order m is periodic, with the smallest period being at most k^m - 1. The coefficient b_0 in the linear recurrence relation in Definition above must not be zero in order for (s_n) to be periodic.

3.1.3. Definition

An LFSR sequence in F_k of order m that satisfies the linear recurrence relation in Definition 3.1.1 is defined as (s_n). A characteristic polynomial of (s_n) and the linear recurrence relation, respectively, is the polynomial

$$f(x) = x^m + \sum_{i=0}^{m-1} b_i x^i \in F_k [x]$$

3.1.4. Definition

A maximal period sequence (also known as an m-sequence) in F_k is an LFSR sequence in which the minimal polynomial is a primitive polynomial over F_k.

Theorem 3.2: [3] Every maximal period sequence s in F_k has a period of at most k^m - 1, where m is the degree of the minimal polynomial of s.

Corollary 3.1: If and only if the minimum polynomial n ∈ F_k [x] satisfies n(0) ≠ 0 an LFSR sequence in F_k is periodic.

3.1.5. Definition

Let u(t) and v(t) be two n-period complex-valued sequences. The inner product $\delta_{u,v}(\tau) = \sum_{t=0}^{n-1} u(t+\tau)\bar{v}(t), \qquad 0 \leq \tau < n,$
where $\bar{v}$ indicates the complex conjugation of v and t + τ is calculated modulo n, is the periodic correlation of u(t) and v(t) at shift τ. The correlation between the sequences u(t) and v(t) is known as the autocorrelation and is denoted by u(t) if they are identical. The cross-correlation is $\delta_{u,v}(\tau)$, when u(t) and v(t) are distinct.

Remark: Sequences with good correlation qualities find use in various communication systems and give rise to a variety of difficult problems in finite fields. Finding single sequences with low autocorrelation for all nonzero shifts and families of sequences with low maximum nontrivial auto- and cross-correlation values between any two sequences in the family are the key application-related challenges.

Remark 3.2: Finding large families of sequences with low (nontrivial) auto- and cross-correlation between all pairs of sequences in the family is crucial in code-division multiple-access (CDMA) systems.

3.1.6. Definition

A family of H sequences of period n with symbols from the alphabet $\mathbb{Z}_k$ = 0,1,...,k-1 is represented by the formula R = {{s_i(t)}} | i = 1, 2,..., H. The cross-correlation between the sequences "s_i(t)" and "s_j((t)" at shift τ "" is denoted by $\delta_{i,j}(\tau\,)$. The parameters of a family R are (n , H , δ_{max}) where

δ_{max} = max {| $\delta_{i,j}(\tau\,)$| : either i ≠ j or $\tau\ \neq 0$ }.

Remark: For a family of sequences with given period n and family size H, there are three well-known constraints on the value of δ_{max}. These constraints are due to Welch, Sidelnikov, and Levenshtein.

3.2. KNOWN SEQUENCE FAMILIES WITH LOW MAXIMUM CORRELATION MAGNITUDE

Theorem 3.3: [3] (the Welch bound) Let R be a family of H cyclically different sequences with period n and let d ≥ 1 be an integer. Then

$$(\delta_{max}\,)^{2d} \geq \frac{1}{H\,n-1}\,\Big(\frac{H\,n^{2d+1}}{\binom{d+n-1}{n-1}} - \,n^{2d}\Big)\ .$$

Corollary 3. 2: (The Welch bound for d = 1)

$$\delta_{max} \geq n\,\sqrt{\frac{H-1}{H\,n-1}}$$

Remark: This means that for even modest values of H, $\delta_{max} \geq \sqrt{n}$.

Theorem 3.4: [3] The Sidelnikov bound satisfies the following inequality. for the sequence family H and arbitrary positive integer d, depending on the prime power k:

1- If k = 2, then

$$(\,\delta_{max})^2 > (\,2d + 1) + (\,n - d) + \frac{d(d+1)}{2} - \frac{2^d n^{2d+1}}{H(2d)!\binom{n}{d}}\ ,\ \ 0\ \leq d\ <\ \frac{2n}{5}$$

2- If k > 2 then

$$(\delta_{max})^2 > \frac{(d+1)}{2}\ (2n-d) - \frac{2^d n^{2d+1}}{H(d!)^2\binom{2n}{d}}\ ,\ \ d \geq 0\ .$$

3.2.1. Sidelnikov Sequence Family

Theorem 3.5. [3] Let E = $\mathbb{F}_{p^n}$ and D = $\mathbb{F}_p$. Let p be a prime, 0 < d < p, and α be an element of order $p^n - 1$. where $a_c\ \in E$ for 1 ≤ c ≤ d . let {s(t)} be a sequence over $\mathbb{F}_p$ of the form

S(t) = $Tr_{E/_D}$ $(\sum_{c=1}^{d} a_d \alpha^{ct}$),

The parameters of the Sidelnikov sequence family are m = $p^n - 1$, E ≥ $p^{n(d-1)}$ and $\delta_{max} \leq (\ d-1)p^{\frac{n}{2}} - 1$

3.2.2. No Sequence

Definition 3.4. Let E = $\mathbb{F}_{2^d}$, D = $\mathbb{F}_2$ and n = 2d , d ≥ 2. Let α be a primitive element of L = $\mathbb{F}_{2^n}$ and let 1 ≤ h ≤ $2^d - 1$, h ≠ 2^i for any i and gcd (h , $2^d - 1$) = 1, where a ∈ L and define

$$S_a(t) = Tr_{E/_D}\ \ ((Tr_{L/_E}\left(\alpha^t + a\alpha^{(2^d+1)t}\right))^h\ ),$$

The No sequence family in [3] is defined by

$$\gamma = \{\{s_a(t)\}|a\ \in L\ \}$$

the parameter of No sequence family are m = $p^n - 1$, E = 2^d and δ_{max} = $2^d + 1$.

3.2.3. The Small Samily of Kasami Sequences Construction

Definition 3.5. Let E = $\mathbb{F}_{2^d}$, D = $\mathbb{F}_2$ and n = 2d , d ≥ 2 . Let α be a primitive element of L = $\mathbb{F}_{2^n}$ and

$$S_a(t) = Tr_{L/_D}(\ \alpha^t) +\ Tr_{E/_D}\ (a\alpha^{(2^d+1)t}),$$

Where a ∈ E, the small family of Kasami sequence [3] is $\mu = \{\{s_a(t)\}|a\ \in E\ \}$.

Theorem 3.6. The parameters of the small family of Kasami sequence are the same as for the No sequence family. The small family of Kasami sequence have smaller linear complicity than the No sequence family.

3.2.4. The Large Family of Kasami Sequence

Definition 3.6. [6] Let n = 2d . d ≥ 2 , let α and β be a primitive elements of $\mathbb{F}_{2^d}$ and $\mathbb{F}_{2^n}$ respectively. For 0 ≤ t ≤ $2^n - 2$, the definition of the large family of Kasami sequence is :

$S_a(t) = \left\{ s_{\mu\rho}(t) : \mu \in \mathbb{F}_{2^n} , \rho \ \in \mathbb{F}_{2^d} \right\} \cup \left\{ s_{\gamma\sigma}(t) : \gamma \in \ \Delta , \ \sigma \ \in \ \aleph \right\}$

Where

$$s_{\mu\rho}(t) = Tr_1^n \left(\alpha^t + \ \mu\alpha^{(2^{d+1}+1)t} \right) + Tr_1^n \left(\rho\alpha^{(2^d+1)t} \right) \text{ and}$$

$$s_{\gamma\sigma}(t) = Tr_1^n \left(\ \gamma\alpha^{(2^{d+1}+1)t} \right) + Tr_1^n \left(\sigma\alpha^{(2^d+1)t} \right)$$

The definition of Δ and ℵ depending on m is as follows :

1. For n ≡ 0 mod 4 , $\Delta = \{ 1 , \alpha , \alpha^2 \} \ and \ \aleph = \{ 1, \beta , \dots , \beta^{\frac{(2^d-1)}{3}-1} \}$
2. For n ≡ 2 mod 4 , $\Delta = \{ 1 \} \ and \ \aleph = \mathbb{F}_{2^d}$.

3.2.5. Gold Sequence

Definition 3.7. [4] Let {s(t)} be an m-sequence of period m = $2^n - 1$. let n be odd, k = $2^d + 1$ and gcd (d, n) = 1. The Gold sequence family is defined by

$$\theta = \{s(t)\} \cup \{s(kt)\} \cup \{\{ s(t+\tau) + s(kt)\} \mid 0 \le \tau \le m\text{-}1\}.$$

The parameter of the family of Gold sequence is m = $2^n - 1$, E= $2^n + 1$ and δ_{max} = $2^{\frac{n+1}{2}} + 1$.

3.2.6. Gold-like Sequence

Definition 3.8: Let p be a prime number and m be an odd positive integer, let ς_i be the enumeration of the elements of the finite field $\mathbb{F}_{2^n}$ for 0 ≤ i ≤ $2^n - 1$. The definition of the Gold-like sequence in [7] is:

$$S = \{s_i(t) : i = 0 , 1,2, \dots , 2^n, 0 \ \le t \ \le \ 2^n - 2 \}$$

where

$$s_i(t) = \begin{cases} Tr_1^n\,(\varsigma_i\,\alpha^t) + f(\alpha^t) & , \quad 0 \le i < 2^n \\ Tr_1^n\,(\alpha^t) & , \qquad\quad i = 2^n \end{cases}$$

The quadratic form is defined as follows:

$$\text{f(x)} = \sum_{d=1}^{\frac{n-1}{2}} Tr_1^n(x^{2^d+1}) \,.$$

The Gold-like family sequence has $2^n + 1$ cyclically distinct sequences of period $2^n - 1$. And its maximum magnitude is $\delta_{max} = 2^{\frac{n+1}{2}} + 1$ and the correlation distribution is

$$C_{i,j}(\tau) = \begin{cases} -1 + 2^n, & 2^n + 1\; times \\ -1, & 2^{3n-1} + 2^{2n} - 2^n - 2\; times \\ -1 + 2^{\frac{n+1}{2}}, (2^{2n} - 2)\left(2^{n-2} + 2^{\frac{n-3}{2}}\right) times \\ -1 - 2^{\frac{n+1}{2}}, (2^{2n} - 2)\left(2^{n-2} + 2^{\frac{n-3}{2}}\right) times \end{cases}$$

3.2.7. The Kumar and Moreno p-ary bent sequence

Definition 3.9. Let α be a primitive element of $\mathbb{F}_{p^n}$ and p be an odd prime. Let n = 2d and g(x) be a p-ary bent function on the vector space V_p^d , { $\theta_1, \dots, \theta_d$ } be a bases of $\mathbb{F}_{p^d}$ over $\mathbb{F}_p$ and $\varphi \in \mathbb{F}_{p^n} - \mathbb{F}_{p^d}$. For γ ∈ $\mathbb{F}_{p^d}^*$. the definition of the Kumar and Moreno p-ary bent sequence in [8] is:

S = $\{s_j(t) : j \in \mathbb{F}_{p^d}, 0 \le t \le p^n - 2\}$

where

$$s_j(t) = g\big(R(\alpha^t)\big) + Tr_1^n(\,(j\,\varphi + \gamma)\alpha^t)$$

And

$$\text{R(x)} = \{\, Tr_1^n(\theta_1 \varphi x), \dots, Tr_1^n(\theta_n \varphi x)$$

3.2.8. S$_a$ Sequence

Definition 3.10. [3] Let p be a prime number and d be an integer number, n = 2d. Let S_a be a p-ary sequence family of period $p^n - 1$. For an integer 1≤ a ≤ $\frac{p^d+1}{p+1}$, the definition of S_a is:

$$S_a = \{s_\rho(t) \mid \rho \in F_a , 0 \le t < p^m - 1\}$$

where

$$s_\rho(t) = Tr_1^n(\alpha^t - \rho\alpha^{kt})$$

And

$$F_a = \{\, \alpha^{ej+a} \,\big|\, j \equiv 0 \, mod \; p+1 \; for \; 0 \le j < (p+1)(p^d-1) \cup \{0\} \; and$$

e = $\frac{p^d+1}{p+1}$

3.2.9. Kim and No Sequences

Definition 3.11. Let n = dk and n be a positive odd integer, d ≥ 3 and d be an odd integer. Let s be a positive integer satisfying gcd(n , s) = k. let 0 ≤ i ≤ $2^n - 1$, and ς_i be the enumeration of the elements of F_{2^n}.

Let g(x) be a quadratic form:

$$g(x) = \sum_{j=1}^{\frac{d-1}{2}} tr_1^n(x^{2^{kj}+1}).$$

Then the definition of Kim and No sequence is

$$S = \{s_a(t) \mid 0 \le a \le 2^n, 0 \le t < 2^n - 2\}$$

Where

$$s_a(t) = \begin{cases} Tr_1^n\,(\varsigma_i\,\alpha^t) + g(\alpha^t) & , \quad 0 \le i < 2^n \\ Tr_1^n\,(\alpha^t) & , \quad\quad i = 2^n \end{cases}$$

The Kim and No family sequence has $2^n + 1$ cyclically distinct sequences of period $2^n - 1$. And its maximum magnitude is δ_{max} = $2^{\frac{n+k}{2}} + 1$ and the correlation distribution is

$$C_{i,j}(\tau) = \begin{cases} -1 + 2^n, & 2^n + 1 \; times \\ -1, & (2^n - 2^{n-k} + 1)(2^{2n} - 2) \; times \\ -1 + 2^{\frac{n+k}{2}}, & \left(2^{n-k-1} - 2^{\frac{n-k-2}{2}}\right)(2^{2n} - 2) times \\ -1 - 2^{\frac{n+k}{2}}, & \left(2^{n-k-1} - 2^{\frac{n-k-2}{2}}\right)(2^{2n} - 2) times \end{cases}$$

Table 3.1: List of some known sequence families and their maximum correlation magnitudes δ_{max}.

Sequence family	p	n	Period	Family size	δ_{max}
Sidelnikov	2	d < p	$p^n - 1$	$\geq p^{n(d-1)}$	(d-1)$p^{\frac{n}{2}} + 1$
No	2	even	$2^n - 1$	$2^{\frac{n}{2}}$	$2^{\frac{n}{2}} + 1$
Small family of kasami	2	even	$2^n - 1$	$2^{\frac{n}{2}}$	$2^{\frac{m}{2}} + 1$
Large family of kasami	2	even	$2^n - 1$	$2^{\frac{n}{2}}(2^n - 1)$	$2^{\frac{n}{2}} + 1$
Gold	2	odd	$2^n - 1$	$2^{\frac{n}{2}}$	$2^{\frac{n+1}{2}} + 1$
Gold-like	2	odd	$2^n - 1$	$2^n + 1$	$2^{\frac{n+1}{2}} + 1$
Kumar and Moreno	Odd	arbitrary	$p^n - 1$	$p^{\frac{n}{2}}$	$p^{\frac{n}{2}} + 1$
S_a	3mod 4	even	$p^n - 1$	p^n	$\frac{p^2}{p+1}p^d + 1$
Kim and No	2	odd	$2^n - 1$	$2^n + 1$	$2^{\frac{n+k}{2}} + 1$

PART 4

A SEQUENCE FAMILY BY TANG ET AL

Many applications, including Code Division Multiple Access (CDMA) communication systems and cryptography systems, make use of sequence sets with strong correlations. Since the late 1960s, numerous families of binary sequences of length $2^n - 1$, where n is a positive integer, have been discovered. The oldest binary family of $2^n + 1$ sequences among them, when n is odd, is the well-known gold sequence family, with three levels of out-of-phase auto- and cross-correlation (nontrivial correlation) values of -1 and $-1 \pm 2^{(n+1)/2}$. Regarding the Sidelnikov bound, the family is ideal. The term "Gold-like sequences" was used by Boztas and Kumar in the 1990s to describe an ideal sequence family that has the same correlation distribution as Gold sequences but a greater linear span [7]. Later, using the quadratic form technique, Kim and No further generalized the Gold-like sequences to become GKW-like sequences. The generalize Gold-like sequences by using the quadratic form technique. With $2^n + 1$ sequences of $2^n - 1$ length, creating a new family of ideal binary sequences whose correlation distribution is the same as that of the Gold sequence for n odd. This family can be thought of as a brand-new subclass of Gold-like sequences.

4.1. PRELIMINARIES

Through this part, the following notation are used:

- n, q and d are odd integers with n = dq and q ≥ 3.
- δ is an element in $\mathbb{F}_{2^d}$ and $\delta \neq 1$. And $\{\delta_0, \delta_1, \cdot \cdot \cdot, \delta_{2^n-1}\}$ is an enumeration of the elements in $\mathbb{F}_{2^n}$.
- $tr_d^n(y) = \sum_{i=0}^{q-1} y^{2^{di}}$ and $tr_1^n(y) = \sum_{i=0}^{n-1} y^{2^1}$ are the trace functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^d}$ and $\mathbb{F}_{2^n}$ to F_2 respectively.

Definition 4.1: Let $u = (u(0), u(1), \ldots, u(L-1))$ and $v = (v(0), v(1), \ldots, v(L-1))$ be two binary sequences of period L, we define the periodic correlation between u and v as

$$R_{u,v(\tau)} = \sum_{t=0}^{L-1}(-1)^{u(t)+v(t+\tau)}, 0 \leq \tau < L. \qquad (4.1)$$

We can transform this equation to the following form:

$$P(\alpha) = \sum_{y \in \mathbb{F}_{2^n}}(-1)^{p(y)+tr_1^n(\alpha y)}, \qquad (4.2)$$

P (α) is called the trace transform of p(y) and p(y) is a quadratic form in $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and α ∈ $\mathbb{F}_{2^n}$.

In [2], the quadratic form has been thoroughly explored. The smallest number of variables required to express the function under the nonsingular coordinate transformations is known as the quadratic form's rank, and it determines the quadratic form in all of its details.

Lemma 4.1: In $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ let p(y) be a quadratic form. The distribution of the trace transform values is given bellow if the rank of the p(y) is 2r, 2 $\leq 2r < n$

$$P(\alpha) = \begin{cases} 2^{n-r}, 2^{2r-1} + 2^{r-1} times \\ 0, \quad 2^n - 2^{2r} \quad times \\ -2^{n-r}, 2^{2r-1} - 2^{r-1}\ times \end{cases} \qquad (4.3)$$

From Lemma 4.1, Calculating the quadratic form's trace transform requires knowledge of its rank. In [2] it is shown that the relationship between the rank 2r and the number of solutions to $y \in F_{2^n}$ to

$$B(y,z) = q(y) + q(z) + q(y+z) = 0, \forall\ z\ \in\ F_{2^n}\ . \qquad (4.4)$$

Suppose that the number of the solution is K, then $2r = n - log_2 K$.

In [7], Bozats and Kumar studied the quadratic form $q(y)$ defined as

$$q(y) = \sum_{i=1}^{\frac{n-1}{2}} tr_1^n(y^{2^i+1}). \qquad (4.5)$$

Lemma 4.2. [7] The associated symplectic form of $f(y)$ is

$$B(y,z) = q(y) + q(z) + q(y+z) = tr_1^n[z(tr_1^n(y) + y)]. \quad (4.6)$$

In 2003, Kim and No generalized the quadratic form q(y) to

$$s(y) = \sum_{i=1}^{\frac{q-1}{2}} tr_1^n\left(y^{2^{di}+1}\right), \qquad (4.7)$$

Lemma 4.3: The associated symplectic form of g(y) is

$B(y,z) = s(y) + s(z) + s(y+z) = tr_1^n[z(tr_d^n(y) + y)]$. (4.8)

Construction a family of sequences based on two quadratic forms q(y) and s(δy) as follows [10].

Definition 4.2. The binary family U of sequences $\{u_i$, i = 0, 1, ⋯, $2^n\}$ of length $2^n - 1$ is defined by

$$u_i(t) = \begin{cases} tr_1^n(\delta_i a^t) + q(a^t) + s(\delta a^t), 0 \ \le i < 2^n \\ tr_1^n(a^t), \qquad\qquad\qquad\qquad i = 2^n \end{cases} \qquad (4.9)$$

The correlation distribution of Family $\mathcal{U}$ is as follows:

$$R_{ij}(T) = \begin{cases} -1 + 2^n, \quad 2^n + 1 \ times \\ -1, \qquad\quad 2^{3n-1} + 2^{2n} - 2^n - 2 \ times \\ -1 + 2^{\frac{n+1}{2}}, (2^{2n} - 2)\left(2^{n-2} + 2^{\frac{n-3}{2}}\right) times \\ -1 - 2^{\frac{n+1}{2}}, (2^{2n} - 2)\left(2^{n-2} + 2^{\frac{n-3}{2}}\right) times \end{cases} \qquad (4.10)$$

Remark 4.1: The sequences in Family U in Definition 4.2 are a Gold-like family when δ = 0. The new sequences Family U in Definition 4.2 have the same correlation distribution as Gold sequences and sequences that are similar to Gold-like sequences when δ ∈ F_{2^d} \{0, 1}, .

4.2. QUADRATIC FORM q(y) + s(δy) + q(λy) + s(δλy)

We examine the quadratic form q(y) + s(δy) + q(λy) + s(δλy), where $\lambda \neq 1 \in F_{2^n}$ is a constant. By (4.6) and (4.8), the related symplectic form for this quadratic form is $B(y,z) = tr_1^n[z(\lambda tr_1^n(\lambda y) + tr_1^n(y) + \ \delta\lambda tr_d^n(\delta\lambda y) + \delta tr_2^n(\delta y) + (1 - \delta^2)(1 + \lambda^2)y]$.

Similar to that, we must count the solutions to

$\lambda tr_1^n(\lambda y) + tr_1^n(y) + \delta\lambda tr_d^n(\delta\lambda y) + \delta tr_2^n(\delta y) + (1 - \delta^2)(1 + \lambda^2)y = 0.$

Suppose that $tr_1^n(y) = \alpha$ and $tr_1^n(\lambda y) = \beta$ Then

$$y = \frac{\delta^2\alpha + tr_1^e(\alpha) + \lambda(\delta^2\beta + tr_1^e(\beta))}{(1+\delta^2)(1+\lambda^2)} \qquad (4.11)$$

Let $Y = tr_d^n\left(\frac{1}{1+\lambda}\right)$. connecting (4.11) into $tr_d^n(y) = \alpha$ and $tr_d^n(\lambda y) = \beta$, we have

$$\left(\delta^2\alpha + tr_1^d(\alpha) + \delta^2 b + tr_1^d(\beta)\right)X^2 + (\delta^2\beta + tr_1^d(\beta))Y = \alpha(1 + \delta^2) \qquad (4.12)$$

And

$$\left(\delta^2\alpha + tr_1^d(\alpha) + \delta^2\beta + tr_1^d(\beta)\right)Y^2 + (\delta^2\beta + tr_1^d(\beta))Y = tr_1^d(\beta) + \beta\ . \ (4.13)$$

There are three cases

- **a)** If Y = 0, then $\alpha = 0$ and $tr_1^d(\beta) = \beta$. Obviously, there are two solutions $(\alpha, \beta) = (0, 0)$ and (0, 1);
- **b)** If Y = 1, then $tr_1^d(\alpha) = \alpha$ and β = 0. It is easy to see that there are two solutions (α, β) = (0, 0) and (1, 0);
- **c)** If Y = γ ∈ F_{2^d} \ {0, 1}, then

$$\delta^2\alpha + tr_1^d(\alpha) + \delta^2\beta + tr_1^d(\beta) = \frac{\alpha(\delta^2+1)\beta + tr_1^d(\beta)}{\gamma}. \qquad (4.14)$$

Then,

$$\gamma(\alpha + b) = \alpha,$$

$$\gamma\left(\alpha + \beta + tr_1^d(\alpha) + tr_1^d(\beta)\right) = \beta + tr_1^d(\beta)$$

There are four cases depending on the values of $tr_1^d(\alpha)$ and $tr_1^d(\beta)$

1. $tr_1^d(\alpha) = 0$ and $tr_1^d(\beta) = 0$ Then

$$\gamma(\alpha + \beta) = \alpha,$$

$$\gamma(\alpha + \beta) = \beta.$$

Immediately, $\alpha = \beta = 0$.

2. $tr_1^d(\alpha) = 1$ and $tr_1^d(\beta) = 1$ Then

$$\gamma(\alpha + \beta) = \alpha,$$

$$\gamma(\alpha + \beta) = \beta + 1.$$

Therefore, α = γ and β = γ +1 lead to a contradiction with $tr_1^d(\alpha) = tr_1^d(\beta) = 1$

3. $tr_1^d(\alpha) = 1$ and $tr_1^d(\beta) = 0$ Then

$$\gamma(\alpha + \beta) = \alpha,$$

$$\gamma(\alpha+\beta+1)=\beta.$$

We have $\alpha=\gamma^2+\gamma$, and $tr_1^d(\gamma)=1$

4. $tr_1^d(\alpha)=0$ and $tr_1^d(\beta)=1$ Then

$$\gamma(\alpha+\beta)=\alpha,$$

$$\gamma(\alpha+\beta+1)=\beta+1.$$

Immediately, $\alpha=\gamma^2+\gamma, \beta=\gamma^2+1$, and $tr_1^d(\gamma)=0$

Thus, for Y = γ ∈ F_{2^d} \ {0, 1}, the associated symplectic form B(y,z) has

1.Two solutions (α,β)=(0, 0) and $(\gamma^2,\gamma^2+\gamma)$ when $tr_1^d(\gamma)=1$;

2. Two solutions (α,β)=(0, 0) and $(\gamma^2+\gamma\,,\gamma^2+1)$ when $tr_1^d(\gamma)=0$;

In summary, the rank of the quadratic form q(y) + s(δy) + q(λy) + s(δλy), is therefore 2r = n − 1.

4.3. PROOF OF THE CORRELATION DISTRIBUTION OF THE SEQUENCES FAMILY $\mathcal{U}$.

In five cases, we examine the correlation function $R_{a,b}(\tau)$ between u_a and u_b

1. $0 \le a = b \le 2^n$ and $\tau = 0$:

   In this trivial case, $R_{a,b}(0) = 2^n - 1$.
2. $a = b = 2^n$ and $0 < \tau < 2^n - 1$:

   Since u_{2^n} is an m-sequence, we have $R_{a,b}(\tau)$ = -1
3. $0 \le a \ne b < 2^n$ and $\tau = 0$:

   In this case, u_a(t)+ u_b(t)=, $tr_1^n((\delta_a+\delta_b)\alpha^t)$and therefore, $R_{a,b}(\tau) = -1$ again from the auto-correlation property of m-sequence $(tr_1^n(\alpha^t), t = 0,1,\dots,2^n-2\,)$
4. $0 \le a < 2^n$ and $b = 2^n$ (or ($a = 2^n$ and $0 \le b < 2^n$)):

   For a fixed $0 \le \tau < 2^n - 1$,

$$R_{a,2n}(\tau)=\sum_{y\in F_2^n}(-1)^{tr_1^n((\delta_i+\lambda)y)+q(y)+s(\delta y)}-1,$$

Where λ = α^τ.

So, the rank of the quadratic form $q(y)+s(\delta y)$ is n − 1. Consequently, it follows from Lemma 4.1 that the distribution of the correlations for a fixed $0 \le \tau < 2^n - 1$ is

$$R_{a,2^n}(\tau) = \begin{cases} -1 + 2^{\frac{n+1}{2}} \ , 2^{n-2} + 2^{\frac{n-3}{2}} times \\ -1, \qquad 2^n - 2^{n-1} \quad times \\ -1 - 2^{\frac{n+1}{2}} \ , 2^{n-2} + 2^{\frac{n-3}{2}} times \end{cases}$$

As τ varies over the range $0 \le \tau < 2^n - 1$, the distribution of the correlations becomes

$$R_{a,2^n}(\tau) = \begin{cases} -1 + 2^{\frac{n+1}{2}} \ , (2^{n-2} + 2^{\frac{n-3}{2}})(2^n - 1) times \\ -1, \qquad (2^n - 2^{n-1})(2^n - 1) \quad times \\ -1 - 2^{\frac{n+1}{2}} \ , (2^{n-2} + 2^{\frac{n-3}{2}})(2^n - 1) times \end{cases}$$

The same distribution holds for $R_{2^n,b}(\tau)$, the case of $a = 2^n$ and $0 \le b < 2^n$.

5. $0 \le a, b < 2^n$ and $0 < \tau < 2^n - 1$:

For a fixed $0 \le \tau < 2^n - 1$, let $\lambda = \alpha^\tau$. Then, the correlation function is

$$R_{a,b}(\tau) = \sum_{y \in F_{2^n}} (-1)^{tr_1^n((\delta_i + \delta_j \lambda)y) + q(y) + s(\delta y) + q(\lambda y) + s(\delta \lambda y)} - 1,$$

the rank of quadratic form q(y) + s(δy) + q(λy) + s(δλy) is n−1. Similar to the distribution in Case 4, the correlation distribution can be computed from Lemma 4.1 as

$$R_{a,b}(\tau) = \begin{cases} -1 + 2^{\frac{n+1}{2}} \ , (2^{n-2} + 2^{\frac{n-3}{2}})2^n(2^n - 2) times \\ -1, \qquad (2^n - 2^{n-1})2^n(2^n - 2) \quad times \\ -1 - 2^{\frac{n+1}{2}} \ , (2^{n-2} + 2^{\frac{n-3}{2}})2^n(2^n - 2) times \end{cases}$$

where τ ranges over $0 < \tau < 2^n - 1$ and a, b varies from 0 to $2^n - 1$, respectively.

We derive the distribution of the correlation values for the Family U sequences by compiling the findings from the above five cases.

PART 5

SOME COMPUTATIONAL RESULTS ON THE PAPER YAN ET ALL. [11]

5.1. PRELIMINARIES

Throughout this part, the following notation are used:

- P is a prime
- e , m , n and r are positive integers with r = 2m , n = be and r = $\left\lfloor \frac{m}{2} \right\rfloor$, where $\lfloor * \rfloor$ means round down.
- k = p^e , we also denote F_{p^e} as F_k and F_{p^n} as F_{k^b}.
- The trace function $tr_b^n(x)$ from F_{p^n} to F_{p^b} is defined by

  $$tr_b^n(x) = x + x^{p^b} + \ldots + x^{p^{b(e-1)}} \quad , x \in F_{p^n} .$$

Definition 5.1: let B = { { b_i(q)} 0 $\leq$ q $\leq N-1$| 1 $\leq i \leq M$} be a family of M p-ary sequences of period N. The periodic correlation function between two sequences is

$$R_{b_i,b_j}(\tau) = \sum_{\mathrm{q}=0}^{N-1} \sigma^{b_i(\mathrm{q})-b_j(\mathrm{q}+\tau)} \quad ,0 \leq \tau \leq N-1 . \quad (5.1)$$

Where σ is a primitive complex p-th root of unity. We say that $b_i = \{b_i(\mathrm{q})\}_{\mathrm{q}=0}^{N-1}$ and $b_j = \{b_j(\mathrm{q})\}_{\mathrm{q}=0}^{N-1}$ are cyclically distinct if $b_i(\mathrm{q}) = b_j(\mathrm{q}+\tau)$ for all q has no integer τ. The cyclical equivalent of b_i *and* b_j can be easily observed if and only if $R_{b_i,b_j}(\tau) = N$ for some τ. The maximum correlation magnitude R_{max} of B is defined as $R_{max} = \max\{ |R_{b_i,b_j}(\tau)| \; either\; i \neq j \; or \; \tau \neq 0\}$.

Then, B is said to be an (N , M , R_{max}) family of sequence.

Definition 5.2: Let u be a primitive element of F_{p^n} , and b, n, m, e and r be positive integer as defined above. The definition of a family B [11] is

$$B = \{b_A(\mathrm{q})\}_{\mathrm{q}=0}^{p^n-2} : A = (a_1, a_2, \ldots, a_r), a_i \in F_{p^n} \; for \; 1 \leq i \leq r \}, \quad (5.2)$$

Where, for each $0 \leq \mathrm{q} \leq p^n - 2$,

$$b_A(\mathrm{q}) = tr_1^n(u^{\mathrm{q}}) + \sum_{i=1}^{r} tr_1^n(a_i u^{(k^{2i-1}+1)\mathrm{q}}). \quad (5.3)$$

Theorem 5.1: There are p^{nt} cyclically distinct sequences of period $p^n - 1$ in the sequence set B described by (5.2) . The sequences in B have a correlation that is (4r + 2) – valued for p= 2 , taking values from the set
$\{ k^b - 1 , -1, -1 \mp k^m, -1 \mp k^{m+1}, \dots , -1 \mp k^{m+2r-1} \}$.
Now we will give further examples of these sequences.

5.2. EXAMPLES:

1. Let n = 4 , b = 4, e = 1, m = 2, r = 1, p = 2, then k = p^e= 2, b = 2m= 4, n = be= 4, r = 1 and u is a primitive element of F_{2^4} satisfying $u^4 + u + 1 = 0$. There are 2^4 cyclically distinct sequences in family B, then we have
$b_A(\mathrm{q}) = tr_1^n(u^{\mathrm{q}}) + tr_1^n(a_1 u^{3\mathrm{q}})$. $a_1 \in F_{2^4}$ for $0 \leq \mathrm{q} \leq 2^4 - 2$.

a=1
[0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0]
a= u
[0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0]
a= u^2
[0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0]
a= u^3
[1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1]
a= u^4
[0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1]
a= u^5
[0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1]
a = u^6
[1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0]
a = u^7
[1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1]
a = u^8
[0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1]
a = u^9
[1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0]
a = u^{10}
[0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0]
A = u^{11}
[1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1]
a = u^{12}
[1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0]

a = u^{13}
[1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1]
a = u^{14}
[1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0]
0
[0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1]

2. Let n = 6, b = 6, e =1, m = 3, r = 1, p = 2 then k = p^e= 2, b = 2m= 6, n = be= 6, r = 1 and u is a primitive element of F_{2^6} . There are 2^6 cyclically distinct sequences in family B, then we have

$$b_A(\text{q}) = \ tr_1^n(\ u^{\text{q}}) + \ tr_1^n(a_1 u^{3\text{q}}). \quad a_1 \ \in \ F_{2^6}\, for\ 0\ \leq \text{q}\ \leq 2^6 - 2\ .$$

a=1
[0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1,
1, 0, 1, 0, 0, 1,0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1]
a= u
[0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0,
0, 0, 1, 1, 1, 0,1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0]
a= u^2
[0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0,
0, 1, 1, 1, 0, 0,0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0]
a= u^3
[1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0,
1, 1, 0, 1, 1, 1,0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1]
a = u^4
[0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1,
1, 1, 1, 0, 0, 0,1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1]
a = u^5
[0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1,
0, 1, 1, 1, 0, 1,1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1]
a = u^6
[1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0,
0, 0, 1, 0, 1, 1,0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0]
a = u^7
[0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0,
0, 1, 0, 1, 0, 0,1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1]
a = u^8
[0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1,
0, 1, 1, 1, 1, 0,1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1]
a = u^9
[0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1,
1, 1, 0, 0, 1, 1,0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0]
a = u^{10}
[0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1,
0, 0, 1, 1, 0, 0,0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1]
a = u^{11}
[1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1,
0, 1, 1, 0, 0, 0,0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1]

$a = u^{12}$
[1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0,
0, 0, 0, 0, 1, 1,1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1]
$a = u^{13}$
[1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1,
1, 1, 1, 1, 0, 1,0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1]

$a = u^{14}$
[0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1,
0, 1, 0, 1, 0, 1,0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0]
$a = u^{15}$
[0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1,
1, 0, 0, 0, 1, 0,1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0]
$a = u^{16}$
[0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0,
0, 1, 1, 1, 1, 1,0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0]
$a = u^{17}$
[0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1,
0, 0, 1, 1, 1, 1,0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1]
$a = u^{18}$
[0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0,0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1]
$a = u^{19}$
[1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1,
0, 1, 1, 0, 1, 1,0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1]
$a = u^{20}$
[0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1,
1, 1, 1, 0, 1, 1,1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1]
$a = u^{21}$
[1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0,
1, 0, 0, 1, 0, 1,1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1]
$a = u^{22}$
[1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1,
0, 1, 0, 0, 1, 1,1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0]
$a = u^{23}$
[1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0,
0, 1, 0, 0, 1, 0,0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1]
$a = u^{24}$
[1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0,
1, 0, 1, 1, 1, 0,0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0]
$a = u^{25}$
[1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1,
0, 0, 0, 0, 1, 0,0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0]
$a = u^{26}$
[1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1,
0, 0, 0, 0, 0, 1,0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0]
$a = u^{27}$

[0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0,
1, 1, 1, 0, 0, 1,0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0]
$a = u^{28}$
[0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1,
1, 0, 0, 0, 0, 1,1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0]
$a = u^{29}$
[1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1,
1, 0, 0, 1, 1, 1,0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0]

$a = u^{30}$
[0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0,
0, 1, 0, 1, 1, 1,1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1]
$a = u^{31}$
[1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0,
1, 0, 0, 1, 1, 0,1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1]
$a = u^{32}$
[0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0,
1, 0, 1, 0, 1, 1,1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0]
$a = u^{33}$
[1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1,
0, 0, 1, 0, 1, 0,1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1]
$a = u^{34}$
[0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0,
1, 0, 1, 0, 0, 0,1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0]
$a = u^{35}$
[0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0,
1, 1, 0, 0, 1, 0,1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1]
$a = u^{36}$
[0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1,
1, 1, 0, 0, 0, 0,0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0]
$a = u^{37}$
[1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0,
1, 1, 0, 1, 0, 0,0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1]
$a = u^{38}$
[1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0,
0, 0, 0, 0, 0, 0,1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1]
$a = u^{39}$
[0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0,
0, 0, 0, 1, 0, 1,0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1]
$a = u^{40}$
[0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0,
0, 0, 1, 1, 0, 1,1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0]
$a = u^{41}$
[1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1,
1, 0, 0, 1, 0, 0,0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0]
$a = u^{42}$
[1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1,
1, 0, 1, 1, 1, 1,1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1]

$a = u^{43}$
[1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1,
1, 1, 1, 1, 1, 0,0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1]
$a = u^{44}$
[1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0,
1, 0, 1, 1, 0, 1,0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0]
$a = u^{45}$
[0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0,
1, 1, 1, 0, 1, 0,0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0]

$a = u^{46}$
[1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0,
0, 1, 1, 0, 0, 1,1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0]
$a = u^{47}$
[1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0,
1, 1, 1, 1, 1, 1,1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0]
$a = u^{48}$
[1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0,
0, 1, 0, 0, 0, 1,0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1]
$a = u^{49}$
[0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1,
0, 1, 0, 1, 1, 0,0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0]
$a = u^{50}$
[1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0,
0, 1, 1, 0, 1, 0,1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0]
$a = u^{51}$
[0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1,
0, 0, 0, 1, 1, 1,1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0]
$a = u^{52}$
[1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1,
0, 0, 1, 0, 0, 1,1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1]
$a = u^{53}$
[1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1,
0, 1, 0, 0, 0, 0,1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0]
$a = u^{54}$
[0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1,
1, 0, 1, 0, 1, 0,0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1]
$a = u^{55}$
[1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1,
1, 1, 0, 1, 1, 0,1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0]
$a = u^{56}$
[0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1,
0, 0, 0, 1, 0, 0,1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0]
$a = u^{57}$
[0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0,
1, 1, 0, 0, 0, 1,1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1]
$a = u^{58}$

[1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0,
0, 0, 1, 0, 0, 0,0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0]

a = u^{59}

[1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1,
1, 0, 1, 1, 0, 0,1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1]

a = u^{60}

[0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0,
0, 0, 0, 1, 1, 0,0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1]

a = u^{61}

[1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1,
1, 1, 0, 1, 0, 1,1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0]

a = u^{62}

[1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0,
1, 1, 1, 1, 0, 0,1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0]

0

[0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0,
1, 0, 0, 0, 1, 1,0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1]

3. Let p = 3, n = 4, b = 4, e = 1, m = 2, r = 1 then k = p^e= 3, b = 2m= 4, n = be= 4, r = 1 and u is a primitive element of F_{3^4} . There are 3^4 cyclically distinct sequences in family B, then we have

$b_A(\mathrm{q}) = tr_1^n(u^{\mathrm{q}}) + tr_1^n(a_1 u^{4\mathrm{q}}). \quad a_1 \in F_{3^4} \, for \, 0 \le \mathrm{q} \le 3^4 - 2$.

a=1

[2, 0, 2, 0, 1, 0, 2, 1, 0, 0, 1, 2, 1, 1, 0, 0, 1, 0, 2, 2, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1,
2, 1, 0, 1, 1, 1, 1]

a = u

[2, 1, 2, 1, 1, 2, 1, 1, 2, 1, 1, 1, 1, 0, 0, 1, 2, 0, 0, 1, 1, 2, 1, 1, 0, 2, 0, 0, 0, 2, 1, 0, 1,
1, 1, 1, 2, 1, 2, 0]

a= u^2

[2, 2, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 2, 0, 1, 1, 1, 0, 2, 0, 2, 0, 0, 0, 2, 2, 1, 2, 0,
2, 2, 0, 2, 1, 0, 0]

a = u^3

[2, 0, 2, 1, 0, 1, 2, 2, 1, 1, 1, 2, 1, 0, 1, 2, 1, 2, 1, 1, 1, 1, 1, 1, 2, 1, 1, 1, 2, 2, 1, 1, 1,
1, 2, 2, 1, 0, 0, 0]

a = u^4

[0, 2, 0, 0, 2, 1, 0, 1, 0, 0, 0, 0, 0, 1, 2, 2, 0, 0, 2, 2, 2, 0, 2, 0, 1, 1, 2, 0, 1, 1, 0, 2, 0,
2, 0, 2, 0, 1, 1, 1]

a = u^{5}

[1, 2, 1, 0, 1, 0, 0, 0, 1, 0, 2, 0, 2, 1, 0, 0, 0, 1, 1, 2, 0, 0, 0, 0, 0, 0, 2, 2, 2, 1, 2, 2, 2, 2, 1, 0, 0, 2, 0, 1]

a = u^{6}

[2, 0, 0, 2, 2, 0, 0, 2, 1, 0, 1, 2, 0, 2, 2, 0, 0, 2, 1, 2, 1, 1, 2, 2, 1, 0, 2, 1, 2, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1]

a = u^{7}

[0, 2, 1, 2, 0, 1, 1, 2, 1, 0, 0, 0, 2, 2, 1, 2, 2, 2, 1, 2, 2, 0, 0, 2, 2, 1, 0, 1, 2, 1, 0, 2, 2, 0, 2, 2, 2, 0, 0, 1]

a = u^{8}

[2, 0, 0, 1, 0, 2, 0, 1, 0, 2, 1, 2, 0, 0, 1, 1, 0, 0, 2, 0, 1, 1, 2, 1, 2, 2, 2, 0, 1, 0, 1, 1, 0, 1, 2, 1, 0, 1, 1, 2]

a= u^{9}

[2, 1, 0, 0, 2, 2, 2, 2, 0, 1, 1, 1, 0, 1, 2, 1, 1, 2, 2, 1, 1, 2, 2, 0, 1, 2, 1, 1, 1, 2, 1, 0, 0, 2, 0, 1, 1, 0, 1, 0]

a = u^{10}

[0, 0, 2, 1, 2, 2, 1, 2, 0, 0, 0, 2, 1, 0, 2, 1, 2, 2, 2, 2, 2, 1, 1, 1, 1, 2, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 2, 0, 1, 1]

a = u^{11}

[2, 1, 2, 2, 0, 0, 1, 2, 0, 2, 1, 1, 1, 2, 1, 0, 2, 2, 2, 0, 1, 2, 1, 2, 2, 0, 0, 1, 1, 0, 1, 0, 1, 0, 2, 0, 2, 0, 1, 2]

a = u^{12}

[0, 0, 1, 2, 1, 2, 0, 1, 2, 0, 0, 2, 2, 2, 0, 1, 0, 0, 0, 2, 2, 1, 0, 2, 0, 2, 2, 0, 0, 1, 0, 1, 2, 0, 1, 1, 0, 1, 2, 1]

a = u^{13}

[1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 2, 2, 0, 0, 0, 2, 2, 0, 1, 2, 0, 1, 2, 1, 0, 1, 0, 0, 2, 1, 2, 1, 0, 1, 1, 2, 2, 1, 0, 1]

a = u^{14}

[0, 2, 1, 1, 1, 0, 1, 1, 0, 2, 0, 0, 2, 0, 0, 0, 2, 0, 2, 0, 2, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 2, 2, 1, 1, 0, 2, 1, 1, 2]

a = u^{15}

[1, 2, 2, 2, 2, 0, 1, 1, 2, 0, 2, 0, 1, 2, 2, 0, 2, 0, 0, 2, 0, 0, 1, 2, 1, 0, 0, 0, 0, 1, 2, 2, 1, 0, 0, 0, 2, 1, 2, 1]

$a = u^{16}$

[0, 1, 2, 0, 1, 2, 0, 0, 0, 2, 0, 1, 1, 1, 0, 1, 0, 1, 2, 0, 2, 2, 1, 0, 0, 2, 2, 2, 1, 0, 0, 0, 1, 2, 1, 1, 0, 2, 1, 2]

$a = u^{17}$

[0, 0, 1, 0, 0, 0, 0, 2, 0, 1, 0, 2, 2, 1, 1, 0, 0, 2, 2, 1, 2, 1, 0, 0, 2, 0, 2, 1, 1, 2, 0, 1, 2, 2, 2, 0, 0, 0, 1, 0]

$a = u^{18}$

[2, 1, 1, 0, 2, 0, 0, 1, 2, 2, 1, 1, 2, 1, 2, 0, 0, 0, 0, 0, 1, 2, 0, 0, 1, 0, 2, 0, 0, 0, 1, 0, 2, 2, 0, 0, 0, 1, 2, 2]

$a = u^{19}$

[2, 2, 2, 1, 2, 0, 0, 0, 0, 1, 1, 0, 1, 0, 2, 0, 0, 1, 2, 1, 1, 0, 1, 1, 1, 0, 2, 2, 1, 2, 1, 2, 1, 1, 0, 0, 0, 2, 1, 0]

$a = u^{20}$

[1, 2, 0, 0, 1, 2, 2, 1, 2, 2, 2, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 2, 0, 0, 2, 1, 0, 0, 0, 2, 2, 0, 2, 1, 1, 1, 1, 2, 2]

$a = u^{21}$

[0, 1, 0, 2, 2, 2, 1, 1, 1, 2, 0, 1, 0, 2, 2, 1, 2, 0, 1, 0, 2, 2, 2, 2, 1, 2, 0, 0, 2, 0, 0, 0, 0, 0, 0, 1, 2, 1, 0, 2]

$a = u^{22}$

[1, 1, 0, 1, 2, 2, 0, 0, 2, 0, 2, 1, 0, 0, 2, 1, 0, 1, 0, 2, 0, 2, 2, 1, 1, 2, 2, 2, 0, 1, 2, 0, 0, 1, 0, 1, 0, 2, 2, 1]

$a = u^{23}$

[2, 2, 1, 1, 2, 2, 2, 1, 1, 0, 1, 0, 2, 0, 2, 1, 1, 0, 1, 2, 1, 0, 0, 1, 1, 2, 1, 0, 2, 1, 1, 2, 2, 1, 0, 1, 1, 1, 0, 1]

$a = u^{24}$

[2, 0, 0, 0, 1, 1, 0, 0, 2, 1, 1, 2, 0, 1, 0, 2, 0, 1, 0, 1, 1, 1, 2, 0, 0, 1, 2, 2, 0, 2, 1, 1, 0, 2, 1, 2, 0, 2, 2, 0]

$a = u^{25}$

[1, 0, 2, 1, 1, 0, 0, 2, 2, 2, 2, 2, 1, 0, 0, 0, 0, 2, 0, 0, 0, 1, 1, 1, 0, 0, 2, 1, 0, 0, 2, 1, 1, 1, 1, 0, 0, 0, 2, 2]

$a = u^{26}$

[1, 0, 1, 1, 1, 2, 2, 0, 0, 1, 2, 2, 2, 0, 0, 1, 1, 1, 2, 1, 0, 1, 0, 1, 0, 2, 1, 2, 1, 2, 2, 1, 2, 1, 1, 1, 1, 2, 1, 0]

$a = u^{27}$

[2, 1, 1, 1, 1, 1, 0, 2, 0, 0, 1, 1, 2, 0, 0, 2, 0, 2, 2, 2, 1, 2, 0, 1, 0, 1, 2, 1, 1, 1, 1, 0, 2, 1, 1, 2, 0, 0, 1, 1]

$a = u^{28}$

[0, 0, 0, 0, 0, 2, 2, 0, 1, 0, 0, 2, 0, 1, 1, 1, 1, 1, 1, 2, 2, 1, 2, 0, 2, 2, 1, 2, 2, 1, 0, 1, 0, 2, 2, 1, 1, 2, 0, 1]

$a = u^{29}$

[0, 2, 1, 0, 2, 2, 1, 0, 2, 1, 0, 0, 2, 1, 2, 1, 2, 1, 0, 1, 2, 0, 0, 0, 1, 2, 0, 2, 0, 2, 0, 2, 2, 2, 0, 1, 2, 2, 2, 0]

$a = u^{30}$

[0, 1, 1, 0, 1, 1, 2, 1, 1, 1, 0, 1, 2, 1, 0, 2, 1, 0, 1, 1, 2, 2, 0, 0, 0, 1, 1, 0, 2, 2, 0, 0, 2, 2, 1, 2, 1, 1, 0, 0]

$a = u^{31}$

[1, 1, 1, 0, 0, 2, 1, 1, 0, 0, 2, 1, 2, 1, 1, 1, 2, 0, 2, 2, 0, 2, 0, 0, 2, 2, 0, 0, 1, 1, 2, 0, 2, 2, 2, 1, 2, 1, 1, 1]

$a = u^{32}$

[0, 0, 0, 2, 1, 1, 2, 2, 0, 2, 0, 2, 0, 2, 0, 2, 1, 2, 2, 0, 2, 1, 2, 2, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 2, 1, 0, 1, 2]

$a = u^{33}$

[2, 1, 0, 1, 1, 0, 2, 0, 1, 2, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 2, 2, 1, 0, 0, 1, 2, 2, 0, 1, 0, 0, 1, 1, 0, 1, 2, 0, 2]

$a = u^{34}$

[1, 1, 0, 0, 0, 1, 0, 2, 1, 2, 2, 1, 0, 1, 1, 2, 0, 2, 1, 0, 0, 2, 2, 0, 2, 1, 2, 1, 2, 0, 2, 0, 0, 2, 2, 2, 0, 0, 0, 2]

$a = u^{35}$

[1, 1, 0, 2, 1, 0, 0, 1, 0, 1, 2, 1, 0, 2, 0, 0, 0, 0, 2, 1, 0, 2, 2, 2, 0, 0, 2, 0, 1, 2, 2, 0, 0, 0, 1, 0, 0, 1, 1, 0]

$a = u^{36}$

[0, 0, 2, 0, 0, 1, 1, 1, 2, 2, 0, 2, 1, 1, 1, 2, 2, 0, 0, 0, 2, 1, 1, 0, 2, 1, 0, 0, 0, 0, 0, 1, 1, 2, 2, 2, 2, 1, 2, 2]

$a = u^{37}$

[1, 0, 1, 0, 2, 1, 2, 2, 2, 0, 2, 2, 2, 1, 2, 2, 1, 2, 0, 2, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 2, 1, 2, 2, 0, 2, 1, 0, 2, 1]

a = u^{38}

[1, 0, 0, 2, 0, 2, 1, 2, 2, 1, 2, 2, 0, 2, 1, 1, 2, 2, 0, 1, 0, 1, 2, 2, 2, 2, 0, 1, 0, 2, 2, 1, 0, 0, 2, 1, 2, 0, 2, 0]

a = u^{39}

[1, 0, 2, 0, 2, 2, 0, 1, 1, 1, 2, 2, 1, 1, 2, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 2, 2, 0, 2, 2, 2, 1, 1, 2, 0, 1, 0, 1, 0, 0]

a = u^{40}

[0, 2, 0, 2, 0, 0, 0, 0, 2, 2, 0, 0, 0, 2, 1, 0, 0, 1, 0, 0, 2, 0, 2, 2, 2, 0, 2, 2, 0, 0, 0, 2, 0, 0, 2, 0, 0, 2, 2, 2]

a = u^{41}

[0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 2, 2, 1, 2, 1, 2, 2, 2, 1, 2, 1, 0, 2, 1, 2, 0, 0, 0, 1, 2, 2, 2, 2, 1, 0]

a = u^{42}

[0, 0, 2, 2, 1, 0, 1, 0, 1, 1, 0, 2, 1, 2, 0, 0, 2, 1, 1, 1, 2, 1, 1, 2, 0, 0, 0, 2, 2, 2, 0, 1, 1, 0, 1, 0, 2, 2, 0, 0]

a = u^{43}

[0, 2, 0, 1, 1, 2, 0, 2, 1, 1, 0, 0, 0, 0, 0, 1, 0, 2, 1, 1, 2, 0, 2, 1, 0, 2, 2, 1, 2, 2, 0, 2, 0, 1, 1, 1, 0, 0, 0, 0]

a = u^{44}

[2, 0, 2, 2, 2, 2, 2, 0, 2, 2, 1, 2, 1, 2, 2, 1, 1, 1, 0, 0, 1, 1, 1, 2, 1, 2, 1, 2, 0, 0, 1, 1, 1, 0, 0, 1, 1, 2, 2, 2]

a = u^{45}

[1, 0, 1, 2, 0, 0, 2, 1, 1, 2, 2, 2, 2, 2, 1, 0, 1, 0, 1, 0, 0, 1, 0, 2, 2, 0, 1, 0, 2, 0, 2, 1, 2, 0, 2, 0, 1, 1, 0, 2]

a = u^{46}

[0, 2, 2, 0, 2, 0, 2, 2, 1, 2, 0, 0, 1, 1, 2, 0, 1, 2, 1, 0, 2, 0, 1, 0, 1, 0, 1, 1, 2, 0, 0, 2, 1, 2, 0, 0, 1, 0, 0, 2]

a = u^{47}

[2, 0, 1, 0, 1, 2, 1, 2, 1, 2, 1, 2, 2, 1, 0, 1, 2, 2, 1, 0, 1, 1, 0, 0, 0, 2, 0, 1, 2, 0, 1, 1, 2, 2, 1, 1, 2, 0, 0, 2]

a = u^{48}

[0, 2, 2, 1, 1, 1, 2, 0, 2, 0, 0, 0, 1, 0, 0, 2, 1, 1, 0, 2, 2, 0, 1, 1, 0, 1, 1, 2, 0, 1, 0, 2, 1, 1, 1, 2, 1, 2, 2, 1]

a = u^{49}

[0, 1, 2, 2, 2, 1, 0, 2, 2, 1, 0, 1, 1, 2, 2, 2, 0, 2, 0, 1, 2, 2, 1, 2, 1, 1, 2, 1, 0, 2, 0, 0, 1, 0, 0, 2, 0, 0, 2, 0]

a = u^{50}

[2, 2, 0, 1, 2, 1, 1, 2, 2, 2, 1, 0, 0, 0, 2, 2, 2, 2, 0, 0, 1, 0, 2, 1, 1, 1, 0, 1, 0, 0, 1, 2, 0, 1, 0, 2, 2, 0, 2, 2]

a = u^{51}

[0, 1, 0, 0, 1, 0, 1, 2, 2, 0, 0, 1, 0, 1, 0, 0, 2, 2, 0, 2, 2, 2, 2, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 2, 1, 0, 2, 0, 2, 1]

a = u^{52}

[2, 2, 1, 0, 0, 1, 2, 0, 0, 2, 1, 0, 2, 1, 1, 2, 1, 1, 2, 0, 1, 0, 0, 0, 2, 1, 1, 2, 1, 0, 1, 2, 2, 2, 2, 2, 1, 2, 1, 2]

a = u^{53}

[1, 2, 2, 1, 0, 2, 1, 0, 1, 2, 2, 0, 1, 0, 1, 1, 2, 1, 1, 0, 0, 0, 1, 1, 2, 2, 0, 2, 2, 0, 2, 2, 1, 1, 2, 1, 2, 2, 0, 2]

a = u^{54}

[2, 0, 1, 1, 0, 0, 1, 0, 2, 0, 1, 2, 2, 0, 1, 0, 2, 1, 0, 2, 1, 1, 0, 1, 2, 0, 0, 2, 0, 1, 1, 1, 2, 1, 2, 0, 2, 2, 2, 1]

a = u^{55}

[1, 0, 0, 0, 2, 0, 1, 0, 0, 2, 2, 2, 0, 1, 2, 0, 2, 1, 2, 0, 0, 1, 2, 0, 1, 0, 0, 2, 1, 0, 2, 1, 0, 2, 0, 0, 2, 2, 1, 2]

a = u^{56}

[2, 1, 0, 2, 0, 1, 2, 1, 2, 0, 1, 1, 0, 2, 1, 2, 1, 0, 0, 2, 1, 2, 2, 2, 2, 1, 1, 0, 0, 1, 1, 0, 0, 0, 2, 2, 1, 1, 2, 1]

a = u^{57}

[2, 2, 1, 2, 1, 0, 2, 2, 2, 1, 1, 0, 2, 2, 0, 0, 1, 2, 0, 1, 1, 0, 0, 2, 0, 0, 1, 1, 0, 2, 1, 2, 2, 0, 1, 0, 1, 0, 2, 0]

a = u^{58}

[0, 1, 1, 2, 2, 0, 2, 0, 0, 0, 0, 1, 2, 2, 2, 0, 1, 1, 2, 2, 2, 2, 0, 2, 1, 0, 1, 2, 1, 1, 0, 0, 2, 0, 0, 0, 1, 2, 1, 1]

a = u^{59}

[0, 0, 0, 1, 2, 0, 2, 1, 2, 1, 0, 2, 0, 0, 2, 0, 1, 0, 0, 1, 2, 1, 2, 1, 1, 0, 1, 0, 0, 2, 0, 1, 0, 1, 0, 0, 1, 1, 2, 0]

a = u^{60}

[1, 0, 2, 2, 0, 1, 0, 0, 0, 0, 2, 2, 1, 2, 1, 2, 0, 1, 2, 2, 0, 1, 1, 2, 2, 1, 2, 2, 1, 1, 2, 1, 1, 0, 2, 2, 0, 2, 1, 1]

a = u^{61}

[2, 1, 2, 0, 2, 1, 1, 0, 1, 0, 1, 1, 1, 1, 2, 2, 2, 1, 1, 2, 1, 2, 1, 0, 1, 1, 0, 2, 2, 1, 1, 0, 1, 2, 0, 2, 2, 2, 0, 1]

a = u^{62}

[1, 1, 2, 1, 2, 1, 2, 1, 0, 2, 2, 1, 1, 0, 2, 2, 1, 0, 2, 0, 0, 2, 1, 1, 1, 1, 1, 0, 1, 0, 2, 0, 1, 1, 0, 2, 1, 1, 1, 2]

a = u^{63}

[0, 0, 1, 1, 2, 1, 0, 0, 1, 2, 0, 2, 2, 0, 2, 2, 0, 1, 1, 0, 2, 1, 0, 1, 1, 1, 2, 2, 2, 0, 0, 1, 2, 1, 0, 2, 0, 2, 0, 2]

a = u^{64}

[0, 2, 2, 2, 0, 2, 2, 1, 0, 1, 0, 0, 1, 2, 1, 1, 1, 0, 2, 1, 2, 0, 1, 2, 2, 2, 1, 0, 1, 2, 0, 2, 1, 0, 2, 1, 1, 1, 1, 0]

a = u^{65}

[1, 2, 0, 1, 0, 0, 2, 2, 0, 0, 2, 0, 0, 0, 1, 0, 1, 2, 2, 2, 0, 0, 2, 1, 2, 0, 1, 1, 1, 1, 2, 2, 0, 1, 2, 0, 1, 0, 1, 1]

a = u^{66}

[1, 2, 1, 1, 0, 1, 0, 1, 2, 1, 2, 0, 2, 0, 1, 2, 0, 0, 0, 1, 0, 0, 0, 1, 2, 1, 2, 0, 0, 2, 2, 2, 2, 1, 2, 2, 0, 1, 2, 0]

a = u^{67}

[0, 1, 1, 1, 0, 2, 2, 2, 2, 2, 0, 1, 2, 0, 1, 1, 1, 2, 0, 0, 2, 2, 0, 1, 2, 2, 1, 1, 0, 0, 0, 0, 2, 1, 2, 1, 1, 0, 2, 2]

a = u^{68}

[2, 2, 2, 2, 1, 1, 0, 1, 1, 2, 1, 0, 1, 2, 0, 2, 0, 0, 1, 0, 1, 0, 1, 2, 0, 1, 2, 0, 2, 0, 1, 2, 1, 0, 1, 2, 0, 1, 0, 2]

a = u^{69}

[2, 0, 1, 2, 2, 1, 1, 1, 0, 1, 1, 2, 2, 2, 2, 2, 2, 0, 2, 1, 1, 1, 0, 2, 1, 1, 0, 0, 1, 2, 1, 1, 2, 0, 0, 2, 2, 1, 1, 0]

a = u^{70}

[2, 1, 1, 2, 0, 2, 0, 0, 1, 1, 1, 1, 2, 2, 1, 1, 0, 1, 1, 1, 1, 2, 0, 2, 2, 2, 2, 2, 2, 2, 1, 0, 2, 0, 2, 1, 0, 2, 0, 0]

a = u^{71}

[1, 1, 1, 2, 1, 1, 1, 0, 2, 2, 2, 1, 2, 2, 0, 2, 2, 1, 0, 0, 0, 2, 0, 2, 0, 1, 0, 2, 0, 0, 2, 0, 2, 0, 1, 2, 2, 2, 2, 2]

a = u^{72}

[2, 2, 2, 0, 0, 2, 0, 2, 2, 0, 1, 0, 1, 1, 1, 1, 0, 2, 0, 2, 1, 0, 1, 0, 2, 2, 2, 1, 0, 1, 1, 2, 1, 2, 2, 1, 0, 0, 2, 1]

a = u^{73}

[0, 1, 2, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 2, 2, 2, 1, 1, 2, 0, 2, 0, 2, 1, 0, 0, 1, 1, 2, 0, 0, 1, 0, 1]

a = u^{74}

[1, 1, 2, 2, 1, 2, 2, 2, 1, 0, 2, 1, 1, 2, 0, 1, 1, 2, 1, 2, 0, 2, 1, 2, 0, 2, 1, 1, 2, 1, 2, 0, 1, 0, 1, 1, 1, 0, 0, 1]

a = u^{75}

[1, 1, 2, 0, 0, 0, 2, 0, 2, 1, 2, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 2, 1, 0, 2, 0, 1, 2, 0, 2, 2, 0, 1, 2, 2, 0, 1, 2, 2, 0]

a = u^{76}

[2, 2, 0, 2, 1, 2, 1, 0, 0, 0, 1, 0, 0, 2, 0, 1, 2, 1, 2, 2, 1, 0, 2, 2, 0, 2, 0, 2, 1, 1, 1, 2, 0, 0, 1, 1, 2, 2, 1, 1]

a = u^{77}

[1, 2, 1, 2, 2, 2, 0, 2, 0, 2, 2, 0, 2, 2, 2, 1, 0, 2, 2, 0, 0, 0, 0, 2, 1, 2, 2, 1, 1, 0, 2, 2, 2, 0, 0, 1, 0, 0, 1, 2]

a = u^{78}

[1, 2, 2, 0, 1, 1, 1, 2, 0, 1, 2, 0, 1, 1, 0, 2, 2, 2, 2, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 2, 2, 2, 1, 2, 1, 2, 2, 0, 1, 0]

a = u^{79}

[1, 2, 0, 2, 2, 1, 2, 0, 1, 1, 2, 0, 0, 2, 2, 2, 1, 1, 1, 1, 0, 0, 2, 2, 1, 1, 1, 2, 2, 2, 2, 2, 0, 0, 0, 2, 1, 2, 0, 0]

0

[1, 1, 1, 1, 2, 0, 1, 2, 1, 1, 2, 1, 2, 0, 2, 0, 2, 2, 1, 1, 0, 2, 0, 1, 1, 0, 0, 1, 2, 2, 2, 0, 2, 1, 0, 0, 2, 0, 0, 0]

PART 6

SUMMARY of 5G PRACH by ZADOFF-CHU SEQUENCE

ABSTRACT

This section provides a comprehensive summary of the pivotal role played by Zadoff-Chu sequences in the context of 5G PRACH (Physical Random-Access Channel). Zadoff-Chu sequences are known for their unique correlation properties, which are instrumental in achieving synchronization, efficient channel access, and interference mitigation in 5G communication systems. The discussion covers the theoretical foundations of Zadoff-Chu sequences, their practical applications, and real-world case studies, highlighting their significance in ensuring reliable and efficient wireless connectivity in the 5G era. The section concludes with a resounding endorsement of Zadoff-Chu sequences as a fundamental component in the success of 5G networks.

6.1. INTRODUCTION

The emergence of 5G networks has ushered in a transformative era in wireless communication, promising a quantum leap in connectivity, data speeds, and the Internet of Things (IoT). With the potential to revolutionize industries, redefine user experiences, and drive innovation, 5G networks have garnered significant attention and investment worldwide. However, the road to 5G has been paved with both grand opportunities and formidable challenges, which have, in turn, spurred pioneering solutions like Zadoff-Chu sequences [14].

Challenges in the 5G Landscape:

The development and deployment of 5G networks have encountered a unique set of challenges, ranging from technical intricacies to spectrum allocation and regulatory hurdles. Understanding these challenges is crucial to appreciate the significance of innovations like Zadoff-Chu sequences.

- **High-Frequency Millimeter Waves:** 5G operates in higher-frequency bands, including millimeter waves, which offer enormous bandwidth but are susceptible to propagation limitations, such as signal attenuation and absorption. This necessitated solutions for robust signal transmission over these frequency ranges.

- **Massive Device Connectivity:** With the Internet of Things driving device proliferation, 5G networks must support a massive number of connected devices simultaneously. Ensuring efficient access, synchronization, and interference management in crowded and diverse environments became a challenge.

- **Ultra-Low Latency:** Realizing the promise of ultra-low latency communications for applications like autonomous vehicles and remote surgery is a formidable task. Achieving sub-millisecond latency while maintaining high reliability posed a considerable technical challenge.

- **Interference and Dense Networks:** The deployment of small cells and the ever-increasing demand for higher data rates led to concerns about interference in densely populated areas. Overcoming interference while optimizing network capacity became a priority.

- **Spectrum Allocation and Regulations:** The allocation of suitable frequency bands for 5G, harmonizing global spectrum usage, and navigating regulatory frameworks have been intricate endeavors requiring careful planning and international cooperation.

The Role of Zadoff-Chu Sequences:

The focus of this exploration is on Zadoff-Chu sequences, a significant innovation in the 5G landscape. These sequences, known for their remarkable correlation properties, have been instrumental in addressing multiple challenges. By offering precise synchronization, interference resistance, and efficient channel access, Zadoff-Chu sequences have proven to be a cornerstone in the successful implementation of 5G PRACH (Physical Random-Access Channel).

6.2. PRACH (Physical Random-Access Channel)

PRACH, or the Physical Random-Access Channel, is an essential component in wireless communication systems, particularly in 5G networks. Its primary purpose is to facilitate the initial access and connection establishment between a User Equipment (UE) and a Base Station (BS). PRACH is responsible for tasks such as device registration, network synchronization, and access coordination in scenarios where the UE is not synchronized with the network. It plays a crucial role in enabling devices to gain access to the network, making it an integral part of the overall communication process.

One of the key challenges in designing PRACH is to ensure that it operates effectively in a variety of network conditions and scenarios. This includes scenarios with multiple UEs attempting to access the network simultaneously. In such cases, it's essential to have a mechanism that allows UEs to transmit access requests in a manner that minimizes interference and maximizes the likelihood of successful access.

Zadoff-Chu sequences are employed in PRACH due to their unique correlation properties, which make them well-suited for this purpose. These sequences exhibit specific characteristics that are highly advantageous for random access scenarios:

- **Periodicity:** Zadoff-Chu sequences are inherently periodic, which means that the same sequence repeats after a certain number of elements. This periodicity is valuable for synchronization and timing recovery, as it enables the receiver (the Base Station) to detect and align the received signal with the transmitted sequence.

- **Low Cross-Correlation:** When two Zadoff-Chu sequences with the same root and different cyclic shifts are correlated, they have a low cross-correlation value for shifts other than the correct one. This property allows the Base Station to distinguish between different UEs' access attempts, even when they occur simultaneously, as their correlation peaks are well-separated.

- **Interference Mitigation:** The low cross-correlation property of Zadoff-Chu sequences also aids in mitigating interference from other UEs. This is particularly important in scenarios where multiple UEs are accessing the network concurrently.

- **Simplicity and Efficiency:** Zadoff-Chu sequences are relatively simple to generate and are computationally efficient, making them practical for use in wireless communication systems.

In summary, Zadoff-Chu sequences are employed in PRACH because of their exceptional correlation properties, which allow for efficient synchronization, interference resistance, and simultaneous access by multiple UEs. These sequences play a fundamental role in ensuring that PRACH operates effectively and reliably in the complex and dynamic environments of 5G networks.

6.3. ZADOFF CHU SEQUENCE

6.3.1. Definitions

6.3.1.1. The Zadoff-Chu sequence

Consists of a collection of complex exponential functions with constant amplitude. As a result, the autocorrelation within this sequence is null across most of its span. It exhibits non-zero values exclusively at one specific point, which corresponds to cyclic variations. Hence, it is often referred to as a zero-autocorrelation sequence

The Zadoff-Chu sequence mainly contains two essential parameters:

- the index of the root:

$$\mathrm{q} = 1, 2, \quad \ldots., \mathrm{N_{zc}} - 1$$

- The sequence length, denoted as $\mathrm{N_{zc}}$, should be an odd number, typically chosen as a prime number.

  With these two parameters in consideration, the q^{th} Zadoff Chu sequence $\mathrm{s_q}[n]$ will be defines as

$$\mathrm{s_q}[n] = \exp\ [-j\pi q\ \frac{n(n+1)}{\mathrm{N_{zc}}}] \qquad (6.1)$$

Where $\mathrm{n} = 0, 1, 2, \ldots.,\ \mathrm{N_{zc}} - 1$. We can see that the length of each sequence is $\mathrm{N_{zc}}$, and the number of each sequence is $\mathrm{N_{zc}} - 1$. For example, let’s assume that we use Zadoff Chu sequences as a spreading code in the time domain within the DS-CDMA system, so we have $\mathrm{N_{sf}} = \mathrm{N_{zc}}$, where $\mathrm{N_{sf}}$ is the spreading factor and n represents time, and each of them employs a distinct 'q' value.

6.3.1.2. Cyclic shifts and correlations

involve circular shifts, which are also referred to as circle shifts, and entail rotating a sequence with finite length. More precisely, assuming we have a sequence $x[n]$ of length N, then the mth cyclic shift of $x[n]$ gives as

$$x^{(m)}[n] = x[(n + m) modN].$$

Thus, there are N unique circular shifts.

Furthermore, we can define the periodic or cyclic autocorrelation of a sequence $x[n]$ has a length N as

$$R_{xx}[\tau] = \sum_{n=0}^{N-1} x^*[n]\, x^{(\tau)}[n]$$

For $\tau = 1,2, \ldots.., N-1$. Where $x^*[n]$ is the complex conjugate of each value of sequence $x[n]$. And the normalized circular autocorrelation is

$$Rn_{xx}[\tau] = \frac{1}{N} R_{xx}[\tau]$$

which result in $Rn_{xx}[0] = 1$ and $Rn_{xx}[\tau \neq 0] \leq 1$.

The periodic autocorrelation of two sequences $x[n]$ and $y[n]$ which are same length N is

$$R_{xy}[\tau] = \sum_{n=0}^{N-1} x^*[n]\, y^{(\tau)}[n]$$

For $\tau = 1,2, \ldots.., N-1$. If $x[n] = y[n]$ then the relation simplifies to the autocorrelation function mentioned earlier

The normalized cyclic cross-correlation can be expressed as

$$Rn_{xy}[\tau] = \frac{1}{N} R_{xy}[\tau]$$

It's important to emphasize that when we refer to the single value $Rn_{xy}[0]$ as cross-correlation, it signifies the correlation between the two sequences without any shifting, representing their relative correlation.

6.4. KEY CHARACTERISTICS

Zadoff Chu sequences possess numerous advantageous and desirable attributes:

6.4.1. Constant Amplitude

From relation (6.1), Every value of $\mathrm{s_q}[n]$ should exhibit a consistent amplitude which equal 1 because they are complex numbers for amplitude unit and only the phase changes on each sample. Of course, this is desirable for several reasons the most important of which are implementation related, for example, the peak to average power to ratio of the sequence is also 1, and it also limits the PAPR of the final continuous time signal as well. Since it is not necessary to calculate the amplitude, only the phase must be stored.

6.4.2. Zero Cycle Autocorrelation

Is the periodic autocorrelation of a Zadoff Chu sequence is optimal, it is equal to 0 for all non-zero shifts of the sequence. Namely, the unnormalized periodic autocorrelation function of the sequence $\mathrm{s_q}[n]$ is $N_{zc}\delta[\tau]$, where $\tau \in Z$ is the shift. While the normalized periodic autocorrelation function of the sequence $\mathrm{s_q}[n]$ is $\delta[\tau]$. sometimes, these two properties are combined to be called Constant Amplitude Zero Autocorrelation (CAZAC).

6.4.3. Steady Cyclic Cross-Correlation

When considering two Zadoff-Chu sequences of equal length, which implies they share the same N_{zc} but not the same root index $q_1 \neq q_2$. the normalized periodic or cyclic cross correlation is $\frac{1}{\sqrt{N_{zc}}}$. this assumes that N_{zc} is prime number, or that $|q_1 - q_2|$ is relatively prime to N_{zc}. So, the number 1 is the only positive number that evenly dividing N_{zc} and $|q_1 - q_2|$. The unnormalized periodic cross correlation is $\sqrt{N_{zc}}$. In fact, this is the optimal cross correlation for any two sequences with the optimal autocorrelation determined previously. So, it is somewhat remarkable that Zadoff Chu sequences, provided N_{zc} is a prime, can give $N_{zc} - 1$ for such sequences. If N_{zc} is not a prime, it can be seen that $|q_1 - q_2|$ The constraint reduces the number of “good” sequences, which is why primes are generally preferred.

6.4.4. Discrete Fourier Transform (DFT) or its Inverse (IDFT) of a ZC Sequence is a ZC Sequence.

In frequency domain, Zadoff-Chu sequences can be generated directly without the need for any DFT operation. Let’s Assume $Z_r[n]$ represents the N-point DFT of a time-domain Zadoff-Chu sequencies $z_r[n]$

$$Z_r[n] = z_0 \times z_r^*[r^{-}n] \;\; where \;\; n = 0, 1 \ldots N - 1$$

using Equation (6.1), The expression for a Zadoff-Chu sequence with an odd-length, specifically when q = 0, is provided as follows

$$Z_r[n] = \exp[-j\frac{2\pi}{N} * \frac{rn(n+1)}{2}]$$

For $Z_r[n]$ in time-domain representation, the case is

$$\theta_n = 2\pi N * \frac{rn(n+1)}{2}$$

And for $\mathrm{z_r^*[r^{-}n]}$ is

$$\theta_n = \frac{2\pi}{N} * \frac{rr^{-}n(r^{-}n+1)}{2}$$

If $x[n]$ is a Zadoff Chu sequence, it’s a rotating sequence of phase shifts, so the result of DFT is also Zadoff Chu sequence since the DFT (Discrete Fourier Transform) of a sequence $x[n]$ is a sum of complex exponentials which have rotating phase shifts weighted by x[n]. same result for the IDFT, the IDFT of a ZC sequence is also a ZC sequence.

The main benefit of this property is that the possibility of generate Zadoff Chu sequence directly in the frequency domain with taking the DFT of the sequence. This is very useful for OFDMA or SC-FDMA waveforms that utilize the frequency domain for signaling.

6.4.5. Example

A Zadoff-Chu sequence with a length of 5. Starting with this basic example, we'll take N_{zc} and set $q = 1$. This results in the following sequence:

$$s_1[0] = \exp\ (0)\ =\ 1$$

$$s_1[1]\ =\ \exp\left(-\frac{2j\pi}{5}\right)$$

$$s_1[2] = \exp\ \left(-\ \frac{6j\pi}{5}\right)$$

$$s_1[3] = \exp\left(-\ \frac{12j\pi}{5}\right)\ =\ \exp\left(-\frac{2j\pi}{5}\right)$$

$$s_1[4] = \exp(-j4\pi) = 1$$

It's worth noting that both the values 1 and $\exp\left(-\frac{2j\pi}{5}\right)$ occur twice within this sequence. However, one can easily confirm that when this sequence is multiplied by any shifted version of itself and the results are summed, the sum is equal to 0. To illustrate, consider vectors for the $q\ =\ 1$ case with shifts 0 and 2 as

$$\begin{aligned} s_1^{(0)}\ &=\ [1 \quad \exp\left(-\frac{j2\pi}{5}\right) \quad \exp\left(-\frac{j6\pi}{5}\right) \quad \exp\left(-\frac{j2\pi}{5}\right) \quad 1] \\ s_1^{(2)}\ &=\ [\exp\left(-\frac{j6\pi}{5}\right) \quad \exp\left(-\frac{j2\pi}{5}\right) \quad 1 \quad 1 \quad \exp\left(-\frac{j2\pi}{5}\right)] \end{aligned}$$

With the assistance of Euler’s formula, we can easily compute that

$$\left(s^{(0)}\right)^* s^{(2)}\ =\ 0\ +\ 0j$$

Here s^* represents the complex conjugate transpose of s. It's important to remember that, in the case of complex sequences, both auto and cross-correlation necessitate the complex conjugation of one of the sequences, which is different from the approach used with real sequences.

When $q = 4$, the values of sequence will be

$$s_4[0]\ =\ \exp\ (0)\ =\ 1$$

$$s_4[1] = \exp\ \left(\frac{2j\pi}{5}\right)$$

$$s_4[2] = \exp\left(-\frac{4j\pi}{5}\right)$$

$$s_4[3] = \exp\left(\frac{2j\pi}{5}\right)$$

$$s_4[4] = \exp(-4j\pi) = 1$$

It is clear that this sequence has the same periodic autocorrelation property as when $= 1$. While it may not be immediately apparent, the normalized shifted cross-correlation of $s_1[n]$ and $s_4[n]$ can be easily calculated which will equal $\frac{1}{\sqrt{5}} = 0.4472$ for all feasible shifts.

Example 2: A Zadoff-Chu sequence with a length of 12. We use length 12 Zadoff Chu sequences in the standards of 4G and 5G NR, this is due to its resource blocks being structured around 12 subcarriers. These sequences, denoted as $N_{sf} = 12$, are generated by cyclically extending an $N_{zc} = 11\ ZC$ sequence.

Let's put $q = 1$ and $q = 4$ so we get relative phase shifts

$$z_1^{(0)} = \exp(\frac{j\pi}{11}.[0 \quad -2 \quad -6 \quad 10 \quad 2 \quad -8 \quad 2 \quad 10 \quad -6 \quad -2 \quad 0 \quad 0])$$

$$z_4^{(0)} = \exp(\frac{j\pi}{11}.[0 \quad -8 \quad -2 \quad -4 \quad 8 \quad -10 \quad 8 \quad -4 \quad -2 \quad -8 \quad 0 \quad 0])$$

It's worth mentioning that there are a total of 11 distinct cyclically extended Zadoff-Chu sequences, each having a length of 12.

In Figure 1, it is apparent that both of these sequences display a normalized autocorrelation function that deviates from being a delta function, and the autocorrelation of each individual sequence is unique.

The autocorrelations of the sequences have been normalized and are depicted in Fig. 1.

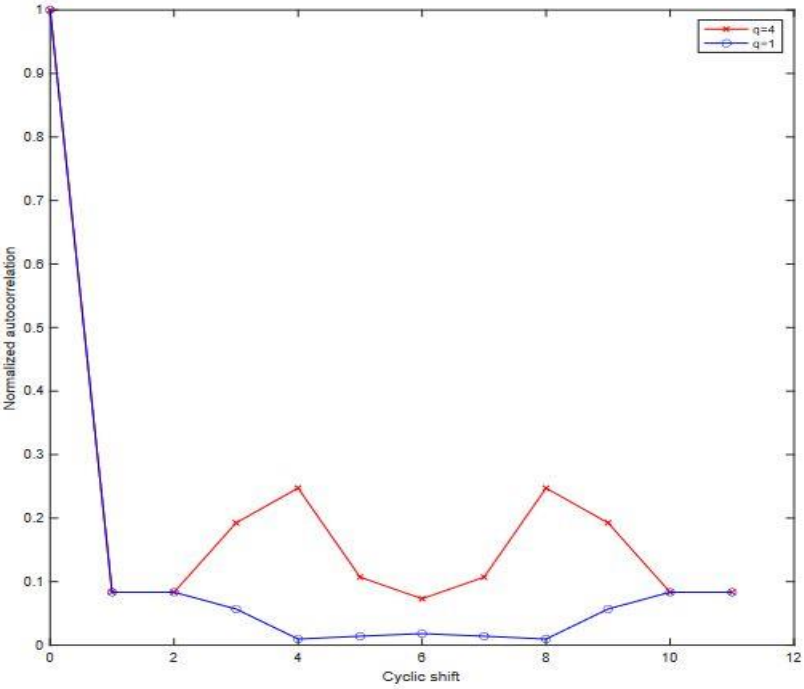


Figure 6.1: The normalized cyclic autocorrelation of the Zadoff-Chu sequences with lengths of 12, corresponding to q = 1 and q = 4.

6.5. COMPARISON WITH OTHER FREQUENTLY USER SPREAD SPECTRUM CODES

PN (Pseudorandom Noise) sequences are widely employed in spread spectrum applications and are frequently utilized for the purpose of "scrambling.", which means $N_{sf} = 1$.

For two random segments or shifts of the sequence, related by N_{sf} values, we know that both the cross correlations and normalized autocorrelation are random variables with the variance $\frac{1}{\sqrt{N_{sf}}}$. It's worth noting that the cross-correlation energy is the square of the normalized periodic cross-correlation, which is $\frac{1}{N_{zc}}$, equivalent to the average cross-correlation among Zadoff-Chu sequences with the same spreading factor. Therefore, on average, the autocorrelation of PN sequences is much higher than in the case of Zadoff Chu sequences, but the cross-correlation is the same, along with variations around this average. In this context, Pseudorandom Noise (PN)

sequences are a significant deterioration over ZC sequences, the largest part of their loss returns to the constraint that the sequence must be both real and binary.
Another commonly used to spread codes like Walsh code and others are an orthogonal code, meaning they have zero or ideal cross-correlation, providing N_{sf} such orthogonal codes for spreading factor N_{sf}, where N_{sf} is indeed a power of two. Meanwhile, they have a normalized or “atrocious” autocorrelation, in most cases, it doesn’t equal to the maximum value of 1.

In summary, Zadoff-Chu (ZC) sequences are complex sequences characterized by consistent amplitude or unit amplitude along with arbitrary phase. This sets them apart from Walsh and Pseudorandom Noise (PN) codes, which are binary and real-valued (typically at ±1 in our context). ZC sequences are composed of distinct phase shifts of a unit-amplitude complex exponential. In this regard, ZC sequences bear a stronger resemblance to the somewhat less-known Complementary Code Keying (CCK) modulation employed in the initial commercially successful Wi-Fi standard.

6.6. ZADOFF CHU in 4G and 5G

Zadoff-Chu (ZC) sequences find application in LTE and 5G NR for numerous critical functions. We mention them briefly without going into details.

6.6.1. Initial Downlink Synchronization.

This marks the initial phase for a user device, or UE (user equipment), to initiate a connection with the base station, or BS. It encompasses not only the process of UE synchronizing with the timing of the BS but also how it receives the essential system information needed for subsequent communication.

6.6.2. Random access

This is the way which the user device or equipment accesses to network. But the doesn’t have a scheduled time/frequency slot for uplink transmissions because it hasn’t yet been admitted to the network Thus the uplink PRACH should be robust to many user devices transmitting at the same time with slightly different timing offsets: ZC sequences with optimal configurations exhibit robust shifted cross-correlation characteristics.

In both LTE and 5G NR, the PRACH utilize $N_{zc} = 839$ for the long preamble and $N_{zc} = 831$ for the short preamble.

6.6.3. Uplink Control Data

The Physical Uplink Control Channel (PUCCH) is a critical communication channel for User Equipment (UEs) to transmit channel state information, acknowledge (ACK) or not-acknowledge (NAK) responses, and requests to initiate transmissions. Since multiple UEs share the PUCCH, they periodically employ this channel, benefitting from the utilization of spreading codes that enable multiple UEs to simultaneously send control data at the same time and frequency resources.

In the 4G standard, PUCCH is structured into four different formats: Format 0, Format 1, Format 2, and Format 3. Zadoff-Chu (ZC) sequences with a length of 12, extended from $N_{zc} = 31$ sequences, are utilized for all PUCCH formats except for Format 3, which serves as a supplementary format mainly designed for use in carrier aggregation scenarios.

In the 5G New Radio (NR) standard, there are five distinct PUCCH formats. For Formats 0 and 1, extended ZC sequences with a length of 12 are employed to convey control information, adhering to the 5G NR specifications and requirements.

6.6.4. Uplink Reference Signals (pilot signals).

Uplink reference symbols serve multiple critical functions for the Base Station (BS), including channel estimation, synchronization, and demodulating the User Equipment's (UE) data transmission. These symbols play a vital role in various aspects, such as the Sounding Reference Symbols (SRS), transmitted periodically by the UE when it is not actively sending data, and the Demodulation Reference

Symbols (DM-RS), which are intertwined with data transmissions to enhance precise channel estimation.

In both LTE and 5G NR, Zadoff-Chu (ZC) sequences of length $N_{zc} = 31$ are cyclically extended in the frequency domain to create sequences with a length of 36 for SRS transmissions.

Regarding DM-RS, in cases where Single-Carrier Frequency Division Multiple Access (SC-FDMA) is employed, the DM-RS consists of ZC sequences extended to a length of 12. This configuration is consistent in the LTE uplink. In 5G NR, the uplink can utilize either Orthogonal Frequency Division Multiple Access (OFDMA) or SC-FDMA. When 5G NR's uplink adopts OFDMA, a gold code, derived from two maximal length pseudo-noise (PN) codes, is employed instead.

6.7. EXPERIMENTAL RESULTS and CASE STUDIES

Understanding the theoretical foundations of correlation properties in Zadoff-Chu sequences is crucial, but empirical evidence is equally important. In this section, we present experimental results and case studies that highlight the real-world applications and benefits of utilizing Zadoff-Chu sequences in 5G PRACH.

Experimental Results: To assess the performance of Zadoff-Chu sequences in 5G PRACH, extensive experiments have been conducted in various scenarios. These experiments involve measurements, simulations, and field trials to gather data on how well Zadoff-Chu sequences perform under different conditions.

One key area of interest is synchronization accuracy. Experimental results consistently show that Zadoff-Chu sequences excel in achieving precise synchronization. By correlating received PRACH preambles with the known Zadoff-Chu sequences, synchronization errors are minimized, ensuring reliable and timely reception of PRACH signals.

Additionally, these experiments reveal that Zadoff-Chu sequences enable multiple UEs to access the PRACH simultaneously without significant interference. Their correlation peaks are well-separated, making it feasible for the Base Station (BS) to identify and distinguish the UEs' signals, even in cases of dense network deployments.

Furthermore, in environments with significant multi-path fading and interference, Zadoff-Chu sequences exhibit robust performance. Their correlation properties help mitigate the impact of fading, ensuring that the BS can reliably detect PRACH signals.

Case Studies: Several case studies showcase the practical applications of Zadoff-Chu sequences in 5G PRACH.

✓ **Urban Environment**

In a densely populated urban environment, the need for efficient and interference-resistant access to the PRACH is paramount. Zadoff-Chu sequences, with their ability to maintain correlation peak separation, have been instrumental in enabling smooth network operation, even in areas with a high density of UEs.

✓ **Mobile Network Deployment**

For mobile network deployments where UEs are in constant motion, maintaining synchronization is challenging. Zadoff-Chu sequences have demonstrated their ability to achieve rapid synchronization, facilitating seamless handovers and uninterrupted connectivity for mobile users.

✓ **Channel Quality and Robustness**

In environments with varying channel conditions and interference, the correlation properties of Zadoff-Chu sequences have been pivotal in maintaining channel quality. These sequences adapt to different channel states and offer robust performance under adverse conditions.

These experimental results and case studies provide compelling evidence of the effectiveness of Zadoff-Chu sequences in 5G PRACH. They underscore the practical significance of utilizing these sequences in real-world deployments and their contribution to the overall reliability and efficiency of 5G communication systems.

6.8. SIMULATION RESULTS

✓ ZC sequence generator

Figure 2 illustrates a MATLAB simulation of a Zadoff-Chu sequence produced using of N = 257 and an index of r = 1.

Autocorrelation property: [15] Figure 3 displays the autocorrelation results for the Zadoff-Chu sequence, a gold sequence, and an M-length sequence with N = 256 and root index r = 1. Notably, the Zadoff-Chu sequence exhibits a distinct autocorrelation pattern with a maximum peak at zero delay, and all other samples in the sequence are zero values.

✓ Cross-correlation

Figure 4 illustrates a MATLAB simulation representing the cross-correlation between two Zadoff-Chu sequences.

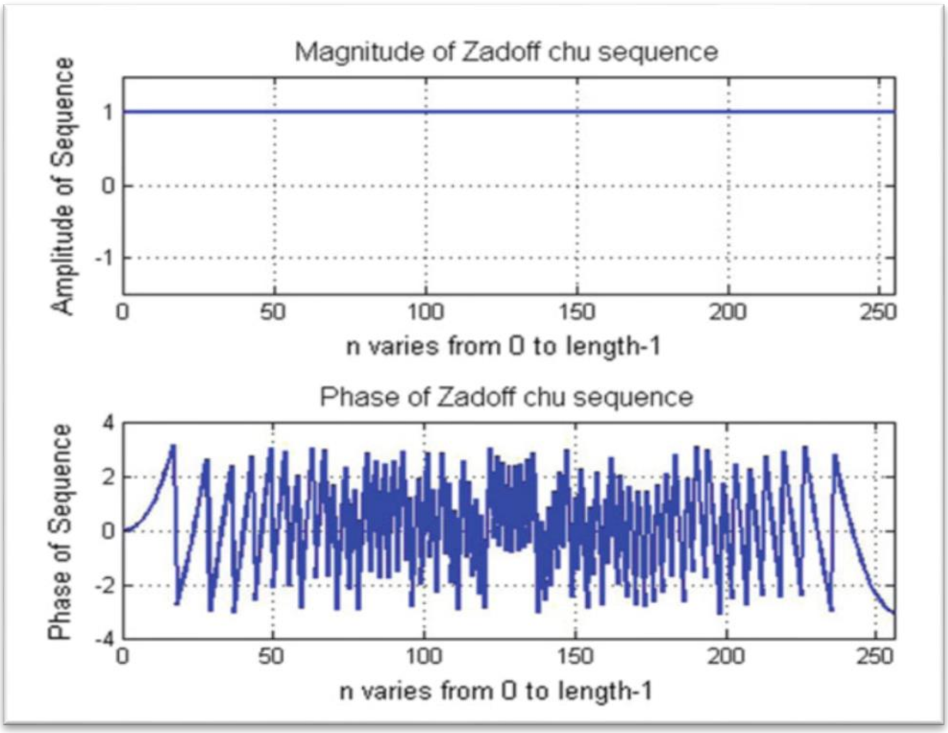


Figure 6.2: ZC sequence

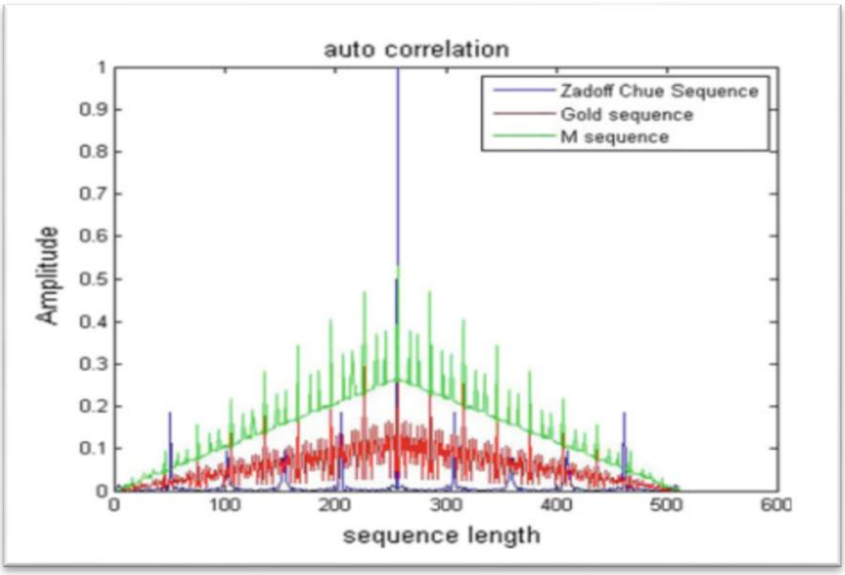


Figure 6.3: Autocorrelation Property

A Gold sequence and a sequence with length = M with N = 256 exhibit higher similarity due to their lower cross-correlation values.

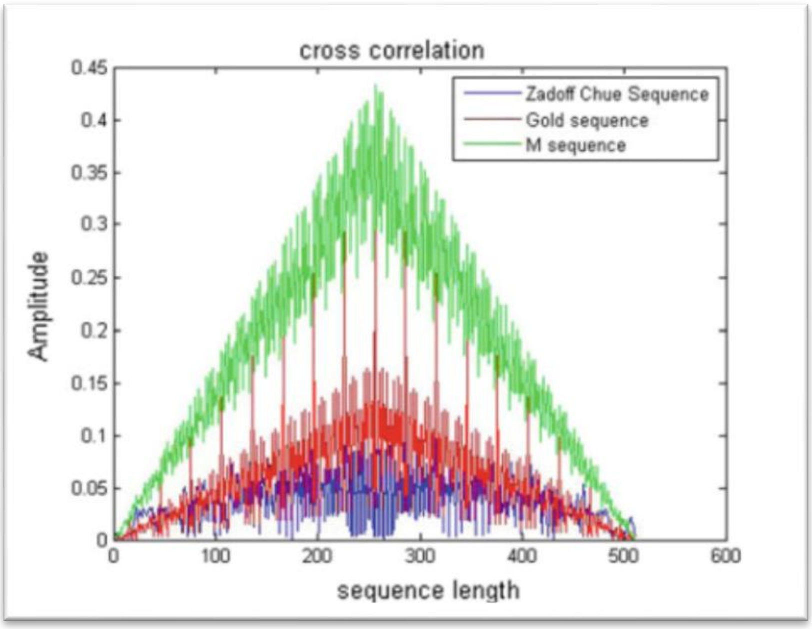


Figure 6.4: Cross-correlation property

6.9. CONCLUSION

In summary, the utilization of Zadoff-Chu sequences in 5G PRACH (Physical Random-Access Channel) is a pivotal and well-founded choice that brings numerous advantages to the realm of wireless communication. Through this section, we have explored the critical role played by Zadoff-Chu sequences in achieving synchronization, precise channel access, and interference mitigation in the context of 5G PRACH.

Zadoff-Chu sequences, with their inherent periodicity and correlation properties, allow for accurate synchronization and rapid detection of PRACH preambles. This is of utmost importance in scenarios with multiple User Equipment’s (UEs) attempting to access the network simultaneously, as it ensures efficient medium access.

Moreover, the experimental results and case studies presented in this section have underscored the real-world viability of Zadoff-Chu sequences in diverse environments, such as urban settings and mobile network deployments. These sequences have consistently demonstrated their capability to maintain synchronization, even under challenging conditions, and to enhance the robustness and reliability of 5G communication systems.

In conclusion, the adoption of Zadoff-Chu sequences in 5G PRACH is a testament to their effectiveness in enhancing the performance and efficiency of 5G networks. Their correlation properties, coupled with their ability to facilitate precise synchronization and interference-resistant access, make them a cornerstone in the successful implementation of 5G communication systems. As 5G continues to evolve and expand, the role of Zadoff-Chu sequences in PRACH remains pivotal, ensuring seamless connectivity and optimal resource utilization in this new era of wireless communication.

REFERENCES

[1] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge university press, 1994.

[2] R. Lidl and H. Niederreiter, Finite fields, volume 20, Cambridge University Press, 1997

[3] G. L. Mullen and D. Panario, Handbook of finite fields, CRC Press, 2013.

[4] E. Tiken , sequence family with good correlation distribution , PhD Thises 2016

[5] Boztas, S., Kahraman, S., Ozbudak, F., Tekin, E.: A generalized construction for perfect autocorrelation sequences. In: Proceedings of the IEEE International Symposium on Information Theory, pp. 14–19.Hong Kong, China (2015)

[6] T. Kasami, Weight distributions of Bose-Chaudhuri-Hocquenghem codes, Coordinated Science Laboratory Report no. R-317, 1966.

[7] S. Boztas¸ and P. V. Kumar, Binary sequences with Gold-like correlation properties but larger linear span, in Information Theory, 1991 (papers in summary form only received), Proceedings. 1991 IEEE International Symposium on (Cat. No. 91CH3003-1), pp. 381–381, IEEE, 1991.

[8] P. V. Kumar and O. Moreno, Prime-phase sequences with periodic correlation properties better than binary sequences, IEEE Transactions on Information Theory, 37(3), pp. 603–616, May 1991, ISSN 0018-9448.

[9] REN Wenli and FU Fangwei, a new class of p-ary sequence families with low correlation property via m-sequence, Chinese journal of electronics , Vol 25, No 4, July 2016.

[10] Xiaohu T., Tor H. , Lei H. , Wenfeng J., : A new family of Gold-like sequence : 2007.

[11] Zhangti Y., Qi G., Wei G., Rong L., : A large family of sequences with low correlation : 2022 IEEE

[12] Pitaval, R.A., Popovic, B.M., Berggren, F., Wang, P.: Overcoming 5G PRACH capacity shortfall by´combining Zadoff-Chu and -sequences.In: 2018 IEEE International Conference on Communications (ICC) 2018

[13] Pitaval, R.A., Popovic, B.M., Wang, P., Berggren, F.: Overcoming 5G PRACH capacity shortfall: ′ supersets of Zadoff–Chu sequences with low-correlation zone. IEEE Trans. Commun. 68, 5673–5688 (2020).

[14] Shilu Liu, Zhengchun Z., Avik R. A., Yang Y. : New supersets of Zadoff-Chu sequences via the Weil bound : springer 2023

[15] Govind R. K., Preetham B. K., Vasile P. : Emerging Trends in photonics, signal processing and communication Engineering : ICPSPCT 2018.

[16] Branislav M. Popovic : Generalized Chirp-like polyphase se with optimum correlation properties : IEEE Trans. Vol. 38. No. 4 1992

RESUME

Rashid Hussein Qasm completed high school education in Altameem High School, after that, he started undergraduate program in Salahaddin University Department of Mathematics in 2005. Then in 2010, he started assignment as a Teacher in Alrwabee high school. To complete M. Sc. education, he moved to Karabük University.