Sequences Design for OFDM and CDMA Systems

by

Fei Huo

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Applied Science
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2011

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

With the emergence of multi-carrier (MC) orthogonal frequency division multiplexing (OFDM) scheme in the current WLAN standards and next generation wireless broadband standards, the necessitation to acquire a method for combating high peak to average power ratio (PMEPR) becomes imminent. In this thesis, we will explore various sequences to determine their PMEPR behaviours, in hopes to find some sequences which could potentially be suitable for PMEPR reduction control under MC system settings. These sequences include m sequences, Sidelnikov sequences, new sequences, Golay sequences, FZC sequences and Legendre sequences. We will also examine the merit factor properties of these sequences, and then we will derive a bound between PMEPR and merit factor.

Moreover, in the design of code division multiple access (CDMA) spreading sequence sets, it is critical that each sequence in the set has low autocorrelations and low cross-correlation with other sequences in the same set. In the thesis, we will present a class of GDJ Golay sequences which contains a large zero autocorrelation zone (ZACZ), which could satisfy the low autocorrelation requirement. This class of Golay sequences could potentially be used to construct new CDMA spreading sequence sets.

Acknowledgements

I would like to specially thank Prof. Guang Gong, my supervisor. Two years ago, I entered M.Sc study under Prof. Guang Gong's superivison, with enthusiastic interest in the field of communication and security, but not having much knowledge at all. I have encountered countless obstacles and difficulties in the past two years. Prof. Guang Gong has been very patient, helpful for giving me suggestions, encouragement and guided me through the research. I am very graceful to have met such a benevolent and caring supervisor. Not only did she give me constructive suggestions, but she also encouraged me to think outside of the box. I wouldn't be where I am today without Prof. Guang Gong. Thank you Prof. Guang Gong!

I would like to thank my committee members, Prof. Weihua Zhuang and Prof. Oussama Damen, for their valuable comments and suggestions on my thesis.

I would like to thank Prof. Anwar. Hasan, Prof. Gordon Agnew, Prof. En-hui Yang, Prof. Weihua Zhuang, Prof. Guang Gong, whom I have taken the courses from. They provide me with the necessary and vital knowledge and foundation in order for me to succeed in my own research.

I would also like to thank to all my colleagues: Dr. Honggang Hu, Dr. Xinxin Fan, Dr. Zhijun Li, Yang Yang, Qi Chai, Bo Zhu, Tassanaviboon Anuchart, Mandal Kalikinkar and Shengke Zeng, for their continuous supports and suggestions on my research. I would like to thank Dr. Honggang Hu for providing me with the help on the sequence design. I would like to thank Dr. Xinxin Fan for helping me with knowledge on the field theory. I would also like to thank Yang Yang, whom I've closely worked with, and whom helped me immeasurably with my research.

I would like to thank all the friends and families, whom have helped me and supported me in one way or another for all these years. It is you people that have shaped what I have become today. I am very grateful.

Finally, I would also like to thank my parents, for your genuine love, and endless support in my life and study. For 25 years, you have always believed in me and have taken very good care of me, lead me to where I am today. Now I have grown up, I hope I have made you proud, and I will not disppoint you for the years to come. Mom and dad, I love you!

Thomas Carlyle once said, *Love is ever the beginning of knowledge as fire is of light.* Let this saying be a self-motivation, to lead me to become a better researcher and a better person.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

In this chapter, we will give a brief history and ongoing developments on two of the most widely adopted wireless systems: Cellular phone and Wireless Local Area Network (WLAN). A complete specification [19] of different generations of cellular and WLAN standards will be provided in Appendix A.

1.1 Cellular Network Standards

1.1.1 First-Generation Systems

First-generation ($1G$) cellular technologies were developed in late 1970s and early 1980s. The best known $1G$ system was Advanced Mobile Phone Service (AMPS), which was developed by Bell Labs and deployed commercially in 1983. Some of the other well known standards include Total Access Communication System (TACS), Nordic Mobile Telephone System (NMT) and NTT. All of these systems were analog systems utilizing Frequency Division Multiple Access (FDMA) scheme [19]. FDMA is a channel access method in which different users are assigned to one or several frequency channels for the transmission of the signals. One detrimental drawback of $1G$ systems was that it lacked *uniform standardization* [39], making it impossible to roam when traveling to a place where a different standard was adopted.

1.1.2 Second-Generation Systems

Time Division Multiple Access (TDMA) Based $2G$ Systems

Due to the incompatibility issues of different $1G$ cellular standards, Groupe Spécial Mobile (GSM) was formed in 1982 to develop a uniform standard for entire Europe [19]. It was deployed in 1989 using time division multiple access (TDMA) in combination with slow frequency hopping (FH) for the voice communication. GSM also evolved to offer packet-based data services via General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE). United States soon followed the step by introducing IS-54 digital cellular standard in 1992. It was later evolved into IS-136 standard. It used the same channel spacing as AMPS to facilitate the analog-to-digital transmission [19]. In 1991, Japan developed its own $2G$ standard, named Personal Digital Cellular (PDC). All these three $2G$ standards were digital systems, different from analog systems of $1G$ cellular standards. Moreover, they all adopted TDMA scheme. TDMA allows multi-users to share the same channel by dividing the transmission time into multiple time frames, each user occupies one or several time frames for the transmission of the signals.

Code Division Multiple Access (CDMA) Based $2G$ Systems

Around the same time, Qualcomm proposed an entirely different $2G$ system based on code division multiple access (CDMA) scheme. This standard was later named IS-95 or cdmaOne. In CDMA, each user is assigned with a spreading sequence, which has low or zero cross-correlations with the sequence assigned to a different user. Signals are deliberately spread by this spreading sequence in the frequency domain to create a new signal occupying a wider bandwidth. This technique is called spread spectrum (SS). At the receiver side, correlations are computed to extract the desired user's signal from the rest of the users. The level of interference will be determined by the cross-correlations of sequences assigned to the different users. The advantages of CDMA over conventional TDMA include:

- Frequency Reuse: In conventional FDMA and TDMA systems, frequency in the immediate adjacent cells cannot be reused to avoid high interference. However, with SS, users are separated by code channels rather than frequency channels. Therefore, this interference issue does not exist.
- Soft Handoff (SHO) Capability: SHO refers to a mobile's ability to maintain a connection to both the old station and the new station during handoff to prevent dropped

calls. This is directly resulted from frequency reuse property. Moreover, the multiple received signals can be combined together to improve transmission quality and signal-to-noise ratio (SNR).

- No Hard Capacity Limit: In conventional FDMA and TDMA systems, if a channel at a particular time slot is occupied, then the user will be blocked. The number of users that the system can support is predetermined. However, in CDMA systems, more users can always be accommodated at the expense of reduced signal quality and SNR.

1.1.3 Third-Generation Systems

Due to these many advantages of CDMA systems over conventional TDMA and FDMA systems, all third generation ($3G$) standards employ CDMA scheme. There are 2 main competing $3G$ technologies. They are cdma2000 which is backward compatible with cdmaOne; and wideband CDMA (W-CDMA) which is backward compatible with GSM. In addition to voice services, $3G$ networks also provide Mbps data rates for high quality audio, video and broadband internet service [19].

1.2 Wireless Local Area Network Standard

WLAN is part of the IEEE 802.11 standards. The initial standard was released in 1997, which occupies 83.5 MHz of bandwidth in 2.4 GHz industrial, scientific and medical (ISM) band. It utilizes PSK modulation along with frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS) [19]. This standard was expanded in 1999 to create 802.11a and 802.11b. 802.11a operates at 5 GHz frequency range, a lesser crowded frequency than 2.4 GHz band. It has switched to orthogonal frequency division multiplexing (OFDM) based air interface instead of FHSS or DSSS [29]. This along with M-Quadrature Amplitude Modulation (MQAM) modulation increases the data rate substantially to 54 Mbps. 802.11b differs from the original 802.11 standard in that it only uses DSSS scheme. It also provides channel coding mechanisms via either Barker sequences or complementary keying (CCK) [29]. The 802.11g standard, finalized in 2003 attempts to combine the best of 802.11a and 802.11b [19]. It operates at 2.4 GHz band for greater range and uses OFDM along with MQAM to provide higher data rate. The latest of 802.11 family released in 2009 was 802.11n. It incorporates multiple-input multiple-output (MIMO) capability along with a 40 MHz channel to the physical layer (PHY), doubling the

channel bandwidth of the original 802.11 PHY standards of 20 MHz. 802.11n can operate at either 2.4 GHz or 5 GHz band. The addition of MIMO architecture along with MQAM and OFDM modulation offers further increased data rate. The 802.11a/b/g/n family of standards are collectively referred to as *Wi-Fi*.

1.3 Future of Wireless Broadband Access

Currently, there are 3 contenders for next generation mobile broadband standard. They are mobile WiMAX from IEEE 802.16 framework; Long Term Evolution (LTE) from 3GPP and Ultra Mobile Broadband (UMB) from 3GPP2 [39]. One common among these 3 technologies is that they all adopt orthogonal frequency division multiple access (OFDMA) as the air interface. This is driven by the need for higher spectral efficiency and higher data rate. Moreover, all 3 competing technologies are based on IP services with no backward compatibility for circuit-switched services. The key features [39] in the next generation mobile broadband include: increased data rates; high spectral efficiency; flexible radio planning; reduced latency; all-IP architecture; open interfaces, spectral flexibility and security. The Figure 1.1 [39] is an illustration of historic development of wireless technologies.

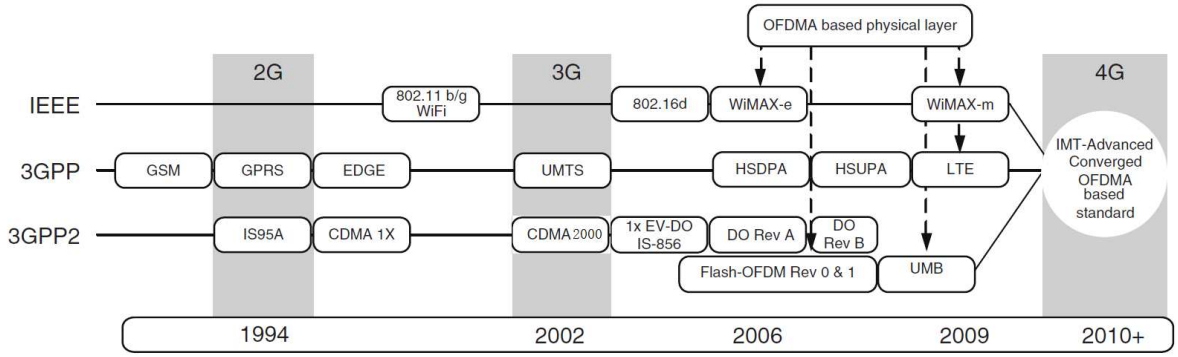

Figure 1.1: Evolutionary Path of Wireless Technology

The goal of this research is to examine the effects of various sequences being applied to OFDM in WLAN systems and CDMA in cellular systems. More specifically, we will focus on the peak to mean average power ratio (PMEPR) and correlation properties of these sequences. This is because sequences with low PMEPR properties are crucial in multi-carrier (MC) systems such as OFDM, while sequences with low autocorrelation values are important in the design of spreading sequences in CDMA systems.

The thesis is organized as follows: In Chapter 2, we will give the necessary background information and introduce the notations used throughout the thesis. In Chapter 3, we will give constructions of different sequences that we will examine for PMEPR and/or merit factor properties. This include m-sequences, quadratic residue sequences, Golay sequences, Sidelnikov sequences, Frank sequences, Frank-Zadoff-Chu (FZC) sequences, DFT spreading sequence sets and perfect spreading sequence sets. In Chapter 4, we will first give a brief overview of the OFDM system, then we will provide detailed simulation results on the PMEPR behavior of these different sequences. In Chapter 5, we will first given an overview on the historic research developments of merit factor, then we will derive a loose upper bound on the relationship between PMEPR and merit factor, finally we will show our simulation results on the merit factor of various sequences. In Chapter 6, we will focus on the new findings of the existence of a large zero autocorrelation zone (ZACZ) for a class of GDJ Golay sequences. There are a total of 3 cases belong to this class. We will provide mathematical proof for 1 of the cases and demonstrate all 3 cases of GDJ Golay sequences with large ZACZ using concrete examples.

Chapter 2

Prelimenaries

2.1 Finite Field

Definition 1 *[20] A group is a set G together with a binary operation * on G such that the following three properties hold:*

1. ** is associative; for any $a, b, c \in G$,*

$$a * (b * c) = (a * b) * c$$

2. *There is an identity element e in G such that for all $a \in G$,*

$$a * e = e * a = a$$

3. *For each $a \in G$, there exists an inverse element $a^{-1} \in G$ such that*

$$a * a^{-1} = a^{-1} * a = e$$

4. *For all $a, b \in G$,*

$$a * b = b * a$$

Then the group is called Abelian or commutative.

Definition 2 *[20] A ring $(R, +, \cdot)$ is a set R, together with two binary operations, denoted by $+$ and $\cdot$, such that*

1. *R is an Abelian group with respect to $+$.*

2. *$\cdot$ is associative*

3. *The distributive laws hold; for all $a, b, c \in G$*

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) and (b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

Definition 3 *[20] A field is a ring $(F, +, \cdot)$ such that F^* together with multiplication $\cdot$ forms a commutative group.*

2.2 Construction of $GF(p^n)$

Definition 4 *A finite field $GF(P^n)$ of order p^n can be constructed using an irreducible polynomial $f(x)$ over $GF(p)$ of degree n. Let α be a root of $f(x)$ such that $f(\alpha) = 0$, then $GF(P^n)$ is defined as follows:*

$$GF(p^n) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} | a_i \in GF(p)\}$$

The following table is an example of finite field $GF(2^3)$ defined by irreducible polynomial $f(x) = x^3 + x + 1$

Table 2.1: $GF(2^3)$ defined by $f(x) = x^3 + x + 1$

as a 3-tuple	as a polynomial	as a power of α
000	0	0
001	1	1
010	α	α
011	α^2	α^2
100	$1 + \alpha$	α^3
110	$\alpha + \alpha^2$	α^4
111	$1 + \alpha + \alpha^2$	α^5
101	$1 + \alpha^2$	α^6

2.3 Trace Function

Definition 5 *[20] Let q be a prime or a power of a prime. For $\alpha \in F = GF(q^n)$ and $K \in GF(q)$, the trace function $Tr_{F/K}(x), x \in F$, is defined by*

$$Tr_{F/K}(x) = x + x^q + \cdots + x^{q^{n-1}}, x \in F$$

If $q = 2$ for the above definition, then $Tr_{F/K}(x)$ is a mapping from $F \in GF(2^n)$ to binary integer 0 and 1, or equivalently

$$Tr_{F/K}(x) = x + x^2 + \cdots + x^{2^{n-1}} \in GF(2), \forall x \in GF(2^n)$$

2.4 Primitive Polynomial

Definition 6 *[20] An irreducible polynomial over $GF(p)$ having a primitive element in $GF(p^n)$ as a zero is called a primitive polynomial over $GF(p)$.*

2.5 Autocorrelation

Definition 7 *Let $H \geq 2$ be an integer and ξ_H be the primitive H-th root of unity, i.e., $\xi_H = \exp(2\pi\sqrt{-1}/H)$. For a sequence $a = (a_0, a_1, \cdots, a_{N-1})$ over Z_H of period N, its* aperiodic autocorrelation function *and* periodic autocorrelation function *are respectively defined by*

$$C_a(u) = \sum_{i=0}^{N-1-u} \xi_H^{a_i - a_{i+u}}, u = 0, 1, \cdots \tag{2.1}$$

and

$$R_a(u) = \sum_{i=0}^{N-1} \xi_H^{a_i - a_{i+u}}, u = 0, 1, \cdots . \tag{2.2}$$

2.6 Generalized Boolean Function

Definition 8 *A* generalized Boolean function $f(x_1, \cdots, x_m)$ *with* m *variables is a mapping from* $\mathbb{Z}_2^m$ *to* $\mathbb{Z}_H$*, which has an unique representation as a multiple polynomial over* $\mathbb{Z}_H$ *of the special form:*

$$f(x_1, \cdots, x_m) = \sum_{I \in \{1, \cdots, m\}} a_I \Pi_{i \in I} x_i, \ a_I \in \mathbb{Z}_H. \tag{2.3}$$

This is called the algebraic normal form *of* f*. The* algebraic degree *is defined by the maximum value of the size of the set* I *with* $a_I \neq 0$*.*

Let $(i_1, \cdots, i_m)$ be the binary representation of the integer $i = \sum_{k=1}^{m} i_k 2^{m-k}$. The *truth table* of a Boolean function $f(x_1, \cdots, x_m)$ is a binary string of length 2^m, where the i-th element of the string is equal to $f(i_1, \cdots, i_m)$. For example, $m = 3$, we have

$$f = (f(0,0,0), f(0,0,1), f(0,1,0), f(0,1,1), f(1,0,0), f(1,0,1), f(1,1,0), f(1,1,1)).$$

2.7 Linear Feedback Shift Register

A binary linear feedback shift register (LFSR) is a device that performs XOR operations based on the feedback function. It shifts the data in each register into adjacent registers, or out of the register if it's on the edge. The Figure 2.1 below is an illustration of LFSR. It contains three main components:

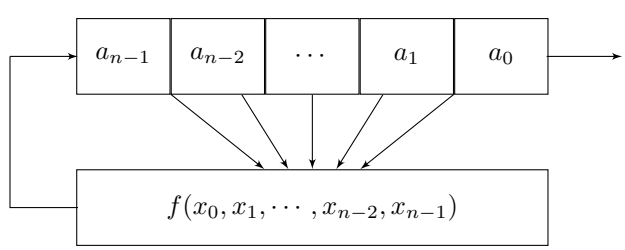

Figure 2.1: Linear Feedback Shift Register(LFSR)

1. n-stage shift register.

2. Initial state $(a_0, a_1, \cdots, a_n - 1)$.

3. Feedback function $f(x_0, x_1, \cdots x_{n-1})$ is a boolean function of n variables defined in Section 2.6, when $H = 2$.

Chapter 3

Known Sequences Constructions

3.1 m-Sequences

m-sequence is also known as maximum length sequence. It is periodic and produces the maximum period. For a binary m-sequence of degree n, the period is $2^n - 1$. A binary m-sequence can be implemented in two ways: LFSR or trace functions.

For the n stage LFSR implementation, the feedback function in the LFSR is given by a primitive polynomial of degree n. The initial state can be any combinations other than all zero states. This will generate a m-sequence of period $2^n - 1$.

Let α be a primitive element in $GF(2^n)$, the trace representation of i-th element of a binary m-sequence $\underline{a}$ is given by

$$a_i = Tr(\beta\alpha^i), \forall i \geq 0, \beta \in GF(2^n).$$

3.2 Quadratic Residue (Legendre) Sequences

Let p be an odd prime number. For an integer i where $0 < i < p$, i is called a quadratic residue modulo p if there exists an integer x such that $x^2 \equiv i \bmod p$. The Legendre symbol $\frac{i}{p}$ is defined by

$$\frac{i}{p} = \begin{cases} 1, & \text{If i is a quadratic residue modulo p} \\ -1, & \text{Otherwise.} \end{cases}$$

Then quadratic residue sequence $\underline{a}$ is constructed by setting $a_0 = 1$, and

$$a_i = \begin{cases} 0 \Longleftrightarrow \frac{i}{p} = 1 \\ 1 \Longleftrightarrow \frac{i}{p} = -1 \end{cases}$$

where $0 < i < p$.

3.3 Golay Sequences

Let $m \geq 2$ be a positive integer and $n = 2^m$. Then a Golay sequence [10, 42] $\underline{a}$ over Z_{2^h} of length n is defined by

$$\begin{aligned} a_i &= a(i_1, i_2, \cdots, i_m) \\ &= 2^{h-1} \sum_{k=1}^{m-1} i_{\pi(k)} i_{\pi(k+1)} + \sum_{k=1}^{m} c_k i_{\pi(k)} + c_0 \end{aligned} \tag{3.1}$$

where π can take any permutations and $c_i \in Z_{2^h}$, $i = 0, 1, \cdots, m$. The sequence $\underline{a}$ and $a_i + 2^{h-1} i_{\pi(1)} + c'$ are together called a Golay complementary pair of length 2^m for any $c' \in Z_{2^h}$.

3.4 Sidelnikov Sequences

Let $GF(q)$ be a finite field with $q = p^m$ and M a divisor of $q-1$, where p is a prime number and m is a positive integer. Let α be a primitive element in $GF(q)$ and $D_k = \{\alpha^{Mi+k} - 1 | 0 \leq i < \frac{q-1}{M}\}$ for $0 \leq k \leq M-1$. The M-ary Sidelnikov sequence [63] $\underline{s} = \{s_t | 0 \leq t \leq q-2\}$ of period $q-1$ is defined by

$$a_i = \begin{cases} 0, & if \quad \alpha^t = -1 \\ k, & if \quad \alpha^t \in D_k \end{cases}$$

Or equivalently, s_t can be defined by

$$s_t \equiv log_\alpha(\alpha^t + 1) \mod M, 0 \leq t \leq q-2$$

Let ξ_M be the M-th root of unity, the modulated Sidelnikov sequences [63] of s_t becomes $\xi_M^{s_t}$.

3.5 Frank Sequences

Let ξ_q be q-th root of unity, a Frank sequence [15] $\underline{a}$ of length q^2 is defined as

$$a_{jq+k} = \xi_q^{rjk} \tag{3.2}$$

where $0 \leq j, k < q$ and $\gcd(r, q) = 1$

3.6 Frank-Zadoff-Chu (FZC) Sequences

Let ξ_N be N-th root of unity, a ZC sequence [8] $\underline{a}$ of length N is defined as

$$a_i = \begin{cases} \xi_N^{\frac{r \times i^2}{2}}, & \text{if } N \text{ is even} \\ \xi_N^{\frac{r \times i(i+1)}{2}}, & \text{if } N \text{ is odd} \end{cases} \tag{3.3}$$

where $0 \leq i < N$, $0 < r < N$ and $\gcd(r, N) = 1$

3.7 DFT Spreading Sequences

Let ξ_N be N-th root of unity, a $N \times N$ DFT spreading sequence d is defined by

$$d_{i,j} = \xi_N^{-ij/N} \tag{3.4}$$

where $0 \leq i, j < N$.

3.8 Perfect Spreading Sequences

A *perfect* sequence is defined as all of the out-of-phase periodic autocorrelations of a sequence are equal to 0. Some known perfect sequences include the Frank sequences, Frank-Zadoff-Chu (FZC) sequences [15, 8] defined in (3.2) and (3.3), the modulatable orthogonal sequences [50] and the generalized chirp-like sequences [44]. They are all polyphase sequences. The construction of spreading sequences set from the perfect sequences is as follows.

Let $\underline{a}$ be a perfect sequence of length N, then for $N \geq L$, a $L \times N$ perfect spreading matrix d is constructed by

$$d_{i,j} = a_{(i+j) \mod N} \tag{3.5}$$

where $0 \leq i < L$, $0 \leq j < N$.

Chapter 4

PMEPR of Different Types of Sequences

4.1 OFDM System

In conventional single-carrier (SC) broadband wireless communication systems, one problem arises as data rate increases. Multi-path propagation of signals introduces significant delays into the system, which results in high Inter Symbol Interference (ISI). Consequently, this increases the bit error rate (BER) of the received signals substantially. The effect of ISI on the transmission error statistics are negligible as long as the delay spread of the symbol is significantly shorter than the duration of the transmitted signal [22]. However, this problem becomes inevitably unavoidable in today's high data rate driven wireless broadband communication systems.

One alternative in an attempt to resolve this downside is to replace the SC system with a multi-carrier (MC) system. Orthogonal frequency division multiplexing (OFDM) is one of the example. It divides the allocated bandwidth into a number of orthogonal narrow-band sub-channels. Data are transmitted over these sub-channels in parallel. The overall data rate is the sum of data rate from all collective sub-channels. This allows the design of a system supporting high data rate, while maintaining ISI at a manageable level.

The concept of OFDM was first introduced by Chang in a seminal paper in 1966 [5]. The term OFDM was later appeared in a separate patent of his in 1970 [6]. OFDM is a special case of Frequency Division Multiplexing (FDM). The key difference between FDM and OFDM resides in the division of spectrum for the sub-carriers. Conventional

FDM systems divide available bandwidth into non-overlapping sub-carriers, while OFDM systems divide the available bandwidth into overlapping sub-carriers. OFDM systems are able to do so because each sub-carrier is orthogonal to all other sub-carriers. i.e.,

$$\frac{1}{T}\int_0^T (e^{2\pi i \Delta f t})^* (e^{(2\pi k \Delta f t)})\,\mathrm{d}t = \delta_{ik}$$

where i, k represent sub-carriers, $(.)^*$ denotes the complex conjugate, and δ is the Kronecker delta function.

The division of bandwidth into overlapping sub-carriers in OFDM systems results in much higher spectral efficiency than conventional FDM systems. This is illustrated in the comparison between Figures 4.1 and 4.2. The saved bandwidth can be made into new sub-carriers to increase the data rate. However, in doing so, OFDM systems are also more sensitive to Inter Carrier Interference (ICI). Any loss in the orthogonality between sub-carriers will significantly impact the performance of OFDM systems.

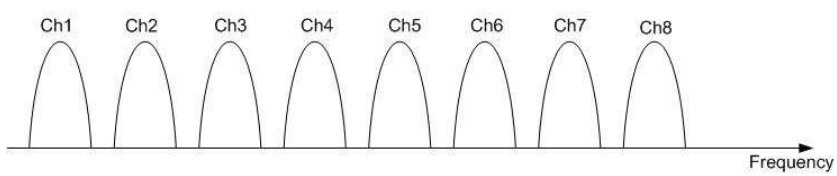

Figure 4.1: FDM system

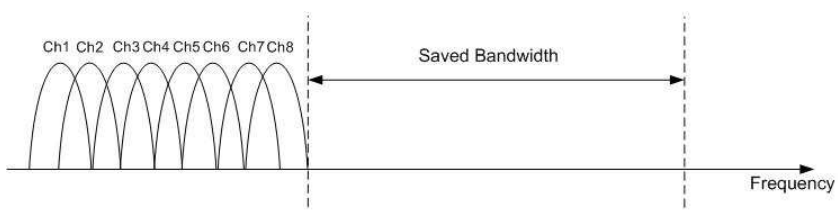

Figure 4.2: OFDM System

The modulation and demodulation of OFDM signals can be implemented in hardware efficiently using Fast Fourier Transform (FFT) and Inverse Fast Fourier Transform (IFFT) respectively. The transmitter and receiver of OFDM system is shown in Figures 4.3 and 4.4.

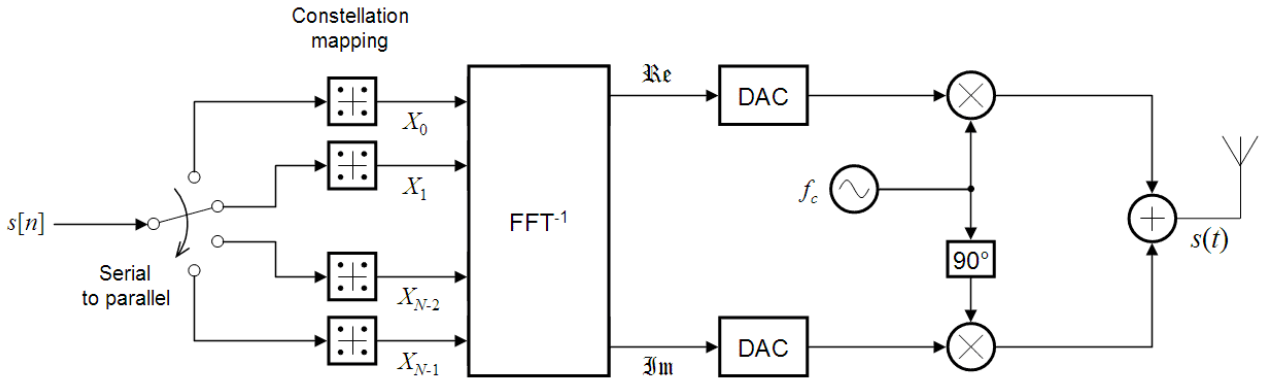

Figure 4.3: OFDM Transmitter

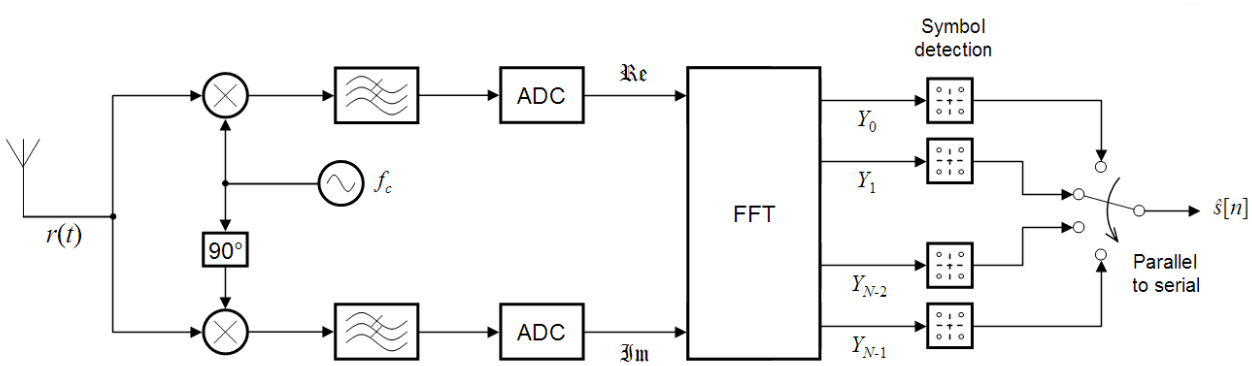

Figure 4.4: OFDM Receiver

While MC systems such as OFDM transmission over wireless channels alleviate high ISI presented in the conventional SC system, it too has drawbacks that need to be contend with, namely high peak-to-mean envelope power ratio (PMEPR) and sensitivity to phase/frequency noise. In this chapter, we will be discussing the PMEPR aspect.

4.2 PMEPR and PAPR

The transmitter and receiver structure of OFDM systems are shown in Figures 4.3 and 4.4 [56]. Based on the OFDM transmitter, one can see that the transmitted baseband OFDM

symbol is defined by

$$s(t) = \sum_{i=0}^{n-1} \xi_H^{a_i + Hi\Delta ft}, 0 \leq t < T \tag{4.1}$$

where $\xi_H = \exp j2\pi/H$, $a_i \in Z_H$, $\Delta f = 1/T$, n represents the total number of sub-carriers. a_i is the transmitted signal, Δf is the frequency separation of each narrow-band sub-carrier. In order for all sub-carriers to be orthogonal to each other, the minimum sub-carrier spacings need to be $1/2T$. However, it is usually kept at $1/T$. The purple line in Figure 4.5 below is the simulated transmitted OFDM symbol with the number of sub-carriers $n = 4$. Different colors in the figures can be observed by the electronic copy of this thesis. The rest are the underlying sub-carrier signals. Note that the amplitude of the OFDM symbol can be significantly greater than the amplitude of the underlying sub-carriers.

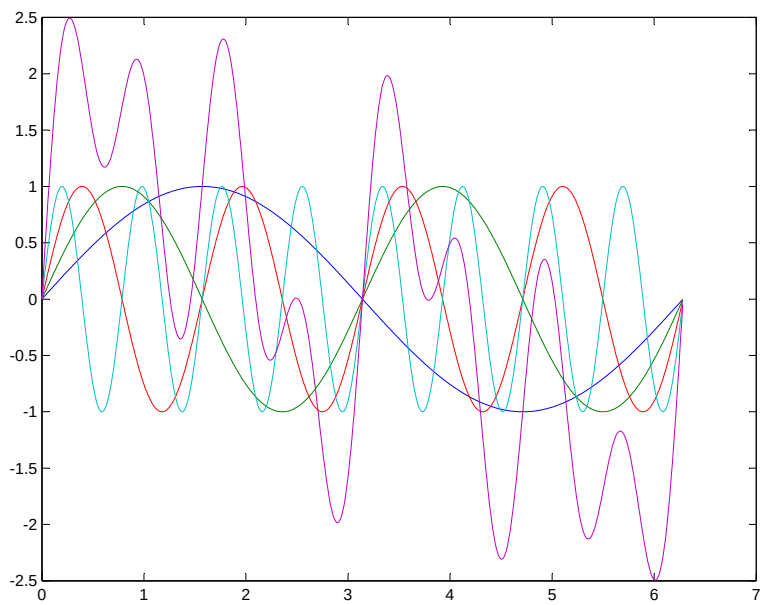

Figure 4.5: OFDM Symbol and Underlying Sub-carriers

Instantaneous envelope power is defined by the amplitude of the OFDM symbol in (4.1) squared as follows

$$P(t) \quad = \quad \sum_{i,j} \xi^{a_i - a_j + H(i-j)\Delta ft}.$$

Let $j = i + u$ and $\xi = \xi_H$ for simplicity. We observe that $\sum_i \xi^{a_i - a_{i+u}}$ is the definition of aperiodic autocorrelation from (2.1). Thus we can replace $\sum_i \xi^{a_i - a_{i+u}}$ with $C_a(u)$. Then

$$\begin{aligned} P(t) &= n + \sum_{u \neq 0} C_a(u) \xi^{-H(u)\Delta f t} \\ &\leq n + \sum_{u \neq 0} |C_a(u)| \\ &\leq n + 2 \sum_{u=1}^{n-1} (n - u) \\ &= n^2. \end{aligned} \tag{4.2}$$

Peak envelope power (PEP) is the supremum over a symbol period of $P(t)$.

$$PMEPR = \frac{PEP}{n}.$$

PMEPR measures the peak to average power ratio in the baseband. On the other hand, PAPR measures the peak to average power ratio in the passband. Namely the transmitted passband signal $\hat{s}(t)$ becomes

$$\hat{s}(t) = \Re(s(t) e^{j2\pi f_c t}).$$

In conclusion, we have PMEPR and PAPR defined as follows:

$$PMEPR = \frac{max_t |s(t)|^2}{n}. \tag{4.3}$$

$$PAPR = \frac{max_t |\Re(s(t) e^{j2\pi f_c t})|^2}{n}. \tag{4.4}$$

PMEPR provides an upper bound on PAPR. If the carrier frequency f_c is much greater than the bandwidth of the signal $s(t)$, then it can be shown that this bound is quite accurate [34]. In all our simulation results, we have chosen to compute the PMEPR values.

If the signal of all sub-carriers adds up constructively, then theoretically PEP can be as high as n^2. Consequently, the maximum value of PMEPR can reach n. This is one of the most detrimental aspect of OFDM systems. It will affect the communication system in the two following ways:

1. Affect power amplifier in the transmitter side.

2. Decrease Signal-to-Quantization Noise Ratio (SQNR) of both Analog-to-Digital Converter (ADC) and Digital-to-Analog Converter (DAC).

A number of techniques have been proposed to combat this problem. This includes amplitude clipping and filtering [33, 2], coding [9, 10, 42, 43, 7], the selected mapping technique [38, 3], and the interleaving technique [26, 13, 30]. In this thesis, we will focus on the coding method. We will examine the PMEPR of some known constructions of sequences. However, in applying the sequences design for OFDM via coding, the length of coded sequences is inevitably longer than the uncoded information bit length. This implies that coding will incur a cost of reduced code rate.

Evaluating power in continuous time domain cannot easily performed. Therefore, PMEPR is usually estimated discretely by sampling the continuous time domain signals. The representation of PMEPR in discrete time domain is denoted by

$$PMEPR = \frac{max_k |\sum_{i=0}^{n-1} \xi^{a_i + Hi\Delta fk/N_s}|^2}{n}, 0 \leq k < Ns \tag{4.5}$$

where N_s is the oversampling rate and it is an integer multiple of n.

In [34], it is shown that for every MC signal $S(t)$, where $n > 3$, the relationship between continuous time signal $S_c(t)$ and discrete time signal $S_d(t)$ is given by the upper bound

$$S_c(t) < \left(\frac{2}{\pi} ln(n) + 1.132 + \frac{4}{n}\right) S_d(t).$$

Then we could derive the bound between PMEPR in continuous time domain and discrete time domain by

$$PMEPR_c < \left(\frac{2}{\pi} ln(n) + 1.132 + \frac{4}{n}\right)^2 \times PMEPR_d. \tag{4.6}$$

Once we have obtained PMEPR of the OFDM symbol in discrete time domain, we have a fairly accurate estimation of real PMEPR. Moreover, the higher the sampling rates, the more accurate the results will be.

Although the PMEPR can be as high as n, [41] [55] [12] [60] [61] [16] have showed that a randomly generated codeword having this high PMEPR is highly improbable. Moreover, [41], [55] and [49] have showed that the asymptotic PMEPR value of a randomly generated codeword of length n is of the order log n.

Binary sequences with the best known PMEPR properties up-to-date are Golay sequences. They have a PMEPR of at most 2 regardless the length of the sequence. A short proof is given as follows. It is shown previously in (4.2) that the power of a sequence $\underline{a}$ is given by

$$P_a(t) = n + \sum_{u \neq 0} R_a(u) \xi^{-H(u)\Delta f t}.$$

Using the property of the sum of periodic autocorrelation functions of a Golay complementary pair $\underline{a}$ and $\underline{b}$ equals to 0, we obtain the following

$$\begin{aligned} P_a(t) + P_b(t) &= 2n + \sum_{u \neq 0} (R_a(u) + R_b(u)) \xi^{-H(u)\Delta f t} \\ &= 2n. \end{aligned}$$

The sum of power of the Golay pair is $2n$. The power of any one Golay sequence is at most $2n$. Consequently, PMEPR of any one sequence is at most 2.

In the following sections, we will examine the PMEPR behaviour of both single sequences and spreading sequences set.

4.3 PMEPR of Single Sequences: Comparisons of New Sequences and Other Known Sequences

In this section, we will present our simulations results. We have computed PMEPR value for 6 classes of single sequences. They are m sequences, Sidelnikov sequences, new sequences, Golay sequences, FZC sequences and Legendre sequences.

4.3.1 New Sequences Construction

A new sequence [54] is constructed by combing an m-sequence $\underline{m} = \{m_i\}$ and an M-ary modulated Sidelnikov sequence $\underline{s} = \{s_i\}$ of the same length n. The resulting sequence $\underline{a} = \{a_i\}$ will be a $2M$-ary sequence with the same length. It is denoted by

$$a_i = (-1)^{m_i} \times s_i$$

where $0 < i < n$.

4.3.2 Sequences Parameters

Golay, m and Legendre sequences are binary sequences. Sidelnikov sequences are chosen to be ternary sequences, new sequences are 6-ary and FZC sequences are n-ary with where n is also the length of FZC sequences. We consider these sequences for both degree 10 and 12. The length of these various sequences is listed in Table 4.3.2 below.

Table 4.1: Length of the Single Sequences

	Length					
	m	Sidelnikov	New	Golay	FZC	Legendre
Degree 10	1023	1023	1023	1024	1024	1021
Degree 12	4095	4095	1023	4096	4096	4093

The parameters used to construct these sequences are as follows.

1. The primitive polynomials used to generate m-sequences and Sidelnikov sequences are $x^{10} + x^3 + 1$ and $x^{12} + x^6 + x^4 + x + 1$ for degree 10 and 12 respectively.

2. New sequences are generated by m-sequences and Sidelnikov sequences described above.

3. From the Golay complementary pair, a_i from (3.1) is selected with identity permutation and all constant terms set to 0

4. For FZC sequences, the length of sequence is 1024 and 4096, both are even integers. Therefore, $a_i = \xi_N^{r \times i^2}$ with r chosen to be 1.

5. The two prime numbers used to generate Legendre sequences are 1021 and 4093 respectively.

In the evaluation of PMEPR for various sequences, not only did we evaluate the PMEPR of the sequence itself, we also modified the length of the sequence. The sequence length ranges from the original length minus 100 by removing the last 100 bits to plus 100 by cyclically appending 100 bits. The idea comes from [4] and [32], in which the merit factor of a sequence is increased by appending a portion of the sequence. In the next chapter, we will show the relationship between PMEPR and merit factor. For now, we just want to observe the change in the behaviour of PMEPR by discarding and appending to the original sequence.

4.3.3 PMEPR Comparisons

The experiment were conducted with 3 different sampling rates. No oversampling ($N_s = n$), 2-times oversampling ($N_s = 2n$) and 8-times oversampling ($N_s = 8n$). We expect results to be less accurate and exist more fluctuations at lower sampling rates. This is precisely the case as we take a look at the following results from Figures 4.6 to 4.17 for sequences of degree 10 and 12. We can observe that graphs at 8-times oversampling rate are much more smoother than the other 2 sampling rates. Their values are also higher suggesting that they are closer to the accurate PMEPR values. Note PMEPR of all sequences in the graph is expressed in terms of db, that is

$$PMEPR_{db} = 10 \times log_{10}(PMEPR_{linear}).$$

The PMEPR of the original sequences of degree 10 and degree 12 is generalized in Table 4.3.3.

Table 4.2: PMEPR of the Single Sequences

	PMEPR					
	m	Sidelnikov	New	Golay	FZC	Legendre
Degree 10	5.84	6.21	9.23	3.01	2.56	8.16
Degree 12	6.93	6.30	8.67	3.01	2.56	7.73

The summary of the minimum and maximum PMEPR value of modified sequences with their corresponding sequence length is generalized in Table 4.3.3. The data are taken from 8-times oversampling because they represent the most accurate data.

The PMEPR of m-sequences increases almost linearly with the length. It ranges from $5.25dB$ to $9.03dB$ and from $6.26dB$ to $8.21dB$ for degree 10 and 12 respectively. This can be seen in Figures 4.6 and 4.7.

The PMEPR behaviour of Sidelnikov sequences is similar to m-sequences. Its PMEPR value is gradually increasing as the length of sequence increases. The PMEPR of Sidelnikov sequences increases from $5.44dB$ to $7.87dB$ for degree 10. For degree 12, the rate of increase in PMEPR over the length is slower. It ranges from $6.10dB$ to $7.30dB$. This can be seen in Figures 4.8 and 4.9.

The PMEPR behaviour of new sequences is quite different between degree 10 and degree 12. For degree 10, the PMEPR value increases substantially over the length of the

Table 4.3: PMEPR of the Modified Single Sequences

		Single Sequences					
		m	Sidelnikov	New	Golay	FZC	Legendre
10	$PMEPR_{min}$	5.25	5.30	7.44	3.01	2.04	6.18
	Length	989	925	923	1024	968	938
	$PMEPR_{max}$	9.03	7.87	10.34	5.47	8.36	9.92
	Length	1123	1116	1120	926	1078	1099
12	$PMEPR_{min}$	6.26	6.10	8.49	3.01	1.94	7.53
	Length	4011	5076	4128	4096	3998	3995
	$PMEPR_{max}$	8.21	7.30	9.01	4.71	8.41	8.69
	Length	4195	4194	3998	3996	4196	4183

sequence. It increases from $7.44dB$ when the sequence length is 923 to $10.34dB$ when the sequence length becomes 1120. This is seen in Figure 4.10. However, for degree 12, the new sequence stays almost flat throughout the entire length. The maximum PMEPR is $9.01dB$ and minimum $8.49dB$, the difference is only about $0.52dB$. This is shown in Figure 4.11.

The shape of PMEPR plot for Golay sequences resembles to an upset-down triangle. We have discussed earlier that the PMEPR of Golay sequences is at most 2, or equivalently $3.01dB$, we see this is exactly the case. The PMEPR reaches the minimum of $3.01dB$ when sequence length is 1024 and 4096 for degree 10 and 12 respectively. However, as soon as some bits are removed or appended, the PMEPR values immediately rise. It reaches maximum value of $5.47dB$ for degree 10 and $4.71dB$ for degree 12 as illustrated in Figures 4.12 and 4.13.

Polyphase FZC sequences have the best value when the entire sequence is retained or a portion of the sequence is removed. However, as soon as we cyclicly append to the sequence, the PMEPR properties deteriorate very rapidly as shown in Figures 4.14 and 4.15. The maximum PMEPR value is $8.36dB$ for degree 10 and $8.41dB$ for degree 12.

The PMEPR behaviour of Legendre sequences is quite similar to new sequences. For degree 10, the PMEPR value increases linearly and consistently as the sequence length increases. The difference between the maximum and minimum PMEPR is about $3.7dB$. This is shown in Figure 4.16. For degree 12 case, the PMEPR values stays almost flat throughout the first half lengths of the sequence, then it increases slowly for the rest of the lengths. The difference between the maximum PMEPR and the minimum PMEPR is only

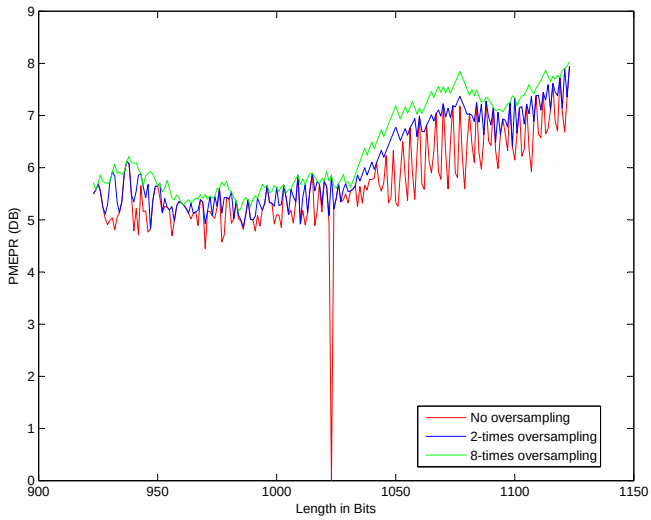

Figure 4.6: PMEPR of m-sequence of Degree 10

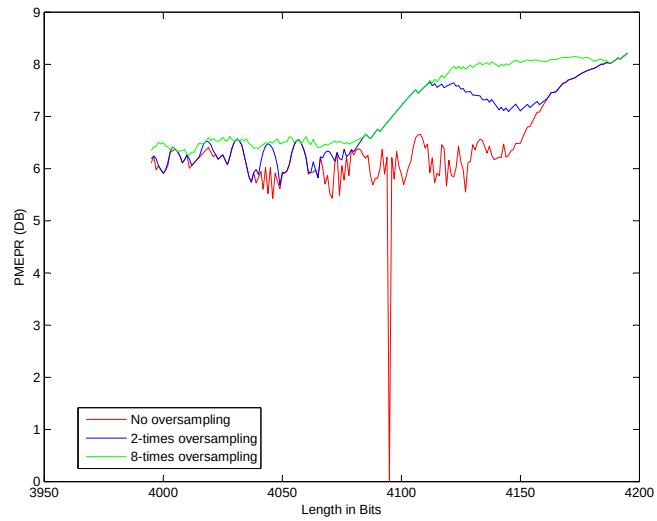

Figure 4.7: PMEPR of m-sequence of Degree 12

approximately $1.2dB$. This is considerably less than the $3.74dB$ difference for the degree 10 case. This is shown in Figure 4.17.

4.4 PMEPR of Spreading Sequence Sets

In this section, we will examine the PMEPR behaviour of 6 classes of spreading sequence sets. They are 5 classes from the previous section plus the DFT spreading sequences defined by (3.4) in section 3.7.

The parameters used to generate the single sequences which is then constructed into spreading sequences are as follows

1. The primitive polynomials used to generate m-sequences and Sidelnikov sequences are $x^6 + x + 1$ and $x^8 + x^4 + x^3 + x^2 + 1$ for degree 6 and 8 respectively.

2. New sequences are generated by the m-sequence and Sidelnikov sequence described above.

3. From Golay Complementary Pair, a_i from (3.1) is selected with identity permutation and all constant terms are set to 0

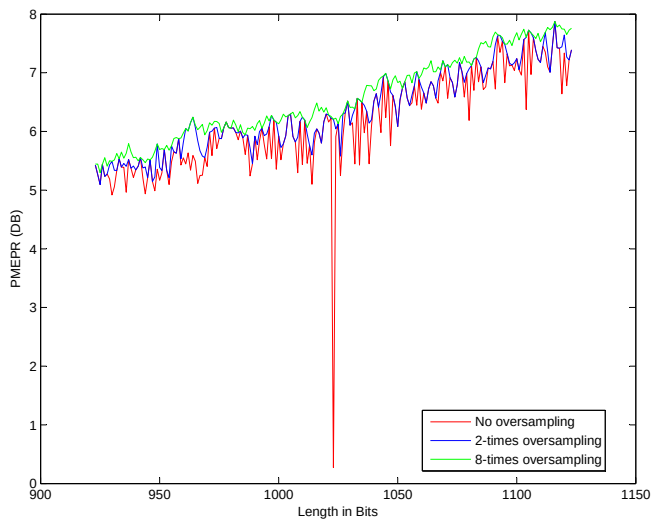

Figure 4.8: PMEPR of Sidelnikov Sequence of Degree 10

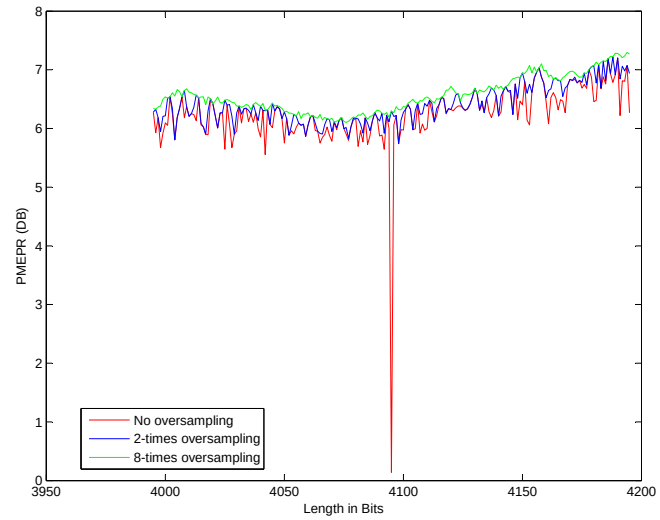

Figure 4.9: PMEPR of Sidelnikov Sequence of Degree 12

4. For FZC sequences of degree 6 and 8, the length of the sequence is 64 and 256 respectively, both are even integers. Therefore, $a_i = \xi_N^{r \times i^2}$ with r chosen to be 1.

From single sequences to construct a spreading sequence set, we will use the same method as described by (3.5) in Section 3.8, An L spreading sequence d_i, $i \leq L$ of length N is defined by

$$d_{i,j} = a_{(i+j) \mod N}$$

where d_i is the ith single sequence, $d_{i,j}$ represents the jth element in sequence d_i, $0 \leq j < N$ and $0 < L \leq N$.

The PMEPR of a spreading sequence in discrete domain is then defined by

$$PMEPR = \frac{max_k |\sum_{i=0}^{L-1} \sum_{j=0}^{N-1} \xi^{d_{i,j} + Hij\Delta fk/N_s}|^2}{NL}, 0 \leq k < N_s, . \tag{4.7}$$

The length N of 6 classes of sequences of degree 6 and 8 is expressed in the Table 4.4.

By applying equation (4.7), and varying the number of rows L from 1 to N, we have obtained PMEPR values for all 6 classes of spreading sequences which are plotted into Figures 4.18 and 4.19 below. PMEPR again is measured in dB.

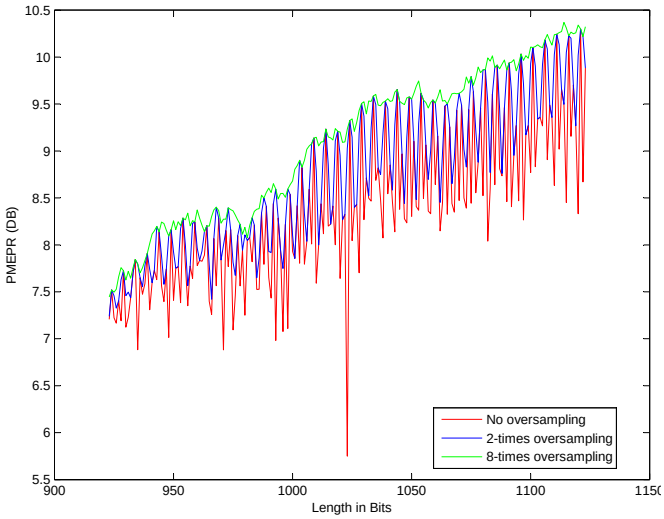

Figure 4.10: PMEPR of New Sequence of Degree 10

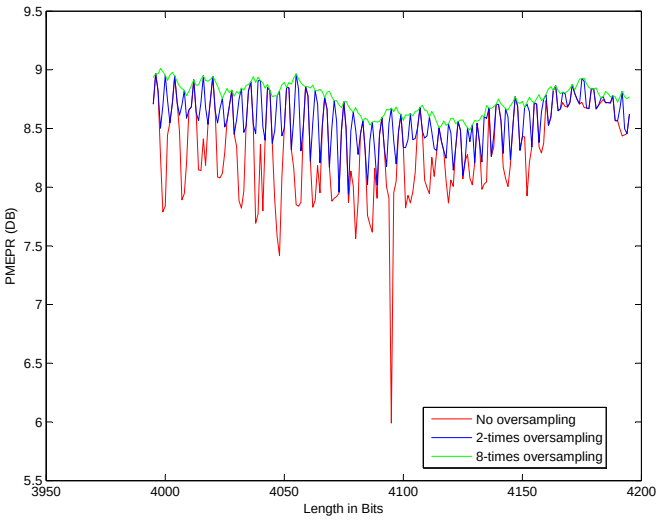

Figure 4.11: PMEPR of New Sequence of Degree 12

Table 4.4: Length of the Spreading Sequence Sets

	Length					
	m	Sidelnikov	New	Golay	FZC	DFT
Degree 6	63	63	63	64	64	64
Degree 8	255	255	255	256	256	256

For degree 6 in Figure 4.18, we observe that FZC, Golay, Sidelnikov and m spreading sequences have similar PMEPR performances. The FZC spreading sequence behaves approximately $2dB$ better at low value of L, while the other 3 spreading sequences behave virtually the same. The new spreading sequence is always few dB higher than these four spreading sequences. The DFT spreading sequence behave very poorly at lower values of L. However, its PMEPR values improve exponentially as the values of L increase. At higher L values, Sidelnikov, DFT and m spreading sequences have approximately the same PMEPRs at $6.3dB$, while the FZC, Golay and new spreading sequences are approximately $3dB - 4dB$ higher.

For degree 8 case in Figure 4.19, the spreading sequence sets of FZC, Golay, Sidelnikov and m sequences are behaving very similarly. Once again, FZC spreading sequences are

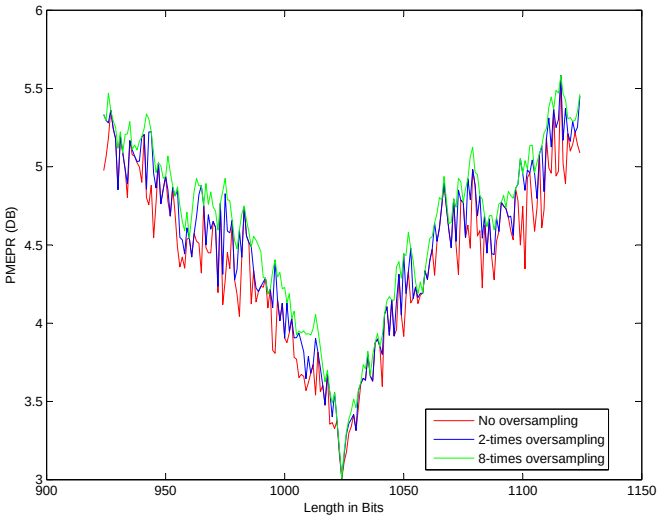

Figure 4.12: PMEPR of Golay Sequence of Degree 10

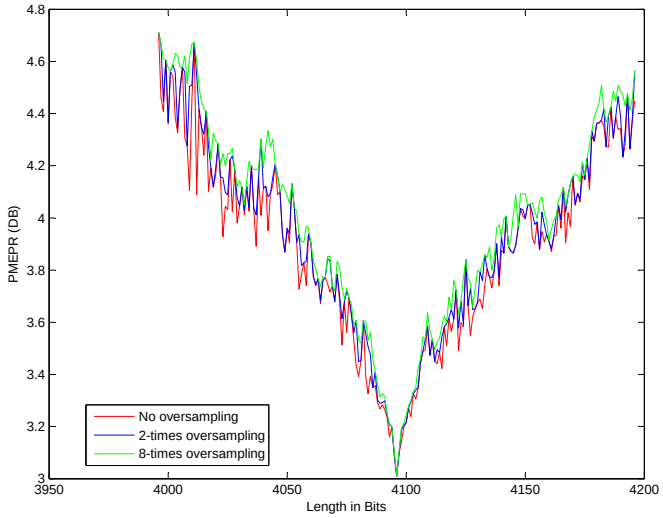

Figure 4.13: PMEPR of Golay Sequence of Degree 12

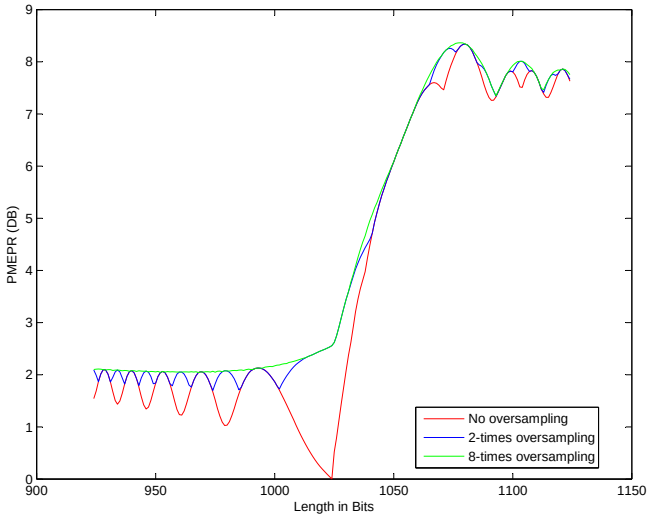

Figure 4.14: PMEPR of FZC Sequence of Degree 10

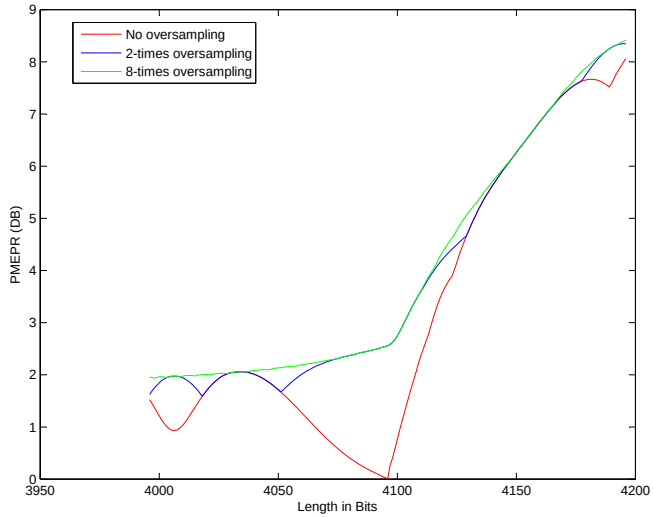

Figure 4.15: PMEPR of FZC Sequence of Degree 12

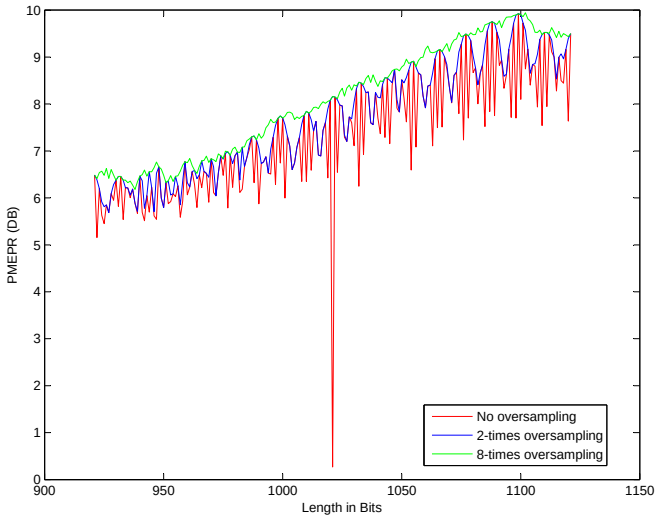

Figure 4.16: PMEPR of Legendre Sequence of Degree 10

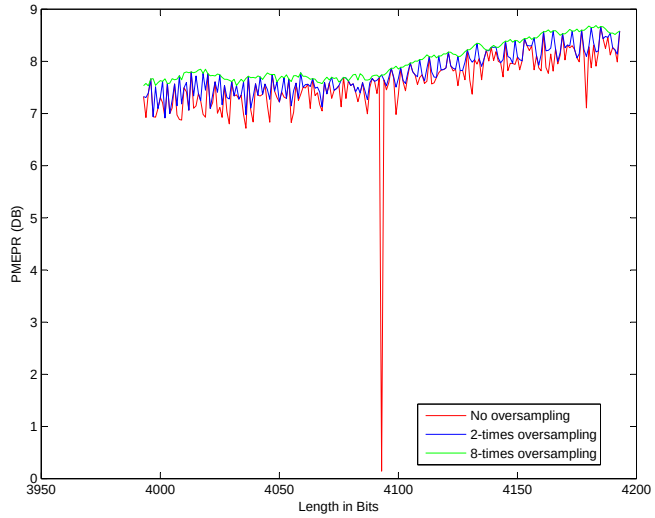

Figure 4.17: PMEPR of Legendre Sequence of Degree 12

approximately $2dB$ better at lower values L, but these 4 classes all converge to approximately $8dB$. DFT spreading sequences still have the worst behaviours at low L. They too improves exponentially as L increases till they converges to $8dB$. New spreading sequences at lower L have approximately the same PMEPR values as Golay, Sidelnikov and m spreading sequences. However, as L increases, new spreading sequences become approximately $3dB$ worse than all the other 5 spreading sequences.

The minimum and maximum PMEPR values for various spreading sequences and their corresponding L at which these values occur are summarized in Table 4.4 below.

Table 4.5: PMEPR of the Spreading Sequences Sets

		Spreading Sequences Set					
		m	Sidelnikov	New	Golay	FZC	DFT
$N = 64$	$PMEPR_{min}$	5.32	4.79	7.14	2.97	2.59	6.45
	L	3	1	1	1	1	64
	$PMEPR_{max}$	9.47	9.06	14.35	10.09	9.00	18.06
	L	33	13	33	63	61	1
$N = 256$	$PMEPR_{min}$	5.45	5.43	7.44	3.01	2.55	7.38
	L	1	1	1	1	1	64
	$PMEPR_{max}$	10.31	11.97	12.59	11.07	8.70	24.08
	L	85	47	119	13	124	1

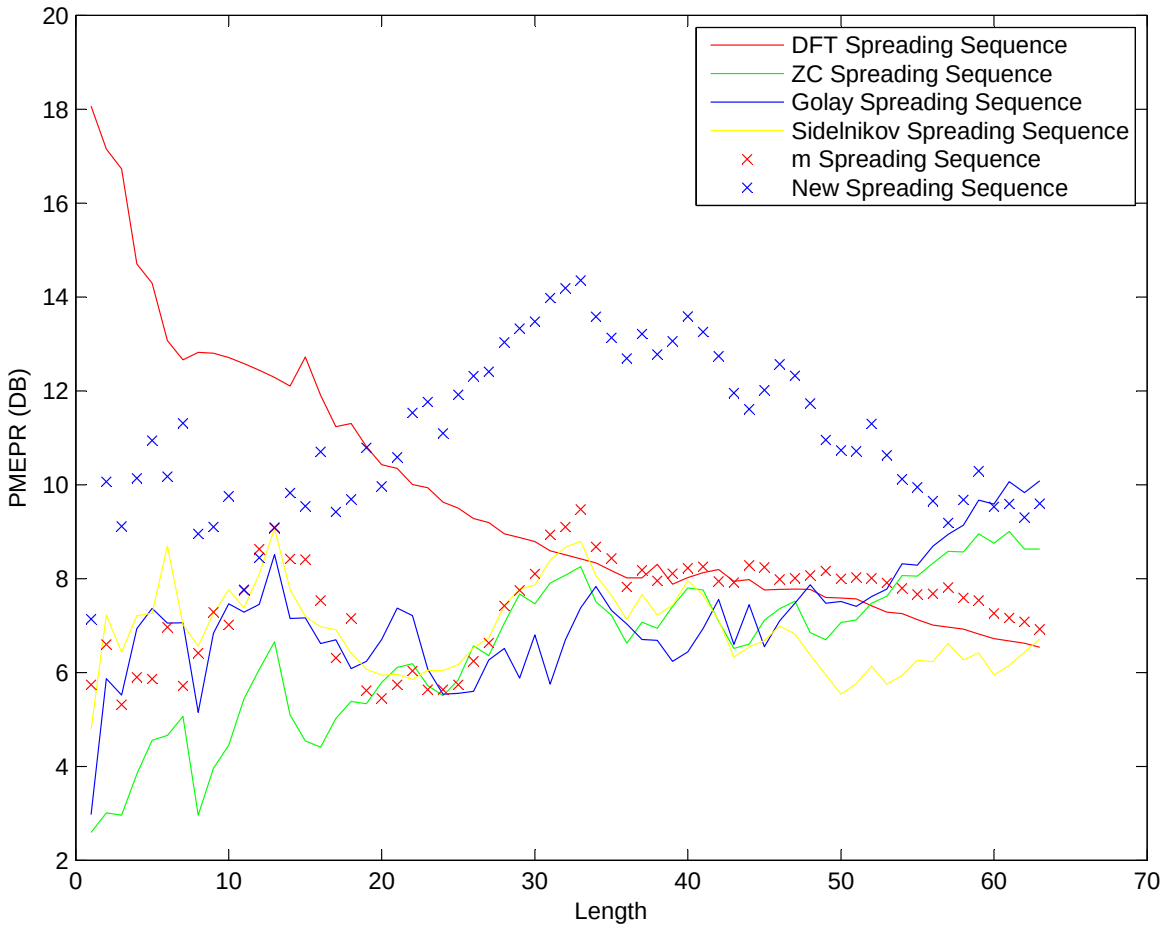

Figure 4.18: Spreading Sequence of Degree 6

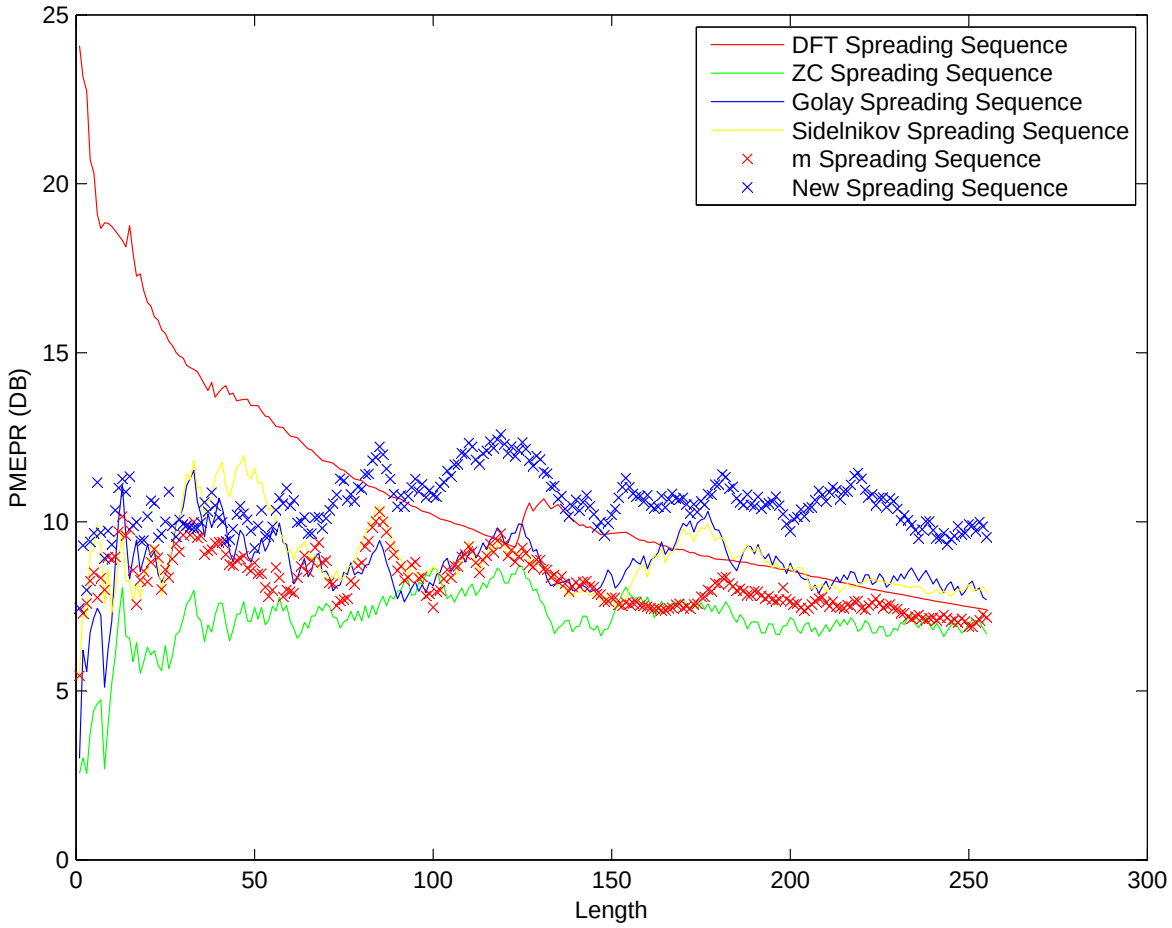

Figure 4.19: Spreading Sequence of Degree 8

Chapter 5

Merit Factor of Different Sequences

5.1 Introduction

The term of *merit factor* refers to the ratio of main lobe energy to the collective side lobe energy. It is defined by Golay [18] in 1972 as follows:

$$F(a) := \frac{n^2}{2\sum_{u=1}^{n-1}(C_a(u))^2} \tag{5.1}$$

where $C_a(u)$ is the aperiodic autocorrelation of a binary sequence $\underline{a}$ defined in section 2.1, and H in this case is 2. Although merit factor was originally intended for binary sequences. It was later extended to polyphase sequences [1].

This measurement has very practical and wide implications in many areas. For example, in communication systems, the side lobe energy can be seen as the energy of the interference signal. In stream ciphers, side lobe energy represents the correlation of the cipher with its own shifted version. In either case, it is desired that the collective sum of side lobe energy to be as small as possible. Sequences should be constructed such that the merit factor are maximized. Much effort has gone into researching what is the maximum merit factor when the length of a binary sequence approaches infinity. This is denoted by

$$\limsup_{n\to\infty} F_n$$

.

Prior to Golay's formal definition of merit factor, Littlewood [36] had already studied the problem of the norms of polynomials with ± 1 coefficients on the unit circle of the

complex plane. The merit factor problem is equivalent to this question involving the Ł$_4$ norm [31]. Littlewood in 1966, Høholdt and Jensen in 1988 had proposed conjectures as follows:

Conjecture 1 *(Littlewood, 1966 [35])* $\limsup_{n\to\infty} F_n = \infty$.

Conjecture 2 *(Høholdt and Jensen, 1988 [27])* $\limsup_{n\to\infty} F_n = 6$. *Sequences having this asymptotic merit factor values are rotated Legendre sequences.*

Moreover, the asymptotic behavior of the merit factor was found by Newman and Byrns [40] in 1990. It states

Proposition 1 *The mean value of* $1/F$*, taken over all sequences of length* n*, is* $\frac{n-1}{n}$.

This implies that the asymptotic mean merit factor of a randomly generated sequence is approximately 1. As we have discussed earlier, sequences with low collective autocorrelation functions or equivalently high merit factor property is important to many areas and applications. Consequently, we would want to construct sequences that have an asymptotic merit factor value that far exceeds 1. In 2005, Borwein *et al.* [4] proposed the idea of by cyclically shifting and appending a portion of the sequence, the value of merit factor can be improved. This technique was later applied to m sequences [32] and Legendre sequences [4]. The asymptotic merit factor values of m sequences and Legendre sequences thus were improved from 3 to 3.34 and from 6 to 6.34 respectively. In fact, rotated Legendre sequences [4] currently have the best asymptotic binary merit factor of all known sequences at $\limsup_{n\to\infty} F_n = 6.34$.

Thus, the current state of merit factor as the length of the sequence approach infinity is

$$6.34 \leq \limsup_{n\to\infty} F_n \leq \infty.$$

5.2 Relationship between PMEPR and Merit Factor

In this section, we will derive an upper bound between PMEPR and merit factor. In the previous chapter, we have defined the PMEPR in 4.2 as:

$$\begin{aligned} PMEPR &= \frac{n + \sum_{u \neq 0} C_a(u) \xi^{-H(u)\Delta f t}}{n} \\ &\leq 1 + \frac{\sum_{u \neq 0} |C_a(u)|}{n} \\ &= 1 + \sqrt{\frac{(\sum_{u \neq 0} |C_a(u)|)^2}{n^2}}. \end{aligned}$$

By applying the Cauchy-Schwarz inequality, we obtain the following:

$$\begin{aligned} &\leq 1 + \sqrt{\frac{\sum_{u \neq 0} |C_a(u)|^2 n}{n^2}} \\ &= 1 + 2\sqrt{\frac{n}{2 \times F_n}} \end{aligned} \tag{5.2}$$

where n is the length of the sequence, and F_n is the merit factor of the sequence. Although this is clearly not a very good bound, because as we discussed in chapter 4 that the asymptotic PMEPR behaviour of a randomly generated codeword of length n is of the order $\log n$ [41, 55, 49]. Nevertheless, it gives an approximation on the relationship between PMEPR and merit factor. We can summarize the above result into the following theorem.

Theorem 1 $PMEPR \leq 1 + 2\sqrt{\frac{n}{2 \times F_n}}$.

5.3 Simulation Results

From [4], we know the merit factor of a sequence can be changed by

1. Append a portion of the sequence.
2. Cyclical rotation of the sequence.

In this section, we will study the merit factor of modified sequences when these 2 methods are applied. We will apply one method at a time and observe its effect.

1. The length of sequences will be varied from 50% of its original length to 150% of its original length. The shortening of the sequence is achieved by removing the last k bits. The lengthening of the sequence is achieved by appending the k initial bits to the back. For example, let sequence $\underline{a} = 1001011100$, if the sequence is shortened by half of the length, then the modified sequence $\underline{a}' = 10010$. If the sequence is lengthened by half of the length, then the modified sequence $\underline{a}'' = 100101110010010$.

2. Cyclically left shift k bits of the sequence. For example, let sequence $\underline{a} = 1001011100$, if the sequence is shifted by 2 bits, then the rotated sequence $\underline{a}' = 0101110010$.

We will examine a total of 6 classes of sequences. They are m sequences, Sidelnikov sequences, new sequences, Golay sequences, FZC sequences and Legendre sequences. They are of degree 10 and degree 12. These 6 sequences are identical to the sequences that we have used for studying PMEPR properties.

5.3.1 Merit Factor of Removed/Appended Sequences

In this section, we will examine the merit factor of each sequence by varying its length. The merit factor of the original sequence is first summarized and listed in Table 5.1 below.

Table 5.1: Merit Factor of the Sequences

		Sequences					
		m	Sidelnikov	Golay	Legendre	FZC	New
Deg10	F_n	3.24	3.03	3.00	1.50	50.32	1.06
Deg12	F_n	3.03	3.01	3.00	1.50	100.56	1.02

We can observe that the behaviour of m sequences and Sidelnikov sequences are very similar. The plot for both sequences is triangular shaped. They both have a minimum and maximum merit factor value of approximately 1.4 and 3.35 respectively. The minimum merit factor value occurs when only 50% of the sequences is retained for both sequences. The maximum merit factor value occurs when both sequences are lengthened by approximately 10%. This is shown in Figures 5.1 - 5.4.

The merit factor of new sequences is approximately 1 when the sequence is retained or some bits are removed. Its value start to decrease as more bits are appended to the

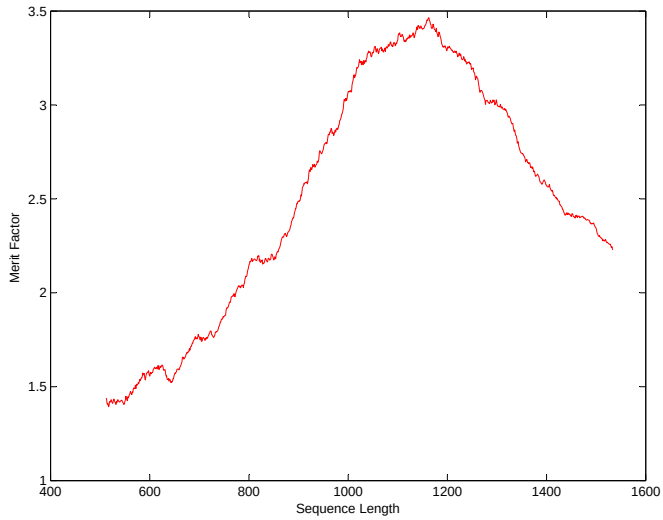

Figure 5.1: Merit Factor of Removed/Appended m Sequence of Length 1023

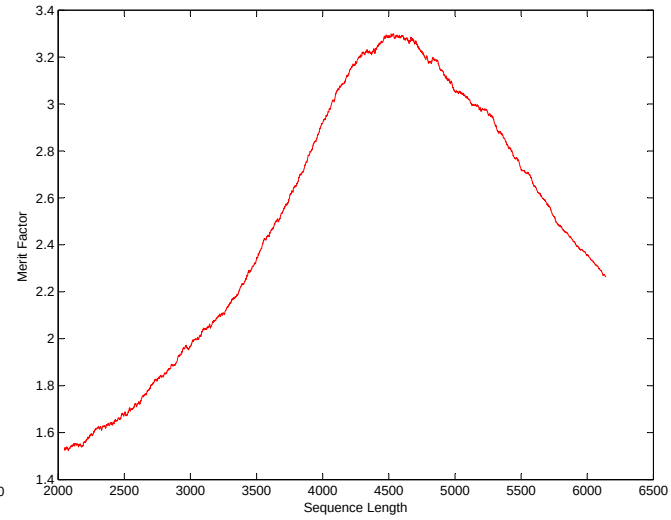

Figure 5.2: Merit Factor of Removed/Appended m Sequence of Length 4095

sequence. This is true for new sequences of both degree 10 and degree 12. These are shown in Figures 5.5 and 5.6.

The shape of merit factor for FZC sequences looks like an impulse function. The maximum occurs when the entire sequence is retained. The maximum values are approximately 50 and 100 for degree 10 and degree 12 respectively. However, as soon as some bits of the sequences are removed or appended, the merit factor drops exponentially until it converges to approximately 1. These are shown in Figures 5.7 and 5.8.

The merit factor of Golay sequences has two very noticeable peaks and bottoms for both degree 10 and degree 12 as shown Figures 5.9 and 5.10. The first peak occurs when only half of the sequence is retained. The second peak occurs when the entire sequence is retained. The first bottom occurs when the length of Golay sequences is at approximately 75%. The second bottom occurs at 150% of the original sequence length. These results are shown in Figures 5.9 and 5.10.

The merit factor of Legendre sequences has two peaks and one bottom. The value of the first peak is around 3.35, this occurs when approximately 60% of the sequence is retained. The second peak occurs when approximately 32% of the sequence is appended. This value of the second peak is a little higher than the first one at about 3.45. The bottom occurs when the entire sequence is retained. It has a minimum value of 1.5. These are shown in

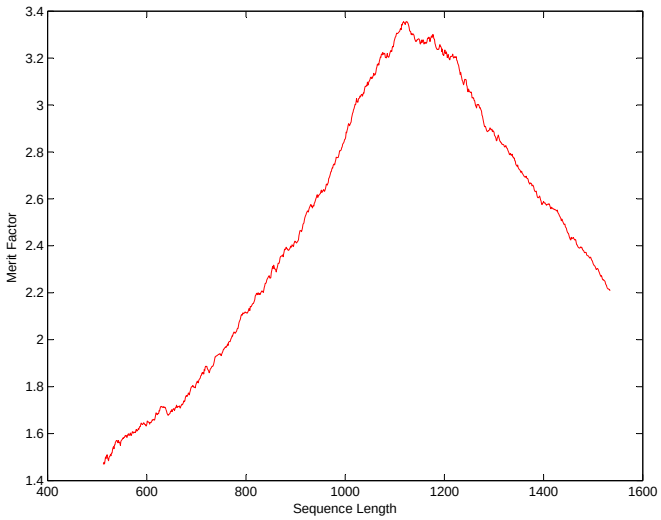

Figure 5.3: Merit Factor of Removed/Appended Sidelnikov Sequence of Length 1023

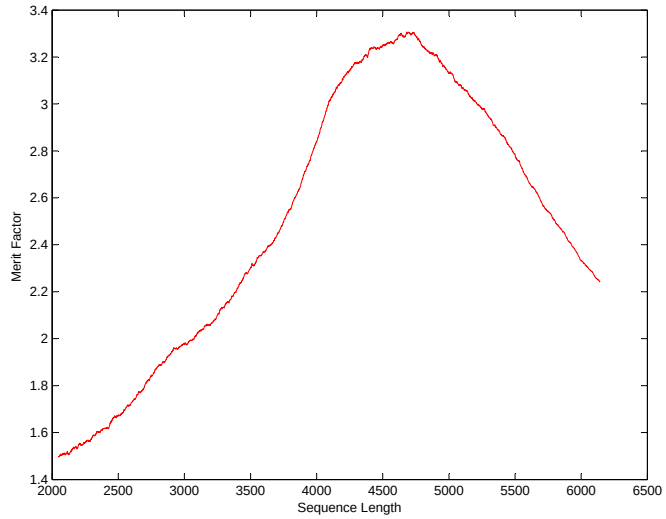

Figure 5.4: Merit Factor of Removed/Appended Sidelnikov Sequence of Length 4095

Figures 5.11 and 5.12.

In general, polyphase FZC sequences have the optimal merit factor. They also exhibit the largest merit factor variations. The maximum value occurs when the entire sequence is retained, as soon as some bits are removed or appended, its merit factor value drops exponentially. The variations of merit factors for Legendre sequences and Golay sequences are also quite significant. With sequences of different length, the merit factor value is doubled. The variations of merit factors in m, Sidelnikov and new sequences are less obvious. For m sequences and Sidelnikov sequences, the merit factor initially increases and then decreases. For new sequences, merit factor is initially flat, it starts to decrease when bits are appended to the sequence. The maximum and minimum merit factor values of different removed/appended sequences are summarized in Table 5.2.

From the simulated data, we can make the following conjecture. For removed/appended sequences, the minimum and maximum merit factors of m sequences, Sidelnikov sequences, Golay sequences and Legendre sequences are almost identical.

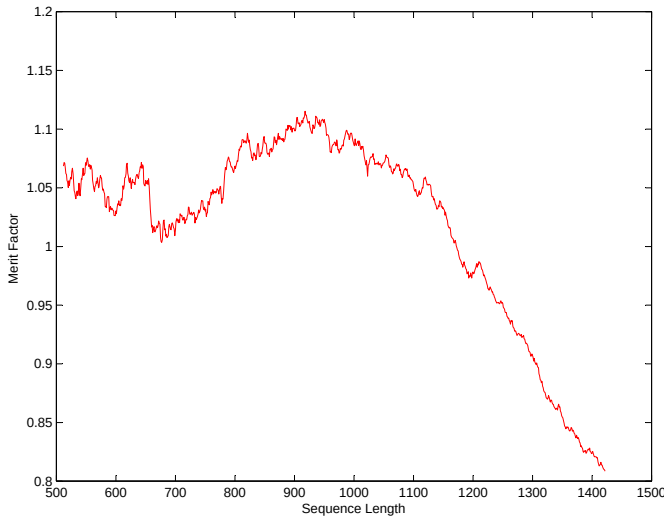

Figure 5.5: Merit Factor of Removed/Appended New Sequence of Length 1023

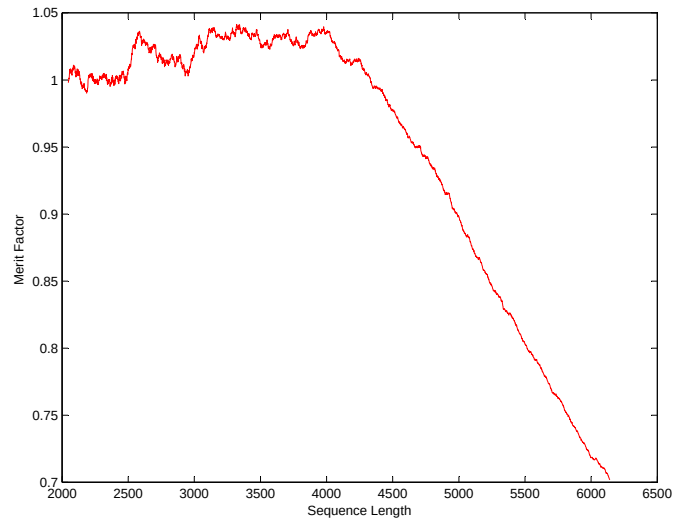

Figure 5.6: Merit Factor of Removed/Appended New Sequence of Length 4095

5.3.2 Merit Factor of Shifted Sequences

The shape of merit factor plots for m sequences of degree 10 and degree 12 is somewhat different. However, their maximum and minimum merit factor values are quite similar. The merit factor of of degree 10 ranges from approximately 2.8 to 3.4, while the merit factor of degree 12 ranges from approximately 2.9 to 3.2. These can be seen in Figures 5.13 and 5.14.

The merit factor of Sidelnikov sequences are symmetrical along the mid point. The maximum merit factor value occurs at mid point for degree 12 case, but this is not true for degree 10. The maximum merit factor value for the degree 10 and degree 12 Sidelnikov sequences are 3.22 and 3.02 respectively. Their minimum merit factor values are approximately identical at 2.80. These can be seen in Figures 5.15 and 5.16.

The plot for merit factor of new sequences are somewhat different between degree 10 and degree 12. However, they have one common, the merit factor values remain almost unchanged with shifted sequences. The largest difference is about 0.10 for degree 10 case and 0.05 for degree 12. These are illustrated in Figures 5.17 and 5.18.

The shape of merit factor plots for Golay sequences between degree 10 and degree 12 is very similar. Their minimum and maximum values are also almost identical. They range

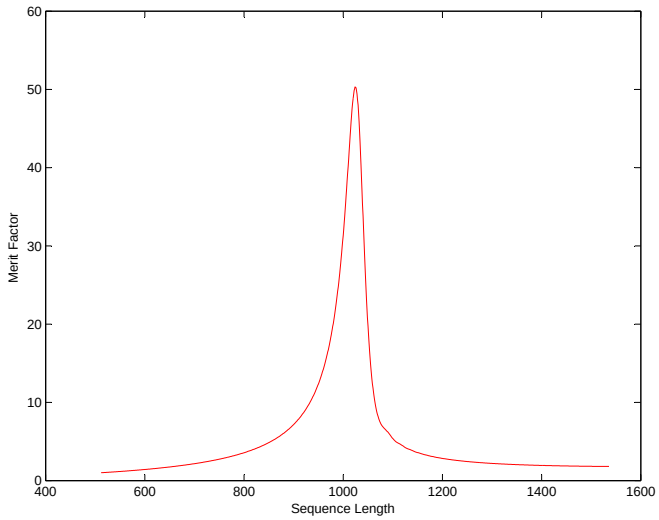

Figure 5.7: Merit Factor of Removed/Appended FZC Sequence of Length 1024

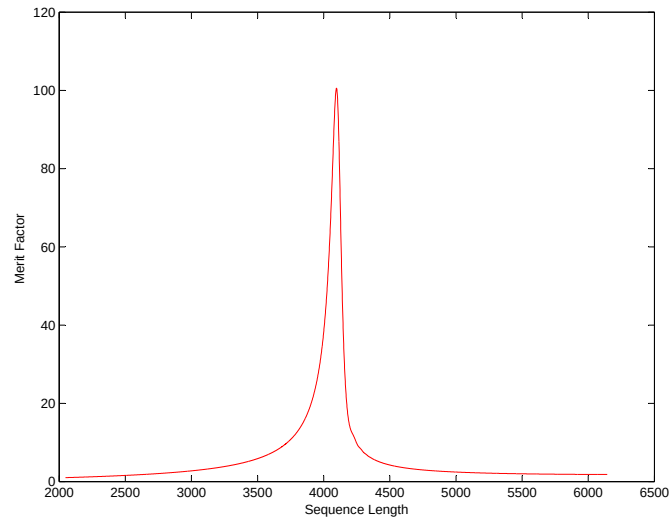

Figure 5.8: Merit Factor of Removed/Appended FZC Sequence of Length 4096

from 1.5 to approximately 3.1 for both cases. These can be seen in Figures 5.19 and 5.20.

There's virtually no variations in the merit factor regardless how many bits are shifted for FZC sequences. Their merit factor values are approximately 50 and 100 for degree 10 and degree 12 respectively. This can be seen in Figures 5.21 and 5.22.

The merit factor of Legendre sequences are also symmetrical along the mid point. The mid point is also where the minimum value occurs. The variations in the merit factor value throughout different shifts are quite substantial. It ranges from the minimum point of 1.5 to maximum point of 6. These are shown in Figures 5.23 and 5.24.

In general, polyphase FZC has the optimal merit factor value. It also has the smallest merit factor variations. The variations for Legendre sequences and Golay sequences are quite significant. The merit factor is quadrupled for Legendre sequences and doubled for Golay sequences for some rotations of sequences. The variations in m sequences and Sidelnikov sequences are approximately 0.4. For new sequences and FZC sequences, merit factor virtually remained unchanged throughout all rotations. The maximum and minimum merit factor values of different rotated sequences are generalized in Table 5.3 below.

From the simulated data, we can make the following conjecture. For the rotated se-

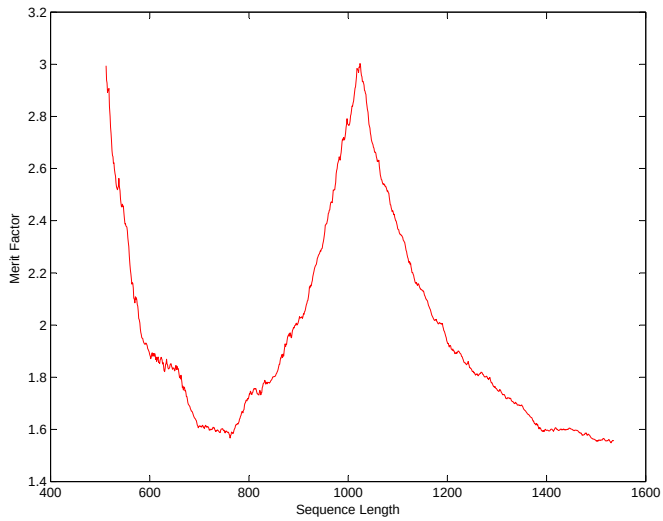

Figure 5.9: Merit Factor of Removed/Appended Golay Sequence of Length 1024

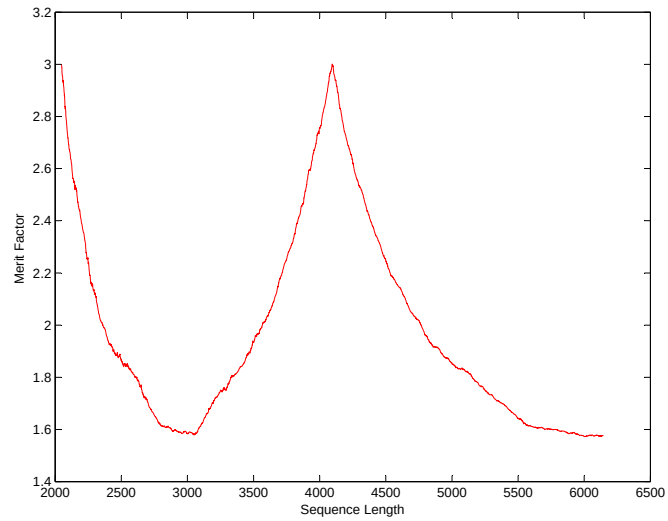

Figure 5.10: Merit Factor of Removed/Appended Golay Sequence of Length 4096

quences, the minimum and maximum merit factors of m sequences and Sidelnikov sequences are almost identical. Golay sequences and Legendre sequences have comparable minimum merit factors, but the maximum merit factor of Legendre sequences is twice as much as Golay sequences. The merit factor of FZC sequences remains almost unchanged throughout different rotations. Moreover, its merit factor doubles when the length of FZC sequences is quadrupled.

5.4 PMEPR and Merit Factor

From the expression derived in (5.2). We can make the following observations. The PMEPR of a sequence is determined by 2 contributing factors. The merit factor of the sequence and aperiodic autocorrelation distributions.

1. If two different sequences have very similar merit factor values, then their PMEPR performance is determined by their aperiodic autocorrelation distributions. In particular, sequences whose out-of-phase aperiodic autocorrelation distributions have very few high peaks and rest are all zeros or very close to zeros will have a lower PMEPR than sequences whose aperiodic autocorrelation distributions are more evenly

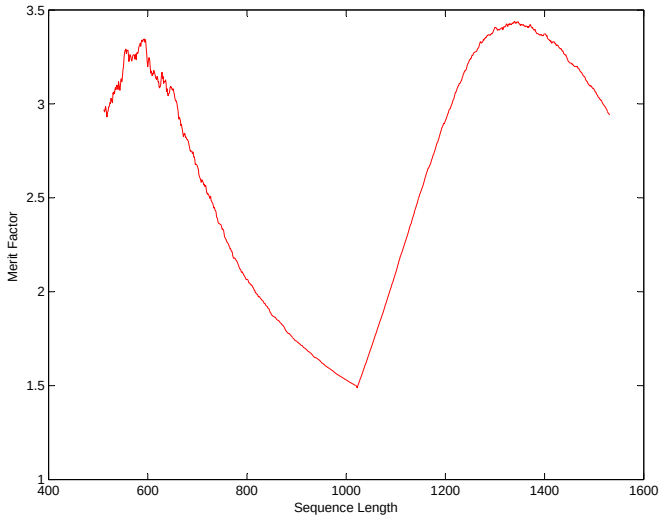

Figure 5.11: Merit Factor of Removed/Appended Legendre Sequence of Length 1023

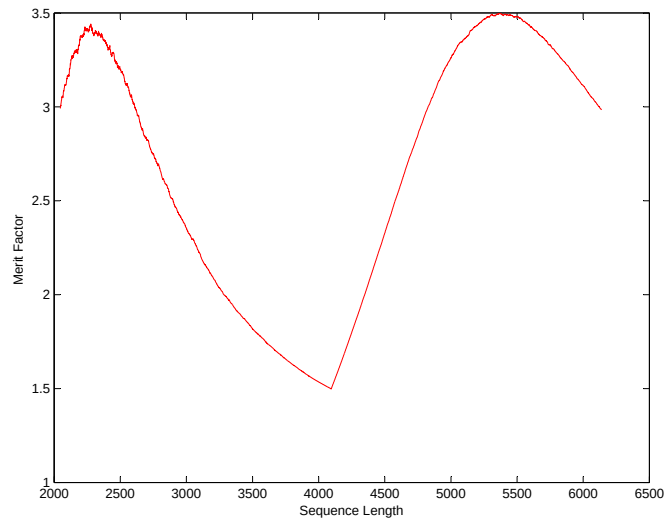

Figure 5.12: Merit Factor of Removed/Appended Legendre Sequence of Length 4093

distributed. An example of this would be m sequences and Golay sequences. From Table 5.1, we have observed that m sequences and Golay sequences have almost identical merit factors. However, their PMEPR comparison is vastly different. From Table 4.3.3, we can see that PMEPR of m sequence is approximately $2.8dB$ and $3.9dB$ higher than Golay sequences of degree 10 and degree 12. The reason is that Golay sequences have a few very large out-of-phase aperiodic autocorrelation peaks. They also contain many 0 out-of-phase aperiodic autocorrelations. The correlation properties of Golay sequences will be discussed in more details in the next chapter. Therefore, Golay sequences have lower PMEPR than m sequences.

2. Better merit factor values do not necessarily translate into lower PMEPR values. This can be seen by the comparison between Legendre sequences and Golay sequences. From Table 5.3, we can see that rotated Legendre sequences have a merit factor of 6. This merit factor value is approximately 2 times better than Golay sequences. However, from Table 4.3.3, we have obtained that PMEPR of Legendre sequences is greater than Golay sequence by approximately $5.16dB$ in degree 10 case, and $4.71dB$ in the degree 12 case. Note that the cyclical shift of the sequence does not affect the PMEPR behaviour.

Table 5.2: Merit Factor of the Removed/Appended Sequences

		Sequences					
		m	Sidelnikov	Golay	Legendre	FZC	New
Deg10	$F_{n_{min}}$	1.39	1.47	1.55	1.49	1.00	0.81
	Length	517	512	1503	1022	512	1422
	$F_{n_{max}}$	3.38	3.36	3.00	3.44	50.32	1.11
	Length	1104	1118	1024	1347	1024	920
Deg12	$F_{n_{min}}$	1.52	1.50	1.57	1.50	1.00	0.70
	Length	2048	2048	5964	4093	2048	6141
	$F_{n_{max}}$	3.30	3.31	3.00	3.49	100.56	1.04
	Length	4522	4680	4096	5429	4096	3320

The aperiodic autocorrelation distributions contribute more to the outcomes of PMEPR. This is shown in the drastic comparison between Golay sequences and Legendre sequences. Therefore, when search for sequences with optimal PMEPR properties, sequences with few large aperiodic autocorrelation peaks and many zeros are preferred over sequences with evenly distributed aperiodic autocorrelations.

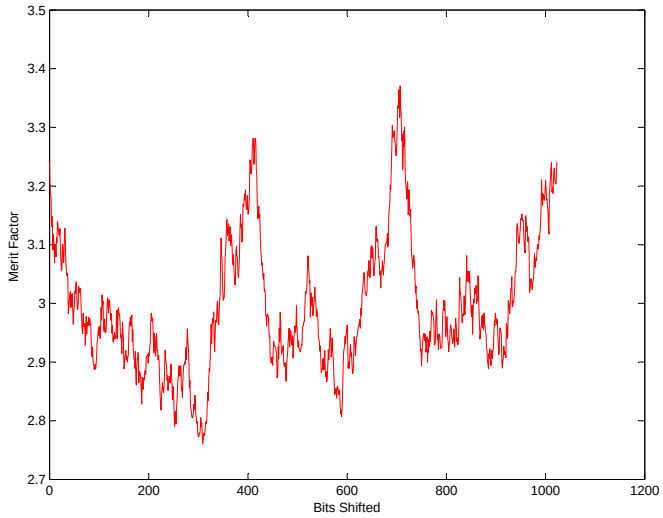

Figure 5.13: Merit Factor of Shifted m Sequence of Length 1023

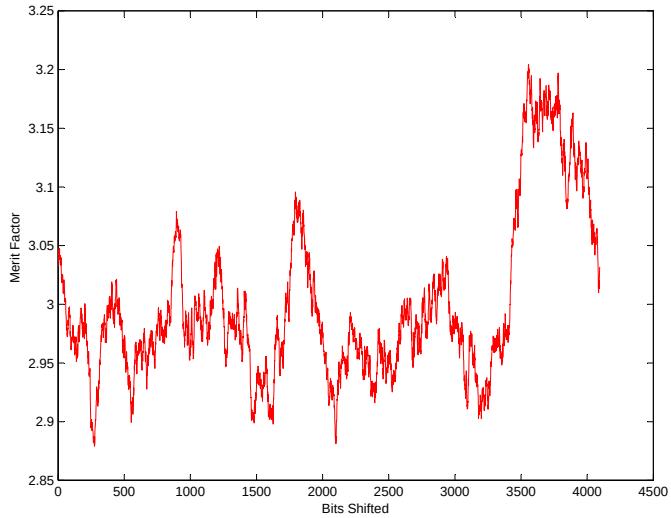

Figure 5.14: Merit Factor of Shifted m Sequence of Length 4095

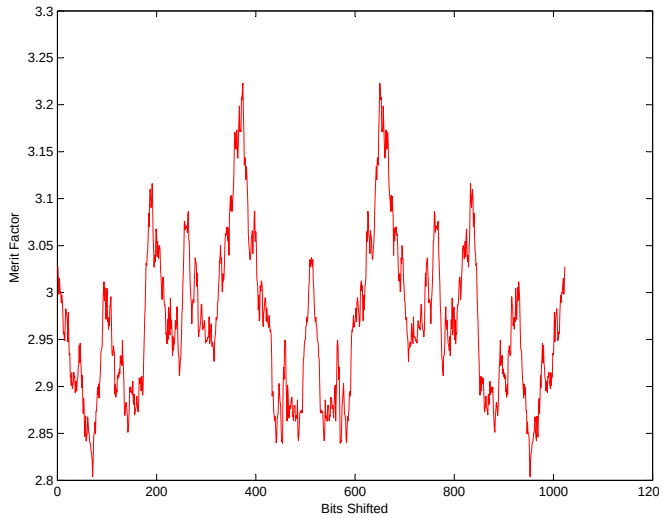

Figure 5.15: Merit Factor of Shifted Sidelnikov Sequence of Length 1023

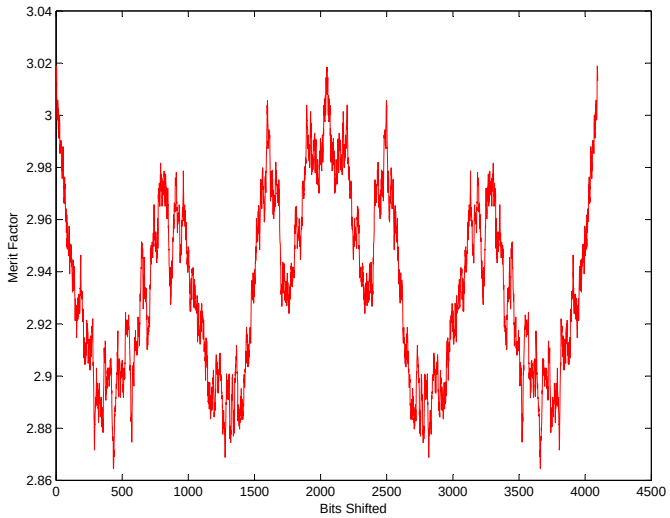

Figure 5.16: Merit Factor of Shifted Sidelnikov Sequence of Length 4095

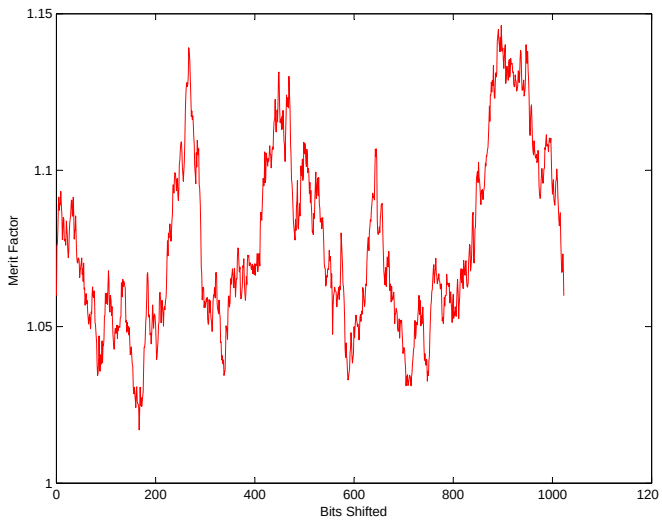

Figure 5.17: Merit Factor of Shifted New Sequence of Length 1023

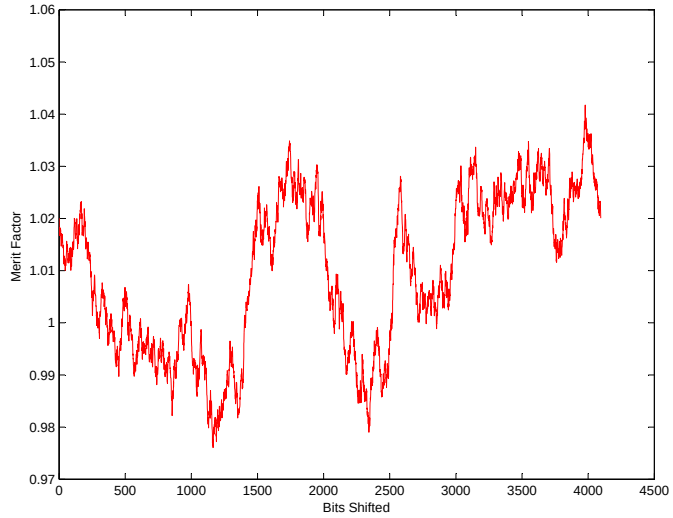

Figure 5.18: Merit Factor of Shifted New Sequence of Length 4095

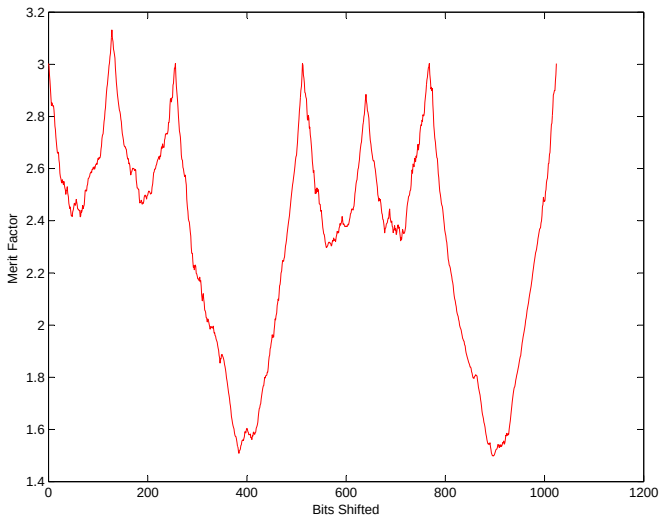

Figure 5.19: Merit Factor of Shifted Golay Sequence of Length 1024

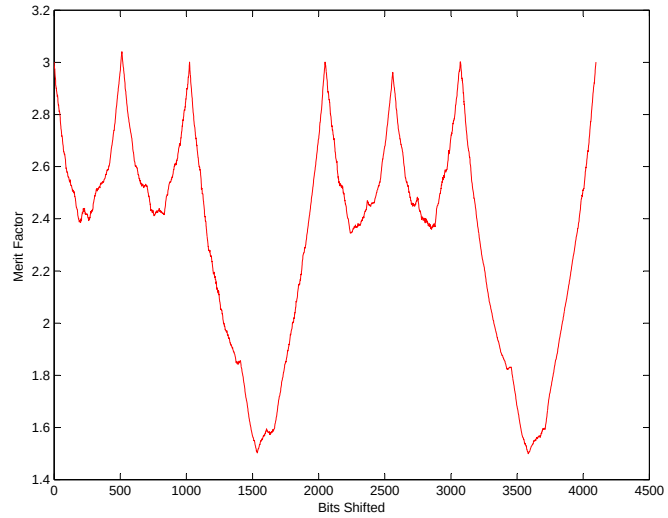

Figure 5.20: Merit Factor of Shifted Golay Sequence of Length 4096

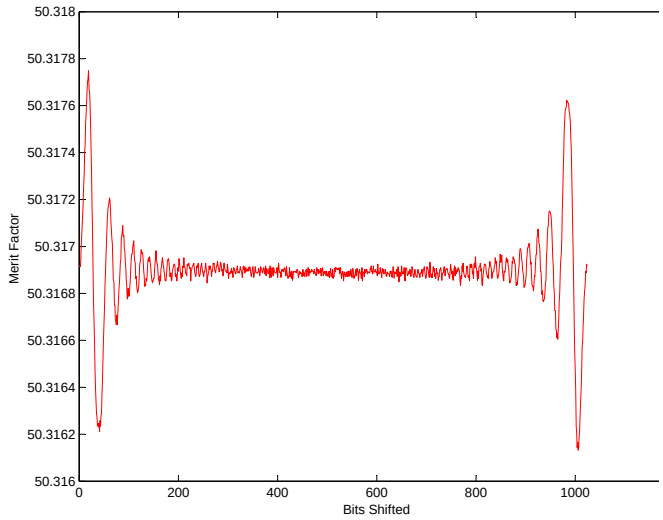

Figure 5.21: Merit Factor of Shifted FZC Sequence of Length 1024

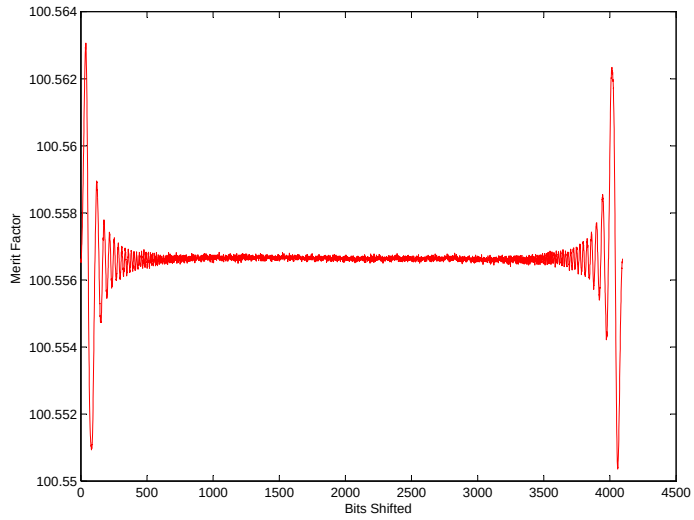

Figure 5.22: Merit Factor of Shifted FZC Sequence of Length 4096

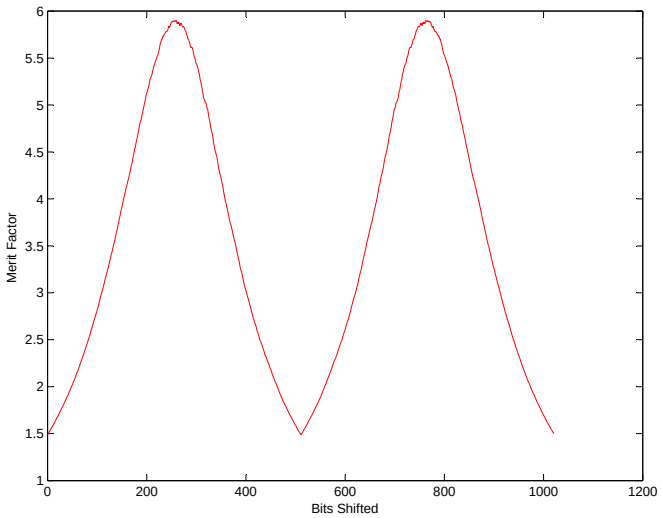

Figure 5.23: Merit Factor of Shifted Legendre Sequence of Length 1023

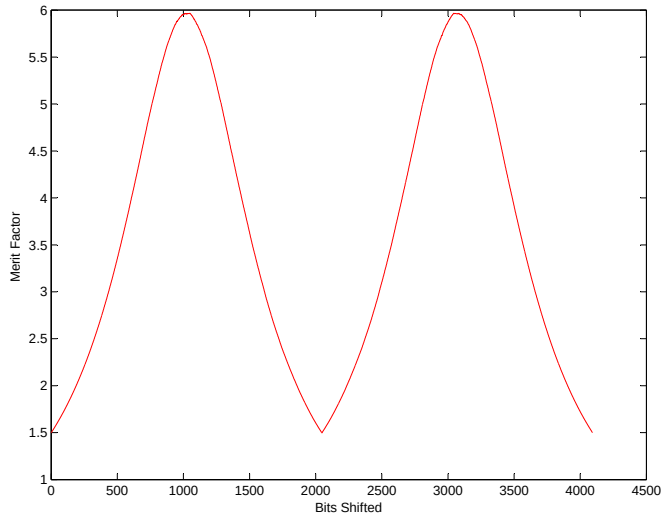

Figure 5.24: Merit Factor of Shifted Legendre Sequence of Length 4093

Table 5.3: Merit Factor of the Rotated Sequences

		Sequences					
		m	Sidelnikov	Golay	Legendre	FZC	New
Deg10	$F_{n_{min}}$	2.76	2.80	1.50	1.49	50.32	1.02
	Bits Shifted	309	953	897	511	1006	167
	$F_{n_{max}}$	3.37	3.22	3.13	5.90	50.32	1.15
	Bits Shifted	707	374	128	259	19	897
Deg12	$F_{n_{min}}$	2.88	2.86	1.50	1.50	100.55	0.98
	Bits Shifted	275	435	3585	2047	4059	1164
	$F_{n_{max}}$	3.20	3.01	3.04	5.97	100.56	1.04
	Bits Shifted	3557	4	512	1050	38	3978

Chapter 6

Large Zero Autocorrelation Zone (ZACZ) of Golay Sequences

6.1 Introduction

In modern communication systems, sequences with good correlation properties are desired for receiver synchronization and detection purposes. In 1961, Golay proposed the idea of aperiodic complementary sequence pairs [17], of which the sum of out-of-phase aperiodic autocorrelation equals to zero. Later on, Davis and Jedwab formulated a method for constructing such pairs by using generalized boolean functions [10], which are called GDJ Golay pairs. Because of this correlation property, Golay complementary sequences have been propsed to construct Hadamard matrix for DS CDMA system [48], and to control PEP in OFDM systems [53, 57, 58, 59].

The utilization of Golay sequences in the two above scenarios are based on the property that the sum of out-of-phase autocorrelation of the pair equals to zero. However, synchronization and detection of the signal is equivalent to compute its own autocorrelation. In this case, the autocorrelation properties of the single sequence is of our interest. This is also the case with conventional CDMA and quasi-synchronous code-division multiple-access (QS-CDMA) systems.

QS-CDMA differs from conventional CDMA systems [20] in that it allows a small time delay in the arrival signals of different users. In this case, sequences with low or zero correlations centered at the origin are desired to eliminate or reduce the multiple access and multi-path interference at the receiver end during detection. Such sequences are called

low correlation zone (LCZ) and zero correlation zone (FZCZ) sequences respectively [37]. As a result, the construction of new LCZ or FZCZ sequences for QS-CDMA system has received much researchers's attention [11, 14, 23, 24, 28, 46, 47, 51, 52, 64].

Our motivation is to examine the correlation property of GDJ Golay sequences when it is being utilized for signal detection and synchronization purposes in applications such as CDMA and conventional linear time invariant (LTI) system. More specifically, if single Golay sequence inherits some fixed or attractive autocorrelation property which can be exploited during detection and thus improves the performance of the system.

The initial construction for Golay complementary pair was found by Davis and Jedwab in [10], the length of each Golay sequence is a power of 2. Later on, Paterson generalized this result from $\mathbb{Z}_{2^h}$ in 3.1 to $\mathbb{Z}_H$ [42], where H is a positive even integer. Thus the generalized Golay complementary pair over alphabets $\mathbb{Z}_H$ of sequences $\underline{a} = (a_m \cdots a_1 a_0)$ and $\underline{b} = (b_m \cdots b_1 b_0)$ can be written as

$$a_i = \frac{H}{2} \sum_{k=1}^{m-1} i_{\pi(k)} i_{\pi(k+1)} + \sum_{k=1}^{m} c_k i_k + c_0 \tag{6.1}$$

where $c_i \in \mathbb{Z}_H$, $i = 0, 1, \cdots, m$.

$$b_i = a_i + \frac{H}{2} i_{\pi(1)} + c' \tag{6.2}$$

where $c' \in Z_H$.

In this chapter, we will present a class of general $\mathbb{Z}_H$ Golay sequences with a ZACZ length up to a quarter of the period of the Golay sequence, H is a positive even integer. This class contains a total of 3 cases. We will give proof to the binary Golay sequences of one of the cases. The complete proof will be provided in a separate paper in [62]. Then we will illustrate all 3 cases of ZACZ pattern with concrete examples.

6.2 Main Results

In this section, we first consider the maximum magnitude of the autocorrelation of binary Golay sequences with identity permutation of length 2^m defined by 3.1. This is denoted by

$$R_{\max} := \max_{c \in \{0,1\}^{m+1}} \max_{1 \le |\tau| \le 2^m - 1} |R_a(u)|.$$

where $c = (c_0, c_1, \cdots, c_m) \in \{0,1\}^{m+1}$. We have exhaustively searched for all combinations of constants. Some examples are given in Table 6.1. From the experimental result seen in the table, we can observe that Golay sequences do not possess good periodic autocorrelation properties. Its maximum periodic autocorrelation value is well above $\sqrt{N}$, where N is the length of the sequence.

Table 6.1: Maximum autocorrelation of the Golay sequences defined by identity permutation

m	$R_{\max}$	$c = (c_0, c_1, \cdots, c_m) \in \{0,1\}^{m+1}$
4	4	$(0,0,0,0,0)$
5	12	$(0,0,0,0,0,0)$
6	20	$(0,0,0,1,0,0,0)$
7	36	$(0,0,0,0,1,0,1,0)$
8	52	$(0,0,0,0,0,1,1,1,1)$
9	100	$(0,0,0,0,0,1,0,1,1,0)$
10	148	$(0,0,0,0,0,0,1,1,1,1,1)$
11	260	$(0,0,0,0,0,0,1,0,1,0,1,0)$
12	436	$(0,0,0,0,0,1,0,0,0,0,1,1,1)$
13	716	$(0,0,0,0,0,0,1,1,1,1,1,0,1,0)$
14	1236	$(0,0,0,0,0,1,0,0,0,0,0,0,1,1,1)$
15	1924	$(0,0,0,0,0,0,1,1,1,0,1,1,1,0,1,0)$

However, we have found with selected permeations π and affine transformations $\sum_{k=1}^{m} c_k i_k$, there exists 3 cases of Golay sequences with large ZACZ of length up to 2^{m-2}.

We will present our results by first listing the 3 sets of conditions imposed on the permutations and affine transformation that would match each case of ZACZ patterns.

(A) (1) $\pi(1) = 1$, $\pi(2) = 2$ and $2c_1 = 0$.

(2) $\pi(2) = 2$, $\pi(3) = 1$, $\pi(4) = 3$, $2c_1 = 0$ and $c_1 = c_2$.

(3) $\pi(1) = 2$, $\pi(2) = 1$, $\pi(3) = 3$, $2c_1 = 0$ and $c_1 = 2c_2 + \frac{H}{2}$.

(B) $\pi(1) = 2$, $\pi(2) = 1$, $\pi(3) = 3$, $2c_1 = 0$ and $c_1 = 2c_2$.

(C) (1) $\pi(1) = 1$, $\pi(2) = 3$, $\pi(3) = 2$ and $2c_1 = 0$.

(2) $\pi(1) = 1$, $\pi(2) = 3$, $\pi(m) = 2$ and $2c_1 = 0$.

(3) $\pi(1) = 2$, $\pi(2) = 4$, $\pi(3) = 1$, $\pi(4) = 3$, $2c_1 = 0$ and $c_1 = 2c_2$.

(4) $\pi(1) = 2$, $\pi(2) = 3$, $\pi(3) = 1$, $\pi(4) = 4$, $2c_1 = 0$ and $c_1 = 2c_2$.

Define a mapping $\pi'(k) = \pi(m+1-k)$, $k \in \{1, \cdots, m\}$. This is effectively the reverse of the original permutations. Replacing π by π', the 3 sets of conditions on permutations π and affine transformation $\sum_{k=1}^{m} c_k i_k$ above can be written as follows.

(A') (1) $\pi(m) = 1$, $\pi(m-1) = 2$ and $2c_1 = 0$.

(2) $\pi(m-1) = 2$, $\pi(m-2) = 1$, $\pi(m-3) = 3$, $2c_1 = 0$ and $c_1 = c_2$.

(3) $\pi(m) = 2$, $\pi(m-1) = 1$, $\pi(m-2) = 3$, $2c_1 = 0$ and $c_1 = 2c_2 + \frac{H}{2}$.

(B') $\pi(m) = 2$, $\pi(m-1) = 1$, $\pi(m-2) = 3$, $2c_1 = 0$ and $c_1 = 2c_2$.

(C') (1) $\pi(m) = 1$, $\pi(m-1) = 3$, $\pi(m-1) = 2$ and $2c_1 = 0$.

(2) $\pi(m) = 1$, $\pi(m-1) = 3$, $\pi(1) = 2$ and $2c_1 = 0$.

(3) $\pi(m) = 2$, $\pi(m-1) = 4$, $\pi(m-2) = 1$, $\pi(m-3) = 3$, $2c_1 = 0$ and $c_1 = 2c_2$.

(4) $\pi(m) = 2$, $\pi(m-1) = 3$, $\pi(m-2) = 1$, $\pi(m-3) = 4$, $2c_1 = 0$ and $c_1 = 2c_2$.

In the rest of this chapter, we will use the following notations. For an integer u, $1 \le u \le 2^m - 1$, and two integers i and i', $0 \le i, i', j, j' < 2^m$, we set $j = (i+u) \mod 2^m$ and $j' = (i'+u) \mod 2^m$. Then let $(i_1, \cdots, i_m)$, $(i'_1, \cdots, i'_m)$, $(j_1, \cdots, j_m)$ and $(j'_1, \cdots, j'_m)$ be the binary representations of integers i, i', j and j'.

Theorem 2 *If the Golay sequence a defined in 6.1, satisfies one of the condition listed in (A) or (A'), Then the sequence a has the following property:*

$$R_a(u) = 0, \quad u \in (0, 2^{m-2}] \cup [3 \cdot 2^{m-2}, 2^m)$$

In other words, in one period $[0, 2^m)$, it has two zero autocorrelation zones of length 2^{m-2}, given by $(0, 2^{m-2}]$ and $[3 \cdot 2^{m-2}, 2^m)$, shown in Figure 6.1.

Theorem 3 *If the Golay sequence a defined in 6.1, satisfies one of the condition listed in (B) or (B'), Then the sequence a has the following property:*

$$R_a(u) = 0, \quad u \in [2^{m-2}, 3 \cdot 2^{m-2}]$$

In other words, in one period $[0, 2^m)$, it has a zero autocorrelation zone of length $2^{m-1} + 1$, given by $[2^{m-2}, 3 \cdot 2^{m-2}]$, shown in Figure 6.2.

Figure 6.1: The Zero Autocorrelation Zone of Golay Sequence a Defined by (3.1) and Condition (A) or (A')

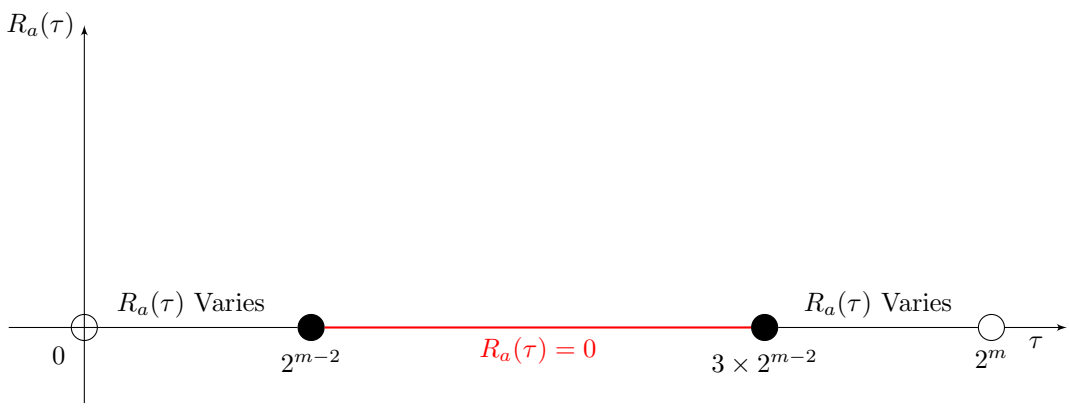

Figure 6.2: The Zero Autocorrelation Zone of Golay Sequence a Defined by (3.1) and Condition (B) or (B')

Theorem 4 *If the Golay sequence a defined in 6.1, satisfies one of the condition listed in (C) or (C'), Then the sequence a has the following property:*

$$R_a(u) = 0, \quad u \in (0, 2^{m-3}] \cup [3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}] \cup [7 \cdot 2^{m-3}, 2^m)$$

In other words, in one period $[0, 2^m)$, it has three zero autocorrelation zones of respective length 2^{m-3}, $2^{m-2}+1$, 2^{m-3}, given by $(0, 2^{m-3}]$, $[3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}]$ and $[7 \cdot 2^{m-3}, 2^m)$, shown in Figure 6.3.

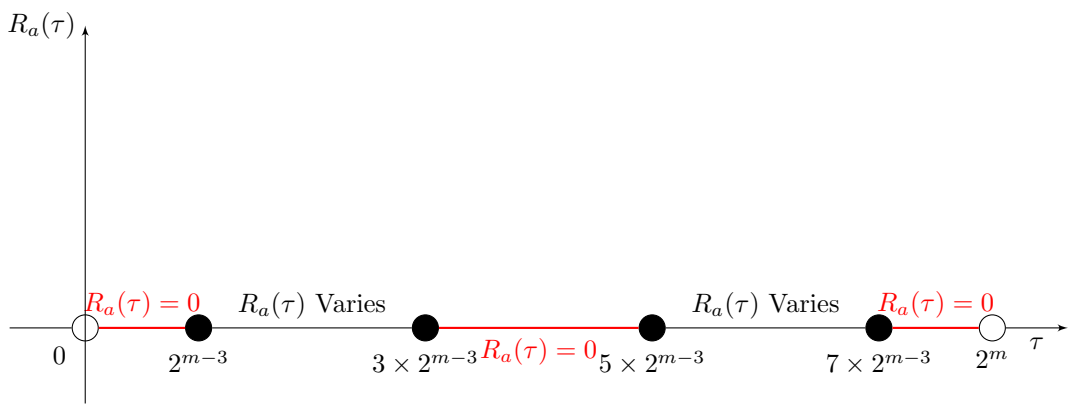

Figure 6.3: The Zero Autocorrelation Zone of Golay Sequence a Defined by (3.1) and Condition (C) or (C')

We have conclude all results obtained in this section into Table 6.2.

6.3 Proof for One Case of Golay Sequences with Large ZACZ

In the following, we will present the proof for the binary Golay sequences in Theorem 2 with a ZACZ of length 2^{m-2} [21]. For the complete proof of general Golay sequences over $\mathbb{Z}_H$, please refer to [62].

Let π be a permutation of $\{1, 2, \cdots, m\}$ with $\pi(1) = 1$ and $\pi(2) = 2$, and $h = 1$. Then the binary Golay sequences (a_i) given by (3.1) has $R_a(u) = 0$ for any $u \in U$, where

$$U = \{k : 1 \leq k \leq 2^{m-2}\} \cup \{k : 3 \cdot 2^{m-2} \leq k \leq 2^m - 1\}.$$

Table 6.2: Parameters of Golay Sequences with Consecutive Zero Autocorrelation Property

Permutation π	$(c_1, c_2) \in \mathbb{Z}_H \times \mathbb{Z}_H$	ZACZ Length
$\pi(1) = 1, \pi(2) = 2$	$2c_1 = 0$	2^{m-2}
$\pi(m) = 1, \pi(m-1) = 2$	$2c_1 = 0$	2^{m-2}
$\pi(2) = 2,\ \pi(3) = 1,\ \pi(4) = 3$	$2c_1 = 0$ & $c_1 - 2c_2 = 0$	2^{m-2}
$\pi(m-1) = 2,\ \pi(m-2) = 1,\ \pi(m-3) = 3$	$2c_1 = 0$ & $c_1 - 2c_2 = 0$	2^{m-2}
$\pi(1) = 2,\ \pi(2) = 1,\ \pi(3) = 3$	$2c_1 = 0$ & $c_1 - 2c_2 + \frac{H}{2} = 0$	2^{m-2}
$\pi(m) = 2,\ \pi(m-1) = 1,\ \pi(m-2) = 3$	$2c_1 = 0$ & $c_1 - 2c_2 + \frac{H}{2} = 0$	2^{m-2}
$\pi(1) = 2,\ \pi(2) = 1,\ \pi(3) = 3$	$2c_1 = 0$ & $c_1 - 2c_2 = 0$	2^{m-2}
$\pi(m) = 2,\ \pi(m-1) = 1,\ \pi(m-2) = 3$	$2c_1 = 0$ & $c_1 - 2c_2 = 0$	2^{m-2}
$\pi(1) = 1,\ \pi(2) = 3,\ \pi(3) = 2$	$2c_1 = 0$	2^{m-3}
$\pi(m) = 1,\ \pi(m-1) = 3,\ \pi(m-2) = 2$	$2c_1 = 0$	2^{m-3}
$\pi(1) = 1,\ \pi(2) = 3,\ \pi(m) = 2$	$2c_1 = 0$	2^{m-3}
$\pi(m) = 1,\ \pi(m-1) = 3,\ \pi(1) = 2$	$2c_1 = 0$	2^{m-3}
$\pi(1) = 2,\ \pi(2) = 4,\ \pi(3) = 1,\ \pi(4) = 3$	$2c_1 = 0$ & $c_1 - 2c_2 = 0$	2^{m-3}
$\pi(m) = 2,\ \pi(m-1) = 4,\ \pi(m-2) = 1,\ \pi(m-3) = 3$	$2c_1 = 0$ & $c_1 - 2c_2 = 0$	2^{m-3}
$\pi(1) = 2,\ \pi(2) = 3,\ \pi(3) = 1,\ \pi(4) = 4$	$2c_1 = 0$ & $c_1 - 2c_2 = 0$	2^{m-3}
$\pi(m) = 2,\ \pi(m-1) = 3,\ \pi(m-2) = 1,\ \pi(m-3) = 4$	$2c_1 = 0$ & $c_1 - 2c_2 = 0$	2^{m-3}

In other words, those sequences have a zero autocorrelation zone of length 2^{m-2}.

Proof 1 Note that $R_a(u) = R_a(n-u)$ for any u. So it is sufficient to prove

$$R_a(u) = \sum_{i=0}^{n-1} (-1)^{a_i - a_{i+u}} \tag{6.3}$$

is equal to zero for any $u \in \{k : 1 \leq k \leq 2^{m-2}\}$.

In the following, for any given $u \in \{k : 1 \leq k \leq 2^{m-2}\}$ and an integer i, set $j = i + u (\bmod\ n)$ and let $(i_1, i_2, \cdots, i_m)$ and $(j_1, j_2, \cdots, j_m)$ be the binary representations of i and j, respectively.

The set $\{i : 0 \le i < n\}$ can be divided into four disjoint subsets:

$$\begin{aligned}
I_1(u) &= \{0 \le i < n : i_{\pi(1)} = j_{\pi(1)}\}; \\
I_2(u) &= \{0 \le i < n : i_{\pi(1)} \ne j_{\pi(1)}, i_{\pi(m)} = j_{\pi(m)}\}; \\
I_3(u) &= \left\{0 \le i < n : \begin{array}{l} i_{\pi(1)} \ne j_{\pi(1)}, i_{\pi(2)} \ne j_{\pi(2)}, \\ i_{\pi(m)} \ne j_{\pi(m)} \end{array}\right\}; \\
I_4(u) &= \left\{0 \le i < n : \begin{array}{l} i_{\pi(1)} \ne j_{\pi(1)}, i_{\pi(2)} = j_{\pi(2)}, \\ i_{\pi(m)} \ne j_{\pi(m)} \end{array}\right\}.
\end{aligned}$$

First we will show that the subset $I_4(u)$ is an empty set. In this case, $i_{\pi(1)} \ne j_{\pi(1)}$ indicates that:

(i) $i_{\pi(1)} = 0$ and $j_{\pi(1)} = 1$; or

(ii) $i_{\pi(1)} = 1$ and $j_{\pi(1)} = 0$.

(i) In this case, one has $j > j_{\pi(1)}2^{m-1} = 2^{m-1} > i$ since $\pi(1) = 1$, $i_{\pi(1)} = 0$ and $j_{\pi(1)} = 1$, i.e., $j > i$. This together with $j - i \equiv u (\text{mod } n)$ indicates that $j = i + u$. While one also has

$$\begin{aligned}
i + u &< (i_{\pi(2)}2^{m-2} + 2^{m-2}) + 2^{m-2} \\
&= j_{\pi(1)}2^{m-1} + j_{\pi(2)}2^{m-2} \\
&\le j
\end{aligned}$$

i.e., $j > i + u$. This is a contradiction.

(ii) In this case, one has $i > i_{\pi(1)}2^{m-1} = 2^{m-1} > j$ since $\pi(1) = 1$, $i_{\pi(1)} = 1$ and $j_{\pi(1)} = 0$, i.e., $j < i$. This together with $j - i \equiv u \ (\text{mod } n)$ indicates that $j = i + u - n$. While one also has

$$\begin{aligned}
i + u &< (i_{\pi(1)}2^{m-1} + i_{\pi(2)}2^{m-2} + 2^{m-2}) + 2^{m-2} \\
&= i_{\pi(2)}2^{m-2} + 2^m \\
&= j_{\pi(2)}2^{m-2} + 2^m \\
&\le j + n
\end{aligned}$$

i.e., $j > i + u - n$. This is a contradiction with $j = i + u - n$.

By the discussion above, the set $I_4(u)$ is an empty set. Then the autocorrelation function $R_a(u)$ given by (6.3) can be written as

$$\begin{aligned} R_a(u) &= \sum_{i\in I_1(u)} (-1)^{a_i-a_j} + \sum_{i\in I_2(u)} (-1)^{a_i-a_j} \\ &\quad + \sum_{i\in I_3(u)} (-1)^{a_i-a_j}. \end{aligned} \tag{6.4}$$

Now we will show that

$$\sum_{i\in I_1(u)} (-1)^{a_i-a_j} = 0 \tag{6.5}$$

$$\sum_{i\in I_2(u)} (-1)^{a_i-a_j} = 0 \tag{6.6}$$

$$\sum_{i\in I_3(u)} (-1)^{a_i-a_j} = 0. \tag{6.7}$$

Proof of Equality (6.5).

Let $i \in I_1(u) = \{0 \le i \le n-1 : i_{\pi(1)} = j_{\pi(1)}\}$. Since $j \ne i$, we can define v as follows:

$$v = \min\{1 \le k \le m : i_{\pi(k)} \ne j_{\pi(k)}\}.$$

It is easy to show $v \ge 2$. Let i' and j' be two integers with binary representations defined by

$$i'_{\pi(k)} = \begin{cases} i_{\pi(k)}, & k \ne v-1 \\ 1 - i_{\pi(k)}, & k = v-1 \end{cases}$$

and

$$j'_{\pi(k)} = \begin{cases} j_{\pi(k)}, & k \ne v-1 \\ 1 - j_{\pi(k)}, & k = v-1 \end{cases}.$$

In other words, i' and j' are obtained from i and j by "flipping" the $(v-1)$-th bit in $(i_{\pi(1)}, \cdots, i_{\pi(m)})$ and $(j_{\pi(1)}, \cdots, j_{\pi(m)})$. It is easy to show that $j' - i' = j - i \equiv u (\text{mod } n)$. Let $I'_1(u)$ be the set of the set of corresponding $i \in I_1(u)$. Note that the following fact holds.

1) i' lies in the same range and also satisfies $i'_{\pi(1)} = j'_{\pi(1)}$.

2) The mapping from $I_1(u)$ to $I_1'(u)$ is a one-to-one mapping.

Hence we can conclude that $I_1(u) = I_1'(u)$.

Given i, j, i', j', we have

$$a_i - a_j - a_{i'} + a_{j'} = 1.$$

This equality indicates that $(-1)^{a_i - a_j}/(-1)^{a_{i'} - a_{j'}} = -1$, and then

$$(-1)^{a_i - a_j} + (-1)^{a_{i'} - a_{j'}} = 0.$$

In this way, the two terms will cancel each other. Hence we have $\sum_{i \in I_1(u)} (-1)^{a_i - a_j} = 0$.

Proof of Equality (6.6).

Let $i \in I_2(u) = \{0 \le i \le n-1 : i_{\pi(1)} \ne j_{\pi(1)}, i_{\pi(m)} = j_{\pi(m)}\}$. In this case, let i' and j' be the two integers with binary representations defined by

$$i'_{\pi(k)} = 1 - j_{\pi(k)}, \quad k = 1, \cdots, m$$

and

$$j'_{\pi(k)} = 1 - i_{\pi(k)}, \quad k = 1, \cdots, m.$$

Let $I_2'(u)$ be the set corresponding to $i \in I_2(u)$, using the same argument as case $i \in I_1(u)$, we can obtain the following.

1) $i'_{\pi(1)} \ne j'_{\pi(1)}, i'_{\pi(m)} = j'_{\pi(m)}$, and $j' - i' = j - i \equiv u \pmod{n}$.

2) $I_2(u) = I_2'(u)$.

3) $(-1)^{a_i - a_j} + (-1)^{a_{i'} - a_{j'}} = 0$.

Hence equality (6.6) holds.

Proof of Equality (6.7).

Let $i \in I_3(u) = \{0 \le i \le n-1 : i_{\pi(1)} \ne j_{\pi(1)}, i_{\pi(2)} \ne j_{\pi(2)}, i_{\pi(m)} \ne j_{\pi(m)}\}$. In this case, let i' and j' be two integers with binary representations defined by

$$i'_{\pi(k)} = \begin{cases} j_{\pi(k)}, & k = 1 \\ 1 - j_{\pi(k)}, & k \ne 1 \end{cases}$$

and

$$j'_{\pi(k)} = \begin{cases} i_{\pi(k)}, & k = 1 \\ 1 - i_{\pi(k)}, & k \neq 1. \end{cases}$$

Let $I'_3(u)$ be the set corresponding to $i \in I_3(u)$, also using the same argument as case $i \in I_1(u)$, we get the following.

1) $i'_{\pi(1)} \neq j'_{\pi(1)}, i'_{\pi(2)} \neq j'_{\pi(2)}, i'_{\pi(m)} \neq j'_{\pi(m)}$, and $j' - i' \equiv j - i \equiv u \pmod{n}$.

2) $I_3(u) = I'_3(u)$.

3) $(-1)^{a_i - a_j} + (-1)^{a_{i'} - a_{j'}} = 0$.

Hence we have that equality (6.7) holds.

By equalities (6.5)-(6.7), $R_a(u)$ given by (6.3) is equal to zero.

6.4 Examples

In this section, we'll use empirical results to demonstrate these three categories of ZACZ. The autocorrelations of 6 Golay sequences labeled by $A_1, \cdots, A_6$ are plotted in Figures 6.4 - 6.7. These data are further generalized into Table 6.3.

The sequences A_1, A_3 and A_5 are binary Golay sequences, which implies H in (6.1) is 2. Maintaining the same permutations and affine transformations, by changing H from 2 to 4, we obtain 3 quaternary Golay sequences in A_2, A_4 and A_6. Note that for the figures of quaternary Golay sequences, autocorrelations are graphed in the form of magnitude, because they contain both real and imaginary parts. We can observe that all 6 sequences contain a large ZACZ. Moreover, each quaternary Golay sequence has exactly the same ZACZ trend as its corresponding binary case. A_1 and A_2 have a ZACZ of length 2^{m-2} around the two sides of the origin. These 2 examples fall under Theorem 2. A_3 and A_4 have a ZACZ of length 2^{m-2} in the middle. They fall under Theorem 3. A_5 and A_6 have a ZACZ of length 2^{m-3} around the origin and 2^{m-2} in the middle. These 2 examples fall under Theorem 4.

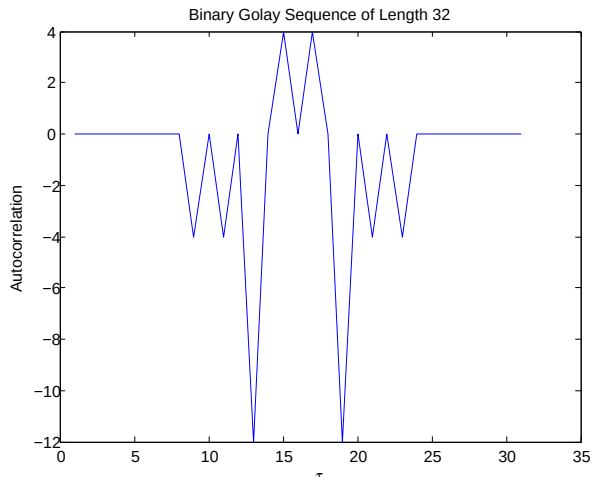

Figure 6.4: The autocorrelation of A_1

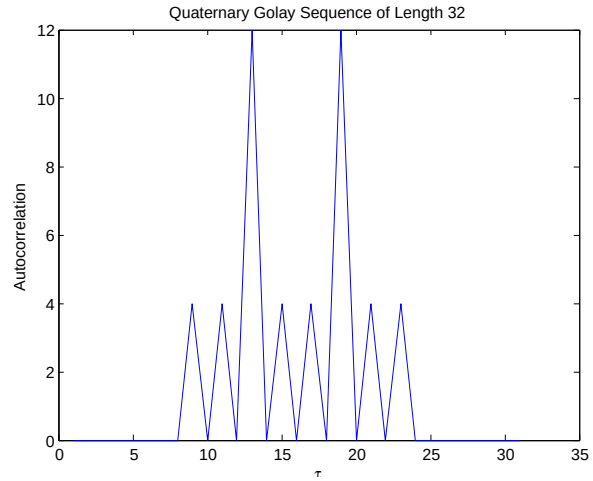

Figure 6.5: The autocorrelation of A_2

6.5 Summary and Discussions

In this chapter, we have shown a class of H-ary GDJ Golay sequences with selected permutations π and affine transformations $\sum_{k=1}^{m} c_k i_k$, of which contains large ZACZ of length 2^{m-2}, where $H \geq 2$ is an even integer. Any H-ary GDJ Golay sequences a belong to this

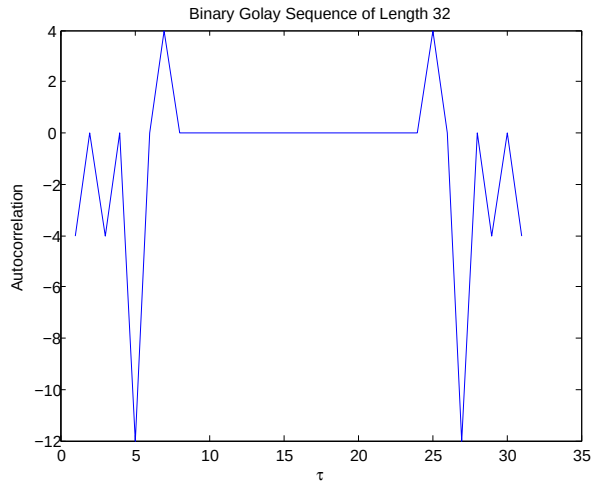

Figure 6.6: The autocorrelation of A_3

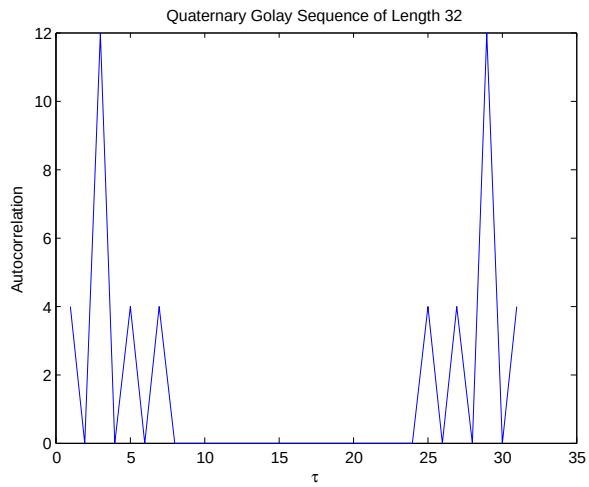

Figure 6.7: The autocorrelation of A_4

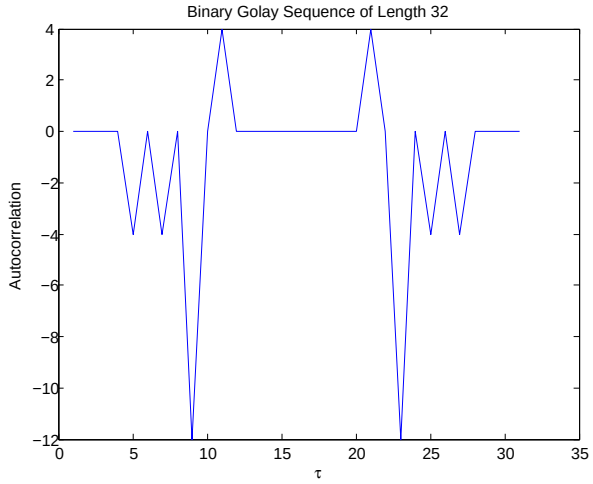

Figure 6.8: The autocorrelation of A_5

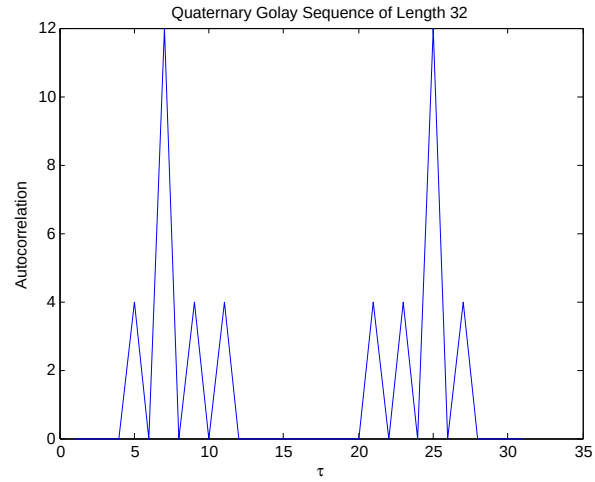

Figure 6.9: The autocorrelation of A_6

Table 6.3: Examples of binary or quaternary Golay sequences of length 32 and their Autocorrelation

Condition	$\pi = (1)$, $(c_0, c_1, c_2, c_3, c_4, c_5) = (0, 0, 1, 1, 0, 0)$, $H = 2$
Sequence	$A_1 = (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$
$\{R_{A_1}(\tau)\}_1^{31}$	$(0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, -12, 0, 4, 0, 4, 0, -12, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0)$
Condition	$\pi = (1)$, $(c_0, c_1, c_2, c_3, c_4, c_5) = (0, 0, 1, 1, 0, 0)$, $H = 4$
Sequence	$A_2 = (0, 0, 0, 2, 1, 1, 3, 1, 1, 1, 1, 3, 0, 0, 2, 0, 0, 0, 0, 2, 1, 1, 3, 1, 3, 3, 3, 1, 2, 2, 0, 2)$
$\{R_{A_2}(\tau)\}_1^{31}$	$(0, 0, 0, 0, 0, 0, 0, 0, 4j, 0, 4j, 0, 12j, 0, -4j, 0, 4j, 0, -12j, 0, -4j, 0, -4j, 0, 0, 0, 0, 0, 0, 0, 0)$
Condition	$\pi = (12)$, $(c_0, c_1, c_2, c_3, c_4, c_5) = (0, 0, 0, 0, 0, 1)$, $H = 2$
Sequence	$A_3 = (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$
$\{R_{A_3}(\tau)\}_1^{31}$	$(-4, 0, -4, 0, -12, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, -12, 0, -4, 0, -4)$
Condition	$\pi = (12)$, $(c_0, c_1, c_2, c_3, c_4, c_5) = (0, 0, 0, 0, 0, 1)$, $H = 4$
Sequence	$A_4 = (0, 1, 0, 3, 0, 1, 2, 1, 0, 1, 0, 3, 0, 1, 2, 1, 0, 1, 0, 3, 2, 3, 0, 3, 2, 3, 2, 1, 0, 1, 2, 1)$
$\{R_{A_4}(\tau)\}_1^{31}$	$(4j, 0, 12j, 0, -4j, 0, 4j, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4j, 0, 4j, 0, -12j, 0, -4j)$
Condition	$\pi = (23)$, $(c_0, c_1, c_2, c_3, c_4, c_5) = (0, 0, 0, 0, 0, 1)$, $H = 2$
Sequence	$A_5 = (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$
$\{R_{A_5}(\tau)\}_1^{31}$	$(0, 0, 0, 0, -4, 0, -4, 0, -12, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, -12, 0, -4, 0, -4, 0, 0, 0, 0)$
Condition	$\pi = (23)$, $(c_0, c_1, c_2, c_3, c_4, c_5) = (0, 0, 0, 0, 0, 1)$, $H = 4$
Sequence	$R_6 = (0, 1, 0, 3, 0, 1, 0, 3, 0, 1, 2, 1, 2, 3, 0, 3, 0, 1, 0, 3, 2, 3, 2, 1, 0, 1, 2, 1, 0, 1, 2, 1)$
$\{R_{A_6}(\tau)\}_1^{31}$	$(0, 0, 0, 0, 4j, 0, 12j, 0, -4j, 0, 4j, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4j, 0, 4j, 0, -12j, 0, -4j, 0, 0, 0, 0)$

class can be generalized into following 3 cases:

1. $R_a(u) = 0, \quad u \in (0, 2^{m-2}] \cup [3 \cdot 2^{m-2}, 2^m)$.
2. $R_a(u) = 0, \quad u \in [2^{m-2}, 3 \cdot 2^{m-2}]$.
3. $R_a(u) = 0, \quad u \in (0, 2^{m-3}] \cup [3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}] \cup [7 \cdot 2^{m-3}, 2^m)$.

Golay sequences with this property can have wide implications in many areas. Potential applications include system synchronization, channel estimation and used to construct signal set. This can be briefly illustrated as follows.

Synchronization: The synchronization of the signal is equivalent to computing its own autocorrelations [25, 45]. If the signal delay does not exceed of the ZACZ, then early synchronization or late synchronization will introduce no interference to the system. There will only be a peak value at the origin (i.e., correct synchronization). Thus the synchronization of system can be achieved.

Channel Estimation : Golay sequences with large ZACZ property can be used as pilot signals for channel estimation purposes in an LTI system. The relationship between input $x(t)$, channel impulse repones $h(t)$ and received signal $y(t)$ and white Gaussian noise $n(t)$ is given by [25]

$$y(t) = x(t) \otimes h(t) + n(t) \tag{6.8}$$

where $\otimes$ is the convolution operator. Once synchronization of signal is achieved as explained above using its large ZACZ property, then the received signal $y(t)$ can be accurately recovered. Note from (6.8), we have The approximated channel impulse response is:

$$\begin{aligned} Y(f) &= X(f)H(f) + N(f) \\ \frac{Y(f)}{X(f)} &= H(f) + \frac{N(f)}{X(f)} \end{aligned}$$

where $X(f)$, $Y(f)$ and $N(f)$ are the Fourier transforms of $x(t)$, $y(t)$ and $n(t)$ respectively.

Therefore, the approximated channel response $\hat{h}(t)$ is:

$$\hat{h}(t) \approx \mathcal{F}^{-1} \frac{Y(f)}{X(f)}$$

where $\mathcal{F}^{-1}$ is the inverse Fourier transform operator.

Construct Signal Set : Another possible application of Golay sequences with large ZACZ is that it can be used to construct spreading sequence sets for CDMA systems. This will be a future research work.

Chapter 7

Conclusions and Future Work

7.1 Conclusions

The trend in the development of wireless technologies of in the past decade is primarily driven by the desire for higher data rate. With increased data rate, conventional SC broadband wireless systems suffers high ISI. This can degrade the system performance considerably. MC systems is a plausible alternative to SC systems that would alleviate the high ISI problem. However, it will introduce high PMEPR. In this thesis, we have conducted simulations to examine PMEPR and merit factor of new sequences as well as sone other known construction of sequences.

Furthermore, In the design for CDMA spreading sequence sets, sequences with 2 properties are desired.

1. Low autocorrelations
2. Sequences within the same set have low cross-correlations

We have also presented a class of GDJ Golay sequences with large ZACZ property, which could potentially be used to construct CDMA spreading sequences sets. The main contributions of this thesis are summarized as follows.

1. PMEPR behaviours and merit factor properties of 6 single sequences are examined. They are m sequences, Sidelnikov sequences, New sequences, Golay sequences, FZC sequences and Legendre sequences. The length of each sequence is varied by removing

or appending some bits to observe the change in PMEPR and merit factor of these sequences. Furthermore, we also performed the rotations on the sequences to observe its effect on the merit factor values.

(a) **PMEPR:** In general, polyphase FZC sequences have the best PMEPR performances when the entire sequence is retained or a portion of bits is removed. Binary Golay sequences behave very well only when the entire sequence is retained. PMEPR of all the other 4 sequences grow linearly with the sequence length.

(b) **Merit Factor:** In general, Polyphase FZC sequences have the maximum merit factor values. However, they tend to deteriorate very rapidly when some bits are removed or appended. m sequences, Sidelnikov and Golay sequences have very similar merit factor performances at approximately 3. Legendre sequences have merit factor value at approximately 1.5. However, cyclical rotations of Legendre sequences can improve this value to 6. New sequences have the merit factor values at about 1, the lowest of all sequences.

2. PMEPR behaviours of 6 spreading sequence sets are also examined. They are m spreading sequences, Sidelnikov spreading sequences, New spreading sequences, Golay spreading sequences, FZC spreading sequences and DFT spreading sequences. In general, FZC spreading sequences has the best PMEPR performance when the number of sequences L in the set is small. On the contrary, DFT spreading sequences has the worst PMEPR value at smaller L. This is because FZC spreading sequences have ideal periodic autocorrelation properties, while DFT spreading sequences have ideal cross-correlation properties. All 6 sequences converge to within a few dB of each other as L increases.

3. A loose bound between PMEPR and merit factor is derived using Cauthy-Schwarz's inequality. Although both theoretical and simulation results have showed that this is not a tight bound. Nevertheless, it gives us some indications on the relationship between PMEPR and merit factor.

4. A new finding on a class of GDJ Golay sequences with large ZACZ over alphabets $\mathbb{Z}_H$ is presented, where H is a positive even integer. With selected permutation and affine transformations, Golay sequences with large ZACZ properties can be divided into 3 following cases:

   (a) $R_a(u) = 0, \quad u \in (0, 2^{m-2}] \cup [3 \cdot 2^{m-2}, 2^m)$.

   (b) $R_a(u) = 0, \quad u \in [2^{m-2}, 3 \cdot 2^{m-2}]$.

(c) $R_a(u) = 0, \quad u \in (0, 2^{m-3}] \cup [3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}] \cup [7 \cdot 2^{m-3}, 2^m)$.

Sequences with large ZACZ centered at the origin can be explored during the detection at the receiver side. Moreover, they can potentially be used to construct spreading sequence sets for CDMA systems.

7.2 Future Work

With the advancement of technologies come new challenges. There are much to be done in this area of research. The followings are a few possible extensions.

1. **Effective Coding and Decoding Scheme:** We have showed PMEPR behaviours of several known constructions of sequences in Chapter 4. However, we haven't presented a feasible encoding and decoding schemes such that information bits can be encoded into a sequence with known PMEPR values, and coded bits can be synchronized and decoded back to information bits at the receiver side. All of these require extensive work.

2. **Code Rate:** In Chapter 4, we have discussed that Golay sequences have a PMEPR of at most 2. This is an excellent property. However, Golay sequences occur as $m!/2$ cosets of $RM_2^h(1, m)$, where m is the number of variables. Let 2^w be the largest integer that is a power of 2 and no greater than $m!/2$. The proposed coding scheme in [10] maps $w + h(m+1)$ information bits over alphabets $\mathbb{Z}_2^h$ to $2^m h$ coded bits. The code rate thus is $\frac{(w+h(m+1))}{2^m h}$. It approaches $\frac{m}{2^m}$ as m approaches ∞. This is not an acceptable rate to be adopted by any broadBand wireless communication standards. More work can be done in search for higher code rate, while keeping the receiver structure relatively simple, as well as maintaining PMEPR at a low level.

3. **Simulating in a Communication Environment:** Once we have a viable encoding and decoding schemes, we can simulate the transmitted and received signals in an environment using software defined radio. We then will be able determine the performance of our proposed schemes in the presence of fading and noise. Furthermore, we can compare our schemes with the current schemes adopted by different standards.

4. **Incorporate MIMO:** Ever since the introduction of MIMO into IEEE 802.11n, it has become an integral part of today's wireless communication standard. The use of multiple antennas at both the transmitter and receiver can

(a) Offer higher data throughput.

(b) Provide link reliability and/or diversity.

Therefore, MIMO should be taken into considerations when designing a coded OFDM scheme.

5. **Cross Correlation of Golay Sequences:** The design of spreading sequence sets for CDMA system requires that each sequence should have low autocorrelation and low cross-correlation with other sequences within the same set. In this thesis, we have presented a class of Golay sequences with large ZACZ centered at the origin. If these sequences also inherit low cross-correlation within this class, then they can potentially be used to construct spreading sequences for CDMA systems.

Appendix A

Specifications of Different Generations of Cellular and Wireless LAN Standards

Table A.1: First-Generation analog cellular phone standards

Parameter	AMPS	TACS	NMT(450/900)	NTT	C-450	RC2000
Uplink Frequencies			453-458			
(MHz)	$824-849$	$890-915$	$/890-915$	$925-940^a$	$450-455.74$	$414.8-418^b$
Downlink Frequencies			463-468			
(MHz)	$869-894$	$935-960$	$/935-960$	$870-885$	$460-465.74$	$424.8-428$
Modulation	FM	FM	FM	FM	FM	FM
Channel Spacing(kHz)	30	25	25/12.5	25	10	12.5
Number of Channels	832	1000	180/1999	600	573	256
Multiple Access	FDMA	FDMA	FDMA	FDMA	FDMA	FDMA

[a] NTT also operated in several other frequency bands around 900 MHz.
[b] RC2000 also operated in several other frequency bands around 200 MHz.

Table A.2: Second-Generation analog cellular phone standards

Parameter	GSM	IS-136	IS-95(cdmaOne)	PDC
Uplink Frequencies(MHz)	$890-915$	$824-849$	$824-849$	$940-956$, $1429-1453$
Downlink Frequencies(MHz)	$935-960$	$869-894$	$869-894$	$810-826$, $1477-1501$
Carrier Separation(kHz)	200	30	1250	25
Number of Channels	1000	832^a	~ 2500	1600^a
Modulation	$GMSK$	$\pi/4-DQPSK$	$BPSK/QPSK$	$\pi/4-DQPSK$
Channel Spacing(kHz)	30	25	25/12.5	25
Number of Channels	832	1000	180/1999	600
Multiple Access	FDMA	FDMA	FDMA	FDMA

[a] 3 users per channel.

Table A.3: Second-Generation digital cellular phone standards

Parameter	GSM	IS-136	IS-95(cdmaOne)	PDC
Uplink Frequencies(MHz)	$890-915$	$824-849$	$824-849$	$940-956$, $1429-1453$
Downlink Frequencies(MHz)	$935-960$	$869-894$	$869-894$	$810-826$, $1477-1501$
Carrier Separation(kHz)	200	30	1250	25
Number of Channels	1000	832^a	~ 2500	1600^a
Modulation	$GMSK$	$\pi/4-DQPSK$	$BPSK/QPSK$	$\pi/4-DQPSK$
Channel Spacing(kHz)	30	25	25/12.5	25
Number of Channels	832	1000	180/1999	600
Multiple Access	FDMA	FDMA	FDMA	FDMA

[a] 3 users per channel.

Table A.4: Third-Generation digital cellular phone standards

	cdma2000				W-CDMA		
Parameter	1X	1XEV-DO	1XEV-DV	3X	UMTS	FOMA	J-phone
Channel Bandwidth(MHz)	1.25	1.25	1.25	3.75	5	5	5
Chip Rate(Mchips/s)	1.2288	1.2288	1.2288	3.6864	3.84	3.84	3.84
Peak Data Rate(Mbps)	.144	2.4	4.8	$5-8$	2.4^a	2.4^a	2.4^a
Modulation	QPSK/MPSK(DL), BPSK/QPSK(UL)				QPSK(DL), BPSK(UL)		
8-10 Mbps with HSDPA							

Table A.5: 802.11 wireless LAN link layer standards

Parameter	802.11	802.11a	802.11b	802.11g	802.11n
Bandwidth(MHz)	83.5	300	83.5	83.5	83.5 @ 2.4GHz 300 @ 5GHz
Frequency Range(GHz)	$2.4 - 2.4835$	$5.15 - 5.25$ $5.25 - 5.35$ $5.725 - 5.825$	$2.4 - 2.4835$	$2.4 - 2.4835$	$2.4 - 2.4835$ $5.15 - 5.25$ $5.25 - 5.35$ $5.725 - 5.825$
Number of Channels	3	12(4 per subband)	3	3	
Modulation	BPSK, QPSK DSSS, FHSS	BPSK, QPSK MQAM OFDM	BPSK, QPSK DSSS	BPSK, QPSK MQAM, OFDM	BPSK, QPSK MQAM, OFDM
Max Data Rate(Mbps)	2	54	11	54	144.4 @ 20MHz 300 @ 40MHz

References

[1] M. Antweiler and L. Bomer. Merit factor of chu and frank sequences. *IEEE Elec. Lett.*, 26(25):2068–2070, Dec. 1990. 33

[2] J. Armstrong. Peak-to-average power reduction for ofdm by repeated clipping and frequency domain filtering. *IEEE Elect. Lett.*, 38(8):246–247, Feb. 2002. 20

[3] R.W. Baüml, R.F.H. Fisher, and J.B. Huber. Reducing the peak-to-average power ratio of multicarrier modulation by selected mapping. *IEEE Elect. Lett*, 32(22):2056–2057, Oct. 1996. 20

[4] P. Borwein, K.-K.S. Choi, and J. Jedwab. Binary sequences with merit factor greater than 6.34. *IEEE Trans. Inform. Theory*, 45:2397–2417, 2004. 22, 34, 35

[5] R.W Chang. Synthesis of band-limited orthogonal signals for multichannel data transmission. *Bell Sys Tech J*, 45:1775–1796, 1966. 15

[6] R.W. Chang. Orthogonal frequency division multiplexing. *U.S. Patent no. 3488445*, 1970. 15

[7] C.V. Chong and V. Tarokh. A simple encodable/decodable ofdm qpsk code with low peak-to-mean envelope power ratio. *IEEE Trans. Info. Theory*, 47(7):3025–3029, 2001. 20

[8] D.C. Chu. Polyphase codes with good periodic correlation properties. *IEEE Trans. Inform. Theory*, IT-18:531–533, 1972. 13

[9] J.A. Davis and J. Jedwab. Peak-to-mean average control and error correction for ofdm transmission using golay sequences and reed-muller codes. *IEEE Elect. Lett.*, 33(4):267–268, Feb. 1997. 20

[10] J.A. Davis and J. Jedwab. Peak-to-mean power control in ofdm, golay complementary sequences, and reed-muller codes. *IEEE Trans. Info. Thoery*, 45(7):2397–2417, Nov. 1999. 12, 20, 48, 49, 65

[11] X.M. Deng and P.Z. Fan. Spreading sequences sets with zero correlation zone. *Electron. Lett*, 36(11):993–994, 2000. 49

[12] N. Dinur and D. Wulich. Peak to average power ratio in high-order ofdm. *IEEE Trans. Commun.*, 49:1063–1072, 2002. 20

[13] P. Van Eetvelt, G. Wade, and M. Tomlinson. Peak to average power reduction for ofdm schemes by selective scrambling. *IEEE Elect. Lett.*, 32(21):1963–1964, Oct. 1996. 20

[14] P.Z Fan and L. Hao. Generalized orthogonal seuqences and their applications in synchronous cdma system. *IEICE. Trans. Fundam.*, E83-A(11):1–16, 2000. 49

[15] R.L. Frank and S.A. Zadoff. Phase shift pulse codes with good periodic correlation properties. *IRE Trans. Inform. Theory*, IT-8:381–382, 1962. 13

[16] M. Friese. On the achievable information rate with peak-power-limited orthogonal frequency-division multiplexing. *IEEE Trans. Inform. Thoery*, 46:2579–2587, 2000. 20

[17] M.J.E. Golay. Complementary series. *IRE Trans. Inform. Theory*, IT-7(2):82–87, Apr. 1961. 48

[18] M.J.E. Golay. A class of finite binary sequences with alternate autocorrelation values equal to zero. *IEEE Trans. Inform. Theory*, IT-18:449–450, 1972. 33

[19] A. Goldsmith. *Wireless Communications*. Cambridge University Press, 2005. 1, 2, 3

[20] S.W. Golomb and G. Gong. *Signal Designs for Good Coorelation*: *For Wireless Communication, Cryptography, and Radar*. Cambridge University Press, Cambridge, U.K, 2005. 6, 7, 8, 48

[21] G. Gong, F. Huo, and Y. Yang. Large zero autocorrelation of golay sequences. *IEEE Globe Communications Conference*, 2011. Submitted. 53

[22] L. Hanzo, C.H. Wong, and M.S. Yee. *Adaptive Wireless Transceivers*. John Wiley & Sons. Ltd, 2002. 15

[23] T. Hayashi. Binary sequences with orthogonal subsequences and a zero-correlation zone: Pair-preserving shuffled sequences. *IEICE Trans. Fundam*, E85-A(6):1420–1425, 2002. 49

[24] T. Hayashi. A generalization of binary zero-correlation zone sequence sets constructed from hadamard matrices. *IEICE Trans. Fundam.*, E87-A(1):559–565, 2004. 49

[25] S. Haykin and M. Moher. *Communication Systems*. John Wiley & Sons, 2009. 61

[26] G.R. Hill, M. Faulkner, and J. Singh. Reducing the peak-to-average power ratio in ofdm by cyclically shifting partial transmit sequences. *IEEE Elect. Lett.*, 36(6):560–561, Mar. 2000. 20

[27] T. Høholdt and H.E. Jensen. Determination of the merit factor of legendre sequences. *IEEE Trans. Inform. Theory*, 34:161–164, 1988. 34

[28] H.G. Hu and G. Gong. New sets of zero or low correlation zone sequences via interleaving techniques. *IEEE Trans. Inform. Theory*, 56(4):1702–1713, Apr. 2004. 49

[29] IEEE-SA. *IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 2007 revision edition, 2007. 3

[30] A.D.S. Jayalath and C. Tellambura. Reducing the peak-to-average power ratio of orthogonal frequency division multiplexing signal through bit or symbol interleaving. *IEEE Elect. Lett.*, 36(13):1161–1163, June 2000. 20

[31] J. Jedwab. A survey of the merit factor problem for binary sequences. *Sequences and their Applications - SETA 2004*, pages 30–55, 2005. 34

[32] J. Jedwab and K.-U. Schmidt. Appended m-sequences with merit factor greater than 3.34. *Sequences and their Applications - SETA 2010*, pages 204–216, 2010. 22, 34

[33] X. Li and Jr. L.J. Cimini. Effect of clipping and filtering on the performance of ofdm. *IEEE Commun. Lett.*, 2(5):131–133, May. 1998. 20

[34] S. Litsynh. *Peak Power Control in Multiarrier Communications*. Cambridge University Press, 2007. 19, 20

[35] J.E. Littlewood. On polynomials $\sum^n \pm z^m, \sum^n \exp^{\alpha_m i} z^m, z = \exp^{\theta i}$. *J. London Math.Soc.*, 41:367–376, 1966. 34

[36] J.E. Littlewood. *Some Problems in Real and Complex Analysis*. Heath Mathematical Monographs. D.C. Heath and Company, 1968. 33

[37] B. Long, P. Zhang, and J. Hu. A generalized qs-cdma system and the design of new spreading codes. *IEEE Trans. Veh. Tech.*, 47:1268–1275, 1998. 49

[38] S.H. Müler and J.B. Huber. A comparison of peak power reduction schemes for ofdm. *Proc. IEEE GLOBECOM 97*, pages 1–5, Nov. 1997. 20

[39] E. Mustafa. *Mobile broadband: including WiMAX and LTE*. Springer Verlag, 2009. 1, 4

[40] D.J. Newman and J.S. Byrnes. The l^4 norm of a polynomail with coefficients ± 1. *Amer. Math. Monthly*, 97:42–45, 1990. 34

[41] H. Ochinai and H. Imai. On the distribution of the peak to average power ratio in ofdm signals. *IEEE Trans. Commun.*, 49:282–289, 2001. 20, 35

[42] K.G Paterson. Generalized reed-muller code and power control for ofdm modulation. *IEEE Trans. Info. Thoery*, 46(1):104–120, Feb. 2000. 12, 20, 49

[43] K.G Paterson and V. Tarokh. On the existence and construction of good codes with low peak-to-average power ratios. *IEEE Trans. Info. Theory*, 46(6):1974–1987, Sep. 2000. 20

[44] B.M. Popović. Generalized chirp-like polyphase sequences with optimum correlation properties. *IEEE Trans. Inform. Theory*, 38(4):1406–1409, July 1992. 13

[45] M.B. Pursley. *Introduction to Digital Communications*. Pearson Prentice Hall, 2005. 61

[46] A. Rathinakumar and A.K. Chaturvedi. A new framework for constructing mutually orthogonal complementary sets and zcz sequences. *IEEE Trans. Inform. Theory*, 52(8):3817–3826, Aug. 2006. 49

[47] A. Rathinakumar and A.K. Chaturvedi. Ieee. trans. inform. theory. *Complete mutually orthogonal Golay complementary sets from Reed-Muller codes*, 54(3):1339–1346, Mar. 2008. 49

[48] J.R. Seberry, B.J. Wysocki, and T.A. Wysocki. On a use of golay sequences for asynchronous ds cdma applications. *Adavanced Signal Processing for Communication Systems The International Series in Engineering and Computer Science*, 703:183–196, 2002 2002. 48

[49] M. Sharif and B. Hassibi. On multicarrier signals where the pmepr of a random codeword is asymptotically *logn*. *IEEE Trans. Info. Thoery*, 50(5):895–903, 2004. 20, 35

[50] N. Suehiro and M. Hatori. Modulatable orthogonal sequences and their application on ssma systems. *IEEE Trans. Inform. Theory*, 34(1):93–100, Jan 1988. 13

[51] X.H. Tang, P.Z Fan, and S. Matsufuji. Lower bounds on the maximum correlation of sequence set with low or zero correlation zone. *Electron. Lett*, 36:551–552, Mar. 2000. 49

[52] X.H. Tang and W.H. Mow. Design of spreading codes for quasisynchronous cdma with intercell interference. *IEEE. J. Sel. Areas. Commun.*, 24(1):84–93, Jan. 2006. 49

[53] R.D.J. van Nee. Ofdm codes for peak-to-average power reduction and error correction. *in Proc. IEEE GLOBECOM*, pages 740–744, Nov. 1996. 48

[54] Z. Wang and G. Gong. New sequences design from weil representation with low two-dimensional correlation in both time and phase shifts. *Technical Report, CACR 2009-01. Poster presentation at IEEE International Symposium on Information Theory (ISIT) 2009. To appear in the IEEE Transactions on Information Theory*, Jan. 2009. 21

[55] S. Wei, D. Goeckel, and P. Kelly. A modern extreme value theory approach to calculating the distribution of the peak to average power ratio in ofdm systems. *Proc. IEEE Int. Communications Conf.*, pages 1686–1690, 2002. 20, 35

[56] Wikipedia. Orthogonal frequency-division multiplexing, May 2011. 17

[57] T.A. Wilkinson and A.E. Jones. Minimization of the peak to mean envelope power ratio of multicarrier transimission schemes by block coding. *in Proc. IEEE 45th Vehicular Technology Conf.*, pages 825–829, Jul. 1995. 48

[58] T.A. Wilkinson and A.E. Jones. Combined coding for error control and increased robustness to system nonlinearities in ofdm. *in Proc. IEEE 46th Vehicular Technology Conf.*, pages 904–908, 1996. 48

[59] D. Wulich. Reductin of peak to mean ratio of multicarrier modulation using cyclic coding. *Electron. Lett*, 32:432–433, 1996. 48

[60] D. Wulich, N. Dinur, and A. Glinowiecki. Level clipped high-order ofdm. *IEEE Trans. Commun.*, 48:928–930, 2000. 20

[61] G. Wunder and H. Boche. Upper bounds on the statistical distribution of the crest factor in ofdm transmission. *IEEE Trans. Info. Thoery*, 49:488–494, 2003. 20

[62] Y. Yang, F. Huo, and G. Gong. Autocorrelation and large zero autocorrelation zone of golay sequencess. Preprint. 49, 53

[63] N.Y Yu and G. Gong. New construction of m-ary seuqence families with low correlation from the structure of sidelnikov sequences. *IEEE Trans. Info. Thoery*, 56(8):4061–4070, Aug. 2010. 12

[64] Z.C. Zhou, X.H. Tang, and G. Gong. A new class of sequences with zero or low correlation zone based on interleaving technique. *IEEE Trans. Inform. Theory*, 54(9):4267–4273, Apr. 2008. 49