SEQUENCE FAMILIES WITH GOOD CORRELATION DISTRIBUTION

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

BY

EDA TEKİN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
CRYPTOGRAPHY

OCTOBER 2016

Approval of the thesis:

SEQUENCE FAMILIES WITH GOOD CORRELATION DISTRIBUTION

submitted by **EDA TEKİN** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy 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** _____

Examining Committee Members:

Prof. Dr. Ferruh Özbudak
Cryptography, METU _____

Assoc. Prof. Dr. Ali Doğanaksoy
Cryptography, METU _____

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

Assoc. Prof. Dr. Sedat Akleylek
Computer Engineering, Ondokuz Mayıs University _____

Assist. Prof. Dr. Burcu Gülmez Temür
Mathematics, Atılım 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: EDA TEKİN

Signature :

ABSTRACT

SEQUENCE FAMILIES WITH GOOD CORRELATION DISTRIBUTION

Tekin, Eda
Ph.D., Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak

October 2016, 74 pages

In this thesis we focus on two main properties of sequences which have wide range of applications in code division multiple access: autocorrelation and cross-correlation. First, necessary properties of sequences, some known perfect autocorrelation sequences and some known sequence families with their cross-correlation properties are given. Then, a perfect autocorrelation sequence [18] is generalized with respect to a number theoretic constraint of n for a given prime power q. This generalization enables the designers to have more flexibility in terms of the deployment of these sequences.

Later, a sequence family with low maximum correlation magnitude is constructed for an arbitrary even positive integer n and its correlation distribution is given. Gold-like sequence family [6] is generalized depending on a plateaued function $f(x)$, for all possible p and n values and its correlation values are obtained. Finally, using Gold function as $f(x)$, the generalized family's correlation distribution is given depending on p and n.

Keywords: Sequences, autocorrelation, cross-correlation, code division multiple access, spread spectrum, wireless communications

ÖZ

İYİ KORELASYON DAĞILIMLI DİZİ AİLELERİ

Tekin, Eda
Doktora, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak

Ekim 2016, 74 sayfa

Bu tezde kod bölmeli çoklu erişimde yaygın uygulamaları olan dizilerin iki temel özelliğine odaklandık: otokorelasyon ve çapraz korelasyon. İlk olarak, dizilerin gerekli özellikleri, bilinen bazı ideal otokorelasyon dizileri ve bilinen bazı dizi aileleri ile bu ailelerin çapraz korelasyonları verilmiştir. Sonra bir ideal otokorelasyon dizisi [18], verilen bir üstel q asal sayısı için n üzerinde bir dizi teorik şarta bağlı olarak genelleştirilmiştir. Bu genelleştirme, tasarımcıların bu dizilerin kullanımı açısından daha fazla esneklik kazanmasına olanak sağlamaktadır.

Daha sonra, verilen bir n çift tam sayısı için, düşük maksimum korelasyon değerine sahip bir dizi ailesi inşa edilip bu ailenin korelasyon dağılımı verilmiştir. Gold-like dizi ailesi [6], $f(x)$ plato fonksiyonuna bağlı olarak, tüm olası p ve n değerleri için genelleştirilmiştir ve ailenin korelasyon değerleri hesaplanmıştır. Son olarak, $f(x)$ fonksiyonunu Gold fonksiyonu alarak, bu genelleştirilmiş dizi ailesinin korelasyon dağılımı p ve n değerlerine bağlı olarak verilmiştir.

Anahtar Kelimeler: Diziler, otokorelasyon, çapraz korelasyon, kod bölmeli çoklu erişim, yayılı spektrum, kablosuz iletişim

To my beloved husband Kubilay

ACKNOWLEDGMENTS

I would like to express my sincere appreciation to my supervisor Prof. Dr. Ferruh Özbudak, for his guidance, support and sharing his knowledge and valuable thoughts with me through my graduate study. I would like to thank for his willingness to give his time and to share his experience in all stages of this study. This work could not have been possible without his supervision.

I am very greatful to Assoc. Dr. Serdar Boztaş for his valuable comments and ideas on this work. His suggestions have improved this work. I also would like to thank members of my thesis committee: Assoc. Prof. Dr. Ali Doğanaksoy, Assoc. Prof. Dr. Murat Cenk, Assoc. Prof. Dr. Sedat Akleylek and Assist. Prof. Dr. Burcu Gülmez Temür.

I would like to give special thanks to Prof. Dr. Ersan Akyıldız, Prof. Dr. Bülent Karasözen, Assoc. Prof. Dr. Sevtap Kestel and Mrs. Nejla Erdoğdu for their guidance, kindness, help and support.

I wish to thank all my friends, especially Kamil Otal, Pınar Çomak and Bükre Yıldırım, and all members of the Institute of Applied Mathematics for their encouragement, support and friendship.

I greatfully acknowledge for the financial support of TUBITAK BIDEB 2214-A Program for ensuring me to visit Royal Melbourne Institute of Technology, Australia during my Ph.D. studies.

In addition, I would like to express my gratitude to my family for their believing in me throughout this thesis despite being far away from me.

Lastly, for my husband Kubilay, words are not enough to convey my appreciation for his perpetual support, patience and understanding which have carried me through to the conclusion of this work.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

$\mathbb{F}_q$	Finite Field with q Elements
p	Prime Number
q	Prime Power
r	Rank
Tr	Trace Function
ζ_p	Complex Primitive p-th Root of Unity
$W_f(\lambda)$	Walsh Transform
$B\left(x,y\right)$	Symplectic Form
$\mathcal{W}$	Radical
$C_{u,v}\left(\tau\right)$	Cross-correlation Function
$C_{\max}$	Maximum Correlation Magnitude
$R_u\left(\tau\right)$	Autocorrelation Function
$\gcd$	Greatest Common Divisor
$L(t)$	$L-$polynomial
N	Number of Unramified Points
MF	Merit Factor

CHAPTER 1

INTRODUCTION

Code division multiple access (CDMA) is a form of spread spectrum transmission which spreads the signal wider than the normal bandwith so that the signal hides under noise. The system is secure when jamming is a threat. With this technology, users of the system can send signal simultaneously without interfering each other.

Basic working principle of this system is: every user is assigned with a different code (sequence) and use this unique sequence to transmit signal. To minimize the interference with other users, the cross-correlation values of these assigned sequences should be small. To send a data, users XOR the data with his/her own spreading sequence and to decode the received signal, receiver XOR the signal with the sender's attained spreading sequence [7].

The spread spectrum is widely used in operational radar systems, navigation, military and telecommunication systems for over eighty years. The amount of interest and investment in this area is constantly growing after the invention of CDMA mobile phones and the 3G mobile radio by industry [29].

First studies on spread spectrum systems were performed during the World War II in the USA, the UK, Germany and the USSR. Most of the information was classified as the studies were supervised by military services. In the 1960s different sequences with some correlation properties were obtained by S. Golomb, N. Zierler, R. Gold, T. Kasami and others. This led to a giant step in the spread spectrum technology and various achievements [13], [28]. The commercial area of the spread spectrum started to increase in the late 1970s, when the mobile phones spread around the world. Then in the late 1980s, the spread spectrum techniques are implemented to the GPS technology, satellite television and mobile radio [13].

The most common methods of the code division multiple access are direct sequence and frequency hopping. Sequences used in these methods should satisfy some spesific properties to have widespread applications. In this thesis, we have focused on two important properties of sequence design: perfect autocorrelation sequences and sequence families with low maximum cross-correlation magnitude.

1.1 Mathematical Background

In this part, we give the necessary mathematical background for sequence design. The definitions and theorems given in this chapter can be found in [19] and [22].

Definition 1.1. A *field* $(F, +, .)$ is a set F, with two binary operations $(+)$ and $(\cdot)$ satisfying the conditions below for all $x, y, z \in F$.

(i) F is closed under $(+)$ and $(\cdot)$, that is, $x + y \in F$ and $x \cdot y \in F$.

(ii) $(+)$ and $(\cdot)$ are associative, that is, $(x+y)+z = x+(y+z)$ and $(x\cdot y)\cdot z = x\cdot(y\cdot z)$.

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

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

(v) $(+)$ and $(\cdot)$ are commutative, that is, $x + y = y + x$ and $x \cdot y = y \cdot x$.

(vi) Distributive laws hold, that is, $x\cdot(y+z) = x\cdot y+x\cdot z$ and $(x+y)\cdot z = x\cdot z+y\cdot z$.

(vii) F has no zero divisors, that is, $x \cdot y = e$ implies $x = e$ or $y = e$.

A field containing finite number of elements is called *finite field*. The *order* of a finite field F, is the number of the different elements of the field. The *characteristic* of a finite field F is the smallest positive integer n which satisfies $nx = 0$ for all $x \in F$ and every finite field has prime characteristic.

For an arbitrary prime number p, let F be the set of $\{0, 1, \ldots, p-1\}$ and the function Ψ be defined by:

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

for all $a \in F$.

Definition 1.2. The field F, constructed by Ψ, is a finite field and it is called *Galois field*. F is denoted by $\mathbb{F}_p$.

Definition 1.3. Let E be a subset of F which is also a field under the operations of F. Then E is called a *subfield* of F and F is called an *extension field* of K.

Theorem 1.1. Existence and Uniqueness of Finite Fields: *For every prime number p and every positive integer n there exists a finite field which has p^n elements. Moreover, every finite field with p^n elements is isomorphic to $\mathbb{F}_{p^n}$. $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$ and it is an extension field of $\mathbb{F}_p$ with the extension degree n.*

Definition 1.4. For a finite field $\mathbb{F}_{p^n}$, a generator of its cyclic group $\mathbb{F}^*_{p^n}$ is called a *primitive element* of $\mathbb{F}_{p^n}$.

Definition 1.5. For a prime power $q = p^n$, let $\alpha \in F = \mathbb{F}_{q^m}$ and $E = \mathbb{F}_q$ be a subfield of F. The *trace* function of α over E is defined as

$$\mathrm{Tr}_{F/E}(\alpha) = \mathrm{Tr}_1^m(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}. \tag{1.1}$$

The trace function satisfies the following properties:

(i) $\mathrm{Tr}(\alpha x + \beta y) = \alpha \mathrm{Tr}(x) + \beta \mathrm{Tr}(y)$, for all $\alpha, \beta \in \mathbb{F}_q$, $x, y \in \mathbb{F}_{q^m}$.

(ii) $\mathrm{Tr}(x^q) = \mathrm{Tr}(x)$, for all $x \in \mathbb{F}_{q^m}$.

(iii) For any $\alpha \in \mathbb{F}_q$ we have

$$\#\{x \in \mathbb{F}_{q^m} \ : \ \mathrm{Tr}(x) = \alpha\} = q^{m-1}.$$

(iv) Let $\alpha \in \mathbb{F}_{q^m}$. If $\mathrm{Tr}(\alpha x) = 0$ for all $x \in \mathbb{F}_{q^m}$ then $\alpha = 0$.

Definition 1.6. Let $\mathbb{F}_p$ be a finite field where p is a prime number, $\mathbb{F}_{p^n}$ be an extension field of $\mathbb{F}_p$ and ζ_p be the complex primitive p-th root of unity. For a given function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, the *Walsh transform* of the function $f(x)$ is equal to the set of correlations between $f(x)$ and the linear functions $\mathrm{Tr}_1^n(\lambda x)$ with $\lambda \in \mathbb{F}_{p^n}$. It is defined by

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_{p^n}} (\zeta_p)^{f(x) - \mathrm{Tr}_1^n(\lambda x)}. \tag{1.2}$$

Definition 1.7. A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is called *s-plateaued* if absolute values of its Walsh transform are in $\{0, p^{\frac{n+s}{2}}\}$, for some $s = 1, ..., n$. Similarly, f is called 0-plateaued if absolute values of its Walsh transform equal to $p^{\frac{n}{2}}$.

Moreover for the prime number $p = 2$, when n is an even integer, a function f is called *bent function* if and only if f is a 0-plateaued function and it is called *semi-bent function* if and only if f is a 2-plateaued function. When $p = 2$ and n is an odd integer, a function f is called *near-bent function* if and only if f is a 1-plateaued function.

A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is called *quadratic form* if it can be written as

$$f(x) = \mathrm{Tr}_1^n(a_0 x^{1+p^0} + a_1 x^{1+p} + a_1 x^{1+p^2} + ... + a_t x^{1+p^t}), \tag{1.3}$$

where $a_i \in \mathbb{F}_{p^n}$, $i = 0, 1, \ldots, t$ and $t = \lceil \frac{n}{2} \rceil$.

There is a known method for computing the Walsh distribution of a quadratic function. To calculate the Walsh distribution of a given quadratic function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, one should compute the plateaued degree of the quadratic form. It is equivalent to computing the rank of the quadratic function $f(x)$. For this purpose, we will take advantage of the symplectic form of the quadratic function. The *symplectic form,* which is symmetric and bilinear, of a given quadratic form $f(x)$ is defined by

$$B(x, y) = f(x + y) - f(x) - f(y). \tag{1.4}$$

The *radical* of a quadratic form is defined by

$$\mathcal{W} = \{x \in \mathbb{F}_p^n : B(x, y) = 0 \quad \forall y \in \mathbb{F}_p^n\}. \tag{1.5}$$

Let M be the number of elements of the radical $\mathcal{W}$, then the rank r of the quadratic form $f(x)$ can be computed by

$$r = n - \log_p M.$$

Note that here $\log_p M = s$ is the plateaued degree of the quadratic function $f(x)$. While constructing new sequence families we will make use of plateaued fuctions as it is easy to find the Walsh distribution of a plateaued function. The Walsh distribution of the plateaued function is given by the following lemma and it can be proved easily by counting and using Parseval.

Lemma 1.2. *If $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is an s-plateaued function, where $1 \leq s \leq n$, then the absolute value of the Walsh transform is*

$$|W_f(\lambda)| = \begin{cases} p^{\frac{n+s}{2}}, & p^{n-s} & \textit{times}, \\ 0, & p^n - p^{n-s} & \textit{times}. \end{cases} \tag{1.6}$$

If $f(x)$ is an 0-plateaued function in $\mathbb{F}_p^n$ over $\mathbb{F}_p$, then the absolute value of the Walsh transform is equal to $p^{\frac{n}{2}}$ exactly p^n times [22].

More specifically when $p = 2$, the the Walsh transform distribution is given by:

$$W_f(\lambda) = \begin{cases} 2^{\frac{n+s}{2}}, & 2^{n-s-1} + 2^{\frac{n-s-2}{2}} & \textit{times}, \\ 0, & 2^n - 2^{n-s} & \textit{times}, \\ -2^{\frac{n+s}{2}}, & 2^{n-s-1} - 2^{\frac{n-s-2}{2}} & \textit{times}, \end{cases} \tag{1.7}$$

for $s \neq 0$. If $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is an 0-plateaued function then

$$W_f(\lambda) = \begin{cases} 2^{\frac{n}{2}}, & 2^{n-1} & \textit{times}, \\ -2^{\frac{n}{2}}, & 2^{n-1} & \textit{times}. \end{cases} \tag{1.8}$$

Definition 1.8. Let $\mathbb{F}_p$ be a finite field where p is a prime number, $\mathbb{F}_{p^n}$ be an extension field of $\mathbb{F}_p$ where n is a positive integer. For two arbitrary sequences $u = (u(0), u(1), ..., u(N-1))$ and $v = (v(0), v(1), ..., v(N-1))$ of period N defined over $\mathbb{F}_{p^n}$, the *periodic cross-correlation* of these sequences is defined by

$$C_{u,v}(\tau) = \sum_{t=0}^{N-1} (\zeta_p)^{u(t \oplus \tau) - v(t)}. \tag{1.9}$$

Here ζ_p denotes the complex primitive p-th root of unity and $\oplus$ denotes the addition modulo N where N is a positive divisor of $p^n - 1$.

Moreover, the *maximum correlation magnitude* of two sequences u and v is defined by

$$C_{\max} = \max\{|C_{u,v}(\tau)| : \ u \neq v, \ \text{ or } \ u = v \ \text{ and } \ \tau \neq 0\}. \tag{1.10}$$

Definition 1.9. Similarly, under the conditions of previous definition, the *periodic autocorrelation* function of a given sequence $u = (u(0), u(1), ..., u(N-1))$ is defined by

$$R_u(\tau) = \sum_{t=0}^{N-1} (\zeta_p)^{u(t\oplus\tau)-u(t)}. \tag{1.11}$$

With a simple change of notation, when u and v are complex valued sequences of period N, then the *periodic cross-correlation* function is defined by

$$C_{u,v}(\tau) = \sum_{t=0}^{N-1} u(t\oplus\tau)\overline{v(t)}, \tag{1.12}$$

and the *autocorrelation* function is defined by

$$R_u(\tau) = \sum_{t=0}^{N-1} u(t\oplus\tau)\overline{u(t)}. \tag{1.13}$$

Remark 1.1. Let ζ_p be the complex primitive p-th root of unity. By substituting the sequences $u(t) = \zeta_p^{f(t)}$ and $v(t) = \zeta_p^{g(t)}$ in the equations 1.12 and 1.13, one get the classical definition of cross-correlation and autocorrelation.

Definition 1.10. Any nonzero sequence $u(t)$ over $\mathbb{F}_q$ is called a maximal length sequence (m-sequence) if it is generated by a primitive polynomial $f(x) \in \mathbb{F}_q[x]$ where α is a root of $f(x)$. Let $\alpha \in \mathbb{F}_{q^n}$ with order $q^n - 1$, $a = \alpha^i$ where $i = 0, ..., q^n - 1$. Then the m-sequence is defined by

$$u(t) = \mathrm{Tr}_1^n(a\alpha^t). \tag{1.14}$$

Remark 1.2. The period of an m-sequence is $q^n - 1$ and its elements are from $\mathbb{F}_q$. Each nonzero element of the sequence occurs exactly q^{n-1} times and 0 occurs $q^{n-1} - 1$ times which means that every m-sequence is balanced.

Definition 1.11. The PSK+ alphabet Ω_n^+, is defined as $\Omega_n^+ = \Omega_n \cup \{0\}$, where $\omega = \exp(\frac{2\pi i}{n})$ is the complex primitive n-th root of unity and $\Omega_n = \{1, \omega, \omega^2, ...\omega^{n-1}\}$.

1.2 Desirable Properties of Sequences

The working procedure of a spread spectrum system is based on first synchronising the receiver and transmitter spreding codes and then data modulation. The most common methods of the spread spectrum systems are *direct sequence* and *frequency hopping*. These are two distinct versions of code division multiple access (CDMA). In this systems maintaining the code synchronisation plays an essential role. To faciliate the synchronisation, sequences which have two valued autocorrelation properties are required [18]. Moreover, with the advent of new generation wireless communication systems,

there is a much greater range of modulation schemes, period lengths, and channel assignment algorithms available to wireless system designers. These systems use higher frequencies and the issue of channel identification, which can be performed in the frequency domain by utilizing a perfect autocorrelation sequence, is also increasingly significant.

The spread spectrum system which is used with multiple access channels are widely used in code division multiple access (CDMA), wireless communication systems and military communications if jamming is a threat [28]. In this manner, families of sequences with good cross-correlation properties plays an important role. The cross-correlation values of a sequence family should be small, over and above, the maximum correlation magnitude $C_{\max}$ should be small. Constructing a new sequence family with these desirable properties, lower bounds such as the Sidelnikov bound [26] (which is the strongest for binary sequences of moderate size) are used to evaluate sequence designs.

When jamming is a threat, using sequences with long periods are important. Using sequences having long periods make difficult the jammer to reconstruct the sequence. In addition to these important properties, the sequences should be easily generated in case of any need. To summarize, the important and desired properties of a sequence should satisfy to be employed in spread spectrum systems and CDMA are given below [18]:

1. The autocorrelation should be two valued.
2. The cross-correlation and the maximum correlation magnitude should be small.
3. Sequences should have long periods.
4. Sequences should be easily generated.

Furthermore, p-ary m-sequences satisfy the three fundamental important properties given in the theorem below. They are called *pair properties* of m-sequences. We will use all these properties while proving our constructions.

Theorem 1.3. *Let s_k be arbitrary, s_1 and s_2 be two distinct m-sequences taking their elements form the finite field $\mathbb{F}_p$, t_1 and t_2 corresponds to two different phases of a sequence. Let B be the set of ordered pairs $\{(s_k, s_{k+r})\}_{k=0}^{M-1}$ with $0 < r < M$ and $M = p^n - 1$. For $N = \frac{M}{(p-1)}$,*

1. *If $\gcd(r, M) \equiv 0 \mod N$, then there exists a $w \in \mathbb{F}_p^*$ satisfying*
   (a) *For all $s_k \in \mathbb{F}_p^*$, (s_k, ws_k) appears in B exactly p^{n-1} times,*
   (b) *The pair $(0, 0)$ appears in B exactly $p^{n-1} - 1$ times.*
2. *Let s_1 and s_2 be two m-sequences under the condition of both of them are not zero. If $\gcd(r, M) \not\equiv 0 \mod N$ then*
   (a) *(s_1, s_2) appears in B exactly p^{n-2} times,*

(b) The pair $(0,0)$ *appears in* B *exactly* $p^{n-2}-1$ *times.*

3. *There exist a primitive element* $< w >= \mathbb{F}_p^*$ *satisfying* $s_{k+rN} = w^r s_k$ *with* $r = 0, 1, 2, \ldots$

1.2.1 Known Sequences with Perfect Autocorrelation Properties

In this chapter we introduce some known perfect autocorrelation sequences. Constraints for the periodicity have been an issue in the sequence constructions. Studies have been focused on finding new sequences with different periods and lengths.

In the thesis of Lee [18], in 1986, the construction of a perfect autocorrelation sequence consists of two main parts. The first part of the construction is called *intermediate mapping* and the second part of the construction is called *terminal mapping*. The composite mapping consists of the combination of the intermediate and the terminal mappings. In his study, he constructed the sequence family over prime fields and used the properties of multiple characters to prove the autocorrelation of his sequences. The details of the construction are given in Definition 1.12.

Definition 1.12. Let I be a cyclic group generated by $a \in \mathbb{C}$ of order $m-1$. The elemenets of this group are the elements of the m-ary sequence. Let $a_1, a_2 \in \mathbb{C}$ having orders m_1 and m_2 respectively, with at least one of them having order $m-1$ where $< a_1 >= J_1 \subseteq I$ and $< a_2 >= J_2 \subseteq I$. Let w_m be a primitive element of $\mathbb{F}_p^*$ and $k = \ldots, -1, 0, 1, \ldots$, then the composite mapping is defined as:

$$\mu(a_k) = \begin{cases} (a_2)^k (a_1)^{v(w_m, a_k)}, & \text{if } a_k \in F_p^* \\ 0, & \text{otherwise} \end{cases} \tag{1.15}$$

where

$$v(w_m, x) = log_{w_m}(x). \tag{1.16}$$

The constraint of the periodicity depends on the choose of a_1, a_2 and w which is mentioned in the item 3 of the Theorem 1.3. Let $w = w_m^s$ then;

1. if $a_2 = a_1^t$ for some positive integer t, then the constraint for the periodicity is $tN + s \equiv 0 \mod m_1$,
2. if $a_1 = a_2^t$ for some positive integer t, then the constraint for the periodicity is $N + ts \equiv 0 \mod m_2$.

In both cases the constraint for the periodicity is a function depending on the parameters p, n and s. And the sequence has perfect autocorrelation, that is;

$$R_{\mu(a_k)}(\tau) = \begin{cases} p^{n-1}, & \text{if } \tau \equiv 0 \mod N \\ 0, & \text{if } \tau \not\equiv 0 \mod N. \end{cases} \tag{1.17}$$

In 2010, Boztaş and Parampalli [4] gave a sequence construction on an arbitrary finite field (not necessarily prime field) when $a_1 = a_2$. In the construction, the constraint for the periodicity is given as $N + s \equiv 0 \mod (q-1)$ and it is a function depending on the parameters q, n and s where q is a prime power. The sequence defined by using PSK+ alphabet with adding zero is given in Definition 1.13.

Definition 1.13. Let q be a prime power, $n \equiv -1 \mod (q-1)$ and let the maximal length sequence $m(t) = \mathrm{Tr}(\alpha^{st})$ where α is a primitive element of $\mathbb{F}_{q^m}^*$, $t = 0, 1, \ldots, q^n - 2$ and $\gcd(s, q^n - 1) = 1$. Let γ be the complex primitive $(q-1)$-th root of unity. The sequence $s(t)$ over Ω_{q-1}^+ is defined by:

$$s(t) = \begin{cases} \gamma^t \phi(m(t)), & \text{if} m(t) \neq 0 \\ 0, & \text{otherwise} \end{cases} \tag{1.18}$$

where the function $\phi(.)$ is defined as follows:

$$\phi(x) = \gamma^{log(\beta, x)}, \quad x \in \mathbb{F}_q^*. \tag{1.19}$$

Here, $\beta = \alpha^{\frac{(q^n-1)}{(q-1)}}$, a primitive element of $\mathbb{F}_q^*$ and $log(\beta, x)$ is the discrete logarithm to base β.

1.2.2 Known Sequence Families with Low Maximum Correlation Magnitude

Sequence families having small maximum correlation magnitude have been well studied in the literature. They play an important role while constructing new sequence families to be used in code division multiple access. There are two important lover bounds which are useful to compare the maximum correlation magnitude of a sequence family. We introduce some known important sequence families having good cross-correlation distribution and their comparisions in this section.

Let S be a sequence family which consists of K cyclicly distinct sequences, all having period N. That is,

$$S = \{s_i(t) : 1 \leq i \leq K\} \tag{1.20}$$

and every sequence $s_i(t)$, $\forall 1 \leq i \leq K$ has period N. Let $C_{\max}$ denote the maximum correlation magnitude of the sequence family S. Then the bounds are given in Theorem 1.4 and Theorem 1.5.

Theorem 1.4. *[22] For the sequence family S and arbitrary positive integer m, the* Welch bound *satisfies the following inequality:*

$$(C_{\max})^{2m} \geq \frac{1}{(KN-1)} \left(\frac{KN^{2m+1}}{\binom{N+m-1}{N-1}} - N^{2m} \right) \tag{1.21}$$

Theorem 1.5. *[22] For the sequence family S and arbitrary positive integer m, depending on the prime power q, the* Sidelnikov bound *satisfies the following inequality:*

1. *When* $q = 2$*, for* $0 \leq m < \frac{2N}{5}$*,*

$$(C_{\max})^2 > (2m+1)(N-m) + \frac{m(m+1)}{2} - \frac{2^m N^{2m+1}}{K(2m)!\binom{N}{m}}. \tag{1.22}$$

2. *When* $q > 2$*, for* $m \geq 0$*,*

$$(C_{\max})^2 > \frac{(m+1)}{2}(2N-m) - \frac{2^m N^{2m+1}}{K(m!)^2\binom{2N}{m}}. \tag{1.23}$$

Now we introduce some known important sequence families with their correlation properties.

Definition 1.14. Let n and $d = 2^k + 1$ be odd integers satisfying $\gcd(n, k) = 1$ and α be a primitive element of $\mathbb{F}_{2^n}$. Let $s(t) = \mathrm{Tr}_1^n(\alpha^t)$ be an m-sequence. Then the *Gold sequence family* [9] is defined as follows:

$$S(t) = \{s(t)\} \cup \{s(dt)\} \cup \{\{s(t+\tau) + s(dt) : 0 \leq \tau \leq 2^n - 2\}\}. \tag{1.24}$$

Definition 1.15. Let $n = 2m$, $m \geq 2$ and α be a primitive element of $\mathbb{F}_{2^n}$. The *small set of Kasami sequences* [14] [15] is defined as follows:

$$S(t) = \{s_w(t) : w \in \mathbb{F}_{2^m},\ 0 \leq t \leq 2^n - 2\} \tag{1.25}$$

where

$$s_w(t) = \mathrm{Tr}_1^n\left(\alpha^t\right) + \mathrm{Tr}_1^m\left(w\alpha^{(2^m+1)t}\right). \tag{1.26}$$

Definition 1.16. Let $n = 2m$, $m \geq 2$, α be a primitive element of $\mathbb{F}_{2^n}$ and β be a primitive element of $\mathbb{F}_{2^m}$. For $0 \leq t \leq 2^n - 2$, the *large set of Kasami sequences* [14] [15] is defined as follows:

$$S_l(t) = \{s_{\gamma\delta}(t) : \gamma \in \mathbb{F}_{2^n},\ \delta \in \mathbb{F}_{2^m}\} \cup \{s_{\zeta\eta}(t) : \zeta \in \Gamma,\ \eta \in \Delta\} \tag{1.27}$$

where

$$s_{\gamma\delta}(t) = \mathrm{Tr}_1^n\left(\alpha^t + \gamma\alpha^{(2^{m+1}+1)t}\right) + \mathrm{Tr}_1^m\left(\delta\alpha^{(2^m+1)t}\right) \tag{1.28}$$

and

$$s_{\zeta\eta}(t) = \mathrm{Tr}_1^n\left(\zeta\alpha^{(2^{m+1}+1)t}\right) + \mathrm{Tr}_1^m\left(\eta\alpha^{(2^m+1)t}\right). \tag{1.29}$$

Here, Γ and Δ is defined depending on n as follows:

1. for $n \equiv 0 \mod 4$, $\Gamma = \{1, \alpha, \alpha^2\}$ and $\Delta = \{1, \beta, \ldots, \beta^{\frac{(2^m-1)}{3}-1}\}$
2. for $n \equiv 2 \mod 4$, $\Gamma = \{1\}$ and $\Delta = \mathbb{F}_{2^m}$.

Definition 1.17. Let k be a positive integer smaller than the prime number p, α be a primitive element of $\mathbb{F}_{p^n}$. For $1 \leq m \leq k$, $a_m \in \mathbb{F}_{p^n}$, the *Sidelnikov sequence family* [26] is defined as follows:

$$S(t) = \mathrm{Tr}_1^n \left(\sum_{m=1}^{k} a_m \alpha^{mt} \right). \tag{1.30}$$

Definition 1.18. Let p be a prime number, V_p^n be an n-dimensional vector space over the finite field $\mathbb{F}_p$. Let $f(x)$ be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ and γ be the complex primitive p-th root of unity, then for all $w \in \mathbb{F}_{p^n}$, the Walsh of the function is:

$$W_f(w) = \frac{1}{\sqrt{p^m}} \sum_{x \in \mathbb{F}_{p^m}} \gamma^{f(x) - \mathrm{Tr}_1^n(wx)} \tag{1.31}$$

and its inverse transform is defined by:

$$\gamma^{f(x)} = \frac{1}{\sqrt{p^m}} \sum_{w \in \mathbb{F}_{p^m}} W_f(w) \gamma^{\mathrm{Tr}_1^n(wx)} \tag{1.32}$$

A function is called generalized bent function if the Walsh transform of $f(x)$ takes values of unit magnitude. The sequences of values $\gamma^{f(x)}$ are called *bent sequences* [24]. Let α be a primitive element of $\mathbb{F}_{p^n}$ then the cross-correlation of a bent sequence with an m-sequence is given by:

$$C_f(\tau) = \sum_{t=0}^{p^n - 2} \gamma^{f(\alpha^t) - \mathrm{Tr}_1^n(\alpha^{t+\tau})} \tag{1.33}$$

Definition 1.19. Let $n = 2m$, $m \geq 2$, α be a primitive element of $\mathbb{F}_{2^n}$, then the *No sequence family* [23] is definde as follows:

$$S(t) = \{ s_w(t) : w \in \mathbb{F}_{2^n},\ 0 \leq t \leq 2^n - 2 \} \tag{1.34}$$

where

$$s_w(t) = \mathrm{Tr}_1^m \left(\left(\mathrm{Tr}_m^n \left(\alpha^t + w\alpha^{(2^m+1)t} \right) \right)^r \right) \tag{1.35}$$

with $1 \leq r \leq 2^m - 1$, $\gcd(r, 2^m - 1) = 1$. Here, r can not be written in the form of 2^i for any positive integer i.

Definition 1.20. Let $n = 2m$, p be an odd prime and α be a primitive element of $\mathbb{F}_{p^n}$. Let $f(x)$ be a p-ary bent function on the vector space V_p^m, $\{\beta_1, \ldots, \beta_m\}$ be a basis of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$ and $\sigma \in \mathbb{F}_{p^n} - \mathbb{F}_{p^m}$. For $\delta \in \mathbb{F}_{p^m}^*$, the *Kumar and Moreno* p-ary bent sequences [17] are defined as follows:

$$S = \{ s_w(t) : w \in \mathbb{F}_{p^m},\ 0 \leq t \leq p^n - 2 \} \tag{1.36}$$

where

$$s_w(t) = f(L(\alpha^t)) + \mathrm{Tr}_1^n((w\sigma + \delta)\alpha^t) \tag{1.37}$$

and

$$L(x) = \{ \mathrm{Tr}_1^n(\beta_1 \sigma x), \ldots, \mathrm{Tr}_1^n(\beta_m \sigma x) \}. \tag{1.38}$$

Definition 1.21. Let n be an odd positive integer, p be a prime number and ζ_i be the enumeration of the elements of the finite field $\mathbb{F}_{2^n}$ for $0 \leq i \leq 2^n - 1$. Then the *Gold-like sequence family* [6] is defined as follows:

$$S = \{s_i(t) : i = 0, 1, 2, ..., 2^n,\ 0 \leq t \leq 2^n - 2\} \tag{1.39}$$

where

$$s_i(t) = \begin{cases} \mathrm{Tr}_1^n(\zeta_i \alpha^t) + p(\alpha^t), & 0 \leq i < 2^n \\ \mathrm{Tr}_1^n(\alpha^t), & i = 2^n. \end{cases} \tag{1.40}$$

The quadratic form $p(x)$ is defined by:

$$p(x) = \sum_{l=1}^{\frac{n-1}{2}} \mathrm{Tr}_1^n(x^{2^l+1}). \tag{1.41}$$

Definition 1.22. Let n and k be two positive integers satisfying $\gcd(k, n) = e$ and $n = em$ where m is an odd positive integer with $m \geq 3$. Let ζ_i be the enumeration of the elements of the finite field $\mathbb{F}_{2^n}$ for $0 \leq i \leq 2^n - 1$. Then the *Kim and No sequence family* [16] is defined as follows:

$$S = \{s_i(t) : i = 0, 1, 2, ..., 2^n,\ 0 \leq t \leq 2^n - 2\} \tag{1.42}$$

where

$$s_i(t) = \begin{cases} \mathrm{Tr}_1^n(\zeta_i \alpha^t) + p(\alpha^t), & 0 \leq i < 2^n \\ \mathrm{Tr}_1^n(\alpha^t), & i = 2^n. \end{cases} \tag{1.43}$$

The quadratic form $p(x)$ is defined by:

$$p(x) = \sum_{l=1}^{\frac{m-1}{2}} \mathrm{Tr}_1^n(x^{2^{el}+1}). \tag{1.44}$$

Definition 1.23. Let n and k be two positive integers satisfying $\gcd(k, n) = e$ and $n = em$ where n and m are odd positive integers with $m \geq 3$. Let ζ_i be the enumeration of the elements of the finite field $\mathbb{F}_{2^n}$ for $0 \leq i \leq 2^n - 1$ and w be an element of $\mathbb{F}_{2^e}$ different than 1. Tang et al. [31] constructed a new sequence family that we will denote by $\mathcal{U}$ is defined as follows:

$$\mathcal{U} = \{u_i(t) : i = 0, 1, 2, ..., 2^n,\ 0 \leq t \leq 2^n - 2\} \tag{1.45}$$

where

$$u_i(t) = \begin{cases} \mathrm{Tr}_1^n(\zeta_i \alpha^t) + p_w(\alpha^t), & 0 \leq i < 2^n \\ \mathrm{Tr}_1^n(\alpha^t), & i = 2^n. \end{cases} \tag{1.46}$$

The quadratic form $p_w(x)$is defined by:

$$p_w(x) = \sum_{l=1}^{\frac{n-1}{2}} \mathrm{Tr}_1^n(x^{2^l+1}) + \sum_{l=1}^{\frac{m-1}{2}} \mathrm{Tr}_1^n((wx)^{2^l+1}). \tag{1.47}$$

Table 1.1: List of some known sequence families and their maximum correlation magnitudes C_{max}.

Sequence Family	**p**	**n**	**Period**	**Family Size**	$\mathbf{C_{max}}$
Gold	2	odd	2^n-1	2^n+1	$2^{\frac{n+1}{2}}+1$
Gold	2	even	2^n-1	2^n+1	$2^{\frac{n+2}{2}}+1$
Small Set of Kasami	2	even	2^n-1	$2^{\frac{n}{2}}$	$2^{\frac{n}{2}}+1$
Large Set of Kasami	2	even	2^n-1	$2^{\frac{n}{2}}(2^n+1)$	$2^{\frac{n+2}{2}}+1$
Sidelnikov	p	$k<p$	p^n-1	$\geq p^{n(k-1)}$	$(k-1)p^{\frac{n}{2}}+1$
Bent	p	even	p^n-1	$p^{\frac{n}{2}}$	$p^{\frac{n}{2}}+1$
No	2	even	2^n-1	$2^{\frac{n}{2}}$	$2^{\frac{n}{2}}+1$
Kumar and Moreno	odd	arbitrary	p^n-1	$p^{\frac{n}{2}}$	$p^{\frac{n}{2}}+1$
Gold-like	2	odd	2^n-1	2^n+1	$2^{\frac{n+1}{2}}+1$
Kim and No(*)	2	m : odd	2^n-1	2^n+1	$2^{\frac{n+e}{2}}+1$
$\mathcal{U}$(*)	2	n,m : odd	2^n-1	2^n+1	$2^{\frac{n+1}{2}}+1$

The comparison of parameters and maximum cross-correlation values of some important sequence families are given in Table 1.1. Note that the sequence families marked with (*), also satisfies the condition $n = em$ as mentioned in the definitions 1.22 and 1.23 above.

CHAPTER 2

PERFECT AUTOCORRELATION SEQUENCES

Designing new sequences with perfect periodic autocorrelation and flexible parameters has always been important. In particular, with the advent of new generation wireless communication systems, there is a much greater range of modulation schemes, period lengths, and channel assignment algorithms available to wireless system designers. In such systems using higher frequencies, the issue of channel identification which can be performed in the frequency domain by utilizing a perfect autocorrelation sequence, is also increasingly significant.

A sequence with perfect autocorrelation has applications relevant to all the above discussed aspects of wireless and radar. For example, CDMA communication enables wireless transmitters to successfully exchange information in the presence of interference from other users and other systems. The two distinct versions of CDMA, *Frequency Hopping* (FH) and *Direct Sequence* (DS) address the issue of interference differently. For details of CDMA, please see the survey in the *Spread Spectrum Communications Handbook* [29]. For sequence construction methods the survey by Helleseth and Kumar is invaluable [10].

In Chapter 2 and Chapter 3 of this thesis, we focus on designing perfect autocorrelation sequences, also referred to as "spreading codes" in DS-CDMA. In particular, the performance of such codes is customary to employ correlations for synchronisation.

There exist very few sequence designs with perfect autocorrelation for symbol alphabets of practical interest, such as the binary ($\{\pm 1\}$) and quaternary ($\{\pm 1, \pm i\}$ with $i = \sqrt{-1}$) alphabet. It is believed that there are no binary sequences with perfect periodic autocorrelation, apart from the sequence $(+1, +1, -1, +1)$ of length 4. This is the famous conjecture that states there are no more circulant Hadamard matrices. Moreover, it is known that quaternary sequences with perfect periodic autocorrelation do not exist [25] for lengths 2^m for $m > 4$. The first two lengths which are open cases are lengths 36 and 40, to the best of our knowledge, while computer searches have unearthed such sequences of lengths $4, 8$ and 16.

Historically, designers studied ternary sequences (i.e., over the alphabet $\{0, \pm 1\}$ to address this shortcoming. For example, ternary sequences of length $(p^n - 1)/(p - 1)$ for primes $p \geq 2$ with perfect autocorrelation exist (see [11, 12, 18]) under some restrictions on n. However, the desire for more flexible choices of period and alphabet are

still there, due to the developments outlined in the first paragraph of this introduction. There is a large literature dealing with sequence design and the applications of such sequences; see [32] and the references therein.

In this chapter we continue our work on the design of nonbinary "extended" PSK sequences with perfect autocorrelation and extend a previous construction to PSK+ alphabets with q elements, where q is not necessarily a prime number. We respectively provide a brief overview of mathematical preliminaries and some definitions and notation for general sequence designs. Then we present a new construction for perfect PSK+ sequences and briefly discuss its properties. Later, we remark on the aperiodic correlation and merit factor in the context of this new design. Finally, we provide a summary of the lengths and alphabets for which we have experimentally found perfect autocorrelation sequences, by means of an exhaustive search, and conclude this chapter. This new construction is published in [3].

2.1 Preliminaries

First we recall the definition of autocorrelation of a complex valued sequence and some necessary properties of $\mathrm{Tr}(\cdot)$ function. The definitions given in this chapter will be used during the construction of a new perfect autocorrelation sequence.

Definition 2.1. Let $u = (u(0), u(1), ..., u(N-1))$ be a complex valued sequence where N is the period of the sequence. The periodic autocorrelation function is defined as

$$R_u(\tau) = \sum_{t=0}^{N-1} u(t \oplus \tau)\overline{u(t)}. \tag{2.1}$$

Here $\oplus$ denotes the addition modulo N, $\overline{u(t)}$ denotes the complex conjugate of $u(t)$ and τ represents the phase shift of the sequence.

Remark 2.1. Note that, if $R_u(\tau) = 0$ for all $\tau \neq 0 \mod N$ then the sequence $u(t)$ is called *perfect autocorrelation sequence*. If $\tau = 0$, then for all sequences $u = u(0), u(1), ..., u(N-1)$, we have *maximum autocorrelation*.

Throughtout this chapter, $q = p^k$ is a prime power and $\mathbb{F}_q$ is the finite field with q elements. $\mathrm{Tr}(x)$ denotes the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ which is defined as

$$\mathrm{Tr}(x) = x^q + x^{q^2} + ... + x^{q^{(n-1)}}. \tag{2.2}$$

Definition 2.2. Any nonzero sequence $u(t)$ over $\mathbb{F}_q$ is called a maximal length sequence (m-sequence) if it is generated by a primitive polynomial $f(x) \in \mathbb{F}_q[x]$ where α is a root of $f(x)$. Let $\alpha \in \mathbb{F}_{q^n}$ with order $q^n - 1$, $a = \alpha^i$ where $i = 0, ..., q^n - 1$. Then the m-sequence is defined by

$$u(t) = \mathrm{Tr}_1^n(a\alpha^t). \tag{2.3}$$

Definition 2.3. The PSK+ alphabet Ω_n^+, is defined as $\Omega_n^+ = \Omega_n \cup \{0\}$, where $\omega = \exp(\frac{2\pi i}{n})$ is the complex primitive n-th root of unity and $\Omega_n = \{1, \omega, \omega^2, ...\omega^{n-1}\}$.

2.2 A New Generalization for Perfect Autocorrelation Sequences

Definition 2.4. Let $m(t)$ be a maximal sequence (m-sequence) over the finite field $\mathbb{F}_q$ with period $M = q^n - 1$, defined as

$$m(t) = \mathrm{Tr}(\alpha^{st}) \text{ for } t = 0, 1, ..., q^n - 2. \tag{2.4}$$

Let $q > 3$, $\gcd(s, q^n - 1) = 1$ and γ be the $(q-1)$-st complex primitive root of unity. A new sequence $S(t)$ over the alphabet Ω^+_{q-1} is defined by:

$$S(t) = \begin{cases} \gamma^t \phi(m(t)), & \text{if } m(t) \neq 0 \\ 0, & \text{otherwise} \end{cases} \tag{2.5}$$

where the function $\phi(.)$ is defined as follows:

$$\phi(x) = \gamma^{2\log(\beta, x)}, \quad x \in \mathbb{F}_q^*. \tag{2.6}$$

Here, $\beta = \alpha^{\frac{q^n-1}{q-1}}$ is a primitive element of $\mathbb{F}_q$ and $\log(\beta, x)$ is the discrete logarithm to base β, that is

$$\beta^r = x \iff \log(\beta, x) = r \tag{2.7}$$

where $r \in \{0, 1, \ldots, \frac{q^n-1}{q-1}\}$.

This $S(t)$ sequence has perfect autocorrelation. To prove this claim, we will take advantage of $\phi(x)$ is a multiplicative character which is proven below.

Lemma 2.1. *The function $\phi(x)$ is a multiplicative character of $\mathbb{F}_q^*$.*

Proof of Lemma 2.1. Let β be a primitive element of $\mathbb{F}_q$ and $x, y \in \mathbb{F}_q^*$ be defined as $x = \beta^{r_1}$ and $y = \beta^{r_2}$ where r_1 and r_2 are nonnegative integers. Then

$$\begin{aligned} \phi(xy) &= \gamma^{2\log(\beta, xy)} = \gamma^{2\log(\beta, \beta^{r_1+r_2})} = \gamma^{2(r_1+r_2)} \\ &= \gamma^{2r_1}\gamma^{2r_2} = \gamma^{2\log(\beta,x)}\gamma^{2\log(\beta,y)} \\ &= \phi(x)\phi(y). \end{aligned}$$

Hence, $\phi(x)$ is a multiplicative character of $\mathbb{F}_q^*$. □

Theorem 2.2. *The sequence $S(t)$ has perfect periodic autocorrelation under the condition of $n + 2s \equiv 0 (mod\ q-1)$ for $q > 3$. The period of the sequence is $N = \frac{M}{q-1} = 1 + q + q^2 + ... + q^{n-1}$.*

Proof. To prove the theorem we first need to show that $S(t)$ has perfect periodic autocorrelation under given restriction. In other words, autocorrelation

$$R_S(\tau) = \sum_{t=0}^{N-1} S(t \oplus \tau)\overline{S(t)} \tag{2.8}$$

equals 0 when $\tau \neq 0$ and as autocorrelation peak $R_S(0) = q^{n-1}$ otherwise. While N is yet to be determined, we know that N divides the period of $m(t)$, that is $N \mid q^n - 1$. The autocorrelation function over the interval K containing K/N periods can be written in the form below ([13], [18]):

$$\begin{aligned} R_S(\tau) &= \frac{N}{K} \sum_{t=0}^{K-1} S(t \oplus \tau)\overline{S(t)} \\ &= \gamma^{\tau} \frac{N}{K} \sum_{t=0}^{K-1} \phi(m(t \oplus \tau))\overline{\phi(m(t))} \end{aligned}$$

where $S(t \oplus \tau) \neq 0$ and $S(t) \neq 0$. Note that here we have eliminated the terms satisfying $S(t \oplus \tau)S(t) = 0$ because they do not effect the value of the total sum. We will continue to the proof in two cases depending on whether τ is a multiple of h or not.

Case 1: Let $h = \frac{q^n-1}{q-1}$ be a fixed integer and let $\tau \neq 0 \mod h$. By using the pair property which is stated in [35] of m-sequences $m(t)$ over $\mathbb{F}_q$, $(m(t \oplus \tau), m(t))$ takes any $(x, y) \in \mathbb{F}_q^2 - \{(0, 0)\}$ exactly q^{n-2} times. Then, the autocorrelation function can be written as follows:

$$\begin{aligned} R_S(\tau) &= \gamma^{\tau} q^{n-2} \frac{N}{K} \sum_{x \in \mathbb{F}_q^*} \sum_{y \in \mathbb{F}_q^*} \phi(x)\overline{\phi(y)} \\ &= \gamma^{\tau} q^{n-2} \frac{N}{K} \sum_{x \in \mathbb{F}_q^*} \phi(x) \sum_{y \in \mathbb{F}_q^*} \overline{\phi(y)} \end{aligned}$$

As Lemma 2.1 states that $\phi(.)$ is multiplicative character. As $q > 3$ it is nontrivial. It satisfies $\sum_{y \in \mathbb{F}_q^*} \phi(y) = 0$. So when $\tau \neq 0 \mod h$, we have

$$R_S(\tau) = 0.$$

Case 2: Let $\tau \equiv 0 \mod h$, that is $\tau = kh$ for some integer k. For a primitive element β of $\mathbb{F}_q$, and for the pair $(S(t \oplus \tau), S(t))$,

$$S(t \oplus \tau) = \beta^k S(t)$$

is satisfied as τ is a multiple of h. By the pair property only the pairs $(\beta^k x, x) \in \mathbb{F}_q^2$ enter the sum. Because of the balance property of q-ary sequences, shown in [35], the nonzero elements of an m-sequence with period $M = q^n - 1$ each occur exactly q^{n-1}

times. Now the autocorrelation function can be written as follows:

$$\begin{aligned} R_S(\tau) = R_S(kh) &= \gamma^{kh} q^{n-1} \frac{N}{K} \sum_{x \in \mathbb{F}_q^*} \phi(\beta^k x)\overline{\phi(x)}, \\ &= \gamma^{kh} q^{n-1} \frac{N}{K} \phi(\beta^k) \sum_{x \in \mathbb{F}_q^*} \phi(x)\overline{\phi(x)}, \\ &= \gamma^{kh} q^{n-1} \frac{N}{K} \gamma^{2\log(\beta,\beta^k)}(q-1), \\ &= \gamma^{kh} q^{n-1} \frac{N}{K} \gamma^{2k}(q-1), \\ &= \gamma^{k(h+2)} q^{n-1}(q-1)\frac{N}{K}, \end{aligned}$$

since

$$\begin{aligned} \sum_{x \in \mathbb{F}_q^*} \phi(x)\overline{\phi(x)} = \sum_{x \in \mathbb{F}_q^*} \phi(x)\phi(x^{-1}) &= \sum_{x \in \mathbb{F}_q^*} \phi(1) \\ = \sum_{x \in \mathbb{F}_q^*} \gamma^{2(q-1)} &= \sum_{x \in \mathbb{F}_q^*} (\gamma^{(q-1)})^2 = 1. \end{aligned}$$

As $q^r \equiv 1 \mod (q-1)$ for every $r \geq 1$, using this fact we obtain

$$h = \frac{q^n - 1}{q-1} = 1 + q + q^2 + ... + q^{n-1} \equiv n \mod (q-1). \tag{2.9}$$

For every k, by taking $n \equiv -2 \mod (q-1)$ we can ensure

$$\gamma^{k(h+2)} \equiv 1 \mod (q-1). \tag{2.10}$$

This menas that $n \equiv -2 \mod (q-1)$ must be satisfied for perfect autocorrelation. With this condition on n, we have

$$R_S(\tau) = q^{n-1}(q-1)\frac{N}{K} \tag{2.11}$$

for any integer k. Moreover using the result of Case 1, for $\tau \neq kh$, the auto-correlation function gives zero. Since the autocorrelation function repeats itself every h samples, period of the sequence $S(t)$ is h. Thus, $N = h = \frac{q^n-1}{q-1}$. □

Lemma 2.3. *If $R_S(\tau)$ is periodic with period N, then the sequence $S(t)$ has the same period N, since*

$$R_S(0) = R_S(N) = \sum_{t=0}^{N-1} \mid S(t) \mid^2 \tag{2.12}$$

is a positive real constant, thus the shifted sequence at N is actually equal to the original sequence, not just a scalar multiple of it.

By Lemma 2.3 we can conclude that the sequence has perfect autocorrelation with the autocorrelation peak q^{n-1} and periodicity $N = \frac{q^n-1}{q-1}$ when $n + 2 \equiv 0 \mod (q-1)$.

Remark 2.2. For a given m-sequence $m(t) = \mathrm{Tr}_q^{q^n}(\alpha^t)$ over $\mathbb{F}_q$ with period $M = q^n - 1$, when $\gcd(s, q^n - 1) = 1$, the function $m'(t) = \mathrm{Tr}_q^{q^n}(\alpha^{st})$ gives us another m-sequence. By using the same properties with the new m-sequence it is easily seen that when $\gcd(s, q^n - 1) = 1$ and $n + 2s \equiv 0 \mod (q-1)$, the sequence has perfect autocorrelation with the autocorrelation peak q^{n-1} and periodicity $N = \frac{q^n-1}{q-1}$. As a result, the constraint for the periodicity is dependent on three parameters which are q, n and s.

2.2.1 Aperiodic Correlation and Merit Factor

Here we give a brief digression on aperiodic correlations. Sequences with perfect periodic correlation are candidates for good aperiodic correlation, which is significant for some synchronisation applications in radar and wireless communications.

Definition 2.5. For a complex valued sequence $u = (u(0), u(1), ..., u(N-1))$, where N is the length of the sequence, the *aperiodic autocorrelation function* is defined by:

$$R_u^{aper}(\tau) = \begin{cases} \sum_{t=0}^{N-1-\tau} u(t+\tau)\overline{u(t)}, & \text{if } 0 \le \tau \le N-1 \\ \sum_{t=0}^{N-1-\tau} \overline{u(t+\tau)}u(t), & \text{if } -N+1 \le \tau < 0. \end{cases} \tag{2.13}$$

Another property of sequences which has been of interest for a long time, and is a very difficult problem when the sequences are binary, is the Merit Factor (MF).

Definition 2.6. For a complex valued sequence $u = (u(0), u(1), ..., u(N-1))$, where N is the length of the sequence, the *merit factor* is defined by:

$$F(u) = \frac{R_u^{aper}(0)^2}{\sum_{\tau \neq 0} |R_u^{aper}(\tau)|^2} = \frac{R_u^{aper}(0)^2}{2\sum_{0<\tau<N} |R_u^{aper}(\tau)|^2} \tag{2.14}$$

In brief, it is very difficult to design binary sequences with MF lower bounded by a constant greater than 6. It is easier to find nonbinary complex valued sequences with growing merit factor, though the alphabet size required may be of the order of $\sqrt{N}$ where N is the length of the sequence. For more details see Borwein et al [1] and Mercer [21], and the references therein. Here, we have a new sequence design with *bounded* alphabet size, so it is of interest to evaluate the MF, which is a measure of the performance of sequences in radar applications.

Example 2.1. Let $q = p = 5$ and $n = 2$. An m-sequence $m(t)$ on $\mathbb{F}_5$ whose length is $N = 5^2 - 1 = 24$ is given below:

$$(1, 1, 4, 0, 3, 1, 3, 3, 2, 0, 4, 3, 4, 4, 1, 0, 2, 4, 2, 2, 3, 0, 1, 2).$$

By taking the primitive polynomial over $\mathbb{F}_5$ of degree $n = 2$ as $x^2 + 3x + 3$ and w as the $(5-1) = 4$-th root of unity we obtain the 5-ary sequence of period $N = \frac{5^2-1}{5-1} = 6$ given by

$$(\phi(t)) = (1, w, -1, 0, -1, w)$$

whose autocorrelation value is $R_\phi(\tau) = 0$ for $\tau \neq 0$ and $R_\phi(0) = 5^{(2-1)} = 5$. In addition, the aperiodic autocorrelation of the sequence is

$$(R_\phi^{aper}(\tau)) = (-i, 0, 0, 0, -i, 5, -i, 0, 0, 0, i)$$

for $\tau \in \{-5, -4, \ldots, 4, 5\}$ respectively, and the MF is found as $25/4 = 6.25$.

2.2.2 Some Computational Results on Existence

Table 2.1: Experimental results of $q-$ary sequences derived from m-sequences

n \ q	**4**	5	7	**8**	**9**	11
2	Exist	Exist*	Exist	Exist	Exist	Exist
3	None	None	None	Exist	None	None
4	Exist*	None	Exist*	Exist	None	Exist
5	Exist	None	None	Exist*	None	None
6	None	Exist*	None	Exist	Exist*	None
n \ q	13	**16**	17	19	23	**25**
2	Exist	Exist	Exist	Exist	Exist	Exist
n \ q	**27**	29	31	**32**	37	**49**
2	Exist	Exist	Exist	Exist	Exist	Exist

It is of interest to find out if the constraints on n derived by the work in the previous section are necessary for finding perfect autocorrelation sequences. In this section, we give some numerical results for some arbitrary values of n for the construction given in Definition 2.4 of the construction by removing the constraint on n. The cases $q = 9$ and $q = 7$, which give $PSK+$ alphabets Ω_8^+ and Ω_6^+, being small alphabets, and especially the first one is interesting in applications [4]. To be precise, we keep the construction but remove the constraint. Interestingly, our construction gives perfect sequences for some values of q and n that can be seen on Table 2.1 where we have marked the corresponding parameter with an asterisk. Exist* notation in the table shows that corresponding parameters are examples of the construction given in this chapter.

Now we will give an example of an experimentally discovered perfect autocorrelation sequence for the prime power $q = 9$ below, where the constraint on n does not hold.

Example 2.2. Let $q = p^2 = 9$ and $n = 2$. Thus, an m-subsequence on $\mathbb{F}_9$ whose length is $N = \frac{9^2-1}{9-1} = 10$ can be written as:

$$(1, 1, \theta, \theta^6, \theta^5, \theta, \theta^7, \theta, 2, 0),$$

where θ is the primitive element of $\mathbb{F}_9$. By taking the primitive polynomial over $\mathbb{F}_9$ of degree $n = 2$ as $x^2 + 2x + \theta^3$ and w as the $(q-1) = 8$-th root of unity we obtain the 9-ary sequence of period $N = 10$ given by

$$(\phi(t)) = (1, w, -1, -w^3, -w^2, -w^3, -1, w, 1, 0)$$

whose autocorrelation value is 0 for $\tau \neq 0$ and $9^{2-1} = 9$ otherwise. Note that, here it is adequate to take first N terms of the m-sequence (i.e. m-subsequence of length N). In addition, the aperiodic autocorrelation of the sequence (given for $0 \leq \tau \leq N-1$, since the rest is determined by conjugate symmetry) is

$$(R_\phi^{aper}(\tau)) = (9, 0, 1, -w^3 + w, -1, 0, 1, w^3 - w, -1, 0)$$

for $\tau \in \{0, \ldots, 8, 9\}$ respectively and the MF can be found as $F(\phi) = 81/16 = 5.0625$.

Remark 2.3. Some lengths resulting in a perfect correlation sequence by using our construction for which no previous perfect correlation sequence was known include $N = 73, 85, 400, 585, 1464, 341, 4681, 3906, 97656, 488281$.

2.3 Results

In this chapter we have generalised a construction for perfect periodic autocorrelation sequences due to [18] and brieflly discussed existence of perfect periodic autocorrelation sequences for the PSK+ alphabet. The generalisation takes the form of being able to use an arbitrary (not necessarily prime size) subfield as the symbol alphabet during the construction. Moreover, we have pointed out the fact that these sequences seem to have decent MF and aperiodic correlation properties.

CHAPTER 3

GENERALIZED PERFECT AUTOCORRELATION SEQUENCES WITH FLEXIBLE PERIODS AND ALPHABET SIZES

The importance of DS-CDMA, perfect autocorrelation sequences and the needs for flexible parameters are discussed in detailed in Chapter 2. Now we improve our study and generalize the costruction given in previous chapter for all possible n and q parameters depending on a positive integer i. We focus on the design of nonbinary "extended" PSK sequences with perfect autocorrelation and extend a previous construction to PSK+ alphabets with q elements, where q is not necessarily a prime, as well as to more flexible periods than before.

This chapter is organised as follows. First some definitions and notations for general sequence designs and a brief overview of mathematical preliminaries are given as a quick reminder. Then, the generalized construction for perfect PSK+ sequences is introduced and the properties of these sequences are discussed. Later, some examples of the new design and a detailed table showing the new sequences in the context of existing designs are given.

3.1 Preliminaries

Definition 3.1. For a complex valued sequence $u = (u(0), u(1), ..., u(N-1))$, where N is the period of the sequence, the periodic autocorrelation function is defined as

$$R_u(\tau) = \sum_{t=0}^{N-1} u(t \oplus \tau)\overline{u(t)}. \tag{3.1}$$

Here $\oplus$ denotes the addition modulo N and $\overline{u(t)}$ denotes the complex conjugate of $u(t)$.

Throughtout this chapter, $q = p^k$ is a prime power and $\mathbb{F}_q$ is the finite field with q elements. $\mathrm{Tr}(x)$ denotes the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ which is defined as

$$\mathrm{Tr}(x) = x^q + x^{q^2} + ... + x^{q^{(n-1)}}. \tag{3.2}$$

Definition 3.2. Any nonzero sequence $u(t)$ over $\mathbb{F}_q$ is called a maximal length sequence (m-sequence) if it is generated by a primitive polynomial $f(x) \in \mathbb{F}_q[x]$ where α is a root of $f(x)$. Let $\alpha \in \mathbb{F}_{q^n}$ with order $q^n - 1$, $a = \alpha^i$ where $i = 0, ..., q^n - 1$. Then the m-sequence is defined by

$$u(t) = \mathrm{Tr}_1^n(a\alpha^t). \tag{3.3}$$

Definition 3.3. The PSK+ alphabet Ω_n^+, is defined as $\Omega_n^+ = \Omega_n \cup \{0\}$, where $\omega = \exp(\frac{2\pi i}{n})$ is the complex primitive n-th root of unity and $\Omega_n = \{1, \omega, \omega^2, ...\omega^{n-1}\}$.

3.2 Generalization of Perfect Autocorrelation Sequences with Flexible Periods

Definition 3.4. For an arbitrary i satisfying $1 \leq i \leq q-2$, let α be a primitive element of $\mathbb{F}_{q^n}$ where $n \equiv -i \mod (q-1)$ for $q > 2$. The m-sequence $m(t)$ be given by $m(t) = \mathrm{Tr}(\alpha^t)$ over $\mathbb{F}_q$ with period $M = q^n - 1$ for $t = 0, 1, ..., q^n - 2$. With the $(q-1)$-st complex primitive root of unity γ, the new sequence $S_i(t)$ over Ω_{q-1}^+ depending on i is defined as

$$S_i(t) = \begin{cases} \gamma^t \phi_i(m(t)), & \text{if } m(t) \neq 0 \\ 0, & \text{otherwise.} \end{cases}$$

Moreover, the function $\phi_i(.)$ is defined as follows:

$$\phi_i(x) = \gamma^{i \log(\beta, x)}, \quad x \in \mathbb{F}_q^*. \tag{3.4}$$

Here $\beta = \alpha^{(q^n-1)/(q-1)}$ is a primitive element of $\mathbb{F}_q$ and $\log(\beta, x)$ is the discrete logarithm to base β, that is

$$\beta^r = x \iff \log(\beta, x) = r \tag{3.5}$$

where $r \in \{0, 1, \ldots, \frac{q^n-1}{q-1}\}$.

This $S_i(t)$ sequence has perfect autocorrelation. To prove this claim, we take advantage of $\phi_i(x)$ being a multiplicative character which is proven below.

Lemma 3.1. *The function $\phi_i(x)$ is a multiplicative character of $\mathbb{F}_q^*$.*

Proof. Let β be a primitive element of $\mathbb{F}_q$ and $x, y \in \mathbb{F}_q^*$ be defined as $x = \beta^{r_1}$ and $y = \beta^{r_2}$ where r_1 and r_2 are nonnegative integers. Then

$$\begin{aligned} \phi_i(xy) &= \gamma^{i \log(\beta, xy)} = \gamma^{i \log(\beta, \beta^{r_1+r_2})} = \gamma^{i(r_1+r_2)} \\ &= \gamma^{ir_1}\gamma^{ir_2} = \gamma^{i \log(\beta, x)}\gamma^{i \log(\beta, y)} \\ &= \phi_i(x)\phi_i(y). \end{aligned}$$

Hence, $\phi_i(x)$ is a multiplicative character of $\mathbb{F}_q^*$. □

Theorem 3.2. *The sequence $S_i(t)$ has perfect periodic autocorrelation under the condition of $n + i \equiv 0 (mod\ q-1)$ for $q > 2$. The period of the sequence is obtained as $N = \frac{M}{q-1} = 1 + q + q^2 + ... + q^{n-1}$.*

Proof. To prove the theorem we need to show $S_i(t)$ has perfect periodic autocorrelation under given restriction. In other words, the autocorrelation

$$R_{S_i}(\tau) = \sum_{t=0}^{N-1} S_i(t \oplus \tau)\overline{S_i(t)} \tag{3.6}$$

equals 0 when $\tau \neq 0$ and as autocorrelation peak $R_{S_i}(0) = q^{n-1}$ otherwise. We know that N divides the period of $m(t)$, that is $N \mid q^n - 1$. The autocorrelation function over the interval K containing K/N periods can be written in the form ([18], [13]):

$$\begin{aligned} R_{S_i}(\tau) &= \frac{N}{K}\sum_{t=0}^{K-1} S_i(t \oplus \tau)\overline{S_i(t)} \\ &= \gamma^{\tau}\frac{N}{K}\sum_{t=0}^{K-1} \phi_i(m(t \oplus \tau))\overline{\phi_i(m(t))} \end{aligned}$$

where $S_i(t \oplus \tau) \neq 0$ and $S_i(t) \neq 0$. Note that here we have eliminated the terms satisfying $S_i(t \oplus \tau)S_i(t) = 0$, because they do not affect the value of the total sum.

Case 1: Let $h = \frac{q^n-1}{q-1}$ be a fixed integer, $q > 2$ be an odd number and $\tau \not\equiv 0 \mod h$. By using the pair property, which is stated in [35], of m-sequences $m(t)$ over $\mathbb{F}_q$, $(m(t \oplus \tau), m(t))$ takes any $(x, y) \in \mathbb{F}_q^2 - \{(0, 0)\}$ exactly q^{n-2} times. Then the autocorrelation function can be written as follows:

$$\begin{aligned} R_{S_i}(\tau) &= \gamma^{\tau} q^{n-2}\frac{N}{K}\sum_{x\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q^*} \phi_i(x)\overline{\phi_i(y)} \\ &= \gamma^{\tau} q^{n-2}\frac{N}{K}\sum_{x\in\mathbb{F}_q^*} \phi_i(x)\sum_{y\in\mathbb{F}_q^*} \overline{\phi_i(y)}. \end{aligned}$$

As Lemma 3.1 states $\phi(.)$ is multiplicative character and it satisfies $\sum_{y\in\mathbb{F}_q^*} \phi(y) = 0$. So when $\tau \neq 0 \mod h$, we have

$$R_{S_i}(\tau) = 0.$$

Case 2: Let $\tau \equiv 0 \mod h$, that is $\tau = kh$ for some integer k. For a primitive element β of $\mathbb{F}_q$, and for the pair $(S_i(t \oplus \tau), S_i(t))$,

$$S_i(t \oplus \tau) = \beta^k S_i(t)$$

is satisfied as τ is a multiple of h. By the pair property, only the pairs $(\beta^k x, x) \in \mathbb{F}_q^2$ enter the sum. Because of the balance property of q-ary sequences, shown in [35], each nonzero element of an m-sequence with period $M = q^n - 1$ occurs exactly q^{n-1} times.

Now the autocorrelation function can be written as follows:

$$\begin{aligned} R_{S_i}(\tau) = R_{S_i}(kh) &= \gamma^{kh} q^{n-1} \frac{N}{K} \sum_{x \in \mathbb{F}_q^*} \phi_i(\beta^k x)\overline{\phi_i(x)}, \\ &= \gamma^{kh} q^{n-1} \frac{N}{K} \phi_i(\beta^k) \sum_{x \in \mathbb{F}_q^*} \phi_i(x)\overline{\phi_i(x)}, \\ &= \gamma^{kh} q^{n-1} \frac{N}{K} \gamma^{i \log(\beta, \beta^k)}(q-1), \\ &= \gamma^{kh} q^{n-1} \frac{N}{K} \gamma^{ik}(q-1), \\ &= \gamma^{k(h+i)} q^{n-1}(q-1)\frac{N}{K}, \end{aligned}$$

since

$$\begin{aligned} \sum_{x \in \mathbb{F}_q^*} \phi_i(x)\overline{\phi_i(x)} = \sum_{x \in \mathbb{F}_q^*} \phi_i(x)\phi_i(x^{-1}) &= \sum_{x \in \mathbb{F}_q^*} \phi_i(1) \\ = \sum_{x \in \mathbb{F}_q^*} \gamma^{i(q-1)} &= \sum_{x \in \mathbb{F}_q^*} (\gamma^{(q-1)})^i = 1. \end{aligned}$$

As $q^r \equiv 1 \mod (q-1)$ for every $r \geq 1$, using this fact we obtain

$$h = \frac{q^n - 1}{q-1} = 1 + q + q^2 + ... + q^{n-1} \equiv n \mod (q-1). \tag{3.7}$$

For every k, by taking $h \equiv -i \mod (q-1)$ we can ensure

$$\gamma^{k(h+i)} \equiv 1 \mod (q-1). \tag{3.8}$$

This means that $n \equiv -i \mod (q-1)$ must be satisfied for perfect autocorrelation. With this condition on n, we have

$$R_{S_i}(\tau) = q^{n-1}(q-1)\frac{N}{K} \tag{3.9}$$

for any integer k. Moreover using the result of Case 1, for $\tau \neq kh$, the autocorrelation function gives zero. Since the autocorrelation function repeats itself every h samples, period of the sequence $S_i(t)$ is h. Thus, $N = h = \frac{q^n-1}{q-1}$. □

Lemma 3.3. *If $R_{S_i}(\tau)$ is periodic with period N, then the sequence $S_i(t)$ has the same period N, since*

$$R_{S_i}(0) = R_{S_i}(N) = \sum_{t=0}^{N-1} \mid S_i(t) \mid^2 \tag{3.10}$$

is a positive real constant, thus the shifted sequence at N is actually equal to the original sequence, not just a scalar multiple of it.

By Lemma 3.3 we can conclude that the sequence has perfect autocorrelation with the autocorrelation peak q^{n-1} with periodicity $N = \frac{q^n-1}{q-1}$ when $n + i \equiv 0 \mod (q-1)$.

Remark 3.1. For a given m-sequence $m(t) = \mathrm{Tr}_q^{q^n}(\alpha^t)$ over $\mathbb{F}_q$ with period $M = q^n - 1$, when $\gcd(s, q^n - 1) = 1$, the function $m'(t) = \mathrm{Tr}_q^{q^n}(\alpha^{st})$ gives us another m-sequence. By using the same properties with the new m-sequence it is easily seen that when $\gcd(s, q^n - 1) = 1$ and $n + is \equiv 0 \mod (q-1)$, the sequence has perfect autocorrelation. The autocorrelation peak of the sequence is q^{n-1} and periodicity $N = \frac{q^n-1}{q-1}$. As a result, the constraint for periodicity is dependent on three parameters which are q, n and s.

3.2.1 Existence of $S_i(t)$ for q Depending on n

In this section, we classify the results for some arbitrary values of n of the construction given in Definition 3.1, using the constraint on n. The cases $q = 9$ and $q = 17$, which give $PSK+$ alphabets Ω_8^+ and Ω_{16}^+ are interesting, being practically very relevant.

Table 3.1 demonstrates that our generalized construction fills in the gaps in the parameters of existing constructions.

Table 3.1: Comparison of new perfect autocorrelation sequences with previous constructions.

n \ q	3	**4**	5	7
2	N†	$E^{(1)}$	$E^{(2)}$	E^* :$i \equiv 4 \mod 6$
3	$E^{(1)}$	N†	$E^{(1)}$	E^* :$i \equiv 3 \mod 6$
4	N†	$E^{(2)}$	N†	$E^{(2)}$
5	$E^{(1)}$	$E^{(1)}$	E^* :$i \equiv 3 \mod 4$	$E^{(1)}$
6	N†	N†	$E^{(2)}$	N†
n \ q	**8**	**9**	11	13
2	E^* :$i \equiv 5 \mod 7$	E^* :$i \equiv 6 \mod 8$	E^* :$i \equiv 8 \mod 10$	E^* :$i \equiv 10 \mod 12$
3	E^* :$i \equiv 4 \mod 7$	E^* :$i \equiv 5 \mod 8$	E^* :$i \equiv 7 \mod 10$	E^* :$i \equiv 9 \mod 12$
4	E^* :$i \equiv 3 \mod 7$	E^* :$i \equiv 4 \mod 8$	E^* :$i \equiv 6 \mod 10$	E^* :$i \equiv 8 \mod 12$
5	$E^{(2)}$	E^* :$i \equiv 3 \mod 8$	E^* :$i \equiv 5 \mod 10$	E^* :$i \equiv 7 \mod 12$
6	$E^{(1)}$	$E^{(2)}$	E^* :$i \equiv 4 \mod 10$	E^* :$i \equiv 6 \mod 12$
n \ q	**16**	17	19	23
2	E^* :$i \equiv 13 \mod 15$	E^* :$i \equiv 14 \mod 16$	E^* :$i \equiv 16 \mod 18$	E^* :$i \equiv 20 \mod 22$
3	E^* :$i \equiv 12 \mod 15$	E^* :$i \equiv 13 \mod 16$	E^* :$i \equiv 15 \mod 18$	E^* :$i \equiv 19 \mod 22$
n \ q	**25**	**27**	29	31
2	E^* :$i \equiv 22 \mod 24$	E^*:$i \equiv 24 \mod 26$	E^*:$i \equiv 26 \mod 28$	E^*:$i \equiv 28 \mod 30$
3	E^*:$i \equiv 21 \mod 24$	E^*:$i \equiv 23 \mod 26$	E^*:$i \equiv 25 \mod 28$	E^*:$i \equiv 27 \mod 30$

The notation $^{(1)}$ in the table above denotes that the sequences are from [4], $^{(2)}$ denotes that the sequences are from [3] and * denotes that the sequences are derived using proved construction. Bold characters highlight prime powers. $:i$ notation corresponds

to necessary i values such that the sequence defined by $S_i(t)$ has perfect autocorrelation. † indicates that no perfect sequence exists for those parameters. E denotes existence and N denotes nonexistence of perfect autocorrelation sequence for specified parameters. For all these examples, the resulting perfect sequences have period $N = \frac{q^n-1}{q-1}$ and alphabet Ω_{q-1}^+.

Now we examine the necessary parameters of this general construction for a given prime power q.

- Let $q = 3$, $i = 1$ then $n \equiv -1 \mod 2$. We can always find an s satisfying $N + s \equiv 0 \mod 2$ and $\gcd(s, 3^n - 1) = 1$. As $N \equiv n \mod 2$ and $n \equiv -1 \mod 2$, $-1 + s \equiv 0 \mod 2$ so $s = 1$ is the obvious solution for all $n \equiv -1 \mod 2$. There exists a perfect autocorrelation $S_1(t)$ sequence for $n = 2k - 1,\ \forall k = 2, 3, \ldots$

- Let $q = 4$, $i = 1, 2$. When $i = 1$, $n \equiv -1 \mod 3$. We can always find an s satisfying $N + s \equiv 0 \mod 3$ and $\gcd(s, 4^n - 1) = 1$. As $N \equiv n \mod 3$ and $n \equiv -1 \mod 3$, $-1 + s \equiv 0 \mod 3$ so $s = 1$ is the obvious solution for all $n \equiv -1 \mod 3$. Smilarly when $i = 2$, $n \equiv -2 \mod 3$. We can always find an s satisfying $N + 2s \equiv 0 \mod 3$ and $\gcd(s, 4^n - 1) = 1$. As $N \equiv n \mod 3$ and $n \equiv -2 \mod 3$, $-2 + 2s \equiv 0 \mod 3$. $s = 1$ is the obvious solution for all $n \equiv -2 \mod 3$. There exists a perfect autocorrelation $S_1(t)$ sequence for $n = 3k - 1,\ \forall k = 1, 2, 3, \ldots$ and there exists a perfect autocorrelation $S_2(t)$ sequence for $n = 3k - 2,\ \forall k = 2, 3, \ldots$

Using the same method we compute some other examples and give a general form of n for which a perfect sequence exists, for a given q.

- Let $q = 5$, $i = 1, 2, 3$. There exists a perfect autocorrelation $S_1(t)$ sequence for $n = 4k - 1,\ \forall k = 1, 2, 3, \ldots$ There exists a perfect autocorrelation $S_2(t)$ sequence for $n = 4k-2,\ \forall k = 1, 2, 3, \ldots$ and there exists a perfect autocorrelation $S_3(t)$ sequence for $n = 4k - 3,\ \forall k = 2, 3, \ldots$

- Let $q = 7$, $i = 1, 2, 3, 4, 5$. There exists a perfect autocorrelation $S_1(t)$ sequence for $n = 6k - 1,\ \forall k = 1, 2, 3, \ldots$, a $S_2(t)$ sequence for $n = 6k - 2,\ \forall k = 1, 2, 3, \ldots$, a $S_3(t)$ sequence for $n = 6k - 3,\ \forall k = 1, 2, 3, \ldots$, a $S_4(t)$ sequence for $n = 6k - 4,\ \forall k = 1, 2, 3, \ldots$ and a $S_5(t)$ sequence for $n = 6k - 5,\ \forall k = 2, 3, \ldots$

In general for a given prime power q,

- for $n = (q - 1)k - 1,\ \forall k = 1, 2, 3, \ldots$ there exists a perfect autocorrelation $S_1(t)$ sequence;

- for $n = (q-1)k-(q-3),\ \forall k = 1, 2, 3, \ldots$ there exists a perfect autocorrelation $S_{(q-3)}(t)$ sequence;

- for $n = (q-1)k - (q-2),\ \forall k = 2, 3, \ldots$ there exists a perfect autocorrelation $S_{(q-2)}(t)$ sequence

since $N + i \equiv 0 \mod q-1$ is the obvious solution for this construction. Thus we can find a perfect autocorrelation sequence for all n values except $n \equiv 0 \mod q-1$ for a given prime power q. We have thus proved:

Proposition 3.4. *For a given prime power q, we can find a perfect autocorrelation sequence over Ω^+_{q-1} with period N, for all $n \not\equiv 0 \pmod{q-1}$.*

Example 3.1. We consider some cases of practical importance in this example. Note that we have periods $N = 6, 31, 156, 781, 3906$ obtained by choosing $n = 2, 3, 4, 5, 6$ for Ω^+_4 and $N = 18, 307$ obtained by choosing $n = 2, 3$ for Ω^+_{16}. These sequences can be directly used in 4PSK and 16PSK systems.

Now we give some examples of perfect autocorrelation sequences proved by this construction.

Example 3.2. Let $q = 7$, $n = 2$ and $i = 4$. Thus, an m-subsequence on $\mathbb{F}_7$ whose length is $N = \frac{7^2-1}{7-1} = 8$ can be written as follows:

$$(1, 1, 3, 1, 4, 0, 2, 5).$$

Let the primitive polynomial over $\mathbb{F}_7$ of degree $n = 2$ be $x^2 + x + 3$ and w be the $(q-1) = 6$-th root of unity. We obtain the 7-ary sequence of period $N = 8$ as

$$(\phi_4(t)) = (1, w, 1, -1, w-1, 0, w-1, -1).$$

The autocorrelation value $R(\tau)$ is 0 for $\tau \neq 0$ and $7^{2-1} = 7$ otherwise.

Example 3.3. Let $q = 2^3 = 8$, $n = 2$ and $i = 5$. Thus, an m-subsequence on $\mathbb{F}_8$ whose length is $N = \frac{8^2-1}{8-1} = 9$ can be written as follows:

$$(1, \theta, 0, \theta, 1, \theta^2, \theta^5, \theta^5, \theta^2).$$

Let the primitive polynomial over $\mathbb{F}_8$ of degree $n = 2$ be $x^2 + \theta x + \theta$ and θ be the primitive element of $\mathbb{F}_8$ where w is the $(q-1) = 7$-th root of unity. We obtain the 8-ary sequence of period $N = 9$ as

$$(\phi_5(t)) = (1, w, 0, w, 1, w^2, w^5, w^5, w^2).$$

The autocorrelation value $R(\tau)$ is 0 for $\tau \neq 0$ and $8^{2-1} = 8$ otherwise.

Example 3.4. Let $q = 2^4 = 16$, $n = 2$ and $i = 13$. Thus, an m-subsequence on $\mathbb{F}_{16}$ whose length is $N = \frac{16^2-1}{16-1} = 17$ can be written as follows:

$$(1, \theta, -\theta^6 - \theta, \theta^7, \gamma, -\theta^5 - 1, \theta^3, \theta^3, -\theta^5 - 1, \gamma, \theta^7, -\theta^6 - \theta, \theta, 1, \theta^2, 0, \theta^2).$$

Let the primitive polynomial over $\mathbb{F}_{16}$ of degree $n = 2$ be $x^2 + \theta^9 x + \theta$ and θ be the primitive element of $\mathbb{F}_{16}$ where w is the $(q-1) = 15$-th root of unity. Let $\gamma = -\theta^7 + \theta^5 - \theta^4 - \theta + 1$. We obtain the 16-ary sequence of period $N = 17$ as

$$(\phi_{13}(t)) = (1, 1, w^3, w^{13}, w^3, w^5, w^9, w^2, w^{14}, w^{13}, w^9, 1, w^{13}, w^{14}, w^6, 0).$$

The autocorrelation value $R(\tau)$ is 0 for $\tau \neq 0$ and $16^{2-1} = 16$ otherwise.

3.3 Results

In this chapter we have generalised a construction for perfect periodic autocorrelation sequences introduced in the thesis of Lee [18] for all possible values of n for a given prime power q with respect to a number of theoretic constraint. The generalisation takes the form of being able to use an arbitrary (not necessarily prime size) subfield as the symbol alphabet during the construction. This construction enables the designers to have more flexibility in terms of the deployment of these sequences, as part of existing and new generation wireless communication and radar systems.

CHAPTER 4

CORRELATION DISTRIBUTION OF A NEW SEQUENCE FAMILY

Binary sequence families with good correlation are widely used in CDMA, wireless communication systems and military communications if jamming is a threat [28]. To faciliate synchronization and to minimize the interference due to other users, the correlation values of the sequence family should be small. As a result of this, minimizing the maximum correlation magnitude $C_{\max}$ value plays an important role when constructing a new sequence family. Lower bounds such as the Sidelnikov bound [26] (which is the strongest for binary sequences of moderate size) are used to evaluate sequence designs.

The basic aim of CDMA is to enable wireless transmitters to successfully exchange information in the presence of potential conflicts which lead to interference. There are two main methods of CDMA, *Frequency Hopping* (FH) and *Direct Sequence* (DS). For details of CDMA networks, we refer the interested reader to the survey in the *Spread Spectrum Communications Handbook* by Simon et al. [28] and for sequence construction methods we recommend the more recent survey [10] as well. In this paper we focus on DS-CDMA

Boztaş and Kumar constructed Gold-like sequences which satisfies Sidelnikov's bound and computed their correlation distribution in [6] using the quadratic form technique. Kim and No generalized the quadratic form in [16]. Later, using these two quadratic forms, Tang et al. gave a new family of Gold-like sequences and computed the correlation distribution in [31]. All these constructions were done when n is an odd integer. When n is even, there are two important families, the small set of Kasami sequences and the large set of Kasami sequences, which have later on been generalised. For this case please see Zeng et al. [34] and the references therein.

This chapter is organised as follows. First we give a basic background about sequence families and correlation functions and some known sequence families with their quadratic forms. Later, the new family is constructed when n is even and its correlation distribution is computed. It is shown that the correlation is six-valued. Finally, the relationship of the new construction to existing designs is discussed.

The new sequence family we constructed turns out to be equivalent to the sequence family given by Udaya and Siddiqi in [33], mentioned in the related work by Kim and

No [16]. This study was published in [5].

4.1 Preliminaries

Throught this chapter, let $x \in \mathbb{F}_2$ be binary field and $\mathbb{F}_{2^n}$ be an extension field of $x \in \mathbb{F}_2$ where n is of the form $n = me$ and n, m, e are positive integers. Let α be a primitive element of $\mathbb{F}_{2^n}$ and ζ be an element of $\mathbb{F}_{2^e}$ different than 1. For given arbitrary two sequences $u = (u(0), u(1), ..., u(N-1))$ and $v = (v(0), v(1), ..., v(N-1))$ of period N, the correlation of these sequences is defined by

$$C_{u,v}(\tau) = \sum_{t=0}^{N-1} (-1)^{u(t+\tau)+v(t)}. \tag{4.1}$$

Maximum correlation magnitude of a sequence is defined as

$$C_{\max} = \max\{|C_{u,v}(\tau)| \text{ if } u \neq v, \text{ or } u = v \text{ and } \tau \neq 0\}. \tag{4.2}$$

For a given function f, the Walsh transform of the function is equal to the correlation between of all the sequences and that is the trace transform of the function which is given as

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(\lambda x)}. \tag{4.3}$$

Here, $f(x)$ is a quadratic form in $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and any quadratic form over $\mathbb{F}_2$ can be written as

$$f(x) = \mathrm{Tr}_1^n(a_0 x^2 + a_1 x^{1+2} + a_1 x^{1+2^2} + ... + a_t x^{1+2^t}), \tag{4.4}$$

where $t = \lceil \frac{m}{2} \rceil$.To calculate the correlation distribution of a given sequence, it is enough to compute the rank of the quadratic form. For this purpose, the symplectic form of the quadratic form is defined by

$$B(x, y) = f(x) + f(y) + f(x + y) \tag{4.5}$$

and it is bilinear. Then the radical is

$$\mathcal{W} = \{x \in \mathbb{F}_{2^n} : B(x, y) = 0 \quad \forall y\}. \tag{4.6}$$

If N is the the number of the elements of the radical $\mathcal{W}$, then the rank $2r$ of the quadratic form $f(x)$ can be computed by

$$2r = n - \log_2 N.$$

Lemma 4.1. *If $f(x)$ is a quadratic form of rank $2r$, $2 \leq 2r < n$ in $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, then the Walsh transform distribution is*

$$W_f(\lambda) = \begin{cases} 2^{n-r}, & 2^{2r-1} + 2^{r-1} \quad \textit{times}, \\ 0, & 2^n + 2^{2r} \quad \textit{times}, \\ -2^{n-r}, & 2^{2r-1} - 2^{r-1} \quad \textit{times}. \end{cases} \tag{4.7}$$

Definition 4.1. A function f is called t-plateaued if the Walsh transform values of f are in $\{0, \pm 2^{\frac{n+t}{2}}\}$ for some $t = 0, 1, ..., n$. Here t is the dimension of the radical.

Definition 4.2. When n is an even integer, a function f is called bent if and only if f is 0-plateaued and called semi-bent if and only if f is 2-plateaued. When n is an odd integer, a function f is called near-bent if and only if f is 1-plateaued.

4.2 Some Known Quadratic Forms Used in Sequence Design

When n is odd, Boztaş and Kumar [6] studied the quadratic form $p(x)$ which is of the form

$$p(x) = \sum_{l=1}^{\frac{n-1}{2}} \mathrm{Tr}_1^n(x^{2^l+1}), \tag{4.8}$$

defined the sequence family $\mathcal{G}$ and gave the correlation distribution of the family in.

Definition 4.3. The Gold-like sequence family $\mathcal{G} = \{g_i : i = 0, 1, 2, ..., 2^n\}$ is defined as

$$g_i(t) = \begin{cases} \mathrm{Tr}_1^n(\zeta_i \alpha^t) + p(\alpha^t), & 0 \le i < 2^n \\ \mathrm{Tr}_1^n(\alpha^t), & i = 2^n. \end{cases}$$

The correlation distribution of the family is

$$C_{i,j}(\tau) = \begin{cases} -1 + 2^n, & 2^n + 1 & \text{times}, \\ -1, & 2^{3n-1} + 2^{2n} - 2^n - 2 & \text{times}, \\ -1 + 2^{\frac{n+1}{2}}, & (2^{2n} - 2)(2^{n-2} + 2^{\frac{n-3}{2}}) & \text{times}, \\ -1 - 2^{\frac{n+1}{2}}, & (2^{2n} - 2)(2^{n-2} - 2^{\frac{n-3}{2}}) & \text{times}. \end{cases} \tag{4.9}$$

Here, the rank of the quadratic forms $p(x)$ and $q(x) = p(x) + p(x\alpha^\tau)$ are equal to $2r = n - 1$. These $p(x)$ and $q(x)$ functions are 1-plateaued and so near-bent.

Later, under the restriction of n odd, Kim and No generalized this $p(x)$ quadratic form to

$$q(x) = \sum_{l=1}^{\frac{m-1}{2}} \mathrm{Tr}_1^n(x^{2^{el}+1}). \tag{4.10}$$

Tang et al. constructed a new family of sequences based on these two $p(x)$ and $q(\zeta x)$ quadratic forms in [31].

Definition 4.4. The sequence family $\mathcal{U} = \{u_i : i = 0, 1, 2, ..., 2^n\}$ is defined as

$$u_i(t) = \begin{cases} \mathrm{Tr}_1^n(\zeta_i \alpha^t) + p(\alpha^t) + q(\zeta \alpha^t), & 0 \le i < 2^n \\ \mathrm{Tr}_1^n(\alpha^t), & i = 2^n \end{cases} \tag{4.11}$$

The correlation distribution of the family is

$$C_{i,j}(\tau) = \begin{cases} -1+2^n, & 2^n+1 & \text{times} \\ -1, & 2^{3n-1}+2^{2n}-2^n-2 & \text{times} \\ -1+2^{\frac{n+1}{2}}, & (2^{2n}-2)(2^{n-2}+2^{\frac{n-3}{2}}) & \text{times} \\ -1-2^{\frac{n+1}{2}}, & (2^{2n}-2)(2^{n-2}-2^{\frac{n-3}{2}}) & \text{times} \end{cases} \tag{4.12}$$

4.3 Construction of the New Sequence Family

In this section, we assume that n is even. Let $f(x)$ be the quadratic form

$$f(x) = \mathrm{Tr}_1^n(cx^{2^{n/2}+1}) + \sum_{l=1}^{\frac{n}{2}-1} \mathrm{Tr}_1^n(x^{2^l+1}) \tag{4.13}$$

where $c \in \mathbb{F}_{2^n}$ satisfies the condition $c^{2^{\frac{n}{2}}} + c = 1$. We shall make use of results from Çakçak and Özbudak [8] to prove the theorem below.

Definition 4.5. Let $\mathbb{F}_{2^n} = \{\zeta_1, \zeta_2, ..., \zeta_{2^n}\}$. The new sequence family $\mathcal{S} = \{s_i : i = 1, 2, ..., 2^n + 1\}$ is defined as

$$s_i(t) = \begin{cases} \mathrm{Tr}_1^n(\zeta_i \alpha^t) + f(\alpha^t), & 1 \le i \le 2^n \\ \mathrm{Tr}_1^n(\alpha^t), & i = 2^n + 1. \end{cases} \tag{4.14}$$

While computing the correlation distribution of the sequence family $\mathcal{S}$, we will take advantage of Lemma 4.2 below.

Lemma 4.2. *The radical $\mathcal{W}$ of the quadratic form $f(x)$ is $\{0\}$, and the rank is $2r = n$.*

Proof. The symplectic form of the quadratic form $f(x)$ is of the form

$$B(x,y) = \sum_{i=1}^{\frac{n}{2}-1} (xy^{2^i} + x^{2^i}y) + cxy^{2^{\frac{n}{2}}} + cx^{2^{\frac{n}{2}}}y \tag{4.15}$$

Then using the necessary transformations, the radical $\mathcal{W}$ becomes the roots of the polynomial

$$W(x) = \sum_{\frac{n}{2}+1}^{n-1} (x^{2^i}) + \sum_{1}^{\frac{n}{2}-1} (x^{2^i}) + x(c^{2^{\frac{n}{2}}} + c) = 0 \tag{4.16}$$

Taking into consideration that $c^{2^{\frac{n}{2}}} + c = 1$ and multiplying the equation with $x^{2^{\frac{n}{2}+1}}$, the problem is reduced to finding the roots of the polynomial

$$W(x) = x + \mathrm{Tr}_1^n(x) = 0. \tag{4.17}$$

If $\mathrm{Tr}_1^n(x) = 0$ then $x = 0$. If $\mathrm{Tr}_1^n(x) = 1$ then $x = 1$. But as n is even $\mathrm{Tr}_1^n(1) = 0$ so this is a contradiction. Hence the radical $\mathcal{W}$ is $\{0\}$, and the rank is $2r = n$. □

Lemma 4.3. *Let* $f(x) = \mathrm{Tr}_1^n(cx^{2^{n/2}+1}) + \sum_{l=1}^{\frac{n}{2}-1} \mathrm{Tr}_1^n(x^{2^l+1})$ *and let the polynomial* $\tilde{f}(x)$ *be defined by:*

$$\tilde{f}(x) = f(\beta x) + f(x) \tag{4.18}$$

where $\beta = \alpha^\tau \in \mathbb{F}_{2^n}$ *and* $\beta \notin \mathbb{F}_2$. *Then the dimension of the radical* $\mathcal{W}$ *is:*

$$\dim(\mathcal{W}) = \begin{cases} 0, & 2^{n-1} \textit{ times,} \\ 2, & 2^{n-1} \textit{ times.} \end{cases} \tag{4.19}$$

Proof. To find the rank of the quadratic form $\tilde{f}(x)$, we use the equation below given by Boztaş and Kumar in [6]:

$$B_f(x, y) = f(x) + f(y) + f(x + y) = \mathrm{Tr}(xy) + \mathrm{Tr}(x)\mathrm{Tr}(y) \tag{4.20}$$

Then for our case, that is for $\tilde{f}(x) = f(\beta x) + f(x)$ we need to find the number of the roots of the symplectic form $B_{\tilde{f}}(x, y)$:

$$\begin{aligned} B_{\tilde{f}}(x, y) &= \mathrm{Tr}(xy) + \mathrm{Tr}(x)\mathrm{Tr}(y) + \mathrm{Tr}(\beta x \beta y) + \mathrm{Tr}(\beta x)\mathrm{Tr}(\beta y) \\ &= \mathrm{Tr}(xy) + \mathrm{Tr}(y\mathrm{Tr}(x)) + \mathrm{Tr}(\beta x \beta y) + \mathrm{Tr}(\beta y \mathrm{Tr}(\beta x)) \\ &= \mathrm{Tr}(y(x + \mathrm{Tr}(x))) + \mathrm{Tr}(\beta y(\beta x + \mathrm{Tr}(\beta x))) \\ &= \mathrm{Tr}(y(x + \mathrm{Tr}(x) + \beta^2 x + \beta \mathrm{Tr}(\beta x))) \end{aligned}$$

To find the rank of $\tilde{f}(x)$, we need to find the number of the roots of the polynomial

$$h(x) = x + \mathrm{Tr}(x) + \beta^2 x + \beta \mathrm{Tr}(\beta x). \tag{4.21}$$

where $\beta = \alpha^\tau \in \mathbb{F}_{2^n}$ and $\beta \notin \mathbb{F}_2$. We give the proof in four cases depending on the values of $\mathrm{Tr}(x)$ and $\mathrm{Tr}(\beta x)$.

a) If $\mathrm{Tr}(x) = 0$ and $\mathrm{Tr}(\beta x) = 0$, then

$$h(x) = x + \beta^2 x = 0 \iff x(1 + \beta^2) = 0.$$

As $(1 + \beta^2) \neq 0$, $x = 0$ is a root of the polynomial $h(x)$.

b) If $\mathrm{Tr}(x) = 0$ and $\mathrm{Tr}(\beta x) = 1$, then

$$h(x) = \beta + x + \beta^2 x = 0 \iff x(1 + \beta^2) = \beta.$$

As $(1 + \beta^2) \neq 0$, $x = \frac{\beta}{1+\beta^2}$ is a root of $h(x)$ under the condition of 4.21, that is:

$$\begin{aligned} h(\frac{\beta}{1+\beta^2}) &= \mathrm{Tr}(\frac{\beta}{1+\beta^2}) + \beta\mathrm{Tr}(\frac{\beta^2}{1+\beta^2}) + \frac{\beta}{1+\beta^2} + \frac{\beta^3}{1+\beta^2} \\ &= \mathrm{Tr}(\frac{\beta}{1+\beta^2}) + \beta[1 + \mathrm{Tr}(\frac{\beta^2}{1+\beta^2})] = 0 \end{aligned}$$

As a result, $x = \frac{\beta}{1+\beta^2}$ is a root of $h(x)$ if $\mathrm{Tr}(\frac{\beta^2}{1+\beta^2}) = 1$ and $\mathrm{Tr}(\frac{\beta}{1+\beta^2}) = 0$.

c) If $\mathrm{Tr}(x) = 1$ and $\mathrm{Tr}(\beta x) = 0$, then

$$h(x) = 1 + x + \beta^2 x + = 0 \iff x(1+\beta^2) = 1.$$

As $(1+\beta^2) \neq 0$, $x = \frac{1}{1+\beta^2}$ is a root of $h(x)$ under the condition of 4.21, that is:

$$\begin{aligned} h(\frac{1}{1+\beta^2}) &= \mathrm{Tr}(\frac{1}{1+\beta^2}) + \beta\mathrm{Tr}(\frac{\beta}{1+\beta^2}) + \frac{1}{1+\beta^2} + \frac{\beta^2}{1+\beta^2} \\ &= \mathrm{Tr}(\frac{1}{1+\beta^2}) + \beta\mathrm{Tr}(\frac{\beta}{1+\beta^2}) + 1 = 0 \end{aligned}$$

As a result, $x = \frac{1}{1+\beta^2}$ is a root of $h(x)$ if $\mathrm{Tr}(\frac{\beta}{1+\beta^2}) = 0$ and $\mathrm{Tr}(\frac{1}{1+\beta^2}) = 1$.

d) If $\mathrm{Tr}(x) = 1$ and $\mathrm{Tr}(\beta x) = 1$, then

$$h(x) = x + \beta^2 x + 1 + \beta = 0 \iff x(1+\beta^2) = 1 + \beta.$$

As $(1+\beta^2) \neq 0$, $x = \frac{1+\beta}{1+\beta^2}$ is a root of $h(x)$ under the condition of 4.21, that is:

$$\begin{aligned} h(\frac{1+\beta}{1+\beta^2}) &= \mathrm{Tr}(\frac{1+\beta}{1+\beta^2}) + \beta\mathrm{Tr}(\frac{\beta+\beta^2}{1+\beta^2}) + \frac{1+\beta}{1+\beta^2} + \frac{\beta^2+\beta^3}{1+\beta^2} \\ &= \mathrm{Tr}(\frac{1+\beta}{1+\beta^2}) + \beta\mathrm{Tr}(\frac{\beta+\beta^2}{1+\beta^2}) + \beta + 1 = 0 \end{aligned}$$

As a result, $x = \frac{1+\beta}{1+\beta^2}$ is a root of $h(x)$ if $\mathrm{Tr}(\frac{1+\beta}{1+\beta^2}) = 1$ and $\mathrm{Tr}(\frac{\beta+\beta^2}{1+\beta^2}) = 1$.

Combining all cases together, we see that the conditions in (b) are equivalent to the conditions in (d). If $\exists \beta \in \mathbb{F}_{2^n} - \mathbb{F}_2$, satisfying $\mathrm{Tr}(\frac{1}{1+\beta^2}) = 1$ and $\mathrm{Tr}(\frac{\beta}{1+\beta^2}) = 0$, then the radical $\mathcal{W} = Sp\{\frac{\beta}{1+\beta^2}, \frac{1}{1+\beta^2}\}$, otherwise the radical $\mathcal{W} = 0$. There exist exactly 2^{n-1} such β where $\mathrm{Tr}(\frac{1}{1+\beta^2}) = 1$ and $\mathrm{Tr}(\frac{\beta}{1+\beta^2}) = 0$, and 2^{n-1} such β where trace conditions does not satisfied, which means that:

$$\dim(\mathcal{W}) = \begin{cases} 0, & 2^{n-1} \text{ times}, \\ 2, & 2^{n-1} \text{ times}. \end{cases}$$

□

Theorem 4.4. *The correlation distribution of the new binary sequence family $\mathcal{S}$ is:*

$$S_{i,j}(\tau) = \begin{cases} -1 + 2^n, & 2^n + 1 & \textit{times} \\ -1, & 2^{3n-2} + 2^{3n-3} + 2^{2n} - 2 & \textit{times} \\ -1 + 2^{\frac{n}{2}}, & (2^{2n-1} - 2)(2^{n-1} + 2^{\frac{n-2}{2}}) & \textit{times} \\ -1 - 2^{\frac{n}{2}}, & (2^{2n-1} - 2)(2^{n-1} - 2^{\frac{n-2}{2}}) & \textit{times} \\ -1 + 2^{\frac{n}{2}+1}, & 2^{2n-3}(2^{n-1} + 2^{\frac{n}{2}}) & \textit{times} \\ -1 - 2^{\frac{n}{2}+1}, & 2^{2n-3}(2^{n-1} - 2^{\frac{n}{2}}) & \textit{times}. \end{cases} \tag{4.22}$$

Proof. For the family $\mathcal{S}$ we will examine the correlation distribution in 5 cases:

Case 1: When $i = j$ and $\tau = 0$:

$$\begin{aligned} C_{i,j}(\tau) = C_{i,i}(0) &= \sum_{0 \le t \le 2^n - 2} (-1)^{s_i(t) + s_i(t)} \\ &= \sum_{0 \le t \le 2^n - 2} (-1)^0 = 2^n - 1. \end{aligned}$$

That is $C_{i,j}(\tau) = -1 + 2^n,\ 2^n + 1$ times.

Case 2: When $i = j = 2^n + 1$ and $\tau \neq 0$ then

$$\begin{aligned} C_{2^n+1,2^n+1}(\tau) &= \sum_{0 \le t \le 2^n - 2} (-1)^{s_{2^n+1}(t) + s_{2^n+1}(t+\tau)} \\ &= \sum_{0 \le t \le 2^n - 2} (-1)^{\mathrm{Tr}(\alpha^t) + \mathrm{Tr}(\alpha^{t+\tau})} \\ &= \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}(x + \beta x)} \\ &= \sum_{y \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}(y)} \\ &= -1 + \sum_{y \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(y)} = -1 \end{aligned}$$

We used $\alpha^\tau = \beta, \quad \alpha^t = x, (1 + \beta x) = y$. That means $C_{i,j}(\tau) = -1$, $2^n - 2$ times.

Case 3: a) Let $i = 2^n + 1$ and $j \neq 2^n + 1$, fix τ, $0 \le \tau \le 2^n - 2$:

$$\begin{aligned} C_{2^n+1,j}(\tau) &= \sum_{0 \le t \le 2^n - 2} (-1)^{\mathrm{Tr}(\alpha^t) + \mathrm{Tr}(\zeta_j \alpha^{t+\tau}) + f(\alpha^{t+\tau})} \\ &= \sum_{0 \le t \le 2^n - 2} (-1)^{\mathrm{Tr}(\alpha^t(1 + \zeta_j \beta)) + f(\alpha^{t+\tau})} \\ &= \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}(\gamma_1 x) + f(\beta x)} \\ &= \sum_{y \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}(\gamma_2 y) + f(y)}. \end{aligned}$$

Where $\alpha^\tau = \beta$, $\alpha^t = x$, $1 + \zeta_j \beta = \gamma_1$, $\beta x = y$ and $\gamma_1 = \gamma_2 \beta$. There exists one to one correpondence between $1 \le j \le 2^n$ and $\gamma_2 \in \mathbb{F}_{2^n}$. Then the exponent can be written of the form:

$$f(x) + \mathrm{Tr}(\gamma_2 x) = g(x) + \Psi_a(x) \tag{4.23}$$

where $g(x)$ is a quadratic form and $\Psi_a(x)$ is linear transformation. Fix a standard basis $\{e_1, e_2, ..., e_n\}$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and let $\dim \mathcal{W} = k$. In [8], it is shown that if n is even

then the polynomial $g(x) = g(e_1x_1, e_2x_2, ..., e_{n-k}x_{n-k})$ can be shown in two types:

Type 1 : $g(e_1x_1, e_2x_2, ..., e_{n-k}x_{n-k}) = x_1x_2 + x_3x_4 + ... + x_{n-k-1}x_{n-k}$
$= H_1(x_1, x_2, ..., x_{n-k})$,

Type 2 : $g(e_1x_1, e_2x_2, ..., e_{n-k}x_{n-k}) = x_1x_2 + x_3x_4 + ... + x_{n-k-1}x_{n-k} + x_{n-k-1}^2 + dx_{n-k}^2$
$= H_2(x_1, x_2, ..., x_{n-k})$,

where $\mathrm{Tr}_1^n(d) = 1$. Let $a_1 = \Psi_a(e_1), a_2 = \Psi_a(e_2), ..., a_{n-k} = \Psi_a(e_{n-k})$ and

$$C_1 = H_1(a_2, a_1, ..., a_{n-k}, a_{n-k-1}),$$
$$C_2 = H_2(a_2, a_1, ..., a_{n-k}, a_{n-k-1}),$$

Çakçak and Özbudak [8] showed that for $i = 1, 2$, Type 1 and Type 2 can be written as:

$$\begin{aligned} &g(e_1x_1, e_2x_2, ..., e_{n-k}x_{n-k}, d_1y_1, ..., d_ky_k) + \Psi_a(e_1x_1, e_2x_2, ..., e_{n-k}x_{n-k}, d_1y_1, ..., d_ky_k) \\ &= H_i(x_1, x_2, ..., x_{n-k}) + (a_1x_1 + a_2x_2, ... + a_{n-k}x_{n-k}) \\ &= H_i(x_1 + a_2, x_2 + a_1, ..., x_{n-k-1} + a_{n-k}, x_{n-k} + a_{n-k-1}) + C_i \end{aligned}$$

Finally, we give the theorem below and then using these information, we continue to our proof of Case 3.

Theorem 4.5. *In [20], for even n, $d \in \mathbb{F}_2$, $\mathrm{Tr}_1^n(d) = 1$, the number of the solutions of the equation*

$$x_1x_2 + x_3x_4 + ... + x_{n-k-1}x_{n-k} = H_1(x_1, x_2, ..., x_{n-k}) = b \tag{4.24}$$

is given by

$$N = 2^{n-k-1} + v(b)2^{\frac{n-k-2}{2}} \tag{4.25}$$

and the number of the solutions of the equation

$$x_1x_2 + x_3x_4 + ... + x_{n-k-1}x_{n-k} + x_{n-k-1}^2 + dx_{n-k}^2 = H_2(x_1, x_2, ..., x_{n-k}) = b$$

is given by

$$N = 2^{n-k-1} - v(b)2^{\frac{n-k-2}{2}}. \tag{4.26}$$

For our case, using these information above, using Type 1 and $k = 0$, the number of the solutions is given by:

$$N = \begin{cases} 2^{n-1} + 2^{\frac{n-2}{2}}, & \text{if} \quad b = 0; \\ 2^{n-1} - 2^{\frac{n-2}{2}}, & \text{if} \quad b = 1. \end{cases} \tag{4.27}$$

We can now continue to our proof of correlation distribution of Case 3. Let $\gamma_2 = a$, then:

$$\begin{aligned} C_{2^n+1,j}(\tau) &= -1 + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(ax)+f(x)} \\ &= -1 + \sum_{x_1,x_2,...,x_n \in \mathbb{F}_2} (-1)^{H_1(x_1+a_2, x_2+a_1, ..., x_n+a_{n-1})+c_1} \\ &= -1 + \sum_{y_1,y_2,...,y_n \in \mathbb{F}_2} (-1)^{H_1(y_1,y_2,...,y_{n-1},y_n)+c_1} = T \end{aligned}$$

When $c_1 = 0$,

$$T = -1 + \sum_{H_1(y_1,\ldots,y_n)=0} (1) + \sum_{H_1(y_1,\ldots,y_n)=1} (-1)$$
$$= 2^{n-1} + 2^{\frac{n-2}{2}} - (2^{n-1} - 2^{\frac{n-2}{2}}) = -1 + 2^{\frac{n}{2}}$$

When $c_1 = 1$ using the same method,

$$T = -1 + \sum_{H_1(y_1,\ldots,y_n)=0} (-1) + \sum_{H_1(y_1,\ldots,y_n)=1} (1) = -1 - 2^{\frac{n}{2}}$$

As a result for $i = 2^n + 1$ and $j \neq 2^n + 1$ the correlation distribution of the sequence family $\mathcal{S}$ is given by:

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

Note that the solution is the same for Type 2.

Case 3: b) For $j = 2^n + 1$, $i \neq 2^n + 1$ as the correlation function is equivalent with the Case 3 (a). The correlation distribution is the same and given by:

$$C_{2^n+1,j}(\tau) = \begin{cases} -1 + 2^{\frac{n}{2}}, & (2^n - 1)(2^{n-1} + 2^{\frac{n-2}{2}})\text{times} \\ -1 - 2^{\frac{n}{2}}, & (2^n - 1)(2^{n-1} - 2^{\frac{n-2}{2}})\text{times}. \end{cases} \tag{4.28}$$

Case 4: Let $\tau = 0$, $1 \leq i, j \leq 2^n$ and $i \neq j$ then:

$$\begin{aligned} C_{i,j}(\tau) &= \sum_{0 \leq t \leq 2^n - 2} (-1)^{s_i(t) + s_j(t)} \\ &= \sum_{0 \leq t \leq 2^n - 2} (-1)^{\mathrm{Tr}(\zeta_i \alpha^t) + f(\alpha^t) + \mathrm{Tr}(\zeta_j \alpha^t) + f(\alpha^t)} \\ &= \sum_{0 \leq t \leq 2^n - 2} (-1)^{\mathrm{Tr}((\zeta_i + \zeta_j)\alpha^t)} \\ &= \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}(x)} = -1 + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(x)} = -1 \end{aligned}$$

where $(\zeta_i + \zeta_j)\alpha^t = x$. Which means $C_{i,j}(\tau) = -1$ exactly $2^n(2^n - 1)$ times.

Case 5: The final case is $\tau \neq 0$, $1 \leq \tau \leq 2^n - 2$ and $1 \leq i, j \leq 2^n$. Then the

correlation function:

$$\begin{aligned} C_{i,j}(\tau) &= \sum_{0\le t\le 2^n-2} (-1)^{s_i(t)+s_j(t+\tau)} \\ &= \sum_{0\le t\le 2^n-2} (-1)^{\mathrm{Tr}(\zeta_i\alpha^t)+f(\alpha^t)+\mathrm{Tr}(\zeta_j\alpha^{t+\tau})+f(\alpha^{t+\tau})} \\ &= \sum_{0\le t\le 2^n-2} (-1)^{\mathrm{Tr}((\zeta_i+\zeta_j\beta)\alpha^t)+f(\alpha^t)+f(\beta\alpha^t)} \\ &= \sum_{x\in\mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}(\gamma x)+f(x)+f(\beta x)} \end{aligned}$$

where $\alpha^\tau = \beta, \zeta_i + \zeta_j\beta = \gamma, \alpha^t = x$. Then we define:

$$\tilde{f}(x) = f(\beta x) + f(x) \tag{4.29}$$

It turns out that $\tilde{f}$ has the rank $2r = n-2$ or $2r = n$, depending on some technical conditions on β. Please see Lemma 4.3 for the details.

For $\beta \in \mathbb{F}_{2^n}$ and β does not satisfy the trace conditions $\mathrm{Tr}(\frac{1}{1+\beta^2}) = 1$ and $\mathrm{Tr}(\frac{\beta}{1+\beta^2}) = 0$ at the same time, then $\tilde{f}(x)$ has full rank. Then the correlation distribution is:

$$C_{2^n+1,j}(\tau) = \begin{cases} -1+2^{\frac{n}{2}}, & 2^n(2^{n-1}-2)(2^{n-1}+2^{\frac{n-2}{2}})\text{times} \\ -1-2^{\frac{n}{2}}, & 2^n(2^{n-1}-2)(2^{n-1}-2^{\frac{n-2}{2}})\text{times}. \end{cases} \tag{4.30}$$

And for $\beta \in \mathbb{F}_{2^n}$ under the condition of $\mathrm{Tr}(\frac{1}{1+\beta^2}) = 1$ and $\mathrm{Tr}(\frac{\beta}{1+\beta^2}) = 0$, $\tilde{f}(x)$ has rank $2r = n-2$, then the exponent of the correlation function can be written as

$$\tilde{f}(x) + \mathrm{Tr}(\gamma x) = g(x) + \Psi_a(x) \tag{4.31}$$

where $g(x)$ is a quadratic form and $\Psi_a(x)$ is linear transformation. Then Type 1 and Type 2 are given by:

$$\begin{aligned} \text{Type 1}: g(e_1x_1, e_2x_2, ..., e_{n-2}x_{n-2}) &= x_1x_2 + x_3x_4 + ... + x_{n-3}x_{n-2} \\ &= H_1(x_1, x_2, ..., x_{n-2}) \\ \text{Type 2}: g(e_1x_1, e_2x_2, ..., e_{n-2}x_{n-2}) &= x_1x_2 + x_3x_4 + ... + x_{n-3}x_{n-2} + x_{n-3}^2 + dx_{n-2}^2 \\ &= H_2(x_1, x_2, ..., x_{n-2}) \end{aligned}$$

where $\mathrm{Tr}_1^n(d) = 1$. Let $a_1 = \Psi_a(e_1), a_2 = \Psi_a(e_2), ..., a_{n-2} = \Psi_a(e_{n-2})$ and

$$\begin{aligned} C_1 &= H_1(a_2, a_1, ..., a_{n-2}, a_{n-3}), \\ C_2 &= H_2(a_2, a_1, ..., a_{n-2}, a_{n-3}). \end{aligned}$$

For $i = 1, 2$, Çakçak and Özbudak [8] showed that for Type 1 and Type 2 the following is satisfied:

$$\begin{aligned} &g(e_1x_1, e_2x_2, ..., e_{n-2}x_{n-2}, d_1y_1, d_2y_2) + \Psi_a(e_1x_1, e_2x_2, ..., e_{n-2}x_{n-2}, d_1y_1, d_2y_2) \\ &\quad = H_i(x_1, x_2, ..., x_{n-2}) + a_1x_1 + a_2x_2, ... + a_{n-2}x_{n-2} \\ &\quad = H_i(x_1 + a_2, x_2 + a_1, ..., x_{n-3} + a_{n-2}, x_{n-2} + a_{n-3}) + C_i \end{aligned}$$

Using the Theorem 4.5, and $k = 2$, then the number of the solutions of Type 1:

$$N = \begin{cases} 4(2^{n-3} + 2^{\frac{n-4}{2}}), & \text{if} \quad b = 0; \\ 4(2^{n-3} - 2^{\frac{n-4}{2}}), & \text{if} \quad b = 1. \end{cases} \tag{4.32}$$

Finally, let $\gamma = a$ and $i = 1, ...n-2$, then the correlation function

$$\begin{aligned} C_{i,j}(\tau) &= -1 + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(ax) + \tilde{f}(x)} \\ &= -1 + \sum_{x_i \in \mathbb{F}_2} (-1)^{H_1(x_1 + a_2, x_2 + a_1, ..., x_{n-2} + a_{n-3}) + c_1} \\ &= -1 + \sum_{y_i \in \mathbb{F}_2} (-1)^{H_1(y_1, y_2, ..., y_{n-2}) + c_1} = T \end{aligned}$$

When $c_1 = 0$,

$$\begin{aligned} T &= -1 + 4(\sum_{H_1(y_1,...,y_{n-2})=0} (1) + \sum_{H_1(y_1,...,y_{n-2})=1} (-1)) \\ &= -1 + 4(2^{n-3} + 2^{\frac{n-4}{2}} - (2^{n-3} - 2^{\frac{n-4}{2}})) = -1 + 2^{\frac{n}{2}+1} \end{aligned}$$

When $c_1 = 1$ by the same method,

$$\begin{aligned} T &= -1 + 4(\sum_{H_1(y_1,...,y_{n-2})=0} (-1) + \sum_{H_1(y_1,...,y_{n-2})=1} (1)) \\ &= -1 - 2^{\frac{n}{2}+1} \end{aligned}$$

After computing the number of $R_{i,j}(\tau) = -1$ case, we have the correlation distribution under the condition of $\mathrm{Tr}(\frac{1}{1+\beta^2}) = 1$ and $\mathrm{Tr}(\frac{\beta}{1+\beta^2}) = 0$, $\tilde{f}(x)$ as:

$$C_{i,j}(\tau) = \begin{cases} -1, & 2^{3n-2} + 2^{3n-3} \quad \text{times} \\ -1 + 2^{\frac{n}{2}+1}, & 2^{2n-3}(2^{n-1} + 2^{\frac{n}{2}}) \text{times} \\ -1 - 2^{\frac{n}{2}+1}, & 2^{2n-3}(2^{n-1} - 2^{\frac{n}{2}}) \text{times}. \end{cases} \tag{4.33}$$

Note that Type 2 gives the same distribution of $R_{i,j}(\tau)$. Then the total correlation distribution for case 5 is given by:

$$C_{i,j}(\tau) = \begin{cases} -1, & 2^{3n-2} + 2^{3n-3} & \text{times} \\ -1 + 2^{\frac{n}{2}}, & 2^n(2^{n-1} - 2)(2^{n-1} + 2^{\frac{n-2}{2}}) & \text{times} \\ -1 - 2^{\frac{n}{2}}, & 2^n(2^{n-1} - 2)(2^{n-1} - 2^{\frac{n-2}{2}}) & \text{times} \\ -1 + 2^{\frac{n}{2}+1}, & 2^{2n-3}(2^{n-1} + 2^{\frac{n}{2}}) & \text{times} \\ -1 - 2^{\frac{n}{2}+1}, & 2^{2n-3}(2^{n-1} - 2^{\frac{n}{2}}) & \text{times}. \end{cases} \tag{4.34}$$

Finally, collecting all 5 cases together, we have the correlation distribution of the se-

quence family $\mathcal{S}$ and it is given by:

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

□

Note that in this proof not only have we computed the correlation distribution, but also we have determined all cross-correlation values exactly depending on $\beta \in \mathbb{F}_{2^n}$.

Corollary 4.6. *According to the correlation function distribution, maximum correlation magnitude $C_{\max}$ of the sequence family is $(1+2^{\frac{n}{2}+1})$.*

We now point out a link between our construction and plateaued boolean functions.

Corollary 4.7. *As has been shown above, the rank of the quadratic form $f(x)$ is equal to $2r = n$, i.e., the function f is 0-plateaued and so f is bent. In Appendix 2 it is shown that the rank of the quadratic form $\tilde{f}(x) = f(x) + f(x\alpha^\tau)$ is equal to $2r = n-2$ when $\mathrm{Tr}(\frac{1}{1+\beta^2}) = 1$ and $\mathrm{Tr}(\frac{\beta}{1+\beta^2}) = 0$ where $\beta = \alpha^\tau$. Under these conditions, $\tilde{f}$ is 2-plateaued and so semi-bent. Otherwise the rank of the quadratic form $\tilde{f}(x)$ is equal to $2r = n$ so again $\tilde{f}$ is 0-plateaued and so bent.*

4.4 Results

In this chapter, we construct a sequence family for even positive integer n over the finite field $\mathbb{F}_{2^n}$. We prove this family's correlation distribution and determine the $\beta \in \mathbb{F}_{2^n}$ elements for all correlation values.

The maximum cross-correlation magnitude $C_{\max}$ of the sequence family is found as $(1+2^{\frac{n}{2}+1})$. This shows that the family has low maximum cross-correlation magnitude which is advantageous for the use of the sequence family in CDMA applications.

Moreover, when n is even, the small set of Kasami sequences $\mathcal{K}$ is defined (see the survey by Helleseth and Kumar [10]) as below:

Definition 4.6. The small Kasami sequence family $\mathcal{K} = \{k_i : i = 0, 1, 2, ..., 2^{n/2}\}$ is defined as

$$k_i(t) = \begin{cases} \mathrm{Tr}_1^n(\alpha^t) + \mathrm{Tr}_1^{n/2}(\eta_i \alpha^{(2^{n/2}+1)t}), & 0 \le i < 2^{n/2} \\ \mathrm{Tr}_1^n(\alpha^t), & i = 2^{n/2}. \end{cases}$$

where $\{\eta_i\}_{i=0,1,...,2^{n/2}-1}$ is an enumeration of the subfield $\mathbb{F}_{2^{n/2}}$ of $\mathbb{F}_{2^n}$.

Comparison: The nontrivial correlation values of the small Kasami sequence family lie in the set

$$\{-1, -1 \pm 2^{n/2}\}$$

which make the small Kasami set optimal with respect to the Sidelnikov lower bound. However, the small Kasami set has a much smaller size compared to our design $\mathcal{S}$. On the other hand, our sequences do not attain the Sidelnikov lower bound, and thus are suboptimal.

CHAPTER 5

CORRELATION DISTRIBUTION OF GOLD-LIKE SEQUENCE FAMILY GENERATED BY PLATEAUED FUNCTIONS

Sequence families having low maximum correlation magnitude are used in direct sequence code division multiple access (DS-CDMA) which allows multiple users to utilizate the system simultaneously in the same bandwith without interfering each other. Different orthogonal and non-orthogonal (such as Gold [9] or Kasami Sequences [15]) codes are assigned to the users according to the required properties of the system. To demodulate the received signal, one needs to multiply it with the code used during the transmission. To keep the signals protected and maintain privacy, density of the transmitted signal should be lower than the noise density. The sender ensures that the receiver can demodulate the hiding signal in the noise if the receiver knows the code used during the trasmission.

The CDMA system performs best when there is a clear separation between the signal of desired users and other users. Receiver can separate the signal by correlating the desired signal code with other received signals. If the signal matches with the code of the user, then the cross-correlation function will be high and the system can extract the signal. Otherwise, the cross-correlation is close to zero. The aim is to faciliate synchronization and to minimize the interference due to other users [28].

For these purposes, sequences having low maximum correlation magnitude $C_{\max}$ play an important role when constructing a new sequence family. Some lower bounds such as Sidelnikov bound [27] are used in sequence design.

Boztaş and Kumar constructed Gold-like sequences which satisfies Sidelnikov's bound and computed their correlation distribution in [6] by using the quadratic form technique. This construction set up when n is an odd integer and $p = 2$.

In this chapter, we generalized Gold-like sequences for arbitrary positive integer n and arbitrary prime number p by using an arbitrary s-plateaued function instead of a fixed quadratic form but keeping the rest of the construction same. Later, we give the correlation values of the sequence family depending on p and n, taking the Gold function as plateaued function.

5.1 Preliminaries

Let p be a prime number, $\mathbb{F}_p$ be a finite field and $\mathbb{F}_{p^n}$ be an extension field of $\mathbb{F}_p$ where n is an odd integer and α is a primitive element of $\mathbb{F}_{p^n}$. For two arbitrary sequences $u = (u(0), u(1), ..., u(N-1))$ and $v = (v(0), v(1), ..., v(N-1))$ of period N, the periodic correlation function of these sequences is defined by

$$C_{u,v}(\tau) = \sum_{t=0}^{N-1} (\zeta_p)^{u(t+\tau)-v(t)}. \tag{5.1}$$

Here ζ_p is the complex primitive p-th root of unity. The maximum correlation magnitude of a sequence family is defined as

$$C_{\max} = \max\{|C_{u,v}(\tau)| : \ u \neq v, \ \text{ or } \ u = v \ \text{ and } \ \tau \neq 0\}. \tag{5.2}$$

For a given function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, the Walsh transform of the function is equal to the set of correlations between f and the linear functions $\mathrm{Tr}_1^n(\lambda x)$ which is given by

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_{p^n}} (\zeta_p)^{f(x)-\mathrm{Tr}_1^n(\lambda x)}. \tag{5.3}$$

Definition 5.1. A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is called s-plateaued if its absolute Walsh transform values are in $\{0, p^{\frac{n+s}{2}}\}$ for some $s = 1, ..., n$. f is called 0-plateaued if its absolute Walsh transform value equals to $p^{\frac{n}{2}}$.

Lemma 5.1. *If $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is an s-plateaued function, where $1 \leq s \leq n$, then the absolute value of the Walsh transform is*

$$|W_f(\lambda)| = \begin{cases} p^{\frac{n+s}{2}}, & p^{n-s} \quad \textit{times}, \\ 0, & p^n - p^{n-s} \quad \textit{times}. \end{cases} \tag{5.4}$$

If $f(x)$ is a 0-plateaued function in $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, then the absolute value of the Walsh transform is exactly $p^{\frac{n}{2}}$, p^n times. More specifically when $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, the Walsh transform distribution is given by:

$$W_f(\lambda) = \begin{cases} 2^{\frac{n+s}{2}}, & 2^{n-s-1} + 2^{\frac{n-s-2}{2}} \quad \textit{times}, \\ 0, & 2^n - 2^{n-s} \quad \textit{times}, \\ -2^{\frac{n+s}{2}}, & 2^{n-s-1} - 2^{\frac{n-s-2}{2}} \quad \textit{times}, \end{cases} \tag{5.5}$$

for $s \neq 0$. If $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is an 0-plateaued function then

$$W_f(\lambda) = \begin{cases} 2^{\frac{n}{2}}, & 2^{n-1} \quad \textit{times}, \\ -2^{\frac{n}{2}}, & 2^{n-1} \quad \textit{times}. \end{cases} \tag{5.6}$$

A quadratic form $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ can be written as

$$f(x) = \mathrm{Tr}_1^n(a_0 x^{1+p^0} + a_1 x^{1+p} + a_1 x^{1+p^2} + ... + a_t x^{1+p^t}), \tag{5.7}$$

where $t = \lceil \frac{n}{2} \rceil$. To calculate the correlation distribution of a given sequence generated by a quadratic function $f(x)$, it is enough to compute the rank of the quadratic form. For this purpose, the symplectic form of the quadratic form is defined by

$$B(x, y) = f(x + y) - f(x) - f(y) \tag{5.8}$$

and it is bilinear. Then the radical is

$$\mathcal{W} = \{x \in \mathbb{F}_{p^n} : B(x, y) = 0 \ \forall y \in \mathbb{F}_{p^n}\}. \tag{5.9}$$

If N is the the number of the elements in the radical $\mathcal{W}$, then the rank r of the quadratic form $f(x)$ can be computed by

$$r = n - \log_p N. \tag{5.10}$$

Lemma 5.2. *A quadratic function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is s-plateaued if and only if $rank f(x) = r = n - s$ for some $s = 0, 1, ..., n$.*

Corollary 5.3. *A quadratic function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is s-plateaued if and only if $s = \log_p N$ where N is the the number of the elements of the radical $\mathcal{W}$ of the quadratic form.*

Definition 5.2. Let $\mathbb{F}$ be an arbitrary field. An algebraic curve over $\mathbb{F}$ is the equation $F(x, y) = 0$. Here, $F/\mathbb{F}$ is the function field.

Definition 5.3. Let C be an algebraic curve defined by $F(x, y) = 0$ over $\mathbb{F}$ and let $\mathcal{F}$ be a field containing $\mathbb{F}$. The $\mathcal{F}$ rational points of C are the solutions of the curve $F(x, y) = 0$ for $x, y \in \mathcal{F}$.

Definition 5.4. The L-polynomial of the algebraic function field $F/\mathbb{F}$ is defined as

$$L(t) = (1 - t)(1 - qt)Z(t)$$

where $Z(t)$ is the zeta function.

During this chapter, let $F/\mathbb{F}_q$ be a function field with genus g over $\mathbb{F}_q$, $L_F(t)$ denote the L-polynomial, $N_r = N(F_r)$ be the number of places of degree 1 of the field extension $F_r = F\mathbb{F}_{q^r}$ of degree r. Necessary theorems are given according to these notations.

Theorem 5.4. *The L-polynomial satisfies the following properties [30]:*

1. *$L(t)$ factors in $\mathbb{C}[t]$ as*

$$L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t)$$

where $\alpha_1, \ldots, \alpha_{2g}$ are complex numbers satisfying

$$\alpha^m + c_{m-1}\alpha^{m-1} + \cdots + c_1\alpha + c_0 = 0$$

for $c_i \in \mathbb{Z}$ and $\alpha_i + \alpha_{g+i} = q$ for $i = 1, \ldots, g$.

2. *If* $L_n(t) = (1-t)(1-q^n t)Z_n(t)$ *is the L-polynomial of the extension field* $F_r = F\mathbb{F}_{q^r}$*, then similarly for* α_i *satisfying the conditions above,*

$$L_r(t) = \prod_{i=1}^{2g}(1-\alpha_i^r t).$$

Corollary 5.5. *For all* $n \geq 1$*, the number of places of degree* 1 *is given as follows*

$$N_n = q^n + 1 - \sum_{i=1}^{2g} \alpha_i^r$$

where $\alpha_1, \ldots, \alpha_{2g}$ *are given in the L-polynomial [30]. In particular for* $n = 1$*, since* $N_1 = N(F)$*,*

$$N = N(F) = q + 1 - \sum_{i=1}^{2g} \alpha_i.$$

Theorem 5.6 (Hasse-Weil Theorem)**.** *The reciprocals of the roots of the L-polynomial* $L(t)$ *satisfy*

$$|\alpha_i| = q^{1/2}$$

for $i = 1, \ldots, 2g$*.*

Theorem 5.7 (Hasse-Weil Bound)**.** *The number* $N_n = N(F_n)$ *of degree one places of the function field* $F_n/\mathbb{F}_{q^n}$ *satisfies*

$$|N_n - (q^n + 1)| \leq 2gq^{n/2}$$

for all $n \geq 1$*.*

A curve is called maximal if it attains the upper Hasse-Weil Bound.

Definition 5.5. The Gold sequence family S is constructed by using the quadratic form $f(x) = \mathrm{Tr}_1^n(x^{2+1})$ when n is an odd integer. The family

$$\mathcal{S} = \{s_i(t) : i = 0, 1, 2, ..., 2^n\}$$

is defined as

$$s_i(t) = \begin{cases} \mathrm{Tr}_1^n(\zeta_i \alpha^t) + f(\alpha^t), & 0 \leq i < 2^n \\ \mathrm{Tr}_1^n(\alpha^t), & i = 2^n \end{cases}$$

where ζ_i is an enumeration of $\mathbb{F}_{2^n}$, α is a primitive element of $\mathbb{F}_{2^n}$, $0 \leq t \leq 2^n - 2$. The correlation values of the Gold sequence family are $\{-1, -1 + 2^{\frac{n+1}{2}}, -1 - 2^{\frac{n+1}{2}}\}$.

Boztaş and Kumar [6] studied the quadratic form $p(x) = \sum_{l=1}^{\frac{n-1}{2}} \mathrm{Tr}_1^n(x^{2^l+1})$ when n is an odd integer. They defined the sequence family $\mathcal{G}$ and gave the correlation distribution of the family.

Definition 5.6. Let n be an odd integer. The Gold-like sequence family

$$\mathcal{G} = \{g_i(t) : i = 0, 1, 2, ..., 2^n\}$$

is defined as

$$g_i(t) = \begin{cases} \mathrm{Tr}_1^n(\zeta_i \alpha^t) + p(\alpha^t), & 0 \leq i < 2^n \\ \mathrm{Tr}_1^n(\alpha^t), & i = 2^n \end{cases} \tag{5.11}$$

where ζ_i is an enumeration $\mathbb{F}_{2^n}$, α is a primitive element of $\mathbb{F}_{2^n}$ and $0 \leq t \leq 2^n - 2$. The correlation distribution of the family is

$$C_{i,j}(\tau) = \begin{cases} -1 + 2^n, & 2^n + 1 \quad \text{times} \\ -1, & 2^{3n-1} + 2^{2n} - 2^n - 2 \quad \text{times} \\ -1 + 2^{\frac{n+1}{2}}, & (2^{2n} - 2)(2^{n-2} + 2^{\frac{n-3}{2}}) \quad \text{times} \\ -1 - 2^{\frac{n+1}{2}}, & (2^{2n} - 2)(2^{n-2} - 2^{\frac{n-3}{2}}) \quad \text{times.} \end{cases} \tag{5.12}$$

5.2 Classification of a Sequence Family Using Plateaued Functions

Definition 5.7. Let $\mathbb{F}_{p^n} = \{\omega_1, \omega_2, ..., \omega_{p^n}\}$ be an enumeration of the elements of the finite field $\mathbb{F}_{p^n}$, α be a primitive element of $\mathbb{F}_{p^n}$ and $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be an s-plateaued function where s is arbitrary. For $0 \leq t \leq p^n - 2$, the sequence family

$$\mathcal{V} = \{v_i(t) : i = 1, 2, ..., p^n + 1\} \tag{5.13}$$

is defined as

$$v_i(t) = \begin{cases} \mathrm{Tr}_1^n(\omega_i \alpha^t) + f(\alpha^t), & 1 \leq i \leq p^n \\ \mathrm{Tr}_1^n(\alpha^t), & i = p^n + 1. \end{cases} \tag{5.14}$$

Theorem 5.8. *For an arbitrary s-plateaued function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ let the sequence family $\mathcal{V}$ be defined as above. Also let*

$$f_\beta(x) = f(\beta x) - f(x)$$

and let N_k be the number of β in $\mathbb{F}_{p^n} - \{0, 1\}$ for which $f_\beta(x)$ is k-plateaued, where $k = 0, 1, ..., m$, $m \leq n$ and

$$N_0 + N_1 + ... + N_m = \#\beta = p^n - 2.$$

Then the correlation distribution of this family satisfies

$$|C_{i,j}(\tau) + (\zeta_p)^l| = \begin{cases} 0, & (p^n - 1)[p^n(p^n - 2) + 2(p^n - p^{n-s})] \\ & +p^n(\sum_{k=1}^{m} N_k(p^n - p^{n-k})) \quad \textit{times} \\ p^n, & p^n + 1 \quad \textit{times} \\ p^{\frac{n+s}{2}}, & 2p^{n-s}(p^n - 1) \quad \textit{times} \\ p^{\frac{n}{2}}, & p^{2n} N_0 \quad \textit{times} \\ p^{\frac{n+1}{2}}, & p^n p^{n-1} N_1 \quad \textit{times} \\ ... & ... \\ p^{\frac{n+m}{2}}, & p^n p^{n-m} N_m \quad \textit{times} \end{cases} \tag{5.15}$$

where $l \in \{0, f(0), -f(0)\}$ and the exact values are given in the proof.

Proof. Throught the proof we will use $\mathrm{Tr}(\cdot)$ for $\mathrm{Tr}_1^n(\cdot)$. The absolute correlation distribution of the sequence family $\mathcal{V}$ is calculated in five cases as follows :

Case 1: When $i = j$ and $\tau = 0$, the cross-correlation function:

$$\begin{aligned} C_{i,j}(\tau) = C_{i,i}(0) &= \sum_{0 \le t \le p^n - 2} (\zeta_p)^{v_i(t) - v_i(t)} \\ &= \sum_{0 \le t \le p^n - 2} (\zeta_p)^0 = p^n - 1 \end{aligned}$$

That is $|C_{i,j}(\tau) + 1| = p^n$ exactly $p^n + 1$ times.

Case 2: When $i = j = p^n + 1$ and $\tau \neq 0$ then the cross-correlation function:

$$\begin{aligned} C_{p^n+1,p^n+1}(\tau) &= \sum_{0 \le t \le p^n - 2} (\zeta_p)^{v_{p^n+1}(t+\tau) - v_{p^n+1}(t)} \\ &= \sum_{0 \le t \le p^n - 2} (\zeta_p)^{\mathrm{Tr}(\alpha^{t+\tau}) - \mathrm{Tr}(\alpha^t)} \\ &= \sum_{x \in \mathbb{F}_{p^n}^*} (\zeta_p)^{\mathrm{Tr}(\beta x - x)} \\ &= \sum_{y \in \mathbb{F}_{p^n}^*} (\zeta_p)^{\mathrm{Tr}(y)} \\ &= -1 + \sum_{y \in \mathbb{F}_{p^n}} (\zeta_p)^{\mathrm{Tr}(y)} = -1 \end{aligned}$$

Here $\alpha^\tau = \beta$, $\alpha^t = x$, $(\beta - 1)x = y$. That means $|C_{i,j}(\tau) + 1| = 0$ exactly $p^n - 2$ times.

Case 3: a) For $i \neq p^n + 1$ and $j = p^n + 1$ fix τ, $0 \le \tau \le p^n - 2$. Then the cross-correlation function:

$$\begin{aligned} C_{i,j}(\tau) &= \sum_{0 \le t \le p^n - 2} (\zeta_p)^{f(\alpha^{t+\tau}) + \mathrm{Tr}(\omega_i \alpha^{t+\tau}) - \mathrm{Tr}(\alpha^t)} \\ &= \sum_{0 \le t \le p^n - 2} (\zeta_p)^{f(\alpha^{t+\tau}) - \mathrm{Tr}((1 - \omega_i \beta)\alpha^t)} \\ &= \sum_{x \in \mathbb{F}_{p^n}^*} (\zeta_p)^{f(\beta x) - \mathrm{Tr}((1 - \omega_i \beta)x)} \\ &= -(\zeta_p)^{f(0)} + \sum_{z \in \mathbb{F}_{p^n}} (\zeta_p)^{f(z) - \mathrm{Tr}((\frac{1}{\beta} - \omega_i)z)} . \end{aligned}$$

Where $\alpha^\tau = \beta$, $\alpha^t = x$ and $\beta x = z$. For fixed β and for $1 \le i \le p^n$, as the ω_i values ranges over $\mathbb{F}_{p^n}$, $(\frac{1}{\beta} - \omega_i)$ takes on all values of $\mathbb{F}_{p^n}$ exactly once.

Now the problem reduces to finding the Walsh distribution so we need to find the plateaued degree of the function $f(x)$. We can then compute the Walsh distribution via

Lemma 5.1 which gives us the correlation distribution. Finally we can determine the number of occurrences by Parseval's identity.

If $f(z)$ is an s-plateaued function, then for $0 \leq \tau \leq p^n - 2, j = p^n + 1$ and $1 \leq i \leq p^n$ the difference between the correlation $C_{i,j}(\tau)$ and $-(\zeta_p)^{f(0)}$ satisfies:

$$|C_{i,j}(\tau) + (\zeta_p)^{f(0)}| = \begin{cases} 0, & (p^n - 1)(p^n - p^{n-s}) \quad \text{times} \\ p^{\frac{n+s}{2}}, & (p^n - 1)p^{n-s} \quad \text{times}, \end{cases} \tag{5.16}$$

via Lemma 5.1.

Case 3: b) For $j \neq p^n + 1$ and $i = p^n + 1$, fix τ, $0 \leq \tau \leq p^n - 2$. Then the cross-correlation function:

$$\begin{aligned} C_{i,j}(\tau) &= \sum_{0 \leq t \leq p^n - 2} (\zeta_p)^{\mathrm{Tr}(\alpha^{t+\tau}) - f(\alpha^t) - \mathrm{Tr}(\omega_j \alpha^t)} \\ &= \sum_{x \in \mathbb{F}_{p^n}^*} (\zeta_p)^{-f(x) - \mathrm{Tr}((\omega_j - \beta)x)} \\ &= -(\zeta_p)^{-f(0)} + \sum_{z \in \mathbb{F}_{p^n}} (\zeta_p)^{-f(x) - \mathrm{Tr}((\omega_j - \beta)x)}. \end{aligned}$$

For fixed β and for $1 \leq j \leq p^n$, i.e for $\omega_j \in \mathbb{F}_{p^n}$, $(\omega_j - \beta)$ takes all values of $\mathbb{F}_{p^n}$. Then the cross-correlation obeys:

$$|C_{i,j}(\tau) + (\zeta_p)^{-f(0)}| = \begin{cases} 0, & (p^n - 1)(p^n - p^{n-s}) \quad \text{times} \\ p^{\frac{n+s}{2}}, & (p^n - 1)p^{n-s} \quad \text{times}. \end{cases} \tag{5.17}$$

Case 4: $\tau = 0,\ 1 \leq i, j \leq p^n$ and $i \neq j$, then the cross-correlation function:

$$\begin{aligned} C_{i,j}(\tau) &= \sum_{0 \leq t \leq p^n - 2} (\zeta_p)^{v_i(t) - v_j(t)} \\ &= \sum_{0 \leq t \leq p^n - 2} (\zeta_p)^{\mathrm{Tr}(\omega_i \alpha^t) + f(\alpha^t) - \mathrm{Tr}(\omega_j \alpha^t) - f(\alpha^t)} \\ &= \sum_{0 \leq t \leq p^n - 2} (\zeta_p)^{\mathrm{Tr}((\omega_i - \omega_j)\alpha^t)} \\ &= \sum_{x \in \mathbb{F}_{p^n}^*} (\zeta_p)^{\mathrm{Tr}(x)} = -1 + \sum_{x \in \mathbb{F}_{p^n}} (\zeta_p)^{\mathrm{Tr}(x)} = -1 \end{aligned}$$

where $(\omega_i - \omega_j)\alpha^t = x$. It means that $|C_{i,j}(\tau) + 1| = 0$ exactly $p^n(p^n - 1)$ times.

Case 5: The final case is $\tau \neq 0,\ 1 \leq \tau \leq p^n - 2,\ 1 \leq i, j \leq p^n$ then:

$$\begin{aligned} C_{i,j}(\tau) &= \sum_{0 \leq t \leq p^n - 2} (\zeta_p)^{v_i(t+\tau) - v_j(t)} \\ &= \sum_{0 \leq t \leq p^n - 2} (\zeta_p)^{\mathrm{Tr}(\omega_i \alpha^{t+\tau}) + f(\alpha^{t+\tau}) - \mathrm{Tr}(\omega_j \alpha^t) - f(\alpha^t)} \\ &= \sum_{0 \leq t \leq p^n - 2} (\zeta_p)^{f(\beta\alpha^t) - f(\alpha^t) - \mathrm{Tr}((\omega_j - \omega_i\beta)\alpha^t)} \\ &= -1 + \sum_{x \in \mathbb{F}_{p^n}} (\zeta_p)^{f(\beta x) - f(x) - \mathrm{Tr}((\omega_j - \omega_i \beta)x)} \end{aligned}$$

where $\alpha^\tau = \beta, \alpha^t = x$. Let β and ω_i be fixed elements of $\mathbb{F}_{p^n}$. For $1 \leq j \leq p^n$, $\omega_j \in \mathbb{F}_{p^n}$ and $(\omega_j - \omega_i\beta)$ takes all values of $\mathbb{F}_{p^n}$ exactly once.

Now the problem reduces to finding the Walsh distribution so we need to find plateaued degree of the function $f(\beta x) - f(x)$. Then we can compute the Walsh transform and this gives us the correlation distribution. We can then determine the number of occurrences by Parseval's identity. If $f(\beta x) - f(x)$ is k-plateaued N_k times for $0 \leq k \leq m$ where $N_0 + N_1 + ... + N_m = p^n - 2$, then for $0 \leq \tau \leq p^n - 2$ and $1 \leq i, j \leq p^n$ the cross-correlation obeys:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & p^n(\sum_{k=1}^m N_k(p^n - p^{n-k})) \quad \text{times} \\ p^{\frac{n}{2}}, & p^{2n}N_0 \quad \text{times} \\ p^{\frac{n+1}{2}}, & p^n p^{n-1} N_1 \quad \text{times} \\ ... & ... \\ p^{\frac{n+m}{2}}, & p^n p^{n-m} N_m \quad \text{times} \end{cases} \tag{5.18}$$

by Lemma 5.1.

Collecting all five cases together, for an arbitrary s-plateaued function $f(x)$ let N_k be the number of β in $\mathbb{F}_{p^n} - \{0, 1\}$ satisfying $f_\beta(x) = f(\beta x) - f(x)$ where $f_\beta(x)$ is k-plateaued depending on k. The correlation distribution of the sequence family $\mathcal{V}$ satisfies:

$$|C_{i,j}(\tau) + (\zeta_p)^l| = \begin{cases} 0, & (p^n - 1)[p^n(p^n - 2) + 2(p^n - p^{n-s})] \\ & +p^n(\sum_{k=1}^m N_k(p^n - p^{n-k})) \quad \text{times} \\ p^n, & p^n + 1 \quad \text{times} \\ p^{\frac{n+s}{2}}, & 2p^{n-s}(p^n - 1) \quad \text{times} \\ p^{\frac{n}{2}}, & p^{2n}N_0 \quad \text{times} \\ p^{\frac{n+1}{2}}, & p^n p^{n-1} N_1 \quad \text{times} \\ ... & ... \\ p^{\frac{n+m}{2}}, & p^n p^{n-m} N_m \quad \text{times} \end{cases} \tag{5.19}$$

where $l \in \{0, f(0), -f(0)\}$ as given in this proof. □

5.3 Correlation Values of Generalized Gold Sequences for Arbitrary p and n

In this section, we constructed our sequence family using the well known Gold function and computed the correlation distribution of this family, depending on the prime number p and positive integer n. Throughout our proof of the correlation distribution we take advantage of the theory of algebraic curves to show the functions $f(x)$ and $f(\beta x) - f(x)$ are plateaued functions. Then we give the correlation distribution using the proof of Theorem 5.8. Finally we support our proof with some computational results of the correlation distribution.

Definition 5.8. For arbitrary prime number p and arbitrary positive integer n the quadratic form corresponding to the Gold function $f(x)$ is defined as:

$$\begin{array}{rcl} f : \mathbb{F}_{p^n} & \rightarrow & \mathbb{F}_p \\ x & \rightarrow & \mathrm{Tr}_1^n(x^{1+p}). \end{array} \tag{5.20}$$

Using the Gold fuction $f(x)$, the sequence family

$$\mathcal{V} = \{v_i(t) : i = 0, 1, 2, ..., p^n\}$$

is defined by:

$$v_i(t) = \begin{cases} \mathrm{Tr}_1^n(\zeta_i \alpha^t) + f(\alpha^t), & 0 \leq i < p^n \\ \mathrm{Tr}_1^n(\alpha^t), & i = p^n \end{cases} \tag{5.21}$$

where ζ_i is an enumeration $\mathbb{F}_{p^n}$, α is a primitive element of $\mathbb{F}_{p^n}$ and $0 \leq t \leq p^n - 2$

Theorem 5.9. *The correlation distribution of the sequence family $\mathcal{V}$, constructed by using the Gold function with arbitrary prime number p and arbitrary positive integer n is given as follows:*

If $p = 2$ and n is odd, then:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & (p^n - 2) + p^n(p^n - 1) + (p^n - p^{n-1})[2(p^n - 1) \\ & +p^n(p^n - 2)] \quad \textit{times} \\ p^{\frac{n+1}{2}}, & p^{n-1}(2(p^n - 1) + p^n(p^n - 2)) \quad \textit{times} \\ p^n, & p^n + 1 \quad \textit{times}. \end{cases} \tag{5.22}$$

If $p = 2$, $n = 4k$, $A = (p^n - p^{\frac{n}{2}+1} - 8)/3$ and $B = (p^{n+1} + p^{\frac{n}{2}+1} - 4)/3$ then:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & (p^n - 2) + 3p^n(p^n - 1) \\ & +(p^n - p^{n-2})(2(p^n - 1) + Ap^n) \quad \textit{times} \\ p^{\frac{n}{2}}, & Bp^{2n} \quad \textit{times} \\ p^{\frac{n+2}{2}}, & p^{n-2}(2(p^n - 1) + Ap^n) \quad \textit{times} \\ p^n, & 3p^n + 1 \quad \textit{times}. \end{cases} \tag{5.23}$$

If $p = 2$, $n = 4k + 2$, $A = (p^n + p^{\frac{n}{2}+1} - 8)/3$ and $B = (p^{n+1} - p^{\frac{n}{2}+1} - 4)/3$ then:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & (p^n - 2) + 3p^n(p^n - 1) \\ & +(p^n - p^{n-2})(2(p^n - 1) + Ap^n) \text{ times} \\ p^{\frac{n}{2}}, & Bp^{2n} \quad \text{times} \\ p^{\frac{n+2}{2}}, & p^{n-2}(2(p^n - 1) + Ap^n) \quad \text{times} \\ p^n, & 3p^n + 1 \quad \text{times}. \end{cases} \tag{5.24}$$

If p is odd and n is odd, then:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & (p^n - 2) + 2p^n(p^n - 1) \quad \text{times} \\ p^{\frac{n}{2}}, & 2p^n(p^n - 1) + p^{2n}(p^n - 3) \quad \text{times} \\ p^n, & 2p^n + 1 \quad \text{times}. \end{cases} \tag{5.25}$$

If p is odd and $n = 4k$, let $A = (p^n - p^{\frac{n}{2}+2} + p^{\frac{n}{2}+1} + 1)/(p + 1)$, then:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & (p^n - 2) + (p + 1)p^n(p^n - 1) \\ & +(p^n - p^{n-2})(2(p^n - 1) + (A - 3)p^n) \text{ times} \\ p^{\frac{n}{2}}, & p^{2n}(p^n - p - A + 1) \quad \text{times} \\ p^{\frac{n+2}{2}}, & p^{n-2}(2(p^n - 1) + (A - 3)p^n) \quad \text{times} \\ p^n, & (p + 1)p^n + 1 \quad \text{times}. \end{cases} \tag{5.26}$$

If p is odd and $n = 4k + 2 > 2$, let N be found computationally as given in the proof, then:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & (p^n - 2) + (p + 1)p^n(p^n - 1) + Np^n(p^n - p^{n-2}) \text{ times} \\ p^{\frac{n}{2}}, & 2p^n(p^n - 1) + p^{2n}(p^n - p - N - 2) \quad \text{times} \\ p^{\frac{n+2}{2}}, & Np^n p^{n-2} \quad \text{times} \\ p^n, & (p + 1)p^n + 1 \quad \text{times}. \end{cases} \tag{5.27}$$

Finally, if p is odd and $n = 2$, then:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & (p^2 - 2) + (p + 1)p^2(p^2 - 1) \quad \text{times} \\ p, & 2p^2(p^2 - 1) + p^4(p^2 - p - 2) \quad \text{times} \\ p^2, & (p + 1)p^2 + 1 \quad \text{times}. \end{cases} \tag{5.28}$$

Proof. To compute the correlation distribution of the sequence family constructed by using the Gold function we need to find the plateaued degree of $f(x)$ and $f(\beta x) - f(x)$ for all $\beta \in \mathbb{F}_{p^n} - \{0, 1\}$ in cases 3 and 5. For the other cases, the correlation distribution is independent of the function used to generate the sequence family, and depends on standard linear trace sums, as in the proof of Theorem 5.9.

Correlation Case 3: To find the plateaued degree of $f(x)$, we need to find the rank of the function. The symplectic form of the function is:

$$B(x, y) = \mathrm{Tr}(xy^p + x^p y) = 0 \iff y(x^p + x^{p^{-1}}) = 0, \forall y \in \mathbb{F}_{p^n}.$$

So the radical equals:

$$\begin{aligned}\mathcal{W} &= \{x \in \mathbb{F}_{p^n} : B(x,y) = 0,\ \forall y \in \mathbb{F}_{p^n}\} \\ &= \{x \in \mathbb{F}_{p^n} : \mathrm{Tr}(y(x^p + x^{p^{-1}})) = 0,\ \forall y \in \mathbb{F}_{p^n}\} \\ &= \{x \in \mathbb{F}_{p^n} : x^{p^2} + x = 0\} \\ &= \{x \in \mathbb{F}_{p^n} : x^{p^2-1} = -1\}\end{aligned} \tag{5.29}$$

For an odd prime number p and an even integer n, when $n = 4k$, the radical:

$$\mathcal{W} = \{x \in \mathbb{F}_{p^n} : x^{p^2} + x = 0\} \tag{5.30}$$

and $x^{p^2} + x$ splits in $\mathbb{F}_{p^n}$, thus $\dim(\mathcal{W}) = 2$ and $f(x)$ is 2-plateaued.

Note that $x^{p^2} + x$ splits in $\mathbb{F}_{p^4}$. For an odd prime number p and an even integer n, when $n = 4k + 2$, $\mathbb{F}_{p^4} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^2}$. Moreover for $x \in \mathbb{F}_{p^2}$, $x^{p^2} = x$ hence the radical:

$$\mathcal{W} = \mathbb{F}_{p^2} \cap (\text{solutions of } (x^{p^2} + x)) = \{0\}. \tag{5.31}$$

Thus $f(x)$ is 0-plateaued.

Similarly when p and n are both odd integers, $\mathbb{F}_{p^4} \cap \mathbb{F}_{p^n} = \mathbb{F}_p$ and for $x \in \mathbb{F}_p$, $x^{p^2} = x$ hence the radical:

$$\mathcal{W} = \mathbb{F}_p \cap (\text{solutions of } (x^{p^2} + x)) = \{0\}. \tag{5.32}$$

Thus $f(x)$ is 0-plateaued.

Using the same method, for the even prime number $p = 2$, $x^{p^2} + x$ splits in $\mathbb{F}_{p^2}$. When $p = 2$ and n is an even integer, $\mathbb{F}_{p^2} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^2}$ and as $x^{p^2} = x = -x$ the radical:

$$\mathcal{W} = \mathbb{F}_{p^2}. \tag{5.33}$$

Thus $f(x)$ is 2-plateaued.

And finally for $p = 2$ and an odd integer n, $\mathbb{F}_{p^2} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^2}$ hence similarly the radical:

$$\mathcal{W} = \mathbb{F}_p. \tag{5.34}$$

Thus $f(x)$ is 1-plateaued.

Corollary 5.10. *Correlation distributions of Case 3 depending on p and n are given as follows: For $p = 2$ and n odd:*

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & 2(p^n - 1)(p^n - p^{n-1}) \ \textit{times} \\ p^{\frac{n+1}{2}}, & 2(p^n - 1)p^{n-1} \ \textit{times.} \end{cases} \tag{5.35}$$

For $p = 2$ and n even:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & 2(p^n - 1)(p^n - p^{n-2}) \ \textit{times} \\ p^{\frac{n+2}{2}}, & 2(p^n - 1)p^{n-2} \ \textit{times.} \end{cases} \tag{5.36}$$

For p odd and n odd:

$$|C_{i,j}(\tau)+1| = \begin{cases} p^{\frac{n}{2}}, & 2p^n(p^n-1) \quad \textit{times.} \end{cases} \tag{5.37}$$

For p odd and $n = 4k$:

$$|C_{i,j}(\tau)+1| = \begin{cases} 0, & 2(p^n-1)(p^n-p^{n-2}) \quad \textit{times} \\ p^{\frac{n+2}{2}}, & 2(p^n-1)p^{n-2} \quad \textit{times.} \end{cases} \tag{5.38}$$

For p odd and $n = 4k+2$:

$$|C_{i,j}(\tau)+1| = \begin{cases} p^{\frac{n}{2}}, & 2p^n(p^n-1) \quad \textit{times.} \end{cases} \tag{5.39}$$

Correlation Case 5: For $\beta \in \mathbb{F}_{p^n} - \{0,1\}$,

$$g_\beta(x) = f(\beta x) - f(x) = \mathrm{Tr}((\beta^{1+p}-1)x^{1+p}). \tag{5.40}$$

Then the symplectic form of the quadratic form is:

$$B_\beta(x,y) = \mathrm{Tr}((\beta^{1+p}-1)xy^p + (\beta^{1+p}-1)x^p y). \tag{5.41}$$

The kernel:

$$\mathcal{W} = \{y \in \mathbb{F}_{p^n} : (\beta^{1+p}-1)y^p + (\beta^{1+p}-1)^{p^{-1}} y^{p^{-1}} = 0\}, \tag{5.42}$$

which means that we need to find the number of the solutions of the equation:

$$(\beta^{1+p}-1)^p y^{p^2} + (\beta^{1+p}-1)y = 0. \tag{5.43}$$

Let $(\beta^{1+p}-1) = \gamma$, then the equation is given by:

$$\gamma^p y^{p^2} + \gamma y = 0. \tag{5.44}$$

For $\gamma \neq 0$, the equation can be written as:

$$\gamma^{p-1} y^{p^2} + y = 0. \tag{5.45}$$

When p is odd $\gamma^{p-1} y^{p^2-1} = -1 = w^{\frac{p^n-1}{2}}$ and when p is even $\gamma^{p-1} y^{p^2-1} = -1 = w^{p^n-1}$.

Now the question is to find the β values when the equation

$$\gamma = \beta^{1+p} - 1 \tag{5.46}$$

equals to 0. $\gamma = 0$ if and only if $\beta^{1+p} = 1$, where $\beta = w^i$ for a primitive element w of $\mathbb{F}_{p^n}$. In other words, $\gamma = 0$ if and only if $w^{i(1+p)} = 1$ if and only if $p^n - 1 \mid i(p+1)$. To find the solutions of the equation 5.46, we will need to use the following information:

When p is even:

$$\gcd(p^n-1, p+1) = \gcd(2^n-1, 3) = \begin{cases} 1, & \text{if } n \text{ is odd,} \\ 3, & \text{if } n \text{ is even.} \end{cases} \tag{5.47}$$

When p is odd:

$$\gcd(p^n-1, p+1) = \begin{cases} 2, & \text{if } n \text{ is odd,} \\ p+1, & \text{if } n \text{ is even.} \end{cases} \tag{5.48}$$

To simpilfy the notation, let $A = (\omega_j - \omega_i\beta)$ and $\gamma = \beta^{1+p} - 1$ where

$$g_\beta(x) = f(\beta x) - f(x) = \mathrm{Tr}((\beta^{1+p}-1)x^{1+p}). \tag{5.49}$$

Then

$$\begin{array}{rcl} |C_{i,j}(\tau)+1| & = & |\sum_{x\in\mathbb{F}_{p^n}} (\zeta_p)^{g_\beta(x)-\mathrm{Tr}(Ax)}| \\ & = & |W_{g_\beta}(A)|. \end{array} \tag{5.50}$$

$\mathbf{p = 2}$ and $\mathbf{n}$ is odd: The solution of the equation 5.46:

$$\gamma = \beta^{p+1} - 1 = 0 \iff i = p^n - 1 \iff \beta = 1,$$

which is impossible. Then for $\gamma \neq 0$ let

$$\begin{array}{rcl} \Psi : \mathbb{F}_{2^n} - \{0,1\} & \to & \mathbb{F}_{2^n} - \{0,-1\} \\ \beta & \to & \gamma = \beta^{p+1} - 1. \end{array} \tag{5.51}$$

Note that Ψ is a one-to-one map. For $y \neq 0$,

$$\gamma^{p-1} y^{p^2-1} = 1 \iff y^3 = \frac{1}{\gamma}. \tag{5.52}$$

As $\gcd(3, 2^n-1) = 1$, choose $a, b \in \mathbb{Z}$ satisfying $1 = 3a + (2^n-1)b$. By multiplying the equations $(y^3)^a = (\frac{1}{\gamma})^a$ and $(y^{2^n-1})^b = 1$ we get

$$y^{3a+(2^n-1)b} = (\frac{1}{\gamma})^a, \tag{5.53}$$

that is $y = (\frac{1}{\gamma})^a$ is the exact solution for all $\beta \in \mathbb{F}_{2^n} - \{0,1\}$.

Corollary 5.11. *When p is even and n is odd $g_\beta(x)$ is 1-plateaued for all β and the correlation distribution for Case 5 is:*

$$|C_{i,j}(\tau)+1| = \begin{cases} 0, & p^n(p^n-2)(p^n-p^{n-1}) \ \textit{times} \\ p^{\frac{n+1}{2}}, & p^n p^{n-1}(p^n-2) \ \textit{times.} \end{cases} \tag{5.54}$$

$\mathbf{p = 2}$ and $\mathbf{n}$ is even: Let $\beta = \alpha^i$. Then the solutions of the equation 5.46 can be found by:

$$\gamma = \beta^{p+1} - 1 = 0 \iff i \in S = \{\frac{p^n-1}{3}, 2\frac{p^n-1}{3}, p^n-1\} \iff \beta \in \mathbb{F}_4^*$$

So for these $\beta \in \mathbb{F}_4 - \mathbb{F}_2$, $\gamma = 0$. When $A = 0$ and $\gamma = 0$ the correlation takes the value $-1 + p^n$, 2 times and similarly when $A \neq 0$ and $\gamma = 0$, the correlation takes the

value -1 exactly 2 times. This means that the function is n-plateaued two times when $\beta \in \mathbb{F}_4 - \mathbb{F}_2$.

For $\gamma \neq 0$ we define a $3-$to-1 map

$$\Psi : \mathbb{F}_{2^n} - \{0, 1\} \to S = \{\gamma : \gamma = \beta^{p+1} - 1\}$$

such that $\Psi^{-1}(0)$ has two values and $\Psi^{-1}(s)$ has three values for each $s \in S^*$ where $S^* = S - \{0\}$. $|S| = \frac{2^n-1}{3}$ and $0 \in S$. As $\gamma \neq 0$, $y^3 = \frac{1}{\gamma}$, that is $y^3 = \frac{1}{\beta^3+1}$.

Number of β is the number of the solutions on the curve $y^3 = x^3 + 1$.

1. Let N_0 be the number of β such that $y^3 = x^3 + 1$ has no solutions, in that case, β will give us a 0-plateaued function.

2. Let N_1 be the number of β such that $y^3 = x^3 + 1$ has 2^n solutions together with $y = 0$; in that case, β will give us an n-plateaued function which is the same as the $\gamma = 0$ case.

3. Let N_3 be the number of β such that $y^3 = x^3 + 1$ has exactly three distinct solutions and such β will give us a 2-plateaued function after adding the trivial solution $y = 0$.

From the theory of algebraic curves in [30], when $n = 2m$ and N_n denotes the number of rational points of the curve over $\mathbb{F}_2^m$ including the point at infinity, we have:

$$N_n = \begin{cases} (2^m + 1)^2, & \text{if m is odd } (n \equiv 2 \mod 4) \\ (2^m - 1)^2, & \text{if m is even } (n \equiv 0 \mod 4). \end{cases} \tag{5.55}$$

When m is odd, that is $n \equiv 2 \mod 4$:

$$N_3 = \frac{(2^m + 4)(2^m - 2)}{3} = \frac{(2^n + 2^{\frac{n}{2}+1} - 8)}{3}, \quad N_0 = 2^n - N_3 - 4 \quad \text{and} \quad N_1^0 = 2.$$

Note that there is exactly 3 points over infinity, three points for $\beta = 0$ and exactly 1 point for $\beta \in \mathbb{F}_4 - \{0\}$ which gives the solution $y = 0$. For cube root $1/\gamma$, the polynomial $g_\beta(x)$ is 2-plateaued $A_1 = (2^n + 2^{\frac{n}{2}+1} - 8)/3$ times and n-plateaued 2 times (for $\beta \in \mathbb{F}_4 - \{0, 1\}$). Otherwise $g_\beta(x)$ is 0-plateaued, $B_1 = (2^{n+1} - 2^{\frac{n}{2}+1} - 4)/3$ times.

Similarly when m is even that is $n \equiv 0 \mod 4$, then

$$N_3 = \frac{(2^m - 4)(2^m + 2)}{3} = \frac{2^n - 2^{\frac{n}{2}+1} - 8}{3}, \quad N_0 = 2^n - N_3 - 4 \quad \text{and} \quad N_1^0 = 2.$$

By the same method the polynomial $g_\beta(x)$ is 2-plateaued $A_2 = (2^n - 2^{\frac{n}{2}+1} - 8)/3$ times and n-plateaued 2 times (for $\beta \in \mathbb{F}_4 - \{0, 1\}$). Otherwise, $g_\beta(x)$ is 0-plateaued $B_2 = (2^{n+1} + 2^{\frac{n}{2}+1} - 4)/3$ times.

Corollary 5.12. *For $p = 2$ and $n = 4k + 2$, the polynomial $g_\beta(x)$ is n-plateaued 2 times, 2-plateaued $A_1 = (2^n + 2^{\frac{n}{2}+1} - 8)/3$ times and 0-plateaued $B_1 = (2^{n+1} - 2^{\frac{n}{2}+1} - 4)/3$ times. Similarly, for $p = 2$ and $n = 4k$, the polynomial $g_\beta(x)$ is n-plateaued 2 times, 2-plateaued $A_2 = (2^n - 2^{\frac{n}{2}+1} - 8)/3$ times and 0-plateaued $B_2 = (2^{n+1} + 2^{\frac{n}{2}+1} - 4)/3$ times. For $i = \{1, 2\}$ depending on $n = 4k + 2$ or $n = 4k$, we can formulize the correlation distribution for Case 5 as:*

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & p^n(A_i(p^n - p^{n-2}) + 2(p^n - 1)) \text{ times} \\ p^{\frac{n}{2}}, & B_i p^{2n} \quad \text{times} \\ p^{\frac{n+2}{2}}, & A_i p^n p^{n-2} \quad \text{times} \\ p^n, & 2p^n \quad \text{times}. \end{cases} \tag{5.56}$$

p is odd and n is odd: Let $\beta = \alpha^i$. We know that

$$\gcd(p^n - 1, p + 1) = 2$$

and $\beta = 1$ is impossible then the solution of the equation 5.46 is $\beta = -1$. For $\beta = -1$ it is seen that $\gamma = 0$. Then when $A = 0$, the cross-correlation $|C_{i,j}(\tau) + 1| = p^n$ and when $A \neq 0$, the cross-correlation $|C_{i,j}(\tau) + 1| = 0$.

When $\gamma \neq 0$,

$$\#\{\beta \in \mathbb{F}_{p^n} - \{0, 1\} : \gamma \neq 0\} = \#\{\beta \in \mathbb{F}_{p^n} - \{0, 1, -1\}\} = p^n - 3.$$

Then we need to check whether the equation $y^{p^2-1} = \frac{-1}{\gamma^{p-1}}$ is solvable or not. To continue our proof, we need the following fact.

Fact: $x^a = b$ is solvable if and only if $x^{\gcd(p^n-1,a)} = b$ is solvable.

As $\gcd(p^n - 1, p^2 - 1) = p - 1$ when n is odd, using this fact we need to find the solutions of the equation

$$y^{p-1} = \frac{-1}{\gamma^{p-1}}. \tag{5.57}$$

It is easily seen that if -1 is $(p - 1)$-th power, then $g_\beta(x)$ is 1-plateaued, otherwise $g_\beta(x)$ is 0-plateaued. As

$$\frac{(p-1)(1 + p + ... + p^{n-1})}{2} = \frac{p^n - 1}{2},$$

we need to check whether $p-1$ divides $(1 + p + ... + p^{n-1})/2$ or not. Note that p and n are odd, so $(1+p+...+p^{n-1})$ is odd. Then, $p-1$ does not divide $(1 + p + ... + p^{n-1})/2$ which means that -1 is not a $(p - 1)$-th power, and so, the polynomial $g_\beta(x)$ is 0-plateaued $p^n - 3$ times.

Corollary 5.13. *For an odd prime number p and odd integer n, $g_\beta(x)$ is n-plateaued when $\beta = \alpha^{\frac{p^n-1}{2}} = -1$, and 0-plateaued $p^n - 3$ times. The correlation distribution for Case 5 is given by:*

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & p^n(p^n - 1) \quad \text{times} \\ p^{\frac{n}{2}}, & p^{2n}(p^n - 3) \quad \text{times} \\ p^n, & p^n \quad \text{times}. \end{cases} \tag{5.58}$$

Moreover, as a further information, when p and n are odd and $\gamma = \beta^{p+1} - 1 \neq 0$, the left hand side of the equation

$$\gamma^p x^{p^2} + \gamma x = 0$$

is a permutation and

$$\gamma^p x^{p^2} + \gamma x = -A$$

has a unique solution. This solution can be found using the method given in [8].

Example 5.1. For $n = 3$ the unique solution $x_0 = a_2 x^{p^2} + a_1 x^p + a_0 x$ of the equation $\gamma^p x^{p^2} + \gamma x = -A$ can be found by:

$$(a_2 x^{p^2} + a_1 x^p + a_0 x) \circ (\gamma^p x^{p^2} + \gamma x) = x \mod x^{p^3} - x.$$

Then,

$$x = (a_2 \gamma^{p^2} + a_0 \gamma^p) x^{p^2} + (a_2 \gamma + a_1 \gamma^p) x^p + (a_1 \gamma^{p^2} + a_0 \gamma) x$$

where $a_0 = \frac{1}{2\gamma}$, $a_1 = \frac{1}{2\gamma^{p^2}}$ and $a_2 = \frac{-\gamma^p}{2\gamma^{p^2+1}}$. Thus the solution of the given equation is found as:

$$x_0 = \frac{-\gamma^p}{2\gamma^{p^2+1}} x^{p^2} + \frac{1}{2\gamma^{p^2}} x^p + \frac{1}{2\gamma} x$$

where $\gamma = \beta^{p+1} - 1$.

p is odd and n is even: Let $< \alpha >= \mathbb{F}_{p^n}^*$ and $< \theta >= \mathbb{F}_{p^2}^*$. Then as $\theta^{p^2-1} = 1$,

$$\gamma = \beta^{p+1} - 1 = 0 \iff \beta \in S = \{\beta_1 = \theta^{p-1}, \beta_2 = c_1 \theta^{p-1}, ..., \beta_p = c_{p-1} \theta^{p-1}\}.$$

The number of the elements of set S is p. As $\theta = \alpha^{1+p^2+...+p^{n-2}}$, then the set of β values are found as:

$$\begin{array}{lcl} \beta_1 & = & \alpha^{(p-1)(1+p^2+...+p^{n-2})} \\ \beta_2 & = & \alpha^{(p-1)(1+p^2+...+p^{n-2})+(1+p+...+p^{n-1})} \\ \dots & & \dots \\ \beta_p & = & \alpha^{(p-1)(1+p^2+...+p^{n-2})+(p-1)(1+p+...+p^{n-1})}. \end{array} \tag{5.59}$$

For these $\beta \in \mathbb{F}_{p^2}^*$, $\gamma = 0$ thus $g_\beta(x)$ is n-plateaued p times. Moreover, for $\beta \notin S$ we want to find the number of the solutions of the polynomial:

$$y^{p^2-1} = \frac{-1}{(\beta^{p+1} - 1)^{p-1}} = \frac{-1}{\gamma^{p-1}}.$$

For $w \in \mathbb{F}_{p^n}^*$, as p is an odd prime number and n is even, $w^{\frac{p^n-1}{2}} = -1$. Then the generator θ of $\mathbb{F}_{p^2}^*$ can be written in terms of w as

$$\theta = w^{\frac{1+p+...+p^{n-1}}{2}}$$

which means that $\theta^{p-1} = -1$. Additionally when $n = 4k$ we know that $\theta^{p^2-1} = -1$. According to the information above, we will give the proof of this case in two subcases depending on n.

$\mathbf{n \equiv 0 \mod 4}$: Note that

$$y^{p^2-1} = \frac{-1}{\gamma^{p-1}} \text{ is solvable in } \mathbb{F}_{p^{4k}} \iff \gamma^{(p-1)(\frac{p^n-1}{p^2-1})} = 1.$$

Since -1 is a (p^2-1)-th power, the equation can be written as

$$y^{p^2-1} = \frac{\theta^{p^2-1}}{\gamma^{p-1}} \tag{5.60}$$

for some $\theta \in \mathbb{F}_{p^n}$. Equation 5.60 is solvable if and only if $y^{p^2-1} = \gamma^{p-1}$ is solvable. In other words, Equation 5.60 is solvable if and only if

$$y^{p+1} = \gamma = \beta^{p+1} - 1$$

is solvable. Thus we need to find the number of the solutions of

$$x^{p+1} = y^{p+1} + 1. \tag{5.61}$$

As a result, as $\gcd(p^n - 1, p^2 - 1) = 1$, when $\beta \in \mathbb{F}_{p^2}$ and $\beta^{p+1} - 1 \neq 0$, $g_\beta(x)$ is 2-plateaued; when $\beta \in \mathbb{F}_{p^n} - \mathbb{F}_{p^2}$, $g_\beta(x)$ is 0-plateaued.

$\mathbf{n \equiv 2 \mod 4}$:

$$y^{p^2-1} = \frac{-1}{\gamma^{p-1}} \text{ is solvable in } \mathbb{F}_{p^{4k+2}} \iff -\gamma^{p-1} = \frac{1}{y^{p^2-1}}.$$

In other words, the equation is solvable if and only if

$$y^{p^2-1} = -(x^{p+1} - 1)^{p-1}.$$

Since -1 is a $(p-1)$-th power, the equation can be written as

$$y^{p^2-1} = \theta^{p-1}(x^{p+1} - 1)^{p-1} \tag{5.62}$$

for some $\theta \in \mathbb{F}_{p^n}$. Thus we need to find the number of solutions of

$$x^{p+1} = \theta y^{p+1} - \theta \tag{5.63}$$

where $\theta^p + \theta = 0,\ \theta \in \mathbb{F}_{p^2}$. As a result, as $\gcd(p^n - 1, p^2 - 1) = 1$, when $\beta \in \mathbb{F}_{p^2}$ and $\beta^{p+1} - 1 \neq 0$, $g_\beta(x)$ is 2-plateaued, and when $\beta \in \mathbb{F}_{p^n} - \mathbb{F}_{p^2}$, $g_\beta(x)$ is 0-plateaued.

To complete the proof, we need to find the number of solutions of the curves $x^{p+1} = y^{p+1} + 1$ and $x^{p+1} = \theta y^{p+1} - \theta$. Before we continue with the proof of the theorem we give some lemmas that will help us in the next steps.

Lemma 5.14. *The number of points N of the set S where*

$$S = \{y \in \mathbb{F}_{p^n} : \exists x \in \mathbb{F}_{p^n} \textit{ with } x^{p+1} = y^{p+1} + 1, y^{p+1} \neq -1 \textit{ and } y^{p+1} \neq 0\}$$

is $N = \frac{p^n - p^{\frac{n}{2}+2} + p^{\frac{n}{2}+1} + 1}{p+1} - 2$ for $n = 4k$.

Proof. We take advantage of some known facts given in the definitions and [30] during this proof.

Claim 1. $x^{p+1} = y^{p+1} + 1$ is a maximal curve over $\mathbb{F}_{p^2}$ with genus $g = \frac{p(p-1)}{2}$ and the number of rational points $N = p^3 + 1$.

Fact 1. In [30], the $L-$polynomial of the curve is given by:

$$L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t) \tag{5.64}$$

where $\alpha_i \in \mathbb{C}$ with $|\alpha_i| = \sqrt{p^2} = p$ and

$$N_1(x) = p^2 + 1 - (\alpha_1 + \alpha_2 + ... + \alpha_{2g}) \tag{5.65}$$

Here N_i denotes the number of places of degree 1 over the finite field $\mathbb{F}_{p^i}$. Then, for $n = 2$,

$$p^3+1 = p^2+1-(\alpha_1+\alpha_2+...+\alpha_{p(p-1)}) \iff p^2(p-1) = \alpha_1 = \alpha_2 = ... = \alpha_{p(p-1)} = -p.$$

Thus

$$L(t) = (1 - pt)^{2g}$$

and

$$N_1(x) = p^2 + 1 + p^2(p - 1).$$

In general for $n = 4k + 2$, the $L-$polynomial of the curve over $\mathbb{F}_{p^n}$ is

$$L(t) = \prod_{i=1}^{2g}(1 - \alpha_i^{\frac{n}{2}} t). \tag{5.66}$$

Thus using the formula, the number of rational points is

$$N_{\frac{n}{2}}(x) = p^n + 1 - (\alpha_1^{\frac{n}{2}} + \alpha_2^{\frac{n}{2}} + ... + \alpha_{2g}^{\frac{n}{2}}). \tag{5.67}$$

Using the same method we get the curve maximal because of

$$N_{\frac{n}{2}}(x) = p^n + 1 - p(p - 1)(-p)^{\frac{n}{2}} = p^n + 1 + p^{\frac{n}{2}+1}(p - 1).$$

Claim 2. $x^{p+1} = y^{p+1} + 1$ is a minimal curve over $\mathbb{F}_{p^4}$ with genus $g = \frac{p(p-1)}{2}$.

Fact 2. The $L-$polynomial of the curve is defined by:

$$L(t) = \prod_{i=1}^{2g}(1 - \alpha_i^2 t) \tag{5.68}$$

where $\alpha_i \in \mathbb{C}$ with $|\alpha_i| = \sqrt{p^2} = p$ and

$$N_2(x) = p^4 + 1 - (\alpha_1^2 + \alpha_2^2 + ... + \alpha_{2g}^2). \tag{5.69}$$

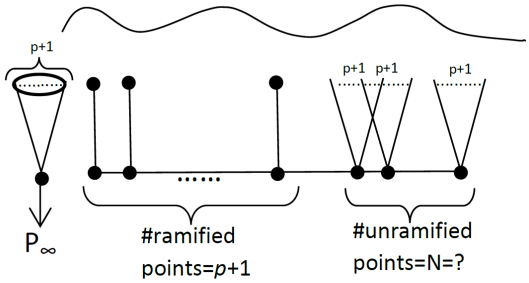

Figure 5.1: Unramified points of the curve $x^{p+1} = y^{p+1} + 1$ over $\mathbb{F}_{p^{4k}}$

Here N_i denotes the number of places of degree one over the finite field $\mathbb{F}_{p^i}$, [30]. For $n = 4$,

$$N_2(x) = p^4 + 1 - p(p-1)p^2 = p^3 + 1$$

and using 5.1, the number of unramified affine points on the curve including $y = 0$ over $\mathbb{F}_{p^4}$ is found as

$$N = \frac{p^4 + 1 - p^3(p-1) - 2(p+1)}{p+1} = p^2 - p - 1.$$

Thus, when $n = 4$, $g_\beta(x)$ is 2-plateaued $p^2 - p - 2$ times.

In general for $n = 4k$, the $L-$polynomial of the curve over $\mathbb{F}_{p^n}$ is given by

$$L(t) = \prod_{i=1}^{2g} (1 - \alpha_i^{\frac{n}{2}} t). \tag{5.70}$$

Thus using the formula, the number of rational points is

$$N_{\frac{n}{2}}(x) = p^n + 1 - (\alpha_1^{\frac{n}{2}} + \alpha_2^{\frac{n}{2}} + ... + \alpha_{2g}^{\frac{n}{2}}).$$

Using the same method we get the curve minimal because the number of the places of degree one is:

$$N_{\frac{n}{2}}(x) = p^n + 1 - p(p-1)(p)^{\frac{n}{2}} = p^n + 1 - p^{\frac{n}{2}+1}(p-1). \tag{5.71}$$

Using Figure 5.1, the number of unramified affine points of the curve including $y = 0$ over $\mathbb{F}_{p^n}$ is found as:

$$\begin{aligned} N &= \frac{p^n - p^{\frac{n}{2}+2} + p^{\frac{n}{2}+1} + 1}{p+1} - 2 \\ &= -2 + (1 - p + p^2 - ... + p^{\frac{n}{2}}) + p^{\frac{n}{2}+2}(p-1)(1 + p^2 + ... + p^{\frac{n}{2}-4}). \end{aligned}$$

When we exclude the point $y = 0$, as it splits, the polynomial $g_\beta(x)$ is 2-plateaued $N - 1$ times. □

Corollary 5.15. *For p odd and $n = 4k$, let*

$$A = \frac{p^n - p^{\frac{n}{2}+2} + p^{\frac{n}{2}+1} + 1}{p+1}.$$

Then $g_\beta(x)$ is n-plateaued for $\beta \in S$ exactly p times, 2-plateaued $A-3$ times and 0-plateaued $p^n - p - A + 1$ times. The correlation distribution for Case 5 is formulated as:

$$|C_{i,j}(\tau)+1| = \begin{cases} 0, & p^n((p^n - p^{n-2})(A-3) + p(p^n-1)) \text{ times} \\ p^{\frac{n}{2}}, & p^{2n}(p^n - p - A + 1) \quad \text{times} \\ p^{\frac{n+2}{2}}, & p^n p^{n-2}(A-3) \quad \text{times} \\ p^n, & pp^n \quad \text{times}. \end{cases} \tag{5.72}$$

For $n = 2$, we will find the number of the set S where

$$S = \{y \in \mathbb{F}_{p^2} : \exists x \in \mathbb{F}_{p^2} \text{ with } x^{p+1} = \theta y^{p+1} - \theta,\ \theta^{p-1} = -1,\ y^{p+1} \neq -1 \text{ and } y^{p+1} \neq 0\}$$

The curve splits in $\mathbb{F}_{p^2}$ if and only if θ is a $(p+1)$-th power for some $u \in \mathbb{F}_{p^2}$. Let $\theta = u^{p+1}$ then

$$\theta^{p-1} = u^{p^2-1} = 1.$$

This is a contradiction with $\theta^{p-1} = -1$. Thus $N = \frac{p+1}{p+1} = 1$ over $\mathbb{F}_{p^2}$ is not minimal so if we exclude the point $y = 0$ then $g_\beta(x)$ is 2-plateaued 0 times.

Corollary 5.16. *For p odd and $n = 2$, $g_\beta(x)$ is n-plateaued p times when $\beta \in S$ and 0-plateaued $p^n - p - 2$ times. The correlation distribution for Case 5 is:*

$$|C_{i,j}(\tau)+1| = \begin{cases} 0, & pp^n(p^n-1) \quad \text{times} \\ p^{\frac{n}{2}}, & p^{2n}(p^n - p - 2) \quad \text{times} \\ p^n, & pp^n \quad \text{times}. \end{cases} \tag{5.73}$$

Note that for $n = 4k+2$ the curves $x^{p+1} = y^{p+1} + 1$ and $x^{p+1} = \theta y^{p+1} - \theta$ where $\theta^p + \theta = 0$ are isomorphic to each other if $\theta = u^{p+1}$ for some $u \in \mathbb{F}_{p^n}$. Because in this case if we let $\theta = u^{p+1},\ x = ux_1,\ y = y_1$ and apply change of variables to the curve

$$x^{p+1} = \theta y^{p+1} - \theta, \tag{5.74}$$

then we would have

$$x^{p+1} = y^{p+1} + 1. \tag{5.75}$$

But as $\theta^{p-1} = u^{p^2-1} = -1 = w^{\frac{p^n-1}{2}}$ and

$$p^2 - 1 \nmid (p^n - 1)/2 = [(p-1)(p+1)(1 + p^2 + ... + p^{n-2})]/2$$

then such $u \in \mathbb{F}_{p^n}$ does not exist for $n = 4k+2$. As a result, these curves are not isomorphic to each other for $n = 4k+2$. Moreover the curve $x^{p+1} = \theta y^{p+1} - \theta$ is not maximal or minimal so we can not determine the number of the degree one places when $n = 4k+2$ using this method. One can only find the number of degree one places $N(x)$ of the curve computationally. If one get $N(x)$, then the correlation distribution of this case is given in the corollary below.

Corollary 5.17. *For p odd and $n = 4k + 2$, let $N(x)$ be found computationaly. Then $g_\beta(x)$ is n-plateaued for $\beta \in S$ exactly p times, 2-plateaued $N = \frac{N(x)}{p+1} - 1$ times and 0-plateaued $p^n - p - N - 2$ times. The correlation distribution for Case 5 is formulated as:*

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & p^n(N(p^n - p^{n-2}) + p(p^n - 1)) \textit{ times} \\ p^{\frac{n}{2}}, & p^{2n}(p^n - p - N - 2) \quad \textit{times} \\ p^{\frac{n+2}{2}}, & p^n p^{n-2}(N) \qquad \textit{times} \\ p^n, & pp^n \qquad\qquad\qquad \textit{times}. \end{cases} \tag{5.76}$$

Collecting all five cases together one can obtain the total correlation distribution of the sequence family depending on p and n as:

If $p = 2$ and n is odd, then:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & (p^n - 2) + p^n(p^n - 1) + (p^n - p^{n-1})[2(p^n - 1) \\ & +p^n(p^n - 2)] \qquad \text{times} \\ p^{\frac{n+1}{2}}, & p^{n-1}(2(p^n - 1) + p^n(p^n - 2)) \qquad \text{times} \\ p^n, & p^n + 1 \qquad \text{times}. \end{cases} \tag{5.77}$$

If $p = 2$, $n = 4k$, $A = (p^n - p^{\frac{n}{2}+1} - 8)/3$ and $B = (p^{n+1} + p^{\frac{n}{2}+1} - 4)/3$. Similarly If $p = 2$, $n = 4k + 2$, $A = (p^n + p^{\frac{n}{2}+1} - 8)/3$ and $B = (p^{n+1} - p^{\frac{n}{2}+1} - 4)/3$ then:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & (p^n - 2) + 3p^n(p^n - 1) \\ & +(p^n - p^{n-2})(2(p^n - 1) + Ap^n) \text{ times} \\ p^{\frac{n}{2}}, & Bp^{2n} \qquad \text{times} \\ p^{\frac{n+2}{2}}, & p^{n-2}(2(p^n - 1) + Ap^n) \qquad \text{times} \\ p^n, & 3p^n + 1 \qquad \text{times}. \end{cases} \tag{5.78}$$

If p is odd and n is odd, then:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & (p^n - 2) + 2p^n(p^n - 1) \qquad \text{times} \\ p^{\frac{n}{2}}, & 2p^n(p^n - 1) + p^{2n}(p^n - 3) \qquad \text{times} \\ p^n, & 2p^n + 1 \qquad \text{times}. \end{cases} \tag{5.79}$$

If p is odd and $n = 4k$, let $A = (p^n - p^{\frac{n}{2}+2} + p^{\frac{n}{2}+1} + 1)/(p + 1)$, then:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & (p^n - 2) + (p + 1)p^n(p^n - 1) \\ & +(p^n - p^{n-2})(2(p^n - 1) + (A - 3)p^n) \text{ times} \\ p^{\frac{n}{2}}, & p^{2n}(p^n - p - A + 1) \qquad \text{times} \\ p^{\frac{n+2}{2}}, & p^{n-2}(2(p^n - 1) + (A - 3)p^n) \qquad \text{times} \\ p^n, & (p + 1)p^n + 1 \qquad \text{times}. \end{cases} \tag{5.80}$$

If p is odd and $n = 4k + 2 > 2$, let N be found computationally, then:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & (p^n - 2) + (p+1)p^n(p^n - 1) + Np^n(p^n - p^{n-2}) \text{ times} \\ p^{\frac{n}{2}}, & 2p^n(p^n - 1) + p^{2n}(p^n - p - N - 2) \quad \text{times} \\ p^{\frac{n+2}{2}}, & Np^n p^{n-2} \quad \text{times} \\ p^n, & (p+1)p^n + 1 \quad \text{times}. \end{cases} \tag{5.81}$$

Finally, if p is odd and $n = 2$, then:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & (p^2 - 2) + (p+1)p^2(p^2 - 1) \quad \text{times} \\ p, & 2p^2(p^2 - 1) + p^4(p^2 - p - 2) \quad \text{times} \\ p^2, & (p+1)p^2 + 1 \quad \text{times}. \end{cases} \tag{5.82}$$

□

We also computed the correlation distribution for some values of p and n using MAGMA [2] and confirmed our results proved in the theorem. Now we give some examples on the correlation distribution of the sequence family $\mathcal{V}$.

Example 5.2. For $p = 3$ and $n = 2$, the correlation distribution of the sequence family $\mathcal{V}$ is found as:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & 295 \text{ times} \\ 3, & 468 \text{ times} \\ 9, & 37 \text{ times}. \end{cases} \tag{5.83}$$

This is the same result with the correlation distribution obtained from the proof.

Example 5.3. For $p = 5$ and $n = 4$, the correlation distribution of the sequence family $\mathcal{V}$ is found as:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & 9839423 \text{ times} \\ 25, & 234375000 \text{ times} \\ 125, & 312450 \text{ times} \\ 625, & 3751 \text{ times}. \end{cases} \tag{5.84}$$

This is the same result with the correlation distribution obtained from the proof.

Example 5.4. For $p = 2$ and $n = 5$, the correlation distribution of the sequence family $\mathcal{V}$ is found as:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & 17374 \text{ times} \\ 8, & 16352 \text{ times} \\ 64, & 33 \text{ times}. \end{cases} \tag{5.85}$$

This is the same result with the correlation distribution obtained from the proof.

Example 5.5. And finally, for $p = 2$ and $n = 6$, the correlation distribution of the sequence family $\mathcal{V}$ is found as:

$$|C_{i,j}(\tau) + 1| = \begin{cases} 0, & 91934 \text{ times} \\ 8, & 147456 \text{ times} \\ 16, & 26592 \text{ times} \\ 64, & 193 \text{ times.} \end{cases} \tag{5.86}$$

This is also the same result with the correlation distribution obtained from the proof.

5.4 Results

In this chapter, we generalize and classify the Gold-like sequence family with arbitrary characteristic, depending on an s-plateaued function $f(x)$. The function $f(x)$ is used to construct the generalized sequence family under the restriction of its time shift $f(\beta x) - f(x)$ being also a plateaued function depending on $\beta \in \mathbb{F}_{p^n}$. Previous constructions which use the Gold-like sequence family are based on a quadratic form function. By our generalization, one can generate new sequence families using arbitrary plateaued functions. Therefore, it is easy to compute their correlation distributions using Theorem 5.8.

Later, as an example, we compute the correlation distribution of the Gold-like sequence family constructed using the Gold function for all prime numbers p and positive integers n. We give the proof by taking advantage of the theory of algebraic curves and our generalization. In some cases, the correlation values depend on some integers that we spesified during the proof. Finally we give some computational results of correlation distributions of the sequence family $\mathcal{V}$ for some spesific p and n values. This chapter leads the interested readers to find more new sequence families with good correlation distributions.

CHAPTER 6

CONCLUSION

The most common methods of the code division multiple access are direct sequence and frequency hopping. These methods have widespread applications in radar systems, military and wireless communication. The sequences should satisfy some spesific properties to have these applications. In this thesis, we focus on two important properties of sequence design: perfect autocorrelation sequences and sequence families with low maximum cross-correlation magnitude.

In Chapter 1, we give a summary of mathematical background that we use during this thesis. We mention necessary properties of sequences, some known important sequences and sequence families. We compare the sequence families according to their family size and maximum correlation magnitude in Table 1.1.

In Chapter 2, we generalise a construction for perfect periodic autocorrelation sequences due to [18] for an arbitrary prime power q and a positive integer n over the PSK+ alphabet. Note that, we have the restriction $n+2 \equiv 0 \mod (q-1)$ in this construction. We experimentally check the existence of these sequences without any restrictions. The important point in this generalisation is that the subfield, which is used as the symbol alphabet, is not necessarily a prime field. Moreover, we give some examples of these sequences which have decent merit factor and aperiodic correlation properties.

In Chapter 3, our aim is to eliminate the restriction which we obtain in Chapter 2. For this purpose, we generalise the sequences in the previous chapter, using a variable i. We give perfect periodic autocorrelation sequences for all possible values of n and for a given prime power q, with respect to the constraint $n+i \equiv 0 \mod (q-1)$. The arbitrary subfield used as symbol alphabet is not necessarily a prime field. This generalisation enables the designers to have more flexibility in terms of the deployment of these sequences.

We focus on designing new sequence families which have low cross-correlation values in Chapter 4. We construct a sequence family for even positive integer n over the finite field $\mathbb{F}_{2^n}$ and prove the correlation distribution of this new family. Furthermore, the correlation values are determined exactly depending on an element $\beta \in \mathbb{F}_{2^n}$. The maximum cross-correlation magnitude $C_{\max}$ of the sequence family is obtained as $(1+2^{\frac{n+2}{2}})$ and this value shows that the sequence family has low maximum cross-

correlation magnitude. Having low maximum correlation magnitude is advantageous for the use of the sequence family in CDMA applications. It is obvious from Table 1.1. that, the new sequence family $\mathcal{S}$ has much bigger size than the small set of the Kasami sequences. On the other hand, small set of the Kasami sequences is optimal according to the Sidelnikov lower bound but the new sequence family does not attain the bound. In addition, the new sequence family $\mathcal{S}$ has the same maximum correlation magnitude with Gold sequence family and the large set of the Kasami sequences for $p = 2$ and even integer n.

In Chapter 5, we generalized and classified the Gold-like sequence family with arbitrary characteristic, depending on an s-plateaued function $f(x)$ which is used to construct the sequence family. Previous constructions, which use the Gold-like sequence family, are based on a quadratic form function. With our generalization method, one can generate new sequence families using arbitrary plateaued functions. Correlation distribution and maximum correlation magnitudes of this new construction are given for arbitrary p and n values. The correlation distribution of the generalized Gold-like sequence family constructed by the Gold function for all prime numbers p and positive integers n are obtained by using the theory of algebraic curves and our generalization. This chapter leads the interested readers to find more new sequence families with good correlation distributions.

REFERENCES

[1] P. Borwein, R. Ferguson, and J. Knauer, The merit factor problem, in J. McKee and C. Smyth, editors, *Number Theory and Polynomials*, pp. 52–70, Cambridge University Press, 2008, ISBN 9780511721274, cambridge Books Online.

[2] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., 24(3-4), pp. 235–265, 1997, ISSN 0747-7171, computational algebra and number theory (London, 1993).

[3] S. Boztaş, S. Kahraman, F. Özbudak, and E. Tekin, A generalized construction for perfect autocorrelation sequences, in *2015 IEEE International Symposium on Information Theory (ISIT)*, pp. 1541–1545, June 2015, ISSN 2157-8095.

[4] S. Boztaş and U. Parampalli, Nonbinary sequences with perfect and nearly perfect autocorrelations, in *2010 IEEE International Symposium on Information Theory*, pp. 1300–1304, June 2010, ISSN 2157-8095.

[5] 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.

[6] S. Boztaş 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.

[7] R. M. Buehrer, *Code Division Multiple Access (CDMA)*, Morgan and Claypool, 2006, ISBN 9781598290417.

[8] E. Çakçak and F. Özbudak, Curves related to Coulter's maximal curves, Finite Fields and Their Applications, 14(1), pp. 209–220, 2008.

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

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

[11] V. Ipatov, Ternary sequences with ideal periodic autocorrelation properties, Radio Engineering and Electronic Physics, 24, pp. 75–79, 1979.

[12] V. Ipatov, Contribution to the theory of sequences with perfect periodic autocorrelation properties, Radio Engineering and Electronic Physics, 25(4), pp. 31–34, 1980.

[13] P. Ipatov Valery, Spread spectrum and CDMA. principles and applications.

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

[15] 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.

[16] 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.

[17] 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.

[18] C. E. Lee, *On a new class of 5-ary sequences exhibiting ideal periodic autocorrelation properties with applications to spread spectrum systems*, PhD Thesis, Department of Electrical Engineering, Mississipi State University, 1986.

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

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

[21] I. Mercer, Merit factor of Chu sequences and best merit factor of polyphase sequences, IEEE Transactions on Information Theory, 59(9), pp. 6083–6086, 2013.

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

[23] 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.

[24] J. Olsen, R. Scholtz, and L. Welch, Bent-function sequences, IEEE Transactions on Information Theory, 28(6), pp. 858–864, Nov 1982, ISSN 0018-9448.

[25] P. Parraud, On the non-existence of (almost-) perfect quaternary sequences, in *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pp. 210–218, Springer, 2001.

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

[27] V. M. Sidel'nikov, On mutual correlation of sequences, Sov. Math. Doklady, 12, pp. 197–201, 1971.

[28] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread spectrum communications*, volume 1, Citeseer, 1985.

[29] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread spectrum communications handbook*, volume 2, Citeseer, 1994.

[30] H. Stichtenoth, *Algebraic function fields and codes*, volume 254, Springer Science & Business Media, 2009.

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

[32] P. Udaya and M. Siddiqi, Optimal and suboptimal quadriphase sequences derived from maximal length sequences over Z_4, Applicable Algebra in Engineering, Communication and Computing, 9(2), pp. 161–191, 1998.

[33] P. Udaya and M. U. Siddiqi, Optimal biphase sequences with large linear complexity derived from sequences over Z_4, IEEE Transactions on Information Theory, 42(1), pp. 206–216, 1996.

[34] X. Zeng, J. Q. Liu, and L. Hu, Generalized Kasami sequences: the large set, IEEE Transactions on Information Theory, 53(7), pp. 2587–2598, 2007.

[35] N. Zierler, Linear recurring sequences, Journal of the Society for Industrial and Applied Mathematics, 7(1), pp. 31–48, 1959.

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Tekin, Eda
Nationality: Turkish
Date and Place of Birth: 30 June 1987, Bursa
Marital Status: Married
Phone: 00903122105609
Fax: 00903122102985

EDUCATION

Degree	Institution	Year of Graduation
M.S.	KBU, Department of Mathematics	2012
B.S.	DPU, Department of Mathematics	2009
High School	Bursa Anatolian Girls High School	2005

PROFESSIONAL EXPERIENCE

Year	Place	Enrollment
2009-	KBU/Department of Mathematics	Research Assistant
2012-	METU/Institute of Applied Mathematics	Research Assistant

PUBLICATIONS

International Journal Publications

- İ. Özen, and E. Tekin, Moments of the support weight distribution of linear codes, Designs, Codes and Cryptography, 67(2), pp. 187–196, 2013.

International Conference Publications

- S. Boztaş, S. Kahraman, F. Özbudak and E. Tekin, A generalized construction for perfect autocorrelation sequences, in *2015 IEEE International Symposium*

on Information Theory (ISIT), pp. 1541-1545, June 2015, ISSN 2157-8095.

- S. Boztaş, F. Özbudak and E. Tekin, Correlation distribution of a new sequence family, 2015 IEEE International Symposium on Information Theory (ISIT), pp. 2707-2711, June 2015, ISSN 2157-8095.
- S. Boztaş, F. Özbudak and E. Tekin, Generalized perfect autocorrelation sequences with flexible periods and alphabet sizes, Sequences and Their Applications (SETA) 2016, accepted.