CORRELATION OF SEQUENCES AND QUADRATIC FORMS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

CANSU GENİŞEL

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
CRYPTOGRAPHY

SEPTEMBER 2017

Approval of the thesis:

CORRELATION OF SEQUENCES AND QUADRATIC FORMS

submitted by **CANSU GENİŞEL** in partial fulfillment of the requirements for the degree of **Master of Science in Department of Cryptography, Middle East Technical University** by,

Prof. Dr. Bülent Karasözen
Director, Graduate School of **Applied Mathematics** ______________

Prof. Dr. Ferruh Özbudak
Head of Department, **Cryptography** ______________

Prof. Dr. Ferruh Özbudak
Supervisor, **Cryptography, METU** ______________

Assist. Prof. Dr. Eda Tekin
Co-supervisor, **Business Administration, Karabük University** ______________

Examining Committee Members:

Assoc. Prof. Dr. Ali Doğanaksoy
Mathematics, METU ______________

Prof. Dr. Ferruh Özbudak
Mathematics, METU ______________

Assoc. Prof. Dr. Murat Cenk
Cryptography, METU ______________

Assist. Prof. Dr. Burcu Gülmez Temur
Mathematics, Atılım University ______________

Assist. Prof. Dr. Eda Tekin
Business Administration, Karabük University ______________

Date: ______________

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: CANSU GENİŞEL

Signature :

ABSTRACT

CORRELATION OF SEQUENCES AND QUADRATIC FORMS

Genişel, Cansu
M.S., Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak
Co-Supervisor : Assist. Prof. Dr. Eda Tekin

SEPTEMBER 2017, 41 pages

Sequences are widely used in code division multiple access communication systems. In a shared communication channel distinct sequences are assigned to distinct users. Low correlation sequences should be used in order to separate each user. In this thesis, quadratic forms and their properties are introduced. Sequence families constructed by quadratic forms and their correlations are studied. We give a construction of a binary sequence family when $n = 3k$ and k is an odd integer. This sequence family has six-valued correlation distribution and its maximum correlation magnitude is given. Our sequence family is a subfamily of Generalized Modified Gold sequence family. At the end, we compare the correlation properties of our sequence family with some other known sequence families.

Keywords : Sequences, quadratic forms, cross correlation, wireless communication

ÖZ

DİZİLERİN KORELASYONU VE KUADRATİK FORMLAR

Genişel, Cansu
Yüksek Lisans, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak
Ortak Tez Yöneticisi : Yrd. Doç. Dr. Eda Tekin

EYLÜL 2017, 41 sayfa

Diziler, kod bölmeli çoklu erişim iletişim sistemlerinde yaygın olarak kullanılırlar. Ortak bir iletişim kanalında farklı kullanıcılara farklı diziler atanır. Her kullanıcıyı ayırmak için düşük korelasyonlu diziler kullanılmalıdır. Bu tezde, kuadratik formlar ve özellikleri verilmiştir. Kuadratik formlar ile inşa edilen ikili dizi aileleri ve onların korelasyonları çalışılmıştır. $n = 3k$ ve k tek tam sayı olduğu durumda bir dizi ailesinin inşası verilmiştir. Bu dizi ailesi altı değerli korelasyon dağılımına sahiptir ve maksimum korelasyon büyüklüğü verilmiştir. Bu dizi ailesi Generalized Modified Gold dizi ailesinin bir alt ailesidir. Tezde son olarak, bu dizi ailesinin ve bazı bilinen dizi ailelerinin korelasyon özellikleri karşılaştırılmıştır.

Anahtar Kelimeler : Diziler, kuadratik formlar, çapraz korelasyon, kablosuz haberleşme

To My Family

ACKNOWLEDGMENTS

Foremost, I would like to express my deepest appreciation for my advisor Prof. Dr. Ferruh Özbudak, for his patience, motivation, and tremendous knowledge. His guidance helped me all the time while doing research and writing this thesis.

I would like to thank my co-advisor Assist. Prof. Dr. Eda Tekin, for her generous support. I am greatful for her insightful and quite valuable comments on this thesis.

I owe a great deal to every mathematician who contributed to my education, especially my professors from MSGSÜ.

Last but not least, I must express my profound gratitude to my family and my friends, for their unfailing support and continuous encouragement throughout my years of study. This accomplishment would not have been possible without them. Thank you.

TABLE OF CONTENTS

CHAPTERS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

p	Prime Number
q	Prime Power
$\mathbb{F}_p$	Finite Field with q Elements
r	Rank
Tr	Trace Function
$\widehat{f}(\beta)$	Walsh Transform
$B_f(\cdot,\cdot)$	Symplectic Form
$\mathcal{W}$	Radical
$C_{\Lambda,\Theta}$	Cross Correlation Function
C_{max}	Maximum Correlation Magnitude

CHAPTER 1

INTRODUCTION

Pseudorandom sequences are generated by deterministic methods, which are periodic or aperiodic with certain randomness properties. In this chapter we first give a brief introduction to the randomness properties of binary sequences. Then we introduce sequences for communication and cryptographic systems. This chapter provides basic knowledge on sequences to the reader to understand the following chapters.

1.1 Randomness Properties of Binary Sequences

A sequence s $= \{s_t\}$ satisfying the following linear recurrence

$$s_{m+k} = \sum_{j=0}^{k-1} a_j s_{m+j} \quad \text{for } \ m = 0, 1, \ldots$$

where $t = 0, 1, \ldots$ and $s_t \in \mathbb{F}_q$ for a positive k and fixed $a_j \in \mathbb{F}_q$, is called an *LFSR sequence* (or *linear feedback shift register sequence*) [13].

Golomb [11] introduced some properties which should be satisifed by pseudorandom sequences generated by linear feedback shift registers (LFSRs). The *Golomb's randomness postulates* are necessary properties for a binary sequence to look random.

- Balance property: In a period of the sequence, the number of 0's and the number of 1's differ by at most 1.
- Run property: A run of zeros (or ones) of length k is k consecutive zeros (or ones) preceded and followed by ones (or zeros). In a period of a sequence, the number of runs of 0's and 1's for each length of runs are equal.
- Ideal two-level autocorrelation: Every out-of-phase autocorrelation of a binary sequence is -1.

There are some other randomness criterias which should be satisfied by pseudorandom sequences [13].

- Large period.
- Low correlation: A family of sequences must have low autocorrelation and crosscorrelation values.
- Ideal $k-$tuple distribution: For a sequence with period N, every $k-$tuple occurs almost equally many times for $1 \leq k \leq \log_2 N$.
- Large linear complexity: Large number of linear feedback shift registers should be used to generate sequences.

It is hard to design binary pseudorandom sequences with all the randomness properties given above. We should design sequences with required properties for their specific applications. In the next section, the importance of sequences with low correlation in communication and cryptographic systems is discussed.

1.2 Sequences for Communication Systems

1.2.1 Spread Spectrum Technology

The *spread spectrum* techniques and code division multiple access (CDMA) are popular technologies commonly used in telecommunication systems, navigation, military and operational radar systems. These techniques resist jamming and interception is hard for an attacker. There are several types of spread spectrum methods such as direct sequence, frequency-hopping, chirp and time-hopping spread spectrum. In Figure 1.1 a general model of spread spectrum communication systems is given.

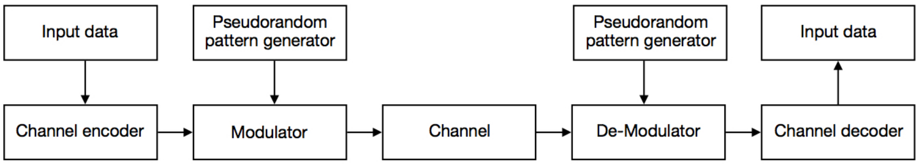


Figure 1.1: General Design of a Spread Spectrum Communication System

In a spread spectrum communication system the transmitted signal is spread over a wide frequency band. Compared to the usual narrow bandwidth services, this system is able to work in lower spectral density levels. In Figure 1.2, the difference in frequency usage of narrowband and spread spectrum systems can be observed. This technology provides some advantages such as:

- Hard to detect: Spread spectrum signals are wider then usual band transmission.

- Hard to intercept or demodulate: Without knowing the codes which are used in this technique it is not possible to decipher the transmission. Moreover since the codes are very long it is not possible to solve the code.
- Harder to jam then narrow bands: The wider input signal means less effect on the system.
- Multiple users can use the same band: Code division multiple access is a form of sharing which allows several spread spectrum systems to operate independently of each other within the same band. More signals are packed into a band.

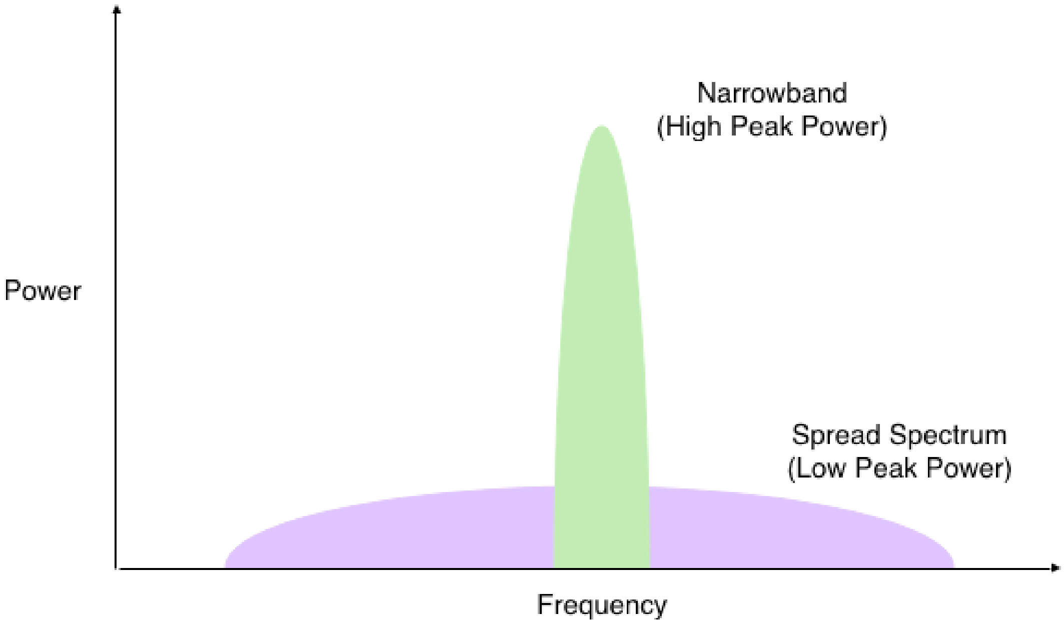


Figure 1.2: Comparison of Narrowband and Spread Spectrum

The history of Spread Spectrum dates back to 1940s [20]. During World War II, a scientist was awarded an early frequency hopping spread spectrum patent. The USA, Germany, the UK and the USSR were the leading countries which make significant contributions to the spread spectrum technology. The U.S. Military used spread spectrum signals over satellites for 30 years [39].

In the 1960s, there are some significant researches in the area of sequences with good correlation properties by S. Golomb, N. Zierler, R. Gold, T. Kasami and others. By means of these works, spread spectrum technology developed and in the 1970s the commercial spread spectrum came up.

Today, spread spectrum techniques are widely used in commercial areas and bandwidths of 10 to 100 times the information rates are used. On the other hand in military systems, bandwidths from 1000 to 1 million times the information rates are used.

In 1993, the first CDMA standard IS-95 was launched and in 1995 CDMA technology was put into commercialization in the USA and Hong Kong. In 2001, CDMA networks

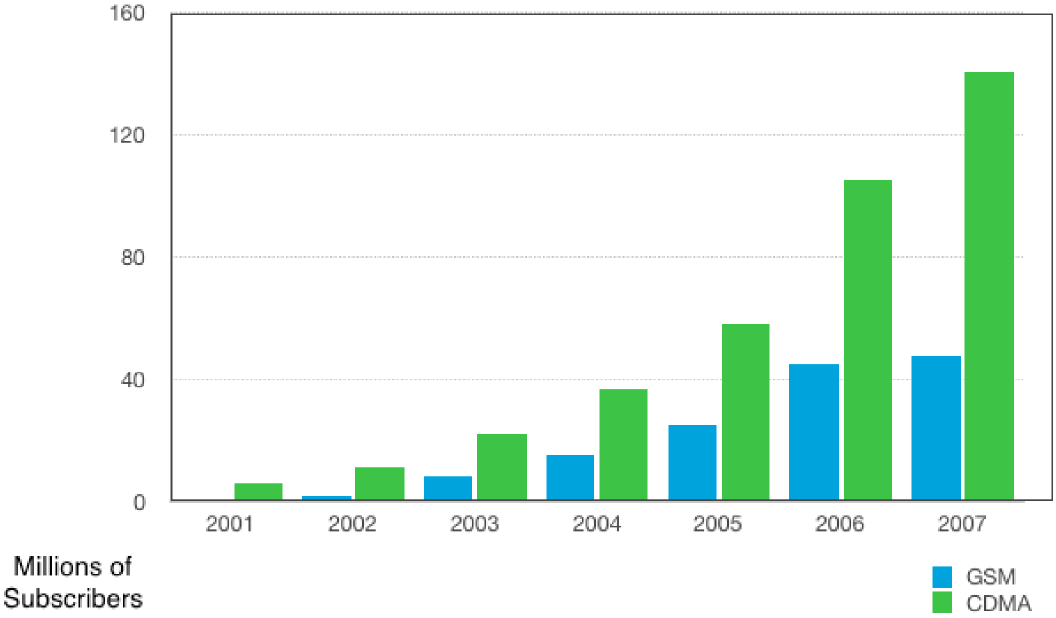


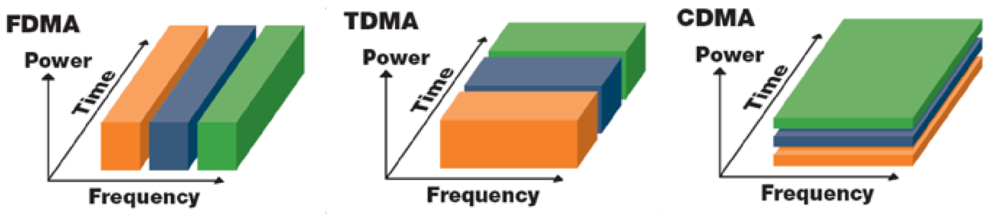
Figure 1.3: CDMA Subscribers Growth Between 2001 and 2007

are constructed by China. Nowadays, CDMA technology is more dominant in Asia, the USA and Canada than the other countries. In 2015 CDMA had %25 market share and 103 million subscribers in these countries where GSM had %5 market share and 19 million subscribers. As of March 2017, there are 7.7 billion mobile subscriptions worldwide which is 317 million more than the previous year. CDMA technology has %3 market share and 215 million subscribers where GSM technology has 3 billion subscribers and %39 market share. On the other hand TC-SCDMA technology has %1 market share and 92 million subcribers and LTE %28 market share and 2.16 billion subscribers worldwide.

1.2.2 TDMA, FDMA and CDMA

There are different types of multiple access systems such as time division multiple access (TDMA), frequency division multiple access (FDMA) and code division multiple access (CDMA). In time division multiple access (TDMA) communication systems, a radio channel is divided into several time zones. Each user is allocated in a time zone and they know the time zone to use for the duration of data transmission. In FDMA the frequency band is divided into sub-bands and any two user can communicate through a sub-band. In CDMA, each user is assigned a code and all users share the same channel.

In CDMA frequency planning is much less than the frequency planning in FDMA or TDMA. Furthermore in TDMA systems the available bandwidth which causes to compromise of transmission quality is small. In Figure 1.4 the difference between these three systems is explained with some graphs. In the next section we will give detailed information about CDMA.



(a) FDMA (b) TDMA (c) CDMA

Figure 1.4: Comparison of FDMA, TDMA and CDMA

1.2.3 Principles of CDMA Systems

Pseudorandom sequences are used in communication systems extensively. Spread spectrum communication systems, radar systems, signal synchronization, simulation and cryptography are some of the application areas for such sequences. Sequences have critical roles in spread spectrum and code division multiple access (CDMA) communication systems.

In code division multiple access (CDMA), channels are not defined by time or frequency. They are defined by a spread spectrum parameter called a *spreading code*. Code division multiple access (CDMA) is a kind of spread spectrum technique, that is data can be transmitted in small parts over a number of the discrete frequencies. Some advantages of CDMA are given as follows:

- increased cellular communications security
- simultaneous conversations,
- low power requirement,
- extended capacity which benefits to rural users.

On the other hand this system has some disadvantages:

- the network is not as mature as GSM,
- can not offer international roaming.

Several calls are superimposed on each other on the channel, with each assigned to a unique sequence code. Each user's signal is spread over the whole radio frequency range by a unique spreading code. The system works as follows. Each user is assigned with a different unique code and they use this code to transmit signal. To send data, users XOR the data with their spreading sequence and to decode the received signal, they XOR the signal with the sender's spreading sequence.

As seen in Figure (1.5) in FDMA, each handset communicates with the base station on its own narrow frequency band. In TDMA the handsets share a wider frequency

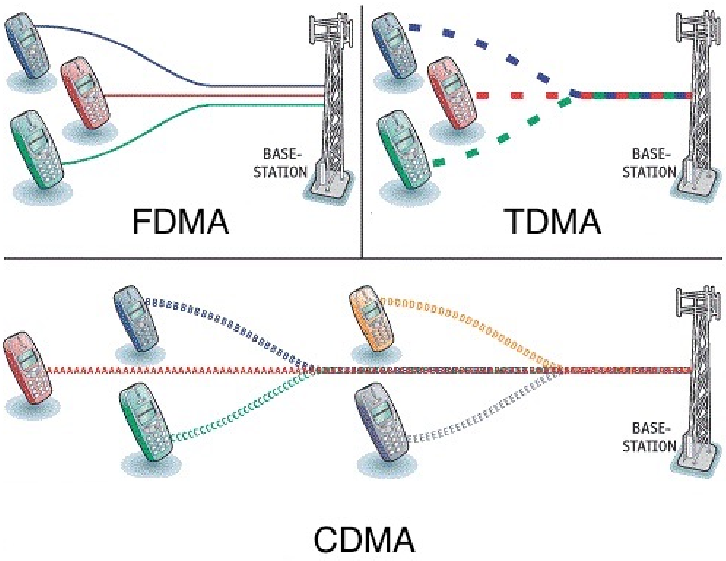


Figure 1.5: Multiple Access Systems

band and takes turns to communicate with the base station. In CDMA each handset uses a sequence or a code to scramble their signal and then multiple users transmit simultaneously on the same frequency band. The base station uses the same codes and unscramble the different users' signal.

1.2.4 Application of Sequences for CDMA Communication Systems

Sequences with low autocorrelation and cross correlation have important use in wireless communication systems. The following research areas on the sequences have specific applications of communication systems.

Orthogonal Codes: In a CDMA communication system all users occupy the same frequency band simultaneously. Different code assignments spread and distinguish each user. The codes assigned to each user or channel should be mutually orthogonal to reduce the mutual interference between distinct users or channels.

The Walsh codes and the orthogonal variable spreading factor codes are used in wireless communication. Each orthogonal code of length n corresponds to each row of an $n \times n$ Hadamard matrix [37]. These codes are used in spreading and channelization.

Sequences with Ideal Two-level Autocorrelation: The design of sequences with ideal autocorrelation is a central mathematical problem in engineering, as it is crucial for a host of applications, including radar and communication networks. These sequences play important roles in positioning and synchronization processes of CDMA.

There are some familiar sequences with ideal two-level autocorrelation; the m-sequences

[11], the GMW sequences [16], the Legendre sequences [21], the Hall's sextic residue sequences [17]. Moreover, there are some recent constructions of families of sequences of period $2^n - 1$ such as the Kasami power function sequences [7], the Welch-Gong(WG) sequences [31, 32] and the Generalized nonbinary sequences [5].

Sequences with Good Aperiodic Autocorrelation: Multicarrier transmission techniques such as orthogonal frequency division multiplexing (OFDM) and multicarrier CDMA (MC-CDMA) have attracted much attention for future communication systems.

The Barker sequences [1] and the Golay complementary sequences [8] are sequences with ideal aperiodic autocorrelation values. These sequences are used in multicarrier transmission techniques such as CDMA (MC-CDMA).

Sequences with Low Correlation: Sequences with low cross correlation used in code division multiple access (CDMA) communications can strongly withstand interference from the other users who share a mutual channel. Sequences are used for identification of users and base stations.

The construction of CDMA sequence families using quadratic functions and investigation of their correlation distributions dates back 1960's to Gold sequences [9], [10]. Since then there have been a number of different such designs with good correlation properties. Some of the recent constructions are given by Boztaş and Kumar in [3], Kim and No in [24], Tang *et al.* in [40], Rothaus in [36], Zhou and Tang in [42]. These families are generalizations of Gold-like sequences constructed using quadratic form techniques. For more recent designs please see the references in [4], [24], [33].

On the other hand, Gong has been studying sequences and their correlations since 1995. Some of her studies on various topics related to sequences can be found in [6], [12], [13], [15], [18] and [32]. Gong presented different constructions for families of sequences over GF(p) with low cross correlation, balance property, and large linear span using short $p-$ary sequences in [14].

1.3 Sequences for Cryptographic Systems

Pseudorandom numbers and sequences have critical roles for the security of a cryptographic system. A secure cryptographic system should posses some properties. High nonlinearity and large linear complexities of pseudorandom sequences are necessary for the security of a system using the sequences.

The nonlinearity N_f of a Boolean function $f(\mathbf{x})$ is given by

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\beta \in \mathbb{F}_2^n} |\widehat{f}(\beta)|$$

where $\widehat{f}(\beta)$ is the Walsh transform of $f(\mathbf{x})$ which will be described and explained briefly in Section 2.3.

Moreover, there is an equivalance between the Walsh transform and the Hadamard transform of a Boolean function. The Hadamard transform of a polynomial function is equivalent to the correlation function between a binary m-sequence and a sequence represented by $f(x)$. A known Boolean function with the highest nonlinearity is the *bent function* [35]. A high nonlinearity provides resistance to the attacks such as fast correlation attack [28]. In conclusion sequences used for cryptographic systems should have low correlation for the high nonlinearity.

On the other hand, there is another essential property for cryptographic applications. It should be hard to make predictions about the whole outputs of a Boolean function by observing a section of the outputs. Deterministic algorithms which work in polynomial time can be used in cryptanalysis [29]. To avoid these attacks, sequences should have large linear complexity. If the linear complexity is large as possible then the reconstruction of the sequences by the Berlekamp-Massey Algorithm is avoided. For additional details, the reader is referred to [2, 27]. In summary, the large linear complexity and the low correlation are obligatory to have a secure cryptographic system.

1.3.1 Application of Sequences for Cryptographic Systems

In cryptographic systems, sequences with significant properties such as large linear complexity and low correlation play important roles. Moreover, the sequences generated by linear feedback shift registers have some other advantages such as fast processing and easy implementation.

In a stream cipher, sequences with low cross correlation are used as key stream generators or in a block cipher, sequences are used as a session key generator. Moreover in a public key cryptosystem, sequences with low cross correlation are used as pseudorandom number generators. These sequences provides resistance to the system against cross correlation attack [27].

1.4 Overview of the thesis

In the previous sections it is explained that sequences with good correlation properties are important for communication and cryptographic systems. In this thesis, we focus on low maximum crosscorrelation magnitude of sequence families. This thesis arranged as follows:

- In Chapter 2, we introduce a summation of mathematical background required to understand the next chapters of this thesis. Then we give some necessary definitions and theorems about finite fields, sequences and quadratic forms.
- In Chapter 3 we focus on sequences with low maximum cross correlation magnitude. First we introduce some of the known sequence families with low maximum crosscorrelation magnitude. Then we construct a family of binary sequences for odd positive integer $n = 3k$ for odd k with $C_{\max} = 1 + 2^{\frac{n+3}{2}}$.

After a referee review we found out that this family is a subfamily of generalized modified Gold sequence family [42]. Furthermore we explain the relation between our sequence family and the Generalized Modified Gold sequence family. Finally we compare all of the given sequence families with good correlation properties.

- In Chapter 4 we present the conclusion.

CHAPTER 2

PRELIMINARIES

In this chapter a general background on finite fields, quadratic forms and sequences is given. For further explanations and applications, the reader is referred to [26] and [30].

2.1 Finite Fields

Definition 2.1. A field $F = (F, +, \cdot)$ is a set F, together with two binary operations (+) and $(\cdot)$ on F such that

- $x + y = y + x$ and $x \cdot y = y \cdot x$ for all $x, y \in F$;
- $(x + y) + z = x + (y + z)$ and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in F$;
- For two binary operations (+) and $(\cdot)$ there exists unique elements e and e' of F with the properties that $x + e = e + x = x$ and $x \cdot e^{'} = e^{'} \cdot x = x$ for all $x, y \in F$;
- given any element x of F, there exists an element $x^{'}$ of F with the property that $x + x^{'} = x^{'} + x = e$;
- given any nonzero element x of F, there exists an element $x^{''}$ of F with the property that $x \cdot x^{''} = x^{''} \cdot x = e^{'}$
- $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(x + y) \cdot z = x \cdot z + y \cdot z$ for all $x, y, z \in F$.

Definition 2.2. Let K be a subset of F that is itself a field under the operations of F. Then K is called a *subfield* of F and F is called an *extension* of K.

Definition 2.3. A field containing no proper subfields is called a *prime* field.

Definition 2.4. A *finite field* is a field that contains a finite number of elements. This number is called the *order* of a finite field.

For a prime number p, let F be the set of $\{0, 1, \ldots, p - 1\}$ of integers and let

$$\begin{aligned} \sigma : \mathbb{Z}/(p) &\to F \\ [a] &\mapsto a, \end{aligned}$$

for $a = 0, 1, \ldots, p-1$. Then F has a field structure induced by σ. F is a finite field and called the *Galois field of order* p, denoted by $\mathbb{F}_p$.

Lemma 2.1. *Let F be a finite field and K be a subfield of F with q elements. Then F is a vector space over K and $|F| = q^m$, where m is the dimension of F over K.*

Lemma 2.2. *Let F be a finite field of order q. Then for all $x \in F$, $x^q = x$.*

Definition 2.5. The *characteristic* of a finite field F is the smallest positive integer n such that $nx = 0$ for all $x \in F$.
Every finite field has prime characteristic.

Theorem 2.3 (Existence and Uniqueness of Finite Fields). *For every prime p and every positive integer $n \geq 1$ there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of the polynomial $x^q - x$ over $\mathbb{F}_p$.*

Definition 2.6. A *primitive element* α of a finite field $\mathbb{F}_p$ is a generator of its multiplicative group $\mathbb{F}_p^*$.

Definition 2.7. Let q be a prime or a power of a prime. For $\alpha \in F = \mathbb{F}_{q^n}$ and $K = \mathbb{F}_q$, the *trace* of α over K is the sum of the conjugates of α and it is defined as

$$Tr_{F/K}(\alpha) = Tr_1^n(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^n-1}.$$

The trace function satisfies the following properties:

1. $Tr_{F/K}(\alpha + \beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta)$, for all $\alpha, \beta \in F$;
2. for any $\alpha \in F$, $Tr_{F/K}(\alpha) \in K$;
3. $Tr_{F/K}(c\alpha) = cTr_{F/K}(\alpha)$ for $c \in K$ and $\alpha \in F$;
4. $Tr_{F/K}$ is a $K-$ linear map from F onto K;
5. $Tr_{F/K}(\alpha^q) = Tr_{F/K}(\alpha)$ for all $\alpha \in F$;
6. $Tr_{F/K}(\alpha) = n\alpha$ for all $\alpha \in K$;
7. let $\alpha \in F$. If $Tr_{F/K}(\alpha\beta) = 0$ for all $\beta \in F$, then $\alpha = 0$,
8. $|\{\beta \in F : Tr_{F/K}(\beta) = \alpha\}| = q^{n-1}$, for any $\alpha \in K$.

Theorem 2.4. *Let K be a finite field. Let F be a finite extension of K and E a finite extension of F. Then*

$$Tr_{E/K}(\alpha) = Tr_{F/K}(Tr_{E/F}(\alpha)), \textit{ for all } \alpha \in E.$$

Definition 2.8. Let $f(x) = x^n - 1 \in \mathbb{F}_q[x]$. Then the roots $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{F}_{q^n}$ of $f(x)$ are called the *n-th roots of unity over* $\mathbb{F}_q$.

Definition 2.9. Let $\mathbb{F}_q$ be a finite field of characteristic p satisfying $p \not| n$ and $\alpha \in \mathbb{F}_{q^n}$. If the cyclic group of n-th roots of unity is generated by α, then α is a *primitive n-th root of unity* over $\mathbb{F}_q$.

2.2 Some Special Functions Over Finite Fields

Definition 2.10. For a positive integer n, an *n-variable Boolean function* is defined from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ and denoted by $f(\mathbf{x})$, where $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_2^n$ and $x_i \in \mathbb{F}_2$. A Boolean function consists of a sum of all possible products of x_{i_j}'s with coefficients 0 or 1, that is,

$$f(\mathbf{x}) = f(x_1, \dots, x_n) = c_0 + \sum_{1 \leq j \leq n} c_{i_1 i_2 \dots i_j} x_{i_1} x_{i_2} \cdots x_{i_j}, \tag{2.1}$$

where $c_0, c_{i_1 i_2 \dots i_j} \in \mathbb{F}_2$ and $\{i_1, \cdots, i_j\} \subset \{1, \cdots, n\}$. The *degree* of the Boolean function $f(\mathbf{x})$ is the maximum value of j where $c_{i_1 i_2 \dots i_j}$ is nonzero. Equation (2.1) is called the *algebraic normal form* of a Boolean function [13].

Remark that with the structure of $\mathbb{F}_{2^n}$, $\mathbb{F}_2^n$ can be endowed and it gives advantages when designing Boolean functions. In this case, the function is denoted by $f(x)$, where $x \in \mathbb{F}_{2^n}$.

Definition 2.11. Let $f(x)$ be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Then, $f(x)$ can be represented as

$$f(x) = \sum_{j \in J} Tr_1^{m_j}(A_j x^j) + A_{2^n-1}, \quad A_j \in \mathbb{F}_{2^{m_j}}, A_{2^n-1} \in \mathbb{F}_2 \tag{2.2}$$

where J is a set containing all coset leaders modulo $2^n - 1$ and $m_j | n$ is the size of the coset C_j [13, 19]. The equation (2.2) is called *trace represantation* of $f(x)$ or a *polynomial*.

2.3 Sequences and Their Properties

Definition 2.12. Let $f(x) \in \mathbb{F}_q[x]$ be a primitive polynomial, which is the minimum polynomial of a primitive element $\alpha \in \mathbb{F}_{q^n}$. A nonzero sequence $s(t)$ over $\mathbb{F}_q$ generated by $f(x)$ is called a maximal length sequence (m-sequence). Let $a = \alpha^i$, where α has order $q^n - 1$ and $i = 0, \dots, q^n - 1$. Then the m-sequence is defined by

$$s(t) = Tr_1^n(a\alpha^t), \quad a \in \mathbb{F}_{q^n}.$$

Definition 2.13. Let $\mathbf{a} = \{a_t\}$ and $\mathbf{b} = \{b_t\}$ be two binary sequences. If there exists an integer τ for all $t \geq 0$, such that

$$a_t = b_t + \tau,$$

then $\mathbf{a}$ and $\mathbf{b}$ are called *cyclically equivalent*. Otherwise they are said to be *cyclically distinct* [13].

Definition 2.14. Let $\mathbf{a} = \{a_t\}$ be a binary sequence of period N and K be the difference between the numbers of 0's and 1's of $\mathbf{a}$ in a period N.

Then, $\mathbf{a}$ is called *balanced* [11] if

$$K = \left| \sum_{t=0}^{N-1} (-1)^{a_t} \right| \leq 1.$$

For even N, $\mathbf{a}$ is balanced if and only if $K = 1$ and for odd N, it is balanced if and only if $K = 0$.

Definition 2.15. Let $\mathbf{a} = \{a_t\}$ and $\mathbf{b} = \{b_t\}$ be two arbitrary binary sequences of period N. The correlation between $\mathbf{a}$ and $\mathbf{b}$ is defined by

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{t=0}^{N-1} (-1)^{a_{t+\tau}+b_t}, \quad 0 \leq \tau \leq N-1. \tag{2.3}$$

Note that if $\mathbf{a}$ and $\mathbf{b}$ are cyclically equivalent, that is $a_t = b_{t+k}$ for all $1 \leq t, k \leq N$, then $C_{\mathbf{a},\mathbf{b}}$ is called the *autocorrelation* of $\mathbf{a}$. Otherwise if $\mathbf{a}$ and $\mathbf{b}$ are cyclically distinct, then $C_{\mathbf{a},\mathbf{b}}$ is called the *cross correlation* of $\mathbf{a}$ and $\mathbf{b}$.

Let $S = \{\mathbf{s_0}, \cdots \mathbf{s_{m-1}}\}$ be a sequence family with m cyclically distinct sequences of period N. Then the *maximum correlation magnitude* of S is defined as

$$C_{max} = \max\{|C_{\mathbf{s}_i,\mathbf{s}_j}(\tau)| \text{ if } \mathbf{s}_i \neq \mathbf{s}_j, \text{ or } \mathbf{s}_i = \mathbf{s}_j \text{ and } \tau \neq 0\}. \tag{2.4}$$

Definition 2.16. Let $f(x)$ be a polynomial function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Then the Hadamard transform of $f(x)$ is defined as

$$\widehat{f}(\beta) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr(\beta x)}, \ \beta \in \mathbb{F}_{2^n}.$$

The inverse transformation is as follows

$$(-1)^{f(\beta)} = \frac{1}{2^n} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\beta x)} \widehat{f}(x), \ \beta \in \mathbb{F}_{2^n}.$$

Definition 2.17. Let $\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{F}_2^n$ and $f(\mathbf{x})$ be a Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Then the Walsh transform of a Boolean function $f(\mathbf{x})$ is defined as

$$\widehat{f}(\mathbf{y}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x})+\mathbf{y}\cdot\mathbf{x}}, \ \mathbf{y} \in \mathbb{F}_2^n.$$

Remark 2.1. The Hadamard transform of a polynomial function corresponds to the Walsh transform of the equivalent Boolean function [13].

Let $\alpha \in \mathbb{F}_{2^n}$ be primitive and f be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ satisfying $f(0) = 0$. Let $\mathbf{a} = \{a_t\}$ and $\mathbf{b} = \{b_t\}$ be two binary sequences of period $2^n - 1$, such that $a_t = f(\alpha^t)$ and $b_t = Tr(\alpha^t)$, where $t = 0, 1, \cdots$. Then there is a relation between the cross correlation of a sequence, and an m-sequence and the Hadamard transform of f, such as

$$C_{\mathbf{a},\mathbf{b}} = -1 + \widehat{f}(\beta), \text{ where } \beta = \alpha^\tau, 0 \leq \tau \leq N-1.$$

Definition 2.18. A Boolean function f is called *t-plateaued* if the Walsh transform values of f are in $\{0, \pm 2^{\frac{n+t}{2}}\}$ for some $t = 0, 1, \cdots, n$.

Furthermore, if n is an even integer, a function f is called *bent* function if and only if f is a 0-plateaued function. The Walsh transform values of a bent function are in $\{0, \pm 2^{\frac{n}{2}}\}$.

2.4 Quadratic Forms

Definition 2.19. A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called *quadratic form* if it can be written as

$$f(x) = \sum_{i=0}^{t} Tr_1^n(a_i x^{1+2^i}), \tag{2.5}$$

where $a_i \in \mathbb{F}_{2^n}$ and $t = \left\lceil \frac{n}{2} \right\rceil$.

Definition 2.20. The *symplectic form* of a quadratic form $f(x)$ is defined by

$$B_f(x, y) = f(x) + f(y) + f(x + y). \tag{2.6}$$

Remark 2.2. The symplectic form of a quadratic form $f(x)$ is symmetric and bilinear.

The *radical* of a quadratic form $f(x)$ is defined as follows

$$\mathcal{W} = \{x \in \mathbb{F}_{2^n} : B_f(x, y) = 0 \quad \forall y \in \mathbb{F}_{2^n}\}. \tag{2.7}$$

Let $2r$ be the rank of the quadratic form $f(x)$. Then $2r = n - \log_2 N$, where N is the number of elements of the radical $\mathcal{W}$.

Lemma 2.5. *Let $f(x)$ be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. If $f(x)$ is a quadratic form of rank $2r$, where $2 \leq 2r < n$, then the Walsh transform of $f(x)$ is*

$$\widehat{f}(\beta) = \begin{cases} 2^{n-r}, & 2^{2r-1} + 2^{r-1} \quad times, \\ 0, & 2^n - 2^{2r} \quad times, \\ -2^{n-r}, & 2^{2r-1} - 2^{r-1} \quad times. \end{cases} \tag{2.8}$$

CHAPTER 3

SEQUENCE FAMILIES WITH LOW CROSSCORRELATION MAGNITUDE

3.1 Known Sequence Families with Low Cross Correlation Magnitude

Sequence families with small correlation magnitude play an important role in CDMA systems. It is critical to find such sequences with low correlation magnitude to be used in such systems.

In this section we give two important well known lower bounds which are used to compare the maximum correlation magnitude of a sequence family. We give a brief introduction to some known sequence families with good cross correlation distribution.

Let $S = \big\{\{s_i(t)\} : 1 \leq i \leq M\big\}$ be a sequence family with M cyclically distinct sequences of period N. Let C_{max} denote the maximum cross correlation magnitude of S.

Theorem 3.1. *[30] For an arbitrary positive integer l with $l \geq 1$, and for the sequence family S defined as above, the Welch bound satisfies the following inequality:*

$$(C_{max})^{2l} \geq \frac{1}{MN-1}\left(\frac{MN^{2l+1}}{\binom{N+l-1}{N-1}} - N^{2l}\right).$$

Theorem 3.2. *[30] For an arbitrary positive integer l with $l \geq 1$, and for the sequence family S defined as above, the Sidelnikov bound satisfies the following inequality:*

1. *When $q = 2$,*

$$(C_{max})^2 > (2l+1)(N-l) + \frac{l(l+1)}{2} - \frac{2^l N^{2l+1}}{M(2l)!\binom{N}{l}}, 0 \leq l \leq \frac{2N}{5}.$$

2. *When $q > 2$,*

$$(C_{max})^2 > \frac{l+1}{2}(2N-l) - \frac{2^l N^{2l+1}}{M(l!)^2\binom{2N}{l}}, l \geq 0.$$

Now we give definitions of some important sequence families.

3.1.1 Gold Sequences

Definition 3.1. Let n be an odd integer, $d = 2^k + 1$, and $gcd(k, n) = 1$. Let α be a primitive element of $\mathbb{F}_{2^n}$ and $s(t) = Tr_1^n(\alpha^t)$ be an $m-$sequence of period $N = 2^n - 1$. Then the Gold sequence family [10] is defined by:

$$S(t) = \{s(t)\} \cup \{s(dt)\} \cup \{\{s(t+\tau) + s(dt) : 0 \leq \tau \leq N-1\}\}.$$

In other words, this family is constructed by using the following quadratic form

$$p(x) = Tr_1^n(x^{1+2}).$$

Then,

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

where

$$s_i(t) = \begin{cases} Tr_1^n(\eta_i \alpha^t) + p(\alpha^t), & 0 \leq i < 2^n \\ Tr_1^n(\alpha^t), & i = 2^n. \end{cases},$$

where η_i is enumeration of $\mathbb{F}_{2^n}$

The Gold sequence family has $2^n + 1$ cyclically distinct sequences of period $2^n - 1$, its maximum correlation magnitude is $C_{max} = 1 + 2^{\frac{n+1}{2}}$ and the correlation values are

$$\{-1, -1 + 2^n, -1 \pm 2^{\frac{n+1}{2}}\}.$$

3.1.2 Kasami Sequences

Definition 3.2. Let $n = 2l$, $l \geq 2$, and α be a primitive element of $\mathbb{F}_{2^n}$. Then the small family of Kasami sequences [22, 23] is defined by

$$S(t) = \{s_u(t) : u \in \mathbb{F}_{2^l}, 0 \leq t \leq N-1\}$$

where

$$s_u(t) = Tr_1^n(\alpha^t) + Tr_1^l(u\alpha^{(1+2^l)t}).$$

The small family of Kasami sequences has 2^l cyclically distinct sequences of period $2^n - 1$ and its maximum correlation magnitude is $C_{max} = 1 + 2^l$.

3.1.3 Sidelnikov Sequences

Definition 3.3. Let k be a positive integer and $k < p$, where p is a prime number. Let α be a primitive element of $\mathbb{F}_{p^n}$. Then for $a_m \in \mathbb{F}_{p^n}$ where $1 \leq m \leq l$, the family of Sidelnikov sequences [38] is defined by

$$S(t) = Tr_1^n\left(\sum_{m=1}^{k} a_m \alpha^{mt}\right).$$

The Sidelnikov sequence family has $M \geq p^{n(k-1)}$ cyclically distinct sequences of period $N = p^n - 1$ and its maximum correlation magnitude is $C_{max} \leq 1 + (k-1)p^{\frac{n}{2}}$.

3.1.4 No Sequences

Definition 3.4. Let $n = 2l$, with $l \geq 2$, and α be a primitive element of $\mathbb{F}_{2^n}$. Let $1 \leq r \leq 2^l - 1$, $gcd(r, 2^l - 1) = 1$, where $r \neq 2^i$ for any i. Then the family of No sequences [33] is defined by

$$S(t) = \{s_u(t) : u \in \mathbb{F}_{2^n}, 0 \leq t \leq N-1\}$$

where

$$s_u(t) = Tr_1^l\Big(\Big(Tr_1^l(\alpha^t + u\alpha^{(2^l+1)t})\Big)^r\Big).$$

The family of No sequences has the same family size and the same maximum correlation magnitude as the small family of Kasami sequences. Also remark that the family of Kasami sequences has the highest linear complexity.

3.1.5 Bent Sequences

Definition 3.5. For a prime number p, let $f(x)$ be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Let $\omega \in \mathbb{F}_{p^n}$ be a complex $p-$th root of unity. Then the Walsh function is defined as follows:

$$W_f(w) = \frac{1}{\sqrt{p^m}} \sum_{x \in \mathbb{F}_{p^m}} \omega^{f(x) - Tr_1^n(wx)}, \quad \text{for all } w \in \mathbb{F}_{p^n}.$$

If the Walsh transform of a function takes values of unit magnitude then it is called a generalized bent function. Moreover the sequences of values $\omega^{f(x)}$ are called *bent sequences* [34]. For a primitive element $\alpha \in \mathbb{F}_{p^n}$ the cross correlation of a bent sequence is as follows:

$$C_f(\tau) = \sum_{t=0}^{p^n-2} \omega^{f(\alpha^t) - Tr_1^n(\alpha^{t+\tau})}.$$

3.1.6 Kumar and Moreno p-ary Bent Sequences

Definition 3.6. Let $n = 2l$, and α be a primitive element of $\mathbb{F}_{p^n}$. Let V_p^l be an $l-$dimensional vector space over $\mathbb{F}_p$. Let $\{\beta_1, \beta_2, \ldots, \beta_l\}$ be a basis of $\mathbb{F}_{p^l}$ over $\mathbb{F}_p$ and $\sigma \in \mathbb{F}_{p^n} - \mathbb{F}_{p^l}$. Then, for $\gamma \in \mathbb{F}_{p^l}^*$, the Kumar and Moreno p-ary bent sequences are defined [25] as follows:

$$S = \{s_u(t) : u \in \mathbb{F}_{p^l}, 0 \leq t \leq p^n - 2\}$$

where

$$s_u(t) = f(L(\alpha^t)) + Tr_1^n((u\sigma + \gamma)\alpha^t)$$

and

$$L(x) = \{Tr_1^n(\beta_1 \sigma x), \dots, Tr_1^n(\beta_l \sigma x)\}.$$

The Kumar and Moreno sequence family has $p^{\frac{n}{2}}$ cyclically distinct sequences of period $N = p^n - 1$ and its maximum correlation magnitude $C_{max} = 1 + p^{\frac{n}{2}}$.

3.1.7 Gold-like Sequences

Definition 3.7. Let p be a prime number and n be a positive odd integer. Let η_i be the enumeration of the elements of $\mathbb{F}_{2^n}$, for $0 \leq i \leq 2^n - 1$,

Let $p(x)$ be the quadratic form defined as follows:

$$p(x) = \sum_{j=0}^{\frac{n-1}{2}} Tr_1^n(x^{1+2^j}).$$

Then the Gold-like sequence family [3] is defined by

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

where

$$s_i(t) = \begin{cases} Tr_1^n(\eta_i \alpha^t) + p(\alpha^t), & 0 \leq i < 2^n \\ Tr_1^n(\alpha^t), & i = 2^n. \end{cases}$$

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

$$C_{i,j}(t) = \begin{cases} -1 + 2^n, & 2^n + 1 \text{ times}, \\ -1, & 2^{3n-1} + 2^{2n} - 2^n - 2 \text{ times}, \\ -1 + 2^{\frac{n+1}{2}}, & (2^{2n-2})(2^{n-2} + 2^{\frac{n-3}{2}}) \text{ times}, \\ -1 - 2^{\frac{n+1}{2}}, & (2^{2n-2})(2^{n-2} - 2^{\frac{n-3}{2}}) \text{ times}. \end{cases}$$

3.1.8 Kim and No Sequences

Definition 3.8. Let n be a positive odd integer with $n = me$, where $m \geq 3$ is an odd integer. Let k be a positive integer satisfying $gcd(n, k) = e$. For $0 \leq i \leq 2^n - 1$, let η_i be the enumeration of the elements of $\mathbb{F}_{2^n}$.

Let $q(x)$ be the quadratic form defined as follows:

$$q(x) = \sum_{h=0}^{\frac{m-1}{2}} Tr_1^n(x^{1+2^{eh}}).$$

Then the Kim and No sequence family [24] is defined by

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

where

$$s_i(t) = \begin{cases} Tr_1^n(\eta_i \alpha^t) + q(\alpha^t), & 0 \leq i < 2^n \\ Tr_1^n(\alpha^t), & i = 2^n. \end{cases}$$

The Kim and No sequence family has $2^n + 1$ cyclically distinct sequences of period $2^n - 1$, its maximum correlation magnitude is $C_{max} = 1 + 2^{\frac{n+e}{2}}$, where e is an integer satisfying $n = me$. The correlation distribution of this family is given as follows

$$C_{i,j}(t) = \begin{cases} -1 + 2^n, & 2^n + 1 \text{ times} \\ -1, & (2^n - 2^{n-e} + 1)(2^{2n} - 2) \text{ times} \\ -1 + 2^{\frac{n+e}{2}}, & (2^{n-e-1} + 2^{\frac{n-e-2}{2}})(2^{2n} - 2) \text{ times} \\ -1 - 2^{\frac{n+e}{2}}, & (2^{n-e-1} - 2^{\frac{n-e-2}{2}})(2^{2n} - 2) \text{ times.} \end{cases}$$

3.1.9 Tang *et al.* Sequences

Tang, Helleseth, Hu and Jiang used two quadratic forms $p(x)$ and $q(x)$, given by Boztas and Kumar and Kim and No respectively. They constructed a new family of Gold-like sequences and they gave the correlation distribution of this family.

Definition 3.9. Let n be a positive odd integer with $n = me$, where $m \geq 3$ is an odd integer. Let k be a positive integer satisfying $gcd(n, k) = e$. For $0 \leq i \leq 2^n - 1$, let η_i be the enumeration of the elements of $\mathbb{F}_{2^n}$ and let $w \in \mathbb{F}_{2^n} \setminus \{1\}$.

Let $p_w(x)$ be the quadratic form defined as follows:

$$p_w(x) = \sum_{h=0}^{\frac{n-1}{2}} Tr_1^n(x^{1+2^h}) + \sum_{h=0}^{\frac{m-1}{2}} Tr_1^n((wx)^{1+2^h}).$$

Then the sequence family constructed by Tang et al. [40] is defined as follows:

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

where

$$s_i(t) = \begin{cases} Tr_1^n(\eta_i \alpha^t) + p_w(\alpha^t), & 0 \leq i < 2^n \\ Tr_1^n(\alpha^t), & i = 2^n. \end{cases}$$

The correlation distribution of the family is as follows

$$C_{i,j}(t) = \begin{cases} -1+2^n, & 2^n+1 \text{ times} \\ -1, & 2^{3n-1}+2^{2n}-2^n-2 \text{ times} \\ -1+2^{\frac{n+1}{2}}, & (2^{2n-2})(2^{n-2}+2^{\frac{n-3}{2}}) \text{ times} \\ -1-2^{\frac{n+1}{2}}, & (2^{2n-2})(2^{n-2}-2^{\frac{n-3}{2}}) \text{ times.} \end{cases}$$

3.1.10 Modified Gold Sequences

Definition 3.10. Let $n = 2l+1$, $n \geq 5$ be and odd integer. The modified Gold sequence family constructed by Rothaus [36] is defined as follows:

$$S(t) = \big\{\{s_\Lambda(t)\} : \Lambda = (\lambda_0, \lambda_1, \lambda_2), \lambda_i \in \mathbb{F}_{2^n} \text{ for } 0 \leq i \leq 2\big\}$$

where

$$s_\Lambda(t) = Tr_1^n\big(\lambda_0\alpha^t\big) + Tr_1^n\big(\lambda_1\alpha^{(1+2^{\frac{n+1}{2}})t}\big) + Tr_1^n\big(\lambda_2\alpha^{(1+2^{\frac{n+3}{2}})t}\big).$$

The modified Gold sequence family has $2^n + 2^{(k-1)n} + \cdots + 2^n + 1$ sequences of period $2^n - 1$, and its maximum correlation magnitude is $1 + 2^{\frac{n+3}{2}}$.

3.1.11 Generalized Modified Gold Sequences

Definition 3.11. Let $n = 2l+1$, m be an integer satisfying $gcd(n,m) = 1$ and k be an integer with $1 \leq k \leq l$. Let α be a primitive element of $\mathbb{F}_{2^n}$. Then the sequence family constructed by Zhou and Tang [42] is defined as follows:

$$S^m(k) = \big\{\{s_\Lambda(t)\} : \Lambda = (\lambda_0, \ldots, \lambda_k), \lambda_i \in \mathbb{F}_{2^n} \text{ for } 0 \leq i \leq k\big\}$$

where

$$s_\Lambda(t) = Tr_1^n(\lambda_0\alpha^t) + \sum_{i=1}^{k} Tr_1^n(\lambda_i\alpha^{(1+2^{(l+j)m})t}).$$

Let

$$\triangle_i = \{(\lambda_0, \ldots, \lambda_k) : \lambda_j \in \mathbb{F}_{2^n} \text{ for } 0 \leq j < i, \lambda_i = 1, \text{and } \lambda_j = 0 \text{ for } i < j \leq k\},$$

and for each $0 \leq i \leq k$, let

$$\mathcal{F}_i^m = \{\{s_\Lambda(t) : \Lambda \in \triangle_i\}.$$

Then

$$\mathcal{F}^m(k) = \bigcup_{i=0}^{k} \mathcal{F}_i^m$$

is a set of cyclically distinct representatives for family $S^m(k)$.

The family $\mathcal{F}^m(k)$ has $2^{kn}+2^{(k-1)n}+\cdots+2^n+1$ cyclically distinct binary sequences of period 2^n-1, and its maximum correlation magnitude is $1+2^{l+k}$. The correlation values of this family are computed for special cases in [42].

Remark 3.1. When $k=1$, the family $\mathcal{F}^m(1)$ is the Gold sequence family. In [10] the correlation distribution of this family is given as follows

$$C_{i,j}(t)=\begin{cases}-1+2^n, & 2^n+1 \text{ times}\\ -1, & (2^{n-1}+1)(2^{2n}-2) \text{ times}\\ -1+2^{\frac{n+1}{2}}, & (2^{n-2}+2^{l-1})(2^{2n}-2) \text{ times}\\ -1-2^{\frac{n+1}{2}}, & (2^{n-2}-2^{l-1})(2^{2n}-2) \text{ times.}\end{cases}$$

Remark 3.2. $\mathcal{F}^1(k)$ is the modified Gold sequence family given by Rothaus in [36].

For $k=2$, the correlation distribution of $\mathcal{F}^m(2)$ is given [42] as follows

$$\begin{cases}-1+2^n, & 2^{2n}+2^n+1 \text{ times,}\\ -1, & 9\cdot 2^{5n-4}+3\cdot 2^{4n-3}+2^{3n}-9\cdot 2^{2n-3}-3\cdot 2^{n-2}-2 \text{ times}\\ -1+2^{\frac{n+1}{2}}, & \frac{1}{3}\cdot(2^{n-2}+2^{l-1})(5\cdot 2^{4n-1}+2^{3n+2}-5\cdot 2^n-8) \text{ times}\\ -1-2^{\frac{n+1}{2}}, & \frac{1}{3}\cdot(2^{n-2}-2^{l-1})(5\cdot 2^{4n-1}+2^{3n+2}-5\cdot 2^n-8) \text{ times}\\ -1+2^{\frac{n+3}{2}}, & \frac{1}{3}\cdot(2^{n-4}+2^{l-2})(2^{4n-1}-2^{3n}-2^n+2) \text{ times}\\ -1-2^{\frac{n+3}{2}}, & \frac{1}{3}\cdot(2^{n-4}-2^{l-2})(2^{4n-1}-2^{3n}-2^n+2) \text{ times.}\end{cases}$$

3.1.12 Yu and Gong Sequences

Definition 3.12. Let $n=2l+1$ be odd and ρ be a positive integer with $1\leq\rho\leq l$. Then the family $\mathcal{S}_o'(\rho)$ of Yu and Gong [41] is defined by

$$\mathcal{S}_o'(\rho)=\left\{s'^{\Lambda}|\Lambda=\{\lambda_0,\cdots,\lambda_{\rho-1}\},\lambda_i\in\mathbb{F}_{2^n}\right\}$$

where $s'^{\Lambda}=\{s_0'^{\Lambda},s_1'^{\Lambda},\cdots,s_{2^n-2}'^{\Lambda}\}$ is a binary sequence of period 2^n-1.

Note that $s_t'^{\Lambda}=s_{\Lambda}'(\alpha^t)$ for a primitive element α of $\mathbb{F}_{2^n}$, where $s_{\Lambda}'(x)$ is the trace representation of $s_t'^{\Lambda}$, and it is given by:

$$s_{\Lambda}'(x)=s_{\lambda_0,\cdots,\lambda_{\rho-1}}'(x)=Tr(\lambda_0 x)+\sum_{i=1}^{\rho-1}Tr(\lambda_i x^{1+2^i})+\sum_{i=\rho}^{l}Tr(x^{1+2^i}),$$

for $x\in\mathbb{F}_{2^n}^*$.

The Yu and Gong sequence family $\mathcal{S}_o'(\rho)$ has $2^{n\rho}$ cyclically distinct binary sequences of period 2^n-1. The correlation of sequences is $(2\rho+2)$-valued and maximum correlation is $1+2^{\frac{n+2\rho-1}{2}}$.

Particularly when $\rho = 2$, the sequence family is given as follows

$$\mathcal{S}_{o}^{'}(2) = \{s^{'\Lambda} | \Lambda = \{\lambda_0, \lambda_1\}, \lambda_i \in \mathbb{F}_{2^n}\},$$

where

$$s_{\lambda_0,\lambda_1}(x) = Tr(\lambda_0 x) + Tr(\lambda_1 x^3) + \sum_{i=2}^{\frac{n-1}{2}} Tr(x^{1+2^i}),$$

for $x \in \mathbb{F}_{2^n}^*$.

This family $\mathcal{S}_{o}^{'}(2)$ has 2^{2n} cyclically distinct binary sequences of period $2^n - 1$ and the correlation of sequences in this family is six-valued and its maximum correlation magnitude is $1 + 2^{\frac{n+3}{2}}$. The complete correlation distribution of any two sequence in this family is given [41] as follows

$$C_{\Lambda,\Theta}(\tau) = \begin{cases} -1 + 2^n, & 2^{2n} \text{ times} \\ -1, & 2^{2n}(9 \cdot 2^{3n-4} - 3 \cdot 2^{2n-2} \\ & +3 \cdot 2^{n-2} - 1) \text{ times} \\ -1 \pm 2^{\frac{n+1}{2}}, & \frac{1}{3} \cdot 2^{2n} 2^{\frac{n-3}{2}} (2^{\frac{n-1}{2}} \pm 1) \\ & (5 \cdot 2^{2n-1} - 2^n - 5) \text{ times} \\ -1 \pm 2^{\frac{n+3}{2}}, & \frac{1}{3} \cdot 2^{2n} 2^{\frac{n-3}{2}} (2^{\frac{n-3}{2}} \pm 1) \\ & \cdot (2^{n-1} - 1)^2 \text{ times.} \end{cases}$$

Our motivation is to construct a new family of binary sequences with low cross correlation magnitude. We shift the coefficient λ_1 in the construction [41] and cancel $\frac{n-3}{2}$ different polynomials from $\mathcal{S}_{o}^{'}(2)$. We give the detailed definition in the next section.

3.2 Our Sequence Construction

Definition 3.13. Let $n = 3k$ and k be an odd integer with $k \geq 3$. Let $\lambda_0, \lambda_1 \in \mathbb{F}_{2^n}$. Let $\alpha \in \mathbb{F}_{2^n}$ be primitive, $s_t^{\Lambda} = s_{\Lambda}(\alpha^t)$ and s_{Λ} is the trace representation of s_t^{Λ}. Then $s_{\Lambda}(x)$ is defined by

$$s_{\Lambda}(x) = Tr\big(\lambda_0 x\big) + Tr\big(\lambda_1 x^{1+2^{\frac{n-3}{2}}}\big) + Tr\big(x^{1+2^{\frac{n-1}{2}}}\big), \text{ for } x \in \mathbb{F}_{2^n}^*.$$

Theorem 3.3. *Let $n = 3k$, and $k \geq 3$ be an odd integer. The sequence family $\mathcal{U}$ has 2^{2n} binary sequences of period $2^n - 1$. The family has six-valued correlation distribution and its maximum correlation magnitude is $1 + 2^{\frac{n+3}{2}}$.*

Proof. The proof of the correlation values of the sequence family $\mathcal{U}$ is given under 4 main subcases depending on the parameters Λ, Θ and τ. It can be summarized as:

- Case 1: $\tau = 0$ and $\Lambda = \Theta$,

- Case 2: $\tau = 0$ and $\Lambda \neq \Theta$,

- Case 3: $\tau \neq 0$ and $\Lambda = \Theta$,

- Case 4: $\tau \neq 0$ and $\Lambda \neq \Theta$.

Proof of Case 1. Let $\tau = 0$ and $\Lambda = \Theta$, that is $\big(\lambda_0, \lambda_1\big) = \big(\theta_0, \theta_1\big)$. Then, the correlation function is

$$\begin{aligned} C_{\Lambda,\Theta}(\tau) &= \sum_{t=0}^{2^n-2} (-1)^{s_\Lambda(t)+s_\Lambda(t)} \\ &= \sum_{t=0}^{2^n-2} (-1)^0 = 2^n - 1. \end{aligned}$$

□

Proof of Case 2. Let $\tau = 0$ and $\Lambda \neq \Theta$, that is $\big(\lambda_0, \lambda_1\big) \neq \big(\theta_0, \theta_1\big)$. Then, the correlation between $s_\Lambda(t)$ and $s_\Theta(t)$ is given by

$$\begin{aligned} C_{\Lambda,\Theta}(\tau) &= \sum_{t=0}^{2^n-2} (-1)^{s_\Lambda(t)+s_\Theta(t)} \\ &= \sum_{x\in\mathbb{F}_{2^n}^*} (-1)^{\mathcal{A}}, \end{aligned}$$

where

$$\mathcal{A} = Tr\Big[\big(\lambda_0 + \theta_0\big)x + \big(\lambda_1 + \theta_1\big)x^{1+2^{\frac{n-3}{2}}}\Big] \text{ and } \alpha^t = x.$$

Then the symplectic form $B_f(x, y)$ of the quadratic form is

$$B_f(x, y) = Tr\Big[\big(\lambda_1 + \theta_1\big)\big(xy^{2^{\frac{n-3}{2}}} + x^{2^{\frac{n-3}{2}}}y\big)\Big].$$

To find the rank of the quadratic form we need to investigate the roots of the symplectic form which defined as the radical of the quadratic form. The radical $\mathcal{W}$ is the roots of the following polynomial

$$\begin{aligned} W(x) =& \Big[(\lambda_1 + \theta_1)x^{2^{\frac{n-3}{2}}} + (\lambda_1 + \theta_1)^{2^{\frac{n+3}{2}}} x^{2^{\frac{n+3}{2}}}\Big] = 0 \\ =& \Big[\big(\lambda_1 + \theta_1\big)^{2^{\frac{n+3}{2}}} x + \big(\lambda_1 + \theta_1\big)^{2^3} x^{2^3}\Big]^{2^{\frac{n-3}{2}}} = 0. \end{aligned} \tag{3.1}$$

Let $\delta = \lambda_1 + \theta_1$, then equation (3.1) can be written as follows

$$W(x) = \Big[\delta^{2^{\frac{n+3}{2}}} x + \delta^{2^3} x^{2^3}\Big]^{2^{\frac{n-3}{2}}} = 0. \tag{3.2}$$

Then,

$$\delta^{2^{\frac{n+3}{2}}} x + \delta^{2^3} x^{2^3} = 0$$

is solvable if and only if

$$x^{2^3-1} = \delta^{2^{\frac{n+3}{2}} - 2^3}$$

is solvable.

As $n = 3k$ and $k = 2k_1 + 1$, for some positive integer k_1,

$$2^{\frac{n-3}{2}} = 2^{\frac{3k-3}{2}} = 2^{\frac{3(k-1)}{2}} = 2^{\frac{3(2k_1+1-1)}{2}} = (2^3)^{k_1} \equiv 1 \mod 2^3 - 1.$$

We observe that the number of solutions of the radical is $N = 8$ and dim $\mathcal{W} = 3$.

So the correlation values in this case are

$$\{-1, -1 + 2^{\frac{n+3}{2}}, -1 - 2^{\frac{n+3}{2}}\}.$$

□

Proof of Case 3. Let $\tau \neq 0$ and $\Lambda = \Theta$, that is $\big(\lambda_0, \lambda_1\big) = \big(\theta_0, \theta_1\big)$. Then, the correlation between $s_\Lambda(t)$ and $s_\Theta(t)$ is given by

$$\begin{aligned} C_{\Lambda,\Theta}(\tau) &= \sum_{t=0}^{2^n-2} (-1)^{s_\Lambda(t) + s_\Lambda(t+\tau)} \\ &= \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathcal{A}}, \end{aligned}$$

where

$$\mathcal{A} = Tr\Big[\big(\lambda_0 + \lambda_0\beta\big)x + \big(\lambda_1 + \lambda_1\beta^{1+2^{\frac{n-3}{2}}}\big)x^{1+2^{\frac{n-3}{2}}} + \big(1 + \beta^{1+2^{\frac{n-1}{2}}}\big)x^{1+2^{\frac{n-1}{2}}}\Big],$$

$\alpha^t = x$ and $\alpha^\tau = \beta$.

Then, the symplectic form $B_f(x, y)$ is as follows,

$$Tr\Big[\lambda_1\big(1 + \beta^{1+2^{\frac{n-3}{2}}}\big)\big(xy^{2^{\frac{n-3}{2}}} + x^{2^{\frac{n-3}{2}}}y\big) + \big(1 + \beta^{1+2^{\frac{n-1}{2}}}\big)\big(xy^{2^{\frac{n-1}{2}}} + x^{2^{\frac{n-1}{2}}}y\big)\Big].$$

Then the radical $\mathcal{W}$ is the roots of

$$\begin{aligned} W(x) =& \Big[\big(\lambda_1\big)^{2^{\frac{n+3}{2}}} \big(1 + \beta^{1+2^{\frac{n+3}{2}}}\big)x + \big(1 + \beta^{2+2^{\frac{n+3}{2}}}\big)x^2 \\ &+ \big(1 + \beta^{2^2+2^{\frac{n+3}{2}}}\big)x^{2^2} + \big(\lambda_1\big)^{2^3}\big(1 + \beta^{2^3+2^{\frac{n+3}{2}}}\big)x^{2^3}\Big]^{2^{\frac{n-3}{2}}} = 0. \end{aligned} \tag{3.3}$$

Let $B_1 = \big(\lambda_1\big)^{2^{\frac{n+3}{2}}} \big(1+\beta^{1+2^{\frac{n+3}{2}}}\big)$ and $B_2 = \big(1+\beta^{2+2^{\frac{n+3}{2}}}\big)$.

Then the equation (3.3) can be written as

$$W(x) = \Big[B_1 x + B_2 x^2 + B_2^{2^{\frac{n+1}{2}}} x^{2^2} + B_1^{2^{\frac{n+3}{2}}} x^{2^3}\Big]^{2^{\frac{n-3}{2}}} = 0.$$

As dim $\mathcal{W} \leq 3$ and since n is odd and $2r = n - \log_2 N$, where $N = |\mathcal{W}|$, we observe that dim $\mathcal{W} = 1$ or dim $\mathcal{W} = 3$. Therefore correlation values in this case are

$$\{-1, -1 \pm 2^{\frac{n+1}{2}}, -1 \pm 2^{\frac{n+3}{2}}\}.$$

□

Proof of Case 4. Let $\tau \neq 0$ and $\Lambda \neq \Theta$, that is $\big(\lambda_0, \lambda_1\big) \neq \big(\theta_0, \theta_1\big)$. Then, the correlation between $s_\Lambda(t)$ and $s_\Theta(t)$ is given by

$$\begin{aligned} C_{\Lambda,\Theta}(\tau) &= \sum_{t=0}^{2^n-2} (-1)^{s_\Lambda(t)+s_\Theta(t+\tau)} \\ &= \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathcal{A}}, \end{aligned}$$

where $\alpha^\tau = \beta$, $\alpha^t = x$, and

$$\mathcal{A} = Tr\Big[\big(\lambda_0 + \theta_0\beta\big)x + \big(\lambda_1 + \theta_1\beta^{1+2^{\frac{n-3}{2}}}\big)x^{1+2^{\frac{n-3}{2}}} + \big(1+\beta^{1+2^{\frac{n-1}{2}}}\big)x^{1+2^{\frac{n-1}{2}}}\Big].$$

Then, the symplectic form $B_f(x,y)$ of the quadratic form is as follows

$$Tr\Big[\big(\lambda_1 + \theta_1\beta^{1+2^{\frac{n-3}{2}}}\big)\big(xy^{2^{\frac{n-3}{2}}} + x^{2^{\frac{n-3}{2}}}y\big) + \big(1+\beta^{1+2^{\frac{n-1}{2}}}\big)\big(xy^{2^{\frac{n-1}{2}}} + x^{2^{\frac{n-1}{2}}}y\big)\Big].$$

Then, the radical $\mathcal{W}$ is the roots of

$$\begin{aligned} W(x) =& \Bigg[\Big(\lambda_1 + \theta_1\beta^{1+2^{\frac{n-3}{2}}}\Big)x^{2^{\frac{n-3}{2}}} \\ &+ \Big(1+\beta^{1+2^{\frac{n-1}{2}}}\Big)x^{2^{\frac{n-1}{2}}} + \Big(1+\beta^{1+2^{\frac{n+1}{2}}}\Big)x^{2^{\frac{n+1}{2}}} \\ &+ \Big(\big(\lambda_1\big)^{2^{\frac{n+3}{2}}} + \big(\theta_1\big)^{2^{\frac{n+3}{2}}}\beta^{1+2^{\frac{n+3}{2}}}\Big)x^{2^{\frac{n+3}{2}}}\Bigg] = 0. \end{aligned} \tag{3.4}$$

The equation (3.4) can be written as

$$\begin{aligned} W(x) =& \Bigg[\Big(\big(\lambda_1\big)^{2^{\frac{n+3}{2}}} + \big(\theta_1\big)^{2^{\frac{n+3}{2}}}\beta^{1+2^{\frac{n+3}{2}}}\Big)x + \Big(1+\beta^{2+2^{\frac{n+3}{2}}}\Big)x^2 \\ &+ \Big(1+\beta^{2^2+2^{\frac{n+3}{2}}}\Big)x^{2^2} + \Big(\big(\lambda_1\big)^{2^3} + \big(\theta_1\big)^{2^3}\beta^{2^3+2^{\frac{n+3}{2}}}\Big)x^{2^3}\Bigg]^{2^{\frac{n-3}{2}}} = 0. \end{aligned} \tag{3.5}$$

As in Case 3, let

$$B_1 = \left((\lambda_1)^{2^{\frac{n+3}{2}}} + (\theta_1)^{2^{\frac{n+3}{2}}}\beta^{1+2^{\frac{n+3}{2}}}\right) \text{ and } B_2 = \left(1+\beta^{2+2^{\frac{n+3}{2}}}\right).$$

Then the equation (3.5) can be represented as

$$W(x) = \Big[B_1 x + B_2 x^2 + B_2^{2^{\frac{n+1}{2}}} x^{2^2} + B_1^{2^{\frac{n+3}{2}}} x^{2^3}\Big]^{2^{\frac{n-3}{2}}}. \tag{3.6}$$

We observe that, dim $\mathcal{W} \leq 3$. Since n is odd and $2r = n-$ dim $\mathcal{W}$, dim $\mathcal{W} = 1$ or dim $\mathcal{W} = 3$. Therefore correlation values in this case are

$$\{-1, -1 \pm 2^{\frac{n+1}{2}}, -1 \pm 2^{\frac{n+3}{2}}\}.$$

$\square$

Collecting all cases together we proved that the correlation of our sequence family is six-valued and it takes the values $\{-1, -1+2^n, -1 \pm 2^{\frac{n+1}{2}}, -1 \pm 2^{\frac{n+3}{2}}\}$. Thus its maximum correlation magnitude $C_{max} = 1 + 2^{\frac{n+3}{2}}$. $\square$

3.2.1 Examples

In this section, for $n = 9$ and $n = 15$ we compute the correlation values of this sequence family.

Example 1. Let $n = 9$. Then

$$s_\Lambda(x) = Tr(\lambda_0 x) + Tr(\lambda_1 x^{1+2^3}) + Tr(x^{1+2^4}).$$

We will investigate the correlation of a pair sequences.

Let

$$s_\Theta(x) = Tr(\theta_0 x) + Tr(\theta_1 x^{1+2^3}) + Tr(x^{1+2^4}).$$

There are 4 cases:

Case 1.

Let $\Lambda = \Theta$ and $\tau = 0$. Then,

$$\begin{aligned} C_{\Lambda,\Theta}(\tau) = C_{\Lambda,\Lambda}(0) &= \sum_{t=0}^{2^n-2}(-1)^{s_\Lambda(t)+s_\Lambda(t)} \\ &= \sum_{t=0}^{2^n-2}(-1)^0 \\ &= 2^n - 1 = 2^9 - 1 \\ &= 511. \end{aligned}$$

Case 2: Let $\Lambda \neq \Theta$ and $\tau = 0$. Then,

$$\begin{aligned} C_{\Lambda,\Theta}(\tau) = C_{\Lambda,\Theta}(0) &= \sum_{t=0}^{2^n-2} (-1)^{s_\Lambda(t)+s_\Theta(t)} \\ &= \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathcal{A}}, \end{aligned}$$

where

$$\mathcal{A} = Tr\Big[\big(\lambda_0 + \theta_0\big)x + \big(\lambda_1 + \theta_1\big)x^{1+2^3}\Big] \text{ and } \alpha^t = x.$$

The symplectic form $B_f(x, y)$ of the quadratic form is given as follows

$$B_f(x, y) = Tr\Big[\big(\lambda_1 + \theta_1\big)\big(xy^{2^3} + x^{2^3}y\big)\Big].$$

Then the radical $\mathcal{W}$ is the roots of

$$W(x) = \Big[\big(\lambda_1 + \theta_1\big)x^{2^3} + \big(\lambda_1 + \theta_1\big)^{2^6} x^{2^6}\Big] = 0. \tag{3.7}$$

The equation (3.7) can be written as

$$W(x) = \Big[\big(\lambda_1 + \theta_1\big)^{2^6} x + \big(\lambda_1 + \theta_1\big)^{2^3} x^{2^3}\Big]^{2^3} = 0. \tag{3.8}$$

Let $\delta = \lambda_1 + \theta_1$, then equation (3.8) can be written as follows

$$W(x) = \Big[\delta^{2^6} x + \delta^{2^3} x^{2^3}\Big]^{2^3} = 0. \tag{3.9}$$

Then,

$$\delta^{2^6} x + \delta^{2^3} x^{2^3} = 0$$

is solvable if and only if

$$x^{2^3-1} = \delta^{2^6-2^3}$$

is solvable.

Clearly, number of solutions of the radical is $N = 8$ and dim $\mathcal{W} = 3$. Thus, the correlation values in this case are

$$\{-1, -1 + 2^6, -1 - 2^6\} = \{-1, 63, -65\}$$

Case 3: Let $\Lambda = \Theta$ and $\tau \neq 0$. Then,

$$\begin{aligned} C_{\Lambda,\Theta}(\tau) = C_{\Lambda,\Lambda}(\tau) &= \sum_{t=0}^{2^n-2} (-1)^{s_\Lambda(t)+s_\Lambda(t+\tau)} \\ &= \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathcal{A}}, \end{aligned}$$

where

$$\mathcal{A} = Tr\Big[\big(\lambda_0 + \lambda_0\beta\big)x + \big(\lambda_1 + \lambda_1\beta^{1+2^3}\big)x^{1+2^3} + \big(1 + \beta^{1+2^4}\big)x^{1+2^4}\Big].$$

Then, the symplectic form $B_f(x, y)$ of the quadratic form is computed as follows

$$B_f(x,y) =tr\Big[(\lambda_1)(1+\beta^{1+2^3})(xy^{2^3}+x^{2^3}y)+(1+\beta^{1+2^4})(xy^{2^4}+x^{2^4}y)\Big].$$

Then to find the dimension of $\mathcal{W}$, we need to investigate the roots of the following polynomial $W(x)$ defined by

$$\begin{aligned} W(x) =&\Big[(\lambda_1)(1+\beta^{1+2^3})x^{2^3}+(1+\beta^{1+2^4})x^{2^4} \\ &+(1+\beta^{1+2^5})x^{2^5}+(\lambda_1)^{2^6}(1+\beta^{1+2^6})x^{2^6}\Big]=0. \end{aligned} \tag{3.10}$$

The equation (3.10) can be written as follows,

$$\begin{aligned} W(x) = &\Big[\big(\lambda_1\big)^{2^6}\big(1+\beta^{1+2^6}\big)x+\big(1+\beta^{2+2^6}\big)x^2 \\ &+\big(1+\beta^{2^2+2^6}\big)x^{2^2}+\big(\lambda_1\big)^{2^3}\big(1+\beta^{2^3+2^6}\big)x^{2^3}\Big]^{2^3}=0. \end{aligned} \tag{3.11}$$

Let $B_1 = \big(\lambda_1\big)^{2^6}\big(1+\beta^{1+2^6}\big)$ and $B_2 = \big(1+\beta^{2+2^6}\big)$.

Then the equation (3.11) can be written as

$$W(x) = \Big[B_1x+B_2x^2+B_2^{2^5}x^{2^2}+B_1^{2^6}x^{2^3}\Big]^{2^3}=0.$$

It is clear that dim $\mathcal{W} \leq 3$ and since $n = 9$ is odd and $2r = n - \log_2 N = 9 - \log_2 N$, where $N = |\mathcal{W}|$, it is clearly seen that dim $\mathcal{W} = 1$ or dim $\mathcal{W} = 3$. Therefore correlation values in this case are

$$\{-1, -1+2^5, -1-2^5, -1+2^6, -1-2^6\} = \{-1, 31, -33, 63, -65\}.$$

Case 4: Let $\Lambda \neq \Theta$ and $\tau \neq 0$. Then,

$$\begin{aligned} C_{\Lambda,\Theta}(\tau) = C_{\Lambda,\Theta}(\tau) &= \sum_{t=0}^{2^n-2}(-1)^{s_\Lambda(t)+s_\Theta(t+\tau)} \\ &= \sum_{x\in\mathbb{F}_{2^n}^*}(-1)^{\mathcal{A}}, \end{aligned}$$

where

$$\mathcal{A} = Tr\Big[\big(\lambda_0+\theta_0\beta\big)x+\big(\lambda_1+\theta_1\beta^{1+2^3}\big)x^{1+2^3}+\big(1+\beta^{1+2^4}\big)x^{1+2^4}\Big].$$

Then, the symplectic form $B_f(x, y)$ of the quadratic form is as follows

$$B_f(x,y) = Tr\Big[\big(\lambda_1+\theta_1\beta^{1+2^3}\big)\big(xy^{2^3}+x^{2^3}y\big)+\big(1+\beta^{1+2^4}\big)\big(xy^{2^4}+x^{2^4}y\big)\Big].$$

Moreover, by finding the roots of the following polynomial $W(x)$ the dimension of the radical can be computed. $W(x)$ is defined by

$$\begin{aligned} W(x) = \Big[&\big(\lambda_1 + \theta_1 \beta^{1+2^3}\big)x^{2^3} + \big(1+\beta^{1+2^4}\big)x^{2^4} \\ &+ \big(1+\beta^{1+2^5}\big)x^{2^5} + \big((\lambda_1)^{2^6} + (\theta_1)^{2^6}\beta^{1+2^6}\big)x^{2^6}\Big] = 0. \end{aligned} \tag{3.12}$$

The equation (3.12) can be written as follows

$$\begin{aligned} W(x) = \Big[&\big((\lambda_1)^{2^6} + (\theta_1)^{2^6}\beta^{1+2^6}\big)x + \big(1+\beta^{2+2^6}\big)x^2 \\ &+ \big(1+\beta^{2^2+2^6}\big)x^{2^2} + \big((\lambda_1)^{2^3} + (\theta_1)^{2^3}\beta^{2^3+2^6}\big)x^{2^3}\big)\Big]^{2^3} = 0. \end{aligned} \tag{3.13}$$

Let $B_1 = \big((\lambda_1)^{2^6} + (\theta_1)^{2^6}\beta^{1+2^6}\big)$ and $B_2 = \big(1+\beta^{2+2^6}\big)$.

Then the equation (3.13) can be written as

$$W(x) = \Big[B_1 x + B_2 x^2 + B_2^{2^5} x^{2^2} + B_1^{2^6} x^{2^3}\Big]^{2^3} = 0.$$

It is clear that dim $\mathcal{W} \leq 3$ and since $n = 9$ is odd and $2r = n - \log_2 N = 9 - \log_2 N$, where $N = |\mathcal{W}|$, we observe that dim $\mathcal{W} = 1$ or dim $\mathcal{W} = 3$. Thus correlation values in this case are

$$\{-1, -1+2^5, -1-2^5, -1+2^6, -1-2^6\} = \{-1, 31, -33, 63, -65\}.$$

Example 2.

Let $n = 15$. Then $s_\Lambda(x)$ is given as follows

$$s_\Lambda(x) = Tr(\lambda_0 x) + Tr(\lambda_1 x^{1+2^6}) + Tr(x^{1+2^7}), \text{ for } x \in \mathbb{F}_{2^{15}}.$$

We will investigate the correlation of a pair sequences. Let

$$s_\Theta(x) = Tr(\theta_0 x) + Tr(\theta_1 x^{1+2^6}) + Tr(x^{1+2^7}).$$

There are 4 cases:

Case 1: Let $\Lambda = \Theta$ and $\tau = 0$. Then,

$$\begin{aligned} C_{\Lambda,\Theta}(\tau) = C_{\Lambda,\Lambda}(0) &= \sum_{t=0}^{2^n-2} (-1)^{s_\Lambda(t)+s_\Lambda(t)} \\ &= \sum_{t=0}^{2^n-2} (-1)^0 \\ &= 2^n - 1 = 2^{15} - 1 \\ &= 32767. \end{aligned}$$

Case 2: Let $\Lambda \neq \Theta$ and $\tau = 0$. Then,

$$\begin{aligned} C_{\Lambda,\Theta}(\tau) = C_{\Lambda,\Theta}(0) &= \sum_{t=0}^{2^n-2} (-1)^{s_\Lambda(t)+s_\Theta(t)} \\ &= \sum_{x\in\mathbb{F}^*_{2^n}} (-1)^{\mathcal{A}}, \end{aligned}$$

where

$$\mathcal{A} = Tr\Big[\big(\lambda_0+\theta_0\big)x + \big(\lambda_1+\theta_1\big)x^{1+2^6}\Big].$$

The symplectic form $B_f(x,y)$ of the quadratic form is as follows

$$B_f(x,y) = Tr\big[\big(\lambda_1+\theta_1\big)\big(xy^{2^6}+x^{2^6}y\big)\big].$$

Then the radical is the roots of the polynomial

$$\begin{aligned} W(x) &= \Big[\big(\lambda_1+\theta_1\big)x^{2^6} + \big(\lambda_1+\theta_1\big)^{2^9}x^{2^9}\Big] = 0 \\ &= \Big[\big(\lambda_1+\theta_1\big)^{2^9}x + \big(\lambda_1+\theta_1\big)^{2^3}x^{2^3}\Big]^{2^6} = 0. \end{aligned} \tag{3.14}$$

Let $\delta = \lambda_1 + \theta_1$, then equation (3.14) can be written as follows

$$W(x) = \Big[\delta^{2^9}x + \delta^{2^3}x^{2^3}\Big]^{2^6} = 0. \tag{3.15}$$

Then,

$$\delta^{2^9}x + \delta^{2^3}x^{2^3} = 0$$

is solvable if and only if

$$x^{2^3-1} = \delta^{2^9-2^3}$$

is solvable.

Clearly, number of solutions of the radical is $N = 8$ and dim $\mathcal{W} = 3$. Thus, the correlation values in this case are

$$\{-1, -1+2^9, -1-2^9\} = \{-1, 511, -513\}.$$

Case 3: Let $\Lambda = \Theta$ and $\tau \neq 0$. Then, the correlation between $s_\Lambda(t)$ and $s_\Theta(t)$ is given by

$$\begin{aligned} C_{\Lambda,\Theta}(\tau) = C_{\Lambda,\Lambda}(\tau) &= \sum_{t=0}^{2^n-2} (-1)^{s_\Lambda(t)+s_\Lambda(t+\tau)} \\ &= \sum_{x\in\mathbb{F}^*_{2^{15}}} (-1)^{\mathcal{A}}, \end{aligned}$$

where,

$$\mathcal{A} = Tr\Big[\big(\lambda_0+\lambda_0\beta\big)x + \big(\lambda_1+\lambda_1\beta^{1+2^6}\big)x^{1+2^6} + \big(1+\beta^{1+2^7}\big)x^{1+2^7}\Big].$$

Then, the symplectic form $B_f(x,y)$ of the quadratic form is given by

$$Tr\Big[\big(\lambda_1\big)\big(1+\beta^{1+2^6}\big)\big(xy^{2^6}+x^{2^6}y\big)+\big(1+\beta^{1+2^7}\big)\big(xy^{2^7}+x^{2^7}y\big)\Big].$$

Furthermore to determine the dimension of the radical the roots of the following polynomial $W(x)$ is computed.

$$\begin{aligned} W(x) = \Big[&\big(\lambda_1\big)\big(1+\beta^{1+2^6}\big)x^{2^6}+\big(1+\beta^{1+2^7}\big)x^{2^7} \\ &+\big(\lambda_1\big)^{2^9}\big(1+\beta^{1+2^9}\big)x^{2^9}+\big(1+\beta^{1+2^8}\big)x^{2^8}\Big]=0. \end{aligned} \tag{3.16}$$

The equation (3.16) can be written as follows,

$$\begin{aligned} W(x) = \Big[&\big(\lambda_1\big)^{2^9}\big(1+\beta^{1+2^9}\big)x+\big(1+\beta^{2+2^9}\big)x^2 \\ &+\big(1+\beta^{2^2+2^9}\big)x^{2^2}+\big(\lambda_1\big)^{2^3}\big(1+\beta^{2^3+2^9}\big)x^{2^3}\Big]^{2^6}=0. \end{aligned}$$

Let $B_1=\big(\lambda_1\big)^{2^9}\big(1+\beta^{1+2^9}\big)$ and $B_2=\big(1+\beta^{2+2^9}\big)$.

Then the equation (3.16) can be written as

$$W(x)=\Big[B_1x+B_2x^2+B_2^{2^8}x^{2^2}+B_1^{2^9}x^{2^3}\Big]^{2^6}=0.$$

We observe that the number of the element of the radical is $N=8$. As $\dim\mathcal{W}\leq 3$ and since $n=15$ is odd and $2r=n-\log_2 N=15-\log_2 8$, $\dim\mathcal{W}=1$ or $\dim\mathcal{W}=3$. Therefore correlation values in this case are

$$\{-1,-1+2^8,-1-2^8,-1+2^9,-1-2^9\}=\{-1,127,-129,511,-513\}.$$

Case 4: Let $\Lambda\neq\Theta$ and $\tau\neq 0$. Then, the correlation between $s_\Lambda(t)$ and $s_\Theta(t)$ is given by

$$\begin{aligned} C_{\Lambda,\Theta}(\tau) &= \sum_{t=0}^{2^n-2}(-1)^{s_\Lambda(t)+s_\Theta(t+\tau)} \\ &= \sum_{x\in\mathbb{F}_{2^{15}}^*}(-1)^{\mathcal{A}}, \end{aligned}$$

where,

$$\mathcal{A}=Tr\big[\big(\lambda_0+\theta_0\beta\big)x+\big(\lambda_1+\theta_1\beta^{1+2^6}\big)x^{1+2^6}+(1+\beta^{1+2^7})x^{1+2^7}\big].$$

Then, the symplectic form of the quadratic form is given by

$$B_f(x,y)=Tr\Big[\big(\lambda_1+\theta_1\beta^{1+2^6}\big)\big(xy^{2^6}+x^{2^6}y\big)+\big(1+\beta^{1+2^7}\big)\big(xy^{2^7}+x^{2^7}y\big)\Big].$$

Then, the radical $\mathcal{W}$ is the roots of

$$W(x) = \Big[\big(\lambda_1 + \theta_1\beta^{1+2^6}\big)x^{2^6} + \big(1 + \beta^{1+2^7}\big)x^{2^7} \\ + \big((\lambda_1)^{2^9} + (\theta_1)^{2^9}\beta^{1+2^9}\big)x^{2^9} + \big(1 + \beta^{1+2^8}\big)x^{2^8}\Big] = 0. \tag{3.17}$$

Then, the equation (3.17) can be written as follows

$$W(x) = \Big[\big((\lambda_1)^{2^9} + (\theta_1)^{2^9}\beta^{1+2^9}\big)x + \big(1 + \beta^{2+2^9}\big)x^2 \\ + \big(1 + \beta^{2^2+2^9}\big)x^{2^2} + \big((\lambda_1)^{2^3} + (\theta_1)^{2^3}\beta^{2^3+2^9}\big)x^{2^3}\Big]^{2^6} = 0. \tag{3.18}$$

As in Case 3, let

$$B_1 = \Big((\lambda_1)^{2^9} + (\theta_1)^{2^9}\beta^{1+2^9}\Big) \text{ and } B_2 = \Big(1 + \beta^{2+2^9}\Big).$$

Then the equation (3.18) can be represented as

$$W(x) = \Big[B_1x + B_2x^2 + B_2^{2^8}x^{2^2} + B_1^{2^9}x^{2^3}\Big]^{2^6} = 0. \tag{3.19}$$

It is easily seen that the number of the element of the radical is $N = 8$. As dim $\mathcal{W} \leq 3$ and since $n = 15$ is odd and $2r = n - \log_2 N = 15 - \log_2 8$, dim $\mathcal{W} = 1$ or dim $\mathcal{W} = 3$. Therefore correlation values in this case are

$$\{-1, -1 + 2^8, -1 - 2^8, -1 + 2^9, -1 - 2^9\} = \{-1, 127, -129, 511, -513\}.$$

Remark 3.3. For $n = 9$ and $n = 15$ the correlation values of the sequence family are computed using the programming language Magma and explained in this chapter properly.

3.3 Comparison

In the previous section we introduced some of the known sequence families with low cross correlation magnitude. Then we briefly explained our construction of a binary sequence family for odd n of the form $n = 3k$ where $k \geq 3$ is an odd integer. The correlation values of this family are computed. In Table 3.1 we give a proper comparison of properties of these sequence families.

Comparing to the known sequence families, our sequence family has good cross correlation properties. Our family is constructed by shifting the second coefficient in the construction [41] and deleting $\frac{n-3}{2}$ polynomials. We note that although the correlation values of our sequence family $\mathcal{U}$ are equal to the correlation values of the sequence family $\mathcal{S}_o^{'}(2)$ of Yu and Gong, our sequence family works faster in applications. For example, in order to obtain a value of a sequence in family $\mathcal{S}_o^{'}(2)$ of Yu and Gong, it is necessary to evaluate $\frac{n+1}{2}$ traces of $\frac{n+1}{2}$ values in $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ in general. However in our family, a value of a sequence is obtained by evaluating only 3 traces of 3 values in $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.

After a referee review, we found out that our sequence family is a subfamily of the Modified Gold sequences [36]. The correlation distribution of this family is given later by Zhou and Tang, and our family is a special condition of this family. Detailed information about this sequence family can be found in [42].

Table 3.1: Comparison of some known sequence families and their maximum correlation magnitudes

p	n	Family	Family Size	Period	C_{max}
2	odd	Gold	$2^n + 1$	$2^n - 1$	$1 + 2^{\frac{n+1}{2}}$
2	even	Gold	$2^n + 1$	$2^n - 1$	$1 + 2^{\frac{n+2}{2}}$
2	even	Small Kasami	$2^{\frac{n}{2}}$	$2^n - 1$	$1 + 2^{\frac{n}{2}}$
2	even	Udaya	$2^n + 1$	$2^n - 1$	$1 + 2^{\frac{n}{2}+1}$
2	even	Bent	$2^{\frac{n}{2}}$	$2^n - 1$	$1 + 2^{\frac{n}{2}}$
2	odd	Chang et al.	2^{2n}	$2^n - 1$	$1 + 2^{\frac{n+3}{2}}$
p	$k < p$	Sidelnikov	$\geq p^{n(k-1)}$	$p^n - 1$	$1 + (k-1)p^{\frac{n}{2}}$
2	even	No	$2^{\frac{n}{2}}$	$2^n - 1$	$1 + 2^{\frac{n}{2}}$
p	odd	Kumar-Moreno	$p^{\frac{n}{2}}$	$p^n - 1$	$1 + p^{\frac{n}{2}}$
2	odd	Gold-like	$2^n + 1$	$2^n - 1$	$1 + 2^{\frac{n+1}{2}}$
2	m odd	Kim-No	$2^n + 1$	$2^n - 1$	$1 + 2^{\frac{n+e}{2}}$
2	n, m odd	Tang et al.	$2^n + 1$	$2^n - 1$	$1 + 2^{\frac{n+1}{2}}$
2	odd	Modified Gold	$2^{2n} + 2^n + 1$	$2^n - 1$	$1 + 2^{\frac{n+3}{2}}$
2	odd	Yu-Gong	$2^{n\rho}$	$2^n - 1$	$1 + 2^{\frac{n+2\rho-1}{2}}$
2	even	Yu-Gong	$2^{n\rho}$	$2^n - 1$	$1 + 2^{\frac{n}{2}+\rho}$
2	odd	G. Modified Gold	$\sum\limits_{i=0}^{k} 2^{in}$	$2^n - 1$	$1 + 2^{l+k}$
2	odd	Our family	2^{2n}	$2^n - 1$	$1 + 2^{\frac{n+3}{2}}$

CHAPTER 4

CONCLUSION

CDMA systems use the spread spectrum technique known as direct sequence spread spectrum. This system has some advantages compared to the other technologies and it has been used in many systems such as cellular telecommunications systems and radar systems. CDMA systems permit several parties to share a single channel and more users to connect at any time. In this system a single channel is divided into several parts through the use of unique codes.

A family of sequences with great correlation specialities has critical roles both in CDMA systems and cryptography. There are several areas of use of these sequences. In CDMA communication systems sequences with low cross correlation are used. Therefore, in this thesis we focus on sequence families with low maximum cross correlation magnitude.

In Chapter 1, we give the historical and theoretical background on spread spectrum technology and multiple access systems. We give an extensive introduction the these techniques. The importance of pseudorandom sequences and research areas in these subjects are described and briefly explained.

In Chapter 2, we introduce the theory of finite fields and quadratic forms. We give necessary definitions and concepts of sequences. Also we mention the properties of sequences, family of sequences and quadratic forms.

In Chapter 3, we introduce certain known families of sequences with low maximum cross correlation magnitude for both odd and even n. Then we construct a family of binary sequences with low maximum cross correlation magnitude. Our aim is to design a sequence family with low cross correlation and for this purpose we studied the family $\mathcal{S}_{\mathrm{o}}^{'}(\rho)$ given by Yu and Gong in [41]. The correlation values of this family $\mathcal{S}_{\mathrm{o}}^{'}(\rho)$ depends on the parameter ρ. It gives flexibility for specific applications and for $\rho = 1$ this family corresponds to the Gold-like sequences constructed by Boztas and Kumar [3]. Moreover when $\rho = 2$, this family has 2^{2n} cyclically distinct sequences and the cross correlation of this family is six-valued and it takes the values $\{-1, -1 + 2^n, -1 \pm 2^{\frac{n+1}{2}}, -1 \pm 2^{\frac{n+3}{2}}\}$. In this case, the family consists of the sums of $\frac{n+1}{2}$ different polynomials depending on n.

In our design, the family $\mathcal{U}$ is constructed when n is and odd integer of the form

$n = 3k$ and k is also an odd integer. Our sequence family is constructed by shifting the coefficient λ_1 in the construction [41] and deleting the $\frac{n-3}{2}$ different polynomials from $\mathcal{S}_{\text{o}}^{'}(2)$. This family has six-valued correlation and its maximum correlation magnitude is $1 + 2^{\frac{n+3}{2}}$. This family consists of the sums of only three different polynomials for all positive integer $n = 3k$. Thus, when compared to Yu-Gong family $\mathcal{S}_{\text{o}}^{'}(2)$ our construction works faster in applications.

However, after a referee review we found out that our family is a subfamily of the modified Gold sequences given by Rothaus in [36]. The correlation distribution of this family is given by Zhou and Tang in [42] for some specific parameters.

Finally we compare the family sizes and maximum correlation magnitudes of all given sequence families in Table 3.1.

REFERENCES

[1] R. Barker, Group syncronization of binary digital systems, Communication theory, pp. 273–287, 1953.

[2] E. R. Berlekamp, Algebraic coding theory, 1968.

[3] S. Boztaş and P. V. Kumar, Binary sequences with Gold-like correlation but larger linear span, IEEE Transactions on Information Theory, 40(2), pp. 532–537, 1994.

[4] S. Boztaş, F. Özbudak, and E. Tekin, Correlation distribution of a new sequence family, in *2015 IEEE International Symposium on Information Theory (ISIT)*, pp. 2707–2711, June 2015, ISSN 2157-8095.

[5] S. Boztaş, F. Özbudak, and E. Tekin, Generalized nonbinary sequences with perfect autocorrelation, flexible alphabets and new periods, Cryptography and Communications, pp. 1–9, 2017.

[6] T. W. Cusick and G. Gong, A conjecture on binary sequences with the “trinomial property”, IEEE Transactions on Information Theory, 47(1), pp. 426–427, 2001.

[7] J. F. Dillon and H. Dobbertin, New cyclic difference sets with singer parameters, Finite Fields and Their Applications, 10(3), pp. 342–389, 2004.

[8] M. Golay, Complementary series, IRE Transactions on Information Theory, 7(2), pp. 82–87, 1961.

[9] R. Gold, Optimal binary sequences for spread spectrum multiplexing (corresp.), IEEE Transactions on Information Theory, 13(4), pp. 619–621, October 1967, ISSN 0018-9448.

[10] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.), IEEE Transactions on Information Theory, 14(1), pp. 154–156, Jan 1968, ISSN 0018-9448.

[11] S. W. Golomb, *Shift Register Sequences*, Aegean Park Press, 1967.

[12] S. W. Golomb and G. Gong, Periodic binary sequences with the “trinomial property”, IEEE Transactions on Information Theory, 45(4), pp. 1276–1279, 1999.

[13] S. W. Golomb and G. Gong, *Signal design for good correlation: for wireless communication, cryptography, and radar*, Cambridge University Press, 2005.

[14] G. Gong, New designs for signal sets with low cross correlation, balance property, and large linear span: Gf (p) case, IEEE Transactions on Information Theory, 48(11), pp. 2847–2867, 2002.

[15] G. Gong and S. W. Golomb, Binary sequences with two-level autocorrelation, IEEE Transactions on Information Theory, 45(2), pp. 692–693, 1999.

[16] B. Gordon, W. Mills, and L. Welch, Some new difference sets, Canad. J. Math, 14(614-625), p. 265, 1962.

[17] M. Hall, A survey of difference sets, Proceedings of the American Mathematical Society, 7(6), pp. 975–986, 1956.

[18] T. Helleseth and G. Gong, New nonbinary sequences with ideal two-level autocorrelation, IEEE Transactions on Information Theory, 48(11), pp. 2868–2872, 2002.

[19] T. Helleseth and P. V. Kumar, Sequences with low correlation, Handbook of coding theory, 2, pp. 1765–1853, 1998.

[20] V. P. Ipatov, *Spread spectrum and CDMA: principles and applications*, John Wiley & Sons, 2005.

[21] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, volume 84, Springer Science & Business Media, 2013.

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

[23] T. Kasami, The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes, Information and Control, 18(4), pp. 369–394, 1971.

[24] S.-H. Kim and J.-S. No, New families of binary sequences with low correlation, IEEE Transactions on Information Theory, 49(11), pp. 3059–3065, 2003.

[25] 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, 1991.

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

[27] J. Massey, Shift-register synthesis and BCH decoding, IEEE transactions on Information Theory, 15(1), pp. 122–127, 1969.

[28] W. Meier and O. Staffelbach, Fast correlation attacks on certain stream ciphers, Journal of Cryptology, 1(3), pp. 159–176, 1989.

[29] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*, CRC press, 1996.

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

[31] J.-S. No, H. Chung, and M.-S. Yun, Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$, IEEE Transactions on Information Theory, 44(3), pp. 1278–1282, 1998.

[32] J.-S. No, S. Golomb, G. Gong, H. Lee, and P. Gaal, Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation, IEEE Trans. Inf. Theory, 44(2), pp. 814–817, 1998.

[33] J.-S. No and P. V. Kumar, A new family of binary pseudorandom sequences having optimal periodic correlation properties and larger linear span, IEEE Transactions on Information Theory, 35(2), pp. 371–379, 1989.

[34] J. Olsen, R. Scholtz, and L. Welch, Bent-function sequences, IEEE Transactions on Information Theory, 28(6), pp. 858–864, 1982.

[35] O. S. Rothaus, On bent functions, Journal of Combinatorial Theory, Series A, 20(3), pp. 300–305, 1976.

[36] O. S. Rothaus, Modified Gold codes, IEEE transactions on information theory, 39(2), pp. 654–656, 1993.

[37] J. Seberry and M. Yamada, Hadamard matrices, sequences, and block designs, Contemporary design theory: a collection of surveys, pp. 431–560, 1992.

[38] V. M. Sidel'nikov, Some k-valued pseudo-random sequences and nearly equidistant codes, Problemy Peredachi Informatsii, 5(1), pp. 16–22, 1969.

[39] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, Spread spectrum communications handbook, 1994.

[40] X. Tang, T. Helleseth, L. Hu, and W. Jiang, A new family of Gold-like sequences, Sequences, Subsequences, and Consequences, pp. 62–69, 2007.

[41] N. Y. Yu and G. Gong, A new binary sequence family with low correlation and large size, IEEE transactions on information theory, 52(4), pp. 1624–1636, 2006.

[42] Z. Zhou and X. Tang, Generalized modified Gold sequences, Designs, Codes and Cryptography, 60(3), pp. 241–253, 2011.