Copyright Notices

Notice 1

Notice 2

NEAR PERFECT SEQUENCES OF ODD AND EVEN LENGTHS

Rema Hariharan

A thesis submitted in fulfillment of the requirements for the award of the degree

Doctor of Philosophy

School of Mathematical Sciences,

Monash University, Australia

May, 2012

To

Hari & Hrishi

And above all ..... my beloved

Amma and Bhagavan

त्वमेव माता च पिता त्वमेव |
त्वमेव बन्धुश्च सखा त्वमेव ||
त्वमेव विद्या द्रविणं त्वमेव |
त्वमेव सर्वं मम देव देव ||

"O Lord, You Are My Mother, Father, Kinsman And Friend.
You Are My Wealth Of Knowledge, Strength, Velour And Power.
You Are My All God Of Gods".

Declaration

This thesis contains no material which has been accepted for the award of any other degree or diploma in any other university or institution. To the best of my knowledge, this thesis contains no material previously published or written by another person, except where due reference is made in the text of the thesis.

Rema Hariharan

Acknowledgement

I sincerely thank my supervisors, Dr Tom.E.Hall and Dr Andrew Tirkel for introducing me to the fascinating world of sequences and their applications, for their suggestions of possible results, for their patience and enthusiasm to read and improve this thesis. I truly acknowledge their empathy and consideration towards me throughout my candidature. It is through their guidance, constant support and encouragement, that I was able to complete this thesis.

I also acknowledge the kind help extended to me by Dr Udaya Parampalli amidst his busy schedule.

I also express my deepest gratitude to Mrs Gertrude Nayak, for her ongoing support and help with due concern and understanding. Her efficiency and dedication beyond her professional commitment to assist me have truly been remarkable and admirable. I would also extend my thanks to the admin and technical staff for their support.

I wish to thank the School for providing me with the travel grant to attend the Conference on Sequence Design and Applications (IWSDA), Fukuoka, Japan, in 2009.

I thank my colleagues, Samuel Blake and Santiago Barrera Acevedo for their assistance with the computer programming, which was an important tool for my computations.

I wish to thank my parents and all of my friends for their love, concern and moral support. My heartfelt thanks go to my best friend Sajan Veliath for his endless support though from a distance.

I specially appreciate my husband, Hari, who has been so supportive and understanding.

Finally, I take the pleasure of thanking the Faculty of Science for the Faculty of Dean's Scholarship to pursue my research.

Abstract

Sequences having zero correlation zones are of vital importance in applications, for example, wireless communications and quasi-synchronous CDMA systems. In this thesis, we construct new near perfect sequences of *odd* and *even* lengths, and those of *odd* lengths are constructed here, for the first time. Near perfect sequences are a special category of zero correlation zone sequences.

Near perfect sequences over roots of unity have many potential applications, in cellular communication systems, radar, position sensing and ultrasonic imaging.

Our contribution consists of three parts.

Part I:

First, we provide a method of constructing new near perfect sequences of odd lengths, over the roots of unity. We use a completely orthogonal pair of sequences and a shift sequence obtained by folding a binary M-sequence of length $2^{2J} - 1$, row-wise, into a $(2^J - 1) \times (2^J + 1)$ array for $J \geq 2$.

We provide many examples of near perfect sequences of odd lengths, illustrating our construction. We prove our main result, that near perfect sequences over the m^{th} roots of unity, m any odd prime, can be constructed for unbounded lengths. These lengths guarantee arbitrarily long zero correlation zones. Global Position Sensing (GPS) uses sequences of lengths approximately equal to 2^{40}. Our method can be used to construct new near perfect sequences of similar lengths, with very large zero correlation zones, since our construction produces near perfect sequences of unbounded lengths.

To examine the universality of our construction, we perform an exhaustive computer search of near perfect sequences of length 15. We found that, of all sequences obtained, one third of the sequences were equivalent to our constructed sequences. We classify these sequences into three types.

We also present a variation of our first construction of near perfect sequences. We obtain shift sequences by the method of folding M-sequences of length $2^{2J} - 1$, *diagonally* (rather than row-wise) into arrays with co-prime sizes.

Part II:

Next, we construct new near perfect sequences of even lengths, by concatenating two distinct near perfect sequences of the same odd length, under some given conditions.

Part III:

Finally, we examine some cross correlation sequences of some of our near perfect sequences of odd lengths. We find that, for each of our new near perfect sequences, say, $\boldsymbol{s}$, the cross correlation between $\boldsymbol{s}$ and $\boldsymbol{s}^*$ is also near perfect.

TABLE OF CONTENTS

List of Tables

1 INTRODUCTION AND HISTORICAL BACKGROUND

1.1 Introduction

The earliest research on sequences started with Fibonacci in the 15th century. Ever since, there have been remarkable contributions to this fascinating research area by many eminent researchers. The autocorrelation is the measure of how much a sequence differs from its shifts (translates). In the binary case, that is, a sequence with entries {0,1}, the autocorrelation just counts the difference between the number of agreements (A) of a binary sequence $\boldsymbol{a}$ for a shift τ and the number of disagreements (D). "Good" sequences are defined as those having one main peak and constant low off-peak values in their autocorrelation function. Sequences with “Good” auto and cross correlation properties have always caught the interest of the researchers over the past 60 years.

Although the earlier studies started with binary sequences and then moved to small phase alphabets, there is a dramatic increase in the search for sequences with low off peak auto and cross correlation properties in recent years. Sequences of this type find their application in radar, sonar, and synchronization. In addition to these applications, there are also important applications like cryptography, security systems and 3G-telephony for mobile and wireless communications based on Code Division Multiple Access (CDMA).

A sequence is called perfect if all the off peak autocorrelation values are zero. Perfect sequences over roots of unity have been studied extensively. Binary

perfect sequences are objects of particular interest. But the only known binary perfect sequence, up to equivalence, is $(1,1,1,-1)$. Unfortunately, in many cases perfect sequences do not exist. This lead to the search for Almost perfect sequences. A sequence is said to be almost perfect if it has exactly one non-zero off peak autocorrelation value. Almost perfect sequences were first studied by Wolfmann[73] and then by Luke[45].

A different definition can be found in Luke[45] where non-zero autocorrelation values are allowed at each shift $\tau \equiv 0 \, mod \left(\frac{N}{m}\right)$ where N is the length of the sequence and m is the alphabet size. The utmost alphabet size that Luke has looked into is $m = 4$. The sequences constructed by Luke were also named Almost perfect sequences [45]. Here after, we shall rename Luke's almost perfect sequences as "near perfect sequences" to avoid confusion. Almost perfect and near perfect sequences have been constructed over the m^{th} roots of unity where $m = 2,3,4,6,8,$ and only for even lengths [45, 73, 75].

In this thesis, we study near perfect sequences of odd and even lengths over alphabet sizes 3,5,7. We follow the approach of Zeng *et al.*[75] for our construction. We prove our main result in Section 4.6, that near perfect sequences over the m^{th} roots of unity, m any odd prime, exist for *unbounded* lengths. Our construction produces an equivalence class of near perfect sequences and an exhaustive computer search revealed other near perfect sequences of length 15 which cannot be obtained from the construction by standard invariance operations. We also consider the cross correlation of near perfect sequences in Chapter 6.

The near perfect sequences of new lengths N constructed in this text, have smaller non-zero cross correlation values than the autocorrelation values, namely for shifts which are multiples of $\left(\frac{N}{m}\right)$, and are commensurate with the sequence lengths used in the Global Positioning System (GPS). We give more details of this result in Chapter 7.

1.2 Outline of the thesis

The rest of the thesis is organized as follows:

The rest of this chapter gives a historical background of sequences.

In Chapter 2, we provide some basic definitions and notations which are relevant for our later chapters.

In Chapter 3, we give the background theory that consists of a brief literature review of perfect sequences. We introduce almost perfect sequences by Wolfmann[73] and near perfect sequences by Luke [45]. We then introduce the construction of a shift sequence obtained by row-wise folding by Games [21] and the results by Zeng *et al.* [75], which are relevant to our results in this thesis.

In Chapter 4, we give the first construction of near perfect sequences of odd lengths. Then we give the autocorrelation calculation and the proof of near perfection. We provide several examples in this chapter, illustrating our results. Some examples are given as powers of roots of unity and other examples are given as index sequences which can also be used for the autocorrelation calculation. We prove our main result that near perfect sequences over the m^{th}

roots of unity, m any odd prime, can be constructed for unbounded lengths. We perform an exhaustive computer search of near perfect sequences of length 15. We found that, of all sequences obtained, one third of the sequences were equivalent to our constructed sequences. We classify these sequences into three types. We also present a variation to the original construction of shift sequences by the method of folding M-sequences of length, $2^{2J} - 1$, $J \geq 2$, diagonally into arrays with co-prime sizes. We end this chapter with a diagrammatic representation of completely orthogonal pairs of sequences used for the construction of near perfect sequences. The results and some examples in this chapter have been presented by the author at the Fourth IEEE International Workshop on Signal Design and its Application in Communications in Fukuoka, Japan, 19-23 October 2009 and are published in the proceedings of that conference [30].

In Chapter 5, we show that new near perfect sequences of even lengths can be constructed by concatenating two distinct near perfect sequences of the same odd length under some given conditions. We provide examples for a better understanding of our construction.

In Chapter 6, we find that, for each of our new near perfect sequences, say, $\boldsymbol{s}$, the cross correlation between $\boldsymbol{s}$ and $\boldsymbol{s}^*$ is also near perfect. An example over the cube roots of unity, of length 3075, has 3 non-zero cross correlation values, each 3.

In Chapter 7, *Conclusions*, we give some prospective applications of near perfect sequences. Several open problems, namely, extension of dimension, construction

of longer near perfect sequences of odd and even lengths, by utilizing shift sequences containing more than one ∞, are given.

1.3 Historical Background

Sequences with pseudonoise properties have been researched over the past 60 years. Many areas of cryptography, coding theory and digital communications require families of sequences with good periodic auto and cross correlation properties. The following are additional attributes of pseudorandom-sequences that are highly desirable for applications.

i. Large linear span (also called linear complexity) – Linear span of a sequence is the length of the shortest linear feedback shift register that generates that sequence.

   The number of cyclically distinct sequences increases with linear span. Large linear span also helps to resist attacks.

ii. Good balance properties - Balance property states that symbols occur as equally often as possible within one period of a sequence.

iii. Long sequence length and

iv. Large family size.

Sequences having one main peak and constant low off-peak values in their autocorrelation function are called pseudonoise sequences [29]. Many papers discuss the properties, construction and application of pseudonoise sequences.

Techniques of pseudorandom sequences have been widely used in communication and cryptography since 1948 when Shannon's Information theory was introduced to solve problems in communication or transmission of signals over channels. The research in pseudorandom sequences can be divided into three periods:

1. Period of pre-application (before 1948)
2. Golden period of M-sequences (*Definition 2.3.12*) (1948-1969)
3. Period of non-linear generators (1969-present)

Before 1948, the study of pseudorandom sequences was of theoretical interest because of their elegant mathematical structure.

M-sequences had been studied for cryptographic purposes before they were considered for communication purposes. Generation of a pseudorandom sequence with a large period was a critical problem around the early 1950's. In March 1955, shift register generators were introduced as potential error correcting code hardware.

Linear feedback shift register (LFSR) sequences were used as pseudorandom sequence generators. Let $F = GF(q)$, where q is a prime or a power of a prime. In a q-ary shift back register with n-stages, there are q^n possible states. The successor of the n-tuple $(0,0,0,\cdots,0)$ is again $(0,0,0,\cdots,0)$. So, only the non-zero states are used and the maximum period possible is $q^n - 1$. A q-ary feed back shift register of length n can generate a sequence of period $q^n - 1$ with a primitive polynomial of degree n over $GF(q)$. When $q = 2$, the length of a binary sequence generated is $2^n - 1$.

A diagram of a binary LFSR which uses a primitive polynomial of degree 4, over $GF(2)$ to generate an M-sequence of length 15, is given below.

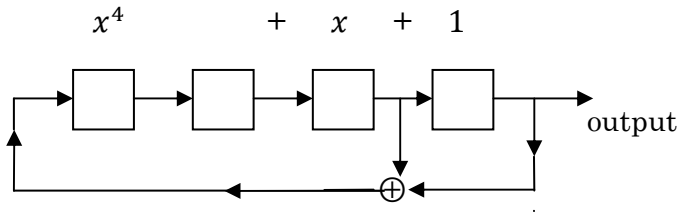


Figure 1. An LFSR corresponding to x^4+x+1

In the literature, these sequences are called by different names viz, Maximal length sequences, M-sequences and since they possess the property of one main peak and constant non-zero off peak autocorrelation values, they are also called pseudonoise sequences [25].

Prof. Golomb's popular book *Shift Register Sequences* [23] deals with much of the work on LFSR sequences. Neal Zierler in [77] has given a detailed and elegant mathematical treatment on M-sequences. The characteristics and the correlation properties are also thoroughly examined. Golomb in his book *Shift Register Sequences* [23] has given the criteria for a sequence to be pseudonoise (*Definition 2.3.18*). These are called Golomb's randomness postulates. The autocorrelation function of a sequence is a measure of how much the given sequence differs from its shifts. Sequences with good correlation properties find their applications in various fields. The first chairman of the IRE Information theory group and early practitioner of correlation techniques, Nathan Marchand, presented a jingle where radar correlation detection methodology was discussed.

Correlation is the best,

It outdoes the rest,

Use it in your guided missile,

All they will hear will be whistle, whistle, whistle, whistle.....[64]

The majority of research in pseudorandom sequences applied to communications has concentrated on binary sequences. This is because the application of these sequences is simpler. $Modulo\ 2$ arithmetic is used and it is easily implemented electronically.

Sequence application in the field of spread spectrum demanded more research and results on complex valued sequences. For the early applications, binary M-sequences were used because of their excellent periodic autocorrelation properties. For M-sequences over $GF(2)$, the autocorrelation values are calculated by Golomb [23] and an extension to arbitrary $GF(q)$ is given in Zierler[77]. Sarwate and Pursley in [59] describe the auto and cross correlation functions of binary as well as complex valued sequences. The invariance properties of the autocorrelation of sequences were also studied by many researchers. One of the invariance properties is the proper decimation of a sequence. The method of taking every f^{th} term of a sequence is called decimating a sequence. Decimation is referred to as sampling in early literature. [59] gives an understanding of preferred decimations leading to preferred pairs of M-sequences that are used to construct Gold, Kasami and other sequences with three valued cross correlation functions. Maximal connectedness of preferred pairs of M-sequences is well explained using diagrams. Everett in [15] from

Telecommunications Research laboratories, Hirst Research Centre, showed that the problems of the existence of Difference sets, cyclic symmetric balanced incomplete block designs and binary pseudonoise sequences are equivalent.

The trace functions were introduced in the later part of the sixties. The trace function is an equally distributed, one-one, onto mapping from a finite field $GF(q^n)$ to the base field $GF(q)$. The trace representation of LFSR sequences is a powerful tool for the analysis of the randomness of pseudorandom-sequences and for the design of pseudorandom sequences with desired properties [65]. Trace functions have a very elegant representation and were used to compute cross correlation of M-sequences. Many books [21, 49, 64, 65] and papers on sequence design discuss the trace function. Later on, in the eighties, trace functions were used as a tool to obtain new sequences. Computation of cross correlation of M-sequences and Gold sequences invariably uses the properties of the trace functions [22, 24, 34]. Olsen *et al.* [53] use these functions to obtain a new construction, namely Bent function sequences. The paper [61] by Scholtz and Welch, giving algebraic explanation of GMW sequences and cascaded GMW sequences by Klapper *et al.*[38], are some examples which make use of trace function representation [54].

Several applications such as coding and Digital watermarking (a process of embedding invisible marks or labels into digital content) have called for two-dimensional and multi-dimensional arrays with two-level autocorrelation functions. A description of two and three-dimensional pseudonoise arrays can be found in Green and Amarasinghe [28]. The search for large families of pseudo-

noise arrays for various applications lead to the study of shift sequences. Different types of shift sequences are discussed by Tirkel *et al.* [67]. An early study of this topic was done by Baumert [2] by folding a suitable M-sequence row-wise and by Games [21] in 1985. Weng [72] had done the decomposition of M-sequences much before Games, by folding an M-sequence diagonally into a $p \times q$ array with p, q co-prime to each other. The shift sequences were initially used to construct sonar sequences. The periodic cross correlation of M-sequences and GMW sequences constructed from the same primitive polynomial is also explained using the shift sequence property in [21]. Binary pseudonoise sequences with off peak autocorrelation values equal to zero have always been of research interest. These sequences are called perfect sequences. Unfortunately, binary perfect sequences of length greater than 4 are unknown. Heimiller [32] has given a construction of perfect sequences of length p^2 where p is an odd prime using a $p \times p$ array. The entries of this array are the p^{th} roots of unity. Later Frank generalised this construction to any positive integer N. There are many recent publications on constructing perfect sequences using different techniques. Mow [52] conjectured that there exists no perfect sequence over the n^{th} roots of unity of length above n^2. The restriction on the lengths of complex valued perfect sequences lead to the exploration of Zero Correlation Zone (ZCZ) sequences, (Sequences that have zero correlation for shifts not greater than a specified shift.) Low Correlation Zone (LCZ) sequences and Almost Perfect (AP)

sequences due to their low off peak autocorrelation values. This topic has caught the interest of many recent researchers. Many approaches are made to construct these sequences. Explanations about ZCZ sequences can be found in Torri *et al.* [31, 69] and about LCZ sequences in [5, 55] and other current research papers. The earliest paper on almost perfect sequences was by Brown and Godwin [6]. An algebraic theory of these sequences can be seen in Langevin [40] and the existence of almost perfect sequences is discussed by Pott and Bradley [57]. Almost perfect and near perfect sequences can also be viewed as special cases of zero correlation zone sequences. Unfortunately, not many designs with small alphabet size, which is the case of practical interest for telecommunications, are currently known.

2 BASIC DEFINITIONS AND NOTATIONS

In this Chapter, we see some definitions which are relevant to the topics discussed. We use Finite fields for the construction of M-sequences and our construction employs roots of unity. We also discuss the auto and cross correlation of sequences.

We begin with the basic definitions of Finite fields in Section 2.1. Definitions of roots of unity are given in Section 2.2. Sections 2.3 and 2.4 deal with the definitions and properties of sequences and arrays respectively.

All sequences are denoted by bold letters whereas scripts and capital letters are used to denote the matrices and arrays.

2.1 Finite Fields

Most of the following definitions are taken from Lidl and Neiderriter [43] and Fraleigh[16].

Definition 2.1.1 *Finite Field*

Consider a set F on which two binary operations, called addition and multiplication, are defined. Then F is called a ***field*** if it

i. Contains two distinguished elements 0 and e with $0 \neq e$.
ii. Is an abelian group with respect to addition, has 0 as the additive identity element, and the non-zero elements of F form an abelian group with respect to multiplication having e as the identity element.

iii. Satisfies the distributive law $a(b+c) = ab + ac$ for $a, b, c \in F$.

A field having a finite number of elements is called a ***finite field***.

Definition 2.1.2 *Subfield/Proper subfield*

Let F be a field. A subset K of F that is itself a field under the operations of F is called a ***subfield*** of F and F is called an extension (field) of K. If $K \neq F$, K is called a ***proper subfield*** of F.

Definition 2.1.3 *Galois field*

For each prime p let $\mathbb{F}_p$ be the set $\{0,1,2,\cdots,p-1\}$ of integers and let $\varphi: \mathbb{Z}/p \to \mathbb{F}_p$ be the mapping defined by $\varphi(a) = a, a = 0,1,2,\cdots,p-1$. Then $\mathbb{F}_p$ is a finite field called a ***Galois field*** of order p, denoted by $GF(p)$. For every prime p there exists a finite field $GF(p^n)$ of order p^n for every positive integer n which is called the extension field of $GF(p)$.

Definition 2.1.4 *Polynomial over a field*

Let F be a field. A polynomial over F is an expression of the form $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ where n is a positive integer and the *coefficients* a_i, $0 \leq i \leq n$, are elements of F. The symbol x not belonging to F is called an indeterminate over F.

A polynomial $f(x)$ over a field F having 1 as the coefficient of the highest power of x appearing is called a *monic* polynomial.

Definition 2.1.5 *Algebraic element*

An element α of an extension field E of a field F is ***algebraic over*** F if $f(\alpha) = 0$ for some non-zero polynomial $f(x) \in F[x]$.

Definition 2.1.6 *Irreducible polynomial*

Let F denote a field. A polynomial $\mathbb{p} \in F[x]$ is called irreducible over F if $\mathbb{p}$ has positive degree and $\mathbb{p} = \mathbb{b}\mathbb{c}$ with $\mathbb{b}, \mathbb{c} \in F[x]$ implies that either $\mathbb{b}$ or $\mathbb{c}$ is a constant polynomial. Otherwise, $\mathbb{p}$ is called reducible over F.

Definition 2.1.7 *Minimal polynomial*

Let $\boldsymbol{E}$ be an extension field of F and $\alpha \in E$ be algebraic over F. Then the uniquely determined monic polynomial $f(x) \in F[x]$ generating the ideal $J[x] = \{f(x) \in F[x]: f(\alpha) = 0\}$ of $F[x]$ is called the minimal polynomial of α over F.

Definition 2.1.8 *Primitive polynomial*

A generator of the cyclic group $GF(p^n)^*$ is called a primitive element of $GF(p^n)$. The group $GF(p^n)^*$ contains the non-zero elements of $GF(p^n)$.

An irreducible polynomial over $GF(p)$ having a primitive element in $GF(p^n)$ as a root is called a primitive polynomial over $GF(p)$. The number of primitive polynomials of degree n over $GF(p)$ is $\frac{1}{n}\phi(p^n - 1)$ where ϕ is the Euler ϕ function[23].

Definition 2.1.9 *Conjugate field elements*

Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a primitive polynomial in x over $GF(q)$, q a power of a prime. Let $\alpha \in GF(q^n)$ be a root of $f(x)$. The conjugates of α are $\alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$, which are the other $(n-1)$ of roots of $f(x)$.

Definition 2.1.10 *Trace Function*

Let q be a prime or a power of a prime. For $x \in F = GF(q^n)$ and $K = GF(q)$. The trace function $Tr_{F/K}(x)$ is defined by $Tr_{F/K}(x) = x + x^q + \cdots + x^{q^{n-1}}$; $x \in F$. The trace maps a field $GF(q^n)$ onto the proper subfield $GF(q)$.

2.2 Roots of unity

Definition 2.2.1 A complex number ω is called an n^{th} root of unity if $\omega^n = 1$.

Definition 2.2.2 An n^{th} root of unity ω is called primitive if $\omega^n = 1$ and $\omega^s \neq 1$ for all $1 \leq s < n$.

Definition 2.2.3 The n^{th} root of unity of the form $\omega = e^{\frac{2\pi i}{n}}$ is called the principal n^{th} root of unity [16].

2.3 Sequences

Definition 2.3.1 *Sequence*

An ordered n-tuple $\boldsymbol{s} = (s_0, s_1, s_2, \cdots, s_{n-1})$ of entries from a set $\mathcal{S}$ is called a ***sequence***. The set $\mathcal{S}$ is called an alphabet and n is called the length of the sequence $\boldsymbol{s}$.

A sequence is said to be ***binary*** if each $s_i \in \{0,1\}$ or $\{+1, -1\}$, for a roots of unity sequence. A binary sequence over $\{+1, -1\}$ is obtained under the mapping $\phi: \phi(a) = (-1)^a$, where $a \in \{0,1\}$. The mapping ϕ matches $GF(2)$ to the bi-phase signal set $(+1, -1)$ for binary inner product correlations.

Definition 2.3.2 *Norm of a sequence*

The ***norm*** of a sequence is defined as the sum of the norms of all its elements. $\|\boldsymbol{s}\| = \sum_{i=0}^{n-1} \|s_i\|$.

Definition 2.3.3 *Period of a sequence*

Let a sequence $\boldsymbol{s} = (s_0, s_1, s_2, \cdots, s_{n-1})$ be a sequence with complex entries. If n is the smallest integer such that $s_{i+n} = s_i$ for every n, then $\boldsymbol{s}$ is called a ***periodic sequence*** with period n.

Definition 2.3.4 *Balance of a sequence*

The sum of all elements of a sequence $\boldsymbol{s}$ is called the ***balance*** of the sequence $\boldsymbol{s}$ and is denoted by $\sum s_i$.

Definition 2.3.5 *Left shift operator*

The ***left shift operator*** $\mathcal{L}$ of a sequence $\boldsymbol{s} = (s_0, s_1, s_2, \cdots, s_{n-1})$, is defined by $\mathcal{L}(\boldsymbol{s}) = (s_1, s_2, s_3, \cdots, s_{n-1}, s_0)$. Then $\mathcal{L}^i(\boldsymbol{s}) = (s_i, s_{i+1}, s_{i+2}, \cdots, s_{i-1})$.

For any integer $i > 0$, $\mathcal{L}^i(\boldsymbol{s}) = \mathcal{L}\left(\mathcal{L}^{i-1}(\boldsymbol{s})\right)$ and $\mathcal{L}^0(\boldsymbol{s}) = \boldsymbol{s}$.

Example 2.3.1

Let $\boldsymbol{a} = (a_0, a_1, a_2, \cdots, a_{14})$ be a sequence of length 15.

Then $\mathcal{L}^{(2)}(\boldsymbol{a}) = (a_2, a_3, a_4, \cdots, a_0, a_1)$.

Definition 2.3.6 *Hamming weight*

Let $\boldsymbol{b} = (b_0, b_1, b_2, \cdots, b_{n-1})$ be a sequence over $GF(q^n)$ with period n. The Hamming weight of $\boldsymbol{b} = \{b_t\}, 0 \leq t \leq n-1$, denoted by $w(\boldsymbol{b})$ is defined as

$$w(\boldsymbol{b}) = \#\{t, 0 \leq t \leq n-1 : b_t \neq 0\}$$

The weight of a polynomial $a(x) = \sum_{i=0}^{n-1} a_i x^i$ over $GF(2)$ is defined by

$w[a(x)] = w(\boldsymbol{a})$ if $\boldsymbol{a} = (a_0, a_1, a_2, \cdots, a_{n-1})$ is a sequence over $GF(2)$.

Definition 2.3.7 *Hamming distance*

Let $\boldsymbol{a} = (a_0, a_1, a_2, \cdots, a_{n-1})$ and $\boldsymbol{b} = (b_0, b_1, b_2, \cdots, b_{n-1})$ be two sequences over $GF(q^n)$. Then the ***Hamming distance*** $\boldsymbol{d(a, b)}$ is the number of positions in which $\boldsymbol{a}$ and $\boldsymbol{b}$ differ.

Definition 2.3.8 *Dot product*

The dot product of two sequences $\boldsymbol{a} = (a_0, a_1, a_2, \cdots, a_{n-1})$ and $\boldsymbol{b} = (b_0, b_1, b_2, \cdots, b_{n-1})$ is defined by

$$\boldsymbol{a}.\boldsymbol{b} = \sum_{i=0}^{n-1} a_i b_i^*$$

where $\boldsymbol{s}^*$ denotes the complex conjugate of $\boldsymbol{s}$.

Definition 2.3.9 *Periodic cross correlation*

The ***periodic cross correlation*** $C_{\boldsymbol{s},\boldsymbol{t}}(\tau)$ of two sequences $\boldsymbol{s} = (s_0, s_1, \cdots, s_{n-1})$ and $\boldsymbol{t} = (t_0, t_1, \cdots, t_{n-1})$ of length n, for a shift τ, is defined by

$$C_{\boldsymbol{s},\boldsymbol{t}}(\tau) = \sum_{i=0}^{n-1} s_i t_{i+\tau}^*$$

where $i + \tau$ is calculated *modulo n.*

When $\boldsymbol{s} = \boldsymbol{t}$, then $C_{\boldsymbol{s},\boldsymbol{t}}(\tau) = \Theta_{\boldsymbol{s}}(\tau)$ and $\Theta_{\boldsymbol{s}}(\tau)$ is called the periodic ***autocorrelation*** value of the sequence $\boldsymbol{s}$, for the shift τ.

In terms of the dot product, the autocorrelation value,

$$\Theta_{\boldsymbol{s}}(\tau) = \boldsymbol{s}.\boldsymbol{s}^{\tau} = \sum_{i=0}^{n-1} s_i s_{i+\tau}^*$$

Definition 2.3.10 *Completely orthogonal sequences*

Two sequences $\boldsymbol{s}$ and $\boldsymbol{t}$ are called ***completely orthogonal*** if $C_{\boldsymbol{s},\boldsymbol{t}}(\tau) = 0$ for all τ including the zero shift.

Example 2.3.1

Let $\boldsymbol{s} = (1,1,-1,-1)$ and $\boldsymbol{t} = (1,i,1,i)$ be two sequences over the 4^{th} roots of unity. Then $\boldsymbol{s}$ and $\boldsymbol{t}$ are completely orthogonal.

Definition 2.3.11 *Perfect sequence*

A sequence $\boldsymbol{s} = (s_0, s_1, s_2, \cdots, s_{n-1})$ over complex numbers is called ***perfect*** if all the off-peak autocorrelation values are zero, that is, $\Theta_{\boldsymbol{s}}(\tau) = 0$ for all shifts τ, $0 < \tau \leq n-1$.

Example 2.3.2

Let $\boldsymbol{s} = (1,1,1,-1)$ be a binary sequence of length 4.

Here, $\Theta_{\boldsymbol{s}}(\tau) = 0$ for all shifts $\tau \neq 0$.

Definition 2.3.12 *M-sequences*

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ be a primitive polynomial with $a_i \in GF(q)$ and q is a prime power. If $f(x)$ specifies an n-stage Linear Feedback Shift Register (LFSR) with an initial state $(a_0, a_1, \cdots a_n)$, $a_i's$ not all zeros, then the output sequence is a q-ary sequence of length $q^n - 1$. This sequence is called a ***Maximal length sequence (M-sequence).***

With any non-zero initial state, the shift register goes through all possible $q^n - 1$ non-zero states before repeating. Thus an M-sequence has period $q^n - 1$. If $q = 2$, a binary M-sequence is generated by an n-stage LFSR with period $2^n - 1$.

Definition 2.3.13 *Decimation of a sequence*

Let $\{u_n\}$ be an arbitrary sequence of period N, and consider the sequence defined by $v_n = u_{fn}$ for all n. The sequence $\{v_n\}$ is said to be the ***decimation*** by f of the sequence $\{u_n\}$. If f divides N, then $\{v_n\}$ has a period $\left(\frac{N}{f}\right)$. If $gcd(N, f) = 1$, then the period of $\{v_n\}$ is N and the decimation is said to be *proper*. In general, the decimation by f of a sequence with period N produces a sequence with period $\frac{N}{\gcd(N,f)}$.

Definition 2.3.14 *Linear span/Linear complexity*

Let $\boldsymbol{a} = (a_0, a_1, a_2, \cdots, a_{n-1})$ be a periodic sequence constructed from a finite field F. Then the degree of the minimal polynomial (*Definition 2.1.7*) of $\boldsymbol{a}$ is called the ***linear span*** or ***linear complexity*** of $\boldsymbol{a}$. In other words, the linear span of a periodic sequence is the length of the shortest LFSR that can generate the sequence. The robustness of a sequence increases with the linear span.

Sarwate and Pursley [59] mention the three-valued cross correlation spectrum for a pair of binary M-sequences $\boldsymbol{u}, \boldsymbol{v}$, of period n, where the sequence $\boldsymbol{v}$ is obtained by a q^{th} decimation (given by Gold and Welch), of $\boldsymbol{u}$, where $q = 2^k + 1$ or $q = 2^{2k} - 2^k + 1$ such that $gcd(n, k) = e$ and $\left(\frac{n}{e}\right)$ is odd.

Definition 2.3.15 *Preferred pair*

Two binary M-sequences of period n, form a ***preferred pair*** if their cross-correlation function takes on the three values $-1, -\left(1 + 2^{\left\lfloor\frac{n+2}{2}\right\rfloor}\right), \left(2^{\left\lfloor\frac{n+2}{2}\right\rfloor} - 1\right)$

where $\lfloor a \rfloor$ denotes the integer part of a real number a.

Definition 2.3.16 *Connected set*

A ***connected set*** of M-sequences is a collection of M-sequences which has the property that each pair in the collection is a preferred pair. A largest possible connected set is called a ***maximal connected set*** and the size of such a set is denoted by M_n.

Definition 2.3.17 *Zero Correlation Zone (ZCZ) sequences*

Let $\mathcal{S}$ be the set of $\mathcal{M}$ complex sequences of length L. Take any two sequences $\boldsymbol{a} = (a_0, a_1, a_2, \cdots, a_{n-1})$ and $\boldsymbol{b} = (b_0, b_1, b_2, \cdots, b_{n-1})$ belonging to $\mathcal{S}$. $\mathcal{S}$ is called an$(L, \mathcal{M}, Z_{cz})$-ZCZ set with a ***zero correlation zone*** width Z_{cz} if

$$\Theta_{\boldsymbol{a},\boldsymbol{b}}(\tau) = \begin{cases} \sum_{i=0}^{n-1} (|a_i|)^2 & if\ \boldsymbol{a} = \boldsymbol{b}, \tau = 0 \\ 0 & if\ \boldsymbol{a} \neq \boldsymbol{b}, \tau = 0 \\ 0 & if\ \ 1 \leq |\tau| \leq Z_{CZ} \end{cases}$$

Thus for any $\boldsymbol{a}, \boldsymbol{b} \in S$, $\Theta_{\boldsymbol{a}}(\tau) = 0$ for $1 \leq |\tau| \leq Z_{cz}$ and $\Theta_{\boldsymbol{a},\boldsymbol{b}}(\tau) = 0$ for $1 \leq |\tau| \leq Z_{cz}$ and $\boldsymbol{a} \neq \boldsymbol{b}$.

Definition 2.3.18 *Pseudonoise sequence*

A binary sequence over $\{+1, -1\}$, of length n, which satisfies the following properties, is called a pseudonoise sequence.

i. Balance property: In every period, the number of $+1's$, is as close as possible to the number of $-1's$.

ii. Run property: The total number of runs of $+1's$, is equal to the total number of runs of $-1's$.

iii. A two-level autocorrelation function.

2.4 Arrays

Definition 2.4.1 *Circulant Array*

An $n \times n$ array of the form $\begin{bmatrix} a_0 & a_{n-1} & \cdots & a_2 & a_1 \\ a_1 & a_0 & \cdots & a_3 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & a_0 & a_{n-1} \\ a_{n-1} & a_{n-2} & a & a_1 & a_0 \end{bmatrix}$ is called a ***circulant*** array. The seed column is $\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ \vdots \\ a_{n-1} \end{bmatrix}$.

Arrays of this type are used in the construction of near perfect sequences.

Definition 2.4.2 *Periodic shift (k,l) of an array $\mathbb{A}$*

For any array $\mathbb{A} = (a_{ij})$, $0 \le i \le m-1; 0 \le j \le n-1$, the shifted array of $\mathbb{A}$ by k places horizontally to the left, and l places vertically upwards, denoted by $\mathbb{A}^{(k,l)}$, has $(i,j)th$ entry equal to $(a_{i+l,j+k})$, $0 \le i \le m-1; 0 \le j \le n-1$.

Definition 2.4.3 The periodic autocorrelation of an array $\mathbb{A} = (a_{ij})$ is

$$\Theta_{\mathbb{A}}(k,l) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{ij} a^*_{i+l,j+k}$$

where $i+l$ and $j+k$ are calculated $modulo$ m and n respectively.

For $k = 0$ and $l = 0$, the autocorrelation value $\Theta_{\mathbb{A}}(0,0)$ is called the *peak value* and for $k = 0$ and $l = 0$, the autocorrelation value for $(k, l) \neq (0,0)$, the values $\Theta_{\mathbb{A}}(k, l)$ are called *off -peak* values. The autocorrelation function $\Theta_{\mathbb{A}}(k, l)$ can be related to a sum of dot products of shifted columns of $\mathbb{A}$:

$$\Theta_{\mathbb{A}}(k, l) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{ij} a^*_{i+l,j+k}$$

Interchanging the summation signs we get,

$$\Theta_{\mathbb{A}}(k, l) = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{m-1} a_{ij} a^*_{i+l,j+k} \right)$$

$$= \sum_{j=0}^{n-1} \left(a_{oj} a^*{}_{l,j+k} + a_{1j} a^*{}_{1+l,j+k} + \cdots + a_{(m-1)j} a^*{}_{(m-1)+l,(n-1)+k} \right)$$

$$= \textstyle\sum_{j=0}^{n-1} \mathrm{c}_j \cdot \mathrm{c}^l{}_{j+k} \qquad (2.4.1)$$

The dot product of the two columns c_j and $\mathrm{c}^l{}_{j+k}$ is unaltered if both columns are rotated l places downwards, that is, $-l$ places upwards, so

$\mathrm{c}_j \cdot \mathrm{c}^l{}_{j+k} = \mathrm{c}_j{}^{-l} \cdot \mathrm{c}^{l-l}{}_{j+k} = \mathrm{c}_j{}^{-l} \cdot \mathrm{c}_{j+k}$

and we have $\Theta_{\mathbb{A}}(k, l) = \textstyle\sum_{j=0}^{n-1} \mathrm{c}_j{}^{-l} \cdot \mathrm{c}_{j+k} \qquad (2.4.2)$

Similarly, the periodic cross correlation of two arrays $\mathbb{A}$ and $\mathbb{B}$ can also be calculated using the dot products of the columns of $\mathbb{A}$ and the corresponding shifted columns of $\mathbb{B}$.

Definition 2.4.4 *Almost square array*

Let $\boldsymbol{a} = (a_0, a_1, \cdots, a_{n^2-2})$ be a sequence of length $n^2 - 1$. The array

$$\begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_n \\ a_{n+1} & a_{n+2} & a_{n+3} & \cdots & a_{2n+1} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ a_{n^2-n-1} & a_{n^2-n} & \cdots & \cdots & a_{\boldsymbol{n^2-2}} \end{bmatrix}$$ of dimension $(n-1) \times (n+1)$ is called an

almost square array.

Definition 2.4.5 *Pseudorandom array*

An array of order $p \times q$ constructed from an M-sequence of length $q^n - 1$ where $q^n - 1 = pq$ and p and q are relatively prime integers, is called a pseudorandom array.

Arrays in *Definitions 2.4.4* and *2.4.5* are used in our construction.

The above definitions are only the fundamental definitions which are useful for the whole text. Other definitions relevant to each section are included in the respective chapters.

3 BACKGROUND THEORY

In this Chapter we review the basics from the literature that is relevant to our research. In Section 3.1 and 3.2 we give an overview of perfect sequences and their properties. Section 3.3 gives several types of perfect sequences over different alphabets and Section 3.4 discusses the conditions of existence and non-existence of perfect sequences. In Sections 3.5 and 3.6 we review the construction of almost perfect sequences by Wolfmann [73], Luke [45] and in Section 3.7 we introduce the definition of the shift sequence by Games [21] and the construction of almost perfect sequences by Zeng *et al.* [75] in Section 3.8.

3.1 Perfect sequences

First, we present a brief literature survey on perfect sequences. We also give a brief description of different known types of perfect sequences.

A sequence is said to be perfect, if all the off-peak values of their periodic autocorrelation values are equal to zero.

Perfect sequences over complex numbers have many applications in diverse areas such as Spread Spectrum Multiple Access (SSMA) systems, pulse compression radars and fast start up equalization and channel estimation [52].

Sequences over n^{th} roots of unity are considered by various authors, when constructing perfect sequences. These sequences are called polyphase or Phase-Shift Keying (PSK) sequences in different contexts.

According to Bomer and Antweiler [3], perfect polyphase sequences and arrays have been constructed in [11], [18] and are studied by many authors such as [3] and [44]. Their periodic and aperiodic correlation properties are given by Heimiller [32], Frank [18] and Golomb *et al.* [3, 76].

3.1.1 Perfect Sequences over the set of Real Numbers $\mathbb{R}$

There are three types of known perfect sequences over the field of real numbers $\mathbb{R}$.

i. Binary perfect sequences with entries from the set $\{-1,1\}$.

   The only known binary perfect sequence is of length 4. It is conjectured that there are no perfect binary sequences of length n, for $4 < n \leq 12{,}100$.

ii. Ternary perfect sequences with entries from $\{-1,0,1\}$

   These sequences given by Chang[8] and Ipatov[37].

   Ipatov[37] generalizes the construction of Chang[8]. The length N of these sequences is $N = \frac{q^{2k+1}-1}{q-1}$, where $q = p^w$, p an odd prime, w a positive integer.

The peak factor of radiation of a sequence $\boldsymbol{s} = (s_0, s_1, s_2, \cdots, s_{N-1})$ is given by

$$\nu = \frac{N}{\Theta_s(0)} max\left|s_i^2\right|$$

where N is the length of $\boldsymbol{s}$ and $\Theta_{\boldsymbol{s}}(0)$, the peak autocorrelation value of $\boldsymbol{s}$. The peak factor should be relatively small, almost equal to 1, for practical uses.

In Ipatov's construction, $max|s_i^2| = 1$. So, $\nu = \frac{N}{\Theta_{\boldsymbol{s}}(0)}$. Ipatov's construction gives $\nu = 1.033$, which is close to 1, and with a very small relative number of zeros per period.

Ipatov comments that the ternary sequences from $\{-1,0,1\}$ with a peak factor close to 1 have unquestionable use in practical applications.

iii. Multilevel perfect sequences with elements having different magnitude. These sequences may or may not include 0 among their entries. Examples of these sequences can be seen in Section 3.3.14.

3.2 Properties of perfect sequences over $\mathbb{C}$

The following invariance properties of autocorrelation of sequences over roots of unity, which is a subset of the set of complex numbers $\mathbb{C}$, are also true for perfect polyphase sequences.

If $\boldsymbol{a} = [a_0, a_1, \cdots, a_{n-1}]$ is a perfect polyphase sequence, then so are the following[64].

For $0 \leq i \leq n-1$,

1) $[a_{i\pm\tau}]$, where τ is any integer and the subscript is calculated $mod\ n$;
2) $[ca_i]$, where c is any complex constant;

3) $[a_i\beta^{im}]$, where m is any integer and β is an n^{th} root of 1;

4) $[a_i{}^*]$, where $*$ denotes complex conjugation;

5) The Discrete Fourier Transform of $\boldsymbol{a}$, $[DFT(\boldsymbol{a})] = A_k = \sum_{t=0}^{n-1} e^{\frac{2\pi i}{n}kt} a_t$, where $e^{\frac{2\pi i}{n}}$ is a primitive n^{th} complex root of unity.

3.3 Known constructions of perfect sequences

3.3.1 Binary perfect sequences

Binary sequences are preferred in practical applications due to their easy implementation. Unfortunately, the only known binary perfect sequence is $[1,1,1,-1]$.

The definition below provides a link to Hadamard matrices.

Definition 3.3.1 Hadamard matrix

A Hadamard matrix is a square matrix whose elements are either +1 or −1 and whose rows and columns are mutually orthogonal, named after the French mathematician, Jacques Hadamard.

If H_n is a Hadamard matrix of order n, then $H_n H_n^T = H_n^T H_n = nI_n$ where I_n is the identity matrix of order n, because the norm of each row or column equals n.

Example 3.3.1 Hadamard matrix of order 2

The simplest non-trivial Hadamard matrix is $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ The recursive application of this matrix produces Sylvester Hadamard matrices of higher order.

Unfolding H_2 row-wise, we get the only known binary sequence $[1,1,1,-1]$. Unfolding all Hadamard matrices do not give rise to perfect sequences. This is a special case.

We have already seen the definition of a circulant array/matrix in Definition 2.4.1.

Example 3.3.2 Circulant Hadamard Matrix of order 4 [2]

The matrix $H_4 = \begin{bmatrix} 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \end{bmatrix}$ is a circulant Hadamard matrix of order 4.

We see that each column of H_4 is a cyclic shift of the perfect binary sequence $[1,1,1,-1]$. There are also other constructions of Hadamard matrices. The Hadamard matrices constructed from extended M-sequences are orthogonal only for the zero shift.

Horadam [36] gives a detailed introduction to Hadamard matrices.

3.3.2 Ternary perfect sequences

Ternary perfect sequences are sequences having entries $\{-1,0,1\}$. These sequences are found for longer lengths than 4. We gave an introduction to these sequences in Section 3.1.

Ternary perfect sequences were first studied by Chang [8] with a method of generating ternary sequences derived from a class of M-sequences over $GF(3)$. Chang [8] gives examples of perfect ternary sequences for lengths 13,121 and 1093.

Chang [8] has also established a relation between the numbers of $+1$ and -1 entries of a ternary sequence as follows:

If a ternary sequence $\{x_k\}$ consists of N_{+1} $+1's$; N_{-1} $-1's$ and N_0 $0's$, then a necessary condition for a perfect ternary sequence is given by

$(N_{+1} - N_{-1})^2 = N_{+1} + N_{-1}$ (*Definition 2.3.4*)

Prior to Chang, Tompkins [68] did a "brute force" method to generate codes of lengths up to 18.

Most of the ternary perfect sequences in the literature are constructed using M-sequences and other Linear Feedback Shift Register (LFSR) sequences. Detailed information about all these sequences can be found in [65],[64].

Perfect ternary sequences of lengths:

- $p^n - 1$, p a prime number, are given by Shedd and Sarwate [63].

- $\frac{q^n-1}{q-1}$, are constructed by Ipatov [37], from Linear Feedback Shift Register sequences over $GF(q^n)$, n odd, and $q = p^r$, where p is an odd prime. These sequences form a subclass of Lee sequences[41].
- $\frac{q^{2m+1}-1}{q-1}, q = 2^s$ are constructed using the results from difference set theory, by Hoholdt and Justesen [35].

3.3.3 Frank sequences [18]

Frank constructed perfect sequences of length N which is a perfect square over q^{th} roots of unity where q is a positive integer.

Consider the matrix

$$E = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 2 & \cdots & q-1 \\ 0 & 2 & 4 & \cdots & 2(q-1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & q-1 & 2(q-1) & \cdots & (q-1)^2 \end{bmatrix} \quad (3.3.1)$$

The entries, namely ij, of E are regarded as the exponents of γ, a primitive q^{th} root of unity.

So, any element ij of the matrix can be converted to,

$a_k = \gamma^{ij}, 0 \leq i, j < q.$

The sequence $\mathcal{F} = \{a_0, a_1, \cdots, a_{N-1}\}$, where the entries are the q^{th} roots of unity, obtained by concatenating the rows of E, is called a Frank sequence.

Example 3.3.3

Let us take $q = 2$. Then the matrix (3.3.1) becomes

$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ which is equivalent to $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ when we map $1 \to (-1)^0$ and $-1 \to (-1)^1$.

When the rows of $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ are concatenated, we get $[1,1,1,-1]$, the only known perfect binary sequence. □

Heimiller constructed polyphase codes of length p^2 consisting of sequences over the p^{th} roots of unity where p is a prime number, using the $p \times p$ matrix, given by

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 2 & \cdots & p-1 \\ 0 & 2 & 4 & \cdots & 2(p-1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & (p-1) & 2(p-1) & \cdots & (p-1)^2 \end{pmatrix} \qquad (3.3.2)$$

The sequence generated by concatenating the rows of (3.3.2) is also perfect. This is a special case of (3.3.1), where q is not necessarily prime. Heimiller noted that the order of p sequences (rows/columns of the matrix) from which the final perfect sequence is formed can be changed or any cyclic permutation of each row/column can be substituted without altering the result of perfection.

Frank in [19] claimed that the sequences given by Heimiller [32] were designed 9 years earlier by him, though Frank's paper was published at a later date than Heimiller.

Frank generalized Heimiller's construction by lifting the restriction that p is a prime number. Frank sequences are of length $N = q^2$, where q is any integer not necessarily prime. Heimiller in [33] agreed that this claim is correct and the sequences of this type are called Frank sequences or Frank-Zadoff-Chu sequences.

3.3.4 Modulatable Frank sequences

In 1988, Suheiro and Hatori [66] presented a general class of Frank sequences with perfect periodic autocorrelation functions. The auto and cross correlation properties are preserved under a modulation process. The modulatable sequences are used for information transmission in spread-spectrum communications.

A Frank sequence of length N^2 is taken. This sequence is multiplied by a string of complex numbers $\boldsymbol{b} = [b_0, b_1, \cdots, b_{N-1}]$ with all entries having norm 1.

We take the $N \times N$ Frank matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \xi_1 & {\xi_1}^2 & \cdots & {\xi_1}^{N-1} \\ 1 & \xi_2 & {\xi_2}^2 & \cdots & {\xi_2}^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi_{N-1} & {\xi_{N-1}}^2 & \cdots & {\xi_{N-1}}^{N-1} \end{pmatrix}$$

We post multiply H by the diagonal matrix B, of order N.

$$B = \begin{pmatrix} b_0 & 0 & 0 & \cdots & 0 \\ 0 & b_1 & 0 & \cdots & 0 \\ 0 & 0 & b_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & b_{N-1} \end{pmatrix}$$

The absolute value of each diagonal element ($b_{i,i}$) of B is 1. So we have

$$HB = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \xi_1 & {\xi_1}^2 & \cdots & {\xi_1}^{N-1} \\ 1 & \xi_2 & {\xi_2}^2 & \cdots & {\xi_2}^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi_{N-1} & {\xi_{N-1}}^2 & \cdots & {\xi_{N-1}}^{N-1} \end{pmatrix} \begin{pmatrix} b_0 & 0 & 0 & \cdots & 0 \\ 0 & b_1 & 0 & \cdots & 0 \\ 0 & 0 & b_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & b_{N-1} \end{pmatrix}$$

$$= \begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_{N-1} \\ b_0 & b_1\xi_1 & b_2{\xi_1}^2 & \cdots & b_{N-1}{\xi_1}^{N-1} \\ b_0 & b_1\xi_2 & b_2{\xi_2}^2 & \cdots & b_{N-1}{\xi_2}^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_0 & b_1\xi_{N-1} & b_2{\xi_{N-1}}^2 & \cdots & b_{N-1}{\xi_{N-1}}^{N-1} \end{pmatrix}$$

Then a sequence $\boldsymbol{a} = \{a_0, a_1, \cdots, a_{N^2-1}\}$ is obtained by concatenating the rows of HB.

The sequence $\boldsymbol{a}$ is called the modulated Frank sequence obtained by modulating the original Frank sequence of length N^2 with a string of complex numbers of absolute value 1. These sequences have higher alphabet sizes while Frank sequences are constructed over roots of unity.

3.3.5 Chu's sequences

Chu [9] gives a construction of perfect sequences for lengths without the restriction of the lengths being perfect squares, as in Frank [18] and Heimiller [32].

Here is Chu's construction.

Let $\{a_n\}$ be a sequence of length N with all entries having magnitude 1, defined as follows.

For any integer M relatively prime to N,

$$a_k = \begin{cases} e^{\frac{2\pi i M k^2}{N}}, & N\ even \\ e^{\frac{2\pi i M k(k+1)}{N}}, & N\ odd \end{cases} \quad (3.3.3)$$

Fan and Darnell [13] and Popovic [56] provide a general version of Chu sequences by modifying the sequence $\{a_k\}$. For any integer q, a linear phase shift $e^{\frac{2\pi i M q k}{N}}$ will not alter the perfection of the sequence by Property 1 in Section 3.2.

If

$$b_k = \begin{cases} e^{\frac{2\pi i M(k^2+qk)}{N}}, & N\ even \\ e^{\frac{2\pi i M(k(k+1)+qk)}{N}}, & N\ odd \end{cases} \quad (3.3.4)$$

is the modified Chu-sequence, then the sequence $\{b_k\}$ is also perfect, where $0 \leq k \leq n-1$.

After the publication of [9], Frank again remarked in [17], that the same sequences were found by Zadoff many years before. Hence Chu's sequences are also referred as Zadoff-Chu sequences in papers like [56].

In 1980, Alltop in [1] gave a construction of perfect quadric phase sequences. He also noted that the quadric phase sequences are similar to those of Chu [9].

For an odd integer $N > 2$, Alltop defines the r^{th} quadric phase sequence $\{a_r\}$ as

$$a_r(k) = e^{\frac{2\pi i r k^2}{N}} \quad (3.3.5)$$

When we substitute $M = r$ and $q = -1$ in (3.3.4), for $N\ odd$, and $\gcd(r, N) = 1$, we get

$$a_r(k) = e^{\frac{2\pi i r(k(k+1)-k)}{N}} = e^{\frac{2\pi i r k^2}{N}}$$

3.3.6 Milewski sequences

Milewski [51] constructed a new class of perfect sequences with greater alphabet size than Frank sequences and smaller alphabet size than Chu sequences in his study of channel estimation and fast start-up equalisation.

If $\boldsymbol{a} = [a_0, a_1, \cdots, a_{n-1}]$ is an n-phase Chu sequence, then Milewski defines his sequence $\boldsymbol{c} = [c_0, c_1, \cdots, c_{N-1}]$ of period $N = n^{2k+1}$ as follows:

For $i = 0,1,2, \cdots, L-1;\ L = n^{k+1}$ and $j = 0,1,2, \cdots, M-1;\ M = n^k$

$$c_{ij} = a_{i\ mod n}\omega^{ij}$$

where ω is the $(k+1)^{th}$ root of unity. These sequences are constructed for lengths different from the lengths of other perfect sequences.

If the period of these sequences is made sufficiently long, it leads to a better channel estimate. The transmitted alphabet is known to the receiver which eliminates the detection errors.

3.3.7 Lewis-Kretschmer sequences

Lewis and Kretschmer [42] constructed two classes of polyphase perfect sequences namely $P3$ and $P4$ codes.

For any positive integer $N,\ 0 \leq r < N,\ P3$ and $P4$ codes are defined as follows:

$$P3: \quad a_r = a^{\frac{i\pi r^2}{N}}$$

$$P4: \quad a_r = a^{\left(\frac{i\pi r^2}{N}\right)+\pi r} \qquad (3.3.6)$$

3.3.8 Generalised Chirp-Like sequences (GCL Sequences)

Popovic [56] generalized Chu's construction to obtain a class of perfect sequences called the modulatable Chu sequences or Generalized Chirp-Like sequences.

Let $\boldsymbol{a} = [a_0, a_1, \cdots, a_{N-1}]$ be a Chu sequence of length $N = sm^2$ where s and m are positive integers, and let $\boldsymbol{b} = [b_0, b_1, \cdots, b_{m-1}]$ be any sequence of m arbitrary complex numbers of absolute values 1. The modulatable Chu sequence

$\boldsymbol{s} = [s_0, s_1, \cdots, s_{N-1}]$ is defined as

$$s_k = \begin{cases} b_k e^{\frac{\pi r i}{N} t^2} & if\ N\ is\ even \\ b_k e^{\frac{\pi r i}{N} t(t+1)} & if\ N\ is\ odd \end{cases} \quad 0 \le k \le n-1 \text{ and } gcd(r, N) = 1 \qquad (3.3.7)$$

Popovic has shown that $P4$ codes can be derived from GCL sequences as a special case. Also, the modulatable Chu sequences include modulatable Frank sequences and Milewski sequences as subclasses [56].

3.3.9 Generalised Bent sequences

Kumar and Chung [10] gave a general construction of generalized bent sequences. These sequences have a large linear span (*Definition 2.3.14*) and are used in cryptography, frequency hopping and in spread spectrum multiple access systems.

Definition 3.3.9.1 Let $\boldsymbol{a} = [a_0, a_1, \cdots, a_{n-1}]$ be any sequence over $\mathbb{C}$, the field of complex numbers. Then the Discrete Fourier Transform coefficients are defined as $A_k = \sum_{j=0}^{n-1} a_j e^{\frac{2\pi i}{n} kj}$, $0 \leq k \leq n-1$.

Definition 3.3.9.2 (Chung and Kumar) [10]

Let $\mathbb{Z}_q^m$ denote the set of all m-tuples with elements taken from the set of integers *modulo* q.

Let $\omega_q = e^{\frac{2\pi i}{q}}$.

A (generalized) bent function , $f: \mathbb{Z}_q^m \to \mathbb{Z}_q$, $q \geq 2, m \geq 1$ is a function having the property that all of the (complex) Fourier coefficients $F(\lambda), \lambda \in \mathbb{Z}_q^m$ of ${\omega_q}^{f(.)}$ defined by

$F(\lambda) = \frac{1}{\sqrt{q^m}} \sum_{x \in \mathbb{Z}_q^m} \omega^{f(x) - \lambda^T x}$ for every $\lambda \in \mathbb{Z}_q^m$ and T denotes the transpose,have magnitude one. The integer m is the *dimension* of the bent function.

The special case when $m = 1$ is studied by Mow [52] by generalizing the one dimensional bent functions $f(.)$ as a mapping from $\mathbb{Z}_q \to \mathbb{Z}_q$.

The sequence $[{\omega_q}^{f(0)}, {\omega_q}^{f(1)}, {\omega_q}^{f(2)}, \cdots, {\omega_q}^{f(q-1)}]$ is called a bent sequence and is perfect if $f: \mathbb{Z}_q \to \mathbb{Z}_q$ is a one dimensional bent function[39]. Gabidulin [20] gives a complete description of one dimensional bent sequences.

It is an interesting fact that this class of perfect sequences includes Frank sequences and a subset of Chu sequences as special cases [13].

3.3.10 Gabidulin sequences

Ernst Gabidulin, a Russian Mathematician, has devised a construction for two types of perfect sequences over roots of unity.

Type 1 Let p be an odd prime and l any positive integer. The first type of sequences are of length p^{2l}.

Any integer $s, 0 \leq s \leq p^{2l} - 1$ can be uniquely represented as

$$s = up^l + v \,, \tag{3.3.9}$$

by the Euclidean division algorithm, where $0 \leq u \leq p^l - 1$ and $0 \leq v \leq p^l - 1$.

Let ω_{p^l} denote the primitive root of unity of degree p^l. A perfect sequence $\boldsymbol{g} = [g_0, g_1, \cdots, g_{p^{2l}-1}]$ is defined as

$$g_s = z_v(\omega_{p^l})^{ruv} \tag{3.3.10}$$

where $0 \leq s \leq p^{2l} - 1$ and r is any integer such that $gcd(r, p) = 1$.
The z_v's are arbitrary complex numbers having magnitude 1, and u and v given by Equation 3.3.9.

Gabidulin noted that if the $z_v's$ are equal to 1 for all v, then this type of sequence becomes a special case of the well known Frank sequences.

Type 2

These sequences are of length $p^{2l}+1$ where p is an odd prime and l any positive integer.

Any integer, $0 \le s \le p^{2l+1}-1$ can be uniquely represented as

$s = up^{l+1} + vp^l + c$ where $0 \le u \le p^l - 1$ and $0 \le v \le p^l - 1$ and $0 \le c \le p^l$.

Let $\omega_{p^{2l}}, \omega_{p^l}$ denote primitive roots of unity of degree $p^{2l}$and p^l respectively. Take any perfect sequence $\boldsymbol{x} = [x_0, x_1, \cdots, x_{p-1}]$ of length p. Then the Type 2 Gabidulin sequence $\boldsymbol{a} = [a_0, a_1, \cdots, a_{p^{2l+1}-1}]$ is defined as

$a_s = x_v(\omega_{p^{l+1}})^{cu}(\omega_{p^l})^{cv}$ where $0 \le s \le p^{2l+1}-1$.

If we choose $\boldsymbol{x} = [x_0, x_1, \cdots, x_{p-1}]$ to be a Chu sequence of length p, then the *Type 2* Gabidulin sequences are equivalent to Milewski [51] sequences .

3.3.11 Mow's unified construction

Mow [52] in his thesis has shown that all classes of perfect roots of unity (polyphase) sequences can be deduced from his unified construction.

Mow's general construction is stated below.

Let $\omega_n = e^{\frac{2\pi i}{n}}$ and

- $s, m \in \mathbb{Z}^+$.
- r_0 any integer co-prime to s.

- n_0 is an arbitrary integer in $\mathbb{Z}_s$ such that $(s+1)n_0$ is even and $r_0 + n_0 \frac{l(l+1)}{2}$ is co-prime to s for all $l \in \{0,1,2,\cdots,m-1\}$.
- $0 \leq k \leq sm-1$.
- r_1 any integer in $\mathbb{Z}_{sm}$ co-prime to m.
- n_1 any integer in $\mathbb{Z}_{sm}$ and π is an arbitrary permutation of the elements in $\mathbb{Z}_m$ and for all $0 \leq l \leq m-1, f(l)$ is a rational valued function.
- the function $f(x)$ is defined by

$$f(km+l) = \frac{m^2(s+1)}{2}\left(r_0 + n_0\frac{l(l+1)}{2}\right)k^2 + m(r_1\pi(l)+n_1)k + f(l).$$

Then the polyphase sequence of length $L = sm^2$ defined by

$[{\omega_n}^{f(0)}, {\omega_n}^{f(1)}, {\omega_n}^{f(2)}, \cdots, {\omega_n}^{f(n-1)}]$ is perfect.

Mow has classified his construction into all known classes of perfect sequences by assigning specific values for s, r_0, n_0, r_1 *and* n_1.

3.3.12 Multi-level perfect sequences over $\mathbb{R}$

- Two-level binary sequences

Luke [47] modified binary M-sequences into two-level *amplitude-asymmetrical* binary sequences by substituting a suitable q for -1 in the M-sequence. This q is calculated using the balance property of an M-sequence. Thus

$$q = \frac{-1}{\left(1 + \frac{2}{\sqrt{(N+1)}}\right)}$$

Example 3.3.12.1[44]

Consider the binary M-sequence $(1,1,1,-1,1,-1,-1)$ of length 7. When -1 is substituted by -0.586, the resulting two-level sequence is perfect.

- Three level modified Legendre sequences

Luke constructed ternary perfect sequences from three level Legendre sequences of lengths $N \equiv 1 \; mod \; 4$, by replacing -1 and 0 in the original Legendre sequence by suitable constants [44].

The definition of a Legendre sequence is given below.

Definition 3.3.12.1

A three-level Legendre sequence $\boldsymbol{u} = [u_0, u_1, \cdots, u_{p-1}]$ is defined as follows:

For $0 \leq k \leq p-1$,

$$u_k = \begin{cases} 0 & if \; k = 0 \\ 1 & if \; k \; is \; a \; quadratic \; residue \; mod \; p \\ -1 & if \; k \; is \; a \; quadratic \; non-residue \; mod \; p \end{cases}$$

Example 3.3.12.2

The Legendre Sequence of length 7 is $\boldsymbol{u} = [0,1,1,-1,1,-1,-1]$ where positions 1,2,4 are quadratic residues mod 7 and positions 3,5,6 are quadratic non-residues mod 7. These sequences have off-peak autocorrelation values of -1.

Example 3.3.12.3 (Luke [44], Table I) The sequence given below is a Legendre sequence of length 17 that is modified by substituting -1 by -0.61 and 0 by 0.2, and is three-level perfect.

$[1,1,-0.61,1,-0.61,-0.61,-0.61,1,1,,,-0.61,-0.61,-0.61,1,-0.61,1,1,0.2]$

3.3.13 Three level perfect sequences over $\mathbb{R}$

Bomer and Antweiler [4] gave a new class of three-level perfect sequences over the set of real numbers, derived from M-sequences of length $N = q^m - 1$, with the elements from $GF(q)$ where q is any prime power. Let $\boldsymbol{a} = [a_0, a_1 \cdots a_{N-1}]$ be an M-sequence of length N, over $GF(q)$. A new three-level sequence $\boldsymbol{b} = [b_0, b_1 \cdots b_{N-1}]$ is formed by the following mapping.

For $0 \leq i \leq N-1$, define

$$b_i = \begin{cases} 1, & if\ a_i = 0 \\ x_1, & if\ a_i = 1 \\ x_2, & otherwise \end{cases}$$

The sequence $\boldsymbol{b}$ is perfect if $x_1 = -\frac{c_2 + (q-3)x_2^2}{2x_2}$ and x_2 is a real root of the equation

$(4(q-2) + (q-3)^2)x_2^4 + 4(q-1)x_2^3 + \big(4c_1 - 2c_2(q-1)\big)x_2^2 - 4c_2x_2 + c_2^2 = 0$, where

$c_1 = \frac{q^{m-2}-1}{q^{m-2}}$ and $c_2 = \frac{q^{m-1}-1}{q^{m-1}}$.

3.3.14 Three-level perfect sequences over $\mathbb{C}$

Bomer and Antweiler[4] again give a construction for three-level perfect sequences of length $N = 3^m - 1$, where m is any positive integer, by mapping the entries of an M-sequence over $GF(3)$ to three different complex values. Let $\boldsymbol{a} = [a_0, a_1 \cdots a_{N-1}]$ be an M-sequence over $GF(3)$. A new three-level sequence with complex entries, $\boldsymbol{b} = [b_0, b_1 \cdots b_{N-1}]$ is formed by the following mapping:

$$b_i = \begin{cases} 1 & if\ a_i = 0 \\ x_1 & if\ a_i = 1;\ \ 0 \le i \le N-1 \\ x_2 & otherwise \end{cases}$$

where, $x_1 = e^{i\beta_1}$, $x_2 = e^{i\beta_2}$ with $\beta_1 = \beta_2 \pm \cos^{-1} c$, $\beta_2 = \pm \cos^{-1}\left(c\sqrt{\frac{2}{1+c}}\right) \pm \frac{1}{2}\cos^{-1} c$ and $c = \frac{1-3^{m-1}}{2.3^{m-1}}$. As the lengths increase, the phase values of x_1 and x_2 tend to $\frac{2\pi}{3}$ and $\frac{4\pi}{3}$.

3.3.15 Fan and Darnell construction

This construction [12] is a special case of Wolfmann's [73] construction that employs M-sequences over rational numbers and Gaussian integers (Complex numbers of the form $a + ib$ where a, b are integers).

The construction of quasi-perfect sequences by Fan and Darnell is given below.

- Quasi-perfect multi-level sequences over $\mathbb{R}$ [12]

An M-sequence $\boldsymbol{u} = [u_0, u_1, \cdots, u_{N-1}]$ over $GF(p)$, p a prime number, of length $N = p^m - 1$ is concatenated with its inverse (*Inverse repeat format*) to form a sequence $\boldsymbol{a} = \{a_j\}_{0 \le j \le 2N-1}$ of length $L = 2N$ with quasi-perfect (almost perfect) autocorrelation functions of the form:

$$\Theta_{\boldsymbol{a}}(\tau) = \begin{cases} P, & \tau = 0 \\ -P, & \tau = N \\ 0, & otherwise \end{cases}$$

When this quasi-perfect sequence $\boldsymbol{a}$ is combined with a sequence $\boldsymbol{b} = \{(-1)^j\}$, $0 \le j \le 2N-1$, using digit-by-digit multiplication, another sequence

$\boldsymbol{c} = [c_0, c_1, \cdots, c_{2N-1}]$ is formed which is p-valued and multi-level. Half of this sequence $\boldsymbol{c}$ is taken and is perfect.

Example 3.3.15.1 [8] Here is an example of a sequence of length 13, by taking $p^m - 1 = 26 = 2 \times 13$ where $p = 3, m = 3$.

The sequence $\boldsymbol{c} = [0, -1, 1, -1, 0, 0, -1, 0, -1, -1, -1, 1, 1]$ in this instance is a ternary perfect sequence of length 13.

The balance determines the number of $+1$'s and -1's.

Multi-level sequences can be constructed by this method by assuming different values for p. The positions of 0's in this type of sequences from a difference set. For each shift, the matches of zeros are equally numerous.

a) Multi-level perfect sequences over $\mathbb{C}$

A similar technique to the above construction is employed to construct multi-level sequences of length $L = 4N$.

Two component quasi-perfect sequences $\boldsymbol{a} = \{a_j\}$ of period, $L = 4N$, N, an odd number and $\boldsymbol{b} = \{(i)^j\}$ of period 4 are combined using digit-by-digit multiplication; the resulting sequence is perfect with period N.

Example 3.3.15.2

Here is an example of a Lee [41] sequence given by Fan and Darnell [12] by taking $L = 5^3 - 1 = 4 \times 31$. The 5-level perfect sequence of length 31 thus obtained is

$\boldsymbol{c} = [0, 0, -1, -1, i, 1, i, -i, 1, 1, -1, 1, 1, 1, i, 0, -1, -i, 1, -i, 0, i, 0, i, 1, -1, i, i, 0, 1, -1]$.

3.4 Non-existence of perfect sequences

i. *Binary Sequences*

There exists a one to one correspondence between binary sequences with two-level autocorrelation and cyclic difference sets in $\mathbb{Z}_n$ [15].

Definition 3.4.1 Let G be a group (written additively), of order v, and D be a k-element subset of G. Then D is called a (v, k, λ)-difference set if its list of differences, that is $\Delta D = \{d - d' : d, d' \in D, d \neq d'\}$, contains each non-zero element of G precisely λ times. If G is cyclic, D is also called cyclic $mod\ v$.

Example 3.4.1 [58]

$D = \{1,2,4\}$ is a (7,3,1)-difference set in the cyclic group $\mathbb{Z}_7$.

If D is a (v, k, λ)-difference set in $\mathbb{Z}_n$, then we can construct a binary sequence

$\boldsymbol{a} = [a_0, a_1, \cdots, a_{n-1}]$ by the following mapping:

$$a_j = \begin{cases} 1 & if\ j \in D \\ -1 & if\ j \notin D \end{cases},\ 0 \leq j \leq n-1.$$

If the number of entries 1 per period is k, then all the non-trivial autocorrelation values ϱ of $\boldsymbol{a}$ of period v is given by, $\varrho = v - 4(k - \lambda)$. The proof of this can be found in [58]. When $\varrho = 0$, then $\boldsymbol{a}$ is perfect.

For $\varrho = 0$, the period v of a sequence has to be $v = 4u^2$. Then the (v, k, λ)-difference set can be rewritten as a $(4u^2, 2u^2 - u, u^2 - u)$-difference set. Difference sets of this type are called *Hadamard difference sets.* The only cyclic

example of such a difference set is the trivial (4,1,0)-difference set which corresponds to the binary sequence $[1,1,1,-1]$ of length 4.

Conjecture 3.4.1 [52] No perfect binary sequence of length other than 4 exists.

A one to one correspondence between a perfect binary sequence and a circulant Hadamard matrix (*Definition 3.3.1*) is established in Baumert [2]. The following conjecture is equivalent to the *Conjecture 3.4.1*.

Conjecture 3.4.2 [52] There is no circulant Hadamard matrix of order other than 1 and 4.

It is widely conjectured that no other non-trivial, cyclic Hadamard difference sets exist. Despite many attempts to prove the non-existence results on difference sets, this *circulant Hadamard matrix conjecture* (*Conjecture 3.4.2*) still remains unsolved.

If any perfect binary sequence exists further, it must be of length $4u^2 > 4$ for some positive integer u, which is equivalent to a $(4u^2, 2u^2 - u, u^2 - u)$ cyclic difference set (*Definition 3.4.1*)[2]. Turyn in [70] and [71] has proved that the result $4u^2 > 4$ implies u is odd and $u \geq 55$. Based on the results by Schmidt [60], Jungnickel and Pott [58] have stated that cyclic Hadamard difference sets of order $1 < u \leq 10{,}000$ do not exist. This implies that no perfect binary sequences of length N exist for $4 < N \leq 12{,}100$.

ii. *Perfect polyphase sequences*

When we consider the different known constructions of perfect sequences in Section 3.3, we observe in [9, 51, 66] that the alphabet size increases with the length of a perfect sequence.

Mow's conjecture below gives a relationship between the length of a perfect polyphase sequence and the minimum alphabet size.

Conjecture 3.4.3 (Mow [52]) Let $L = sm^2$, for $s, m \in \mathbb{Z}^+$ and s is square free. The phase alphabet size of the perfect polyphase sequences of length L must be hN, where h is any positive integer, and N is the minimum phase alphabet size given by

$$N = \begin{cases} 2sm & for\ even\ s\ and\ odd\ m \\ sm & otherwise \end{cases}$$

The above conjecture implies that there exists no perfect sequence over n^{th} roots of unity of length above n^2.

iii. *Ma and Ng's non-existence results of p-ary polyphase sequences*

Using the results from difference sets, Ma and Ng [48] prove that if p is an odd prime.

There are no p-ary polyphase perfect sequences of length:

- p^s for $s \geq 3$,
- $2p^s$ for $s \geq 1$ and
- pq for prime $q > p$.

They have also proved that there are no ternary perfect sequences of length

$3q_1q_2$, where $3 < q_1 < q_2$.

iv. *Non-Existence of Almost p-ary perfect sequences*

Definition 3.4.3 A sequence over p^{th} roots of unity with a single zero also as one of the entries is called an Almost p-ary sequence.

In Section 3 of the paper by Chee *et. al* [74], it is proved that almost p-ary perfect sequences do not exist for certain periods. In Table 2 in Appendix [74], they have listed the existence of almost p-ary perfect sequences of period $n+1$ for $3 \leq n \leq 100$ and p is a prime divisor of $(n-1)$.

Note: Luke in [46] has proved that there exists no perfect *almost binary seque*nce of length $n+1$ for $n > 1$(Appendix VI in [46]) .

3.5 Almost perfect sequences

Since perfect sequences, over roots of unity, exist only for perfect square or multiple of perfect square lengths, the recent literature discusses the construction of Almost perfect sequences.

Almost perfect sequences by Wolfmann [73] and another definition by Luke [45] were introduced in Chapter 1. A detailed mathematical treatment for constructing these sequences can be found in [40].

Let us examine these sequences in detail below.

Definition 3.5.1 *Almost perfect sequences* [73]

Almost perfect sequences are complex periodic sequences such that all the off-peak autocorrelation values are zero except one.

Definition 3.5.2 *D-perfect sequences* [73]

Let D be an integer and $D \geq 1$. A complex periodic sequence $\boldsymbol{S}$ is said to be a D-perfect autocorrelation sequence if $\Theta_s(\tau) = 0$ for $\tau = 1,2,\cdots,D$.

Wolfmann defines almost perfect sequences as a special case of D-perfect sequences.

Wolfmann [73] uses the following theory to construct D-perfect sequences with lengths, a multiple of 4. D-perfect sequences can also be called zero correlation zone sequences (*Definition 2.3.17*).

Wolfmann considers only $\{+1,-1\}$ sequences.

There are many practical applications, where a binary sequence is actually transmitted as a sequence of positive and negative entries with modulus 1. Some applications such as coded aperture astronomy require $\{0,1\}$ sequences.

Description of Binary sequences

Let $\tilde{x} = (x_0, x_1, \cdots, x_{n-1})$ and $\tilde{y} = (y_0, y_1, \cdots, y_{n-1})$ be two $(-1,+1)$ vectors. If $+1$ is replaced by 0 and -1 by 1 by means of $(-1)^c \to c$ then $\tilde{x}$ and $\tilde{y}$ are transformed into the binary vectors $\tilde{a} = (a_0, a_1, \cdots, a_{n-1})$ and $\tilde{b} = (b_0, b_1, \cdots, b_{n-1})$.

Hence the inner product of $\tilde{x}$ and $\tilde{y}$ is $c = n - 2d(\tilde{a}, \tilde{b})$, where $d(\tilde{a}, \tilde{b})$ is the Hamming distance (*Definition 2.3.7*) between $\tilde{a}$ and $\tilde{b}$.

If $\tilde{g} = (g_0, g_1, \cdots, g_{n-1})$ is the binary vector of a sequence $\boldsymbol{g}$, then its autocorrelation is

$\Theta_{\boldsymbol{g}}(i) = n - 2d(\tilde{g}, \tilde{g}(i))$, where $g(i) = (g_{n-i}, g_0, \cdots, g_{n-i+1})$. We note that $\Theta_{\boldsymbol{g}}(i)$ is zero only if n is even and $d(\tilde{g}, \tilde{g}(i))$ is $\frac{n}{2}$.

Definition 3.5.3 Let $\tilde{g} = (g_0, g_1, \cdots, g_{n-1})$ be the generator vector of a binary sequence $\boldsymbol{g}$. The polynomial $g(x) = g_0 + g_1 x + \cdots + g_{n-1}x^{n-1}$, of period n, is the polynomial representation of its generator vector and is called the generator polynomial.

Remark

If $g(x)$ is the generator polynomial of a binary sequence $\boldsymbol{g}$ of period n, then

a) The autocorrelation $\Theta_{\boldsymbol{g}}(i)$ is equal to $n - 2w(m_i(x))$ where $m_i(x) = (x^i + 1)g(x)$ and w is the Hamming weight (*Definition 2.3.8*) of the polynomial $m_i(x)$.

b) A sequence $\boldsymbol{g}$ is D-perfect if and only if $w(m_i(x)) = \frac{n}{2}$ and $i = 1,2, \cdots D$.

Proposition 3.5.1[73]

If there exists a D-perfect autocorrelation sequence of period n, then n is a multiple of 4.

Proof:

Let $\boldsymbol{g}$ be a D-perfect autocorrelation sequence. So we know,

$\Theta_{\boldsymbol{g}}(i) = n - 2w(m_i(x)) = 0$ for $i = 1,2, \cdots D$.

Let $i = 1$. Then $m_1(x) = (x+1)g(x)$ (3.5.1)

For shift 1, $\boldsymbol{g}$ has autocorrelation value zero, according to the definition of a D-perfect sequence.

That is, $n - 2w\big(m_1(x)\big) = 0$.

So, $w\big(m_1(x)\big) = \frac{n}{2}$

That is, $w\big((x+1)g(x)\big) = \frac{n}{2}$

Putting $x = 1$ in Equation 3.5.1, we get,

$m_1(1) = 2g(1) = 0$. This implies the number of ones in $m_1(x)$ is even.

Let $w\big(m_1(x)\big) = 2k$.

Then, $n = 2 \times 2k = 4k$.

Thus, n is a multiple of 4. ■

If a binary sequence $\boldsymbol{a}$ is D-perfect with $D = \frac{n}{2}$, then $\boldsymbol{a}$ is perfect. We know that a binary perfect sequence of length n is equivalent to circulant Hadamard matrix of order n and there is no circulant Hadamard matrix of order n if $4 < n \leq 12100$ [2]. Thus Wolfmann considers the optimal case of $D = \frac{n}{2} - 1$ in that range.

We observe that the periods of almost perfect sequences constructed by Wolfmann are multiples of four; the shortest being 8. Wolfmann did an exhaustive computer search to find binary almost perfect sequences up to the length $n = 100$ (Table 1 Wolfmann[73]) .

Example 3.5.1 Binary almost perfect sequence of length 8

The binary almost perfect sequence of length 8 is [1,1,0,1,0,0,0,0] with periodic autocorrelation values 8 for zero shift and -4 for shift $\tau = 4$, and zero for all the other shifts.

Wolfmann [73] reported that his search did not yield almost perfect binary sequences of lengths $n = 32, 44, 68, 72, 80, 92$.

While Wolfmann[73] constructed binary almost perfect sequences, there was a question whether other sequences exist that have similar properties and for higher alphabet sizes. As a result, Luke [45] in 1996 introduced almost (near) perfect sequences over small phase alphabet. We shall examine these sequences in the next Section.

3.6 Luke's construction

Luke modified Wolfmann's definition of almost perfect sequences by allowing more non-zero off peak autocorrelation values. He has also considered non-binary cases for small size alphabets.

Luke defines (almost) near perfect sequences as below:

Definition 3.6.1[45]

Sequence $\boldsymbol{G}$ over the m^{th} roots of unity and of length N, where m divides N, is said to be *Near perfect* if it possesses Periodic Auto Correlation Function (PACF) which satisfies $\Theta_{\boldsymbol{G}}(\tau) = 0$ for $\tau \not\equiv 0 \ mod \left(\frac{N}{m}\right)$.

Luke derives these sequences from q-ary M-sequences by a k-valued character operation as defined below.

Definition 3.6.2 *Multiplicative character* [43]

Let G be a finite abelian group (written multiplicatively) of order $|G|$ with identity element 1_G. A character χ of G is a homomorphism from G into the multiplicative group U of complex numbers of absolute value 1, that is, a mapping from G to U with $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in G$.

Let G be a finite cyclic group of order n, and let g be a generator of G.

For a fixed integer j, $0 \leq j \leq n-1$, the function $\chi_j(g^k) = e^{\frac{2\pi ijk}{n}}, k = 0,1,\cdots,n-1$,

defines a character of G. If χ is any character of G, then $\chi(g)$ must be an n^{th} root of unity.

That is, $\chi(g) = e^{\frac{2\pi ij}{n}}$ for some $j, 0 \leq j \leq n-1$.

We now give a general definition of the trace function.

Definition 3.6.3 [49]

Let $GF(p^{m_2})$ be the field with p^{m_2} elements and x be a primitive element of $GF(p^{m_2})$.

The trace function $Tr_{m_1}^{m_2}: GF(p^{m_2}) \rightarrow GF(p^{m_1})$, m_1 divides m_2, is defined as

$Tr_{m_1}^{m_2}(x) = \sum_{i=0}^{\frac{m_2}{m_1}} x^{p^{m_1 i}} = x^{p^{m_1}} + x^{p^{2m_1}} + \cdots$, where $GF(p^{m_1})$ is proper subfield of $GF(p^{m_2})$.

The trace function thus defined has the following mathematical properties [49].

When $x \in GF(p^{m_2})$,

1) $Tr_{m_1}^{m_2}(x)$ has values in $GF(p^{m_1})$
2) $Tr_{m_1}^{m_2}\left(x^{(p^{m_1})^i}\right) = Tr_{m_1}^{m_2}(x)$, for all i. That is, conjugate field elements (*Definition 2.1.7*) have equal trace.
3) $Tr_{m_1}^{m_2}(ax + by) = aTr_{m_1}^{m_2}(x) + bTr_{m_1}^{m_2}(y)$ for all $a, b \in GF(p^{m_1})$ and $x, y \in GF(p^{m_2})$.
4) There are $p^{m_2 - m_1}$ elements in $GF(p^{m_2})$ which have trace value a for each $a \in GF(p^{m_1})$.
5) If $GF(p^{m_1}) \subset GF(p^{m_2}) \subset GF(p^{m_3})$, then

   $Tr_{m_1}^{m_3}(x) = Tr_{m_1}^{m_2}\left(Tr_{m_2}^{m_3}(x)\right)$.

3.6.1 Luke's method of construction

A q-ary M-sequence of degree 2 is constructed using the Trace function (*Definition 3.6.3*).

Example 3.6.1.1

Construction of $GF(3^2)$ from $GF(3)$ and a 3-ary M-sequence of degree 2.

We take the primitive polynomial $f(x) = x^2 + x + 2$ (Fig.18, [49])

Let α be a primitive element of $GF(3^2)$. The table below shows the powers of α and the respective pseudo polynomials [62].

Powers of α	Pseudo polynomials
0	0
1	1
α	α
α^2	$2\alpha + 1$
α^3	$2\alpha + 2$
α^4	2
α^5	2α
α^6	$\alpha + 2$
α^7	$\alpha + 1$

Table 3.6.1

Hence $GF(3^2) = \{0,1,\alpha, 2\alpha + 1, 2\alpha + 2, 2, 2\alpha, \alpha + 2, \alpha + 1\}$.

We know from Property 2 of the trace function that the conjugate field elements $\left\{1, p^{m_1}, p^{(m_1)^2}, \cdots, p^{(m_1)^{m_2-1}}\right\}$ have equal trace. The conjugate elements are grouped into one class, called a conjugacy class.

The conjugacy classes and the trace calculation for $GF(3^2)^*$ are given below.

Conjugacy classes	Trace
$[\alpha,\alpha^3]$	$\alpha+\alpha^3 = 2$
$[\alpha^2, \alpha^6]$	$\alpha^2 + \alpha^6 = 0$
$[\alpha^4, \alpha^4]$	$\alpha^4 + \alpha^4 = 1$
$[\alpha^5, \alpha^7]$	$\alpha^5 + \alpha^7 = 1$
[1,1]	1+1=2

Table 3.6.2

Thus, a 3-ary M-sequence over $GF(3)$ is [2,2,0,2,1,1,0,1].

Let $\boldsymbol{c} = \{c_i\},\ 0 \le i \le q^2 - 1$ denote an M-sequence defined by

$c_i = Tr_J^{2J}(\alpha^i)$, where $q = p^J$, p an odd prime, $J = 1,2,3,\cdots$, and α is a primitive element of $GF(q^2)$.

The M-sequences thus constructed are of lengths $M = q^2 - 1$. Each M-sequence is segmented into $q - 1$ subsequences of length $T = q + 1$. The entries of each sequence are elements of the Galois field $GF(q)$ and are represented as the powers of a primitive element γ of $GF(q)$.

That is, $c_i = \gamma^i$ where $i = -\infty, 0,1,2,\cdots, q-2$. So $\boldsymbol{c} = \{c_i\}$, contains the powers of γ.

The element zero is represented as $\gamma^{-\infty}$. Each subsequence of an M-sequence of degree two contains the element zero exactly once.

Another sequence $\{c_i^{'}\}$ is formed by listing the index of the primitive element γ of $GF(q)$ corresponding to each c_i.

The k-valued multiplicative character χ_k which satisfies the condition $q \equiv 1 \, mod \, k$ is used to construct a sequence $\boldsymbol{s} = \{s_i\} \quad i = 0,1,2,\cdots, kT-1$ over k^{th} roots of unity.

The k-valued multiplicative character χ_k on all non-zero elements γ^j of $GF(q)$ is

$\chi_k(\gamma^j) = e^{\frac{2\pi ij}{k}}$.

Properties of χ_k

i. $\chi_k(x \cdot y) = \chi_k(x) \cdot \chi_k(y)$

ii. $\sum_{j=0}^{q-2} \chi_k(\gamma^j) = 0$

This k-valued multiplicative character is used to construct the sequence $\boldsymbol{s}$, with alphabet size k, where the elements of $\boldsymbol{s}$ are given by the mapping,

$$s_i = \begin{cases} \chi_k(c_i) & for \; c_i \neq 0 \\ 1 & for \; c_i = 0 \end{cases}$$

where $i = 0,1,2,\cdots, kT-1$.

The period of the sequence thus generated will be $N = kT = k(q+1)$. The sequence is near perfect and this is proved in [45].

The near perfect sequence $\{s_i\}$ constructed in this way, can be written as

$s_i = e^{\frac{2\pi i}{k}\delta_i}$, where

$$\delta_i = \begin{cases} c_i{}' \bmod \gamma \quad for\ c_i \neq 0 \\ 0 \qquad\qquad for\ c_i = 0 \end{cases} \tag{3.6.1}$$

Luke has represented entries of his near perfect sequences by the indices, δ_i. This does not alter the calculation of the autocorrelation values.

This type of construction was first introduced by Lee in 1992 [41] followed by Luke in 1997 [45].

Example 3.6.1.2 [45]

Take $q = p^1 = 7$. The length of degree 2 M-sequence is $7^2 - 1 = 48$ and the M-sequence is

$\mathbb{M} = [0,2,5,3,3,2,3,5,0,6,1,2,2,6,2,1,0,4,3,6,6,4,6,3,0,5,2,4,4,5,4,2,0,1,6,5,5,$

$1,5,6,0,3,4,1,1,3,1,4\ ]$.

This sequence can be segmented into 6 subsequences of length $T = 8$. The alphabet sizes $k = 2,3,6$ satisfy the condition $7 \equiv 1\ (mod\ k)$.

A ternary near perfect sequence of length $N = 3 \times 8 = 24$ is constructed by taking 3 consecutive sub-sequences of $\mathbb{M}$,

$\{c_i\} = \{0,4,3,6,6,4,6,3;\ 0,5,2,4,4,5,4,2;\ 0,1,6,5,5,1,5,6\}$

We take a primitive element $\gamma = 3$, of $GF(7)$.

The sequence $\{c_i{}'\}$ is formed by listing the exponents of γ corresponding to each element in $\{c_i\}$. The element 0 is usually represented as $\gamma^{-\infty}$.

So we have, $\{c_i{}'\} = \{-\infty,4,1,3,3,4,3,1; -\infty,5,2,4,4,5,4,2; -\infty,0,3,5,5,0,5,3\}$ which are the exponents of 3 corresponding to each element in $\{c_i\}$.

According to the definition of δ_i from Equation 3.6.1,

$$\delta_i = \begin{cases} c_i{}' mod\ 3 & for\ c_i \neq 0 \\ 0 & for\ c_i = 0 \end{cases}$$

and so, $\{\delta_i\} = (0,1,1,0,0,1,0,1,0,2,2,1,1,2,1,2,0,0,0,2,2,0,2,0)$.

The periodic autocorrelation function is near perfect (Luke) with $k = 3$ and its magnitude is given by

$$|\Theta_s(\tau)| = (24,0,0,0,0,0,0,0.19.67,0,0,0,0,0,0,0,19.67,0,0,0,0,0,0,0).$$

Example 3.6.1.3[45]

The shortest near perfect binary sequence obtained using Luke's method is given.

Choose $q = 3$.

An M-sequence of length 8 over $GF(3)$ is $\{c_i\} = (1,0,1,1,2,0,2,2)$

Taking the powers of the primitive element 2, of $GF(3)$, we get

$\{c_i{}'\} = (0, -\infty, 0,0,1, -\infty, 1,1)$

$$\delta_i = \begin{cases} c_i{}' mod\ 2 & for\ c_i \neq 0 \\ 0 & for\ c_i = 0 \end{cases}$$

giving $\{\delta_i\} = (0,0,0,0,1,0,1,1)$.

Observation: This sequence is a binary almost perfect sequence with peak autocorrelation value 8 and non-zero off peak autocorrelation value -4. This is the shortest binary almost perfect sequence given in the table of sequences in [73].

The table below describes the near perfect sequences of length N with alphabet size $k = 3, 4$ given by Luke [45] up to the length 200.

N	24	24	40	42	56	60	72	78	96	104	114	120	132	150	152	168	186	200
q	7	5	9	13	13	19	17	25	31	25	37	29	43	49	37	41	61	49
k	3	4	4	3	4	3	4	3	3	4	3	4	3	3	4	4	3	4

Table 3.6.3 [45]

3.7 Shift sequence (Games)[21]

In this Section we introduce the row-wise folding of an M-sequence constructed using the trace mapping from an extension field $GF(p^{2J})$ to its base field $GF(p)$ to obtain a shift sequence associated with the primitive polynomial $f(x)$ of degree $2J$ over $GF(p)$. We use this type of shift sequences in our construction of near perfect sequences in Section 4.3.

An M-sequence $\boldsymbol{u} = (u_0, u_1, u_2, \cdots, u_{2^J-2})$ of span J (*Definition 2.3.14*) is generated by the trace function $Tr_1^J(\beta^i)$ where $u_i = Tr_1^J(\beta^i)$ where β is a primitive element of (2^J), $\beta = \alpha^n$ and $n = \frac{2^{2J}-1}{2^J-1}$.

Definition 3.7.1[21]

Let $GF(p^{2J})$ be the field with p^{2J} elements and α be a primitive element of $GF(p^{2J})$. We assume that $GF(p^{2J})$ is constructed from a primitive polynomial $f(x)$ of degree $2J$ over $GF(p)$.

For $i \in \mathbb{Z}_{p^{2J}-1,}$ define a sequence $\boldsymbol{e}$ by

$$e_i = \begin{cases} \infty & if\ Tr_J^{2J}(\alpha^i) = 0 \\ e & if\ Tr_J^{2J}(\alpha^i) \neq 0,\ Tr_J^{2J}(\alpha^i) = \beta^e \end{cases} \quad (3.7.1)$$

The resulting sequence is $\boldsymbol{e} = (e_0, e_1, e_2, \cdots, e_{2^{2J}-2})$. This is called the shift sequence associated with the primitive polynomial $f(x)$ [21].

Note: This is a specific shift sequence which maps $GF(p^{2J})$ to $GF(p)$. A general shift sequence can be defined from any extension field to a proper subfield. Another method of folding M-sequences into $\mathbb{p} \times \mathbb{q}$ arrays where $\mathbb{p}$ and $\mathbb{q}$ are co-prime is demonstrated in [7, 28, 49, 72]. This type of folding yields shift sequences with one or more ∞. These shift sequences are periodic where as Games's shift sequences are not. We shall see this type of decomposition in detail in Section 4.11.

Now let us examine how we obtain the shift sequence $\boldsymbol{e}$, by folding an M-sequence row-wise.

Take an M-sequence of span $2J$ generated by the trace function Tr_J^{2J}. Let

$\boldsymbol{t} = (t_0, t_1, t_2, \cdots, t_{2^{2J}-2})$ be the sequence of period $2^{2J} - 1$ defined by

$t_i = Tr_1^{2J}(\alpha^i), i \in \mathbb{Z}_{2^{2J}-1}$.

The results based on difference sets in [2, 26] show that since $J\ divides\ 2J$, the M-sequence of span J can be associated with $\boldsymbol{t}$.

If the terms of $\boldsymbol{t}$ are arranged in a $(2^J - 1) \times n$ array say $\mathbb{P}(\boldsymbol{t})$, where $n = (2^J + 1)$,

then $\mathbb{P}(\boldsymbol{t})$ has the (i, j) entry,

$\mathbb{P}(\boldsymbol{t})(i,j) = t_{in+j}, i \in \mathbb{Z}_{2^J-1}; j \in \mathbb{Z}_n$ (3.7.2)

The columns of $\mathbb{P}(\boldsymbol{t})$ are shifts $E^{\sigma}(\boldsymbol{u})$ of the sequence $\boldsymbol{u}$. Here E is the shift operator (*Definition 2.3.5*).

Example:

$(Eu)_i = u_{i+1}, i \in \mathbb{Z}_{2^J-1}$.

Recall from Equation 3.7.2,

$\mathbb{P}(\boldsymbol{t})(i,j) = t_{in+j} = Tr\left(\alpha^{in+j}\right), n = (2^J + 1)$

$= Tr_1^J(Tr_J^{2J}\left(\beta^i.\alpha^j\right)$

$= Tr_1^J(\beta^i\, Tr_J^{2J}\left(\alpha^j\right))$

If $Tr_J^{2J}\left(\alpha^j\right) = 0$, that is, $e_j = \infty$, then $\mathbb{P}(\boldsymbol{t})(i,j) = 0$ for $i \in \mathbb{Z}_{2^J-1}$ and the j^{th} column of $\mathbb{P}(\boldsymbol{t})$ is identically zero since $Tr_1^J\left(\beta^i.0\right) = 0$, for all i.

Otherwise,

$Tr_J^{2J}\left(\alpha^j\right) = \beta^{e_j}$ and

$\mathbb{P}(\boldsymbol{t})(i,j) = Tr_1^J\left(\beta^i.\beta^{e_j}\right)$

$= Tr_1^J\left(\beta^{i+e_j}\right) = t_{i+e_j}$ and the j^{th} column of $\mathbb{P}(\boldsymbol{t})$ is $E^{e_j}(\boldsymbol{t})$.

For $\sigma \in \mathbb{Z}_{2^J-1}$, we write $\sigma = in + j$ where $i \in \mathbb{Z}_{2^J-1}$, $j \in \mathbb{Z}_n$.

Then we have,

$Tr_J^{2J}(\alpha^{\sigma}) = Tr_J^{2J}\left(\alpha^{in+j}\right)$

$$= Tr_J^{2J}\left(\alpha^{in}.\alpha^j\right)$$

$$= Tr_J^{2J}\left(\beta^i.\alpha^j\right)$$

$$= \beta^i Tr_J^{2J}\left(\alpha^j\right).$$

If $Tr_J^{2J}\left(\alpha^j\right) = 0$, that is $e_j = \infty$, then $e_\sigma = \infty$.

Otherwise, $Tr_J^{2J}(\alpha^\sigma) = \beta^i\beta^{e_j} = \beta^{e_j+i}$. So, $e_\sigma = e_j + i$.

The terms of $\boldsymbol{e}^{(0)} = (e_0, e_1, e_2, \cdots, e_{n-1})$ also give the shifts of the M-sequence of span J which comprise the columns of $\mathbb{P}(\boldsymbol{t})$. Actually, the shift sequence is determined by its first $n = 2^J+1$ terms (Games [21]).

3.7.1 Properties of the shift sequence [21]

1. The shift sequence $\boldsymbol{e} = (e_0, e_1, e_2, \cdots, e_{2^{2J}-2})$ contains ∞ exactly once.
2. For fixed $k \in \mathbb{Z}_n$, the list of differences $\left(e_{j+k} - e_j\right) mod(n-2)$ where $j \in \mathbb{Z}_n$ contains each element of $\mathbb{Z}_{n-2}$ exactly once and ∞ exactly twice. This is called the Distinct Difference Property.

The proof of the Distinct Difference Property can be found in Games [21].

We shall see an example of row-wise folding of an M-sequence of length 63 to obtain a shift sequence $\boldsymbol{e}$.

Example 3.7.1

Take $p = 2,\ J = 3$. We choose the primitive polynomial

$f(x) = x^6 + x^5 + x^4 + x + 1$, where $n = 2^3 + 1 = 9$. An M-sequence

(0,1,1,1,1,1,1,0,1,0,1,1,1,0,0,0,1,1,0,0,1,1,1,0,1,1,0,0,0,0,0,1,1,1,1,0,0,1,0,0,1,0,1,0,1,0,0,1,1,

0,1,0,0,0,0,1,0,0,0,1,0,1,1) of length 63 is generated by the trace mapping

$Tr_1^6: GF(2^6) \rightarrow GF(2)$ and is folded along the rows of a 7 x 9 array $\mathbb{P}$, as shown:

$\mathbb{P} =$

0	1	1	1	1	1	1	0	1
0	1	1	1	0	0	0	1	1
0	0	1	1	1	0	1	1	0
0	0	0	0	1	1	1	1	0
0	1	0	0	1	0	1	0	1
0	0	1	1	0	1	0	0	0
0	1	0	0	0	1	0	1	1

Note: The trace mapping to an intermediate proper subfield requires only one row to determine the shift sequences, whilst the trace map to the base field requires the whole array to be filled in order to obtain the shift sequence.

The columns of $\mathbb{P}$ are numbered $0,1,2,\ldots,8$ and rows are numbered $0,1,2,\ldots 6$. We take column $C_5 = \mathbb{u} = [1,0,0,1,0,1,1]^T$, where T denotes the transpose, as a reference column. The sequence $\mathbb{u}$ is obtained by the trace mapping $Tr_1^3: GF(2^3) \rightarrow GF(2)$. Each column of $\mathbb{P}$ except the all zeros column is some shift of $\mathbb{u}$. The shift sequence of the columns in $\mathbb{P}$, relative to $\mathbb{u}$, is then $\boldsymbol{e} = (\infty, 6,5,5,3,0,3,4,6)$. We see that $\boldsymbol{e}$ contains ∞ exactly once.

The Distinct Difference Property (*Subsection 3.7.1*) is an important property that is required in the calculation of the autocorrelation values. We require this property for the autocorrelation calculation of the sequences constructed in Section 4.3. The Distinct Difference Property of $\boldsymbol{e}$ is made more clear from the following table.

Table of differences $(e_{j+k} - e_j)\ mod\ 7$ for *Example 3.7.1* Games [21]

k	$(e_{j+k} - e_j) mod\ 7 : j \in \mathbb{Z}(9)$								
1	∞	6	0	5	4	3	1	2	∞
2	∞	6	5	2	0	4	3	∞	1
3	∞	4	2	5	1	6	∞	3	0
4	∞	1	5	6	3	∞	4	2	0
5	∞	4	6	1	∞	0	3	2	5
6	∞	5	1	∞	4	6	3	0	2
7	∞	0	∞	2	3	6	1	4	5
8	∞	∞	2	1	3	4	5	0	6

Table 3.7.1

The autocorrelation calculation involves the differences. For a sequence over m^{th} roots of unity, the Distinct Difference Property guarantees that every exponent of ω_m appears exactly once in the correlation computation, where ω_m is an m^{th} root of unity.

3.8 Almost perfect sequences [75]

In 2005, Zeng *et al.* [75] showed a method of construction of almost perfect sequences (Wolfmann) based on the shift sequence associated with a primitive polynomial $f(x)$ of degree $2J$ over a finite field $GF(p)$ ($p\ odd\ prime\ and\ J = 1,2,\cdots$) and a pair of completely orthogonal almost perfect sequences.

This method gives almost perfect sequences of even lengths for higher alphabet sizes 4, 6 and 8. Zeng *et al.* have given examples of almost perfect sequences with up to 8^{th} roots of unity. The sequences over 4^{th} and 8^{th} roots of unity are generated when $p^J + 1 \equiv 2(mod\ 4)$ and $p^J + 1 \equiv 2(mod\ 8)$ respectively.

This method allows us to construct a set of long p-ary sequences with desired properties.

The construction uses the shift sequence discussed in Section 3.7 and the trace function (*Definition 3.6.3*).

The properties of the shift sequence $\boldsymbol{e} = (e_0, e_1, e_2, \cdots, e_{n-1})$ are used to define an ordered set.

The basic method for constructing almost perfect sequences discussed above involves two steps as shown below:

Step 1

Two almost perfect, completely orthogonal sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ of length m where $m = 2,4,6,8$ and a shift sequence $\boldsymbol{e} = (e_0, e_1, e_2, \cdots, e_{n-1})$, $n = p^J + 1,\ J = 1,2,\cdots$ constructed by Equation 3.7.1 are used to define an ordered set $\mathbb{A}$.

An ordered set $\mathbb{A}$ is defined as

$$\mathbb{A} = \{A_0, A_1, \cdots, A_{n-1}\}$$

where $A_i = \begin{cases} \mathcal{L}^{e_i}(\boldsymbol{a}) & if \quad e_i \neq \infty \\ \boldsymbol{b} & if \quad e_i = \infty \end{cases}$

Step 2

An $m \times n$ matrix $\mathbb{U} = (U_{i,j})$ is formed whose j^{th} column is A_j of the set $\mathbb{A}$. Each A_j contains m elements since $\boldsymbol{a}$ and $\boldsymbol{b}$ are of length m. So there are m rows and $n = p^J + 1$, columns, in the matrix. The entries of $\mathbb{U}$ are listed row by row starting from the first row first column element to the last row last column element. Then we obtain a sequence $\boldsymbol{u} = (u_o, u_1, \cdots, u_{mn-1})$ of length mn. This $m \times n$ matrix $\mathbb{U}$ is the matrix form of $\boldsymbol{u}$. The sequence $\boldsymbol{u}$ thus obtained is almost perfect according to Wolfmann's definition.

That is, the sequence $\boldsymbol{u} = (u_o, u_1, \cdots, u_{mn-1})$ has exactly one non-zero off-peak autocorrelation value for the shift $\tau = \frac{n}{2}$.

The following example is given in [75].

Example 3.8.1 An almost perfect sequence of length 20 over the 4^{th} roots of unity constructed in [75] is given below.

Take $m = 2,\ p = 3,\ J = 2,\ \boldsymbol{a} = (1, -1)\ \boldsymbol{b} = (j, j)$ where $j \in \{1, -1, i, -i\}$.

The primitive polynomial is $f(x) = x^4 + x^3 + 2$ over $GF(3)$ [50] of degree 4.

We obtain an M-sequence of length 80 over $GF(3)$, that is folded row-wise into an 8×10 array.

Thus we have,

$$\mathbb{P} = \begin{array}{|c|c|c|c|c|c|c|c|c|c|}\hline 1 & 1 & 1 & 2 & 0 & 1 & 2 & 1 & 1 & 2 \\ \hline 1 & 2 & 0 & 2 & 0 & 2 & 2 & 1 & 1 & 0 \\ \hline 2 & 0 & 1 & 1 & 0 & 0 & 1 & 2 & 2 & 2 \\ \hline 0 & 2 & 1 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\ \hline 2 & 2 & 2 & 1 & 0 & 2 & 1 & 2 & 2 & 1 \\ \hline 2 & 1 & 0 & 1 & 0 & 1 & 1 & 2 & 2 & 0 \\ \hline 1 & 0 & 2 & 2 & 0 & 0 & 2 & 1 & 1 & 1 \\ \hline 0 & 1 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ \hline \end{array}$$

We use $C_2 = (1,0,1,1,2,0,2,2)^T$, where T denotes the transpose of C_2, as the reference column, shaded in the array $\mathbb{P}$ above.

The shift sequence relative to C_2 is $\boldsymbol{e} = (2,3,0,6,\infty,3,6,2,2,4)$.

The associated matrix $\mathbb{U}$ is formed below:

$$\mathbb{U} = \begin{array}{|r|r|r|r|c|r|r|r|r|r|}\hline 1 & -1 & 1 & 1 & j & -1 & 1 & 1 & 1 & 1 \\ \hline -1 & 1 & -1 & -1 & j & 1 & -1 & -1 & -1 & -1 \\ \hline \end{array}$$

Unfolding $\mathbb{U}$ row-wise, we get an almost perfect sequence $(1,-1,1,1,j,-1,1,1,1,1,-1,1,-1,-1,j,1,-1,-1,-1,-1)$ of length 20 over the 4^{th} roots of unity with an off-peak autocorrelation value -16.

3.9 Non-Existence of almost perfect Wolfmann sequences

Wolfmann's construction did not yield binary almost perfect sequences of certain even lengths.

Pott and Bradley [57] used difference set theory to answer a couple of questions set by Wolfmann. They have shown that an almost perfect binary sequence of period n with x coefficients +1 in one generating cycle, exists if and only if there exists a cyclic $\left(\frac{n}{2}, 2, x\left(x-\frac{n}{2}\right), \left(x-\frac{n}{2}+1\right), \left(x-\frac{n}{4}\right)\right)$ divisible difference set (*Definition*, Page 302 in [57]).

In the case of Wolfmann, $x = \left(\frac{n}{2}-1\right)$, corresponds to divisible difference sets with parameters $\left(v, 2, (v-1), 0, \frac{v-2}{2}\right)$ where $v = \frac{n}{2}$. In connection with Wolfmann's paper, Pott and Bradley, by Theorem 4 [57], claim that almost perfect autocorrelation sequences of period $n \leq 452$ exist if and only if $\left(\frac{n}{2}-1\right)$ is a prime power.

Wolfmann's exhaustive search was up to $n = 100$. Wolfmann had questioned whether almost perfect sequences of lengths $n = 32, 44, 68, 72, 80, 92$ exist. These are the only numbers between 4 and 100 for which $\left(\frac{n}{2}-1\right)$ is not a prime power.

The construction of Luke and Zeng *et al.* yield both binary and non-binary near perfect and almost perfect sequences. However, it should be noted that all these construction methods again give only almost/near perfect sequences of some even lengths.

4 NEAR PERFECT SEQUENCES OF ODD LENGTHS

In this chapter we construct, for the first time, near perfect sequences of odd length. We use a shift sequence obtained by folding an M-sequence of length $2^{2J}-1$ into a $(2^J-1)\times(2^J+1)$ array. The chapter is organized as follows. In Section 4.1, we give preliminary definitions and results. Section 4.2 deals with the construction of near perfect sequences. We present the main result of the thesis in Section 4.6, namely, near perfect sequences of *unbounded* lengths can be constructed by the method described in Section 4.2. The results of Sections 4.2 and 4.3 were presented at the Fourth International Workshop on Signal Design and its Application in Communications, held in Fukuoka, Japan, 19-23, October 2009, and are published in IEEE Conference Proceedings, 2009 [30].

In Chapter 3, Section 3.5, we introduced the construction of almost perfect sequences of even length N over m^{th} roots of unity where $m = 2$, by Wolfmann [73], that have exactly one non-zero off-peak autocorrelation value for the shift $\tau = \frac{N}{2}$. Also almost (near) perfect sequences by Luke [45] were introduced in Section 3.6. Luke constructed almost (near) perfect sequences of length $N = m(p^J+1)$, for alphabet sizes $m = 2,3$ & 4 and p an odd prime, $J = 1,2,\ldots$.

The near perfect sequences constructed in this chapter are new. We give examples of our constructed near perfect sequences of several odd lengths in Section 4.5.

4.1 Preliminaries

Definition 4.1.1 *Near perfect sequences (Luke)*

Sequences over the m^{th} roots of unity and of length N where m divides N, are called near perfect sequences if they possess Periodic Autocorrelation Function (PACF) which satisfy, for any shift τ,

$$\Theta_s(\tau) = 0 \qquad \text{for } \tau \not\equiv 0 \; mod \left(\tfrac{N}{m}\right)$$

We recall, from Section 3.7, a definition of a shift sequence,

$\boldsymbol{e} = \{e_i : i = 0,1,2,\cdots,n-1\}$, associated with a primitive polynomial $f(x)$ (*Definition 2.1.6*) over *GF(2)*.

We see now another example of a shift sequence, obtained by folding an M-sequence of length 15. We shall use this shift sequence of length 2^2+1 to obtain a near perfect sequence of length 15. (Example 4.5.1)

Example 4.1.1

Construction of a shift sequence of length $5(mod\ 3)$.

We construct an M-sequence of length 15 with a primitive polynomial of degree 4 over $GF(2)$, namely,

$f(x) = x^4 + x^3 + 1$. (Table C, [43])

The M-sequence generated by $f(x)$ is $\boldsymbol{t} = [1,1,1,1,0,1,0,1,1,0,0,1,0,0,0]$

As in Chapter 3, Section 3.7, we fold $\boldsymbol{t}$ row-wise to form a 3×5 array $\mathbb{P}(\boldsymbol{t})$, starting from the first row, first column position.

So we have,

$$\mathbb{P}(\boldsymbol{t}) = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

We choose $\boldsymbol{u} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$ as a reference column.

The columns, except the all zeros column of $\mathbb{P}(\boldsymbol{t})$, are shifts of the M-sequence $\boldsymbol{u} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$.

From $\mathbb{P}(\boldsymbol{t})$, we obtain the shift sequence $\boldsymbol{e} = (0,1,0,0,\infty) mod\ 3$ of length 5, where the entries 0,1,0,0 in $\boldsymbol{e}$, are the shifts of $\boldsymbol{u}$ in $\mathbb{P}(\boldsymbol{t})$, and ∞ corresponds to the column of zeros. □

We are now ready for the construction of our near perfect sequences.

4.2 Construction of near perfect sequences

In this Section, we give a construction of near perfect sequences from any pair of completely orthogonal sequences $\boldsymbol{a}$; $\boldsymbol{a} \neq (1,1,1,\cdots,1)$ and $\boldsymbol{b}$ of length m, over the m^{th} roots of unity, m an odd prime, and a shift sequence (Section 3.7) associated with a primitive polynomial $f(x)$ of degree $2J$ over $GF(2)$, $J = 2,4,6,\cdots$.

The reason for J being even is to give small alphabet sizes, $m = 3,5,7$. If J is odd, we get larger alphabet sizes. The choice of J is based on applications, not on theory.

Recall from *Definition 2.3.5* that, $\mathcal{L}^{e_i}(\boldsymbol{a})$ is the left shift of $\boldsymbol{a}$ by e_i places.

Our construction is analogous to that of Zeng *et al.* [75] . However, it should be noted that our completely orthogonal pairs of sequences are constructed with different powers of a primitive m^{th} root of unity.

Construction

Step 1

Take a pair of completely orthogonal sequences $\boldsymbol{a}$, $\boldsymbol{a} \neq (1,1,1,\cdots,1)$ and $\boldsymbol{b}$ of length m, over the m^{th} roots of unity, $m = 3,5,7,\cdots$, and a shift sequence $\boldsymbol{e} = (e_0, e_1, e_2, \cdots, e_{n-1})$ as constructed in Section 3.7. We define an ordered set

$\mathbb{A} = \{A_0, A_1, \cdots, A_{n-1}\}$ by

$$A_{i=}\begin{cases}\mathcal{L}^{e_i}(\boldsymbol{a})\ if\ e_i \neq \infty \\ \boldsymbol{b} \quad otherwise\end{cases} \tag{4.2.1}$$

$\mathbb{A}$ is called the set associated with the sequences $\boldsymbol{a}, \boldsymbol{b}$ *and* $\boldsymbol{e}$.

Step 2

Let $\mathbb{S} = (S_{i,j})$ be the $m \times n$ matrix whose j^{th} column is A_j, say

$$\mathbb{S} = \begin{bmatrix} s_0 & s_1 & s_2 & \cdots & s_{n-1} \\ s_n & \cdots & \cdots & \cdots & s_{2n-1} \\ s_{2n} & \cdots & \cdots & \cdots & s_{3n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ s_{(m-1)n} & s & \cdots & \cdots & s_{mn-1} \end{bmatrix}$$

Listing all entries of $\mathbb{S}$ by concatenating the rows, we obtain a sequence $\boldsymbol{s} = (s_0, s_1, s_2, \cdots, s_{mn-1})$, of length $mn = N$. The sequence $\boldsymbol{s}$ is called the sequence

associated with the ordered set $\mathbb{A}$. The matrix $\mathbb{S}$ is called the associated matrix of the sequence $\boldsymbol{s}$. (*End of construction*)

The sequences constructed by this method are near perfect, as shown in the next Section.

4.3 Calculation of autocorrelation of the constructed sequences

To show the near perfection of the sequences constructed in Section 4.2, we first give the formula to find the autocorrelation values. The formula given below is adapted and modified from Zeng *et al.* [75]. We assume $p = 2$ instead of an odd prime and $\boldsymbol{a} \neq (1,1,1,\cdots,1)$ and $\boldsymbol{b}$ are any two sequences of length m, an odd prime, over m^{th} roots of unity, which are completely orthogonal. Here we lift the restriction by Zeng *et al.*, of $\boldsymbol{a}$ and $\boldsymbol{b}$ being almost perfect (Wolfmann) and completely orthogonal. The objective of Zeng *et al.* was to construct almost perfect sequences (Wolfmann) over alphabet sizes $m = 2,4,6\ and\ 8$. Hence they had adopted this strict restriction. To construct near perfect sequences of odd lengths, by the method described in Section 4.2, we need $\boldsymbol{a}$ and $\boldsymbol{b}$ of odd length. It should be noted that all the almost perfect sequences (Wolfmann) are of even lengths. We do not assume $\boldsymbol{a}$ and $\boldsymbol{b}$ to be almost perfect. In our case, we consider *almost square* arrays, so that the shift sequence contains exactly one ∞. But there exist other shift sequences with more than one ∞ when we fold a sequence diagonally into a $\mathbb{p} \times \mathbb{q}$ array where $\mathbb{p}$ and $\mathbb{q}$ are co-prime.

The following theorem gives a formula to calculate the autocorrelation values of the near perfect sequences constructed in Section 4.2.

Theorem 4.3.1

Let $\boldsymbol{s} = (s_0, s_1, s_2, \cdots, s_n, \cdots, s_{2n}, \cdots, s_{(m-1)n}, \cdots, s_{mn-1})$ be a sequence of length mn obtained from our construction. The autocorrelation $\Theta_{\boldsymbol{s}}(\tau)$ for any shift $\tau = qn + r$ with $0 \leq q \leq m$ and $0 \leq r \leq n$ is given by

$$\Theta_{\boldsymbol{s}}(\tau) = \sum_{j=0}^{n-r-1} \Theta_{A_j A_{r+j}}(q) + \sum_{j=n-r}^{n-1} \Theta_{A_j A_{r+j(mod\, n)}}(q+1)$$

The first sum covers the case $r + j < n$ and the second sum covers the case $r + j \geq n$.

Proof:

We have $\boldsymbol{s} = (s_0, s_1, s_2, \cdots, s_n, \cdots, s_{2n}, \cdots, s_{(m-1)n}, \cdots, s_{mn-1})$

Let us fold $\boldsymbol{s}$ row-wise into an $m \times n$ array $\mathbb{A}$, to obtain

$$\mathbb{A} = \begin{bmatrix} s_0 & s_1 & s_2 & \cdots & s_{n-1} \\ s_n & \cdots & \cdots & \cdots & s_{2n-1} \\ s_{2n} & \cdots & \cdots & \cdots & s_{3n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ s_{(m-1)n} & s & \cdots & \cdots & s_{mn-1} \end{bmatrix}$$

Let $A_0, A_1, A_2, \cdots, A_{n-1}$ denote the columns of $\mathbb{A}$. Each column A_j is a left shift of $\boldsymbol{a}$ if $\boldsymbol{e_i} \neq \infty$ and $\boldsymbol{b}$ if $\boldsymbol{e_i} = \infty$.

Consider any shift $\tau = qn + r$ where $0 \leq q \leq m$ and $0 \leq r \leq n$.

So, $\mathcal{L}^{\tau}(\boldsymbol{s}) = (s_\tau, s_{\tau+1}, s_{\tau+2}, \cdots, s_n, \cdots, s_{2n}, \cdots, s_{\tau-3}, s_{\tau-2}, s_{\tau-1})$

Let $\mathbb{B}$ be the array form of $\mathcal{L}^{\tau}(\boldsymbol{s})$, obtained by folding $\mathcal{L}^{\tau}(\boldsymbol{s})$ into m rows each of length n. Then we have

$$\mathbb{B} = \begin{bmatrix} s_{\tau} & s_{1+\tau} & s_{2+\tau} & \cdots & s_{n-1+\tau} \\ s_{n+\tau} & s_{n+1+\tau} & s_{n+2+\tau} & \cdots & s_{2n-1+\tau} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ s_{(n-1)+\tau} & \cdots & \cdots & s_{\tau-2} & s_{\tau-1} \end{bmatrix}$$

Let $B_0, B_1, B_2, \cdots, B_{n-1}$ denote the columns of $\mathbb{B}$. Any column B_j of $\mathbb{B}$ is given by

$$B_j = \begin{cases} \mathcal{L}^q\left(A_{r+j(modn)}\right) & if \;\; r+j < n \\ \mathcal{L}^{q+1}\left(A_{r+j(modn)}\right) & if \;\; r+j \geq n \end{cases} \tag{4.3.1}$$

As seen in Chapter 2, Definition 2.14, the autocorrelation of $\mathbb{A}$ for a shift (k, l) of $\mathbb{A}$ is the summation of the correlation of the overlaying columns,

Here, B_j is a shift of A_j. Thus,

$$\Theta_{\boldsymbol{s}}(\tau) = \sum_{j=0}^{n-1} A_j . B_j$$

So we have**,**

$$\Theta_{\boldsymbol{s}}(\tau) = \sum_{j=0}^{n-r-1} \Theta_{A_j A_{r+j}}(q) + \sum_{j=n-r}^{n-1} \Theta_{A_j A_{r+j(mod\, n)}}(q+1) \tag{4.3.2}$$

■

Given a pair of completely orthogonal sequences over the m^{th} roots of unity, $m = 3,5,7,\cdots,$ and a shift sequence $\boldsymbol{e} = (e_0, e_1, e_2, \cdots, e_{n-1})$, we now prove the near perfection of a sequence constructed by the method described in Section 4.2.

Theorem 4.3.2

Let $\boldsymbol{a} = \{a_i\}$ and $\boldsymbol{b} = \{b_i\},\ a_i, b_i \in \{1, \omega, \omega^2, \cdots, \omega^{m-1}\}$ and $a \neq (1,1,1\cdots,1)$ be sequences of length m, over the m^{th} roots of unity, $m = 3,5,7,\cdots,$ such that $\boldsymbol{a}$ and $\boldsymbol{b}$ are completely orthogonal. Let the associated matrix be $\mathbb{A}$, formed using the shift

sequence $\boldsymbol{e} = (e_0, e_1, e_2, \cdots, e_{n-1}), n = 2^J + 1, J = 2,4,6, \cdots$. If $m\ divides\ (n-2)$, then $\boldsymbol{s}$ is a near perfect sequence of length $mn = N$.

Proof:

We know that the columns (A_j) of the associated matrix $\mathbb{A}$, from Equation 4.2.1 are

$$A_{j=}\begin{cases}\mathcal{L}^{e_j}(\boldsymbol{a})\ if\ e_j \neq \infty \\ \boldsymbol{b} \quad otherwise\end{cases}$$

Since the shift sequence contains exactly one ∞, exactly one column of the associated matrix $\mathbb{A}$ is $\boldsymbol{b}$, corresponding to the ∞ in $\boldsymbol{e}$. All the other columns are the corresponding left shifts $(\mathcal{L}^{e_i}(\boldsymbol{a}), e_i \in e; e_i \neq \infty)$ of $\boldsymbol{a}$.

Based on Equation 4.3.1, the columns B_j are given as follows:

(i) When $e_{(r+j)modn} \neq \infty$, we have

$$B_j = \mathcal{L}^q(\mathcal{L}^{e_{(r+j)modn}}(\boldsymbol{a}))$$

$$= \mathcal{L}^{q+e_{(r+j)modn}}(\boldsymbol{a}) \quad \text{when } r + j < n$$

and $$B_j = \mathcal{L}^{q+1}(\mathcal{L}^{e_{(r+j)modn}}(\boldsymbol{a}))$$

$$= \mathcal{L}^{q+1+e_{(r+j)modn}}(\boldsymbol{a}) \quad \text{when } r + j \geq n$$

where $\mathcal{L}^{q+1+e_{(r+j)modn}}$ is caused by the wrap around.

(ii) When $e_{(r+j)modn} = \infty$, we have

$$B_j = \begin{cases}\mathcal{L}^q(\boldsymbol{b}) & if\ \ r + j < n \\ \mathcal{L}^{q+1}(\boldsymbol{b}) & if\ \ r + j \geq n\end{cases} \qquad (4.3.3)$$

Take any shift $\tau = qn + r \qquad 0 \leq q < m, \quad 0 \leq r < n$

Our autocorrelation calculation consists of two cases.

Case 1 $r \neq 0$

In this case, $\tau \not\equiv 0 \; mod \left(\frac{N}{m}\right)$

We show the autocorrelation value for these shifts is zero.

Consider the differences in the shift sequence of the type $\left(e_{r+j} - e_j\right) mod(n-2)$

where $j < n$. The list of differences contains ∞ exactly twice (Table 3.7.1).

In this case $\Theta_{\boldsymbol{s}}(\tau)$ has three summands, namely, when

i. $e_j \neq \infty, e_{r+j} \neq \infty$

ii. $e_j = \infty, e_{r+j} \neq \infty$

iii. $e_j \neq \infty, e_{r+j} = \infty$

That is,

$$\Theta_{\boldsymbol{s}}(\tau) = \sum_{e_j \neq \infty, e_{r+j} \neq \infty} \Theta_{\boldsymbol{a}}\left(e_{r+j} - e_j + r\right) + \sum_{e_j \neq \infty, e_{r+j} = \infty} \Theta_{\boldsymbol{a},\boldsymbol{b}}(\tau_1) + \sum_{e_j = \infty, e_{r+j} \neq \infty} \Theta_{\boldsymbol{b},\boldsymbol{a}}(\tau_2) \tag{4.3.4}$$

where $\tau_1 = \begin{cases} e_{(r+j)(mod\, n)} + r & if \quad r + j < n \\ e_{(r+j)(mod\, n)} + r + 1 & if \quad r + j \geq n \end{cases}$ and

$$\tau_2 = \begin{cases} q - e_j & if \quad r + j < n \\ q + 1 - e_j & if \quad r + j \geq n \end{cases}$$

Since $\boldsymbol{a}$ and $\boldsymbol{b}$ are completely orthogonal, we have, $\Theta_{\boldsymbol{a},\boldsymbol{b}}(\tau_1)$ and $\Theta_{\boldsymbol{b},\boldsymbol{a}}(\tau_2)$ are zero.

So, $\Theta_{\boldsymbol{s}}(\tau) = \sum_{e_j \neq \infty, e_{r+j} \neq \infty} \Theta_{\boldsymbol{a}}\left(e_{r+j} - e_j + r\right)$

According to the Distinct Difference Property (*Subsection 3.7.1*), the set $(e_{r+j} - e_j + r)$ contains every element *modulo* m exactly once.

Let $e_{r+j} - e_j + r = \ell \pmod{m}$.

Then $\Theta_{\boldsymbol{s}}(\tau) = \sum_{\ell=0}^{n-3} \Theta_{\boldsymbol{a}}(\ell \bmod m)$.

We assume m divides $(n-2)$ and so

$$\Theta_{\boldsymbol{s}}(\tau) = \frac{(n-2)}{m} \sum_{\ell=0}^{m-1} \Theta_{\boldsymbol{a}}(\ell)$$

Since $\boldsymbol{a} = \{a_i\};\ a_i \in \{1, \omega, \omega^2, \cdots, \omega^{m-1}\}$, we get $\sum_{\ell=0}^{m-1} \Theta_{\boldsymbol{a}}(\ell)=0$, ω being an m^{th} root of unity.

Therefore, $\Theta_{\boldsymbol{s}}(\tau) = \frac{(n-2)}{m} \times 0 = 0$.

That is, $\Theta_{\boldsymbol{s}}(\tau) = 0$ for $r \neq 0$.

Case 2 $\quad r = 0$

In this case, $\tau \equiv 0 \bmod \left(\frac{N}{m}\right)$

We show the autocorrelation values for these shifts are non-zero.

We have $r + j < n$.

Then Equation 4.3.2 reduces to

$$\Theta_{\boldsymbol{s}}(\tau) = \sum_{j=0}^{n-1} \Theta_{A_j A_j}(q)$$

From Equation 4.2.1, we have one of the $A_j's$ is $\boldsymbol{b}$, corresponding to the ∞ in $\boldsymbol{e}$. It can be easily seen that all the columns of $\mathbb{A}$ fall on top of each other for shifts $\tau = qn$ where $q = 0,1,2,\ldots,m-1$. So the components of $\Theta_{\boldsymbol{s}}(\tau)$ are autocorrelation values of $\boldsymbol{a}$ and $\boldsymbol{b}$ for shifts $q = 0,1,2 \ldots m-1$.

Thus we have, $\Theta_{\boldsymbol{s}}(\tau)=(n-1)\Theta_{\boldsymbol{a}}(q) + \Theta_{\boldsymbol{b}}(q)$. (4.3.5)

■

We shall provide a simple example to demonstrate the Case 2, where $r = 0$.

Example 4.3.1

Take any near perfect sequence $\boldsymbol{s} = (a_0, a_1, a_2, \cdots, a_{14})$ of length 15.

The associated matrix for $\boldsymbol{s}$ is $\mathbb{A} = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ a_5 & a_6 & a_7 & a_8 & a_9 \\ a_{10} & a_{11} & a_{12} & a_{13} & a_{14} \end{bmatrix}$

Consider the shift $q = 5$ of $\boldsymbol{s}$. Then the associated matrix for this shift is

$$\mathbb{A}_5 = \begin{bmatrix} a_5 & a_6 & a_7 & a_8 & a_9 \\ a_{10} & a_{11} & a_{12} & a_{13} & a_{14} \\ a_0 & a_1 & a_2 & a_3 & a_4 \end{bmatrix}$$

It is easily noticed that each column of $\mathbb{A}$ is shifted upwards by 1 to obtain the respective columns of $\mathbb{A}_5$. ■

4.4 Reduced shift sequences

In this section we give the construction of other shift sequences of longer lengths. These shift sequences are called *Reduced shift sequences* and are used to construct near perfect sequences of longer odd lengths for different alphabet sizes.

We have seen from [21] and [72] that an M-sequence of length $2^{2J}-1$ can be folded row-wise or diagonally, so that the resulting M-array $\mathbb{P}$ is almost square (*Definition 2.4.4*), of dimension $(2^J-1)\times(2^J+1)$. Here, each column is a shift of an M-sequence of length (2^J-1) corresponding to a shift sequence of length (2^J+1).

Definition 4.4.1

Take the shift sequence $\boldsymbol{e}=(e_0,e_1,e_2,\cdots,e_{n-1})\ modulo\ n, n=2^J+1$. If the column length (2^J-1), of the almost square M-array $\mathbb{P}$ is written as a product of primes say $m_1m_2\cdots$, where $m_1<m_2<\cdots$, and we reduce each entry of $\boldsymbol{e}\ modulo\ m_1$, to obtain a shift sequence $\boldsymbol{e}'=\left(e_0',e_1',\cdots,e_{n-1}'\right)$, then $\boldsymbol{e}'$ is called a *reduced shift sequence* modulo m_1.

4.4.1 Properties of the reduced shift sequences

1) The reduced shift sequence $\boldsymbol{e}'=(e_0',e_1',\cdots,e_{n-1}')$ where each $e_i'=e_i(mod\ m)$, $0\le i\le n-1$ contains ∞ exactly once.

This is obvious since $\boldsymbol{e}'$ is obtained by reducing each element of $\boldsymbol{e}$, which contains exactly one ∞.

2) The differences $(e'_{j+k} - e'_j)$, k-apart of $\boldsymbol{e}'$ are equally numerous and ∞ appears exactly twice.

To prove Property 2 of reduced shift sequences, we use the Fundamental Theorem of Arithmetic and Class Theory.

Theorem 4.4.1 (Fundamental Theorem of Arithmetic) Every positive integer can be uniquely expressed as a product of primes.

Corollary 4.4.2 An integer $n > 1$ can be uniquely written as $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$; where for each $i = 1,2,\cdots,r$, k_i are positive integers and p_i are primes such that $p_1 < p_2 < \cdots < p_r$.

Proof of Property 2

By Corollary 4.4.2, any integer of the form $(2^J - 1)$ can be factorised into a product of primes.

So we have, $(2^J - 1) = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$; for every $i = 1,2,\cdots,r$, k_i are positive integers and p_i are primes such that $p_1 < p_2 < \cdots < p_r$.

Let $m = p_1$, be our alphabet size.

Let $\boldsymbol{e} = (e_0, e_1, \cdots, e_{n-1})$ be the shift sequence obtained by the row-wise folding shown in Section 3.6. Games [21] has proved that, for fixed $k \in \mathbb{Z}_n$, the list of differences $D_k = \{(e_{j+k} - e_j) \, mod(n-2) : j = 0,1,2,\cdots n-1\}$, contains each element of $\mathbb{Z}_{n-2}$ exactly once and each of $+\infty, -\infty$ exactly once.

Thus $D_k = \{0,1,2,\cdots,n-3\} \cup \{+\infty, -\infty\}$

We reduce every element of the set $\{0,1,2,\cdots,n-3\}$ modulo m to obtain the list of classes $\langle [0]modm, [1]modm, \cdots, [n-3]modm\rangle$. Here $0,1,2,\cdots,m-1$, are the class-representatives. The occurrence of each class representative is equally numerous and each class representative appears $\left(\frac{n-2}{m}\right)$ times.

Now, for $k \in \mathbb{Z}_n$, let $D'_k = D_k \backslash \{\infty, -\infty\}$ be the set of differences k- apart without the elements $+\infty, -\infty$.

If we reduce every element of D'_k modulo m, we have the list $\langle (e_{i+k} - e_i)\ mod(n-2) | i = 0,1,2,\cdots n-1\rangle$, and then each class $[𝕚]mod\ m$ for $𝕚 = 0,1,\cdots,m-1$ appears exactly $\left(\frac{n-2}{m}\right)$ times by the assumption that m divides $(n-2)$.

From the class theory we have $\left([e_{j+k}]\ mod\ m - [e_j] mod\ m\right) = \left([e_{j+k}] - [e_j]\right) mod\ m$ for $j,k = 0,1,2,\cdots n-3$. Then the finite differences k-apart of the reduced shift sequence $([e_0]modm, [e_1]modm, \cdots, [e_{n-3}]modm)$ are equally numerous. ■

We have the column length of an M-array formed by folding an M-sequence of length $(2^{2J}-1)$, as (2^J-1). So, if we fix the alphabet size as m, and if m is a factor of (2^J-1), we can construct reduced shift sequences as described above.

We provide a useful example for a better understanding of reduced shift sequences.

Example 4.4.1

We use an M-sequence of length 15 to determine the shift sequence of length 17 *modulo* 15. For this we first take an M-sequence of length $2^8 - 1 = 255$ which can be folded row-wise into a 15×17 array.

$$\mathbb{P} = \begin{bmatrix} 0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&0 \\ 1&0&1&1&1&0&0&0&0&0&0&1&1&0&1&1&0 \\ 0&1&0&0&1&1&0&1&1&1&0&0&1&0&0&0&0 \\ 0&1&0&1&0&1&1&0&1&1&0&1&0&1&0&0&0 \\ 1&0&1&1&0&0&0&0&1&1&1&1&1&0&1&1&0 \\ 1&1&1&1&0&1&0&1&1&1&0&1&0&0&1&1&0 \\ 0&0&0&1&1&0&1&1&0&0&0&1&1&1&0&0&0 \\ 1&1&1&0&0&1&1&0&0&0&1&0&1&1&1&1&0 \\ 0&1&0&0&0&1&0&1&0&0&1&0&1&0&0&0&0 \\ 1&1&1&0&1&1&1&0&1&1&0&0&1&1&1&1&0 \\ 1&1&1&1&1&1&0&1&0&0&1&1&0&0&1&1&0 \\ 1&0&1&0&0&0&1&1&0&0&0&0&0&1&1&1&0 \\ 1&0&1&0&1&0&1&1&1&1&1&0&0&1&1&1&0 \\ 0&0&0&1&0&0&1&1&1&1&1&1&1&1&0&0&0 \\ 0&1&0&1&1&1&1&0&0&0&1&1&0&1&0&0&0 \end{bmatrix}$$

We take the M-sequence $\mathbb{m} = (1,0,1,0,1,1,0,0,1,0,0,0,1,1,1)$ of length 15 as the reference sequence to determine the shift sequence. All the columns of this array are shifts of $\mathbb{m}$. The length of the M-sequence, $\mathbb{m}$, is $3 \times 5 = 15$.

The shift sequence of the array $\mathbb{P}$ is

$e = (5,7,5,11,0,7,3,4,12,12,2,11,8,3,6,5,\infty) mod\ 15$.

Every entry of this shift sequence can be reduced *modulo* 3 and *modulo* 5 to obtain reduced shift sequences *mod* 3 and *mod* 5 respectively.

These reduced shift sequences are $\boldsymbol{e_1} = (2,1,2,2,0,1,0,1,0,0,2,2,2,0,0,2,\infty) mod\ 3$ and $\boldsymbol{e_2} = (0,2,0,1,0,2,3,4,2,2,2,1,3,3,1,0,\infty) mod\ 5$.

We shall use $\boldsymbol{e_1}$ to obtain a near perfect sequence of length 51 over the cube roots of unity by constructing the associated matrix of order 3×17 (See *Example 4.5.3* below).

The shift sequence $\boldsymbol{e_2}$ is used to construct a near perfect sequence of length 85 over roots of unity with an associated matrix of order 5×17 (See *Example 4.5.4* below).

Note: *Theorem 4.3.2* is valid for reduced shift sequences also, because, the differences $(e_{r+j} - e_j)$ are equally numerous, which again yield near perfect autocorrelation values.

4.5 Examples of near perfect sequences of odd length

In this section we see different examples of near perfect sequences constructed by the above methods.

Near perfect sequences of length 15 are the shortest near perfect sequences obtained by our construction.

We assume $a \neq (1,1,\cdots,1)$ of length m as in *Theorem 4.3.2*. We assume J to be even, to get desirable and small alphabet sizes which are useful for practical applications.

Example 4.5.1 Near perfect sequence of length 15

Take $\boldsymbol{a} = (1, \omega, \omega^2); \boldsymbol{b} = (1,1,1)$. We use the shift sequence $\boldsymbol{e} = (0,1,0,0,\infty) mod\ 3$ obtained in *Example 4.1.1*. We see that $\boldsymbol{e}$ contains ∞ exactly once. As seen in Section 4.3, we form an associated matrix

$\mathbb{A} = \begin{bmatrix} 1 & \omega & 1 & 1 & 1 \\ \omega & \omega^2 & \omega & \omega & 1 \\ \omega^2 & 1 & \omega^2 & \omega^2 & 1 \end{bmatrix}$ of dimension 3×5.

Now we concatenate the rows of $\mathbb{A}$ to obtain a near perfect sequence of length $3 \times 5 = 15$.

So we have $\boldsymbol{s} = (1, \omega, 1,1,1, \omega, \omega^2, \omega, \omega, 1, \omega^2, 1, \omega^2, \omega^2, 1)$, which has the near perfect periodic autocorrelation function

$\Theta_{\boldsymbol{s}}(\tau)$=$(15, 0,0,0,0,\ -3 + 10.3923i,\ 0,0,0,0,\ -3 - 10.3923i,\ 0,0,0,0)$.

$|\Theta_{\boldsymbol{s}}(\tau)|$=$(15, 0,0,0,0, 10.82,\ 0,0,0,0,\ 10.82,\ 0,0,0,0)$.

Example 4.5.2 Near perfect sequence of length 15 (2)

We can also use $J = 2$, $\boldsymbol{a} = (1, \omega, \omega^2)$ and $\boldsymbol{b} = (1, \omega^2, \omega)$ and the same shift sequence to get another near perfect sequence of length 15 over the cube roots of unity.

Here we have $\boldsymbol{s}$ =$(1, \omega, 1,1,1, \omega, \omega^2, \omega, \omega, \omega^2, \omega^2, 1, \omega^2, \omega^2, \omega)$ with the near perfect periodic autocorrelation function

$\Theta_{\boldsymbol{s}}(\tau)$= $(15, 0,0,0,0,\ -7.5 + 7.79423i,\ 0,0,0,0,\ -7.5 - 7.79423i,\ 0,0,0,0)$.

Again $|\Theta_{\boldsymbol{s}}(\tau)| = (15, 0,0,0,0, 10.82, 0,0,0,0, 10.82, 0,0,0,0)$.

Example 4.5.3 Near perfect sequence of length 51

To obtain a near perfect Sequence of length 51, we take

J =4, $\boldsymbol{a} = (1, \omega, \omega^2)$; $\boldsymbol{b}$ = (1,1,1) and the reduced shift sequence

$\boldsymbol{e}$ =(2,1,2,2,0,1,0,1,0,0,2,2,2,0,0,2, ∞) mod 3 as seen in *Example 4.4.1*.

The near perfect sequence obtained is of length 51 over the cube roots of unity as shown below.

$\boldsymbol{s} = (\omega^2, \omega, \omega^2, \omega,^2 1, \omega, 1, \omega, 1,1, \omega^2, \omega^2, \omega^2, 1,1, \omega^2,1,1,\omega^2, 1,1, \omega, \omega^2, \omega, \omega^2, \omega, \omega, 1,1,1, \omega,$

$\omega, 1,1, \omega, 1, \omega, \omega, \omega^2, 1, \omega^2, 1, \omega^2, \omega^2, \omega, \omega, \omega, \omega^2, \omega^2, \omega, 1)$

The near perfect periodic autocorrelation function of $\boldsymbol{s}$ is

$\Theta_s(\tau) = (51, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, -21 + 41.5692i, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,$

$-21 - 41.5692i, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$

Example 4.5.4 Near perfect sequence of length 85

We provide another example with,

J =4, $\boldsymbol{a} = (1, \lambda, \lambda^2, \lambda^3, \lambda^4)$; $\boldsymbol{b}$ = (1,1,1,1,1) and the reduced shift sequence

$\boldsymbol{e}$ = (0,2,0,1,0,2,3,4,2,2,2,1,3,3,1,0, ∞)mod 5

With these, we get a near perfect sequence of length 85 over the fifth roots of unity.

$(1, \lambda^2, 1, \lambda, 1, \lambda^2, \lambda^3, \lambda^4, \lambda^2, \lambda^2, \lambda^2, \lambda, \lambda^3, \lambda^3, \lambda, 1,1, \lambda, \lambda^3, \lambda, \lambda^2, \lambda, \lambda^3, \lambda^4, 1\ , \lambda^3, \lambda,^3\ , \lambda^3, \lambda^2, \lambda^4, \lambda^4$

$\lambda^2, \lambda, 1, \lambda^2, \lambda^4, \lambda^2, \lambda^3, \lambda^2, \lambda^4, 1, \lambda, \lambda^4, \lambda^4, \lambda^4, \lambda^3, 1,1, \lambda^3, \lambda^2, 1, \lambda^3, 1, \lambda^3, \lambda^4, \lambda^3, 1, \lambda\ \lambda^2, 1,1,1, \lambda^4, \lambda, \lambda, \lambda^4,$

$\lambda^3, 1, \lambda^4, \lambda, \lambda^4, 1, \lambda^4, \lambda, \lambda^2, \lambda^3, \lambda, \lambda, \lambda, 1, \lambda^2, \lambda^2, 1, \lambda^4, 1)$

The near perfect periodic autocorrelation function is

$\Theta_{\boldsymbol{s}}(\tau)$= (85,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,

$\mathbb{a}$, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, $\mathbb{b}$, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,

$\mathbb{b}^*$, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, $\mathbb{a}^*$, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) where

$\mathbb{a} = 29.7214 + 76.0845i$ and $\mathbb{b} = -59.7214 + 47.0228i$.

Table 4.5.1, below shows, for several choices of the value for J, and of the alphabet size m, the corresponding lengths of the near perfect sequences, obtained by our construction, and listed in Section 4.5.

J	$n = 2^J + 1$	Alphabet size (m)	Length of the NP sequence ($N = mn$)
2	5	3	15
4	17	3	51
4	17	5	85
6	65	3	195
6	65	7	455
8	257	3	771
8	257	5	1285
10	1025	3	3075

Table 4.5.1

We now give examples of near perfect sequences listed in Table 4.5.1 from lengths 195 to 3075. The magnitude of the autocorrelation values are listed below each sequence.

In all examples, we take, $z = e^{\frac{2\pi i}{m}}$, where $m = 3,5, or\ 7$, which is the alphabet size, and the M-array dimensions are also given.

Example 4.5.5

$Alphabet\ size: m = 3$
$M - Array\ Dimension: 63 \times 65$

Near perfect sequence of length 195

$\boldsymbol{s} = \{1, z^2, 1, z^2, z^2, 1, z^2, z^2, z^2, 1, 1, 1, z^2, z^2, z, 1, 1, 1, z, 1, z^2, z^2, z^2, z^2, z,$
$z^2, 1, 1, z, 1, z^2, z, z, z^2, z^2, z^2, z, z^2, 1, z, 1, z^2, z^2, 1, z, 1, z^2, 1, z^2, 1, z, z,$
$z^2, 1, z^2, z^2, 1, z^2, z^2, z, z^2, z^2, 1, 1, z, z, 1, z, 1, 1, z, 1, 1, 1, z, z, z, 1, 1, z^2,$
$z, z, z, z^2, z, 1, 1, 1, 1, z^2, 1, z, z, z^2, z, 1, z^2, z^2, 1, 1, 1, z^2, 1, z, z^2, z, 1, 1,$
$z, z^2, z, 1, z, 1, z, z^2, z^2, 1, z, 1, 1, z, 1, 1, z^2, 1, 1, 1, z, z^2, z^2, z, z, z^2, z, z, z^2,$
$z, z, z, z^2, z^2, z^2, z, z, 1, z^2, z^2, z^2, 1, z^2, z, z, z, z, 1, z, z^2, z^2, 1, z^2, z, 1, 1,$
$z, z, z, 1, z, z^2, 1, z^2, z, z, z^2, 1, z^2, z, z^2, z, z^2, 1, 1, z, z^2, z, z, z^2, z, z, 1, z,$
$z, 1, z^2, 1\}$

$\Theta_{\boldsymbol{s}}(\tau) = \{195, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,$
$0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,$
$0, 0, 0, 0, 0, 0, 0, 190.5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,$
$0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,$
$0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 190.5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,$
$0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,$
$0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0\}$

Example 4.5.6

$Alphabet\ size: m = 7$
$M - Array\ Dimension: 63 \times 65$

Near perfect sequence of length 455

$\boldsymbol{s} = \{1, 1, z^4, z^3, z^2, z^3, z^3, z^4, z^5, z^2, 1, 1, z^3, z^2, z^5, z^2, z, z^4, 1, z^6, z^4, 1, 1, z^3,$
$z^3, z^3, 1, z^2, z, 1, z^4, z^6, z, 1, z^4, z^5, z^6, z^4, z^5, z^3, z^6, z, z^6, z^4, z^6, z^3, z, z^3, z,$
$z^2, z^5, z^2, z^2, z^2, z^3, z^3, z^5, 1, z^4, z^5, z, z^3, 1, z^4, z^3, z, z, z^5, z^4, z^3, z^4, z^4, z^5,$
$z^6, z^3, z, z, z^4, z^3, z^6, z^3, z^2, z^5, z, 1, z^5, z, z, z^4, z^4, z^4, z, z^3, z^2, z, z^5, 1, z^2, z,$
$z^5, z^6, 1, z^5, z^6, z^4, 1, z^2, 1, z^5, 1, z^4, z^2, z^4, z^2, z^3, z^6, z^3, z^3, z^3, z^4, z^4, z^6, z,$

$z^5, z^6, z^2, z^4, 1, z^5, z^4, z^2, z^2, z^6, z^5, z^4, z^5, z^5, z^6, 1, z^4, z^2, z^2, z^5, z^4, 1, z^4, z^3,$
$z^6, z^2, z, z^6, z^2, z^2, z^5, z^5, z^5, z^2, z^4, z^3, z^2, z^6, z, z^3, z^2, z^6, 1, z, z^6, 1, z^5, z, z^3,$
$z, z^6, z, z^5, z^3, z^5, z^3, z^4, 1, z^4, z^4, z^4, z^5, z^5, 1, z^2, z^6, 1, z^3, z^5, 1, z^6, z^5, z^3, z^3,$
$1, z^6, z^5, z^6, z^6, 1, z, z^5, z^3, z^3, z^6, z^5, z, z^5, z^4, 1, z^3, z^2, 1, z^3, z^3, z^6, z^6, z^6, z^3,$
$z^5, z^4, z^3, 1, z^2, z^4, z^3, 1, z, z^2, 1, z, z^6, z^2, z^4, z^2, 1, z^2, z^6, z^4, z^6, z^4, z^5, z, z^5,$
$z^5, z^5, z^6, z^6, z, z^3, 1, z, z^4, z^6, 1, 1, z^6, z^4, z^4, z, 1, z^6, 1, 1, z, z^2, z^6, z^4, z^4, 1,$
$z^6, z^2, z^6, z^5, z, z^4, z^3, z, z^4, z^4, 1, 1, 1, z^4, z^6, z^5, z^4, z, z^3, z^5, z^4, z, z^2, z^3, z,$
$z^2, 1, z^3, z^5, z^3, z, z^3, 1, z^5, 1, z^5, z^6, z^2, z^6, z^6, z^6, 1, 1, z^2, z^4, z, z^2, z^5, 1, 1, z,$
$1, z^5, z^5, z^2, z, 1, z, z, z^2, z^3, 1, z^5, z^5, z, 1, z^3, 1, z^6, z^2, z^5, z^4, z^2, z^5, z^5, z, z,$
$z, z^5, 1, z^6, z^5, z^2, z^4, z^6, z^5, z^2, z^3, z^4, z^2, z^3, z, z^4, z^6, z^4, z^2, z^4, z, z^6, z, z^6, 1,$
$z^3, 1, 1, 1, z, z, z^3, z^5, z^2, z^3, z^6, z, 1, z^2, z, z^6, z^6, z^3, z^2, z, z^2, z^2, z^3, z^4, z, z^6,$
$z^6, z^2, z, z^4, z, 1, z^3, z^6, z^5, z^3, z^6, z^6, z^2, z^2, z^2, z^6, z, 1, z^6, z^3, z^5, 1, z^6, z^3, z^4,$
$z^5, z^3, z^4, z^2, z^5, 1, z^5, z^3, z^5, z^2, 1, z^2, 1, z, z^4, z, z, z, z^2, z^2, z^4, z^6, z^3, z^4, 1,$
$z^2, 1, z^3, z^2\}$

$\boldsymbol{\Theta_s(\tau)} =$ {455,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,452,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
446,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,441,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,441,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,446,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,452,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0}

Example 4.5.7

Alphabet size: $m = 3$
$M - Array\ Dimension$: 255×257

Near perfect sequence of length 771

$\boldsymbol{s} = \{1, z, z, z, 1, z, 1, z, 1, 1, z^2, z^2, z, 1, z^2, 1, z, z^2, 1, z^2, 1, 1, 1, z, z^2, z, z^2, 1, 1, 1,$
$z, z, 1, z^2, 1, 1, 1, z, z^2, z^2, z, 1, z, z, z^2, 1, 1, 1, z^2, z^2, z^2, 1, z, z, 1, 1, 1, 1, 1, z^2, z,$
$1, z, 1, z, 1, 1, z^2, z^2, z, z^2, 1, 1, z^2, 1, 1, 1, z, 1, 1, 1, z^2, z, z^2, z^2, z^2, 1, z^2, z^2, 1, 1,$
$z^2, z^2, z^2, 1, z, 1, z^2, z, z^2, z, 1, z^2, z, z, z, 1, z, 1, z, z, z, 1, 1, 1, z^2, 1, z^2, z^2, z^2, 1, 1,$
$1, z^2, 1, z, z, z, z^2, 1, z, z^2, z, 1, z, 1, 1, z, z, 1, z, z^2, 1, 1, 1, z^2, z, z, z, z, z, z^2, 1,$
$z^2, z^2, 1, 1, z^2, z, z, z^2, z^2, z, 1, z^2, z, 1, z^2, z, z^2, z^2, 1, z^2, z, z^2, z^2, 1, z^2, z^2, z^2, 1, z,$
$z^2, 1, z^2, z, z^2, 1, 1, 1, 1, z^2, 1, 1, z, 1, 1, z^2, z, z, z, z, z, z^2, 1, 1, 1, z^2, 1, z, z, z^2, 1,$
$z^2, z^2, z, z^2, 1, z^2, 1, z, z, 1, 1, z^2, 1, z, 1, z^2, z, 1, 1, z^2, z, 1, 1, 1, z, z^2, z, z^2, z^2, 1,$
$z^2, z^2, 1, z, z, 1, z^2, 1, z, 1, 1, z, z^2, z^2, z, z^2, z^2, z^2, z, z^2, z, z^2, z, z, 1, 1, z^2, z, 1, z,$
$z^2, 1, z, 1, z, z, z, z^2, 1, z^2, 1, z, z, z, z^2, z^2, z, 1, z, z, 1, z^2, 1, 1, z^2, z, z^2, z^2, 1, z, z,$
$z, 1, 1, 1, z, z^2, z^2, z, z, z, z, z, 1, z^2, z, z^2, z, z^2, z, z, 1, 1, z^2, 1, z, z, 1, z, z, z, z^2,$
$z, z, z, 1, z^2, 1, 1, 1, z, 1, 1, z, z, 1, 1, 1, z, z^2, z, 1, z^2, 1, z^2, z, 1, z^2, z^2, z^2, z, z^2, z,$
$z^2, z^2, z^2, z, z, z, 1, z, 1, 1, 1, z, z, z, 1, z, z^2, z^2, z^2, 1, z, z^2, 1, z^2, z, z^2, z, z, z^2, z^2,$

$z,z^2,1,z,z,z,1,z^2,z^2,z^2,z^2,z^2,1,z,1,1,z,z,1,z^2,z^2,1,1,z^2,z,1,z^2,z,1,z^2,$
$1,1,z,1,z^2,1,1,z,1,1,1,z,z^2,1,z,1,z^2,1,z,z,z,z,1,z,z,z^2,z,z,1,z^2,z^2,$
$z^2,z^2,z^2,1,z,z,z,1,z,z^2,z^2,1,z,1,1,z^2,1,z,1,z,z^2,z^2,z,z,1,z,z^2,z,1,z^2,$
$z,z,1,z^2,z,z,z,z^2,1,z^2,1,1,z,1,1,z,z^2,z^2,z,1,z,z^2,z,z,z^2,1,1,z^2,1,1,1,$
$z^2,1,z^2,1,z^2,z^2,z,z,1,z^2,z,z^2,1,z,z^2,z,z^2,z^2,z^2,1,z,1,z,z^2,z^2,z^2,1,1,z^2,$
$z,z^2,z^2,1,1,z,z,1,z^2,1,1,z,z^2,z^2,z^2,z,z,z,z^2,1,1,z^2,z^2,z^2,z^2,z^2,z,1,z^2,$
$1,z^2,1,z^2,z^2,z,z,1,z,z^2,z^2,z,z^2,z^2,z^2,1,z^2,z^2,z^2,z,1,z,z,z,z^2,z,z,z^2,z^2,$
$z,z,z,z^2,1,z^2,z,1,z,1,z^2,z,1,1,1,z^2,1,z^2,1,1,1,z^2,z^2,z^2,z,z^2,z,z,z,z^2,$
$z^2,z^2,z,z^2,1,1,1,z,z^2,1,z,1,z^2,1,z^2,z^2,1,1,z^2,1,z,z^2,z^2,z^2,z,1,1,1,1,1,$
$z,z^2,z,z,z^2,z^2,z,1,1,z,z,1,z^2,z,1,z^2,z,1,z,z,z^2,z,1,z,z,z^2,z,z,z,z^2,1,$
$z,z^2,z,1,z,z^2,z^2,z^2,z^2,z,z^2,z^2,1,z^2,z^2,z,1,1,1,1,1,z,z^2,z^2,z^2,z,z^2,1,1,z,$
$z^2,z,z,1,z,z^2,z,z^2,1,1,z^2,z^2,z,z^2,1,z^2,z,1,z^2,z^2,z,1,z^2,z^2,z^2,1,z,1,z,z,$
$z^2,z,z,z^2,1,1,z^2,z,z^2,1,z^2,z^2,1,z,z\}$

$\Theta_{\boldsymbol{s}}(\tau)=${771,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,766,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,766,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0}

Example 4.5.8

$$\begin{array}{c} Alphabet\ size: m = 5 \\ M - Array\ Dimension: 255 \times 257 \end{array}$$

Near perfect sequence of length 1285

$\boldsymbol{s} = \{1, z^2, z^4, z^4, z^4, 1, z, z, z^4, z^4, z^3, z^3, 1, z, z, z^3, z^3, z^3, z^4, z, z, z^2, z, z^3, z^4, z^2, z^3,$
$z, z^2, z^2, z, z^3, 1, z^2, z^4, z, 1, z^2, z, 1, z^4, z^3, z^2, z^4, 1, 1, z^3, z^3, z, z, 1, z^2, z^2, z^3, z^2,$
$z^2, z^3, z^4, z^3, z^4, z^4, z^3, z^4, z, z^2, 1, z, z, z, z^2, z^3, z^2, z, z^3, z, z^2, z^3, z^2, 1, z, z^3, 1, 1,$
$z, 1, z^4, z^3, z^3, 1, 1, z^4, z^4, z, z^4, z^2, z^2, z^4, z^2, z^4, z^2, z^4, 1, z, z^2, z^3, z^3, z, z^4, z^4, z^3,$
$z^3, z^4, z^4, z^2, z, z^3, z^3, z^3, z, z, z^2, z^4, z^4, z, z^3, z^4, z^2, z^4, z^2, z, z^4, z^2, z^2, z^4, 1, z, z^3,$
$z^4, z^3, z^3, z^2, z^4, z^2, z, 1, z, 1, z^3, z^4, z^2, 1, z^4, z, 1, z, z, 1, z^3, z, z^3, 1, z^3, z, z^3, 1, z^3,$
$z^2, z, z^4, z^2, z, 1, z^3, z, z^3, z^4, z^4, z, 1, z^2, 1, z^3, z^3, z, z^3, z^3, 1, z^2, 1, z^4, z, z^2, z^4, z^4,$
$z^3, z^3, z^3, z^2, z^3, z, z^4, z, z^4, z^3, z, z, 1, z^4, 1, z^4, z^4, 1, z^3, z^4, 1, z^4, z, z^4, 1, 1, z, z^3,$
$z^4, z^2, 1, z, z, z, z, z, 1, z^3, z^2, 1, z^4, 1, z^3, z, 1, z, z^3, z^4, z^3, z^4, z, z^3, 1, 1, z, 1, z^4,$
$z^4, z^2, z^4, z^4, z^4, z^2, z, z^3, 1, 1, 1, z, z^2, z^2, 1, 1, z^4, z^4, z, z^2, z^2, z^4, z^4, z^4, 1, z^2, z^2, z^3,$
$z^2, z^4, 1, z^3, z^4, z^2, z^3, z^3, z^2, z^4, z, z^3, 1, z^2, 1, z^3, z^2, z, 1, z^4, z^3, 1, z, z, z^4, z^4, z^2, z^2,$
$z, z^3, z^3, z^4, z^3, z^3, z^4, 1, z^4, 1, 1, z^4, 1, z^2, z^3, z, z, z^2, z^2, z^2, z^3, z^4, z^3, z^2, z^4, z^2, z^3, z^4,$
$z^3, z, z^2, z^4, z, z, z^2, z, 1, z^4, z^4, z, z, 1, 1, z^2, 1, z^3, z^3, 1, z^3, 1, z^3, 1, z, z^2, z^3, z^4, z^4,$
$z^2, 1, 1, z^4, z^4, 1, 1, z^3, z^2, z^4, z^4, z^4, z^2, z^2, z^3, 1, 1, z^2, z^4, 1, z^3, 1, z^3, z^2, 1, z^3, z^3, 1,$
$z, z^2, z^4, 1, z^4, z^4, z^3, 1, z^3, z^2, z, z^2, z, z^4, 1, z^3, z, 1, z^2, z, z^2, z^2, z, z^4, z^2, z^4, z, z^4,$
$z^2, z^4, z, z^4, z^3, z^2, 1, z^3, z^2, z, z^4, z^2, z^4, 1, 1, z^2, z, z^3, z, z^4, z^4, z^2, z^4, z^4, z, z^3, z, 1,$
$z^2, z^3, 1, 1, z^4, z^4, z^4, z^3, z^4, z^2, 1, z^2, 1, z^4, z^2, z^2, z, 1, z, 1, 1, z, z^4, 1, z, 1, z^2, 1, z,$
$z, z^2, z^4, 1, z^3, z, z^2, z^2, z^2, z^2, z^2, z, z^4, z^3, z, 1, z, z^4, z^2, z, z^2, z^4, 1, z^4, 1, z^2, z^4, z,$
$z, z^2, z, 1, 1, z^3, 1, 1, 1, z^3, z^2, z^4, z, z, z, z^2, z^3, z^3, z, z, 1, 1, z^2, z^3, z^3, 1, 1, 1, z, z^3,$
$z^3, z^4, z^3, 1, z, z^4, 1, z^3, z^4, z^4, z^3, 1, z^2, z^4, z, z^3, 1, z^4, z^3, z^2, z, 1, z^4, z, z^2, z^2, 1, 1,$
$z^3, z^3, z^2, z^4, z^4, 1, z^4, z^4, 1, z, 1, z, z, 1, z, z^3, z^4, z^2, z^3, z^3, z^3, z^4, 1, z^4, z^3, 1, z^3, z^4,$
$1, z^4, z^2, z^3, 1, z^2, z^2, z^3, z^2, z, 1, 1, z^2, z^2, z, z, z^3, z, z^4, z^4, z, z^4, z, z^4, z, z^2, z^3, z^4,$
$1, 1, z^3, z, z, 1, 1, z, z, z^4, z^3, 1, 1, 1, z^3, z^3, z^4, z, z, z^3, 1, z, z^4, z, z^4, z^3, z, z^4, z^4, z,$
$z^2, z^3, 1, z, 1, 1, z^4, z, z^4, z^3, z^2, z^3, z^2, 1, z, z^4, z^2, z, z^3, z^2, z^3, z^3, z^2, 1, z^3, 1, z^2, 1,$
$z^3, 1, z^2, 1, z^4, z^3, z, z^4, z^3, z^2, 1, z^3, 1, z, z, z^3, z^2, z^4, z^2, 1, 1, z^3, 1, 1, z^2, z^4, z^2, z,$
$z^3, z^4, z, z, 1, 1, 1, z^4, 1, z^3, z, z^3, z, 1, z^3, z^3, z^2, z, z^2, z, z, z^2, 1, z, z^2, z, z^3, z, z^2,$
$z^2, z^3, 1, z, z^4, z^2, z^3, z^3, z^3, z^3, z^3, z^2, 1, z^4, z^2, z, z, z^2, 1, z^3, z^2, z^3, 1, z, 1, z, z^3, 1, z^2,$
$z^2, z^3, z^2, z, z, z^4, z, z, z, z^4, z^3, 1, z^2, z^2, z^2, z^3, z^4, z^4, z^2, z^2, z, z, z^3, z^4, z^4, z, z, z,$
$z^2, z^4, z^4, 1, z^4, z, z^2, 1, z, z^4, 1, 1, z^4, z, z^3, 1, z^2, z^4, 1, 1, z^4, z^3, z^2, z, 1, z^2, z^3, z^3, z,$
$z, z^4, z^4, z^3, 1, 1, z, 1, 1, z, z^2, z, z^2, z^2, z, z^2, z^4, 1, z^3, z^4, z^4, z^4, 1, z, 1, z^4, z, z^4, 1,$
$z, 1, z^3, z^4, z, z^3, z^3, z^4, z^3, z^2, z, z, z^3, z^3, z^2, z^2, z^4, z^2, 1, 1, z^2, 1, z^2, 1, z^2, z^3, z^4, 1,$
$z, z, z^4, z^2, z^2, z, z, z^2, z^2, 1, z^4, z, z, z, z^4, z^4, 1, z^2, z^2, z^4, z, z^2, 1, z^2, 1, z^4, z^2, 1, 1,$
$z^2, z^3, z^4, z, z^2, z, z, 1, z^2, 1, z^4, z^3, z^4, z^3, z, z^2, 1, z^3, z^2, z^4, z^3, z^4, z^4, z^3, z, z^4, z, z^3,$
$z, z^4, z, z^3, z, 1, z^4, z^2, 1, z^4, z^3, z, z^4, z, z^2, z^2, z^4, z^3, 1, z^3, z, z, z^4, z, z, z^3, 1, z^3, z^2,$
$z^4, 1, z^2, z^2, z, z, z, 1, z, z^4, z^2, z^4, z^2, z, z^4, z^4, z^3, z^2, z^3, z^2, z^2, z^3, z, z^2, z^3, z^2, z^4,$
$z^2, z^3, z^3, z^4, z, z^2, 1, z^3, z^4, z^4, z^4, z^4, z^4, z^3, z, 1, z^3, z^2, z^3, z, z^4, z^3, z^4, z, z^2, z, z^2,$
$z^4, z, z^3, z^3, z^4, z^3, z^2, z^2, 1, z^2, z^2, z^2, 1, z^4, z, z^3, z^3, z^3, z^4, 1, 1, z^3, z^3, z^2, z^2, z^4, 1,$
$1, z^2, z^2, z^2, z^3, 1, 1, z, 1, z^2, z^3, z, z^2, 1, z, z, 1, z^2, z^4, z, z^3, 1, 1, z, 1, z^4, z^3, z^2, z,$
$z^3, z^4, z^4, z^2, z^2, 1, 1, z^4, z, z, z^2, z, z, z^2, z^3, z^2, z^3, z^3, z^2, z^3, 1, z, z^4, 1, 1, 1, z, z^2, z,$
$1, z^2, 1, z, z^2, z, z^4, 1, z^2, z^4, z^4, 1, z^4, z^3, z^2, z^2, z^4, z^4, z^3, z^3, 1, z^3, z, z, z^3, z, z^3, z,$
$z^3, z^4, 1, z, z^2, z^2, 1, z^3, z^3, z^2, z^2, z^3, z^3, z, 1, z^2, z^2, z^2, 1, 1, z, z^3, z^3, 1, z^2, z^3, z, z^3,$
$z, 1, z^3, z, z, z^3, z^4, 1, z^2, z^3, z^2, z^2, z, z^3, z, 1, z^4, 1, z^4, z^2, z^3, z, z^4, z^3, 1, z^4, 1, 1, z^4,$
$z^2, 1, z^2, z^4, z^2, 1, z^2, z^4, z^2, z, 1, z^3, z, 1, z^4, z^2, 1, z^2, z^3, z^3, 1, z^4, z, z^4, z^2, z^2, 1, z^2,$
$z^2, z^4, z, z^4, z^3, 1, z, z^3, z^3, z^2, z^2, z^2, z, z^2, 1, z^3, 1, z^3, z^2, 1, 1, z^4, z^3, z^4, z^3, z^3, z^4,$

$z^2, z^3, z^4, z^3, 1, z^3, z^4, z^4, 1, z^2, z^3, z, z^4, 1, 1, 1, 1, 1, z^4, z^2, z, z^4, z^3, z^4, z^2, 1, z^4, 1,$
$z^2, z^3, z^2, z^3, 1, z^2, z^4, z^4, 1, z^4, z^3, z^3, z, z^3, z^3, z^3, z\}$

$\Theta_s(\tau)=${1285,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1275.96,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,1281.55,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,1281.55,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1275.96,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0}

Example 4.5.9

Alphabet size: $m = 3$ *Array Dimension*: 1023×1025

Near perfect sequence of length 3075

$\boldsymbol{s} = \{1, z, 1, z^2, z^2, 1, z^2, z, 1, 1, 1, 1, z, 1, z, z^2, z^2, z, z, 1, 1, z^2, 1, z^2, z^2, z, 1, 1, z,$
$1, z^2, 1, z^2, z^2, z^2, 1, z^2, z^2, z, z, z^2, z^2, z^2, z^2, z^2, 1, z, z^2, z, z^2, z, z^2, z^2, 1, 1, z^2, 1, 1,$
$z^2, z^2, z, 1, z^2, z^2, z^2, z^2, 1, z, 1, z, z^2, z^2, z, z^2, z, z^2, z, 1, z^2, z, z^2, 1, z, 1, 1, z^2, z, 1,$
$z, z^2, z, z, z, z^2, z^2, z, z, z, z, z^2, 1, z^2, z, 1, z, z, 1, z, 1, z^2, 1, z^2, z^2, 1, z, 1, 1, 1, z,$
$z^2, z, 1, z, 1, z, z^2, z, 1, z, z^2, z, 1, z, z^2, z^2, z^2, z^2, z^2, 1, z^2, z, z^2, z, 1, z^2, z^2, 1, z, z,$
$z, z, z^2, 1, 1, 1, z, z, z^2, z, 1, z^2, 1, z, z, z, z^2, z^2, z, 1, z, z^2, 1, z^2, 1, z, z^2, 1, z, z^2, z^2,$
$z, 1, z^2, 1, 1, 1, z, z^2, 1, z, z, z^2, 1, 1, 1, z, 1, z, z^2, z, z, 1, z, z, z, 1, z, 1, z, 1, z, z,$
$z^2, z^2, z, z, z, 1, z^2, 1, 1, z, 1, z, z^2, z, z^2, z^2, z, z, 1, z^2, z^2, z, z, 1, 1, 1, z, 1, 1, z, 1,$
$z, 1, z, z, z, z, z, 1, z, z^2, z^2, z, 1, z^2, z, 1, 1, z^2, z, z^2, z^2, 1, 1, z, z^2, z, 1, 1, 1, z, z^2,$
$z, 1, z^2, z^2, z^2, 1, z^2, 1, 1, 1, z^2, z, z^2, 1, 1, z^2, z^2, z^2, z, z^2, z, z^2, 1, 1, 1, z^2, z^2, z^2, z^2,$
$z^2, z^2, z, 1, z^2, 1, z^2, z, 1, z, 1, 1, z, 1, z, 1, 1, 1, z^2, 1, z, z, z, z, 1, z, z, z, z^2, z, z, 1,$
$1, z^2, z^2, 1, z, z^2, z^2, 1, z^2, z, z^2, 1, z, z^2, z, z, z, z^2, z^2, z^2, z, z^2, 1, z, z^2, z^2, z, 1, z, 1,$
$z^2, z^2, 1, z, z^2, 1, 1, 1, z, 1, z, z^2, 1, z^2, z^2, z, z, 1, 1, z, 1, z^2, 1, 1, z^2, z, 1, z, z^2, z^2, z,$
$1, 1, z, z, z^2, z, z, z^2, z^2, z^2, z^2, 1, 1, 1, 1, z^2, z, 1, z^2, z, z, 1, z^2, 1, z, z, z^2, z^2, z, 1, 1,$
$z^2, 1, z, z, z, 1, z^2, 1, 1, z, 1, z^2, z^2, z^2, z^2, 1, z, 1, z^2, z^2, z^2, 1, z, 1, z, 1, z, z, z, 1, 1,$
$1, 1, 1, 1, z^2, 1, z, z, 1, z^2, z, 1, z, z, z^2, z^2, 1, z^2, z^2, 1, z^2, z, z, 1, 1, z^2, z^2, z^2, z, z, 1,$
$z, z, z^2, 1, 1, z, 1, z, z, z, 1, z^2, z^2, z, z^2, z, z^2, z^2, 1, 1, z, z, 1, z^2, 1, 1, z^2, z^2, 1, z, z,$
$z^2, z, 1, z, z^2, z, z^2, 1, z, z^2, z, 1, z, z, z, z, 1, z, z^2, 1, z, z^2, 1, 1, z, z^2, 1, 1, 1, z^2, 1,$
$z^2, z, z^2, 1, 1, 1, 1, z, 1, z, 1, z^2, 1, z, 1, z^2, z, z^2, 1, z^2, z^2, z^2, z^2, 1, 1, 1, z, 1, z^2, z, 1,$
$z, z^2, z^2, z^2, 1, z, z, z, z^2, 1, 1, z, z, z, z^2, 1, z^2, z, z, z^2, 1, z^2, z^2, 1, 1, 1, z, z, 1, z, z,$
$z, z, z^2, 1, z^2, z, 1, 1, z^2, 1, z^2, z, z, z^2, 1, 1, 1, 1, z^2, z^2, 1, z, z^2, z^2, z^2, z^2, z^2, 1, 1, z,$
$z, 1, z, z^2, z^2, 1, z, 1, z^2, z, z, z, z, 1, 1, z^2, 1, 1, z^2, 1, z^2, 1, 1, z, z, z^2, 1, z, 1, z^2, z,$
$1, z, 1, 1, z^2, z^2, 1, z^2, z, z, z^2, z^2, z^2, 1, z^2, z^2, z^2, z, z, z^2, z^2, z, z, 1, 1, z^2, 1, z, z, z^2,$
$z, 1, z^2, z^2, z^2, z^2, 1, z^2, z^2, z^2, 1, 1, 1, z^2, z, z, z^2, 1, z^2, z^2, z, z, z^2, 1, 1, 1, z^2, z^2, 1,$
$z, 1, 1, 1, 1, z^2, 1, 1, z, 1, 1, z, z, z, z^2, 1, z, 1, 1, 1, 1, 1, 1, 1, 1, z^2, z^2, z, 1, 1, z^2, z,$
$1, 1, z, z, 1, 1, z^2, 1, 1, z^2, z, z^2, z^2, 1, z, z^2, 1, z^2, z, 1, z, 1, z, z, z, z^2, 1, 1, 1, 1, 1,$
$1, z^2, 1, 1, z^2, z, z, z^2, z^2, 1, z, z^2, 1, z, 1, z, z, z, 1, 1, z, z^2, 1, z^2, z, z^2, z^2, z, 1, 1, z,$
$1, 1, z^2, z^2, z^2, z, z^2, z^2, z, z^2, 1, 1, z, z, z^2, z^2, z^2, z, z, 1, 1, z, z, z, z, z, 1, 1, 1, 1, 1,$
$z, z^2, z, z^2, z, 1, z, z^2, 1, z^2, z^2, z^2, 1, z^2, z, z, z^2, 1, z, z, z, z^2, z^2, 1, z, 1, z^2, z, 1, 1,$
$z^2, z, 1, z^2, 1, z^2, z^2, z, z, 1, z^2, 1, z^2, 1, z^2, 1, z, z, 1, z, z, 1, z^2, z^2, z, z, z^2, z, z, z, 1,$
$z, z, z, z^2, 1, z, 1, 1, z^2, z, z^2, z^2, 1, z, z^2, 1, z, 1, z, 1, 1, 1, z^2, 1, 1, z^2, z, 1, z^2, z, z^2,$
$1, z^2, z, z, z^2, z^2, 1, 1, 1, 1, z, z^2, 1, z, 1, z, z, z, 1, z, z, 1, 1, z^2, 1, z^2, z^2, z^2, z^2, z, z, z,$
$1, 1, z^2, z, 1, z^2, z, 1, z^2, z^2, 1, z, z^2, z, 1, z, 1, 1, z, 1, z, z, 1, z^2, z, z, z^2, 1, z^2, z^2, z,$
$1, z, z^2, z, z, 1, 1, z, z^2, z, z, z, 1, z^2, 1, z^2, z, z, z^2, z, 1, z^2, z^2, z^2, z^2, 1, z^2, 1, z, z, 1,$
$1, z^2, z^2, z, z^2, z, z, 1, z^2, z^2, 1, z^2, z, z^2, z, z, z, z^2, z, z, 1, 1, z, z, z, z, z, z^2, 1, z, 1,$
$z, 1, z, z, z^2, z^2, z, z^2, z^2, z, z, 1, z^2, z, z, z, z, z^2, 1, z^2, 1, z, z, 1, z, 1, z, 1, z^2, z, 1,$
$z, z^2, 1, z^2, z^2, z, 1, z^2, 1, z, 1, 1, 1, z, z, 1, 1, 1, 1, z, z^2, z, 1, z^2, 1, 1, z^2, 1, z^2, z, z^2,$
$z, z, z^2, 1, z^2, z^2, z^2, 1, z, 1, z^2, 1, z^2, 1, z, 1, z^2, 1, z, 1, z^2, 1, z, z, z, z, z, z^2, z, 1, z,$
$1, z^2, z, z, z^2, 1, 1, 1, 1, z, z^2, z^2, z^2, 1, 1, z, 1, z^2, z, z^2, 1, 1, 1, z, z, 1, z^2, 1, z, z^2, z,$

$z^2,1,z,z^2,1,z,z,1,z^2,z,z^2,z^2,z^2,1,z,z^2,1,1,z,z^2,z^2,z^2,1,z^2,1,z,1,1,z^2,1,$
$1,1,z^2,1,z^2,1,z^2,1,1,z,z,1,1,1,z^2,z,z^2,z^2,1,z^2,1,z,1,z,z,1,1,z^2,z,z,1,$
$1,z^2,z^2,z^2,1,z^2,z^2,1,z^2,1,z^2,1,1,1,1,1,z^2,1,z,z,1,z^2,z,1,z^2,z^2,z,1,z,z,$
$z^2,z^2,1,z,1,z^2,z^2,z^2,1,z,1,z^2,z,z,z,z^2,z,z^2,z^2,z^2,z,1,z,z^2,z^2,z,z,z,1,z,$
$1,z,z^2,z^2,z^2,z,z,z,z,z,z,1,z^2,z,z^2,z,1,z^2,1,z^2,z^2,1,z^2,1,z^2,z^2,z^2,z,z^2,1,$
$1,1,1,z^2,1,1,1,z,1,1,z^2,z^2,z,z,z^2,1,z,z,z^2,z,1,z,z^2,1,z,1,1,1,z,z,z,1,$
$z,1,1,z,z,1,z^2,1,z^2,z,z,z^2,1,z,z^2,z^2,z^2,1,z^2,1,z,z^2,z,z,1,1,z^2,z^2,1,z^2,$
$z,z^2,z^2,z,1,z^2,1,z,z,1,z^2,z^2,1,1,z,1,1,z,z,z,z,z^2,z^2,z^2,z^2,z,1,z^2,z,1,1,$
$z^2,z,z^2,1,1,z,z,1,z^2,z^2,z,z^2,1,1,1,z^2,z,z^2,z^2,1,z^2,z,z,z,z,z^2,1,z^2,z,z,$
$z,z^2,1,z^2,1,z^2,1,1,1,z^2,z^2,z^2,z^2,z^2,z^2,z,z^2,1,1,z^2,z,1,z^2,1,1,z,z,z^2,z,z,$
$z^2,z,1,1,z^2,z^2,z,z,z,1,1,z^2,1,1,z,z^2,z^2,1,z^2,1,1,1,z^2,z,z,1,z,1,z,z,z^2,$
$z^2,1,1,z^2,z,z^2,z^2,z,z,z^2,1,1,z,1,z^2,1,z,1,z,z^2,1,z,1,z^2,1,1,1,1,z^2,1,z,$
$z^2,1,z,z^2,z^2,1,z,z^2,z^2,z^2,z,z^2,z,1,z,z^2,z^2,z^2,z^2,1,z^2,1,z^2,z,z^2,1,z^2,z,1,$
$z,z^2,z,z,z,z,z^2,z^2,z^2,1,z^2,z,1,z^2,1,z,z,z,z^2,1,1,1,z,z^2,z^2,1,1,1,z,z^2,z,$
$1,1,z,z^2,z,z,z^2,z^2,z^2,1,1,z^2,1,1,1,1,z,z^2,z,1,z^2,z^2,z,z^2,z,1,1,z,z^2,z^2,$
$z^2,z^2,z,z,z^2,1,z,z,z,z,z,z^2,z^2,1,1,z^2,1,z,z,z^2,1,z^2,z,1,1,1,1,z^2,z^2,z,$
$z^2,z^2,z,z^2,z,z^2,z^2,1,1,z,z^2,1,z^2,z,1,z^2,1,z^2,z^2,z,z,z^2,z,1,1,z,z,z,z^2,z,$
$z,z,1,1,z,z,1,1,z^2,z^2,z,z^2,1,1,z,1,z^2,z,z,z,z,z^2,z,z,z,z^2,z^2,z^2,z,1,1,$
$z,z^2,z,z,1,1,z,z^2,z^2,z^2,z,z,z^2,1,z^2,z^2,z^2,z^2,z,z^2,z^2,1,z^2,z^2,1,1,1,z,z^2,$
$1,z^2,z^2,z^2,z^2,z^2,z^2,z^2,z,z,1,z^2,z^2,z,1,z^2,z^2,1,1,z^2,z^2,z,z^2,z^2,z,1,z,z,$
$z^2,1,z,z^2,z,1,z^2,1,z^2,1,1,1,z,z^2,z^2,z^2,z^2,z^2,z^2,z,z^2,z^2,z,1,1,z,z,z^2,1,z,$
$z^2,1,z^2,1,1,1,z^2,z^2,1,z,z^2,z,1,z,z,1,z^2,z^2,1,z^2,z^2,z,z,z,1,z,z,1,z,z^2,$
$z^2,1,1,z,z,z,1,1,z^2,z^2,1,1,1,1,1,z^2,z^2,z^2,z^2,z^2,1,z,1,z,1,z^2,1,z,z^2,z,z,$
$z,z^2,z,1,1,z,z^2,1,1,1,z,z,z^2,1,z^2,z,1,z^2,z^2,z,1,z^2,z,z^2,z,z,1,1,z^2,z,z^2,$
$z,z^2,z,z^2,1,1,z^2,1,1,z^2,z,z,1,1,z,1,1,1,z^2,1,1,1,z,z^2,1,z^2,z^2,z,1,z,z,$
$z^2,1,z,z^2,1,z^2,1,z^2,z^2,z^2,z,z^2,z^2,z,1,z^2,z,1,z,z^2,z,1,z,z,z^2,z^2,z^2,z^2,1,$
$z,z^2,1,z^2,1,1,1,z^2,1,1,z^2,z^2,z,z^2,z,z,z,z,1,1,1,z^2,z^2,z,1,z^2,z,1,z^2,z,z,$
$z^2,1,z,1,z^2,1,z^2,z^2,1,z^2,1,1,z^2,z,1,1,z,z^2,z,z,1,z^2,1,z,1,1,z^2,z^2,1,z,1,$
$1,1,z^2,z,z^2,z,1,1,z,1,z^2,z,z,z,z,z^2,z,z^2,1,1,z^2,z^2,z,z,1,z,1,1,z^2,z,z,$
$z^2,z,1,z,1,1,1,z,1,1,z^2,z^2,1,1,1,1,1,z,z^2,1,z^2,1,z^2,1,1,z,z,1,z,z,1,1,$
$z^2,z,1,1,1,1,z,z^2,z,z^2,1,1,z^2,1,z^2,1,z^2,z,1,z^2,1,z,z^2,z,z,z,1,z^2,z,z^2,1,$
$z^2,z^2,z^2,1,1,z^2,z^2,z^2,z^2,1,z,1,z^2,z,z^2,z^2,z,z^2,z,1,z,1,1,z,z^2,z,z,z,z^2,1,$
$z^2,z,z^2,z,z^2,1,z^2,z,z^2,1,z^2,z,z^2,1,1,1,1,1,z,1,z^2,1,z^2,z,1,1,z,z^2,z^2,z^2,$
$z^2,1,z,z,z,z^2,z^2,1,z^2,z,1,z,z^2,z^2,z^2,1,1,z^2,z,z^2,1,z,1,z,z^2,1,z,z^2,1,1,$
$z^2,z,1,z,z,z,z^2,1,z,z^2,z^2,1,z,z,z,z^2,z,z^2,1,z^2,z^2,z,z^2,z^2,z^2,z,z^2,z,z^2,z,$
$z^2,z^2,1,1,z^2,z^2,z^2,z,1,z,z,z^2,z,z^2,1,z^2,1,1,z^2,z^2,z,1,1,z^2,z^2,z,z,z,z^2,z,$
$z,z^2,z,z^2,z,z^2,z^2,z^2,z^2,z^2,z,z^2,1,1,z^2,z,1,z^2,z,z,1,z^2,1,1,z,z,z^2,1,z^2,z,$
$z,z,z^2,1,z^2,z,1,1,1,z,1,z,z,z,1,z^2,1,z,z,1,1,1,z^2,1,z^2,1,z,z,z,1,1,1,$
$1,1,1,z^2,z,1,z,1,z^2,z,z^2,z,z,z^2,z,z^2,z,z,z,1,z,z^2,z^2,z^2,z^2,z,z^2,z^2,z^2,1,$
$z^2,z^2,z,z,1,1,z,z^2,1,1,z,1,z^2,1,z,z^2,1,z^2,z^2,z^2,1,1,1,z^2,1,1,z^2,1,1,z^2,$
$z,z^2,z,1,1,z,z^2,1,z,z,z,z^2,z,z^2,1,z,1,1,z^2,z^2,z,z,z^2,z,1,z,z,1,z^2,z,z^2,$
$1,1,z^2,z,z,z^2,z^2,1,z^2,z^2,1,1,1,1,z,z,z,z,1,z^2,z,1,z^2,z^2,z,1,z,z^2,z^2,1,1,$
$z^2,z,z,1,z,z^2,z^2,z^2,z,1,z,z,z^2,z,1,1,1,1,z,z^2,z,1,1,1,z,z^2,z,z^2,z,z^2,z^2,$
$z^2,z,z,z,z,z,z,1,z,z^2,z^2,z,1,z^2,z,z^2,z^2,1,1,z,1,1,z,1,z^2,z^2,z,z,1,1,1,$
$z^2,z^2,z,z^2,z^2,1,z,z,z^2,z,z^2,z^2,z^2,z,1,1,z^2,1,z^2,1,1,z,z,z^2,z^2,z,1,z,z,1,$
$1,z,z^2,z^2,1,z^2,z,z^2,1,z^2,1,z,z^2,1,z^2,z,z^2,z^2,z^2,z^2,z,z^2,1,z,z^2,1,z,z,z^2,$
$1,z,z,z,1,z,1,z^2,1,z,z,z,z,z^2,z,z^2,z,1,z,z^2,z,1,z^2,1,z,1,1,1,1,z,z,z,$
$z^2,z,1,z^2,z,z^2,1,1,1,z,z^2,z^2,z^2,1,z,z,z^2,z^2,z^2,1,z,1,z^2,z^2,1,z,1,1,z,z,$

$z,z^2,z^2,z,z^2,z^2,z^2,z^2,1,z,1,z^2,z,z,1,z,1,z^2,z^2,1,z,z,z,z,1,1,z,z^2,1,1,1,$
$1,1,z,z,z^2,z^2,z,z^2,1,1,z,z^2,z,1,z^2,z^2,z^2,z^2,z,z,1,z,z,1,z,1,z,z,z^2,z^2,1,$
$z,z^2,z,1,z^2,z,z^2,z,z,1,1,z,1,z^2,z^2,1,1,1,z,1,1,1,z^2,z^2,1,1,z^2,z^2,z,z,1,$
$z,z^2,z^2,1,z^2,z,1,1,1,1,z,1,1,1,z,z,z,1,z^2,z^2,1,z,1,1,z^2,z^2,1,z,z,z,1,$
$1,z,z^2,z,z,z,z,1,z,z,z^2,z,z,z^2,z^2,z^2,1,z,z^2,z,z,z,z,z,z,z,z,1,1,z^2,z,$
$z,1,z^2,z,z,z^2,z^2,z,z,1,z,z,1,z^2,1,1,z,z^2,1,z,1,z^2,z,z^2,z,z^2,z^2,z^2,1,z,z,$
$z,z,z,z,1,z,z,1,z^2,z^2,1,1,z,z^2,1,z,z^2,z,z^2,z^2,z^2,z,z,z^2,1,z,1,z^2,1,1,z^2,$
$z,z,z^2,z,z,1,1,1,z^2,1,1,z^2,1,z,z,z^2,z^2,1,1,1,z^2,z^2,z,z,z^2,z^2,z^2,z^2,z^2,z,$
$z,z,z,z,z^2,1,z^2,1,z^2,z,z^2,1,z,1,1,1,z,1,z^2,z^2,1,z,z^2,z^2,z^2,1,1,z,z^2,z,1,$
$z^2,z,z,1,z^2,z,1,z,1,1,z^2,z^2,z,1,z,1,z,1,z,z^2,z^2,z,z^2,z^2,z,1,1,z^2,z^2,1,$
$z^2,z^2,z^2,z,z^2,z^2,z^2,1,z,z^2,z,z,1,z^2,1,1,z,z^2,1,z,z^2,z,z^2,z,z,z,1,z,z,1,$
$z^2,z,1,z^2,1,z,1,z^2,1,1,z,z,z,z,z^2,1,z,z^2,z,z^2,z^2,z^2,z,z^2,z^2,z,z,1,z,1,1,$
$1,1,z^2,z^2,z^2,z,z,1,z^2,z,1,z^2,z,1,1,z,z^2,1,z^2,z,z^2,z,z,z^2,z,z^2,z^2,z,1,z^2,$
$z^2,1,z,1,1,z^2,z,z^2,1,z^2,z^2,z,z,z^2,1,z^2,z^2,z^2,z\}$

$\Theta_{\boldsymbol{s}}(\tau) =$ {3075,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,3070.5,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,

0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,3070.5,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,

```
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0}
```

Though we have provided only the above mentioned examples, near perfect sequences of unbounded odd lengths can be obtained by our construction.

4.6 Proof of the main result

In this Section, we give the main result of this thesis, namely that near perfect sequences can be constructed for *unbounded* lengths.

Theorem 4.6.1

Near perfect sequences can be constructed for unbounded lengths, namely, $N = m(2^J + 1)$, where m is any odd prime and J is any positive integer greater than or equal to 2.

For the proof of this Theorem, we need the following lemmas and theorems.

Lemma 4.6.1 [65]

If t, u, v are integers with $t \geq 2, u \geq 1, v \geq 1$, then $(t^v - 1)$ *divides* $(t^u - 1)$ if and only if v *divides* u.

Proof:

We use the division algorithm to write $u = Qv + R \; where \; 0 \leq R < v$. Then we have,

$$\frac{t^u - 1}{t^v - 1} = \frac{t^{Qv+R} - 1}{t^v - 1}$$

$$= \; t^R . \frac{t^{Qv} - 1}{t^v - 1} + \frac{t^R - 1}{t^v - 1}$$

Since $t^{Qv} - 1 = (t^v - 1)(t^{(q-1)v} + \cdots + t^q + 1)$, $t^{Qv} - 1$ is divisible by $t^v - 1$.

Now, $\frac{t^R - 1}{t^v - 1}$ is less than one. Also, $\frac{t^u - 1}{t^v - 1}$ is an integer if and only if $R = 0$.

Therefore, $v \; divides \; u$. □

<u>*Example*:</u> Let $t = 2$. Then $(2^v - 1) \; divides \; (2^u - 1)$ if and only if $v \; divides \; u$.

Corollary 4.6.2

Let v_1 be the smallest integer such that $m \; divides \; (2^{v_1} - 1)$, where m is an odd prime. Then $m \; divides \; (2^{v_1 v_2} - 1)$ for any v_2.

Proof:

Put $u = v_1 v_2$ and $v = v_1$ in *Lemma 4.6.1*.

From *Lemma 4.6.1,* $(2^{v_1} - 1) \; divides \; (2^{v_1 v_2} - 1)$.

So, $m \; divides \; (2^{v_1 v_2} - 1)$.

Theorem 4.6.2 [43] For every prime p and every positive integer $\mathbb{m}$, there exists a finite field with $p^{\mathbb{m}}$ elements.

We denote this field by $GF(p^{\mathbb{m}})$.

Theorem 4.6.3 [43] Let $GF(p^{\mathbb{m}})$ be the finite field with $p^{\mathbb{m}}$ elements. Then every subfield of $GF(p^{\mathbb{m}})$ has order $p^{\mathbb{mm}}$ where $\mathbb{mm}$ is a positive divisor of $\mathbb{m}$. Conversely, if $\mathbb{mm}$ is a positive divisor of $\mathbb{m}$, then there is exactly one subfield of $GF(p^{\mathbb{m}})$ with $p^{\mathbb{mm}}$ elements.

Now we are ready to prove *Theorem 4.6.1*

Proof:

From Section 3.7, we know that an M-sequence of degree $\mathbb{m}$ can be constructed by the trace mapping from $GF(p^{\mathbb{m}})$ to $GF(p)$.

Theorem 4.6.2 shows that we can construct M-sequences for unbounded lengths. Now, if we take $p = 2$ and $\mathbb{m} = 2J$, then the row-wise folding of an M-sequence of length $2^{2J} - 1$ gives an almost square array $\mathbb{P}_{(2^J-1)\times(2^J+1)}$ (Section 3.7) with exactly one column of zeros. All the other columns of $\mathbb{P}_{(2^J-1)\times(2^J+1)}$ are cyclic shifts of an M-sequence of length $(2^J - 1)$, constructed from a trace mapping from $GF(2^J) \rightarrow GF(2)$. We obtain a shift sequence $\boldsymbol{e}$ from $\mathbb{P}_{(2^J-1)\times(2^J+1)}$ containing exactly one ∞ (Equation 3.7.1).

We know from Theorem 4.6.3 that there exists $GF(2^J) \subset GF(2^{2J})$ for every J.

From *Corollary 4.6.2*, if m divides $(2^J - 1)$, for the smallest integer J, then m divides $(2^{2J} - 1)$.

We assume m as the alphabet size and construct an associated matrix $\mathbb{A}$, of size $m \times (2^J + 1)$ for $J \geq 2$. We obtain a shift sequence of length $(2^J + 1)$. These shift sequences are used to construct near perfect sequences.

Now we have two cases.

Case 1 The shift sequence $\boldsymbol{e}$ is not reduced (*Example 4.1.1*).

In this case, the shift sequence $\boldsymbol{e}$ satisfies the Distinct Difference Property (Subsection 3.7.1, Property 2) that guarantees near perfection.

Case 2 The shift sequence $\boldsymbol{e}$ is reduced (Section 4.4).

By Property 2 of reduced shift sequences in Subsection 4.4.1, we know that the differences $(e_{j+k} - e_j)\ mod(2^J - 1)$ are equally numerous. Again due to this property we obtain near perfection.

Hence in either case, when we unfold $\mathbb{A}$, we obtain a near perfect sequence of length $m(2^J + 1)$ for every $J \geq 2$.

■

4.7 Classification of near perfect sequences of length 15

In this Section, we classify the near perfect sequences of length 15 obtained by exhaustive computer search. We obtained 1080 near perfect sequences of length 15. There are near perfect sequences in the list which do not come from our construction. We give examples of each type (Type I, Type II, and Type III) of sequences for a better understanding of the classification.

Without any ambiguity, we may also refer to a sequence by its index sequence. The autocorrelation functions can still be calculated from this representation.

To make the computation easy, the following near perfect sequences of length 15 are described in terms of the indices (exponents of roots of unity). In the following examples we give the index sequences corresponding to the original near perfect sequence.

We call the near perfect sequences of length 15 obtained by our construction "sequences of Type I". Examples of Type I are provided in Section 4.5.

Now we see Type II and Type III near perfect sequences of length 15 which do not arise from our construction.

Example 4.7.1

We define a near perfect sequence of length 15 over 3 roots of unity, to be Type II, if it has a run of 4 identical entries.

For example, we have the following sequence:

$\boldsymbol{s_{ii}} = (0,0,0,0,2,0,1,0,0,2,1,0,1,1,2)$

The associated matrix for this sequence is

$$\mathbb{A} = \begin{bmatrix} 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 2 \\ 1 & 0 & 1 & 1 & 2 \end{bmatrix}$$

We take the perfect sequence $A_0 = (0,0,1)$ as the reference column. We see that the columns A_1, A_2, A_3 of the associated matrix are shifts of A_0. We assume the last column (2,2,2) contributes an ∞ to the shift sequence. We see that the shift sequence is $(0,1,0,0,\infty)$.

The autocorrelation values of $\boldsymbol{s_{ii}}$ are

$$\Theta_{\boldsymbol{s_{ii}}}(\tau) = (15,0,0,0,0,3,0,0,0,0,3,0,0,0,0)$$

Note: Examination of the computer generated, complete list of Type II sequences found that all their autocorrelation values were real.

We see another example which is different from Type I and Type II.

Example 4.7.2

From the exhaustive list, we have extracted another type of sequence, which has maximum run of three identical entries, and having 3 as the magnitude of the off-peak autocorrelation values. We give an example of this Type III near perfect sequence:

$\boldsymbol{s_{iii}} = (0,0,0,1,0,2,1,1,1,0,0,1,2,0,2)$

The associated matrix for $\boldsymbol{s_{iii}}$ is

$$\mathbb{A} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 2 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 0 & 2 \end{bmatrix}$$

The autocorrelation values of $\boldsymbol{s_{iii}}$ are

$$\Theta_{\boldsymbol{s_{iii}}}(\tau) = (15,0,0,0,0,-1.5 + 2.59808i, 0,0,0,0,-1.5 - 2.59808i, 0,0,0)$$

with the magnitude $\left|\Theta_{\boldsymbol{s_{iii}}}(\tau)\right| = (15,0,0,0,0,3,0,0,0,0,3,0,0,0,0)$

The table below describes the classification of all near perfect sequences of length 15 over three roots of unity, obtained by exhaustive computer search. We give an example of each type of sequence in Table 4.7.1.

We use the completely orthogonal pair $\boldsymbol{a} = (1, \omega, \omega^2); \boldsymbol{b} = (1,1,1)$ for Type I a and the completely orthogonal pair $\boldsymbol{a} = (1, \omega, \omega^2); \boldsymbol{b} = (1, \omega^2, \omega)$ for Type I b. Type I c is obtained by multiplying Type I a and I b by the consecutive powers $1, \omega, \omega^2$.

We have 360 sequences starting with 0 as the first entry in the index sequence. Similarly we have two more sets of 360 sequences each starting with entries 1 and 2 respectively. This sorts the complete list of 1080 near perfect sequences of length 15.

Type of Near Perfect Sequence	Example (Index sequence)	Number of equivalent sequences
Type I a	(0,1,0,0,0,1,2,1,1,0, 2,0,2,2,0),	60
Type I b	(0,1,0,0,0,1,2,1,1,2, 2,0,2,2,1)	60
Type I c	(0,2,2,0,1,0,2,2,0,0,0,2,2,0,2)	60
Type II	(0,0,0,0,2,0,1,0,0,2,1,0,1,1,2)	60
Type III	(0,0,0,1,0,2,1,1,1,0,0,1,2,0,2)	120

Table 4.7.1

4.8 Operations preserving near perfection of sequences over roots of unity

In this Section, we study operations that preserve the near perfect auto-correlation function.

Proofs of some basic properties of arbitrary sequences are the same as those over the roots of unity, which are easily proved. So we omit some simple proofs here.

We have seen some basic properties of perfect sequences over complex numbers in Section 3.1. Now we give the operations pertaining to near perfect sequences below. All the sequences considered below are over the roots of unity.

4.8.1 Shift of a near perfect sequence

Proposition 4.8.1: A sequence $\boldsymbol{s} = (s_0, s_1, s_2, \cdots, s_{N-1})$, is near perfect, if and only if any shift of $\boldsymbol{s}$ is near perfect.

4.8.2 Multiplying by a constant factor

Proposition 4.8.2: If each element of a sequence $\boldsymbol{s} = (s_0, s_1, s_2, \cdots, s_{N-1})$, is multiplied by a constant, the resulting sequence is also near perfect.

Proof:

Let $\boldsymbol{t} = (cs_0, cs_1, cs_2, \cdots, cs_{N-1})$, where c is a constant.

Consider the autocorrelation of the sequence $\boldsymbol{t}$, for any shift $0 \leq \tau \leq n-1$,

$$\Theta_{\boldsymbol{t}}(\tau) = \sum_{i=0}^{mn-1} (cs_i)(cs_{i+\tau})^*$$

$$= \sum_{i=0}^{n-1} cc^* (s_i s_{i+\tau}^*)$$

$$= \|c\| \sum_{i=0}^{n-1} s_i s_{i+\tau}^*$$

$$= \|c\| \Theta_{\mathbf{s}}(\tau)$$

Thus, $$\Theta_{\boldsymbol{t}}(\tau) = \begin{cases} \|c\|N & if \quad \tau = 0 \\ 0 & if \quad \Theta_{\mathbf{s}}(\tau) = 0 \\ \|c\|\Theta_{\boldsymbol{s}}(\tau) & if \quad \Theta_{\mathbf{s}}(\tau) \neq 0 \end{cases}$$

4.8.3 Conjugation of a near perfect sequence

Proposition 4.8.3: The conjugate of a near perfect sequence is also near perfect.

Proof:

Let $\boldsymbol{s} = (s_0, s_1, s_2, \cdots, s_{N-1})$ be a near perfect sequence. Then the conjugate of $\boldsymbol{s}$ is $\boldsymbol{s}^* = (s_0^*, s_1^*, \cdots, s_{N-1}^*)$. The autocorrelation calculation of $\boldsymbol{s}^*$ is

$$\Theta_{(\mathbf{s}^*)}(\tau) = \sum_{i=0}^{n-1} (s_i^*)\,(s_i^*)^*$$

$$= \sum_{i=0}^{n-1} (s_i^*)\,s_i = \Theta_{\boldsymbol{s}}(\tau)$$

4.8.4 Decimation of a near perfect sequence

Proposition 4.8.4: A proper decimation of a near perfect sequence over roots of unity is also near perfect and the non-zero off peak autocorrelation values are preserved and possibly rearranged.

To prove this Proposition, we first prove *Lemma 4.8.5.*

We see from the following Theorem that any proper decimation preserves the autocorrelation values.

Theorem 4.8.4 [64] Let $\boldsymbol{a} = \{a_n\}$ be an arbitrary sequence of complex numbers with period N, and let $\boldsymbol{c} = \{c_n\}$ be the decimation by t of $\{a_n\}$, where $gcd(t, N) = 1$. Then $\Theta_{\boldsymbol{c}}(\tau) = \Theta_{\boldsymbol{a}}(t\tau)$ where $\Theta_{\boldsymbol{a}}(\tau)$ denotes the autocorrelation value of $\boldsymbol{a}$ for $0 \leq \tau \leq N-1$.

We see a variation of *Theorem 4.8.4* in *Lemma 4.8.5.*

Lemma 4.8.4.1: A proper decimation of a sequence permutes the off-peak autocorrelation values of the original sequence.

Proof:

Let $\boldsymbol{a} = [a_0, a_1, \cdots, a_{N-1}]$ be any complex sequence of period N.

Take d such that $\gcd(N, d) = 1$.

Let $\boldsymbol{b} = [b_0, b_1, \cdots, b_{N-1}]$ be the decimation of $\boldsymbol{a}$ by d, where $b_i = a_{id}$ for $i = 0,1,2, \cdots, N-1$.

For $\tau = 0,1,2, \cdots, N-1$, we prove that $\Theta_\tau(\boldsymbol{b}) \in \Theta(\boldsymbol{a})$

We know that $\Theta_\tau(\boldsymbol{b}) = \sum_{i=0}^{N-1} b_i b_{i+\tau}^* = \sum_{i=0}^{N-1} a_{id} a_{(i+\tau)d}^*$ (4.8.1)

Now, there exists $i_0 \in \mathbb{N}$ such that $i_0 + \tau \equiv 0 \; mod \; N$.

So we can write Equation 4.8.1 as, $\Theta_\tau(\boldsymbol{b}) = \sum_{i=0}^{i_0-1} a_{id} a_{(i+\tau)d}^* + \sum_{i=i_0}^{N-1} a_{id} a_{(i+\tau)d}^*$

$$= \sum_{i=i_0}^{N-1} a_{id} a_{(i+\tau)d}^* + \sum_{i=0}^{i_0-1} a_{id} a_{(i+\tau)d}^*$$

$$= \sum_{i=i_0}^{N-1} a_{(i+\tau)d}^* \, a_{id} + \sum_{i=0}^{i_0-1} a_{(i+\tau)d}^* \, a_{id}.$$

That is, $\Theta_\tau(\boldsymbol{b}) = (a_{(i_0+\tau)d}^* a_{i_0 d} + a_{(i_0+1+\tau)d}^* a_{(i_0+1)d} + \cdots + a_{(N-1+\tau)d}^* a_{(N-1)d}) + (a_{\tau d}^* a_0 + \cdots + a_{(i_0-1+\tau)d}^* a_{(i_0-1)d})$

Let $k = i_0 d$.

Then,

$\Theta_\tau(\boldsymbol{b}) = \left(a_{0d}^* a_k + a_d^* a_{k+d} + a_{2d}^* a_{k+2d} + \cdots + a_{(\tau-1)d}^* a_{k+(\tau-1)d}\right) + (a_{\tau d}^* a_0 + \cdots + a_{(N-1)d}^* a_{k+(N-1)d})$ where all suffixes are calculated $modulo \; N$.

Since $\gcd(N, d) = 1$, $\{0d, 1d, 2d, \cdots (n-1)d\}$ is a permutation of $\{0,1,2, \cdots (n-1)\}$ that leaves 0 fixed.

So, $\Theta_\tau(\boldsymbol{b}) = a_0^* a_k + a_1^* a_k + a_2^* a_{k+2} + \cdots + a_{(N-1)}^* a_{k+(N-1)}$

$$= a_0^*(a_k{}^*)^* + a_1^*(a_{k+1}{}^*)^* + a_2^*(a_{k+2}{}^*)^* + \cdots + a_{(N-1)}^*(a_{k+N-1}{}^*)^*$$

$$= (a_0 a_k^* + a_1 a_{k+1}^* + a_2 a_{k+2}^* + \cdots + a_{N-1} a_{k+N-1}^*)^*$$

$$= (\Theta_k(\boldsymbol{a}))^*$$

That is, $\Theta_\tau(\boldsymbol{b}) = (\Theta_k(\boldsymbol{a}))^*$ where $k = i_0 d$. ■

Proof of *Proposition 4.8.4.*

Assume $\boldsymbol{a} = [a_0, a_1, \cdots, a_{N-1}]$ to be a near perfect sequence of length $N = 3(2^J + 1)$ where $J = 2,4,6, \cdots$.

Take the shift $\tau = \frac{N}{3} = (2^J + 1)$, for which the first non-zero off peak occurs.

We want to show that $\Theta_{\frac{N}{3}}(\boldsymbol{b}) = \begin{cases} \left(\Theta_{\frac{N}{3}}(\boldsymbol{a})\right)^* \\ \left(\Theta_{\frac{2N}{3}}(\boldsymbol{a})\right)^* \end{cases}$

We know that $\Theta_\tau(\boldsymbol{b}) = (\Theta_k(\boldsymbol{a}))^*$ where $k = i_0 d$, according to *Lemma 4.8.5.*

In this case, $i_0 = N - \tau = 3(2^J + 1) - (2^J + 1) = 2(2^J + 1) = \frac{2N}{3}$.

So, $\Theta_{\frac{N}{3}}(\boldsymbol{b}) = \left(\Theta_{2(2^J+1)d}(\boldsymbol{a})\right)^* = \left(\Theta_{\frac{2Nd}{3}}(\boldsymbol{a})\right)^*$

Since the suffixes are calculated *modulo* $N = 3(2^J + 1)$, we have that $2(2^J + 1)d$ is either $(2^J + 1) = \frac{N}{3}$ or $2(2^J + 1) = \frac{2N}{3}$, for any d such that $\gcd(N, d) = 1$.

Thus, we have $\Theta_{\frac{N}{3}}(\boldsymbol{b}) = \begin{cases} \left(\Theta_{\frac{N}{3}}(\boldsymbol{a})\right)^* \\ \left(\Theta_{\frac{2N}{3}}(\boldsymbol{a})\right)^* \end{cases}$

For $\tau = \frac{2N}{3} = 2(2^J + 1)$, the proof is similar. ■

Note: A similar proof holds for any odd prime number of roots of unity.

Example 4.8.4 Let us consider the index sequence of a near perfect sequence of length 15, $\boldsymbol{u} = (0,1,0,0,0,1,2,1,1,0,2,0,2,2,0)$. There are $\phi(15) = 8$ proper decimations of $\boldsymbol{u}$. The decimations of $\boldsymbol{u}$ are given below.

$\boldsymbol{u}[1] = (0,1,0,0,0,1,2,1,1,0,2,0,2,2,0)$ $\boldsymbol{u}[8] = (0,1,1,0,0,2,0,0,0,2,1,2,2,0,1)$

$\boldsymbol{u}[2] = (0,0,0,2,1,2,2,0,1,0,1,1,0,0,2)$ $\boldsymbol{u}[11] = (0,0,1,0,0,2,2,0,2,0,1,1,2,1,0)$

$\boldsymbol{u}[4] = (0,0,1,2,1,1,0,2,0,2,2,0,0,1,0)$ $\boldsymbol{u}[13] = (0,2,0,0,1,1,0,1,0,2,2,1,2,0,0)$

$\boldsymbol{u}[7] = (0,1,0,2,2,1,2,0,0,0,2,0,0,1,1)$ $\boldsymbol{u}[14] = (0,0,2,2,0,2,0,1,1,2,1,0,0,0,1)$

All these decimations have the same autocorrelation values as $\boldsymbol{u}$ up to conjugation, namely

$\Theta_s(\tau) = (15, 0,0,0,0, -3 + 10.3923i, 0,0,0,0, -3 - 10.3923i, 0,0,0,0).$

$|\Theta_s(\tau)| = (15, 0,0,0,0, 10.82, 0,0,0,0, 10.82, 0,0,0,0).$

4.8.5 Multiplying the elements of a near perfect sequence by consecutive powers of roots of unity

Proposition 4.8.5: For a near perfect sequence $\boldsymbol{s} = (s_0, s_1, s_2, \cdots, s_{N-1})$ over the m^{th} roots of unity, with period $N = mn$, the sequence $\boldsymbol{x} = (s_0, s_1\omega, s_2\omega^2, \cdots s_{m-1}\omega^{m-1}, s_m, s_{m+1}\omega, \cdots, s_{N-1}\omega^{m-1})$ is also near perfect.

Proof:

We have two cases.

Case 1

$\tau \neq kn,\ 1 \leq k \leq m-1$. This implies $\tau \not\equiv 0\ mod\left(\frac{N}{m}\right)$ and $\Theta_{\boldsymbol{s}}(\tau) = 0$. The autocorrelation value

$$\Theta_{\boldsymbol{x}}(\tau) = \sum_{i=0}^{N-1} s_i \omega^i \left(s_{i+\tau}\omega^{i+\tau}\right)^*$$

$$= \sum_{i=0}^{N-1} s_i \omega^i \left(s_{i+\tau}\right)^* \omega^{-i-\tau}$$

$$= \omega^{N-\tau} \sum_{i=0}^{N-1} s_i \left(s_{i+\tau}\right)^*$$

$$= \omega^{N-\tau}\Theta_{\boldsymbol{s}}(\tau) = 0.$$

Case 2

$\tau = kn,\ 1 \leq k \leq m-1$. This implies $\tau \equiv 0\ mod\left(\frac{N}{m}\right)$ and $\Theta_{\boldsymbol{s}}(\tau) \neq 0$.

The autocorrelation value

$$\Theta_{\boldsymbol{x}}(\tau) = \sum_{i=0}^{N-1} s_i \omega^i \left(s_{i+\tau}\omega^{i+kn}\right)^*$$

$$= \sum_{i=0}^{N-1} s_i \left(s_{i+\tau}\right)^* \omega^{-kn}$$

$$= \omega^{(m-k)n} \sum_{i=0}^{N-1} s_i \, (s_{i+\tau})^*$$

$$= \omega^{(m-k)n} \Theta_s(\tau) \neq 0$$

Note: The exponents of ω are calculated $mod\ m$.

4.9 Connected sets and completely orthogonal pairs

In this Section, we analyse the number of completely orthogonal pairs to form a connected set (*Definition 2.3.16*).

Zeng *et al.* have obtained the almost perfect (Wolfmann) completely orthogonal pairs by exhaustive computer search. Below, we give a Lemma to construct a maximal set of completely orthogonal sequences of length m.

Our construction of near perfect sequences require completely orthogonal ordered pairs of sequences $\boldsymbol{a}$, $\boldsymbol{b}$.

Lemma 4.9.1

The number of choices of completely orthogonal ordered pairs of sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ over m^{th} roots of unity used in our construction, for any odd prime m, in a maximal set is $\frac{m(m-1)}{2}$.

Proof:

We define two sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ over the powers of a primitive root λ^i.

So we have**,**

$\boldsymbol{a} = \left(\lambda^{ki}\right)$ and $\boldsymbol{b} = (\lambda^{li}) \quad 0 \leq i \leq m-1,\ 1 \leq k \leq m-1; 0 \leq l \leq m-1, k \neq l$

and $\boldsymbol{a} \neq (1,1,1 \cdots,1)$.

Now we have two cases.

Case 1

$\boldsymbol{b} = (1,1,1 \cdots,1)$

Then there are $(m-1)$ choices for $\boldsymbol{a}$ excluding $(1,1,1 \cdots,1)$, giving $(m-1)$ ordered pairs of completely orthogonal sequences $\boldsymbol{a}$ and $\boldsymbol{b}$.

Case 2

$\boldsymbol{b} \neq (1,1,1 \cdots,1)$

Then we can choose $\boldsymbol{a}$ in $(m-1)$ ways and $\boldsymbol{b}$ in $(m-2)$ ways.

So, we have

$(m-1)(m-2)$ choices of sequences which give us $\frac{(m-1)(m-2)}{2}$ ordered pairs.

Consider both cases.

The total number of choices for $\boldsymbol{a}$ and $\boldsymbol{b} = (m-1) + \frac{(m-1)(m-2)}{2}$

$$= \frac{(m-1)(2+m-2)}{2} = \frac{m(m-1)}{2}$$

■

Table 4.9.1 below, shows the alphabet sizes m and the number of completely orthogonal pairs.

m	3	4	5	6	7
Number of completely orthogonal pairs $\frac{m(m-1)}{2}$	3	6	10	15	21

Table 4.9.1

4.10 Alternate method of obtaining a shift sequence

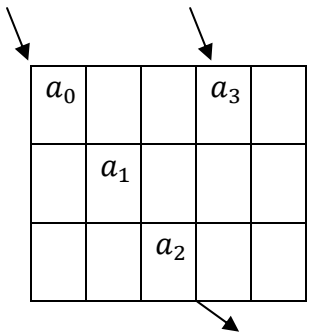
In this section, we give another method of folding a sequence, this time, diagonally into an array [72]. These arrays also have similar properties to those arrays constructed above by folding a sequence row- wise.

Pseudonoise (PN) sequences (*Definition 2.3.18*) of length $N = n_1 n_2$ are folded diagonally into $n_1 \times n_2$ arrays where n_1 and n_2 are co-prime. The reason for n_1 and n_2 being chosen co-prime is that the sequence can be folded into the array in a single pass. A detailed description of PN sequences, their properties and the diagonal folding of a sequence into an array is again demonstrated in detail by Mac Williams and Sloane [49] in 1976.

Example 4.10.1

The construction of a pseudorandom array (*Definition 2.4.5*) of dimension 3×5 by folding a sequence $(a_0, a_1, \cdots, a_{14})$ of length 15 is shown as follows:

Start at North West corner and move towards south east. When an edge is reached continue from opposite side, as shown below:



The completed array is

a_0	a_6	a_{12}	a_3	a_9
a_{10}	a_1	a_7	a_{13}	a_4
a_5	a_{11}	a_2	a_8	a_{14}

4.10.1 Near perfect sequence obtained by diagonal unfolding of the associated matrix

Diagonal folding is an alternate method to obtain other shift sequences. All near perfect sequences of length 15 obtained by diagonal folding are equivalent to the near perfect sequences of length 15 obtained by row-wise folding.

We give an example of constructing another shift sequence by diagonal folding. We shall start by folding an M-sequence of length $2^l - 1$ diagonally as seen in *Example 4.10.1.*

An M-sequence of period $\eta = 2^l - 1$, can be generated by an l-stage shift register.

A single period of this M-sequence can be represented as

$\boldsymbol{m} = (m_0, m_1, m_2, \cdots, m_{\eta-1})$.

Take the case when $\eta = 2^4 - 1 = 3 \times 5 = 15 = \eta_1\eta_2$.

The sequence $\boldsymbol{m}$ can be folded diagonally into an $\eta_1 \times \eta_2$ matrix as follows:

$$\mathbb{M}_{3,5} = \begin{bmatrix} m_0 & m_6 & m_{12} & m_3 & m_9 \\ m_{10} & m_1 & m_7 & m_{13} & m_4 \\ m_5 & m_{11} & m_2 & m_8 & m_{14} \end{bmatrix}$$

In general, the elements of the matrix $\mathbb{M}_{\eta_1,\eta_2}$ are $a_{ij} = m_k$, $k = 0,1,2,\cdots, 2^l - 2$ with $i = k(mod\ \eta_1)\ and\ j = k(mod\ \eta_2)$ where i, j, k are all counted starting from 0. There exists a one-to-one mapping T from the set of sequences $\boldsymbol{m}$, onto the set of $\eta_1 \times \eta_2$ matrices, given by, $T(\boldsymbol{m}) = \mathbb{M}_{\eta_1,\eta_2}$.

We have seen in Section 3.7, that row-wise folding of M-sequences of length $2^{2J} - 1$ into an array of order $(2^J - 1) \times (2^J + 1)$, gives an entire row of zeros and all the other rows are some shifts of an M-sequence of length $(2^J - 1)$. Now we will see that the diagonal folding and row-wise folding give similar properties.

Theorem 4.10.1[72]

Let $\boldsymbol{m}$ be a binary M-sequence of length $\eta = 2^l - 1 = \eta_1\eta_2$ with $gcd(\eta_1,\eta_2) = 1$ and $T(\boldsymbol{m}) = \mathbb{M}_{\eta_1,\eta_2}$. If $\eta_1 = 2^c - 1$, then each column of $\mathbb{M}_{\eta_1,\eta_2}$is either an M sequence of length $2^c - 1$ or a sequence of $2^c - 1$ zeros.

The detailed proof of this Theorem can be found in Weng [72].

Now we determine the number of all zero columns and the number of M- sequence columns of length $2^c - 1$ in $\mathbb{M}_{\eta_1,\eta_2}$.

Lemma 4.10.2 [72] There are exactly $\eta_2 - 2^{l-c}$ all zero columns in the matrix $\mathbb{M}_{\eta_1,\eta_2} = T(\boldsymbol{m})$ where $\boldsymbol{m}$ is a binary M-sequence of length $2^l - 1 = (2^c - 1)\eta_2$.

Proof:

According to the Balance property [64] of M-sequences, a binary M-sequence of length $2^l - 1$ contains 2^{l-1} ones and a binary M-sequence of length $2^c - 1$ contains 2^{c-1} ones. Hence, from *Theorem 4.10.1*, there are $\frac{2^{l-1}}{2^{c-1}} = 2^{l-c}$ non-zero columns and therefore $\eta_2 - 2^{l-c}$ all zero columns. ■

We now find a shift sequence from $\mathbb{M}_{\eta_1,\eta_2}$. The non-zero columns will be shifts of a binary M-sequence of length $2^c - 1$ [72]. Again, we assume a column of the matrix as the reference column to find the non-zero entries in the shift sequence and the all zero columns contribute an ∞ to the shift sequence. The shift sequence thus formed is different from the shift sequence formed by using the row-wise folding of an M-sequence of length $\eta = 2^l - 1 = \eta_1\eta_2$.

We make this method more clear with the help of an example.

Example 4.10.2

A binary M-sequence of length 15 is [1,1,1,1,0,1,0,1,1,0,0,1,0,0,0].

The diagonally folded matrix is

$$\mathbb{M}_{3,5} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Here we proceed in the same manner as in *Example 4.1.1*, by taking $\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$ as the reference column to construct the shift sequence.

The shift sequence obtained, $\boldsymbol{e} = (1,2,2,1,\infty)$, is used to construct a near perfect sequence of length 15.

Take an array $\mathbb{M}_{\eta_1,\eta_2} = \left(m_{i,j}\right)$, $0 \le i \le \eta_1 - 1, 0 \le j \le \eta_2 - 1$, of dimension $\eta_1 \times \eta_2$. For any integers k, l, the shifted matrix $A^{(k,l)}$ is defined by

$m_{ij}{}^{(k,l)} = m_{i+k,j+l}$ where $i + k$ is calculated $mod\ \eta_1$ and $j+l$ is calculated $mod\ \eta_2$.

Here the M-sequence (1,1,0) of length 3 is taken as the reference to determine the entries of $\boldsymbol{e}$.

The associated matrix is

$$\mathbb{U} = \begin{bmatrix} \omega & \omega^2 & \omega^2 & \omega & 1 \\ \omega^2 & 1 & 1 & \omega^2 & 1 \\ 1 & \omega & \omega & 1 & 1 \end{bmatrix}$$

Unfolding $\mathbb{U}$ diagonally gives us $(\omega, 1, \omega, \omega, 1,1, \omega^2, 1,1,1, \omega^2, \omega, \omega^2, \omega^2, 1)$, which is a near perfect sequence of length 15 with periodic autocorrelation function of magnitude,

$$|\Theta_{\boldsymbol{s}}(\tau)| = (15,0,0,0,0,10.82, 0,0,0,0, 10.82, 0,0,0,0).$$

Observation: The shift sequences obtained by row-wise folding and diagonal unfolding are different. In *Example 4.10.2*, diagonal unfolding gives the conjugate of the sequence obtained by row-wise unfolding.

Conjecture 4.10.3 New near perfect sequences of longer lengths can be constructed by diagonal unfolding.

We can also obtain other shift sequences containing more $\infty's$ by diagonal folding. For example, a binary M-sequence of length 255 can be folded into an almost-square array (*Definition 2.4.4*) of dimension 15×17. The same sequence can also be folded into 51×5 and 85×3 arrays which are not almost squares. These arrays have more than one all zero columns. This type of folding is discussed in detail in [27, 28].

We have only considered the folding of sequences into an almost-square array, where we obtain shift sequences containing exactly one ∞. We do not know yet, whether shift sequences with more than one ∞ can be used to construct near perfect sequences. We leave it as an open question for future work.

4.11 Diagrammatic representation of completely orthogonal pairs

The main purpose of this Section is a diagrammatic representation of completely orthogonal pairs of sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ for

i. A better understanding of maximal sets/choices of $\boldsymbol{a}$ and $\boldsymbol{b}$.

ii. To examine the general case of preferred completely orthogonal pairs in future, and its relation to graph theory.

Sarwate and Pursley [14] have given a diagrammatic representation for the preferred pairs (*Definition 2.3.15*) of M-sequences for the construction of Gold sequences. They use the sequences in the preferred pairs, as the vertices of a polygon to form a connected set. (Sarwate and Pursley [14], Section IV A).

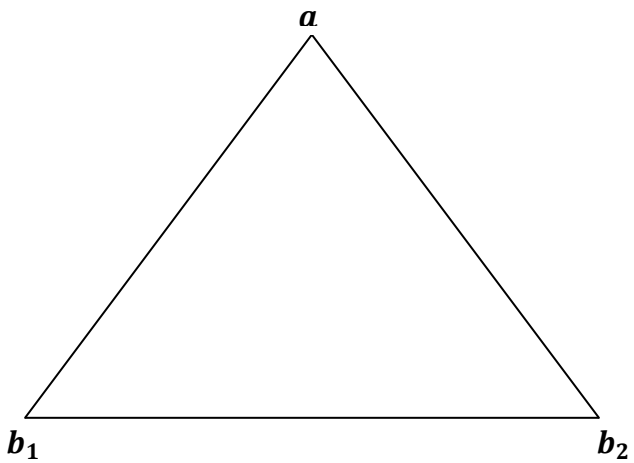
We use a similar approach to represent the preferred pairs of completely orthogonal sequences, using diagrams, which are used to construct near perfect sequences. In our context, a preferred pair consists of a pair of completely orthogonal sequences.

The sequences need not contain the m^{th} roots of unity in the ascending order to form a completely orthogonal pair. The following diagrams show the connectivity of the sequences using two dimensional diagrams. Each vertex represents a sequence of length m, over m^{th} roots of unity and the edges connect a pair of completely orthogonal sequences.

We give two examples for $m = 3$ and $m = 5$ as illustrations.

Example 4.11.1

m=3

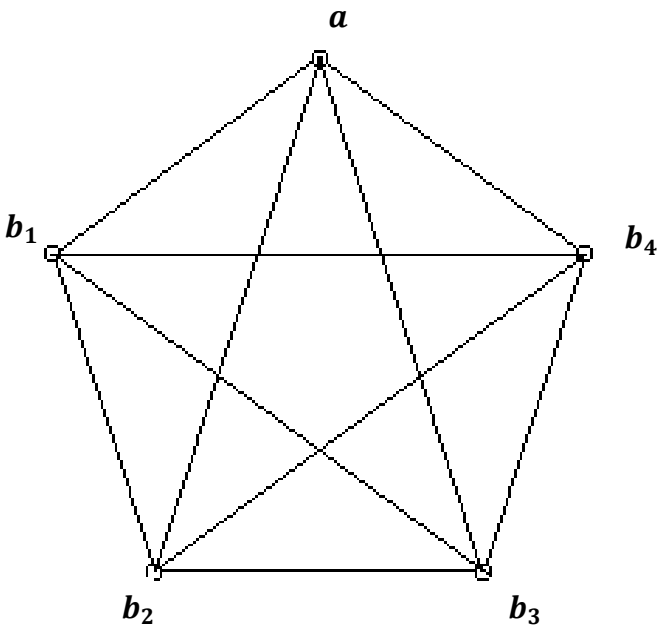


where $\boldsymbol{a} = (1, \omega, \omega^2)$, $\boldsymbol{b_1} = (1,1,1)$, $\boldsymbol{b_2} = (1, \omega^2, \omega)$

Here, $(\boldsymbol{a}, \boldsymbol{b_1})$; $(\boldsymbol{a}, \boldsymbol{b_2})$ and $(\boldsymbol{b_2}, \boldsymbol{b_1})$ are completely orthogonal pairs.

Example 4.11.2

m=5



where

$\boldsymbol{a} = (1, \lambda, \lambda^2, \lambda^3, \lambda^4)$, $\boldsymbol{b_1} = (1,1,1,1,1)$, $\boldsymbol{b_2} = (1, \lambda^2, \lambda^4, \lambda, \lambda^3)$, $\boldsymbol{b_3} = (1, \lambda^3, \lambda, \lambda^4, \lambda^2)$, $\boldsymbol{b_4} = (1, \lambda^4, \lambda^3, \lambda^2, \lambda)$; giving us 10 completely orthogonal pairs.

(Number of completely orthogonal pairs = Total number of edges).

5 NEW NEAR PERFECT SEQUENCES OF EVEN LENGTHS CONSTRUCTED BY CONCATENATION

In this Chapter, we give near perfect sequences of even length obtained by concatenating (one after the other) two distinct near perfect sequences of the same odd length.

Luke had found near perfect sequences over alphabet sizes 3, 4 and for some even lengths (Table 3.6.3). In Section 5.2, we provide a method to construct near perfect sequences of other even lengths not covered by Luke.

5.1 Construction of near perfect sequences of even length

We have seen the construction of near perfect sequences of odd lengths and examples in Sections 4.2 to 4.9.

We give below conditions for concatenating two near perfect sequences of the same odd length, to obtain a near perfect sequence of even length.

Let

i. $\boldsymbol{a}, \boldsymbol{b_1}, \boldsymbol{b_2}$ be sequences over the m^{th} roots of unity, m any odd prime such that $\boldsymbol{a}$ and $\boldsymbol{b_2}$; $\boldsymbol{b_1}$ and $\boldsymbol{b_2}$ are completely orthogonal.

ii. $\boldsymbol{S_1}$ be a near perfect sequence of length mn, $n = 2^J + 1$, $J \geq 2$, constructed using the completely orthogonal pair $\boldsymbol{a}$ and $\boldsymbol{b_1}$,

iii. $\boldsymbol{S_2}$ be another near perfect sequence of length mn constructed using the completely orthogonal pair $\boldsymbol{a}$ and $\boldsymbol{b_2}$ (Section 4.2).

Conjecture 5.1.1

If two near perfect sequences of length $\boldsymbol{S_1}$, $\boldsymbol{S_2}$ of length mn, under the above conditions, are concatenated, $\boldsymbol{S_1}$ followed by $\boldsymbol{S_2}$, a near perfect sequence $\boldsymbol{S}$ of length $2mn$ is obtained and the autocorrelation value $\Theta_{\boldsymbol{S}}(\tau)$ for any shift $0 \leq \tau < 2mn$ and an alphabet size m is given by $\Theta_{\boldsymbol{S}}(\tau) = 0$ where $\tau \not\equiv 0 \ mod\left(\frac{N}{2m}\right)$.

We now give three examples.

Example 5.1.1

Take

(i) A near perfect sequence $\boldsymbol{S_1}$, of length 15 over three roots of unity, constructed using $\boldsymbol{a} = (1, \omega, \omega^2)$ and $\boldsymbol{b} = (1,1,1)$ as the completely orthogonal pairs,

AND

(ii) Another near perfect sequence $\boldsymbol{S_2}$, of length 15 over three roots of unity, is constructed using $\boldsymbol{a} = (1, \omega, \omega^2)$ and $\boldsymbol{b} = (1, \omega^2, \omega)$ as the completely orthogonal pairs (Example 4.5.2).

When $\boldsymbol{S_1}$ and $\boldsymbol{S_2}$ are concatenated by writing $\boldsymbol{S_1}$ followed by $\boldsymbol{S_2}$, we get a near perfect sequence $\boldsymbol{S}$, of even length, 30.

The sequence $\boldsymbol{S}$ is given by

$\boldsymbol{S}$ = (0,1,0,0,0,1,2,1,1,0,2,0,2,2,0,0,1,0,0,0,1,2,1,1,2,2,0,2,2,1) over the cube roots of unity, of length 30, and is near perfect.

The periodic autocorrelation function of $\boldsymbol{S}$ is

$\Theta_{\boldsymbol{S}}(\tau)$ ={$30, 0,0,0,0, \ -10.5 + 18.1865i, 0,0,0,0, \ -12 - 20.7846i$, $0,0,0,0, 24, \ 0,0,0,0,$ $-12 + 20.7846i, \ 0,0,0,0, \ -10.5 - 18.1865i, \ 0,0,0,0$}.

Example 5.1.2

When $\boldsymbol{a} = (1, \omega^2, \omega)$; $\boldsymbol{b_1} = (1,1,1)$ and $\boldsymbol{b_2} = (1, \omega, \omega^2)$ are used, the sequence in this example turns out to be the conjugate of the sequence in Example 5.1.1.

Here, $\boldsymbol{S}$ = (0,2,0,0,0,2,1,2,2,0,1,0,1,1,0,0,2,0,0,0,2,1,2,2,1,1,0,1,1,2) with the periodic autocorrelation function

$\Theta_{\boldsymbol{S}}(\tau)$ ={$30, \ 0,0,0,0, \ -10.5 - 18.1865i, \ 0,0,0,0, \ -12. + 20.7846i$, $0,0,0,0, 24, 0,0,0,0,$ $-12. - 20.7846i, 0,0,0,0, -10.5 + 18.1865i, \ 0,0,0,0$}.

Example 5.1.3

We construct a near perfect sequence of length 102 by concatenating two near perfect sequences of length 51 over the cube roots of unity where $\boldsymbol{a} = (1, \omega, \omega^2)$; $\boldsymbol{b_1} = (1,1,1)$ and $\boldsymbol{b_2} = (1, \omega^2, \omega)$.

Here, $\boldsymbol{S}$ is

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

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

The periodic autocorrelation function is $\Theta_{\boldsymbol{s}}(\tau) = \{102,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,$

$-46.5 + 80.5404i, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,$

$-48. -83.1384i, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,96,0,0,0,0,0,0,0,0,0,0,0,0,0,0,$

$-48. +83.1384i, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,$

$-46.5 - 80.5404i, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0\}.$

From the conditions stated in Section 5.1, we can construct near perfect sequences of other even lengths. Our components for the construction of near perfect sequences are

i. The mutually and completely orthogonal sequences $\boldsymbol{a}, \boldsymbol{b_1}$ and $\boldsymbol{b_2}$. From Section 4.9, we observe that for $m = 3$, we at least have three sequences that satisfy our construction criteria. For larger m, there exist more orthogonal pairs (Table 4.9.1). But we need m to be smaller for practical purposes.

ii. The shift sequences used in our construction are of length $(2^J + 1)$, and are derived from M-sequences. We know that M-sequences exist for unbounded lengths (Theorem 4.6.3). It is already proven that near perfect sequences of odd length over the m^{th} roots of unity, can be constructed for unbounded lengths (Theorem 4.6.1), by taking arbitrary large values for J. The near perfect sequences of even lengths in this section are constructed by concatenating two different near perfect sequences of same odd lengths. So, near perfect sequences of even lengths also can be constructed for unbounded lengths.

6 CROSS CORRELATION OF NEAR PERFECT SEQUENCES

We have seen the autocorrelation values of near perfect sequences in Chapter 4. The periodic cross correlation is also important for practical applications as is the periodic autocorrelation. Let us now examine the periodic cross correlation of our constructed near perfect sequences.

Let $\boldsymbol{b} = \boldsymbol{d} = (1,1,1,\cdots,1)$ and let $\boldsymbol{a}, \boldsymbol{c}$ be sequences such that $(\boldsymbol{a}, \boldsymbol{b})$ and $(\boldsymbol{c}, \boldsymbol{d})$ form two pairs of completely orthogonal sequences of length m over the m^{th} roots of unity.

Use $(\boldsymbol{a}, \boldsymbol{b})$ to construct a sequence $\boldsymbol{S}_1$ and $(\boldsymbol{c}, \boldsymbol{d})$ to construct a sequence $\boldsymbol{S}_2$ as in Chapter 4.

If the sequence $\boldsymbol{S}_2$ is the conjugate of the sequence $\boldsymbol{S}_1$, equivalently if $\boldsymbol{a} = \boldsymbol{c}^*$, then the cross correlation spectrum of $\boldsymbol{S}_1$ and $\boldsymbol{S}_2$ is near perfect.

Theorem 6.1

Let $\boldsymbol{S}_1$and $\boldsymbol{S}_2$ be two near perfect sequences of length N over the m^{th} roots of unity, constructed from completely orthogonal sequence pairs $(\boldsymbol{a}, \boldsymbol{b})$ and $(\boldsymbol{c}, \boldsymbol{d})$ respectively where $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}$ are of odd prime length m.

If $\boldsymbol{S}_2$ is the conjugate of $\boldsymbol{S}_1$, then the cross correlation of $\boldsymbol{S}_1$and $\boldsymbol{S}_2$ for any shift τ is

$$C_{\boldsymbol{S}_1, \boldsymbol{S}_2}(\tau) = \begin{cases} m & if\ \tau \equiv 0\ mod\left(\frac{N}{m}\right) \\ 0 & otherwise \end{cases}$$

The calculation of the cross correlation values is very similar to that of the autocorrelation values.

Proof:

Let $\mathbb{S}$ and $\mathbb{T}$ denote the associated matrices of $\boldsymbol{S}_1$ and $\boldsymbol{S}_2$ constructed using the shift sequence $\boldsymbol{e}$. Let S_j and T_j denote the columns of $\mathbb{S}$ and $\mathbb{T}$ respectively.

So we have, $C_{\boldsymbol{S}_1, \boldsymbol{S}_2}(\tau) = C_{\mathbb{S},\mathbb{T}}(\tau)$ for any shift $\tau = qn + r$ where $0 \leq q < m$ and

$0 \leq r < n$.

We modify the Equation 4.3.2 for autocorrelation to calculate the cross correlation of $\mathbb{S}$ and $\mathbb{T}$.

We have,

$$C_{\boldsymbol{S}_1, \boldsymbol{S}_2}(\tau) = \sum_{j=0}^{n-r-1} C_{S_j, T_{r+j}}(q) \qquad r + j < n$$

$$+ \sum_{j=n-r}^{n-1} C_{S_j, T_{r+j}}(q+1) \quad r + j \geq n \qquad (6.1.1)$$

We know from (4.2.1) that

$$S_j = \begin{cases} L^{e_j}(\boldsymbol{a}) & if\ e_j \neq \infty \\ \boldsymbol{b} & otherwise \end{cases}$$

and

$$T_j = \begin{cases} L^{e_j}(\boldsymbol{c}) & if\ e_j \neq \infty \\ \boldsymbol{d} & otherwise \end{cases}$$

Now we have two cases.

Case 1 $r \neq 0$

The summation (6.1.1) depends on the differences of the entries in the shift sequence $\boldsymbol{e}$ (Equation 4.3.4).

The list of differences contains exactly 2 $\infty's$ (Table 3.7.1).

In this case, there are no matching columns for $\mathbb{S}$ and $\mathbb{T}$.

The cross correlation formula is

$$C_{\boldsymbol{s}_1,\boldsymbol{s}_2}(\tau) = \sum_{e_j \neq \infty, e_{r+j} \neq \infty} C_{\boldsymbol{a},\boldsymbol{c}}\left(e_{r+j} - e_j + r\right) + \sum_{e_j \neq \infty, e_{r+j} = \infty} \Theta_{\boldsymbol{a},\boldsymbol{d}}(\tau_1) + \sum_{e_j = \infty, e_{r+j} \neq \infty} \Theta_{\boldsymbol{b},\boldsymbol{c}}(\tau_2)$$

where $$\tau_1 = \begin{cases} e_{(r+j)(mod\ n)} + r & if \quad r + j < n \\ e_{(r+j)(mod\ n)} + r + 1 & if \quad r + j \geq n \end{cases}$$

and

$$\tau_2 = \begin{cases} q - e_j & if \quad r + j < n \\ q + 1 - e_j & if \quad r + j \geq n \end{cases}$$

So, $C_{\boldsymbol{s}_1,\boldsymbol{s}_2}(\tau) = \sum_{e_j \neq \infty, e_{r+j} \neq \infty} C_{\boldsymbol{a},\boldsymbol{c}}\left(e_{r+j} - e_j + r\right)$ +0+0

$$= \sum_{e_j \neq \infty, e_{r+j} \neq \infty} C_{\boldsymbol{a},\boldsymbol{c}}\left(e_{r+j} - e_j + r\right) \qquad (6.1.2)$$

since $\boldsymbol{a}$ and $\boldsymbol{d}$ are completely orthogonal, the cross correlation $C_{\boldsymbol{a},\boldsymbol{d}}$ is 0 and $C_{\boldsymbol{b},\boldsymbol{c}}$ is also 0 as $\boldsymbol{b}$ and $\boldsymbol{c}$ are completely orthogonal.

Let ($e_{r+j} - e_j + r) = \ell (mod\ m)$ say, (Distinct Difference Property, Section 3.7).

Then,

$$C_{\boldsymbol{s}_1, \boldsymbol{s}_2}(\tau) = \frac{n-2}{m} \sum_{\ell=0}^{m} C_{\boldsymbol{a},\boldsymbol{c}}(\ell)$$

$$= \frac{n-2}{m} \sum_{\ell=0}^{m} a_i c_i^*(\ell)$$

We take $\boldsymbol{a} = \boldsymbol{c}^*$. Then the above equation continues as

$$C_{\boldsymbol{s}_1, \boldsymbol{s}_2}(\tau) = \frac{n-2}{m} \sum_{\ell=0}^{m} a_i a_i(\ell)$$

$$= \frac{n-2}{m} \sum_{\ell=0}^{m} {a_i}^2(\ell)$$

Each $a_i \in \{1, \lambda_i, {\lambda_i}^2, \cdots, {\lambda_i}^{m-1}\}$ where λ_i is an m^{th} root of unity.

Thus, $C_{\boldsymbol{s}_1, \boldsymbol{s}_2} = \frac{n-2}{m} \sum_{\ell=0}^{m} {a_i}^2(\ell) = 0.$

<u>*Case 2*</u> $\tau = qn; \quad r = 0$

Then $C_{\boldsymbol{s}_1, \boldsymbol{s}_2}(\tau) = \sum_{j=0}^{n-1} C_{S_j, T_j}(q)$

Here, we observe that the column number is the same for $\mathbb{S}$ and $\mathbb{T}$ (*Example 4.3.1*). So Equation (4.3.5) will be

$$C_{\boldsymbol{s}_1, \boldsymbol{s}_2}(\tau) = (n-1)\mathrm{C}_{\boldsymbol{a},\boldsymbol{c}}(q) + \mathrm{C}_{\boldsymbol{b},\boldsymbol{d}}(q) \qquad (6.1.3)$$

When $\boldsymbol{a} = \boldsymbol{c}^*$, $\boldsymbol{a}$ and $\boldsymbol{c}$ are completely orthogonal. So $\mathrm{C}_{\boldsymbol{a},\boldsymbol{c}}(q) = 0$.

Since we assume that, $\boldsymbol{b} = \boldsymbol{d} = (1,1,1,\cdots,1)$, we have, $\mathrm{C}_{\boldsymbol{b},\boldsymbol{d}}(q) = m$.

Thus, $C_{\boldsymbol{s}_1, \boldsymbol{s}_2}(\tau) = (n-1) \times 0 + m = m.$

Then we obtain a near perfect cross correlation spectrum for any shift τ as

$(m, \underbrace{000\cdots}_{(n-1)zeros}, m, \underbrace{000\cdots}_{(n-1)zeros}, m, \underbrace{000\cdots}_{(n-1)zeros}, m, \cdots)$, where $n = 2^J + 1$; $m = 3,5,7,\cdots$;

$J = 2,4,6,\cdots$. ■

Example 6.1

Take a near perfect sequence $\boldsymbol{S}$ of length 51, over the cube roots of unity, namely,

$\boldsymbol{S}$ = {2,1,2,2,0,1,0,1,0,0,2,2,2,0,0,2,0,0,2,0,0,1,2,1,2,1,1,0,0,0,1,1,0,0,1,0,1,1,2,0,2,0,2,2,1,1,1,2,2,1,0}

$\boldsymbol{S}^*$ = {1,2,1,1,0,2,0,2,0,0,1,1,1,0,0,1,0,0,1,0,0,2,1,2,1,2,2,0,0,0,2,2,0,0,2,0,2,2,1,0,1,0,1,1,2,2,2,1,1,2,0}

The cross correlation spectrum $C_{\boldsymbol{S},\boldsymbol{S}^*}$ is

(3,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,3,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,3,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,3,0,0,0,0,0,0,0,0,0,0,0,0,0,0).

Example 6.2

Take the near perfect sequence $\boldsymbol{S}$ of length 3075 (*Example 4.5.9*) over the cube roots of unity. The three non-zero cross correlation values of $\boldsymbol{S}$ and $\boldsymbol{S}^*$are each 3.

The non-zero values in the cross correlation spectrum occur for the same shifts as the non-zero values in the autocorrelation, and we say that the cross correlation is also near perfect. So for sequence design, if these shifts are excluded, the sequences are effectively perfect and orthogonal. We also observe that the non-zero cross correlation values are typically lower than the non-zero off peak autocorrelation values (Section 4.5). This excellent cross correlation would permit the use of these sequences for many applications such as wireless communications. The large zero correlation zone and smaller non-zero cross correlation values will result in almost no mutual interference.

7 CONCLUSIONS

7.1 Final Summary of Results

We have introduced near perfect sequences of several *odd* and *even* lengths over m^{th} roots of unity, where m is an odd prime. Many examples of near perfect sequences are given. Near perfect sequences of odd lengths constructed in this work are new and the Type II and Type III near perfect sequences of length 15 are found by exhaustive computer search. Examples of all these sequences are provided.

Some new near perfect sequences of even lengths are constructed by concatenating two distinct near perfect sequences of the same odd length.

The major result is in Section 4.6, that there exist, and we provide the construction of, near perfect sequences of *unbounded* lengths.

For future work, we suggest consideration of other shift sequences with more than one ∞, which are obtained by diagonal folding of an M-sequence, with different pairs of completely orthogonal sequences or a triplet of sequences to construct other near perfect sequences of odd and even lengths.

We give some open questions in Section 7.2 below.

7.2 Open Questions

Open Question 7.2.1: Can near perfect sequences of odd lengths, other than $m(2^J + 1)$, over m^{th} roots of unity, m any odd prime, be constructed? Recall Table 4.5.1.

Open Question 7.2.2: Can we find any construction method for Type II and Type III near perfect sequences of length 15?

Open Question 7.2.3: Is there any other method of synthesis of two near perfect sequences of odd lengths to obtain other near perfect sequences of even lengths?

Open Question 7.2.4: Is it possible to extend the dimension of near perfect sequences to two and three dimensions (arrays and volumes)?

7.3 Potential Applications

Near perfect sequences are a special category of zero correlation zone sequences. Zero correlation zone sequences have applications in various areas such as cellular communication systems, radar, position sensing and ultrasonic imaging. Zero correlation zone sequences have out of phase autocorrelation values zero in specified shifts. In our construction, the first shift that gives non-zero auto correlation value is the shift $\frac{N}{m} = k$ (and k can be made arbitrarily large). In Global Positioning System (GPS), M-sequences of length approximately equal to 2^{40} are used which have all the off peak autocorrelation values, -1.

For example, with our construction, if we choose an M-sequence of length $2^{84} - 1$, then we obtain a near perfect sequence over the cube roots of unity of length $3(2^{42} + 1)$ that has a zero correlation zone of length 2^{42}. Once again, since the lengths of near perfect sequences are unbounded, the zero correlation zone can be made long enough for desirable applications. The non-zero values of the cross correlation of a selected pair of near perfect sequences over m^{th} roots of unity is m, which is highly useful for many applications such as wireless communications.

Wolfmann's and Luke's almost perfect sequences occur in the literature only for even lengths over m^{th} roots of unity, where $m = 2,4,6,8$. Perfect sequences over roots of unity also exist only for certain lengths. Near perfect sequences could be considered to be the next alternative to perfect and almost perfect sequences in most of the applications.

8 REFERENCES

[1] W.O. Alltop, *Complex sequences with low periodic correlations (Corresp.)*, Information Theory, IEEE Transactions on 26 (1980), pp. 350-354.

[2] L.D. Baumert, *Difference Sets, Lecture Notes in Mathematics,* ed, Vol. 182, Springer-Verag Press, 1971.

[3] L. Bomer, and M. Antweiler, *Perfect N-phase sequences and arrays [spread spectrum communication]*, IEEE Journal on Selected Areas in Communications 10 (1992), pp. 782-9.

[4] ---, *Perfect three-level and three-phase sequences and arrays*, , IEEE Transactions on Communications 42 (1994), pp. 767-772.

[5] S. Boztas, and U. Parampalli, *Nonbinary sequences with perfect and nearly perfect autocorrelations*, in *IEEE International Symposium on Information Theory. ISIT 2010* Piscataway, NJ, USA, 2010, pp. 1300-4.

[6] R.F. Brown, and G.C. Godwin, *New class of pseudorandom binary sequences*, IEE Electronic Letters 3 (1967), pp. 198-199.

[7] D. Calabro, and J.K. .Wolf, *On the synthesis of two-dimensional arrays with desirable correlation properties*, Information and Control 11 (1968), pp. 537-560.

[8] J.A. Chang, *Ternary sequence with zero correlation*, Proceedings of the IEEE 55 (1967), pp. 1211-1213.

[9] D.C. Chu, *Polyphase codes with good periodic correlation properties*, IEEE Transactions on Information Theory IT-18 (1972), pp. 531-2.

[10] H. Chung, and P.V. Kumar, *A new general construction for generalized bent functions*, IEEE Transactions on Information Theory IT-35

(1989), pp. 206-209.

[11] D.Calabro, and J.K..Wolf, *On the synthesis of two-dimensional arrays with desirable correlation properties*, Information and Control 11 (1968), pp. 537-560.

[12] M. Darnell, *New classes of perfect sequences derived from m-sequences*, Applied signal processing 3 (1996), pp. 223-7.

[13] M. Darnell, and P.Z. Fan, *The Synthesis of Perfect Sequences*, in *5th IMA Conference on Cryptography and Coding*, 1995, pp. 63-73.

[14] Dilip.V.Sarwate, and Micheal.B.Pursley, *Crosscorrelation Properties of Pseudorandom and Related Sequences*, Proceedings of the IEEE vol-68 (1980), pp. 593-608.

[15] D. Everett, *Periodic digital sequences with pseudonoise properties*, GEC Journal of Science & Technology 33 (1966), pp. 115-126.

[16] J.B. Fraleigh, *A First course in Abstract Algebra,* 7th ed, Greg Tobin, 2003.

[17] R.L. Frank, *Comments on 'Polyphase codes with good periodic correlation properties' by Chu, David C*, Information Theory, IEEE Transactions on 19 (1973), pp. 244-244.

[18] ---, *Polyphase Codes with Good Nonperiodic Correlation Properties*, IEEE Transactions on Information Theory IT-9 (April, 1962), pp. 43-45.

[19] R.L. Frank, S.A. Zadoff, and R.C. Heimiller, *Phase shift pulse codes with good periodic correlation properties*, Institute of Radio Engineers Transactions on Information Theory IT-8 (October, 1962), pp. 381-382.

[20] E.M. Gabidulin, *Partial classification of sequences with perfect auto-correlation and bent functions*, IEEE, New York, NY, USA, 1995, pp. 467.

[21] R.A. Games, *Crosscorrelation of M-sequences and GMW-sequences with the same primitive polynomial*, Discrete Applied Mathematics 12 (1985), pp. 139-46.

[22] R. Gold, *Maximal Recursive Sequences with 3-valued /recyrsuve Cross-correlation Functions*, IEEE Transactions Informations theory IT-14 (1968), pp. 154-156.

[23] S.W. Golomb, *Shift Register Sequences,* ed, Holden-Day San Francisco, 1967.

[24] ---, *New Concepts in Multi-User Communication,* ed, Norwich,UK, 1982.

[25] G. Gong, *C&O739x, Sequence Analysis, Lecture Notes on Sequence Design (C&O 739x, 1999)*, 1999, pp. 1-7.

[26] B. Gordon, W.H. Mills, and L.R. Welch, *Some new difference sets*, Canadian Journal of Mathematics 14 (1962), pp. 614-625.

[27] D.H. Green, *Structural properties of pseudorandom arrays and volumes and their related sequences*, IEE Proceedings 132 (1985), pp. 133-145.

[28] D.H. Green, and S.K. Amarasinghe, *Families of sequences and arrays with good periodic correlation properties*, IEE Proceedings E (Computers and Digital Techniques) 138 (1991), pp. 260-8.

[29] T.E. Hall, A. Tirkel, and C.F. Osborne, *Families of Matrices with Good Auto and Cross-Correlation*, ARS Combinatoria 61 (2001), pp. 187-196.

[30] R. Hariharan, *Near perfect sequences of odd length*, in *IEEE Proceedings of the Fourth International Workshop on Signal Design and its Applications in Communications*, Fukuoka, Japan, 2009, pp. 4-7.

[31] T. Hayashi, *Zero-correlation zone sequence set constructed from a perfect sequence*, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E90-A (2007), pp. 1107-11.

[32] R.C. Heimiller, *Phase shift pulse codes with good periodic correlation properties*, IRE Transactions on Information Theory IT -7 (1961), pp. 254-257.

[33] ---, *Author's Comment*, IRE Transactions on Information Theory 8 (1962), pp. 382.

[34] T. Helleseth, *Some Results about the Cross-Correlation Function between two Maximal Linear Sequences*, Discrete Mathematics 16 (1976), pp. 209-232.

[35] T. Hoholdt, and J. Justesen, *Ternary Sequences with Perfect Periodic Auto-correlation*, IEEE Transactions on Information theory 29 (1983), pp. 597-600.

[36] K.J. Horadam, *Hadamard Matrices and Their Applications,* ed, Princeton University Press, Princeton, NJ, 2007.

[37] V.P. Ipatov, *Ternary sequences with ideal periodic autocorrelation properties*, Radio engineering and electronic physics 24 (1979), pp. 75-9.

[38] A. Klapper, A.H. Chan, and M. Goresky, *Cascaded GMW sequences*, IEEE Transactions on Information Theory 39 (1993), pp. 177-83.

[39] P.V. Kumar, R.A. Scholtz, and L.R. Welch, *Generalized bent functions and their properties*, Journal of Combinatorial Theory, Series A 40 (1985), pp. 90-107.

[40] P. Langevin, *Almost Perfect Binary Functions*, Applicable algebra in engineering, communication and computing 4 (1993), pp. 95-102.

[41] C.E. Lee, *On a new class of 5-ary sequences exhibiting ideal periodic autocorrelation properties with applications to spread spectrum systems*, Mississippi State University, 1986.

[42] B.L. Lewis, and F.F. Kretschmer, *Linear Frequency Modulation Derived polyphase Pulse Compression Codes*, IEEE Transactions on Aerospace and Electronic Systems AES-18 (1982), pp. 637-641.

[43] R. Lidl, and H. Niederreiter, *Encyclopedia of Finite Fields and its applications,* 2nd ed, Vol. 20, Cambridge University Press, 1997.

[44] H.D. Luke, *Sequences and arrays with perfect periodic correlation*, IEEE Transactions on Aerospace and Electronic Systems 24 (1988), pp. 287-94.

[45] ---, *Almost-perfect polyphase sequences with small phase alphabet*, IEEE Transactions on Information Theory 43 (1997), pp. 361-3.

[46] ---, *Binary and quadriphase sequences with optimal autocorrelation properties: A survey*, IEEE Transactions on Information Theory 49 (2003), pp. 3271-3282.

[47] ---, *Sequences and arrays with perfect periodic correlation*, IEEE Transactions on Aerospace and Electronic Systems 24 (May 1988), pp. 287-94. Available at http://dx.doi.org/10.1109/7.192096.

[48] S.L. Ma, and W.S. Ng, *On Non-Existence of Perfect and Nearly Perfect Sequences*, International Journal of Information and Coding Theory 1 (2009), pp. 15-38.

[49] F.J. MacWilliams, and N.J.A. Sloane, *Pseudo-random sequences and arrays*, Proceedings of the IEEE 64 (1976), pp. 1715-29.

[50] ---, *The Theory of Error-Correcting Codes,* ed, North Holland, 1981.

[51] A. Milewski, *Periodic sequences with optimal properties for channel estimation and fast start-up equalization*, IBM Journal of Research and Development 27 (1983), pp. 426-31.

[52] W.H. Mow, *A Study of Correlation of Sequences*, The Chinese University of Hong Kong, 1993.

[53] J.D. Olsen, R.A. Scholtz, and L.R. Welch, *Bent-function sequences*, IEEE Transactions on Information Theory 28 (1982), pp. 858-64.

[54] U. Parampalli, *Polyphase and Frequency Hopping Sequences Obtained from Finite Rings*, Indian Institute of Technology, 1992.

[55] U. Parampalli, T. Xiaohu, and S. Boztas, *On the Construction of Binary Sequence Families with Low Correlation and Large Sizes*, in *IEEE International Symposium on Information Theory. ISIT 2010,* Piscataway, NJ, USA, 2010, pp. 1253-7.

[56] B.M. Popovic, *Generalized chirp-like polyphase sequences with optimum correlation properties*, IEEE Transactions on Information Theory 38 (1992), pp. 1406-9.

[57] A. Pott, and S.P. Bradley, *Existence and nonexistence of almost-perfect autocorrelation sequences*, IEEE Transactions on Information Theory 41 (1995), pp. 301-4.

[58] A. Pott, Kumar, P.V, Helleseth, T, Jungnickel, D., *Difference Sets, Sequences and their Correlatiion Properties*, *Nato Science Series,* ed, Kluwer Academic Publishers, 1999.

[59] D.V. Sarwate, and M.B. Pursley, *Crosscorrelation Properties of Pseudorandom and Related Sequences*, Proceedings of the IEEE 68 (1980), pp. 593-619.

[60] B. Schmidt, *Cyclotomic Integers and Finite Geometry*, Journal of American Mathematical Society 12 (1999), pp. 929-952.

[61] R.A. Scholtz, and Welch.L.R, *GMW Sequences*, IEEE Transactions Informations theory IT-30 (1984), pp. 548-553.

[62] M.R. Schroeder, *Number Theory in Science and Communication,* ed, Springer-Verlag: Berlin, 1997.

[63] D.A. Shedd, and D.V. Sarwate, *Construction of Sequences with Good Correlation Properties*, IEEE Transactions on Information theory IT-25 (1979).

[64] M.K. Simon, Omura, J.K, Scholtz, R.A, Levitt, B.K, *Spread Spectrum Communications Handbook,* Revised Edition ed, McGraw-Hill, Inc. , New York, 1994.

[65] Solomon.W.Golomb, and G. Gong, *Signal design for good correlation For Wireless Communication, Cryptography and Radar,* ed, Cambridge University Press, 2005.

[66] N. Suehiro, and M. Hatori, *Modulatable Orthogonal Sequences and Their Application to SSMA Systems*, IEEE Transactions on Information theory 34 (1988), pp. 93-100.

[67] A. Tirkel, and T.E. Hall, *Matrix construction using cyclic shifts of a column*, in *International Symposium on Information Theory*, 2005.

[68] D.N. Tompkins, Codes with zero correlation, Hughes Aircraft Company,, Culver city, Calif, June, 1960.

[69] H. Torii, M. Nakamura, and N. Suehiro, *A new class of zero-correlation zone sequences*, Information Theory, IEEE Transactions on 50 (2004), pp. 559-565.

[70] R. Turyn, *Sequences with small correlation*, John Wiley and Sons Inc, New York, NY, USA, 1968, pp. 195-228.

[71] R.J. Turyn, *Character Sums and Difference Sets,*, Pacific Journal of Mathematics 15 (1965), pp. 319-346.

[72] L.J. Weng, *Decomposition of M-sequences and its applications*, IEEE Transactions on Information Theory 17 (1971), pp. 457-63.

[73] J. Wolfmann, *Almost perfect Autocorrelation sequences*, IEEE Transactions on Information Theory vol-38 (1992), pp. 1412-1418.

[74] C. Yeow Meng, T. Yin, and Z. Yue, *Almost p-Ary perfect sequences*, Springer Verlag, Berlin, Germany, 2010, pp. 399-415.

[75] X. Zeng, L. Hu, and Q. Liu, *A Novel Method for Constructing Almost Perfect Polyphase Sequences*, (2006), pp. 346-353.

[76] Zhang.N, and S.W. Golomb, *Sixty phase generalised Barker sequences*, IEEE Transactions Informations theory 35 (1989), pp. 911-912.

[77] N. Zierler, *Linear recurring sequences*, Journal of the Society for Industrial and Applied Mathematics 7 (1959), pp. 31.

APPENDIX

Search for near perfect sequences in Mathematica. (Sam Blake, 2009)

Code

```
CorrelationValue2D [seq_List, shift_] := Dot [seq, Conjugate [RotateRight [seq, shift]]]

CV [seq_List] := Table [CorrelationValue2D [seq, n], {n, 0, Length [seq] - 1}]

NearPerfectQ [seq_, root_Integer] := With[{cv = CV [seq] // N // Chop},
    And[
      Union @ Differences [Flatten [Position [cv, Except [0]]]] === {Length [seq] / root},
      Count [cv, Except [0]] === root
    ]
  ]

ListToSequence [lst_List, root_Integer ? Positive ] := Exp [2 I Pi # / root] & /@ lst

FastNearPerfectQ = Compile [{{seq, _Complex, 1}, {root, _Integer}}, Catch [
        Scan [
          If[Chop [N [Dot [seq, Conjugate [RotateRight [seq, #]]]]] != 0, Throw [False ]] &,
          Complement [Range [Length [seq]], Join [{root}, Length [seq] / root Range [root]]]
        ];
        True
      ]];

incrementsequence = Compile [{{shifts, _Integer, 1}, {base, _Integer}},
      Module [{len, out = shifts},
        len = Length [shifts];
        Do [
          If[out [[iter]] =!= base - 1,
            out [[iter]] ++;
            Do [out [[i]] = 0, {i, iter + 1, len}];
            Break []
          ],
          {iter, len, 1, -1}];
        out
      ]];

makepalindromic [test_, length_ ? OddQ ] := Join [{0}, test, Reverse [test]]

makepalindromic [test_, length_ ? EvenQ ] := Join [test, Reverse [test]]
```

```
NearPerfectPalindromicSearch [length_Integer, root_Integer] := Module [{iter = 0, place, test, max, res},
  place = Table [0, {Floor [length / 2]}];
  max = root^Floor[length/2];
  res = Reap [
      Monitor [
        While [iter ++ < max,
          place = incrementsequence [place, root];
          test = makepalindromic [place, length];
          If [FastNearPerfectQ [N @ ListToSequence [test, root], root], Print [test]; Sow [test]]
        ], ProgressIndicator [iter, {0, max}]]
    ];
  If [res === {Null, {}}, {}, res [[-1, 1]]]
]

NearPerfectSearch [length_Integer, root_Integer] := Module [{iter = 0, test, max, res},
  test = Table [0, {length}];
  max = root^length;
  res = Reap [
      Monitor [
        While [iter ++ < max,
          test = incrementsequence [test, root];
          If [FastNearPerfectQ [N @ ListToSequence [test, root], root], Print [test]; Sow [test]]
        ], ProgressIndicator [iter, {0, max}]]
    ];
  If [res === {Null, {}}, {}, res [[-1, 1]]]
]
```